

Министерство науки и высшего образования Российской Федерации  
Федеральное государственное бюджетное  
образовательное учреждение высшего образования  
«ПЕРМСКИЙ ГОСУДАРСТВЕННЫЙ  
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ»

**А. А. Волочков**

# **КОНЕЧНЫЕ ГРУППЫ**

## **ВВЕДЕНИЕ В ТЕОРИЮ**

**Часть 1**

*Допущено методическим советом  
Пермского государственного национального  
исследовательского университета в качестве  
учебного пособия для студентов, обучающихся  
по направлению подготовки бакалавров  
«Математика»*



Пермь 2018

УДК 512.542  
ББК 22.144  
В68

**Волочков А. А.**

В68 Конечные группы. Введение в теорию [Электронный ресурс]: учеб. пособие / А. А. Волочков; Перм. гос. нац. исслед. ун-т. – Электрон. дан. – Пермь, 2018. – Ч. 1. – 1 Мб; 132 с. – Режим доступа: <http://www.psu.ru/files/docs/science/books/uchebnie-posobiya/volochkov-konechnye-gruppy-ch-1.pdf>. – Загл. с экрана.

ISBN 978-5-7944-3153-7

ISBN 978-5-7944-3154-4 (Ч. 1)

Пособие соответствует программе курса «Конечные группы». Излагаются основы теории конечных групп: группы, их гомоморфизмы, основные теоремы о них, нормальные подгруппы, минимальные нормальные подгруппы, композиционные ряды и теорема Жордана Гельдера, действия групп на множествах и перестановочные представления, их характеры, теорема Бернсайда, прямые и декартовы произведения, полупрямые произведения, сплетения, их стандартные действия, скрученные сплетения.

Издание предназначено для студентов, обучающихся на механико-математических факультетах.

**УДК 512.542**  
**ББК 22.144**

*Издается по решению ученого совета механико-математического факультета  
Пермского государственного национального исследовательского университета*

*Рецензенты:* кафедра «Высшая математика» Пермского национального исследовательского политехнического университета (зав. кафедрой – д-р физ.-мат. наук, профессор **А. Р. Абдуллаев**); д-р физ.-мат. наук, профессор, зав. кафедрой алгебры и математической логики Ярославского государственного университета им. П. Г. Демидова **Л. С. Казарин**

ISBN 978-5-7944-3153-7

ISBN 978-5-7944-3154-4 (Ч. 1)

© ПГНИУ, 2018

© Волочков А. А., 2018

# Оглавление

|          |                                                 |           |
|----------|-------------------------------------------------|-----------|
| <b>1</b> | <b>Введение</b>                                 | <b>5</b>  |
| 1.1      | Группоиды и моноиды . . . . .                   | 5         |
| 1.2      | Группы . . . . .                                | 12        |
| 1.3      | Кольца, модули, алгебры . . . . .               | 15        |
| 1.4      | Подгруппы . . . . .                             | 25        |
| 1.5      | Нормальные подгруппы . . . . .                  | 29        |
| 1.6      | Морфизмы . . . . .                              | 34        |
| 1.7      | Аutomорфизмы . . . . .                          | 43        |
| 1.8      | Композиционные ряды . . . . .                   | 48        |
| <b>2</b> | <b>Действия групп на множествах</b>             | <b>52</b> |
| 2.1      | Первые определения . . . . .                    | 52        |
| 2.2      | Орбиты . . . . .                                | 62        |
| 2.3      | Теорема Лагранжа . . . . .                      | 65        |
| 2.4      | Стабилизатор точки . . . . .                    | 68        |
| 2.5      | Транзитивные действия . . . . .                 | 73        |
| 2.6      | Характеры действий . . . . .                    | 80        |
| 2.7      | Лемма Бернсайда . . . . .                       | 82        |
| 2.8      | Действия и факторизации . . . . .               | 86        |
| <b>3</b> | <b>Коммутаторы</b>                              | <b>89</b> |
| <b>4</b> | <b>Основные теоретико-групповые конструкции</b> | <b>95</b> |
| 4.1      | Прямые произведения . . . . .                   | 95        |
| 4.2      | Минимальные нормальные подгруппы . . . . .      | 102       |
| 4.3      | Действия групп на группах . . . . .             | 105       |
| 4.4      | Полупрямые произведения . . . . .               | 106       |
| 4.5      | Сплетения . . . . .                             | 111       |

|          |                                            |            |
|----------|--------------------------------------------|------------|
| 4.6      | Действия сплетений на множествах . . . . . | 120        |
| 4.6.1    | Действие сплетения на парах . . . . .      | 121        |
| 4.6.2    | Действие сплетения на функциях . . . . .   | 121        |
| <b>5</b> | <b>Приложение</b>                          | <b>123</b> |
| 5.1      | Декартовы произведения . . . . .           | 123        |
| 5.2      | Отношения эквивалентности . . . . .        | 128        |
| 5.3      | Отношения порядка . . . . .                | 130        |
| 5.4      | Категории . . . . .                        | 131        |

# Глава 1

## Введение

### 1.1 Группоиды и моноиды

**Пример 1.1.1.** Пусть  $G$  — одно из следующих множеств:

- множество натуральных чисел  $\mathbb{N}$ ;
- множество целых чисел  $\mathbb{Z}$ ;
- множество рациональных чисел  $\mathbb{Q}$ ;
- множество вещественных чисел  $\mathbb{R}$ ;
- множество комплексных чисел  $\mathbb{C}$ ;
- множество кватернионов  $\mathbb{H}$ ;
- множество октав  $\mathbb{O}$ ;
- множество  $M_{m,n}(R)$  матриц  $m \times n$  с элементами в одном из предыдущих множеств  $R$ ;
- множество  $M_n(R)$  матриц  $n \times n$  с элементами в  $R$ ;
- множество векторов векторного пространства  $V$  над полем  $F \in \{\mathbb{Q}, \mathbb{R}, \mathbb{C}\}$ ;
- множество  $R^S$  всех функций  $S \rightarrow R$  из множества  $S$  в  $R$ ;
- множество  $X^X$  всех отображений множества  $X$  в  $X$ .

Тогда на  $G$  имеется обычная операция  $f$  сложения или умножения, которая каждой паре  $(a, b) \in G^2$  сопоставляет результат  $(a, b)f \in G$  операции  $f$ , примененной к этой паре. Получаем отображение  $f : G^2 \rightarrow G$ ,  $(a, b) \mapsto (a, b)f$  для всех  $a, b \in G$ . Следовательно, можно рассматривать выбранную операцию на  $G$  как отображение  $f : G^2 \rightarrow G$ .

Существует много других примеров этого рода, и наша точка зрения приводит к определению.

**Определение 1.1.1.** Алгебраической операцией на множестве  $G$  называют любое отображение  $f : G \times G \rightarrow G$ .

Такие операции называют иногда «внутренними» в знак того, что аргументы операции и ее результат лежат в одном и том же множестве. Однако существуют примеры, не укладывающиеся в эту схему.

**Пример 1.1.2.** Пусть  $F$  — одно из полей  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ . Тогда имеется операция деления, которая каждой паре  $(a, b) \in F \times (F \setminus \{0\})$  ставит в соответствие элемент  $a/b \in F$ , и возникает отображение  $F \times (F \setminus \{0\}) \rightarrow F$ ,  $(a, b) \mapsto a/b$ . Операцию деления на  $\mathbb{Z}$  можно рассматривать как отображение  $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}) \rightarrow \mathbb{Q}$ ,  $(a, b) \mapsto a/b$ .

**Пример 1.1.3.** Пусть  $F$  — одно из полей  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ , а  $V$  — векторное пространство над  $F$ . Тогда имеется операция умножения элементов из  $F$  на элементы  $V$  с результатами в множестве  $V$ , и данную операцию можно рассматривать как отображение  $F \times V \rightarrow V$ ,  $(\alpha, v) \mapsto \alpha v$ .

**Пример 1.1.4.** Скалярное умножение векторов 3-мерного евклидова пространства  $E$  можно рассматривать как отображение  $E \times E \rightarrow \mathbb{R}$ , которое каждой паре  $(a, b) \in E^2$  сопоставляет ее скалярное произведение  $ab \in \mathbb{R}$ .

**Пример 1.1.5.** Если  $p, q, r \in \mathbb{N}$ ,  $R \in \{\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{H}, \mathbb{O}\}$ , то имеется операция умножения матриц из  $M_{p,q}(R)$  на матрицы из  $M_{q,r}(R)$ , причем результаты этих операций лежат в  $M_{p,r}(R)$ , и мы можем рассматривать данное умножение как отображение  $M_{p,q}(R) \times M_{q,r}(R) \rightarrow M_{p,r}(R)$ ,  $(A, B) \mapsto AB$ .

**Пример 1.1.6.** Пусть  $A, B, C$  — множества,  $X = \text{Mor}(A, B)$  (множество всех отображений  $A \rightarrow B$ ),  $Y = \text{Mor}(B, C)$ ,  $Z = \text{Mor}(A, C)$ . Тогда любое отображение из  $X$  мы можем умножить на любое отображение из  $Y$ , получив некоторое отображение из  $Z$ , то есть в данном случае мы можем рассматривать произведение как отображение  $X \times Y \rightarrow Z$ ,  $(f, g) \mapsto fg$ .

Обобщая эти и многие другие примеры, мы получаем

**Определение 1.1.2.** *Алгебраической операцией, или просто операцией, называют любое отображение вида  $f : A \times B \rightarrow C$ .*

Можно считать, что  $f$  — это некоторая операция сложения элементов из  $A$  с элементами из  $B$  с результатами в  $C$ , и если  $(a, b) \in A \times B$ , то тогда разумно обозначить  $(a, b)f$  через  $a + b$ . Возникающая отсюда система обозначений называется аддитивной. С другой стороны, можно считать, что  $f$  — это некоторая операция умножения элементов из  $A$  на элементы из  $B$  с результатами в  $C$ , и обозначить  $(a, b)f$  через  $ab$ . Возникающая отсюда система обозначений называется мультипликативной. Если говорят об умножении (сложении)  $A \times B \rightarrow C$ , то подразумевают некоторую операцию  $f : A \times B \rightarrow C$ , для которой используют мультипликативную (аддитивную) систему обозначений.

Мы будем пользоваться мультипликативной записью, если не оговаривается противное, и предоставим читателю перевод на «аддитивный» язык.

**Определение 1.1.3.** *Группоидом называют любое непустое множество  $G$  вместе с одной произвольной алгебраической операцией на  $G$ .*

Например, на любом из множеств  $G$  в 1.1.1 имеются одна или две естественные операции. Взяв любую из них, получаем группоид  $G$ . В западной литературе группоид иногда называется магмой. Часто встречается ситуация, когда имеется множество  $R$ , которое рассматривается вместе с некоторыми операциями сложения и умножения на  $R$ . Множество  $R$  вместе с его операцией сложения будем обозначать  $R^+$ , то же множество вместе с его операцией умножения будем обозначать  $R^\times$ . Например,  $\mathbb{Z}^+$  — множество целых чисел, рассматриваемое как группоид относительно сложения,  $\mathbb{Z}^\times$  — множество целых чисел, рассматриваемое как группоид относительно умножения. Если мы хотим сказать, что рассматриваем множество  $G$  как группоид относительно операции  $f : G^2 \rightarrow G$ , то будем говорить «группоид  $(G, f)$ ».

**Пример 1.1.7.** Пусть  $G$  — группоид,  $\cdot : G^2 \rightarrow G$  — новая операция умножения на  $G$ ,  $a \cdot b := ba$  для всех  $a, b \in G$ . Группоид  $(G, \cdot)$  будем обозначать  $G^\circ$ , а элемент  $g \in G$ , рассматриваемый как элемент  $G^\circ$ , будем обозначать  $g^\circ$ . Тогда  $a^\circ b^\circ := (ba)^\circ$  для всех  $a, b \in G$ . Группоид  $G^\circ$  можно назвать отражением группоида  $G$ , так как в нем правое и левое меняются местами. Заметим, что  $(G^\circ)^\circ = G$ , поэтому мы считаем, что  $(a^\circ)^\circ = a$  для всех  $a \in G$ .

**Определение 1.1.4.** Пусть  $A, B$  — группоиды. Отображение  $\phi : A \rightarrow B$  называется морфизмом, если  $(xy)\phi = (x\phi)(y\phi)$  для всех  $x, y \in A$ .

Морфизмы часто называются гомоморфизмами. Очевидно, тождественное отображение  $\text{id}_A : A \rightarrow A$  любого группоида  $A$  является морфизмом.

**Предложение 1.1.1.** *Группоиды и их морфизмы вместе с операцией умножения отображений образуют категорию.*

*Доказательство.* Упражнение. □

**Определение 1.1.5.** *В мультипликативной системе обозначений единицей группоида  $G$  называется любой элемент  $e \in G$  такой, что  $eg = ge = g$  для всех  $g \in G$ . Аналогично, в аддитивной системе обозначений нулем группоида  $G$  называется любой элемент  $0 \in G$  такой, что  $0 + g = g + 0 = g$  для всех  $g \in G$ .*

Например, в  $\mathbb{N}^+$  нет нуля, а в  $\mathbb{N}^\times$  имеется единица. В группоиде векторов обычного трехмерного пространства по операции векторного произведения нет единицы.

**Предложение 1.1.2.** *В любом группоиде имеется не более одной единицы.*

*Доказательство.* Пусть  $e, e'$  — единицы группоида  $G$ . Тогда  $e = ee' = e'$ . □

Иногда удобно единицу группоида  $G$  обозначать  $1_G$ .

**Определение 1.1.6.** *Элементы  $x, y$  группоида  $G$  называются перестановочными, или коммутирующими, если  $xy = yx$ .*

**Определение 1.1.7.** *Группоид  $G$  называется коммутативным, или абелевым, если любые два его элемента перестановочны, то есть  $xy = yx$  для всех  $x, y \in G$ .*

Например,  $\mathbb{H}^+$  — абелев группоид,  $\mathbb{H}^\times$  — неабелев группоид, так как  $ij = k$ ,  $ji = -k \neq k$ . Аддитивную запись обычно используют для коммутативных группоидов.

**Определение 1.1.8.** *Если имеется алгебраическая операция  $A_1 \times A_2 \rightarrow A_3$ , и  $B_i \subseteq A_i$ ,  $i \in \{1, 2\}$ , то произведение  $B_1 B_2$  определим как  $\{b_1 b_2 : b_i \in B_i, i \in \{1, 2\}\}$ . Если  $B_1 = \{b_1\}$ , то вместо  $\{b_1\} B_2$  пишут  $b_1 B_2$ . Аналогично, если  $B_2 = \{b_2\}$ , то вместо  $B_1 \{b_2\}$  пишут  $B_1 b_2$ .*

В частности, семейство всех подмножеств группоида  $G$  само естественным образом является группоидом, и если  $A, B \subseteq G$ ,  $x \in G$ , то

$$AB = \{ab : a \in A, b \in B\},$$

$$xA = \{xa : a \in A\},$$

$$Ax = \{ax : a \in A\}.$$

Еще один пример появится в 2.1.1. Заметим, что при  $B_1 = \{b_1\}$  и  $B_2 = \{b_2\}$  неправильно писать  $B_1 B_2 = b_1 b_2$ , так как  $B_1 B_2 = \{b_1 b_2\} \neq b_1 b_2$ .

**Пример 1.1.8.** Множество  $\mathbb{Z}$  целых чисел является группоидом по обычной операции умножения целых чисел, и если  $m \in \mathbb{Z}$ , то  $m\mathbb{Z} = \{mz : z \in \mathbb{Z}\}$  — множество всех целых чисел, кратных  $m$ . Аналогично,  $\mathbb{Z}$  является группоидом по сложению, поэтому для  $r \in \mathbb{Z}$  выполняется равенство  $r + m\mathbb{Z} = \{r + mz : z \in \mathbb{Z}\}$ . Такое множество называется классом вычетов числа  $r$  по модулю  $m$ .

**Определение 1.1.9.** Группоид  $G$  называется полугруппой, если его алгебраическая операция ассоциативна, то есть  $x(yz) = (xy)z$  для всех  $x, y, z \in G$ .

Например,  $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{H}, M_n(\mathbb{C})$  — полугруппы и по сложению, и по умножению, но  $\mathbb{O}^\times$  не является полугруппой, хотя  $\mathbb{O}^+$  — полугруппа. Векторы обычного 3-мерного пространства по операции векторного произведения тоже не образуют полугруппу.

**Предложение 1.1.3.** Пусть  $G$  — полугруппа,  $n \in \mathbb{N}$ ,  $a_1, \dots, a_n \in G$ . Тогда произведение  $a_1 \dots a_n$  не зависит от расстановки в нем скобок.

*Доказательство.* Упражнение. □

**Определение 1.1.10.** Морфизм полугрупп определяется как морфизм соответствующих группоидов.

Если  $A$  — полугруппа, то, очевидно, тождественное отображение  $\text{id}_A : A \rightarrow A$  является морфизмом  $A \rightarrow A$ .

**Предложение 1.1.4.** Полугруппы и их морфизмы вместе с операцией умножения отображений образуют категорию.

*Доказательство.* Упражнение. □

**Определение 1.1.11.** Моноидом называется любая полугруппа с единицей.

**Пример 1.1.9.** Каждое из множеств  $\mathbb{Z}_{\geq 0}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$  является абелевым моноидом относительно обычных операций сложения и умножения,  $\mathbb{H}^+$  — тоже абелев моноид,  $\mathbb{H}^\times$  — неабелев моноид.  $\mathbb{N}^\times$  — моноид,  $\mathbb{N}^+$  не является моноидом.

**Пример 1.1.10.** Пусть  $X$  — множество,  $M$  — множество всех отображений  $X \rightarrow X$ , тогда  $M$  — моноид относительно операции умножения отображений, и тождественное отображение  $\text{id}_X$  множества  $X$  является единицей  $M$ . Этот моноид неабелев при  $|X| > 1$ . Действительно, пусть  $a, b \in X$  и  $a \neq b$ ,  $f_a, f_b : X \rightarrow X$ , причем  $xf_a = a$ ,  $xf_b = b$  для всех  $x \in X$ . Тогда  $f, g \in M$  и  $fg \neq gf$ , так как  $f_af_b = f_b$  и  $f_bf_a = f_a$ .

**Пример 1.1.11.** Семейство всех подмножеств моноида само является моноидом относительно операции умножения подмножеств 1.1.8.

**Пример 1.1.12.** Если  $\mathcal{C}$  — категория и  $A \in \text{Ob}(\mathcal{C})$ , то  $\text{Mor}(A, A)$  является моноидом по операции умножения морфизмов категории  $\mathcal{C}$ .

**Определение 1.1.12.** Отображение  $\phi : A \rightarrow B$  моноидов называется морфизмом моноидов, если  $\phi$  является морфизмом группоидов и единицу моноида  $A$  переводит в единицу моноида  $B$ .

Например, тождественное отображение  $\text{id}_M : M \rightarrow M$  произвольного моноида  $M$  является морфизмом  $M \rightarrow M$ .

**Предложение 1.1.5.** Моноиды и их морфизмы вместе с операцией умножения отображений образуют категорию.

*Доказательство.* Упражнение. □

**Лемма 1.1.6.** Пусть  $\phi : A \rightarrow B$  — морфизм группоидов (моноидов). Если отображение  $\phi$  обратимо, то  $\phi^{-1} : A \leftarrow B$  — морфизм группоидов (моноидов).

*Доказательство.* Упражнение. □

Так как группоиды (моноиды) и их морфизмы образуют категорию, то уже имеется определение изоморфизма группоидов (моноидов) (см. 5.4.5): Морфизм группоидов (моноидов)  $\phi : A \rightarrow B$  называется изоморфизмом, если найдется такой морфизм группоидов (моноидов)  $\tau : A \leftarrow B$ , что  $\phi\tau = \text{id}_A$ ,  $\tau\phi = \text{id}_B$ . Удобно получить другое описание изоморфизмов.

**Предложение 1.1.7.** Морфизм группоидов (моноидов)  $\phi : A \rightarrow B$  является изоморфизмом тогда и только тогда, когда отображение  $\phi$  биективно.

*Доказательство.* Если  $\phi$  — изоморфизм, то отображение  $\phi$  обратимо, и в силу 5.1.10  $\phi$  — биекция. Обратно, если  $\phi$  — биекция, то отображение  $\phi$  обратимо, и в силу 1.1.6  $\phi^{-1} : A \leftarrow B$  — морфизм. Так как морфизмы  $\phi, \phi^{-1}$  взаимно обратны, то  $\phi$  — изоморфизм. □

**Определение 1.1.13.** Подмножество  $H$  группоида  $G$  называется замкнутым по умножению, если  $ab \in H$  для всех  $a, b \in H$ .

Если  $H$  — замкнутое по умножению подмножество группоида  $G$ , то на  $H$  возникает естественная операция  $H^2 \ni (a, b) \mapsto ab \in H$ , которую мы всегда будем неявно подразумевать, если не оговаривается противное.

**Определение 1.1.14.** Подмножество  $H$  моноида  $G$  называется подмоноидом  $G$ , если  $H$  замкнуто по умножению и  $1_G \in H$ .

Очевидно, подмоноид сам является моноидом.

**Определение 1.1.15.** Пусть  $G$  — группоид с единицей  $e$ ,  $g \in G$ . Элементом, обратным к  $g$ , называют любой элемент  $h \in G$  такой, что (в мультипликативной системе обозначений)  $gh = hg = e$ . Аналогично, в аддитивной системе обозначений элементом, противоположным к  $g$ , называют любой элемент  $h \in G$  такой, что  $g + h = h + g = 0$ .

Очевидно, если  $a$  — элемент, обратный к  $b$ , то  $b$  — элемент, обратный к  $a$ .

**Определение 1.1.16.** Элемент  $g$  группоида  $G$  с единицей  $e$  называется обратимым, если для  $g$  существует элемент  $G$ , обратный к  $g$ .

Ясно, что если элемент  $a$  обратим и  $b$  — обратный к  $a$  элемент, то и  $b$  обратим.

**Пример 1.1.13.** Элемент  $z \in \mathbb{Z}^\times$  обратим тогда и только тогда, когда  $z \in \{\pm 1\}$ . Все элементы  $\mathbb{Z}^+$  имеют противоположные элементы.

**Пример 1.1.14.** Пусть  $X$  — множество,  $G$  — множество всех отображений  $X \rightarrow X$ . В силу 5.1.10 элемент  $a \in G$  обратим тогда и только тогда, когда  $a$  — перестановка  $X$ , то есть когда  $a : X \rightarrow X$  — биекция.

**Пример 1.1.15.** Пусть  $R = \mathbb{C}$ . В курсе линейной алгебры доказывается, что матрица  $A \in M_n(R)$  обратима тогда и только тогда, когда  $\det(a) \neq 0$ . Вообще, если  $R$  — любое коммутативное кольцо, то  $A$  обратима тогда и только тогда, когда  $\det(A)$  — обратимый элемент  $R$  по умножению (см. 1.3.3). Например, если  $R = \mathbb{Z}$ , то  $A$  обратима тогда и только тогда, когда  $\det(A) \in \{\pm 1\}$ .

**Пример 1.1.16.** Все ненулевые элементы группоидов  $\mathbb{Q}^\times, \mathbb{R}^\times, \mathbb{C}^\times, \mathbb{H}^\times, \mathbb{O}^\times$  обратимы.

**Предложение 1.1.8.** Любой элемент моноида имеет не более одного обратного элемента.

*Доказательство.* Пусть  $G$  — моноид,  $g \in G$ ,  $h, h'$  — элементы  $G$ , обратные к  $g$ . Тогда

$$h = h1 = h(gh') = (hg)h' = 1h' = h'.$$

□

Элемент, обратный (противоположный) к  $g$ , обозначается  $g^{-1}$  (соответственно,  $-g$ ).

**Лемма 1.1.9.** *Если элемент  $a$  моноида  $G$  обратим, то и  $a^{-1}$  обратим, причем  $(a^{-1})^{-1} = a$ .*

*Доказательство.* Это уже обсуждалось чуть ранее.  $\square$

**Определение 1.1.17.** *Множество обратимых элементов моноида  $M$  будем обозначать  $M^*$ .*

**Предложение 1.1.10.** *Если элементы  $a, b$  моноида  $M$  обратимы, то и  $ab$  обратим, причем  $(ab)^{-1} = a^{-1}b^{-1}$ .*

*Доказательство.* Упражнение.  $\square$

Произведение необратимых элементов может быть обратимым.

**Пример 1.1.17.** Пусть  $V$  — векторное пространство над полем  $F$ ,  $R$  — его кольцо линейных операторов, тогда  $R$  — моноид по умножению. Предположим, что  $V$  — пространство всевозможных последовательностей  $(x_i)_{i \in \mathbb{N}}$  элементов  $F$ . Пусть  $a, b$  — такие отображения  $V \rightarrow V$ , что  $a : (x_1, x_2, \dots) \mapsto (0, x_1, x_2, \dots)$ ,  $b : (x_1, x_2, \dots) \mapsto (x_2, x_3, \dots)$ . Тогда  $a, b \in R$  и  $ab = \text{id}_V$ , но  $a, b$  не обратимы. Однако, если  $V$  — конечномерное пространство и  $a, b \in R$ , причем  $ab$  обратим, то и  $a, b$  обратимы. Действительно,  $\det(a)\det(b) = \det(ab) \neq 0$ , поэтому  $\det(a), \det(b) \neq 0$ , следовательно,  $a, b$  обратимы. Убедитесь, что если  $V$  бесконечномерно, то существуют необратимые  $a, b \in R$  такие, что  $ab = \text{id}_V$ .

**Лемма 1.1.11.** *Пусть  $a, b$  — элементы моноида  $M$ , причем один из элементов  $a, b$  обратим. Если  $ab$  обратим, то и второй элемент обратим.*

*Доказательство.* Упражнение.  $\square$

## 1.2 Группы

**Определение 1.2.1.** *Группой называется любой моноид, все элементы которого обратимы.*

**Определение 1.2.2.** *Группа  $G$  называется конечной, если множество ее элементов конечно, и бесконечной — в противном случае.*

**Определение 1.2.3.** Группа  $G$  называется абелевой, или коммутативной, если  $ab = ba$  для всех  $a, b \in G$ .

**Определение 1.2.4.** Квазигруппой называется группоид  $G$ , для любых элементов  $a, b$  которого каждое из уравнений  $ax = b$  и  $ya = b$  имеет ровно одно решение в  $G$ . Квазигруппа с единицей называется лупой.

Любая группа является лупой, но обратное неверно, как показывает один из следующих примеров.

**Упражнение 1.2.1.** Пусть  $R$  — одно из множеств  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{H}, \mathbb{O}$ . Проверьте следующие утверждения:

- 1) множество  $\{0\}$  — группа по сложению.
- 2) множество  $\{1\}$  — группа относительно умножения.
- 3) множество  $\{\pm 1\} = \{-1, 1\}$  — группа относительно умножения.
- 4) множество  $C_n := \{z \in \mathbb{C} : z^n = 1\}$  всех комплексных корней степени  $n \in \mathbb{N}$  из единицы — группа по умножению.
- 5) множество  $\bigcup_{n \in \mathbb{N}} C_n$  всех комплексных корней из единицы (всевозможных степеней) — группа по умножению.
- 6) пусть  $p$  — простое число,  $G = \bigcup_{k \in \mathbb{Z}_{\geq 0}} C_{p^k}$ . Тогда  $G$  — группа по умножению. Эта группа называется  $p$ -группой Прюфера, или квазициклической  $p$ -группой.
- 7) множество кватернионов  $\mathbb{Q}_8 := \{\pm 1, \pm i, \pm j, \pm k\}$  — группа относительно умножения.
- 8) множество октав  $L := \{\pm 1, \pm e_1, \dots, \pm e_7\}$  — неассоциативная (но альтернативная) некоммутативная лупа по умножению.
- 9)  $R^+$  — группа по сложению.
- 10)  $R^\times$  не является группой.
- 11) при  $R \neq \mathbb{O}$  множество  $R \setminus \{0\}$  — группа по умножению. Эту группу мы обозначим  $R^*$ .
- 12) множество  $\mathbb{O} \setminus \{0\}$  не является группой относительно умножения, но является неассоциативной альтернативной некоммутативной лупой, которую мы обозначаем  $\mathbb{O}^*$ .

- 13) множество  $\mathbb{Z} \setminus \{0\}$  не является группой относительно умножения.
- 14) если  $R \neq \mathbb{O}$ , то  $S(R) := \{z \in R : |z| = 1\}$  — группа по умножению. При  $R = \mathbb{O}$  множество  $S(R)$  является неассоциативной альтернативной некоммутативной лупой по умножению.  $S(R)$  — это сфера радиуса 1 с центром в точке 0, имеющая размерность  $\dim_{\mathbb{R}}(R) - 1$ .
- 15) множество  $\mathbb{R}^{\mathbb{R}}$  всех функций  $\mathbb{R} \rightarrow \mathbb{R}$  — группа по операции сложения функций.
- 16) множество  $R^{\mathbb{N}}$  всех последовательностей чисел из  $R$  — группа относительно операции сложения последовательностей.

**Пример 1.2.1.** Пусть  $G$  — группа. Легко убедиться, что ее отражение  $G^{\circ}$  тоже является группой.

**Теорема 1.2.2.** Множество  $M^*$  обратимых элементов моноида  $M$  является группой относительно умножения в  $M$ .

*Доказательство.* В силу 1.1.10  $M^*$  замкнуто по умножению и, очевидно,  $1 := 1_M \in M^*$ . Следовательно,  $M^*$  — моноид. В силу 1.1.9  $M^*$  замкнуто по взятию обратного элемента. Таким образом,  $M^*$  — группа.  $\square$

**Пример 1.2.2.** Если  $M$  — моноид всех отображений множества  $X$  в  $X$ , то, в силу 5.1.10,  $M^*$  состоит из всевозможных биекций  $X \rightarrow X$ . Такие биекции называются перестановками множества  $X$ , или перестановками элементов  $X$ . Следовательно, группа  $M^*$  состоит из всех перестановок множества  $X$ . Эта группа обозначается  $\text{Sym}(X)$  и называется симметрической группой множества  $X$ . Если  $X = \{1, \dots, n\}$ , где  $n \in \mathbb{N}$ , то обозначим  $S_n := \text{Sym}(X)$ .

**Определение 1.2.5.** Морфизм групп определяется как морфизм соответствующих группоидов. Таким образом, отображение  $\phi : G \rightarrow H$  групп называется морфизмом групп, если для любых  $a, b \in G$  выполняется равенство  $(ab)\phi = (a\phi)(b\phi)$ .

Впоследствии мы будем изучать понятие морфизма групп достаточно подробно, а пока ограничимся самыми тривиальными наблюдениями. Если  $A$  — группа, то, очевидно, тождественное отображение  $\text{id}_A : A \rightarrow A$  является морфизмом  $A \rightarrow A$ .

**Предложение 1.2.3.** Группы и их морфизмы вместе с операцией умножения отображений образуют категорию.

*Доказательство.* Упражнение.  $\square$

Если  $G$  — группа,  $a \in G$ ,  $n \in \mathbb{Z}$ , то мы полагаем  $a^0 = 0$ , если  $n > 0$ , то  $a^n = \underbrace{a \dots a}_n$ , и если  $n < 0$ , то  $a^n = (a^{-1})^{-n}$ .

**Предложение 1.2.4.** Пусть  $G$  — группа,  $a, b \in G$ ,  $m, n \in \mathbb{Z}$ . Тогда

- 1)  $(a^m)^n = a^{mn}$ ;
- 2)  $a^m a^n = a^{m+n}$ ;
- 3) если  $ab = ba$ , то  $(ab)^n = a^n b^n$ .

На «аддитивном» языке:

- 1)  $m(na) = (mn)a$ ;
- 2)  $ta + na = (m+n)a$ ;
- 3) если  $a + b = b + a$ , то  $n(a + b) = na + nb$ .

Доказательство. Упражнение. □

## 1.3 Кольца, модули, алгебры

**Определение 1.3.1.** Кольцом называется произвольное множество, наделенное двумя алгебраическими операциями, называемыми сложением и умножением, удовлетворяющими следующим условиям:

- 1) по сложению  $R$  — абелева группа.
- 2) по умножению  $R$  — моноид.
- 3) для любых  $a, b, c \in R$  выполняются равенства  $a(b + c) = ab + ac$  и  $(a + b)c = ac + bc$ .

**Пример 1.3.1.** Множества  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{H}$  — кольца относительно обычных операций сложения и умножения. Октавы не образуют кольцо, так как умножение октав не ассоциативно. Целые неотрицательные числа не образуют кольцо, так как не все элементы этого множества имеют противоположные.

**Пример 1.3.2.** Пусть  $R$  — любое кольцо,  $M_n(R)$  — множество всех матриц  $n \times n$  с элементами в  $R$ . Тогда  $M_n(R)$  — кольцо по обычным операциям сложения и умножения матриц.

**Пример 1.3.3.** Пусть  $I, J$  — произвольные множества,  $R$  — кольцо. Под матрицей  $I \times J$  с элементами в  $R$  мы понимаем любое отображение  $I \times J \rightarrow R$ . Если  $a : I \times J \rightarrow R$ , то в матрице  $a$  на пересечении строки с номером  $i \in I$  и столбца с номером  $j \in J$  стоит элемент  $(i, j)a$ , который мы переобозначим  $a_{i,j}$ , а саму матрицу  $a$  будем иногда записывать как  $(a_{i,j})_{(i,j) \in I \times J}$ . В силу наших теоретико-множественных обозначений множество всех матриц  $I \times J \rightarrow R$  есть  $R^{I \times J}$ . Операции над такими матрицами проводятся по обычным правилам — если  $a, b \in R^{I \times J}$ , то  $a + b = (a_{i,j} + b_{i,j})_{(i,j) \in I \times J}$ , для  $\lambda \in R$   $\lambda a = (\lambda a_{i,j})_{(i,j) \in I \times J}$ ,  $a\lambda = (a_{i,j}\lambda)_{(i,j) \in I \times J}$ . Назовем матрицу  $a \in R^{I \times J}$  *финитной*, если в каждой ее строке имеется лишь конечное число ненулевых элементов, то есть для каждого  $i \in I$  множество  $\{j \in J : a_{i,j} \neq 0\}$  конечно. Множество всех финитных матриц из  $R^{I \times J}$  обозначим  $M_{I,J}(R)$ . Как обычно, пишем  $M_I(R) := M_{I,I}(R)$ . Для финитных матриц можно определить произведение по обычному правилу. Пусть  $I, J, K$  — множества,  $a \in M_{I,J}(R)$ ,  $b \in M_{J,K}(R)$ . Тогда мы полагаем  $ab = (\sum_{j \in J} a_{i,j}b_{j,k})_{(i,k) \in I \times K}$ . Финитность матриц  $a, b$  обеспечивает конечность числа ненулевых слагаемых в этих суммах (убедитесь в этом), поэтому определение корректно. Легко убедиться, что введенные нами операции над финитными матрицами обладают всеми обычными свойствами, в частности, множество  $M_I(R)$  является кольцом.

Если  $I = \{1, \dots, m\}$ ,  $J = \{1, \dots, n\}$ , где  $m, n \in \mathbb{N}$ , то  $M_{I,J}(R)$  — это обычные матрицы, и тогда  $M_{I,J}(R) = M_{m,n}(R)$ . Вместо матриц, финитных по строкам, можно было бы рассматривать матрицы, финитные по столбцам.

**Пример 1.3.4.** Пусть  $X$  — множество,  $R$  — кольцо,  $A$  — множество всех отображений  $X \rightarrow R$ . Если  $f, g \in A$ , то можно определить их сумму и произведение поточечно, то есть  $f+g, fg$  — такие отображения  $X \rightarrow R$ , что  $x(f+g) = xf + xg$  и  $x(fg) = (xf)(xg)$  для всех  $x \in X$ . Тогда  $A$  — кольцо относительно данных операций.

**Определение 1.3.2.** Подмножество  $A$  кольца  $B$  называется *подкольцом* в  $B$ , если выполняются следующие условия:

- 1) единица кольца  $B$  принадлежит  $A$ ;
- 2)  $x + y \in A$  для всех  $x, y \in A$ ;
- 3)  $-x \in A$  для всех  $x \in A$ ;
- 4)  $xy \in A$  для всех  $x, y \in A$ .

Очевидно, подкольцо само является кольцом относительно операций объемлющего кольца.

**Пример 1.3.5.** Кольца  $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{H}$  образуют цепочку подколец. Множество целых четных чисел не является подкольцом в  $\mathbb{Z}$ , так как оно не содержит единицу обобщающего кольца  $\mathbb{Z}$ .

**Пример 1.3.6.** Пусть  $I$  — множество, возможно, бесконечное,  $R$  — кольцо,  $A = M_I(R)$  — кольцо финитных матриц  $I \times I \rightarrow R$ . Обозначим  $B$  множество всех матриц из  $R^{I^2}$ , финитных и по строкам, и по столбцам. Ясно, что  $B \subseteq A$ . Множество  $B$  удовлетворяет всем условиям определения подкольца за одним исключением — если  $I$  бесконечно, то единица кольца  $A$  не принадлежит  $B$ . Вообще, если  $I$  бесконечно, то  $B$  — «кольцо без единицы».

**Пример 1.3.7.** Пусть  $R$  — кольцо,  $n \in \mathbb{N}$ . Напомним, что квадратная матрица называется треугольной, если ниже ее диагонали все элементы нулевые. Проверьте, что треугольные матрицы  $n \times n$  над кольцом  $R$  образуют подкольцо в кольце  $M_n(R)$ .

**Определение 1.3.3.** Кольцо  $R$  называется коммутативным, если  $ab = ba$  для всех  $a, b \in R$ .

**Пример 1.3.8.** Кольца  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$  коммутативны, кольцо  $\mathbb{H}$  не коммутативно, и если в кольце  $R$  есть ненулевые элементы, то кольцо  $M_n(R)$  некоммутативно для любого  $n \in \mathbb{N} \setminus \{1\}$ . Убедитесь в этом, используя матрицы

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

**Определение 1.3.4.** Пусть  $R$  — кольцо,  $a, b \in R$ . Элемент  $b$  называется обратным к  $a$ , если  $ab = ba = 1$ . Если элемент  $a$  имеет обратный элемент, то  $a$  называется обратимым элементом.

Как уже было доказано в 1.1.8,  $a$  имеет не более одного обратного элемента. Если обратный элемент имеется, то он обозначается  $a^{-1}$ .

**Упражнение 1.3.1.** Пусть  $R$  — кольцо,  $e$  — его единица. Докажите, что  $e = 0$  тогда и только тогда, когда  $R = \{0\}$ .

Кольцо, состоящее только из нуля, называется нулевым.

**Определение 1.3.5.** Кольцо  $R$  называется телом, если  $R \neq \{0\}$  и все ненулевые элементы  $R$  обратимы.

**Определение 1.3.6.** Коммутативное тело называется полем.

Таким образом, поле — это ненулевое коммутативное кольцо, все ненулевые элементы которого обратимы.

**Пример 1.3.9.**  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$  — поля по обычным операциям сложения и умножения.  $\mathbb{H}$  — некоммутативное тело. Кольцо целых чисел не является полем, так как не все его ненулевые элементы обратимы.

Множество обратимых элементов кольца  $R$  обозначим  $R^*$ .

**Предложение 1.3.2.** Если  $R$  — кольцо, то множество  $R^*$  его обратимых элементов является группой по операции умножения кольца  $R$ .

*Доказательство.* По умножению  $R$  — моноид, следовательно, в силу 1.2.2,  $R^*$  — группа по умножению.  $\square$

Эту группу будем называть мультипликативной группой кольца  $R$ .

**Упражнение 1.3.3.** Пусть  $R$  — коммутативное кольцо,  $n \in \mathbb{N}$ ,  $X \in M_n(R)$ . В линейной алгебре вводится присоединенная матрица  $X^* \in M_n(R)$  и доказывается, что  $X \cdot X^* = X^* \cdot X = \det(X) \cdot 1_n$ , где  $1_n$  — единичная матрица  $n \times n$ . Используя этот факт, докажите, что матрица  $X$  обратима тогда и только тогда, когда  $\det(X)$  — обратимый элемент  $R$ .

**Пример 1.3.10.** Пусть  $R$  — произвольное кольцо, возможно, некоммутативное,  $M := M_n(R)$  — кольцо матриц  $n \times n$  над кольцом  $R$ . Обратимые матрицы из  $M$  образуют группу, которую мы обозначим  $\mathrm{GL}_n(R)$ , то есть  $M_n(R)^* = \mathrm{GL}_n(R)$ . Если  $R$  коммутативно, то матрица  $A \in M$  обратима тогда и только тогда, когда  $\det(A) \in R^*$ . В частности, если  $F$  — поле, то  $\mathrm{GL}_n(F)$  состоит из всех матриц  $A \in M_n(F)$  с ненулевым определителем, то есть невырожденных матриц. Так как  $\mathbb{Z}^* = \{\pm 1\}$ , то  $\mathrm{GL}_n(\mathbb{Z})$  состоит из всех матриц  $A \in M_n(\mathbb{Z})$ , определители которых равны 1 или  $-1$ , то есть унимодулярных матриц  $n \times n$ .

**Пример 1.3.11.** Пусть  $I$  — произвольное множество,  $M := M_I(R)$  — кольцо финитных матриц  $I \times I$  над кольцом  $R$ . Обратимые матрицы из  $M$  образуют группу, которую мы обозначим  $\mathrm{GL}_I(R)$ , то есть  $M_I(R)^* = \mathrm{GL}_I(R)$ .

**Определение 1.3.7.** Пусть  $A, B$  — кольца, тогда отображение  $\phi : A \rightarrow B$  называется морфизмом, если для любых  $x, y \in A$  выполняются следующие условия:

- 1)  $1\phi = 1$ ;
- 2)  $(x + y)\phi = x\phi + y\phi$ ;

$$3) (xy)\phi = (x\phi)(y\phi)$$

**Пример 1.3.12.** Если  $R$  — кольцо, то тождественное отображение  $\text{id}_R : R \rightarrow R$  является морфизмом  $R \rightarrow R$ .

**Пример 1.3.13.** Пусть  $A$  — подкольцо кольца  $B$ ,  $\phi : A \rightarrow B$ ,  $a\phi = a$  для всех  $a \in A$ . Тогда  $\phi$  — морфизм колец.

**Пример 1.3.14.** Пусть  $R$  — кольцо,  $a \in R^*$ ,  $\phi : R \rightarrow R$ ,  $x\phi = a^{-1}xa$ . Убедитесь, что  $\phi$  — морфизм.

**Пример 1.3.15.** Пусть  $X$  — множество,  $R$  — кольцо,  $A = R^X$  — кольцо всех функций  $X \rightarrow R$ ,  $x_0 \in X$ ,  $\phi : A \rightarrow R$ ,  $f\phi = x_0 f$  для всех  $f \in A$ . Тогда  $\phi$  — морфизм колец.

**Упражнение 1.3.4.** Докажите, что кольца и их морфизмы образуют категорию.

**Предложение 1.3.5.** Морфизм колец является изоморфизмом тогда и только тогда, когда он является биекцией.

*Доказательство.* Это следует из 1.1.7. □

**Определение 1.3.8.** Пусть  $R$  — кольцо,  $M$  — абелева группа.  $M$  называется модулем над кольцом  $R$ , или  $R$ -модулем, если фиксирована операция умножения  $R \times M \rightarrow M$ , такая, что для всех  $r, r_1, r_2 \in R, m, m_1, m_2 \in M$  выполняются следующие условия:

- 1)  $1m = m$ ;
- 2)  $(r_1 r_2)m = r_1(r_2 m)$ ;
- 3)  $r(m_1 + m_2) = rm_1 + rm_2$ ;
- 4)  $(r_1 + r_2)m = r_1 m + r_2 m$ ;

Такие модули называются также левыми модулями, так как в произведениях элементов из  $R$  и элементов  $M$  элементы  $R$  стоят слева. Аналогично определяются правые  $R$ -модули.

**Определение 1.3.9.** Пусть  $R$  — кольцо,  $M$  — абелева группа.  $M$  называется правым модулем над кольцом  $R$ , или правым  $R$ -модулем, если фиксирована операция умножения  $M \times R \rightarrow M$ , такая, что для всех  $r, r_1, r_2 \in R, m, m_1, m_2 \in M$  выполняются следующие условия:

- 1)  $m1 = m$ ;
- 2)  $m(r_1 r_2) = (mr_1)r_2$ ;
- 3)  $(m_1 + m_2)r = m_1 r + m_2 r$ ;
- 4)  $m(r_1 + r_2) = mr_1 + mr_2$ .

**Пример 1.3.16.** Если  $F$  — поле,  $V$  — векторное пространство, то  $V$  — модуль над  $F$ .

**Пример 1.3.17.** В силу 1.2.4 любая абелева группа является  $\mathbb{Z}$ -модулем.

**Пример 1.3.18.** Пусть  $R$  — кольцо,  $I$  — множество,  $M = R^I$  — множество всех отображений  $I \rightarrow R$ . Для  $f, g \in M$ ,  $\alpha \in R$  мы можем определить такие отображения  $f + g, \alpha f : I \rightarrow R$ , что для любого  $x \in I$  выполняются равенства  $x(f + g) = xf + xg$  и  $x(\alpha f) = \alpha(xf)$ . Очевидно, эти операции превращают  $M$  в  $R$ -модуль. Можно определить произведение  $f\alpha : I \rightarrow R$ ,  $x(f\alpha) = (xf)\alpha$  для всех  $x \in I$ . Тогда  $M$  превращается в правый  $R$ -модуль. Если  $I = \{1, \dots, n\}$ , где  $n \in \mathbb{N}$ , то можно отождествить  $R^I$  и  $R^n$ .

**Пример 1.3.19.** Пусть  $F$  — поле,  $V$  — векторное пространство,  $\phi : V \rightarrow V$  — линейный оператор  $V$ . Обозначим  $R := F[X]$  и определим умножение  $V \times R \rightarrow V$  так:  $v \cdot f(x) := v\phi^x$  для всех  $f \in R$ ,  $v \in V$ , тогда  $V$  становится правым  $R$ -модулем.

**Пример 1.3.20.** Если  $R$  — кольцо, то  $R$  является  $R$ -модулем относительно операции умножения из  $R$ . Аналогично,  $R$  является левым  $R$ -модулем.

**Пример 1.3.21.** Пусть  $\phi : A \rightarrow B$  — морфизм колец,  $M$  —  $B$ -модуль. Определим операцию умножения  $A \times M \rightarrow M$  так:  $at := (a\phi)t$  для всех  $a \in A$ ,  $t \in M$ . Тогда  $M$  превращается в  $A$ -модуль. Эта конструкция имеет очевидный «правый» аналог.

**Пример 1.3.22.** Если кольцо  $R$  коммутативно и  $M$  — левый  $R$ -модуль, то можно определить умножение  $M \times R \rightarrow M$  так:  $tr := rt$  для всех  $t \in M$ ,  $r \in R$ . Легко убедиться, что относительно данного умножения  $M$  является правым  $R$ -модулем. Аналогично, если  $M$  — правый  $R$ -модуль, то можно определить умножение  $R \times M \rightarrow M$  правилом  $rt := tr$  для всех  $r \in R$ ,  $t \in M$ , и относительно этого произведения  $M$  станет левым  $R$ -модулем. Таким образом, если кольцо  $R$  коммутативно, то нет различия между понятиями левого и правого  $R$ -модуля. Для некоммутативных колец такие различия появляются.

Семейство  $(c_i)_{i \in I}$  называется почти нулевым, если множество индексов  $i \in I$ , для которых  $c_i \neq 0$ , конечно.

**Определение 1.3.10.** Пусть  $R$  — кольцо,  $M$  —  $R$ -модуль. Семейство  $(e_i)_{i \in I}$  элементов  $M$  называется базисом  $M$ , если для любого  $a \in M$  существует и единственно почти нулевое семейство  $(c_i)_{i \in I}$  элементов  $R$  такое, что  $a = \sum_{i \in I} c_i e_i$ . Множество  $S \subseteq M$  называется базисом  $M$ , если семейство  $(s)_{s \in S}$  является базисом  $M$ .

Если  $(e_i)_{i \in I}$  — базис модуля  $M$ , то отображение  $i \mapsto e_i$  инъективно.

**Определение 1.3.11.** Модуль, имеющий хотя бы один базис, называется свободным.

Если  $R$  — тело, то, как доказывается в курсе линейной алгебры, любой  $R$ -модуль свободен. Если  $R$  не является телом, то  $R$ -модуль может не быть свободным. Например, любая конечная ненулевая абелева группа является несвободным  $\mathbb{Z}$ -модулем, так как, очевидно, свободный ненулевой  $\mathbb{Z}$ -модуль должен быть бесконечным. Отображение  $f : X \rightarrow Y$  назовем почти нулевым, если множество  $(Y \setminus \{0\})f^{-1}$  конечно (см. 5.1.14).

**Теорема 1.3.6.** Для любого кольца  $R$  и произвольного множества  $I$  существует свободный модуль  $F$  с базисом вида  $(e_i)_{i \in I}$ .

*Доказательство.* Множество  $F$  всех почти нулевых отображений  $I \rightarrow R$ , очевидно, является  $R$ -модулем по обычным поточечным операциям сложения отображений и умножения их на элементы  $R$ . Если для каждого  $i \in I$  обозначить  $e_i$  отображение  $I \rightarrow R$ , равное 1 в точке  $i$  и нулю в остальных точках  $I$ , то семейство  $(e_i)_{i \in I}$  образует базис  $F$ .  $\square$

Такой свободный модуль иногда обозначается  $R^{(I)}$ . Понятно, что для конечного  $I$  выполняется равенство  $R^I = R^{(I)}$ . Так как отображение  $i \mapsto e_i$  инъективно, то можно отождествить элементы  $i, e_i$ , и тогда множество  $I$  превращается в базис модуля  $F$ . Мы получили следующую теорему.

**Теорема 1.3.7.** Для любого множества  $S$  и произвольного кольца  $R$  существует свободный  $R$ -модуль  $F$ , базисом которого является  $S$ .

**Определение 1.3.12.** Пусть  $R$  — кольцо,  $A, B$  —  $R$ -модули. Отображение  $\phi : A \rightarrow B$  называется морфизмом  $R$ -модулей, или линейным отображением, если выполняются следующие условия:

1)  $(a_1 + a_2)\phi = a_1\phi + a_2\phi$  для всех  $a_1, a_2 \in A$ ;

2)  $(ra)\phi = r(a\phi)$  для всех  $r \in R, a \in A$ .

**Пример 1.3.23.** Пусть  $F$  — поле,  $A, B$  — векторные пространства над  $F$ ,  $\phi : A \rightarrow B$  — отображение. Тогда  $\phi$  является морфизмом  $F$ -модулей тогда и только тогда, когда  $\phi$  — линейное отображение векторных пространств.

**Пример 1.3.24.** Пусть  $R$  — кольцо,  $M$  —  $R$ -модуль. Тогда  $\text{id}_M$  — линейное отображение  $M \rightarrow M$ .

**Пример 1.3.25.** Пусть  $R$  — кольцо,  $A, B$  —  $R$ -модули,  $\phi : A \rightarrow B$ ,  $a\phi = 0$  для всех  $a \in A$ . Тогда  $\phi$  — линейное отображение.

**Пример 1.3.26.** Пусть  $A, B$  — абелевы группы, тогда они являются  $\mathbb{Z}$ -модулями. Очевидно, любой морфизм групп  $A \rightarrow B$  является морфизмом  $\mathbb{Z}$ -модулей.

**Пример 1.3.27.** Пусть  $F$  — поле,  $A, B$  — векторные пространства над  $F$ ,  $\alpha : A \rightarrow A$ ,  $\beta : B \rightarrow B$  — линейные операторы. Как было отмечено ранее,  $A, B$  тогда превращаются в модули над кольцом  $R = F[X]$  многочленов. Пусть  $\phi : A \rightarrow B$  — отображение множеств. Убедитесь, что  $\phi$  — морфизм  $R$ -модулей тогда и только тогда, когда  $\phi$  — линейное отображение векторных пространств, и коммутативна диаграмма

$$\begin{array}{ccc} A & \xrightarrow{\phi} & B \\ \alpha \downarrow & & \downarrow \beta \\ A & \xrightarrow{\phi} & B \end{array}$$

**Упражнение 1.3.8.** Докажите, что  $R$ -модули и их морфизмы образуют категорию.

Следовательно, все сказанное в 5.4 переносится на кольца, модули и их морфизмы.

**Предложение 1.3.9.** Морфизм  $R$ -модулей является изоморфизмом тогда и только тогда, когда он является биекцией.

*Доказательство.* Это следует из 1.1.7 и простой проверки условия 2) для обратного отображения.  $\square$

**Упражнение 1.3.10.** Пусть  $R$  — кольцо, и  $\alpha, \beta : A \rightarrow B$  — морфизмы  $R$ -модулей. Определим их сумму  $\alpha + \beta$  — как такое отображение  $A \rightarrow B$ , что для любого элемента  $x \in A$  выполняется равенство  $x(\alpha + \beta) = x\alpha + x\beta$ . Докажите, что  $\alpha + \beta$  — морфизм  $R$ -модулей.

Пусть  $R$  — кольцо и  $M$  —  $R$ -модуль. Напомним, что эндоморфизм объекта  $A$  — это любой морфизм  $A \rightarrow A$ . Множество всех эндоморфизмов модуля  $M$  обозначается  $\text{End}_R(M)$ . Эндоморфизмы  $M$  можно складывать и умножать, получая эндоморфизмы  $M$ .

**Упражнение 1.3.11.**  $\text{End}_R(M)$  — кольцо.

Если  $A$  — свободный левый модуль над кольцом  $R$  с базисом  $e = (e_i)_{i \in I}$ ,  $B$  — свободный левый  $R$ -модуль с базисом  $f = (f_j)_{j \in J}$ ,  $\phi : A \rightarrow B$  — морфизм  $R$ -модулей, то мы определяем матрицу морфизма  $\phi$  как единственную финитную матрицу  $a \in M_{I,J}(R)$  такую, что  $e_i \phi = \sum_{j \in J} a_{i,j} f_j$  для всех  $i \in I$ . Эту матрицу обозначим  $\phi_{e,f}$ . Если  $A = B$ , то  $\phi_e := \phi_{e,e}$ . Отображение  $\text{End}_R(A) \rightarrow M_I(R)$ ,  $\phi \mapsto \phi_e$  назовем координатным, соответствующим базису  $e$ . Как доказывается в курсе линейной алгебры, координатное отображение  $\text{End}_R(A) \rightarrow M_I(R)$  является изоморфизмом колец. В частности, для каждой матрицы  $a \in M_I(R)$  существует единственный эндоморфизм  $\phi : A \rightarrow A$  такой, что  $\phi_e = a$ . Этот эндоморфизм обозначим  $a^e$ .

Напомним, что семейство  $a = (a_i)_{i \in I}$  элементов множества  $X$  — это отображение  $a : I \rightarrow X$ , причем для всех  $i \in I$  элемент  $a(i)$  обозначается  $a_i$ .

**Теорема 1.3.12.** (Универсальное свойство свободного модуля) Пусть  $R$  — кольцо,  $F$  — свободный  $R$ -модуль с базисом  $e = (e_i)_{i \in I}$ ,  $M$  — произвольный  $R$ -модуль. Тогда для любого отображения  $\phi : I \rightarrow M$  существует и единствен морфизм  $\bar{\phi} : F \rightarrow M$  такой, что коммутативна следующая диаграмма.

$$\begin{array}{ccc} & F & \\ e \nearrow & & \searrow \bar{\phi} \\ I & \xrightarrow{\phi} & M \end{array}$$

*Доказательство.* Если  $x \in F$ , то существует единственное почти нулевое семейство  $(c_i)_{i \in I}$  элементов  $R$  такое, что  $x = \sum_{i \in I} c_i e_i$ . Мы полагаем  $x \bar{\phi} = \sum_{i \in I} c_i (i \phi)$ . Очевидно,  $\bar{\phi}$  — морфизм  $R$ -модулей  $F \rightarrow M$ , для которого коммутативна указанная диаграмма, поэтому  $\bar{\phi}$  существует. Единственность следует из линейности  $\bar{\phi}$  и того, что  $e_i \bar{\phi} = i \phi$  для всех  $i \in I$ .  $\square$

**Определение 1.3.13.** Пусть  $R$  — коммутативное кольцо,  $A, B, C$  —  $R$ -модули. Отображение  $\phi : A \times B \rightarrow C$  называется билинейным, если для всех  $a, a_1, a_2 \in A$ ,  $b, b_1, b_2 \in B$  и  $\lambda \in R$  выполняются следующие условия:

- 1)  $(a_1 + a_2, b)\phi = (a_1, b)\phi + (a_2, b)\phi$ ;
- 2)  $(\lambda a, b)\phi = \lambda((a, b)\phi)$ ;
- 3)  $(a, b_1 + b_2)\phi = (a, b_1)\phi + (a, b_2)\phi$ ;
- 4)  $(a, \lambda b)\phi = \lambda((a, b)\phi)$ .

**Определение 1.3.14.** Пусть  $R$  — коммутативное кольцо.  $R$ -алгебра — это произвольный  $R$ -модуль  $A$  вместе с некоторой билинейной операцией умножения  $A^2 \rightarrow A$ .

$R$ -алгебра называется коммутативной или ассоциативной, если таковой является ее операция умножения. Ясно, как определить единицу алгебры.

Отображение  $\phi : A \rightarrow B$   $R$ -алгебр называется морфизмом, если  $\phi$  — морфизм  $R$ -модулей и  $(xy)\phi = (x\phi)(y\phi)$  для всех  $x, y \in A$ . Если, кроме того,  $A, B$  — алгебры с единицами и  $1\phi = 1$ , то мы говорим, что  $\phi$  — морфизм  $R$ -алгебр с единицами. Если  $A$  — подмножество в  $R$ -алгебре  $B$ , то мы назовем  $A$  подалгеброй, если  $A$  — подмодуль  $R$ -модуля  $B$  и множество  $A$  замкнуто по умножению.

Пусть  $G$  — произвольный группоид,  $R$  — любое коммутативное кольцо. Возьмем любой свободный  $R$ -модуль  $A$  с базисом  $G$  (в силу 1.3.7 такой  $R$ -модуль существует). Тогда каждый элемент  $a \in A$  единственным образом может быть записан в виде  $a = \sum_{g \in G} a_g g$ , где  $(a_g)_{g \in G}$  — некоторое почти нулевое семейство элементов  $R$ . Если  $a = \sum_{g \in G} a_g g$ ,  $b = \sum_{h \in G} b_h h$  — два элемента  $A$ , то мы определяем их произведение

$$ab := \sum_{g, h \in G} a_g b_h (gh).$$

Группируя слагаемые, получаем, что

$$ab = \sum_{g \in G} \left( \sum_{\substack{u, v \in G \\ uv = g}} a_u b_v \right) g.$$

Очевидно, полученное произведение  $A^2 \rightarrow A$  билинейно. Таким образом,  $A$  естественным образом является  $R$ -алгеброй. Если  $G$  — моноид, то  $A$  является кольцом, и тогда  $A$  называется *моноидной  $R$ -алгеброй* моноида  $G$ . Если  $G$  — группа, то  $A$  называется *групповой  $R$ -алгеброй* группы  $G$ . Мы будем обозначать  $A =: RG$ . Если  $H$

— подгруппа группы  $G$ , то под  $RH$  мы понимаем линейную оболочку (относительно кольца  $R$ ) множества  $H$ . Очевидно,  $RH$  является групповой  $R$ -алгеброй группы  $H$  и подалгеброй в  $RG$ .

## 1.4 Подгруппы

**Определение 1.4.1.** Подмножество  $H$  группы  $G$  называется подгруппой, если выполняются следующие условия:

- 1)  $H \neq \emptyset$ ;
- 2)  $H$  замкнуто по умножению, то есть для любых  $a, b \in H$   $ab \in H$ ;
- 3)  $H$  замкнуто по обращению, то есть для любого  $h \in H$   $h^{-1} \in H$ .

Если  $H$  — подгруппа  $G$ , то мы пишем  $H \leq G$ . Очевидно, подгруппа сама является группой относительно операции  $H^2 \ni (a, b) \mapsto ab \in H$ .

**Пример 1.4.1.** Пусть  $G$  — группа. Тогда  $G \leq G$  и  $\{1\} \leq G$ . Подгруппы  $\{1\}$ ,  $G$  называются тривиальными.

**Упражнение 1.4.1.** Пусть  $R$  — одно из колец  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{H}$ . Проверьте следующие утверждения (обозначения см. в 1.2.1):

- 1) если  $m, n \in \mathbb{N}$  и  $m \mid n$ , то  $C_m \leq C_n$ ;
- 2) если  $m \in \mathbb{N}$ , то  $C_m \leq \bigcup_{n \in \mathbb{N}} C_n$ ;
- 3) если  $p$  — простое число, то  $p$ -группа Прюфера является подгруппой в группе всех комплексных корней из единицы;
- 4)  $\mathbb{Q}_8 \leq \mathbb{H}^*$ ;
- 5)  $\mathbb{Q}_{>0}, \mathbb{R}_{>0} \leq \mathbb{R}^* \leq \mathbb{C}^* \leq \mathbb{H}^*$ ;
- 6) если  $R \neq \mathbb{O}$ , то  $S(R) \leq R^*$ ;
- 7) пусть  $G$  — множество всех сходящихся последовательностей чисел из  $R$ , тогда  $G$  — подгруппа в группе всех последовательностей  $R^{\mathbb{N}}$  относительно операции сложения последовательностей;

- 8) множество  $C^n(\mathbb{R})$   $n$  раз непрерывно дифференцируемых функций  $\mathbb{R} \rightarrow \mathbb{R}$ ,  $n \in \mathbb{N}$  — подгруппа в  $\mathbb{R}^{\mathbb{R}}$  относительно операции сложения функций.

Далее мы нередко будем перемножать подмножества групп, опираясь на определение 1.1.8.

**Предложение 1.4.2.** Пусть  $G$  — группа,  $A \leq G$ ,  $g \in G$ . Тогда

$$g \in A \Leftrightarrow gA = A \Leftrightarrow Ag = A.$$

*Доказательство.* Упражнение. □

**Предложение 1.4.3.** Пусть  $A, B$  — подгруппы группы  $G$ . Тогда  $A \leq B \Leftrightarrow AB = B$ .

*Доказательство.* Если  $A \leq B$ , то в силу 1.4.2  $AB = \cup_{a \in A} aB = \cup_{a \in A} B = B$ . Обратно, если  $AB = B$ , то  $A \subseteq AB = B$ . □

**Определение 1.4.2.** Если  $A$  — подмножество группы  $G$ , то мы вводим обозначение  $A^{-1} = \{a^{-1} : a \in A\}$ .

Теперь можно иначе сформулировать определение подгруппы.

**Определение 1.4.3.** Непустое подмножество  $H$  группы  $G$  называется подгруппой, если  $HH \subseteq H$  и  $H^{-1} \subseteq H$ .

**Предложение 1.4.4.** Непустое подмножество  $H$  группы  $G$  является подгруппой тогда и только тогда, когда  $HH = H$  и  $H^{-1} = H$ .

*Доказательство.* Упражнение. □

**Предложение 1.4.5.** Непустое подмножество  $H$  группы  $G$  является подгруппой тогда и только тогда, когда  $HH^{-1} \subseteq H$ .

*Доказательство.* Упражнение. □

**Теорема 1.4.6.** Непустое конечное подмножество  $H$  группы  $G$  тогда и только тогда является подгруппой, когда  $H$  замкнуто по умножению.

*Доказательство.* Если  $H \leq G$ , то  $H$  замкнуто по умножению. Обратно, пусть  $H$  замкнуто по умножению и покажем, что  $H$  замкнуто по обращению. Пусть  $a \in H$ . Из замкнутости  $H$  по умножению следует, что  $a^k \in H$  для всех  $k \in \mathbb{N}$ . Так как  $H$  конечно, то не может случиться так, что все элементы  $a^k$ ,  $k \in \mathbb{N}$  различны, следовательно,  $a^k = a^l$  для некоторых  $k, l \in \mathbb{N}$ ,  $k > l$ , поэтому  $1 = a^k(a^l)^{-1} = a^{k-l}$ . Итак, имеется  $n \in \mathbb{N}$  такое, что  $a^n = 1$ . Если  $n = 1$ , то  $a = 1$ , и тогда  $a^{-1} = a \in H$ . Предположим, что  $n > 1$ . Тогда  $aa^{n-1} = a^{n-1}a = 1$  и  $a^{n-1} \in H$ , так как  $H$  замкнуто по умножению. Отсюда следует, что  $a^{-1} = a^{n-1} \in H$ . □

**Предложение 1.4.7.** Если  $A, B$  — подмножества группы  $G$ , то  $(AB)^{-1} = B^{-1}A^{-1}$ .

*Доказательство.* Упражнение.  $\square$

**Определение 1.4.4.** Подмножества  $A, B$  группоида  $G$  называются перестановочными, если  $AB = BA$ .

**Теорема 1.4.8.** Пусть  $A, B$  — подгруппы группы  $G$ . Тогда  $AB \leq G$ , если и только если  $AB = BA$ .

*Доказательство.* Пусть  $AB \leq G$ . Тогда  $AB = (AB)^{-1} = B^{-1}A^{-1} = BA$ . Обратно, пусть  $AB = BA$  и покажем, что  $AB \leq G$ . Так как  $(AB)^{-1} = B^{-1}A^{-1} = BA = AB$ , то  $AB$  замкнуто по обращению. Так как  $(AB)(AB) = A(BA)B = A(AB)B = AAB B = AB$ , то  $AB$  замкнуто по умножению.  $\square$

**Определение 1.4.5.** Семейство  $A_1, \dots, A_n$  подгрупп группы  $G$  назовем:

- 1) перестановочным, если подгруппы  $A_i, A_j$  перестановочны для всех  $i, j \leq n$ .
- 2) слабо перестановочным, если для каждого  $i$  такого, что  $1 < i \leq n$  множества  $A_1 \cdot \dots \cdot A_{i-1}, A_i$  перестановочны.

Очевидно, перестановочное семейство слабо перестановочно.

**Теорема 1.4.9.** Пусть  $A_1, \dots, A_n$  — слабо перестановочные подгруппы группы  $G$ . Тогда  $A_1 \dots A_n \leq G$ . В частности, это верно, если подгруппы  $A_j$ ,  $j \leq n$  попарно перестановочны.

*Доказательство.* Для  $i \leq n$  обозначим  $A^i = A_1 \dots A_i$ . Докажем, что для каждого  $i \leq n$   $A^i \leq G$ . Допустим, что это не так, и  $i \leq n$  — наименьший индекс, для которого  $A^i \not\leq G$ . Тогда  $i > 1$ . По условию, множества  $A^{i-1}, A_i$  перестановочны, и в силу минимальности  $i$   $A^{i-1} \leq G$ . Применяя 1.4.8, заключаем, что  $A^i = A^{i-1}A_i \leq G$  — противоречие.  $\square$

**Предложение 1.4.10.** Пересечение любого семейства подгрупп группы  $G$  — подгруппа группы  $G$ .

*Доказательство.* Упражнение.  $\square$

**Определение 1.4.6.** Пусть  $S$  — подмножество группы  $G$ . Тогда пересечение всех подгрупп, содержащих  $S$ , мы называем подгруппой, порожденной  $S$ , и обозначаем его  $\langle S \rangle$ .

Очевидно,  $S \subseteq \langle S \rangle \leq G$ , и если  $A \subseteq B \subseteq G$ , то  $\langle A \rangle \leq \langle B \rangle$ . Кроме того, если  $A \leq G$ , то  $\langle A \rangle = A$ .

**Теорема 1.4.11.** Пусть  $S$  — подмножество группы  $G$ ,  $H \leq G$ . Тогда  $S \subseteq H \Leftrightarrow \langle S \rangle \leq H$ .

*Доказательство.* Очевидно,  $S \subseteq \langle S \rangle$ , поэтому, если  $\langle S \rangle \leq H$ , то  $S \subseteq H$ . Обратно, пусть  $S \subseteq H$ . По определению,  $\langle S \rangle$  содержится в каждой подгруппе  $G$ , содержащей  $S$ . В частности,  $\langle S \rangle \leq H$ .  $\square$

Таким образом,  $\langle S \rangle$  — наименьшая подгруппа  $G$ , содержащая  $S$ . Мы определяем произведение нулевого числа элементов моноида как единицу.

**Теорема 1.4.12.** Пусть  $S$  — подмножество группы  $G$ . Тогда  $g \in \langle S \rangle$  если и только если  $g$  можно записать как произведение нескольких элементов  $S \cup S^{-1}$ .

Эта теорема показывает, что  $\langle S \rangle$  состоит из всевозможных элементов вида  $s_1^{\varepsilon_1} \cdot \dots \cdot s_n^{\varepsilon_n}$ , где  $n \in \mathbb{N}$ ,  $s_1, \dots, s_n \in S$ ,  $\varepsilon_1, \dots, \varepsilon_n \in \{\pm 1\}$ . В частности, если  $a \in G$ , то  $\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$ .

*Доказательство.* Пусть  $W$  — множество элементов  $G$ , которые можно записать как произведение нескольких элементов  $S \cup S^{-1}$ . Очевидно,  $W \leq G$ . Покажем, что  $W = \langle S \rangle$ . Очевидно,  $S \subseteq W \leq G$ , поэтому  $\langle S \rangle \leq W$ . С другой стороны,  $W \leq \langle S \rangle$ , так как  $S \subseteq \langle S \rangle$  и  $\langle S \rangle$  замкнуто по произведению и обращению. Поэтому  $W = \langle S \rangle$ .  $\square$

**Определение 1.4.7.** Если в группе  $G$  имеется такой элемент  $g$ , что  $G = \langle g \rangle$ , то  $G$  называется циклической группой, а элемент  $g$  называется порождающим элементом группы  $G$ .

**Определение 1.4.8.** Если  $n \in \mathbb{N}$ ,  $A_1, \dots, A_n \subseteq G$ , то полагаем  $\langle A_1, \dots, A_n \rangle := \langle \cup_{i=1}^n A_i \rangle$ .

**Лемма 1.4.13.** Если  $A_1, \dots, A_n$  — слабо перестановочные подгруппы  $G$ , то

$$\langle A_1, \dots, A_n \rangle = \prod_{i=1}^n A_i.$$

*Доказательство.* Это следует из 1.4.9.  $\square$

**Теорема 1.4.14.** (Модулярное тождество) Пусть  $A, B, C$  — подгруппы группы  $G$ , причем  $A \leq C$ . Тогда  $A(B \cap C) = AB \cap C$ .

*Доказательство.* Так как  $B \cap C \subseteq B$ ,  $B \cap C \subseteq C$ , то  $A(B \cap C) \subseteq AB$  и  $A(B \cap C) \subseteq AC = C$ , поэтому  $A(B \cap C) \subseteq AB \cap C$ . Обратно, пусть  $g \in AB \cap C$ . Тогда  $g = ab = c$  для некоторых  $a \in A, b \in B, c \in C$ . Отсюда  $B \ni b = a^{-1}c \in AC = C$ , поэтому  $b \in B \cap C$ . Следовательно,  $g \in A(B \cap C)$ , т.е.  $A(B \cap C) \supseteq AB \cap C$ .  $\square$

**Предложение 1.4.15.** Пусть  $G$  — группа,  $A_1, A_2 \leq G$ ,  $A_1 \cap A_2 = \{1\}$ ,  $X_i, Y_i \subseteq A_i$  для каждого  $i \in \{1, 2\}$ . Тогда выполняются следующие утверждения:

- 1) отображение  $\phi : A_1 \times A_2 \rightarrow A_1 A_2$ , такое, что  $(a_1, a_2)\phi = a_1 a_2$  для всех  $a_i \in A_i$ , является биекцией.
- 2)  $X_1 X_2 \subseteq Y_1 Y_2 \Leftrightarrow X_1 \subseteq Y_1$  и  $X_2 \subseteq Y_2$ ;
- 3)  $X_1 X_2 = Y_1 Y_2 \Leftrightarrow X_1 = Y_1$  и  $X_2 = Y_2$ ;
- 4)  $(X_1 X_2) \cap (Y_1 Y_2) = (X_1 \cap Y_1)(X_2 \cap Y_2)$ .

*Доказательство.* Упражнение.  $\square$

**Определение 1.4.9.** Назовем подгруппу  $M$  группы  $G$  максимальной и будем писать  $M \triangleleft G$ , если  $M < G$  и не существует подгруппы  $N \leq G$  такой, что  $M < N < G$ .

Подгруппа  $H < G$  называется собственной.

**Лемма 1.4.16.** Любая собственная подгруппа конечной группы содержится в некоторой максимальной подгруппе.

*Доказательство.* Допустим, что  $G$  конечна и  $A < G$ . Пусть  $X := \{B : A \leq B < G\}$ . Очевидно,  $X$  непусто (например,  $A \in X$ ) и конечно, поэтому найдется элемент  $B \in X$ , имеющий наибольший порядок среди всех элементов  $X$ . Очевидно,  $B$  — максимальная подгруппа  $G$  (если  $B < C < G$ , то  $C \in X$  и  $|C| > |B|$ , что противоречит максимальной порядку  $B$  в  $X$ ) и  $A \leq B$ .  $\square$

## 1.5 Нормальные подгруппы

Для любых элементов  $a, b$  группы  $G$  полагаем  $a^b := b^{-1}ab$ . Если  $S \subseteq G$ ,  $g \in G$ , то обозначим  $S^g := \{s^g : s \in S\} = g^{-1}Sg$ .

**Лемма 1.5.1.** Пусть  $G$  — группа. Для всех  $a, b, c \in G$  имеют место следующие равенства:

$$1) a^1 = a;$$

$$2) (a^b)^c = a^{bc};$$

$$3) (ab)^c = a^c b^c.$$

Для произвольных  $S, T \subseteq G$ ,  $a, b \in G$  имеют выполняются следующие утверждения:

$$1) S^1 = S;$$

$$2) (S^a)^b = S^{ab};$$

$$3) (ST)^a = S^a T^a;$$

$$4) S \subseteq T \Leftrightarrow S^a \subseteq T^a;$$

$$5) S = T \Leftrightarrow S^a = T^a;$$

$$6) (S \cap T)^a = S^a \cap T^a;$$

$$7) (S \cup T)^a = S^a \cup T^a;$$

$$8) (S \setminus T)^a = S^a \cap T^a;$$

$$9) \langle S \rangle^a = \langle S^a \rangle.$$

*Доказательство.* Упражнение. □

**Теорема 1.5.2.** Пусть  $G$  — группа,  $A \subseteq G$ ,  $B \leq G$ . Равносильны следующие условия:

$$1) A^b \subseteq A \text{ для всех } b \in B;$$

$$2) A^b = A \text{ для всех } b \in B;$$

$$3) Ab = bA \text{ для всех } b \in B.$$

*Доказательство.* Покажем, что  $(1) \Rightarrow (2)$ . Пусть выполнено условие (1) и  $b \in B$ . Тогда  $b^{-1} \in B$ , и по условию (1)  $A^{b^{-1}} \subseteq A$ , следовательно,  $(A^{b^{-1}})^b \subseteq A^b$ , то есть  $A \subseteq A^b$ . С другой стороны,  $A^b \subseteq A$ , следовательно,  $A^b = A$ . Очевидно,  $(2) \Rightarrow (3) \Rightarrow (1)$ . □

**Определение 1.5.1.** Пусть  $G$  — группа,  $A \subseteq G$ ,  $B \leq G$ . Говорят, что  $B$  нормализует  $A$ , или что множество  $A$  нормально относительно  $B$ , или что  $A$  —  $B$ -инвариантно, если выполняется одно из условий 1.5.2. В таком случае мы пишем  $A \subseteq_B G$ . Если  $A$  нормально относительно  $G$ , то  $A$  называется нормальным подмножеством  $G$ . Высказывание « $A$  — нормальная подгруппа  $G$ » записывается так:  $A \trianglelefteq G$ .

Очевидно, в абелевой группе все подгруппы нормальны. Обратное утверждение неверно (группа, все подгруппы которой нормальны, называется *дедекиндовой*, неабелева дедекиндова группа называется *гамильтоновой*. Одним из примеров гамильтоновой группы является группа кватернионов  $\mathbb{Q}_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ . Известно описание всех гамильтоновых групп, конечных и бесконечных).

**Определение 1.5.2.** Неединичная группа, не имеющая нетривиальных нормальных подгрупп называется *простой*.

В определенном смысле любая конечная группа «сконструирована» из конечных простых групп. Одним из крупнейших достижений математики XX века является их полная классификация.

**Предложение 1.5.3.** Пусть  $G$  — группа,  $A \trianglelefteq G$ . Тогда  $A$  перестановочна с любой подгруппой  $G$ . В частности,  $AB \leq G$  для любой подгруппы  $B \leq G$ .

*Доказательство.* Очевидно. □

Если подгруппа  $A$  группы  $G$  перестановочна с каждой подгруппой  $B \leq G$ , то она называется *квазинормальной*, или *перестановочной* подгруппой. Очевидно, нормальные подгруппы квазинормальны, но обратное верно не всегда. Группы, все подгруппы которых квазинормальны называются группами Ивасава (Iwasawa group), или модулярными группами, и строение конечных модулярных групп известно. Более важным является другое обобщение понятия нормальной подгруппы — субнормальные подгруппы, которыми мы займемся позднее.

**Предложение 1.5.4.** Пусть  $G$  — группа,  $n \in \mathbb{N}$  и  $A_1, \dots, A_n \trianglelefteq G$ . Тогда  $\prod_{i=1}^n A_i \trianglelefteq G$  и  $\bigcap_{i=1}^n A_i \trianglelefteq G$ .

*Доказательство.* Упражнение. □

**Определение 1.5.3.** Нормализатором  $N_H(S)$  подмножества  $S$  группы  $G$  в подгруппе  $H \leq G$  называется множество  $\{h \in H : S^h = S\}$ .

**Лемма 1.5.5.** Пусть  $G$  — группа,  $S \subseteq G$ ,  $H \leq G$ . Тогда  $N_H(S) \leq H$ .

*Доказательство.* Упражнение, или см. 2.4.3.  $\square$

**Теорема 1.5.6.** Пусть  $A, B \leq G$  и  $A = \langle A_0 \rangle$ ,  $B = \langle B_0 \rangle$ ,  $B_0^{-1} \subseteq B_0$ . Тогда равносильны условия:

- 1)  $B$  нормализует  $A$ ;
- 2)  $a^b \in A$  для всех  $a \in A_0$ ,  $b \in B_0$ .

Если  $A$  конечна, то можно отказаться от условия  $B_0^{-1} \subseteq B_0$ . Если  $B$  нормализует  $A_0$ , то  $B$  нормализует и  $\langle A_0 \rangle$ .

*Доказательство.* Очевидно, первое условие влечет второе. Обратно, пусть выполняется второе условие. Пусть  $b \in B_0$ , тогда  $A^b = \langle A_0 \rangle^b = \langle A_0^b \rangle \leq \langle A \rangle = A$  (см. 1.5.1, утверждение 9)). Итак,  $A^b \leq A$  для всех  $b \in B_0$ . Так как  $b^{-1} \in B_0$ , то  $A^{b^{-1}} \leq A$ , откуда  $A \leq A^b$ . Следовательно,  $A^b = A$  для всех  $b \in B_0$ . Таким образом,  $B_0 \leq N_G(A)$ , поэтому  $B = \langle B_0 \rangle \leq N_G(A)$ .

Пусть  $A$  конечна и откажемся от условия  $B_0^{-1} \subseteq B_0$ . Пусть снова  $b \in B_0$ . Так как  $|A^b| = |A|$  (очевидно, отображение  $A \ni a \mapsto a^b \in A^b$  — биекция), то из  $A^b \leq A$  следует  $A^b = A$ , то есть  $B_0 \leq N_G(A)$ , поэтому  $B = \langle B_0 \rangle \leq N_G(A)$ . Последнее утверждение теоремы следует из утверждения 9) леммы 1.5.1.  $\square$

Добавим, что  $B_0^{-1} \subseteq B_0 \Leftrightarrow B_0^{-1} = B_0$ . Действительно,  $B_0^{-1} = B_0 \Rightarrow B_0^{-1} \subseteq B_0$ . Обратно,

$$B_0^{-1} \subseteq B_0 \Rightarrow B_0 \subseteq B_0^{-1} \Rightarrow B_0^{-1} \subseteq B_0 \subseteq B_0^{-1} \Rightarrow B_0 = B_0^{-1}.$$

Если  $A, B$  — подмножества группы  $G$ , то обозначим  $A^B := \{a^b : a \in A, b \in B\}$ .

**Определение 1.5.4.** Пусть  $A, B \leq G$ . Тогда подгруппа  $\langle A^B \rangle$  называется нормальным замыканием  $A$  относительно  $B$ , и обозначается  $\text{пс}_B(A)$ .

**Теорема 1.5.7.** Пусть  $A, B \leq G$ . Тогда  $\text{пс}_B(A)$  — наименьшая подгруппа  $G$ , содержащая  $A$  и нормализуемая  $B$ .

*Доказательство.* Если  $b \in B$ , то  $(A^B)^b = A^{Bb} = A^B$ . В силу 1.5.6  $B$  нормализует  $\langle A^B \rangle$ . Если  $A \leq H \leq G$ , и  $B$  нормализует  $H$ , то  $A^B \subseteq H^B \subseteq H$ , поэтому  $\langle A^B \rangle \leq H$ . Таким образом,  $\langle A^B \rangle$  — наименьшая подгруппа  $G$ , содержащая  $A$  и нормализуемая  $B$ .  $\square$

Далее мы изложим первые сведения о субнормальных подгруппах.

**Определение 1.5.5.** Рядом группы  $G$  длины  $n \in \mathbb{Z}_{\geq 0}$  назовем любое конечное множество  $C$  подгрупп  $G$ , которое можно записать в виде  $C = \{C_i\}_{i \in \{0, \dots, n\}}$ , где  $C_i \leq C_{i+1}$  для всех  $i < n$ . Ряд  $C$  называется субнормальным, если  $C_i \trianglelefteq C_{i+1}$  для всех  $i < n$ . Ряд  $C$  называется нормальным, если все его элементы — нормальные подгруппы. Мы говорим, что ряд  $C$  соединяет подгруппы  $A, B$ , если  $C_0 = A$  и  $C_n = B$ .

**Определение 1.5.6.** Подгруппа  $H$  группы  $G$  называется субнормальной, если существует субнормальный ряд, соединяющий  $H$  и  $G$ . Высказывание « $H$  — субнормальная подгруппа» будем записывать так:  $H \trianglelefteq G$ .

**Предложение 1.5.8.** Пусть  $A, B, C$  — подгруппы группы  $G$ . Если  $A \trianglelefteq B \trianglelefteq C$ , то  $A \trianglelefteq C$ .

*Доказательство.* Это очевидно. □

**Лемма 1.5.9.** Пусть  $G$  — группа,  $A \trianglelefteq B \leq G$ ,  $C \leq G$ . Тогда  $A \cap C \trianglelefteq B \cap C$ .

*Доказательство.* Пусть  $g \in B \cap C$ , тогда  $(A \cap C)^g = A^g \cap C^g$ . Так как  $g \in B$  и  $A \trianglelefteq B$ , то  $A^g = A$ . Из  $g \in C$  следует, что  $C^g = C$ . Отсюда  $(A \cap C)^g = A \cap C$ . □

**Предложение 1.5.10.** Пусть  $G$  — группа,  $A \trianglelefteq B \leq G$ ,  $C \leq G$ . Тогда  $A \cap C \trianglelefteq B \cap C$ .

*Доказательство.* Так как  $A \trianglelefteq B$ , то существует субнормальный ряд

$$A = A_0 \trianglelefteq A_1 \trianglelefteq \dots \trianglelefteq A_n = B.$$

В силу 1.5.9

$$A \cap C = A_0 \cap C \trianglelefteq A_1 \cap C \trianglelefteq \dots \trianglelefteq A_n \cap C = B \cap C,$$

то есть  $A \cap C \trianglelefteq B \cap C$ . □

**Предложение 1.5.11.** Если  $A \trianglelefteq G$  и  $A \leq B \leq G$ , то  $A \trianglelefteq B$ .

*Доказательство.* Это прямое следствие 1.5.10. □

**Предложение 1.5.12.** Пусть  $G$  — группа,  $A, B \trianglelefteq G$ . Тогда  $A \cap B \trianglelefteq G$ .

*Доказательство.* Из  $A \trianglelefteq G$  и 1.5.10 следует, что  $A \cap B \trianglelefteq B$ . Так как  $B \trianglelefteq G$ , то по 1.5.8  $A \cap B \trianglelefteq G$ . □

**Предложение 1.5.13.** Пусть  $G$  — группа,  $A \leq G$  — простая подгруппа,  $B \trianglelefteq G$ . Тогда либо  $A \cap B = \{1\}$ , либо  $A \leq B$ .

*Доказательство.* Пусть  $B = B_0 \triangleleft B_1 \triangleleft \dots \triangleleft B_n = G$  — субнормальный ряд от  $B$  до  $G$  и допустим, что заключение рассматриваемого утверждения неверно, а  $n$  минимально при этом условии. Если  $n = 0$ , то  $B = G$  и  $A \leq B$  — противоречие, следовательно,  $n \geq 1$ . В частности,  $B_{n-1} \triangleleft G$ . Так как  $B_{n-1} \trianglelefteq G$ , то в силу 1.5.9  $A \cap B_{n-1} \trianglelefteq A$ . Группа  $A$  проста, поэтому  $A \cap B_{n-1} = \{1\}$  или  $A \cap B_{n-1} = A$ . Если  $A \cap B_{n-1} = \{1\}$ , то, так как  $B_{n-1} \geq B$ ,  $A \cap B = \{1\}$  — противоречие, поэтому  $A \cap B_{n-1} = A$ . Отсюда следует, что  $A \leq B_{n-1}$ . Субнормальный ряд  $B = B_0 \triangleleft B_1 \triangleleft \dots \triangleleft B_{n-1}$  от  $B$  до  $B_{n-1}$  имеет длину меньше  $n$ , поэтому для  $B_{n-1}$  доказываемое утверждение верно, следовательно,  $A \cap B = \{1\}$  или  $A \leq B$  — противоречие.  $\square$

## 1.6 Морфизмы

Напомним, что отображение  $\phi : G \rightarrow H$  групп называется морфизмом, или гомоморфизмом (групп), если  $(ab)\phi = (a\phi)(b\phi)$  для всех  $a, b \in G$ .

**Упражнение 1.6.1.** Убедитесь, что следующие отображения групп являются морфизмами:

- 1)  $\sigma : \mathbb{R}^* \rightarrow \{\pm 1\}$ ,  $x\sigma = 1$  если  $x > 0$ , и  $x\sigma = -1$  если  $x < 0$ ;
- 2)  $n \in \mathbb{N}$ ,  $\sigma : S_n \rightarrow \{\pm 1\}$ ,  $x\sigma$  — знак перестановки  $x$ ;
- 3)  $n \in \mathbb{N}$ ,  $R$  — любое коммутативное кольцо,  $\sigma : \text{GL}_n(R) \rightarrow R^*$ ,  $x\sigma = \det(x)$ ;
- 4)  $D$  — любое из тел  $\mathbb{R}, \mathbb{C}, \mathbb{H}$ ,  $\phi : D \rightarrow \mathbb{R}_{>0}$ ,  $x\phi = |x|$ .

**Упражнение 1.6.2.** Пусть  $A, B$  — группоиды. Отображение  $\phi : A \rightarrow B$  называется антиморфизмом, если  $(xy)\phi = (y\phi)(x\phi)$  для всех  $x, y \in A$ . Докажите, что для произвольного отображения  $\phi : A \rightarrow B$  равносильны следующие утверждения:

- 1)  $\phi : A \rightarrow B$  — антиморфизмом;
- 2)  $\phi : A^\circ \rightarrow B$  — морфизм;
- 3)  $\phi : A \rightarrow B^\circ$  — морфизм;

**Предложение 1.6.3.** Пусть  $\phi : A \rightarrow B$  — морфизм моноидов. Тогда  $A^*\phi \subseteq B^*$ , поэтому  $\phi$  можно рассматривать как морфизм групп  $A^* \rightarrow B^*$ .

*Доказательство.* Пусть  $x \in A^*$ , тогда найдется такой элемент  $y \in A$ , что  $xy = yx = 1$ . Отсюда

$$(xy)\phi = (yx)\phi = 1\phi \Rightarrow (x\phi)(y\phi) = (y\phi)(x\phi) = 1,$$

то есть  $x\phi \in B^*$ . □

**Предложение 1.6.4.** Пусть  $\phi : A \rightarrow B$  — морфизм колец. Тогда  $A^*\phi \subseteq B^*$ , поэтому  $\phi$  можно рассматривать как морфизм групп  $A^* \rightarrow B^*$ .

*Доказательство.* Кольца  $A, B$  являются моноидами по умножению, а  $\phi : A \rightarrow B$  — их морфизм, и в силу 1.6.3  $A^*\phi \subseteq B^*$ . □

Утверждение 1.6.4 означает, что группу обратимых элементов кольца (моноида) можно рассматривать как функтор из категории колец (моноидов) в категорию групп. Напомним, что множество всех морфизмов  $G \rightarrow H$  обозначается  $\text{Mor}(G, H)$ .

**Упражнение 1.6.5.** Пусть  $G, H$  — группы,  $\iota : G \rightarrow G$ ,  $g\iota := g^{-1}$  для всех  $g \in G$ ,  $X = \text{Mor}(G, H)$ ,  $Y$  — множество всех антиморфизмов  $G \rightarrow H$ . Тогда существует и единственна биекция  $\phi : X \rightarrow Y$ , такая, что  $f\phi = f\iota$  для всех  $f \in X$ .

**Упражнение 1.6.6.** Пусть  $\alpha : A \rightarrow B$ ,  $\beta : B \rightarrow C$  — отображения группоидов. Можно сказать, что морфизмы — это  $(+1)$ -морфизмы, а антиморфизмы — это  $(-1)$ -морфизмы. Докажите, что если  $\alpha$  —  $\epsilon_1$ -морфизм, а  $\beta$  —  $\epsilon_2$ -морфизм, то  $\alpha\beta$  —  $\epsilon_1\epsilon_2$ -морфизм ( $\epsilon_1, \epsilon_2 \in \{\pm 1\}$ ).

Заметим, что группы вместе с их морфизмами и антиморфизмами тоже образуют категорию.

**Предложение 1.6.7.** Морфизм групп является изоморфизмом тогда и только тогда, когда он является биекцией.

*Доказательство.* Это следует из 1.1.7. □

Очевидно, то же верно и для антиморфизмов — антиморфизм является изоморфизмом (в категории групп, морфизмов и антиморфизмов) тогда и только тогда, когда он биективен.

Если существует изоморфизм  $A \rightarrow B$ , то говорят, что  $A$  и  $B$  изоморфны, и пишут  $A \simeq B$ . Интуитивно изоморфность  $A$  и  $B$  означает, что  $A$  и  $B$  аналогичны во всех отношениях, обладают одинаковыми свойствами.

**Упражнение 1.6.8.** Пусть  $G$  — группа,  $\phi : G \rightarrow G^\circ$ ,  $g\phi = (g^{-1})^\circ$  для всех  $g \in G$ . Тогда  $\phi$  — изоморфизм. Следовательно, всегда  $G \simeq G^\circ$ .

Очевидным образом можно определить отражение кольца. Любопытно, что существуют кольца, даже конечные, неизоморфные своему отражению.

**Лемма 1.6.9.** Пусть  $\alpha : G \rightarrow H$  — морфизм конечных групп,  $|G| = |H|$ . Равносильны условия:

- 1)  $\alpha$  — изоморфизм;
- 2)  $\alpha$  сюръективно;
- 3)  $\alpha$  инъективно.

*Доказательство.* Упражнение. □

**Определение 1.6.1.** Сюръективный морфизм называется эпиморфизмом, инъективный морфизм — мономорфизмом, морфизм  $G \rightarrow G$  называется эндоморфизмом объекта  $G$ . Множество всех эндоморфизмов объекта  $G$  обозначим  $\text{End}(G)$ .

Если существует мономорфизм групп  $\phi : A \rightarrow B$ , то говорят, что  $A$  вкладывается в  $B$ . Тогда можно отождествить каждый элемент  $a \in A$  с его образом  $a\phi$ , и группа  $A$  станет подгруппой  $B$ . Мономорфизм можно обозначать стрелкой  $\hookrightarrow$ . Формула  $A \hookrightarrow B$  означает, что  $A$  вкладывается в  $B$ . Если существует эпиморфизм  $\phi : A \rightarrow B$ , то  $B$  называется образом  $A$  относительно  $\phi$ , при этом  $A$  называется расширением  $B$  (с помощью  $\phi$ ). Эпиморфизм обозначается стрелкой  $\twoheadrightarrow$ . Формула  $A \twoheadrightarrow B$  означает, что существует эпиморфизм  $A \rightarrow B$ .

Если  $G$  — абелева группа, записываемая аддитивно,  $f, g \in \text{End}(G)$ , то мы определим  $f + g$  как такое отображение  $f + g : G \rightarrow G$ , что  $x(f + g) = xf + xg$  для всех  $x \in G$ .

**Теорема 1.6.10.** Множество всех эндоморфизмов группы  $G$  является моноидом по операции умножения отображений. Если  $G$  — абелева группа, то  $\text{End}(G)$  является кольцом относительно операций сложения и умножения отображений.

*Доказательство.* Упражнение. □

**Предложение 1.6.11.** Пусть  $\phi : A \rightarrow A'$  — морфизм групп. Тогда для любых  $a, b \in A$ ,  $k \in \mathbb{Z}$  выполняются следующие утверждения;

- 1)  $1\phi = 1'$ , где  $1$  — единица  $A$ ,  $1'$  — единица  $A'$ ;
- 2)  $a^{-1}\phi = (a\phi)^{-1}$ ;
- 3)  $a^k\phi = (a\phi)^k$ ;

$$4) a^b \phi = (a\phi)^{b\phi}.$$

*Доказательство.* 1. Пусть  $g \in A$ . Тогда  $g\phi = (1g)\phi = (1\phi)(g\phi)$ . Умножая равенство  $g\phi = (1\phi)(g\phi)$  справа на  $(g\phi)^{-1}$ , получаем, что  $1' = 1\phi$ .

$$2. 1 = aa^{-1} \Rightarrow 1 = 1\phi = (aa^{-1})\phi = (a\phi)(a^{-1}\phi) \Rightarrow a^{-1}\phi = (a\phi)^{-1}.$$

3. Если  $k > 0$ , то  $a^k \phi = (a \dots a)\phi = (a\phi) \dots (a\phi) = (a\phi)^k$ . Если  $k = 0$ , то  $a^k \phi = 1\phi = 1 = (a\phi)^k$ . Пусть  $k < 0$ . Тогда  $a^k \phi = ((a^{-1})^{-k})\phi = (a^{-1}\phi)^{-k} = ((a\phi)^{-1})^{-k} = (a\phi)^k$ .

4. Очевидно.  $\square$

**Упражнение 1.6.12.** Пусть  $G$  — группа,  $n \in \mathbb{Z}$ . Группа  $G$  называется  $n$ -абелевой, если отображение  $x \mapsto x^n$  является эндоморфизмом  $G$ .

- 1) Убедитесь, что абелевы группы  $n$ -абелевы для всех  $n \in \mathbb{Z}$ .
- 2) Пусть группа  $A$  имеет экспоненту  $n$ , группа  $B$  имеет экспоненту  $n - 1$ , группа  $C$  — абелева,  $X \leq A \times B \times C$ . Если  $\phi : X \rightarrow Y$  — эпиморфизм, то  $Y$   $n$ -абелева. Имеется теорема Алперина:  $Y$  —  $n$ -абелева группа тогда и только тогда, когда найдется группа  $A$  экспоненты  $n$ , группа  $B$  экспоненты  $n - 1$  и абелева группа  $C$  такие, что в  $A \times B \times C$  имеется подгруппа  $X$  и эпиморфизм  $\phi : X \rightarrow Y$ . Данное утверждение останется верным, если термин «группа» заменить на «конечная группа».

В ситуации, когда имеется морфизм  $\phi : G \rightarrow H$ , бывает удобным принять так называемое «соглашение о черте», согласно которому для  $x \in G$  и  $X \subseteq G$  мы обозначаем  $\bar{x} := x\phi$ ,  $\bar{X} := X\phi$ , а если  $x \in H$  или  $X \subseteq H$ , то  $\bar{x} := x\phi^{-1}$ ,  $\bar{X} := X\phi^{-1}$  соответственно. Иногда мы сразу будем обозначать морфизм  $G \rightarrow H$  чертой, и тогда мы пишем  $- : G \rightarrow H$ .

**Предложение 1.6.13.** Пусть  $\phi : G \rightarrow H$  — морфизм групп. Обозначим  $G' := H$ ,  $H' := G$ ,  $X \in \{G, H\}$ .

- 1) Если  $A \leq B \leq X$ , то  $\bar{A} \leq \bar{B} \leq X'$ .
- 2) Если  $A \trianglelefteq B \leq X$ , то  $\bar{A} \trianglelefteq \bar{B} \leq X'$ .
- 3) Если  $A \trianglelefteq \trianglelefteq B \leq X$ , то  $\bar{A} \trianglelefteq \trianglelefteq \bar{B} \leq X'$ .

*Доказательство.* Упражнение.  $\square$

**Определение 1.6.2.** Ядром  $\ker(\phi)$  морфизма групп  $\phi : A \rightarrow B$  называется множество  $\{x \in A : x\phi = 1\}$ .

**Упражнение 1.6.14.** Найдите ядра морфизмов из 1.6.1.

**Теорема 1.6.15.** Пусть  $\phi : G \rightarrow H$  — морфизм групп. Тогда  $\ker(\phi) \trianglelefteq G$ .

*Доказательство.* Так как  $\{1_H\} \trianglelefteq H$ , то из 1.6.13 следует, что  $\overline{\{1_H\}} \trianglelefteq \overline{H}$ . Так как  $\ker(\phi) = \overline{\{1_H\}}$ ,  $\overline{H} = G$ , то  $\ker(\phi) \trianglelefteq G$ .  $\square$

**Предложение 1.6.16.** Морфизм групп  $\phi : A \rightarrow B$  инъективен тогда и только тогда, когда  $\ker(\phi) = \{1\}$ .

*Доказательство.* Пусть  $\phi$  инъективно и  $a \in \ker(\phi)$ , тогда  $a\phi = 1 = 1\phi$ , следовательно,  $a = 1$  и  $\ker(\phi) = \{1\}$ . Обратно, пусть  $\ker(\phi) = \{1\}$  и  $x\phi = y\phi$ . Тогда

$$1 = (x\phi)(y\phi)^{-1} = (x\phi)(y^{-1}\phi) = (xy^{-1})\phi.$$

Отсюда следует, что  $xy^{-1} \in \ker(\phi) = \{1\}$ , следовательно,  $x = y$ .  $\square$

**Теорема 1.6.17.** Пусть  $\phi : G \rightarrow H$  — морфизм групп,  $S \subseteq G$ . Тогда  $\langle S \rangle \phi = \langle S\phi \rangle$ .

*Доказательство.* Так как  $S \subseteq \langle S \rangle$ , то  $S\phi \subseteq \langle S \rangle \phi \leq H$ . Следовательно,  $\langle S\phi \rangle \leq \langle S \rangle \phi$ . Обозначим  $K = \langle S\phi \rangle$ . Так как  $S\phi \subseteq K$ , то  $S \subseteq K\phi^{-1}$ , откуда  $\langle S \rangle \leq K\phi^{-1}$ . Тогда  $\langle S \rangle \phi \leq (K\phi^{-1})\phi \leq K$ . Таким образом,  $\langle S \rangle \phi \leq \langle S\phi \rangle$  и теорема доказана.  $\square$

**Теорема 1.6.18.** Пусть  $\alpha, \beta : G \rightarrow H$  — морфизмы групп,  $S \subseteq G$ ,  $G = \langle S \rangle$ . Тогда  $\alpha = \beta$  если и только если  $s\alpha = s\beta \ \forall s \in S$ .

*Доказательство.* Если  $\alpha = \beta$ , то  $s\alpha = s\beta \ \forall s \in S$ . Обратно, пусть  $s\alpha = s\beta \ \forall s \in S$ . Обозначим  $M = \{g \in G : g\alpha = g\beta\}$ . Очевидно,  $M \leq G$  и  $S \subseteq M$ . Но тогда  $\langle S \rangle \leq M$  и, так как  $G = \langle S \rangle$ , то  $M = G$ , то есть  $\alpha = \beta$ .  $\square$

**Теорема 1.6.19.** (Об эпиморфизме) Пусть  $\alpha : A \twoheadrightarrow B$  — эпиморфизм групп,  $\gamma : A \rightarrow C$  — произвольный морфизм групп, такой, что  $\ker(\alpha) \subseteq \ker(\gamma)$ . Тогда существует и только один морфизм  $\beta : B \rightarrow C$  такой, что коммутативна диаграмма

$$\begin{array}{ccc} & B & \\ \alpha \nearrow & & \searrow \beta \\ A & \xrightarrow{\gamma} & C \end{array} .$$

(то есть  $\alpha\beta = \gamma$ ). Если  $\ker(\alpha) = \ker(\gamma)$ , то  $\beta$  инъективен. Если  $\gamma$  сюръективен, то и  $\beta$  сюръективен.

*Доказательство.* Пусть  $\phi : G \rightarrow H$  — морфизм групп,  $x, y \in G$ .

$$x\phi = y\phi \Leftrightarrow (x\phi)^{-1}(y\phi) = 1 \Leftrightarrow (x^{-1}\phi)(y\phi) = 1 \Leftrightarrow (x^{-1}y)\phi = 1 \Leftrightarrow x^{-1}y \in \ker(\phi).$$

Таким образом,  $x\phi = y\phi \Leftrightarrow x^{-1}y \in \ker(\phi)$ . Из этого замечания и условия  $\ker(\alpha) \subseteq \ker(\gamma)$  следует, что выполнены все условия теоремы 5.1.11, из которой следует, что существует и единственно отображение  $\beta : B \rightarrow C$ , для которого коммутативна наша диаграмма.

Докажем, что  $\beta$  — морфизм. Пусть  $b_1, b_2 \in B$ ,  $a_1, a_2 \in A$ ,  $b_i = a_i\alpha$ ,  $i \in \{1, 2\}$ .

$$\begin{aligned} (b_1b_2)\beta &= ((a_1\alpha)(a_2\alpha))\beta = ((a_1a_2)\alpha)\beta = (a_1a_2)\gamma = (a_1\gamma)(a_2\gamma) = (a_1\alpha\beta)(a_2\alpha\beta) = \\ &= (b_1\beta)(b_2\beta). \end{aligned}$$

Пусть  $\ker(\alpha) = \ker(\gamma)$ . Покажем, что  $\beta$  инъективно. Пусть  $x, y \in A$ . Так как  $\ker(\alpha) = \ker(\gamma)$ , то  $x\alpha = y\alpha \Leftrightarrow x\gamma = y\gamma$ . В силу теоремы о сюръективном отображении  $\beta$  инъективно.

Если  $\gamma$  сюръективно, то, в силу теоремы 5.1.11 о сюръективном отображении,  $\beta$  сюръективно.  $\square$

**Определение 1.6.3.** Если  $H$  — подгруппа  $G$  и  $a \in G$ , то множество  $aH$  (см. 1.1.8) называется *правым классом смежности элемента  $a$  по  $H$* . Аналогично, множество  $Ha$  называется *левым классом смежности  $a$  по  $H$* .

Если  $H \trianglelefteq G$ , то  $aH = Ha$  для всех  $a \in G$ , следовательно любой левый класс смежности по  $H$  является правым классом смежности и наоборот, поэтому говорят просто о классах смежности по  $H$ .

**Определение 1.6.4.** Пусть  $H \trianglelefteq G$ . Множество всех классов смежности  $G$  по  $H$  обозначается  $G/H$  и называется *фактор-группой  $G$  по  $H$* .

**Лемма 1.6.20.** Если  $\phi : A \rightarrow B$  — эпиморфизм группоидов и  $A$  — группа, то и  $B$  — группа.

*Доказательство.* Упражнение.  $\square$

**Теорема 1.6.21.** Пусть  $H \trianglelefteq G$ , тогда  $G/H$  — группа относительно операции умножения подмножеств  $G$ . Отображение  $\phi : G \rightarrow G/H$ , такое, что  $d\phi = Hd$  для всех  $g \in G$  является эпиморфизмом групп, причем  $\ker(\phi) = H$ .

*Доказательство.* Пусть  $a, b \in G$ . Тогда в силу нормальности  $H$

$$(Ha)(Hb) = HaHb = HHab = Hab \in G/H,$$

то есть

$$(Ha)(Hb) = H(ab). \quad (1.6.1)$$

Таким образом, произведение двух элементов  $G/H$  — элемент  $G/H$ . Следовательно, относительно операции умножения подмножеств  $G$  множество  $G/H$  — группоид. С другой стороны, соотношение 1.6.1 означает, что  $(a\phi)(b\phi) = (ab)\phi$  для любых  $a, b \in G$ , то есть  $\phi$  — морфизм. Очевидно,  $G\phi = G/H$ , то есть  $\phi$  — эпиморфизм группоидов. Согласно 1.6.20  $G/H$  — группа. Так как  $\phi$  — морфизм групп, то единица группы  $G/H$  совпадает с  $1\phi = H1 = H$ . Наконец,  $g \in \ker(\phi) \Leftrightarrow g\phi = 1 \Leftrightarrow Hg = H \Leftrightarrow g \in H$  в силу 1.4.2.  $\square$

Эпиморфизм  $\phi$  в дальнейшем будем называть естественным морфизмом  $G \rightarrow G/H$ .

**Теорема 1.6.22.** Пусть  $\phi : G \rightarrow H$  — морфизм групп. Тогда  $G\phi \simeq G/\ker(\phi)$ .

*Доказательство.* Обозначим  $H' := G\phi$ . Мы можем рассматривать  $\phi$  как эпиморфизм  $G \rightarrow H'$ . Этот эпиморфизм обозначим  $\phi'$ . Ясно, что  $\ker(\phi) = \ker(\phi')$ . Пусть  $K = \ker(\phi')$  и  $\nu : G \rightarrow G/K$  — естественный морфизм, тогда  $\ker(\nu) = \ker(\phi')$ . Так как  $\nu$  — эпиморфизм, то, в силу теоремы об эпиморфизмах 1.6.19, существует морфизм  $\psi : G/K \rightarrow H'$ , такой, что  $\nu\psi = \phi'$ . Так как  $\ker(\nu) = \ker(\phi')$ , то  $\psi$  инъективно, а из сюръективности  $\phi'$  следует сюръективность  $\psi$ , поэтому  $\psi$  — изоморфизм.  $\square$

**Теорема 1.6.23.** Пусть  $G$  — группа,  $N \trianglelefteq G$ ,  $A \leq G$ . Тогда  $A \cap N \trianglelefteq A$  и  $AN/N \simeq A/A \cap N$ .

*Доказательство.* Пусть  $\phi : G \rightarrow G/N$  — естественный морфизм,  $\phi' : A \rightarrow G/N$  — такое отображение, что  $a\phi' = a\phi$  для всех  $a \in A$ . Очевидно,  $\phi'$  — морфизм и  $\ker(\phi') = A \cap \ker(\phi) = A \cap N$ , поэтому  $A \cap N \trianglelefteq A$ .

$$AN/N = (AN)\phi = (A\phi)(N\phi) = (A\phi)\{1\} = A\phi = A\phi' \simeq A/\ker(\phi') = A/A \cap N.$$

$\square$

**Лемма 1.6.24.** Пусть  $\phi : G \rightarrow G'$  — морфизм групп,  $A \subseteq G$ . Тогда  $\overline{A} = A\ker(\phi)$ .

*Доказательство.* Обозначим  $K = \ker(\phi)$  и воспользуемся соглашением о черте для  $\phi$ . Очевидно,  $\overline{AK} = \overline{A}\overline{K} = \overline{A}\{1\} = \overline{A}$ , поэтому  $AK \subseteq \overline{A}$ . Обратно, пусть  $g \in \overline{A}$ , тогда  $\bar{g} \in \overline{A}$ , следовательно,  $\bar{g} = \bar{a}$  для некоторого  $a \in A$ . Отсюда выводим, что  $1 = \bar{a}^{-1}\bar{g} = \overline{a^{-1}g}$ , то есть  $a^{-1}g \in K$ . Умножая на  $a$  получаем, что  $g \in AK$ . Таким образом,  $AK \supseteq \overline{A}$ .  $\square$

**Следствие 1.6.25.** Пусть  $\phi : G \rightarrow H$  — эпиморфизм групп,  $K = \ker(\phi)$ . Если  $A \subseteq G$ , то  $A\phi = H \Leftrightarrow G = AK$ .

**Теорема 1.6.26.** Пусть  $G$  — группа. Выполняются следующие утверждения:

- 1) пусть  $\phi : G \rightarrow H$  — морфизм групп,  $N = \ker(\phi)$ . Если  $N \leq B \trianglelefteq A \leq G$ , то  $A\phi/B\phi \simeq A/B$ ;
- 2) если  $N \trianglelefteq G$ ,  $N \leq B \trianglelefteq A \leq G$ , то

$$(A/N)/(B/N) \simeq A/B;$$

*Доказательство.* 1. Воспользуемся соглашением о черте для эпиморфизма  $\alpha : A \rightarrow A\phi$ , где  $a\alpha = a\phi$  для всех  $a \in A$ . В силу 1.6.13  $\overline{B} \trianglelefteq \overline{A}$ . Рассмотрим эпиморфизмы ( $\beta$  — естественный эпиморфизм)  $A \xrightarrow{\alpha} \overline{A} \xrightarrow{\beta} \overline{A}/\overline{B}$  и их композицию  $\gamma = \alpha\beta$ . Тогда  $\gamma : A \rightarrow \overline{A}/\overline{B}$  — эпиморфизм (т.к. произведение сюръективных отображений сюръективно) и

$$\ker(\gamma) = (1)\gamma^{-1} = (1\beta^{-1})\alpha^{-1} = \ker(\beta)\alpha^{-1} = \overline{B}\alpha^{-1} = \overline{\overline{B}}.$$

В силу 1.6.24,  $\overline{\overline{B}} = BN = B$ , так как  $N \leq B$ . Итак,  $\gamma : A \rightarrow \overline{A}/\overline{B}$  — эпиморфизм и  $\ker(\gamma) = B$ . В силу 1.6.22  $\overline{A}/\overline{B} \simeq A/B$ .

2. Нужно в качестве  $\phi$  взять естественный эпиморфизм  $A \rightarrow A/N$ .  $\square$

**Теорема 1.6.27.** Пусть  $G$  — группа,  $B \trianglelefteq A \leq G$ ,  $C \leq G$ . Тогда  $B \cap C \trianglelefteq A \cap C$  и  $A \cap C / B \cap C$  вкладывается в  $A/B$ .

*Доказательство.*

$$A/B \geq (A \cap C)B/B \simeq (A \cap C)/(A \cap C \cap B) = A \cap C / B \cap C.$$

$\square$

Следующая теорема обобщает 1.6.26.

**Теорема 1.6.28.** Пусть  $G$  — группа,  $B \trianglelefteq A \leq G$ ,  $N \trianglelefteq G$ . Тогда  $(A \cap N)B/B \trianglelefteq A/B$  и

$$(AN/N)/(BN/N) \simeq (A/B)/((A \cap N)B/B),$$

причем  $(A \cap N)B/B \simeq A \cap N/B \cap N$ .

*Доказательство.* Так как  $B \leq A$ , то  $A = AB$ , поэтому  $AN = ABN$ . В силу модулярного тождества 1.4.14,  $A \cap BN = B(N \cap A)$ .

$$(AN/N)/(BN/N) \simeq AN/BN = ABN/BN = A/(A \cap BN) = A/B(N \cap A) \simeq$$

$$(A/B)/(B(N \cap A)/B),$$

$$(A \cap N)B/B \simeq A \cap N/A \cap N \cap B = A \cap N/B \cap N.$$

□

**Теорема 1.6.29.** (О соответствии) Пусть  $\phi : G \rightarrow H$  — эпиморфизм групп,  $K = \ker(\phi)$ ,  $K \leq A, B \leq G$  или  $A, B \leq H$ . Тогда имеют место следующие утверждения:

- 1)  $\overline{\overline{A}} = A$ . Если  $X \subseteq G$ , то  $\overline{\overline{X}} = XK$ ;
- 2)  $A \leq B \Leftrightarrow \overline{A} \leq \overline{B}$ ;
- 3)  $A = B \Leftrightarrow \overline{A} = \overline{B}$ ;
- 4)  $A \trianglelefteq B \Leftrightarrow \overline{A} \trianglelefteq \overline{B}$ ;
- 5) если  $B \leq A$ , то  $[A : B] = [\overline{A} : \overline{B}]$  (см. 2.3.1);
- 6) если  $B \trianglelefteq A$ , то  $A/B \simeq \overline{A}/\overline{B}$ ;
- 7)  $\overline{A \cap B} = \overline{A} \cap \overline{B}$ ;
- 8)  $\overline{N_B(A)} = N_{\overline{B}}(\overline{A})$ .

*Доказательство.*

1. Если  $X \subseteq G$ , то из 1.6.24 извлекаем, что  $\overline{\overline{X}} = XK$ , что при  $K \leq X \leq G$  дает  $\overline{\overline{X}} = X$ . Если  $A \leq H$ , то из сюръективности  $\phi$  следует, что  $\overline{\overline{A}} = A$ .

2. Если  $A \leq B$ , то, очевидно,  $\overline{A} \leq \overline{B}$ . Обратно, пусть  $\overline{A} \leq \overline{B}$ . Тогда  $\overline{\overline{A}} \leq \overline{\overline{B}}$ , откуда  $A \leq B$ .

3.  $A = B \Leftrightarrow A \leq B$  и  $A \geq B \Leftrightarrow \overline{A} \leq \overline{B}$  и  $\overline{A} \geq \overline{B} \Leftrightarrow \overline{A} = \overline{B}$ .

4. Если  $A \trianglelefteq B$ , то, в силу 1.6.13,  $\overline{A} \trianglelefteq \overline{B}$ . Обратно, пусть  $\overline{A} \trianglelefteq \overline{B}$ . Как было только отмечено,  $\overline{\overline{A}} \trianglelefteq \overline{\overline{B}}$ , следовательно,  $A \trianglelefteq B$ .

5. Предположим, что  $B \leq A \leq G$ . Обозначим  $A/B = \{aB : a \in A\}$ ,  $\overline{A}/\overline{B} = \{\overline{aB} : a \in A\}$ . Если  $a \in A$ , то  $\overline{aB} = \overline{a}B \in \overline{A}/\overline{B}$ , поэтому существует отображение  $\psi : A/B \rightarrow \overline{A}/\overline{B}$  такое, что  $(aB)\psi = \overline{aB}$  для всех  $a \in A$ . Покажем, что  $\psi$  — биекция. Сначала докажем, что  $\psi$  инъективно. Пусть  $x, y \in A$  и  $(xB)\psi = (yB)\psi$ .

$$\overline{xB} = \overline{yB} \Rightarrow \overline{\overline{xB}} = \overline{\overline{yB}} \Rightarrow xBK = yBK \Rightarrow xB = yB.$$

Мы доказали, что  $\psi$  инъективно. Покажем, что  $\psi$  сюръективно. Любой элемент  $\overline{A}/\overline{B}$  можно записать в виде  $\overline{aB}$  для некоторого  $a \in A$ . Тогда  $\overline{aB} = (aB)\psi$ ,  $aB \in A/B$ , следовательно,  $\psi$  сюръективно. Итак,  $\psi : A/B \rightarrow \overline{A}/\overline{B}$  — биекция, поэтому  $[A : B] = [\overline{A} : \overline{B}]$ . Теперь пусть  $B \leq A \leq H$ . В силу только что доказанного,  $[\overline{A} : \overline{B}] = [\overline{\overline{A}} : \overline{\overline{B}}] = [A : B]$ .

6. Если  $A, B \leq G$ , то это было доказано ранее — теорема 1.6.26. Если  $A, B \leq H$ , то  $\overline{A}/\overline{B} \simeq \overline{\overline{A}}/\overline{\overline{B}} = A/B$ .

7. Если  $A, B \leq H$ , то, как известно,  $(A \cap B)\phi^{-1} = A\phi^{-1} \cap B\phi^{-1}$ . Пусть  $K \leq A, B \leq G$ ,  $A \cap B =: C$ . Очевидно,  $C$  — наибольшая подгруппа  $G$ , содержащая  $K$  и содержащаяся в  $A$  и  $B$ . Отсюда следует, что  $\overline{C}$  — наибольшая подгруппа  $\overline{G}$ , содержащаяся в  $\overline{A}$  и  $\overline{B}$ , то есть  $\overline{C} = \overline{A} \cap \overline{B}$ .

(8) Пусть  $K \leq A, B \leq G$  и  $g \in B$ . Тогда  $\overline{g} \in N_{\overline{B}}(\overline{A}) \Leftrightarrow \overline{A}^{\overline{g}} = \overline{A} \Leftrightarrow \overline{A}^g = \overline{A}$ . Так как  $K \leq A^g$ ,  $K \leq A$ , то  $\overline{A}^g = \overline{A} \Leftrightarrow A^g = A \Leftrightarrow g \in N_B(A)$ . Итак,  $\overline{g} \in N_{\overline{B}}(\overline{A}) \Leftrightarrow g \in N_B(A)$ . Отсюда  $\overline{N_B(A)} = N_{\overline{B}}(\overline{A})$ .

Теперь пусть  $A, B \leq H$ . В силу только что доказанного,  $\overline{N_B(A)} = N_{\overline{B}}(\overline{A}) = N_B(A)$ , поэтому  $\overline{\overline{N_B(A)}} = \overline{N_B(A)}$ , откуда  $N_{\overline{B}}(\overline{A}) = \overline{N_B(A)}$ .

□

## 1.7 Автоморфизмы

**Определение 1.7.1.** Пусть  $\mathcal{C}$  — категория,  $G \in \text{Ob}(\mathcal{C})$ . Изоморфизм  $G \rightarrow G$  называется автоморфизмом объекта  $G$ . Множество всех автоморфизмов объекта  $G$  обозначается  $\text{Aut}(G)$ .

В частности, автоморфизм группы  $G$  — это любой изоморфизм  $G \rightarrow G$ .

**Теорема 1.7.1.** Пусть  $\mathcal{C}$  — категория,  $G \in \text{Ob}(\mathcal{C})$ . Множество  $\text{Aut}(G)$  является группой относительно операции умножения морфизмов  $\mathcal{C}$ .

*Доказательство.* Эндоморфизмы  $G$  образуют моноид по операции умножения морфизмов, и  $\text{Aut}(G)$  — множество обратимых элементов данного моноида. В силу 1.2.2  $\text{Aut}(G)$  — группа.  $\square$

В частности, множество  $\text{Aut}(G)$  автоморфизмов группы  $G$  является группой по операции умножения отображений. Теорема 1.7.1 показывает, что группы вездесущи — с любым математическим объектом связана его группа автоморфизмов.

**Упражнение 1.7.2.** Всевозможные автоморфизмы и антиавтоморфизмы группы  $G$  образуют группу  $\text{Aut}^+(G)$ , причем  $\text{Aut}(G) \trianglelefteq \text{Aut}^+(G)$  (см. 4.1.20).

**Пример 1.7.1.** Пусть  $R$  — кольцо,  $M$  — левый  $R$ -модуль.  $R$ -модули и их морфизмы образуют категорию, поэтому возникает понятие автоморфизма  $R$ -модуля  $M$  — это любой обратимый морфизм  $M \rightarrow M$ . Автоморфизмы  $M$  образуют группу, которая обозначается  $\text{GL}(M)$ . Если  $M$  — свободный левый  $R$ -модуль с базисом  $e = (e_i)_{i \in I}$ , то, как было отмечено ранее, координатное отображение  $\phi : \text{End}(M) \rightarrow M_I(R)$ , каждому эндоморфизму  $\alpha$  модуля  $M$  сопоставляющее его матрицу  $\alpha_e$  в базисе  $e$ , является изоморфизмом колец, поэтому (в силу 1.6.4)  $\phi$  индуцирует изоморфизм групп обратимых элементов этих колец, а они равны  $\text{GL}(M)$  и  $\text{GL}_I(R)$ , поэтому  $\phi$  можно рассматривать как изоморфизм  $\text{GL}(M) \rightarrow \text{GL}_I(R)$ .

**Упражнение 1.7.3.** Пусть  $G$  — группа. Докажите следующие утверждения.

- 1) Отображение  $x \mapsto x^{-1}$  является автоморфизмом  $G$  тогда и только тогда, когда  $G$  абелева (но всегда является антиавтоморфизмом).
- 2) Если  $G$  — конечная абелева группа,  $n \in \mathbb{Z}$ , то отображение  $x \mapsto nx$  является автоморфизмом  $G$  тогда и только тогда, когда  $\gcd(n, |G|) = 1$ .
- 3) Если  $R$  — коммутативное кольцо,  $n \in \mathbb{N}$ , то отображение  $a \mapsto (a^{-1})^{tr}$  является автоморфизмом группы  $\text{GL}_n(R)$ .
- 4) Отображение  $(a_{p,q})_{p,q} \mapsto (\overline{a_{p,q}})_{p,q}$  является автоморфизмом группы  $\text{GL}_n(\mathbb{C})$ .
- 5) Если  $V$  — векторное пространство над телом  $D$ , то любой обратимый линейный оператор пространства  $V$  можно рассматривать как автоморфизм абелевой группы  $V$ .

**Определение 1.7.2.** Центром  $Z(G)$  группы  $G$  называется множество всех ее элементов, перестановочных с каждым элементом  $G$ , то есть

$$Z(G) = \{a \in G : ab = ba \ \forall b \in G\}.$$

Подмножество  $S \subseteq G$  называется центральным, если  $S \subseteq Z(G)$ .

Ясно, что группа  $G$  абелева тогда и только тогда, когда  $G = Z(G)$ . Очевидно,  $Z(G)$  — абелева нормальная подгруппа группы  $G$ .

**Предложение 1.7.4.** *Любое центральное подмножество группы нормально. В частности, любая центральная подгруппа — абелева нормальная.*

*Доказательство.* Это очевидно. □

**Определение 1.7.3.** Пусть  $A \subseteq G$ ,  $B \leq G$ . Множество элементов  $b \in B$ , перестановочных со всеми элементами  $A$ , называется централизатором  $A$  в  $B$  и обозначается  $C_B(A)$ .

**Теорема 1.7.5.** Пусть  $G$  — группа и для  $g \in G$   $\phi_g : G \rightarrow G$ ,  $x\phi_g = x^g$ . Тогда

- 1) для каждого  $g \in G$  отображение  $\phi_g$  является автоморфизмом  $G$ ;
- 2) отображение  $\phi : g \mapsto \phi_g$  является морфизмом  $G \rightarrow \text{Aut}(G)$ ;
- 3)  $\ker(\phi) = Z(G)$ ;
- 4)  $\phi$  — вложение тогда и только тогда, когда  $Z(G) = \{1\}$ ;
- 5)  $\phi_g^\sigma = \phi_{g\sigma}$  для всех  $g \in G$  и  $\sigma \in \text{Aut}(G)$ ;
- 6) если обозначить  $\text{Inn}(G) := \phi(G)$  то  $\text{Inn}(G) \trianglelefteq \text{Aut}(G)$ ;
- 7)  $\text{Inn}(G) \simeq G/Z(G)$ ;
- 8)  $C_{\text{Aut}(G)}(\text{Inn}(G)) = C_{\text{Aut}(G)}(G/Z(G))$ , где  $C_{\text{Aut}(G)}(G/Z(G))$  — множество всех  $\sigma \in \text{Aut}(G)$  таких, что для каждого  $g \in G$  выполняется равенство  $(gZ(G))\sigma = gZ(G)$ ;
- 9) если  $Z(G) = \{1\}$ , то и  $C_{\text{Aut}(G)}(\text{Inn}(G)) = \{1\}$ , в частности,  $Z(\text{Aut}(G)) = \{1\}$ .

*Доказательство.* Упражнение. □

Мы видим, что если  $Z(G) = \{1\}$ , то и  $Z(\text{Aut}(G)) = \{1\}$ , причем можно считать (отождествляя  $g \in G$  и  $\phi_g$ ), что  $G \trianglelefteq \text{Aut}(G)$ , кроме того,  $C_{\text{Aut}(G)}(G) = \{1\}$ . Например, это верно для простой неабелевой группы  $G$ . Группа  $G$  называется полной (complete), если  $Z(G) = \{1\}$  и  $\text{Aut}(G) = \text{Inn}(G)$ . Очевидно,  $G$  полна тогда и только тогда, когда морфизм  $\phi$  из 1.7.5 является изоморфизмом.

**Определение 1.7.4.** Автоморфизм  $\phi_g$  из 1.7.5 называется внутренним автоморфизмом  $G$ , индуцированным элементом  $g$ . Группа  $\text{Inn}(G)$  называется группой внутренних автоморфизмов  $G$ .

Так как  $\text{Inn}(G) \trianglelefteq \text{Aut}(G)$ , то можно построить факторгруппу  $\text{Aut}(G)/\text{Inn}(G)$ . Эта группа называется группой внешних автоморфизмов  $G$  и обозначается  $\text{Out}(G)$ .

Если  $H$  — нормальная подгруппа группы  $G$ , и  $\sigma \in \text{Inn}(G)$ , то  $H\sigma = H$ , поэтому можно рассматривать сужение  $\sigma|_H$  (см. 5.1.13), которое, очевидно, является автоморфизмом  $H$ . Ясно, что отображение  $\text{Inn}(G) \ni \sigma \mapsto \sigma|_H \in \text{Aut}(H)$  является морфизмом. Назовем этот морфизм морфизмом ограничения.

**Предложение 1.7.6.** Пусть  $G$  — группа,  $H \trianglelefteq G$ . Тогда существует и единственен такой морфизм  $G/H \rightarrow \text{Out}(H)$ , что  $gH \mapsto (\phi_g|_H) \text{Inn}(H)$  для всех  $g \in G$ .

*Доказательство.* Пусть  $\phi : G \rightarrow \text{Inn}(G)$  как в 1.7.5,  $\alpha : \text{Inn}(G) \rightarrow \text{Aut}(H)$  — морфизм ограничения,  $\beta : \text{Aut}(H) \rightarrow \text{Out}(H)$  — естественный эпиморфизм. Тогда  $\psi := \phi\alpha\beta$  — морфизм  $G \rightarrow \text{Out}(H)$ . Обозначим  $\nu : G \rightarrow G/H$  — естественный эпиморфизм. Если  $h \in H$ , то  $\phi_h|_H \in \text{Inn}(H)$ , поэтому  $H \leq \ker(\psi)$ . В силу 1.6.19 существует ровно один морфизм  $\theta$  такой, что коммутативна диаграмма

$$\begin{array}{ccc} & G/H & \\ \nu \nearrow & & \searrow \theta \\ G & \xrightarrow{\psi} & \text{Out}(H) \end{array}.$$

Очевидно,  $(gH)\theta = (\phi_g|_H) \text{Inn}(H)$  для всех  $g \in G$ . □

Морфизм  $\theta : G/H \rightarrow \text{Out}(H)$  будем называть естественным.

**Определение 1.7.5.** Подгруппа  $H$  группы  $G$  называется характеристической, если  $H\phi \leq H$  для любого  $\phi \in \text{Aut}(G)$ . Если  $H$  — характеристическая подгруппа  $G$ , то мы пишем  $H \text{ char } G$ .

Например, единичная подгруппа и сама группа  $G$  — характеристические подгруппы  $G$ . Легко убедиться, что центр группы  $G$  — характеристическая подгруппа. Следующее утверждение очевидно.

**Предложение 1.7.7.** Любая характеристическая подгруппа нормальна.

В частности,  $Z(G) \trianglelefteq G$ .

**Предложение 1.7.8.** Если  $H \text{ char } G$ , то  $H\phi = H$  для всех  $\phi \in \text{Aut}(G)$ .

*Доказательство.* Пусть  $\phi \in \text{Aut}(G)$ , тогда  $\phi^{-1} \in \text{Aut}(G)$  и, так как  $H \text{ char } G$ , то  $H\phi \leq H$  и  $H\phi^{-1} \leq H$ .

$$H\phi^{-1} \leq H \Rightarrow (H\phi^{-1})\phi \leq H\phi \Rightarrow H \leq H\phi,$$

поэтому  $H\phi = H$ . □

**Определение 1.7.6.** Мы называем подгруппу  $H$  группы  $G$  вполне характеристической, если  $H\phi \leq H$  для любого  $\phi \in \text{End}(G)$ .

Очевидно, вполне характеристическая подгруппа — характеристическая, следовательно, нормальная подгруппа.

**Теорема 1.7.9.** Пусть  $A, B$  — подгруппы группы  $G$ .

- 1) Если  $A \text{ char } B \text{ char } G$ , то  $A \text{ char } G$ .
- 2) Если  $A \text{ char } B \trianglelefteq G$ , то  $A \trianglelefteq G$ .
- 3) Если  $A, B \text{ char } G$ , то и  $A \cap B, AB \text{ char } G$ .

*Доказательство.* 1. Пусть  $\varphi \in \text{Aut}(G)$ . Так как  $B \text{ char } G$ , то  $B\varphi \leq B$ , поэтому мы можем рассматривать отображение  $\phi' : B \rightarrow B$ ,  $b\phi' = b\varphi$ . Очевидно,  $\phi' \in \text{Aut}(B)$ . Из  $A \text{ char } B$  следует, что  $A\phi' \leq A$ , то есть  $A\phi \leq A$ .

2. Пусть  $g \in G$ . Так как  $B \trianglelefteq G$ , то  $B^g = B$ , и мы можем рассматривать отображение  $\phi : B \rightarrow B$ ,  $b\phi = b^g$  для всех  $b \in B$ . Легко видеть, что  $\phi \in \text{Aut}(B)$ . Так как  $A \text{ char } B$ , то  $A = A\phi = A^g$ , поэтому  $A \trianglelefteq G$ .

3. Пусть  $\phi \in \text{Aut}(G)$ . Тогда

$$(A \cap B)\phi = A\phi \cap B\phi = A \cap B,$$

$$(AB)\phi = (A\phi)(B\phi) = AB.$$

□

Аналогично доказывается следующая теорема.

**Теорема 1.7.10.** Пусть  $A, B$  — подгруппы группы  $G$ ,  $A$  вполне характеристична в  $B$ ,  $B$  вполне характеристична в  $G$ . Тогда  $A$  вполне характеристична в  $G$ .

## 1.8 Композиционные ряды

**Определение 1.8.1.** Пусть имеется субнормальный ряд

$$\{1\} = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_n = G.$$

Группы  $G_i/G_{i-1}$  называются его факторами. Субнормальный ряд от  $\{1\}$  до  $G$  с простыми факторами называется композиционным. Факторы композиционного ряда называются композиционными факторами группы  $G$ .

**Лемма 1.8.1.** Пусть  $G$  — группа,  $A \trianglelefteq G$ ,  $- : G \rightarrow G/A$  — естественный эпиморфизм,  $(A_i)_{i=0}^m$  — композиционный ряд для  $A$ ,  $(B_i)_{i=0}^n$  — композиционный ряд для  $\overline{G}$ . Тогда

$$\{1\} = A_0 \triangleleft A_1 \triangleleft \dots \triangleleft A_m \triangleleft \overline{B_1} \triangleleft \dots \triangleleft \overline{B_n} = G$$

— композиционный ряд для  $G$ .

*Доказательство.* Это следует из 1.6.29. □

**Определение 1.8.2.** Подгруппа  $A$  группы  $G$  называется максимальной нормальной, если  $A \triangleleft G$  и нет подгрупп  $B \leq G$  таких, что  $A < B \triangleleft G$ .

**Лемма 1.8.2.** Пусть  $G$  — конечная группа,  $H \triangleleft G$ . Тогда найдется такая максимальная нормальная подгруппа  $M$  группы  $G$ , что  $H \leq M$ .

*Доказательство.* Очевидно, любая подгруппа максимального возможного порядка из множества  $\{A \triangleleft G : H \leq A\}$  подходит на роль  $M$ . □

В частности, в неединичной конечной группе есть максимальные нормальные подгруппы.

**Лемма 1.8.3.** Нормальная подгруппа  $A$  группы  $G$  является максимальной нормальной тогда и только тогда, когда  $G/A$  — простая группа.

*Доказательство.* Пусть  $A$  — нормальная подгруппа  $G$  и применим соглашение о черте к естественному эпиморфизму  $G \rightarrow G/A$ . Предположим, что  $A$  — максимальная нормальная подгруппа  $G$  и покажем, что  $\overline{G}$  проста. Так как  $A \triangleleft G$ , то  $\overline{G} \neq \{1\}$ . Пусть  $B \trianglelefteq \overline{G}$ . В силу 1.6.29  $A \leq \overline{B} \trianglelefteq G$ . Так как  $A$  — максимальная нормальная, то либо  $\overline{B} = A$ , либо  $\overline{B} = G$ . Следовательно, либо  $B = \{1\}$ , либо  $B = \overline{G}$ . Таким образом,  $\overline{G} \neq \{1\}$  и  $\overline{G}$  не имеет нетривиальных нормальных подгрупп, то есть  $\overline{G}$  проста. Обратно, пусть  $\overline{G}$  проста. Допустим, что  $A < B \triangleleft G$ . Тогда в силу 1.6.29  $\{1\} < \overline{B} \triangleleft \overline{G}$  — противоречие, так как  $\overline{G}$  проста. □

**Теорема 1.8.4.** *Любая конечная группа имеет композиционный ряд.*

*Доказательство.* Допустим, что это не так, и  $G$  — минимальный контрпример. Тогда  $G \neq \{1\}$  и  $G$  имеет максимальную нормальную подгруппу  $M$ . Так как  $|M| < G$ , то  $M$  имеет композиционный ряд. Согласно 1.8.3 группа  $G/M$  проста и в силу 1.8.1  $G$  имеет композиционный ряд — противоречие.  $\square$

Не каждая бесконечная группа имеет композиционный ряд.

**Определение 1.8.3.** *Длиной  $\ell(G)$  группы  $G$ , имеющей композиционный ряд, назовем минимум длин композиционных рядов группы  $G$ .*

**Лемма 1.8.5.** *Пусть  $G$  — группа,  $A, B \triangleleft G$ , группы  $G/A$ ,  $G/B$  просты. Тогда выполняется одно из следующих утверждений:*

1)  $A = B$ .

2)  $G = AB$ , и тогда, если обозначить  $C = A \cap B$ , то  $G/A \simeq B/C$  и  $G/B \simeq A/C$ .

*Доказательство.* Заметим, что  $BA/A \trianglelefteq G/A$ . Так как  $G/A$  — простая группа, то  $BA/A = \{1\}$  или  $BA/A = G/A$ , следовательно, либо  $BA = A$ , либо  $BA = G$ . Допустим, что  $AB = A$ , тогда  $B \leq A$ . Отсюда следует, что  $A/B \trianglelefteq G/B$ . Так как  $G/B$  — простая группа, то  $A/B = \{1\}$  или  $A/B = G/B$ . Если  $A/B = G/B$ , то  $A = G$ , что невозможно, поэтому  $A/B = \{1\}$ , то есть  $A = B$ . Предположим, что  $BA = G$ . Обозначим  $C := A \cap B$ . Заметим, что

$$G/A = BA/A \simeq B/B \cap A = B/C,$$

$$G/B = AB/B \simeq A/A \cap B = A/C.$$

Итак,  $G/A \simeq B/C$ ,  $G/B \simeq A/C$ .  $\square$

Для удобства последующего рассуждения введем некоторый формализм. Две строки  $(A_i)_{i=1}^m$ ,  $(B_j)_{j=1}^n$  групп назовем эквивалентными и напишем  $(A_i)_{i=1}^m \sim (B_j)_{j=1}^n$ , если  $m = n$ , и найдется перестановка  $\sigma \in S_n$  такая, что  $A_{i\sigma} \simeq B_i$  для всех  $1 \leq i \leq n$ . Кроме того, мы воспользуемся операцией соединения строк:

$$(A_i)_{i=1}^m (B_j)_{j=1}^n = (A_1, \dots, A_m, B_1, \dots, B_n).$$

**Теорема 1.8.6.** *Пусть*

$$\{1\} = A_0 \triangleleft A_1 \triangleleft \dots \triangleleft A_m = G,$$

$$\{1\} = B_0 \triangleleft B_1 \triangleleft \dots \triangleleft B_n = G$$

— композиционные ряды группы  $G$ . Тогда  $m = n$  и найдется такая перестановка  $\sigma \in S_n$ , что  $A_{i\sigma}/A_{i\sigma-1} \simeq B_i/B_{i-1}$  для всех  $1 \leq i \leq n$ .

*Доказательство.* Докажем, что для любой группы, имеющей композиционный ряд, верна не только рассматриваемая теорема, но и то, что любая ее нормальная подгруппа, факторгруппа по которой проста, тоже имеет композиционный ряд. Предположим, что это неверно, и  $G$  — контрпример минимальной длины  $\ell(G) = m$ . Очевидно,  $m, n > 1$ . Обозначим  $A := A_{m-1}$ ,  $B := B_{n-1}$ . В силу 1.8.5 либо  $A = B$ , либо  $BA = G$ .

Допустим, что  $A = B$ . Группа  $A$  имеет композиционный ряд длины  $m-1$ , поэтому  $\ell(A) < m$ , следовательно, для  $A$  утверждение верно. Таким образом,

$$(A_i/A_{i-1})_{i=1}^{m-1} \sim (B_j/B_{j-1})_{j=1}^{n-1}.$$

Очевидно,  $A_m/A_{m-1} \simeq B_n/B_{n-1}$ , следовательно,

$$(A_i/A_{i-1})_{i=1}^m = (A_i/A_{i-1})_{i=1}^{m-1}(A_m/A_{m-1}) \sim (B_j/B_{j-1})_{j=1}^{n-1}(B_n/B_{n-1}) = (B_j/B_{j-1})_{j=1}^n.$$

Предположим, что  $BA = G$ . В силу 1.8.5  $G/A \simeq B/C$ ,  $G/B \simeq A/C$ . Так как для  $A$  доказываемое утверждение верно, и  $C \leq A$ , то в  $C$  имеется композиционный ряд  $\{1\} = C_0 \triangleleft C_1 \triangleleft \dots \triangleleft C_p = C$ . Так как  $A/C \simeq G/B$ , то  $\{1\} = C_0 \triangleleft C_1 \triangleleft \dots \triangleleft C_p \triangleleft A$  — композиционный ряд для  $A$ . В силу верности для  $A$  доказываемого утверждения,

$$(A_i/A_{i-1})_{i=1}^{m-1} \sim (C_i/C_{i-1})_{i=1}^p(A/C).$$

В частности,  $m-1 = p+1$ , откуда  $p = m-2$ . Отсюда следует, что

$$(A_i/A_{i-1})_{i=1}^m \sim (C_i/C_{i-1})_{i=1}^{m-2}(A/C)(G/A).$$

Так как  $B/C \simeq G/A$  — простая группа, то

$$\{1\} = C_0 \triangleleft C_1 \triangleleft \dots \triangleleft C_{m-2} = C \triangleleft B$$

— композиционный ряд для  $B$ . В частности,  $\ell(B) < m$ , следовательно, для  $B$  выполняется доказываемое утверждение, и

$$(B_i/B_{i-1})_{i=1}^{n-1} \sim (C_i/C_{i-1})_{i=1}^{m-2}(B/C).$$

Отсюда выводим, что

$$(B_i/B_{i-1})_{i=1}^n \sim (C_i/C_{i-1})_{i=1}^{m-2}(B/C)(G/B) \sim (C_i/C_{i-1})_{i=1}^{m-2}(G/A)(A/C) \sim (A_i/A_{i-1})_{i=1}^m.$$

Итак, любые два композиционных ряда  $G$  эквивалентны. Так как  $G$  — контрпример к доказываемому утверждению, то найдется такая нормальная подгруппа  $H \triangleleft G$ , что  $G/H$  проста, и  $H$  не имеет композиционного ряда. В силу 1.8.5 либо  $A = H$ , либо  $G =$

*АН.* Если  $A = H$ , то в  $H$  есть композиционный ряд  $\{1\} = A_0 \triangleleft A_1 \triangleleft \dots \triangleleft A_{m-1} = A$ . Допустим, что  $G = AH$  и обозначим  $I := A \cap H$ . В силу 1.8.5  $G/A \simeq H/I$ ,  $G/H \simeq A/I$ , следовательно,  $A/I$  — простая группа. Так как  $\ell(A) < m$ , то в  $I$  найдется композиционный ряд. Так как  $H/I \simeq G/A$  — простая группа, то  $H$  имеет композиционный ряд — противоречие.  $\square$

Мы видим, что любые два композиционных ряда группы  $G$  имеют одинаковые длины и одинаковые наборы композиционных факторов. Следовательно, они зависят лишь от самой группы  $G$ . В частности,  $\ell(G)$  равна длине любого композиционного ряда  $G$ .

**Теорема 1.8.7.** Пусть  $G$  — группа,  $H \trianglelefteq G$ . Если  $H$  и  $G/H$  имеют композиционные ряды, то и  $G$  имеет композиционный ряд, причем  $\ell(G) = \ell(H) + \ell(G/H)$ .

*Доказательство.* Это следует из 1.8.1 и 1.8.6.  $\square$

## Глава 2

# Действия групп на множествах

### 2.1 Первые определения

**Определение 2.1.1.** Правым действием группы  $G$  на множестве  $\Omega$  называется любое умножение  $\Omega \times G \rightarrow \Omega$ , удовлетворяющее следующим условиям:

- 1)  $\omega 1 = \omega$  для всех  $\omega \in \Omega$ ;
- 2)  $\omega(ab) = (\omega a)b$  для всех  $a, b \in G$  и  $\omega \in \Omega$ .

Правые действия будем просто называть действиями.

**Определение 2.1.2.** Левым действием группы  $G$  на множестве  $\Omega$  называется любое умножение  $G \times \Omega \rightarrow \Omega$ , удовлетворяющее следующим условиям:

- 1)  $1\omega = \omega$  для всех  $\omega \in \Omega$ ;
- 2)  $(ab)\omega = a(b\omega)$  для всех  $a, b \in G$  и  $\omega \in \Omega$ .

**Определение 2.1.3.** Перестановочным представлением группы  $G$  на множестве  $\Omega$  называется произвольный морфизм  $G \rightarrow \text{Sym}(\Omega)$ .

Далее мы покажем, что понятия левого действия, правого действия и перестановочного представления группы  $G$  на множестве  $\Omega$  равносильны.

**Лемма 2.1.1.** Пусть группа  $G$  действует слева на множестве  $\Omega$ . Определим умножение  $\Omega \times G \rightarrow \Omega$  равенством  $\omega g := g^{-1}\omega$  для всех  $\omega \in \Omega$ ,  $g \in G$ . Тогда данное умножение является правым действием  $G$  на  $\Omega$ .

Указанное правое действие будем называть ассоциированным с исходным левым действием.

*Доказательство.* Пусть  $\omega \in \Omega$ ,  $a, b \in G$ .

$$\omega 1 = 1^{-1}\omega = 1\omega = \omega,$$

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

□

Аналогично проверяется следующая лемма.

**Лемма 2.1.2.** Пусть группа  $G$  действует справа на множестве  $\Omega$ . Определим умножение  $G \times \Omega \rightarrow \Omega$  равенством  $g\omega := \omega g^{-1}$  для всех  $g \in G$ ,  $\omega \in \Omega$ . Тогда данное умножение является левым действием  $G$  на  $\Omega$ .

Это левое действие будем называть ассоциированным с исходным правым действием.

**Теорема 2.1.3.** Пусть  $G$  — группа,  $\Omega$  — множество,  $L$  — множество левых действий  $G$  на  $\Omega$ ,  $R$  — множество правых действий  $G$  на  $\Omega$ ,  $\alpha$  — отображение  $L \rightarrow R$ , каждому левому действию  $G$  на  $\Omega$ , сопоставляющее ассоциированное правое действие. Тогда  $\alpha$  — биекция.

*Доказательство.* Пусть  $\iota : G \times \Omega \rightarrow \Omega \times G$ ,  $\iota(g, \omega) := (\omega, g^{-1})$ ,  $\kappa : \Omega \times G \rightarrow G \times \Omega$ ,  $\kappa(\omega, g) := (g^{-1}, \omega)$ . Тогда  $\iota$  и  $\kappa$  взаимно обратны, и если  $f \in L$ , то  $\kappa f \in R$ , а если  $f \in R$ , то  $\iota f \in L$ . Очевидно,  $f\alpha = \kappa f$  для всех  $f \in L$ . Пусть  $\beta$  — отображение  $R \rightarrow L$ , каждому правому действию  $G$  на  $\Omega$  сопоставляющее ассоциированное левое действие, тогда  $f\beta = \iota f$  для всех  $f \in R$ . Покажем, что  $\alpha, \beta$  взаимно обратны. Пусть  $f \in L$ , тогда

$$f\alpha\beta = \kappa f\beta = \kappa \iota f = f,$$

Пусть  $f \in R$ .

$$f\beta\alpha = \iota f\alpha = \iota \kappa f = f.$$

Итак, отображения  $\alpha, \beta$  взаимно обратны, поэтому  $\alpha$  — биекция. □

Таким образом, понятия левого и правого действий, по сути, равносильны. Напомним, что множество обратимых элементов моноида  $M$  является группой относительно операции умножения  $M$ , которую мы обозначаем  $M^*$ .

**Лемма 2.1.4.** Пусть  $G$  — группа,  $M$  — моноид и  $\phi : G \rightarrow M$  — произвольное отображение. Если  $\phi$  — морфизм моноидов, то  $G\phi \subseteq M^*$ .

*Доказательство.* Это следует из 1.6.3. □

**Лемма 2.1.5.** Пусть группа  $G$  действует на множестве  $\Omega$ . Для каждого  $g \in G$  обозначим  $\rho_g : \Omega \rightarrow \Omega$  такое отображение, что  $\omega\rho_g = \omega g$  для любого  $\omega \in \Omega$ . Тогда отображение  $\rho : g \mapsto \rho_g$  является перестановочным представлением  $G$  на  $\Omega$ .

*Доказательство.* В силу 2.1.4 достаточно доказать, что  $\rho$  — морфизм моноида  $G$  в моноид всех отображений  $\Omega \rightarrow \Omega$ . Пусть  $\omega \in \Omega$ . Тогда  $\omega\rho_1 = \omega 1 = \omega$ , поэтому  $\rho_1 = 1_\Omega$ . Пусть  $a, b \in G$ , тогда

$$\omega\rho_{ab} = \omega(ab) = (\omega a)b = (\omega\rho_a)\rho_b = \omega(\rho_a\rho_b),$$

следовательно,  $\rho_{ab} = \rho_a\rho_b$ . □

Морфизм  $\rho : G \rightarrow \text{Sym}(\Omega)$  назовем перестановочным представлением  $G$  на  $\Omega$ , ассоциированным с исходным действием  $G$  на  $\Omega$ .

**Следствие 2.1.6.** Если  $G$  действует на множестве  $\Omega$  и  $g \in G$ , то отображение  $\omega \mapsto \omega g$  является биекцией  $\Omega \rightarrow \Omega$ .

**Лемма 2.1.7.** Пусть  $\rho : G \rightarrow \text{Sym}(\Omega)$  — перестановочное представление  $G$  на  $\Omega$ . Тогда умножение  $\Omega \times G \rightarrow \Omega$  такое, что  $\omega g = \omega\rho_g$  для всех  $\omega \in \Omega$ ,  $g \in G$ , является действием  $G$  на  $\Omega$ .

Это действие назовем ассоциированным с исходным перестановочным представлением  $\rho$ .

*Доказательство.* Пусть  $\omega \in \Omega$ ,  $a, b \in G$ , тогда

$$\omega 1 = \omega\rho_1 = \omega 1_\Omega = \omega,$$

$$\omega(ab) = \omega\rho_{ab} = \omega(\rho_a\rho_b) = (\omega\rho_a)\rho_b = (\omega a)b.$$

□

**Теорема 2.1.8.** Пусть  $G$  — группа,  $\Omega$  — множество,  $A$  — множество действий  $G$  на  $\Omega$ ,  $H = \text{Mor}(G, \text{Sym}(\Omega))$  — множество всех перестановочных представлений  $G$  на  $\Omega$ , отображение  $\alpha : A \rightarrow H$  каждому действию  $G$  на  $\Omega$  сопоставляет ассоциированное перестановочное представление  $G$  на  $\Omega$ . Тогда  $\alpha$  — биекция.

*Доказательство.* Пусть отображение  $\beta : H \rightarrow A$  каждому перестановочному представлению  $G$  на  $\Omega$  сопоставляет ассоциированное действие  $G$  на  $\Omega$ . Покажем, что  $\alpha, \beta$  взаимно обратны. Пусть  $f \in A, g \in G, \omega \in \Omega$ , тогда

$$(\omega, g)(f\alpha\beta) = (\omega, g)((f\alpha)\beta) = \omega(f\alpha)_g = (\omega, g)f,$$

следовательно,  $\alpha\beta = 1_A$ . Пусть  $\rho \in H$ , тогда

$$\omega(\rho(\beta\alpha))_g = \omega((\rho\beta)\alpha)_g = (\omega, g)(\rho\beta) = \omega\rho_g,$$

то есть  $\beta\alpha = 1_H$ . □

Мы видим, что понятия левого, правого действий и перестановочного представления равносильны и являются лишь разными способами говорить об одном и том же. Тем не менее все эти понятия оказываются удобными.

**Следствие 2.1.9.** *Множество действий  $G$  на  $\Omega$  канонически изоморфно множеству морфизмов  $G \rightarrow \text{Sym}(\Omega)$ .*

К связи между левыми и правыми действиями можно подойти иначе, используя группу  $G^\circ$  (см. 1.1.7, 1.2.1, 1.6.8). Предположим, что мы имеем левое действие  $G$  на  $\Omega$ . Определим операцию умножения  $\Omega \times G^\circ \rightarrow \Omega$  так:  $\omega g^\circ := g\omega$ . Пусть  $\omega \in \Omega, a, b \in G$ , тогда

$$\begin{aligned} \omega 1^\circ &= 1\omega = \omega, \\ \omega(a^\circ b^\circ) &= \omega(ba)^\circ = (ba)\omega = b(a\omega) = b(\omega a^\circ) = (\omega a^\circ)b^\circ. \end{aligned}$$

Таким образом, мы получили правое действие  $G^\circ$  на  $\Omega$ , которое будем называть отражением исходного левого действия  $G$  на  $\Omega$ . Аналогично, имея правое действие  $G$  на  $\Omega$ , можно построить левое действие  $G^\circ$  на  $\Omega$  по правилу  $g^\circ\omega := \omega g$  для всех  $g \in G, \omega \in \Omega$ . Это действие тоже назовем отражением исходного правого действия  $G$  на  $\Omega$ . Итак, если имеется левое (правое) действие  $G$  на  $\Omega$ , то его отражение — это правое (левое) действие  $G^\circ$  на  $\Omega$ . Можно сказать, что левое (правое) действие  $G$  на  $\Omega$  можно рассматривать как правое (левое) действие  $G^\circ$  на  $\Omega$ .

**Лемма 2.1.10.** *Пусть  $L$  — множество всех левых действий  $G$  на  $\Omega$ ,  $R$  — множество всех правых действий  $G^\circ$  на  $\Omega$ . Тогда отображения  $\alpha : L \rightarrow R, \beta : R \rightarrow L$ , сопоставляющие каждому действию его отражение, взаимно обратны.*

*Доказательство.* Пусть  $f \in L, \omega \in \Omega, g \in G$ .

$$(g, \omega)(f(\alpha\beta)) = (g, \omega)((f\alpha)\beta) = (\omega, g^\circ)(f\alpha) = (g, \omega)f,$$

следовательно,  $f(\alpha\beta) = f$ , то есть  $\alpha\beta = \text{id}_L$ . Аналогично доказывается, что  $\beta\alpha = \text{id}_R$ . □

**Теорема 2.1.11.** Пусть  $G$  — группа,  $L$  — множество всех левых действий  $G$  на  $\Omega$ ,  $H = \text{Mor}(G^\circ, \text{Sym}(\Omega))$ . Отображение  $\phi : L \rightarrow H$ , каждому действию  $\alpha \in L$  сопоставляющее представление  $G^\circ \rightarrow \text{Sym}(\Omega)$ , ассоциированное с отражением  $\alpha$ , является биекцией.

*Доказательство.* Пусть  $R$  — множество всех действий  $G^\circ$  на  $\Omega$ . Сопоставление каждому действию из  $L$  его отражения является биекцией  $L \rightarrow R$ , и сопоставление действиям из  $R$  ассоциированных с ними представлений  $G^\circ \rightarrow \text{Sym}(\Omega)$  является биекцией  $R \rightarrow Y$ . Так как  $\phi$  является композицией этих биекций, то  $\phi$  — биекция.  $\square$

**Следствие 2.1.12.** Множество левых действий  $G$  на  $\Omega$  канонически изоморфно множеству антиморфизмов  $G \rightarrow \text{Sym}(\Omega)$ .

Обычно мы говорим о правых действиях, но иногда будет удобным пользоваться и некоторыми левыми действиями. Для действий групп на множествах иногда разумно использовать аддитивный язык, то есть вместо  $g\omega$  писать  $g + \omega$ . Мы оставляем читателю перевод всех наших утверждений о действиях на аддитивный язык.

**Пример 2.1.1.** Пусть  $\Omega$  — обычное 3-мерное пространство,  $G$  — любая подгруппа его группы (по сложению) векторов. Если  $\omega \in \Omega$  и  $g \in G$ , то мы можем точку  $\omega$  перенести на вектор  $g$ , при этом мы получаем некоторую точку пространства  $\Omega$ , которую обозначаем  $\omega + g$ . Очевидно, данная операция сложения является действием  $G$  на  $\Omega$ .

**Пример 2.1.2.** Выберем в  $\Omega$  любую точку и обозначим ее  $O$ . Возьмем любую прямую  $L$ , проходящую через  $O$ , и представим, что все пространство  $\Omega$  — это твердое тело, которое может вращаться на любой угол вокруг оси  $L$ . Любое такое вращение можно рассматривать как биекцию  $\Omega \rightarrow \Omega$ . Нетрудно показать, что множество  $G$  всех вращений  $\Omega$  вокруг точки  $O$  (со всевозможными осями) является группой относительно операции умножения отображений. Если  $\omega \in \Omega$ ,  $g \in G$ , то мы можем определить  $\omega \cdot g := \omega g$ , то есть  $\omega g$  — это точка, полученная вращением  $g$  точки  $\omega$ . Очевидно, получаем действие  $G$  на  $\Omega$ .

**Пример 2.1.3.** Предположим, что  $\Omega$  — множество,  $G \leq \text{Sym}(\Omega)$ . Тогда имеется естественное умножение  $\Omega \times G \ni (\omega, g) \mapsto \omega g \in \Omega$ , где  $\omega g$  — значение отображения  $g$  в точке  $\omega$ . Очевидно, данное умножение является действием  $G$  на  $\Omega$ .

**Пример 2.1.4.** Пусть  $H$  — подгруппа группы  $G$ ,  $\Omega = G$ . Тогда обычное умножение в группе  $G$  определяет действие  $H$  на  $\Omega$ , то есть мы полагаем  $\omega \cdot h := \omega h$  для произвольных  $\omega \in \Omega$ ,  $h \in H$ . Действие мы обозначили точкой, чтобы отличать

его от операции умножения в группе  $G$ . Имея в виду это действие, мы будем говорить, что  $H$  действует на  $\Omega$  правыми умножениями. Аналогично можно было бы определить действие  $H$  на  $G$  левыми умножениями, полагая  $h \cdot \omega := h^{-1}\omega$  для всех  $\omega \in \Omega$ ,  $h \in H$ .

**Пример 2.1.5.** Пусть  $H$  — подгруппа группы  $G$ ,  $\Omega$  — множество всех левых классов смежности  $G$  по  $H$ , то есть  $\Omega = \{Hg : g \in G\}$ . Тогда для  $a, b \in G$  мы можем определить  $(Ha) \cdot b := (Ha)b$  — произведение множества  $Ha$  на  $b$  (см. 1.1.8). Очевидно,  $(Ha) \cdot b = Hab \in \Omega$ , и мы получаем действие  $G$  на  $\Omega$ . Множество  $\Omega$  в дальнейшем будем обозначать  $G/H$ . Построенное действие назовем стандартным действием  $G$  на множестве  $G/H$ .

**Пример 2.1.6.** Снова пусть  $G$  — группа,  $\Omega = G$ ,  $H \leq G$ . Определим операцию умножения  $\Omega \times H \rightarrow \Omega$  соотношением  $\omega \cdot g = \omega^g$  для всех  $\omega \in \Omega$ ,  $g \in H$  (напомним, что  $\omega^g = g^{-1}\omega g$ ). В силу 1.5.1 получаем действие  $H$  на множестве  $G$ . Это действие называется действием сопряжениями подгруппы  $H$  на множестве  $G$ .

**Пример 2.1.7.** Пусть  $G$  — группа,  $H \leq G$ ,  $\Omega$  — множество всех подмножеств  $G$ . Определим операцию умножения  $\Omega \times H \rightarrow \Omega$  соотношением  $S \cdot g = S^g$  для всех  $S \in \Omega$ ,  $g \in H$  (напомним, что  $S^g = g^{-1}Sg = \{s^g : s \in S\}$ ). В силу 1.5.1 получаем действие  $H$  на множестве  $\Omega$ . Это действие называется действием сопряжениями подгруппы  $H$  на множестве подмножеств  $G$ .

Укажем некоторые способы, позволяющие изменить действующую группу или множество, на котором действует группа.

**Пример 2.1.8.** Пусть  $G$  действует на множестве  $\Omega$ . Определим  $\Omega_0 := \Omega$ ,  $\Omega_n := \Omega_{n-1} \cup P(\Omega_{n-1})$  при  $n > 0$ ,  $\hat{\Omega} := \bigcup_{n \in \mathbb{Z}_{\geq 0}} \Omega_n$ . Интуитивно,  $\hat{\Omega}$  — семейство всех множеств, сконструированных из элементов  $\Omega$  с помощью конечнократного применения операции построения множества из элементов  $\Omega$  и уже построенных ранее множеств. На  $\Omega_0 = \Omega$  уже определено действие  $G$ . Допустим, что мы определили действие  $G$  на  $\Omega_m$ . Пусть  $a \in \Omega_{m+1} \setminus \Omega_m$ ,  $g \in G$ . Тогда  $a \subseteq \Omega_m$  и  $a \notin \Omega_m$ . Мы полагаем  $ag := \{xg : x \in a\}$ . Легко убедиться, что мы получаем таким образом действие  $G$  на  $\hat{\Omega}$ . В частности, если  $\Lambda \subseteq \Omega$ , то  $\Lambda g = \{xg : x \in \Lambda\}$  и если  $\Lambda$  — семейство подмножеств  $\Omega$ , то есть  $\Lambda \subseteq P(\Omega)$ , то  $\Lambda g = \{Ag : A \in \Lambda\}$ . Именно это действие мы будем использовать по умолчанию, когда речь пойдет о действии  $G$  на подмножествах  $\Omega$ , семействах подмножеств  $\Omega$ , и.т.д.

Если  $G$  действует на множестве  $\Omega$ ,  $A \subseteq \Omega$ ,  $B \subseteq G$ , то, используя 1.1.8, можно определить произведение

$$AB := \{ab : a \in A, b \in B\}. \quad (2.1.1)$$

**Определение 2.1.4.** Пусть группа  $G$  действует на множестве  $\Omega$ . Подмножество  $\Lambda \subseteq \Omega$  называется  $G$ -инвариантным, если  $\Lambda G \subseteq \Lambda$ .

**Предложение 2.1.13.** Пусть группа  $G$  действует на множестве  $\Omega$ . Если подмножество  $\Lambda \subseteq \Omega$   $G$ -инвариантно, то  $\Lambda G = \Lambda$ .

*Доказательство.* По определению,  $\Lambda G \subseteq \Lambda$ . С другой стороны,  $\Lambda \subseteq \Lambda 1 \subseteq \Lambda G$ .  $\square$

**Пример 2.1.9.** В обозначениях определения 2.1.4 ясно, что  $G$  естественным образом действует на  $\Lambda$  по правилу  $\Lambda \times G \ni (y, g) \mapsto yg \in \Lambda$ .

**Пример 2.1.10.** Пусть группа  $G$  действует на множестве  $\Omega$ , тогда это действие можно продолжить на  $\hat{\Omega}$  (см. 2.1.8). Следующие подмножества  $\hat{\Omega}$ , очевидно,  $G$ -инвариантны, поэтому  $G$  естественным образом действует на каждом из них:

- 1) семейство всех подмножеств  $\Omega$ ;
- 2) семейство всех  $m$ -элементных подмножеств  $\Omega$ ,  $m \in \mathbb{N}$ ;

Вообще, если  $\Lambda \subseteq \hat{\Omega}$  и  $\Lambda$   $G$ -инвариантно, то  $G$  действует на множестве  $\Lambda$  как указано в 2.1.8. Например, нередко возникает какое-то  $G$ -инвариантное разбиение  $\Lambda$  множества  $\Omega$ , тогда можно рассматривать действие  $G$  на  $\Lambda$ .

**Пример 2.1.11.** Пусть  $D$  — тело,  $V$  — линейное пространство над  $D$ ,  $G \leq \text{GL}(V)$ ,  $n \in \mathbb{N}$ ,  $\Omega$  — множество всех  $n$ -мерных подпространств  $V$ . Очевидно,  $G$  действует на  $V$  по правилу  $(x, g) \mapsto xg$  и множество  $\Omega$   $G$ -инвариантно, поэтому  $G$  естественным образом действует на  $\Omega$ .

**Пример 2.1.12.** Пусть группа  $G$  действует на множестве  $\Omega$ , и  $\phi : \Omega \rightarrow \Lambda$  — некоторое сюръективное отображение, причем для всех  $\omega_1, \omega_2 \in \Omega$  и  $g \in G$  из  $\omega_1\phi = \omega_2\phi$  следует  $(\omega_1g)\phi = (\omega_2g)\phi$ . Тогда существует и единственно действие  $G$  на  $\Lambda$  такое, что  $(\omega\phi)g = (\omega g)\phi$  для всех  $\omega \in \Omega$ ,  $g \in G$  (то есть  $\phi$  — морфизм  $G$ -множеств, см. 2.4.8). В самом деле, пусть  $g \in G$  и рассмотрим отображение  $\rho_g\phi$ , где  $\rho : G \rightarrow \text{Sym}(\Omega)$  — перестановочное представление, ассоциированное с действием  $G$  на  $\Omega$ . По условию, для всех  $\omega_1, \omega_2 \in \Omega$  и  $g \in G$  из  $\omega_1\phi = \omega_2\phi$  следует  $\omega_1(\rho_g\phi) = \omega_2(\rho_g\phi)$ , и из теоремы об эпиморфизмах множеств 5.1.11 следует, что найдется отображение  $\bar{\rho}_g : \Lambda \rightarrow \Lambda$ , для которого коммутативна диаграмма

$$\begin{array}{ccc} & \Lambda & \\ \phi \nearrow & & \searrow \bar{\rho}_g \\ \Omega & \xrightarrow{\rho_g\phi} & \Lambda \end{array} .$$

Для  $\lambda \in \Lambda$ ,  $g \in G$  полагаем  $\lambda g := \lambda \bar{\rho}_g$ . Из коммутативности диаграммы следует, что для всех  $\omega \in \Omega$ ,  $g \in G$

$$(\omega\phi)g = (\omega\phi)\bar{\rho}_g = \omega\rho_g\phi = (\omega g)\phi,$$

то есть  $(\omega\phi)g = (\omega g)\phi$ . Отсюда следует, что определенная нами операция  $\Lambda \times G \rightarrow \Lambda$  является действием. Единственность очевидна.

**Пример 2.1.13.** Если  $G \leq H$  и  $H$  действует на множестве  $\Omega$ , то имеется естественное действие  $G$  на  $\Omega$  по правилу  $(g, \omega) \mapsto g\omega$ . Вообще, пусть  $\phi : G \rightarrow H$  — морфизм групп, и  $H$  действует на множестве  $\Omega$ . Определим умножение  $\Omega \times G \rightarrow \Omega$  так:  $\omega g = \omega(g\phi)$  для всех  $\omega \in \Omega$ ,  $g \in G$ . Очевидно, получаем действие  $G$  на  $\Omega$ . Если  $H$  действует на  $\Omega$  слева, то аналогичное рассуждение приводит к левому действию  $G$  на  $\Omega$  по правилу  $g\omega := (g\phi)\omega$ .

Следующие два примера иллюстрируют этот принцип.

**Пример 2.1.14.** Пусть  $A, B$  — множества,  $\Omega = \text{Mor}(A, B)$ , группа  $G$  действует на  $A$ ,  $\rho : G \rightarrow \text{Sym}(A)$  — ассоциированное перестановочное представление. Очевидно,  $\text{Sym}(A)$  действует слева на  $\Omega$  по правилу  $(\alpha, \phi) \mapsto \alpha\phi$  для всех  $\alpha \in \text{Sym}(A)$ ,  $\phi \in \Omega$ . В силу 2.1.13 возникает левое действие  $G$  на  $\Omega$  по правилу  $(g, \phi) \mapsto (g\rho)\phi$  для всех  $g \in G$ ,  $\phi \in \Omega$ . Если  $a \in A$ ,  $g \in G$ ,  $\phi \in \Omega$ , то  $a(g\phi) = a(g\rho)\phi = (ag)\phi$ . Итак, мы нашли левое действие  $G$  на  $\Omega$  по правилу

$$a(g\phi) = (ag)\phi$$

для всех  $a \in A$ ,  $g \in G$ ,  $\phi \in \Omega$ . Назовем это левое действие  $G$  на  $\Omega$  стандартным. Если записывать функции как индексированные семейства, то предыдущее равенство можно записать так:

$$g(\phi_a)_{a \in A} = (\phi_{ag})_{a \in A}.$$

**Пример 2.1.15.** Пусть  $A, B$  — множества,  $\Omega = \text{Mor}(A, B)$  и группа  $G$  действует на  $B$ . Очевидно,  $\text{Sym}(B)$  действует на  $\Omega$  по правилу  $(\phi, \alpha) \mapsto \phi\alpha$  для всех  $\phi \in \Omega$ ,  $\alpha \in \text{Sym}(B)$ . Так как мы имеем ассоциированное перестановочное представление  $\rho : G \rightarrow \text{Sym}(B)$ , то в силу 2.1.13 возникает действие  $G$  на  $\Omega$  по правилу  $(\phi, g) \mapsto \phi\rho_g$ . Если  $a \in A$ ,  $\phi \in \Omega$ ,  $g \in G$ , то  $a(\phi g) = a(\phi\rho_g) = (a\phi)g$ . Итак, мы нашли действие  $G$  на  $\Omega$  по правилу

$$a(\phi g) = (a\phi)g$$

для всех  $a \in A$ ,  $\phi \in \Omega$ ,  $g \in G$ . Назовем это действие  $G$  на  $\Omega$  стандартным. Перепишем последнее равенство, записывая функции как индексированные семейства.

$$(\phi_a)_{a \in A}g = (\phi_ag)_{a \in A}.$$

**Определение 2.1.5.** Ядром действия  $G$  на  $\Omega$  называется ядро ассоциированного перестановочного представления  $G \rightarrow \text{Sym}(\Omega)$ .

**Лемма 2.1.14.** Пусть  $K$  — ядро действия  $G$  на  $\Omega$ . Тогда выполняются следующие утверждения:

- 1)  $K = \{g \in G : \omega g = \omega \ \forall \omega \in \Omega\};$
- 2)  $K \trianglelefteq G$ .

*Доказательство.* Упражнение. □

**Определение 2.1.6.** Говорят, что группа точно действует на множестве, если ядро этого действия единичное.

**Лемма 2.1.15.** Действие  $G$  на  $\Omega$  является точным тогда и только тогда, когда ассоциированное перестановочное представление  $G \rightarrow \text{Sym}(\Omega)$  является вложением.

*Доказательство.* Это следствие 1.6.16. □

Таким образом, группу  $G$ , точно действующую на множестве  $\Omega$ , можно рассматривать как подгруппу  $\text{Sym}(\Omega)$ . С другой стороны, любая подгруппа  $\text{Sym}(\Omega)$  очевидным образом точно действует на  $\Omega$ . Теперь мы обсудим еще один способ изменения группы, действующей на множестве.

**Пример 2.1.16.** Пусть  $\phi : G \rightarrow H$  — эпиморфизм,  $G$  действует на множестве  $\Omega$ ,  $\ker(\phi)$  действует на  $\Omega$  тривиально. Тогда существует и единственно действие  $H$  на  $\Omega$  такое, что  $\omega(g\phi) = \omega g$  для всех  $\omega \in \Omega, g \in G$ . Действительно, пусть  $\rho : G \rightarrow \text{Sym}(\Omega)$  — перестановочное представление, ассоциированное с действием  $G$  на  $\Omega$ . Очевидно,  $\ker(\phi) \leq \ker(\rho)$ , и в силу теоремы об эпиморфизмах 1.6.19 существует морфизм  $\sigma : H \rightarrow \text{Sym}(\Omega)$  такой, что коммутативна диаграмма

$$\begin{array}{ccc} & H & \\ \phi \nearrow & & \searrow \sigma \\ G & \xrightarrow{\rho} & \text{Sym}(\Omega) \end{array} .$$

Получаем перестановочное представление  $\sigma : H \rightarrow \text{Sym}(\Omega)$ , и мы наделяем  $H$  действием на  $\Omega$ , ассоциированным с  $\sigma$ . Пусть  $\omega \in \Omega, g \in G$ , тогда

$$\omega(g\phi) = \omega((g\phi)\sigma) = \omega(g\rho) = \omega g.$$

Итак, искомое действие существует, а его единственность очевидна. Если  $\ker(\phi) = \ker(\rho)$ , то  $\sigma$  инъективно и  $H$  точно действует на  $\Omega$ . Таким образом, если  $G$  действует на  $\Omega$ , и  $K$  — ядро этого действия, то  $G/K$  точно действует на  $\Omega$  по правилу  $\omega\bar{g} = \omega g$  для всех  $\omega \in \Omega$ ,  $g \in G$ . (мы применили соглашение о черте к естественному морфизму  $G \rightarrow G/K$ ).

Далее мы рассмотрим некоторые конструкции, позволяющие строить новые действия из нескольких уже имеющихся.

**Пример 2.1.17.** Пусть группа  $G$  действует на множествах  $\Omega_i$ ,  $i \in I$ , и  $\Omega = \times_{i \in I} \Omega_i$ . Тогда для  $g \in G$ ,  $\omega = (\omega_i)_{i \in I} \in \Omega$  мы можем определить умножение  $\omega g := (\omega_i g)_{i \in I}$ . Легко видеть, что мы получаем таким образом действие  $G$  на  $\Omega$ .

**Пример 2.1.18.** Пусть  $\Delta$  — множество и для каждого  $\delta \in \Delta$  группа  $G_\delta$  действует на множестве  $\Omega_\delta$ ,  $\Omega := \times_{\delta \in \Delta} \Omega_\delta$ ,  $G = \times_{\delta \in \Delta} G_\delta$ . Тогда для  $\omega = (\omega_\delta)_{\delta \in \Delta} \in \Omega$ ,  $g = (g_\delta)_{\delta \in \Delta} \in G$  мы можем определить умножение

$$\omega g := (\omega_\delta g_\delta)_{\delta \in \Delta}.$$

Легко видеть, что получается действие  $G$  на  $\Omega$ . Имеется важный частный случай этой конструкции — когда все  $\Omega_\delta$  совпадают с некоторым множеством  $\Gamma$ , а все  $G_\delta$  совпадают с некоторой группой  $A$ , тогда  $\Omega = \Gamma^\Delta$ ,  $G = A^\Delta$ , и  $A^\Delta$  действует на  $\Gamma^\Delta$  по правилу

$$(\gamma_\delta)_{\delta \in \Delta} (a_\delta)_{\delta \in \Delta} = (\gamma_\delta a_\delta)$$

для всех  $(\gamma_\delta)_{\delta \in \Delta} \in \Gamma^\Delta$ ,  $(a_\delta)_{\delta \in \Delta} \in A^\Delta$ .

**Пример 2.1.19.** Пусть  $\Delta$  — множество, и для каждого  $\delta \in \Delta$  группа  $G_\delta$  действует на множестве  $\Omega_\delta$ ,  $\Omega := \cup_{\delta \in \Delta} \Omega_\delta \times \{\delta\}$ ,  $G := \times_{\delta \in \Delta} G_\delta$ . Тогда для  $\delta \in \Delta$ ,  $\omega \in \Omega_\delta$ ,  $g = (g_\delta)_{\delta \in \Delta} \in G$  мы можем определить произведение

$$(\omega, \delta)g := (\omega g_\delta, \delta)_{\delta \in \Delta}.$$

Легко видеть, что мы получаем таким образом действие  $G$  на  $\Omega$ .

Если  $\Omega_\delta \cap \Omega_{\delta'} = \emptyset$  при  $\delta \neq \delta'$ , то можно обозначить  $\Omega := \cup_{\delta \in \Delta} \Omega_\delta$ , и для  $\delta \in \Delta$ ,  $\omega \in \Omega_\delta$ ,  $g = (g_\delta)_{\delta \in \Delta} \in G$  определить  $\omega g := \omega g_\delta$ . Снова получаем действие  $G$  на  $\Omega$ .

**Пример 2.1.20.** Пусть в предыдущем примере 2.1.19 все  $\Omega_\delta$  совпадают с множеством  $\Gamma$  и  $B$  — группа, действующая на  $\Delta$ . Тогда  $\Omega = \Gamma \times \Delta$ , и для произвольных  $(\gamma, \delta) \in \Omega$ ,  $b \in B$  можно определить произведение

$$(\gamma, \delta)b := (\gamma, \delta b).$$

Очевидно, получаем действие  $B$  на  $\Omega$ .

**Пример 2.1.21.** Пусть группы  $G_1, G_2$  перестановочно действуют на  $\Omega$ , то есть  $(\omega g_1)g_2 = (\omega g_2)g_1$  для всех  $\omega \in \Omega$ ,  $g_1 \in G_1$ ,  $g_2 \in G_2$ . Обозначим  $G = G_1 \times G_2$ . Для  $g = (g_1, g_2) \in G$ ,  $\omega \in \Omega$  полагаем  $\omega g := (\omega g_1)g_2$ . Очевидно, данное умножение задает действие  $G$  на  $\Omega$ . Например, пусть  $A, B$  — подгруппы группы  $G$ ,  $A$  действует на  $G$  левыми умножениями,  $B$  действует на  $G$  правыми умножениями. Очевидно, эти действия перестановочны и получаем действие  $A \times B$  на  $G$  по правилу  $(g, (a, b)) \mapsto a^{-1}gb$ .

## 2.2 Орбиты

**Определение 2.2.1.** Пусть  $G$  действует на множестве  $\Omega$ . Орбитой  $\mathcal{O}_G(a)$ , или  $G$ -орбитой точки  $a \in \Omega$  называется множество  $aG = \{ag : g \in G\}$ .

Плоскостью обычного 3-мерного пространства  $\Omega$  будем называть любую его точку, прямую, плоскость и само  $\Omega$  (точка — 0-мерная плоскость, прямая — 1-мерная плоскость, плоскость — 2-мерная плоскость,  $\Omega$  — 3-мерная плоскость пространства  $\Omega$ ). Мы говорим, что вектор пространства  $\Omega$  параллелен плоскости, если его с помощью параллельного переноса можно разместить целиком в данной плоскости.

**Пример 2.2.1.** Пусть  $\Omega$  — обычное 3-мерное пространство,  $P$  —  $k$ -мерная плоскость в  $\Omega$ ,  $G$  — множество всех векторов  $\Omega$ , параллельных  $P$ . Очевидно,  $G$  — группа по сложению векторов. Пусть  $a \in \Omega$ , тогда  $a + G$  —  $k$ -мерная плоскость, параллельная  $P$  и содержащая  $a$ .

**Пример 2.2.2.** Пусть  $\Omega$  — обычное 3-мерное пространство,  $G$  — группа его вращений вокруг некоторой точки  $O \in \Omega$ ,  $a \in \Omega$ . Тогда  $aG$  — сфера с центром  $O$ , проходящая через точку  $a$ .

**Пример 2.2.3.** Пусть  $H$  подгруппа группы  $G$ ,  $\Omega = G$  и  $H$  действует на  $\Omega$  правыми умножениями. Очевидно,  $H$ -орбита любой точки  $a \in \Omega$  совпадает с  $aH$ , правым классом смежности элемента  $a$  по  $H$ . Аналогично, Если  $H$  действует на  $\Omega$  левыми умножениями, то  $H$ -орбита любой точки  $a \in \Omega$  совпадает с  $Ha$ , левым классом смежности элемента  $a$  по  $H$ .

**Пример 2.2.4.** Пусть подгруппа  $H$  группы  $G$  действует сопряжениями на  $G$ , тогда для любой точки  $a \in G$   $\mathcal{O}_H(a) = \{a^g : g \in H\}$ . Такое множество называется классом сопряженности элемента  $a$  относительно  $H$  и обозначается  $a^H$ .

**Пример 2.2.5.** Пусть подгруппа  $H$  группы  $G$  действует сопряжениями на подмножествах  $G$ , тогда для любого подмножества  $S \subseteq G$   $\mathcal{O}_H(S) = \{S^g : g \in H\}$ . Такое

множество называется классом сопряженности подмножества  $S$  относительно  $H$  и обозначается  $\{S\}^H$ .

**Пример 2.2.6.** В обозначениях примера 2.1.21  $\mathcal{O}(g) = AgB$  — это так называемый двойной класс смежности элемента  $g$  по подгруппам  $A, B \leq G$ .

**Определение 2.2.2.** Пусть группа  $G$  действует на множестве  $\Omega$ . Мы говорим, что точки  $a, b \in \Omega$   $G$ -эквивалентны, и пишем  $a \sim b$ , если  $ag = b$  для некоторого  $g \in G$ .

**Пример 2.2.7.** Пусть  $\Omega = G$ , или  $\Omega = P(G)$ , и подгруппа  $H \leq G$  действует на  $\Omega$  сопряжениями. Тогда  $G$ -эквивалентные элементы  $a, b \in \Omega$  называются сопряженными относительно  $H$ , или сопряженными, если  $H = G$ . Таким образом,  $a, b$  сопряжены относительно  $H$  тогда и только тогда, когда  $a^h = b$  для некоторого  $h \in H$ .

**Теорема 2.2.1.** Пусть группа  $G$  действует на множестве  $\Omega$ . Тогда отношение  $G$ -эквивалентности является отношением эквивалентности на множестве  $\Omega$ .

*Доказательство.* 1. Рефлексивность. Пусть  $a \in \Omega$ . Так как  $a1 = a$ , то  $a \sim a$ , следовательно, отношение  $G$ -эквивалентности рефлексивно.

2. Транзитивность. Пусть  $a, b, c \in \Omega$  и  $a \sim b$ ,  $b \sim c$ . Тогда  $ag = b$  и  $bh = c$  для некоторых  $g, h \in G$ . Отсюда  $c = bh = (ag)h = a(gh)$ , поэтому  $a \sim c$ .

3. Симметричность. Пусть  $a, b \in \Omega$  и  $a \sim b$ , тогда  $ag = b$  для некоторого  $g \in G$ . Умножая последнее равенство справа на  $g^{-1}$ , получаем, что  $a = bg^{-1}$ , следовательно,  $b \sim a$ .  $\square$

В предыдущих примерах орбит, связанных с 3-мерным пространством, в каждом случае семейство всех орбит образовывало разбиение  $\Omega$ . Оказывается, это верно всегда.

**Теорема 2.2.2.** Пусть группа  $G$  действует на множестве  $\Omega$ .

- 1) Множество всех  $G$ -орбит является разбиением  $\Omega$ .
- 2) Если  $\mathcal{O}$  —  $G$ -орбита, и  $a \in \mathcal{O}$ , то  $\mathcal{O} = aG$ .
- 3) Любая орбита  $G$ -инвариантна.
- 4) Любое  $G$ -инвариантное подмножество в  $\Omega$  является объединением некоторых  $G$ -орбит.

*Доказательство.* Для  $\omega \in \Omega$  обозначим  $[\omega] := \{\omega' \in \Omega : \omega \sim \omega'\}$  — класс  $\omega$  по отношению  $\sim$ .

1. Очевидно,  $[\omega] = \omega G$  для любой точки  $\omega \in \Omega$ , поэтому семейство всех орбит множества  $\Omega$  совпадает с семейством всех классов  $G$ -эквивалентности. Последнее семейство, как известно, образует разбиение  $\Omega$  (см. 5.2.1).

2. Пусть  $\mathcal{O}$  —  $G$ -орбита. Так как  $\mathcal{O}$  — класс отношения  $G$ -эквивалентности и  $a \in \mathcal{O}$ , то  $\mathcal{O} = [a] = aG$ .

3.

$$\mathcal{O}G = (aG)G = a(GG) = aG = \mathcal{O},$$

поэтому  $\mathcal{O}$  —  $G$ -инвариантное подмножество.

4. Пусть  $S$  —  $G$ -инвариантное подмножество  $\Omega$ ,  $s \in S$ . Тогда  $s \in sG \subseteq S$ , поэтому

$$S = \bigcup_{s \in S} \{s\} \subseteq \bigcup_{s \in S} sG \subseteq S.$$

Следовательно,  $S = \bigcup_{s \in S} sG$ . □

**Пример 2.2.8.** Рассмотрим действие правыми умножениями подгруппы  $H$  группы  $G$  на множестве  $G$ . Тогда семейство всех  $H$ -орбит — это в точности семейство всех правых классов смежности  $G$  по  $H$ , и мы приходим к выводу, что данное семейство — разбиение множества  $G$ . Аналогично, рассматривая действие левыми умножениями  $H$  на множестве  $G$ , приходим к заключению, что множество всех левых классов смежности  $G$  по  $H$  тоже образует разбиение множества  $G$ . Мы доказали следующую теорему.

**Теорема 2.2.3.** Пусть  $H$  — подгруппа группы  $G$ . Тогда семейство всех левых классов смежности  $G$  по  $H$  является разбиением множества  $G$ . То же самое верно и для правых классов смежности  $G$  по  $H$ .

Резюмируем наши наблюдения в важном частном случае отношения сопряженности относительно подгруппы.

**Теорема 2.2.4.** Пусть  $H \leq G$ ,  $\Omega = G$  или  $\Omega = P(G)$ . Имеют место следующие утверждения:

- 1) отношение сопряженности относительно  $H$  является отношением эквивалентности на  $\Omega$ ;
- 2) множество всех классов сопряженности элементов  $\Omega$  относительно подгруппы  $H$  является разбиением множества  $\Omega$ ;

- 3)  $a \in a^H$  для всех  $a \in \Omega$ ;
- 4) если  $a, b \in \Omega$ , то либо  $a^H = b^H$ , либо  $a^H \cap b^H = \emptyset$ ;
- 5) если  $C$  — класс сопряженности относительно  $H$ , и  $a \in C$ , то  $C = a^H$ ;
- 6) любое  $H$ -инвариантное подмножество  $\Omega$  является объединением некоторых классов сопряженности относительно  $H$ .

**Лемма 2.2.5.** Пусть группы  $A, B$  перестановочно действуют на множестве  $\Omega$ ,  $\omega \in \Omega$ ,  $b \in B$ . Тогда  $\mathcal{O}_A(\omega)b = \mathcal{O}_A(\omega b)$ . В частности,  $B$  действует на множестве  $A$ -орбит.

*Доказательство.*  $\mathcal{O}_A(\omega)b = (\omega A)b = (\omega b)A = \mathcal{O}_A(\omega b)$ . □

**Пример 2.2.9.** Пусть  $H \leq G$ ,  $\Omega := G$ ,  $H$  действует на  $\Omega$  по правилу  $(\omega, h) \mapsto h^{-1}\omega$  для всех  $\omega \in \Omega$ ,  $h \in H$ ,  $G$  действует на  $\Omega$  по правилу  $(\omega, g) \mapsto \omega g$  для всех  $\omega \in \Omega$ ,  $g \in G$ . Очевидно, эти действия перестановочны, и  $\mathcal{O}_H(\omega) = H\omega$  — левый класс смежности по  $H$  элемента  $\omega$ . Таким образом,  $H$ -орбиты — это левые классы смежности  $G$  по  $H$ . В силу 2.2.5  $G$  действует на множестве  $G/H$  левых классов смежности  $G$  по  $H$  по правилу  $(H\omega, g) \mapsto H\omega g$ .

**Пример 2.2.10.** Пусть  $V$  — векторное пространство над полем  $F$ ,  $G = \text{GL}(V)$ ,  $\Omega = V \setminus \{0\}$ . Тогда обычные действия  $F^*$  и  $\text{GL}(V)$  на  $\Omega$  перестановочны,  $F^*$ -орбиты — это одномерные подпространства  $V$ , из которых удален  $0$ , и  $G$  действует на семействе этих проколотых прямых по правилу  $(F^*\omega, g) \mapsto F^*(\omega g)$  для всех  $\omega \in \Omega$ ,  $g \in G$ .

**Лемма 2.2.6.** Пусть группа  $G$  действует на множестве  $\Omega$ ,  $P$  — множество всех  $G$ -орбит  $\Omega$ ,  $\phi : \Omega \rightarrow P$ ,  $\omega \mapsto \omega G$ . Тогда  $(\omega G)\phi^{-1} = \omega G$  для всех  $\omega \in \Omega$ .

*Доказательство.* Действительно, в силу 2.2.2  $P$  — разбиение множества  $\Omega$ , и отображение  $\phi$  каждому элементу  $\omega \in \Omega$  ставит в соответствие единственную орбиту  $\omega G$ , в которой содержится  $\omega$ , поэтому  $(\omega G)\phi^{-1}$  — это множество всех элементов  $\Omega$ , лежащих в той же орбите  $\omega G$ , что и  $\omega$ . Очевидно, это множество равно  $\omega G$ . □

## 2.3 Теорема Лагранжа

После небольшой подготовки мы с помощью теоремы 2.2.3 получим фундаментальный результат — теорему Лагранжа.

**Теорема 2.3.1.** Пусть  $H$  — подгруппа группы  $G$ ,  $a \in H$ , тогда

$$|aH| = |Ha| = |H|.$$

*Доказательство.* Рассмотрим отображение  $\phi : H \rightarrow aH$ ,  $h\phi = ah$  для всех  $h \in H$ . Очевидно,  $\phi$  — биекция, поэтому  $|aH| = |H|$ . Кроме того, отображение  $\iota : G \rightarrow G$ ,  $g\iota = g^{-1}$  является биекцией, поэтому

$$|Ha| = |(Ha)\iota| = |(Ha)^{-1}| = |a^{-1}H| = |H|.$$

□

**Теорема 2.3.2.** Пусть  $G$  — группа,  $H \leq G$ . Тогда множество всех правых классов смежности  $G$  по  $H$  равномощно множеству всех левых классов смежности  $G$  по  $H$ .

*Доказательство.* Пусть  $L$  — множество всех левых классов смежности  $G$  по  $H$ ,  $R$  — множество всех правых классов смежности  $G$  по  $H$ ,  $\iota : G \rightarrow G$ ,  $g\iota = g^{-1}$  для всех  $g \in G$ . Если  $g \in G$ , то

$$(Hg)\iota = (Hg)^{-1} = g^{-1}H^{-1} = g^{-1}H \in R,$$

поэтому мы можем ввести отображение  $\iota_1 : L \rightarrow R$ ,  $C\iota_1 = C^{-1}$  для всех  $C \in L$ . Покажем, что  $\iota_1$  — биекция. Для этого заметим, что  $\iota$  любой правый класс смежности переводит в левый класс смежности. Более точно, если  $g \in G$ , то

$$(gH)\iota = (gH)^{-1} = H^{-1}g^{-1} = Hg^{-1} \in L,$$

поэтому можно ввести отображение  $\iota_2 : R \rightarrow L$ ,  $C\iota_2 = C^{-1}$  для всех  $C \in R$ . Покажем, что  $\iota_1, \iota_2$  взаимно обратны. Пусть  $g \in G$ .

$$(Hg)(\iota_1\iota_2) = ((Hg)\iota_1)\iota_2 = ((Hg)^{-1})^{-1} = Hg,$$

поэтому  $\iota_1\iota_2 = \text{id}_L$ .

$$(gH)(\iota_2\iota_1) = ((gH)\iota_2)\iota_1 = ((gH)^{-1})^{-1} = gH.$$

Следовательно,  $\iota_2\iota_1 = \text{id}_R$ . Мы доказали, что  $\iota_1, \iota_2$  взаимно обратны, поэтому  $\iota_1$  — биекция. □

Таким образом, количество левых классов смежности  $G$  по  $H$  равно количеству правых классов смежности  $G$  по  $H$ .

**Определение 2.3.1.** Это количество называется индексом  $G$  по  $H$ , или индексом  $H$  в группе  $G$ , и обозначается  $[G : H]$ .

Очевидно,  $[G : H] = 1$  тогда и только тогда, когда  $G = H$ .

**Теорема 2.3.3.** (Теорема Лагранжа) Пусть  $H$  — подгруппа группы  $G$ . Тогда

$$|G| = [G : H]|H|.$$

*Доказательство.* Пусть  $\Omega$  — множество всех левых классов смежности  $G$  по  $H$ . В силу 2.2.3  $\Omega$  — разбиение  $G$ , причем все элементы этого разбиения имеют одну и ту же мощность —  $|H|$  (в силу 2.3.1), поэтому

$$|G| = \sum_{C \in \Omega} |C| = \sum_{C \in \Omega} |H| = |\Omega||H| = [G : H]|H|.$$

□

Отсюда немедленно получаем важное следствие.

**Теорема 2.3.4.** Порядок подгруппы  $H$  конечной группы  $G$  делит порядок  $G$ .

Из теоремы Лагранжа тривиально вытекает еще одно полезное следствие.

**Теорема 2.3.5.** Пусть  $H$  — подгруппа конечной группы  $G$ . Тогда

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

**Определение 2.3.2.** Правой трансверсалью группы  $G$  по подгруппе  $H$  называется произвольное семейство  $(t_i)_{i \in I}$  элементов  $G$  такое, что для каждого  $g \in G$  имеется единственный индекс  $i \in I$  такой, что  $t_i \in gH$ .

Чтобы построить правую трансверсаль  $G$  по  $H$ , нужно в каждом правом классе смежности  $G$  по  $H$  выбрать по одному элементу — образованное этими элементами множество является правой трансверсалью. Аналогично определяются левые трансверсали. Очевидно, если  $(t_i)_{i \in I}$  — трансверсаль  $G$  по  $H$ , то  $[G : H] = |I|$ .

**Теорема 2.3.6.** Пусть  $G \geq H \geq I$  — группы,  $(s_i)_{i \in I}$  — правая трансверсаль  $G$  по  $H$ ,  $(t_j)_{j \in J}$  — правая трансверсаль  $H$  по  $I$ . Тогда  $(s_i t_j)_{(i,j) \in I \times J}$  — правая трансверсаль  $G$  по  $I$ . В частности,

$$[G : H][H : I] = [G : I].$$

*Доказательство.*

$$G = \cup_{i \in I} s_i H = \cup_{i \in I} s_i (\cup_{j \in J} t_j I) = \cup_{i \in I} \cup_{j \in J} s_i t_j I = \cup_{(i,j) \in I \times J} s_i t_j I.$$

Остается доказать, что из  $s_i t_j I \cap s_{i'} t_{j'} I \neq \emptyset$  следует  $(i, j) = (i', j')$ . Пусть  $s_i t_j I \cap s_{i'} t_{j'} I \neq \emptyset$ . Очевидно,  $\emptyset \subset s_i t_j I \cap s_{i'} t_{j'} I \subseteq s_i H \cap s_{i'} H$ , поэтому  $i = i'$ . Далее,  $\emptyset \neq s_i t_j I \cap s_i t_{j'} I = s_i (t_j I \cap t_{j'} I)$ , следовательно,  $t_j I \cap t_{j'} I \neq \emptyset$ , откуда  $j = j'$ . □

## 2.4 Стабилизатор точки

**Определение 2.4.1.** Пусть  $G$  — группа.  $G$ -множеством называется произвольное множество  $\Omega$ , наделенное некоторым действием  $G$  на  $\Omega$ .

**Определение 2.4.2.** Пусть  $\Omega$  —  $G$ -множество,  $S \in \hat{\Omega} \setminus \Omega$ . Тогда

$$G_S := \{g \in G : sg = s \forall s \in S\}$$

— точечный стабилизатор  $S$ , в частности, для  $S \in \hat{\Omega}$

$$G_{\{S\}} = \{g \in G : Sg = S\}$$

— глобальный стабилизатор  $S$  (и точечный стабилизатор множества  $\{S\}$ ). Если  $S = \{a\}$ ,  $a \in \Omega$ , то мы пишем  $G_a := G_{\{a\}}$  и называем  $G_a$  стабилизатором точки  $a$ . Таким образом,  $G_a = \{g \in G : ag = a\}$  при  $a \in \Omega$ .

**Пример 2.4.1.** Рассмотрим стандартное действие группы  $G$  на множестве  $G/H$  (см. 2.1.5),  $H \leq G$ . В силу 1.4.2 стабилизатор точки  $H$  равен  $H$ .

**Пример 2.4.2.** Рассмотрим действие подгруппы  $H$  группы  $G$  сопряжениями на множестве  $\Omega := G$ , то есть  $\omega.g := \omega^g = g^{-1}\omega g$  для всех  $\omega \in \Omega$ ,  $g \in H$ . Тогда

$$\omega.g = \omega \Leftrightarrow \omega^g = \omega \Leftrightarrow g^{-1}\omega g = \omega \Leftrightarrow \omega g = g\omega,$$

то есть  $\omega.g = \omega$  тогда и только тогда, когда  $g, \omega$  перестановочны. Следовательно, если  $S \subseteq G$ , то  $H_S = \{h \in H : hs = sh \forall s \in S\}$ . Мы приходим к определению.

**Определение 2.4.3.** Пусть  $G$  — группа,  $H \leq G$ ,  $S \subseteq G$ . Центризатором  $S$  в  $H$  называется множество всех элементов  $H$ , перестановочных со всеми элементами  $S$ , то есть множество  $\{h \in H : hs = sh \forall s \in S\}$ . Центризатор  $S$  в  $H$  обозначается  $C_H(S)$ . Если  $S = \{a\}$ , то пишем  $C_H(a) := C_H(\{a\})$ .

Таким образом,  $H_S = C_H(S)$ . В частности, если  $a \in G$ , то  $H_a = C_H(a)$ .

**Пример 2.4.3.** Рассмотрим действие подгруппы  $H$  группы  $G$  сопряжениями на множестве  $\Omega$  всех подмножеств  $G$ , то есть  $S.g := S^g$  для всех  $S \in \Omega$ ,  $g \in H$ . Тогда

$$g \in H_{\{S\}} \Leftrightarrow S.g = S \Leftrightarrow S^g = S.$$

Мы приходим к определению.

**Определение 2.4.4.** Пусть  $G$  — группа,  $H \leq G$ ,  $S \subseteq G$ . Нормализатором  $S$  в  $H$  называется множество  $\{g \in H : S^g = S\}$ . Нормализатор  $S$  в  $H$  обозначается  $N_H(S)$ .

Таким образом,  $H_{\{S\}} = N_H(S)$ .

**Пример 2.4.4.** Если  $\Sigma$  — некоторое семейство подмножеств  $G$  и  $G$  действует на  $\Omega := G$  сопряжениями, то  $G_\Sigma = \bigcap_{A \in \Sigma} N_G(A)$  — системный нормализатор.

**Предложение 2.4.1.** Пусть  $G$  — группа,  $H \leq G$ ,  $a \in G$ . Тогда  $N_H(a) = C_H(a)$ .

*Доказательство.* Очевидно.  $\square$

**Предложение 2.4.2.** Пусть  $\Omega$  —  $G$ -множество,  $S \in \hat{\Omega}$ . Тогда  $G_S$  — подгруппа  $G$ .

*Доказательство.* Заметим, что  $G_S = \bigcap_{s \in S} G_s$ . Очевидно, стабилизатор точки — подгруппа  $G$ , и пересечение любого семейства подгрупп — подгруппа.  $\square$

В частности,

**Следствие 2.4.3.** Стабилизаторы, централизаторы, нормализаторы, системные нормализаторы являются подгруппами.

**Определение 2.4.5.** Перестановочной парой назовем любую упорядоченную пару  $(\Omega, G)$ , в которой  $\Omega$  — множество,  $G$  — группа, и  $G$  действует на  $\Omega$ .

Строго говоря, нужно было бы к паре  $(\Omega, G)$  добавить подразумеваемое действие  $f : \Omega \times G \rightarrow \Omega$  группы  $G$  на  $\Omega$ , и иметь дело с тройками  $(\Omega, G, f)$ , но это слишком громоздко. Кроме того, обычно рассматривают случай  $G \leq \text{Sym}(\Omega)$  когда ясно, какое действие рассматривается.

**Определение 2.4.6.** Пусть группа  $G_i$  действует на множестве  $\Omega_i$ ,  $i \in \{1, 2\}$ . Морфизмом  $(\Omega_1, G_1) \rightarrow (\Omega_2, G_2)$  назовем любую пару  $(\phi, \psi)$ , где  $\phi : \Omega_1 \rightarrow \Omega_2$  — отображение,  $\psi : G_1 \rightarrow G_2$  — морфизм, причем  $(\omega g)\phi = (\omega\phi)(g\psi)$  для всех  $\omega \in \Omega$ ,  $g \in G_1$ .

Мы часто будем применять к морфизмам пар соглашение о черте, и обозначать  $\bar{g} := g\psi$ ,  $\bar{\omega} := \omega\phi$  для всех  $g \in G$ ,  $\omega \in \Omega$ . Если мы не хотим вводить буквенные обозначения для отображений  $\Omega_1 \rightarrow \Omega_2$ ,  $G_1 \rightarrow G_2$ , и пользуемся соглашением о черте, то напишем « $- : (\Omega_1, G_1) \rightarrow (\Omega_2, G_2)$  — морфизм пар».

В терминах соглашения о черте можно сказать, что морфизмом  $(\Omega_1, G_1) \rightarrow (\Omega_2, G_2)$  называется любая пара отображений  $\Omega_1 \ni \omega \mapsto \bar{\omega} \in \Omega_2$ ,  $G_1 \ni g \mapsto \bar{g} \in G_2$ , причем второе из них — морфизм групп, и  $\overline{\omega g} = \bar{\omega} \bar{g}$  для всех  $\omega \in \Omega$ ,  $g \in G_1$ . Очевидно,  $(\text{id}_\Omega, \text{id}_G)$  является морфизмом  $(\Omega, G) \rightarrow (\Omega, G)$ .

**Упражнение 2.4.4.** Докажите следующие утверждения:

- 1) перестановочные пары и их морфизмы образуют категорию;
- 2) морфизм пар является изоморфизмом тогда и только тогда, когда он состоит из биекций.

**Определение 2.4.7.** Если группа  $G$  действует на множестве  $\Omega$ ,  $\omega \in \Omega$ ,  $g \in G$  и  $\omega g = g$ , то мы говорим, что  $\omega$  — неподвижная точка элемента  $g$ , а  $g$  фиксирует или не сдвигает  $\omega$ .

Если  $G$  действует на множестве  $\Omega$ ,  $H \subseteq G$ ,  $\Lambda \subseteq \Omega$ , то мы обозначаем

$$C_\Lambda(H) := \{\lambda \in \Lambda : \lambda g = \lambda \ \forall g \in H\},$$

$$C_H(\Lambda) := \{g \in H : \lambda g = \lambda \ \forall \lambda \in \Lambda\}.$$

Очевидно,  $C_H(\Lambda) = H_\Omega$ ,  $C_\Lambda(H)$  — множество точек  $\Lambda$ , неподвижных относительно всех элементов  $H$ ,  $C_H(\Lambda)$  — множество всех элементов  $H$ , не сдвигающих любую точку  $\Lambda$ . Если  $\Lambda = \{\lambda\}$ , то мы пишем  $C_H(\lambda) := C_H(\{\lambda\})$ . Тогда  $C_H(\lambda) = H_\lambda$  — множество всех элементов  $H$ , не сдвигающих точку  $\lambda$ . Аналогично, если  $H = \{g\}$ , то пишем  $C_\Lambda(g) := C_\Lambda(\{g\})$ . Множество  $C_\Lambda(g)$  состоит из всех точек  $\Lambda$ , неподвижных относительно  $g$ .

**Предложение 2.4.5.** Пусть группа  $G$  действует на множестве  $\Omega$ , группа  $G'$  действует на множестве  $\Omega'$ , и  $- : (\Omega, G) \rightarrow (\Omega', G')$  — изоморфизм. Тогда  $\overline{G_\omega} = \overline{G_\omega}$  для любой точки  $\omega \in \Omega$ . Если  $g \in G$ , то  $C_{\overline{\Omega}}(\overline{g}) = \overline{C_\Omega(g)}$ .

*Доказательство.*

$$\overline{g} \in \overline{G_\omega} \Leftrightarrow \omega \overline{g} = \omega \Leftrightarrow \overline{\omega g} = \omega \Leftrightarrow \omega g = \omega \Leftrightarrow g \in G_\omega,$$

следовательно,  $\overline{G_\omega} = \overline{G_\omega}$ . Аналогично,

$$\omega \in C_{\overline{\Omega}}(\overline{g}) \Leftrightarrow \omega \overline{g} = \omega \Leftrightarrow \overline{\omega g} = \omega \Leftrightarrow \omega g = \omega \Leftrightarrow \omega \in C_\Omega(g).$$

□

Если группа  $G$  действует на множестве  $\Omega$ , то можно считать без ограничения общности, что  $\Omega \cap G = \emptyset$ . Тогда морфизм  $- : (\Omega_1, G_1) \rightarrow (\Omega_2, G_2)$  это такое отображение  $- : \Omega_1 \cup G_1 \rightarrow \Omega_2 \cup G_2$ , что  $\overline{\Omega_1} \subseteq \Omega_2$ ,  $\overline{G_1} \subseteq G_2$ , причем отображение  $G_1 \ni g \mapsto \overline{g} \in G_2$  является морфизмом групп, и  $\overline{\omega g} = \omega \overline{g}$  для всех  $\omega \in \Omega$ ,  $g \in G_1$ .

**Лемма 2.4.6.** Пусть  $\Omega$  —  $G$ -множество,  $g \in G$ . Тогда отображение  $- : \Omega \cup G \rightarrow \Omega \cup G$ , такое, что  $\bar{\omega} = \omega g$ ,  $\bar{x} = x^g$  для всех  $\omega \in \Omega$ ,  $x \in G$ , является автоморфизмом пары  $(\Omega, G)$ .

*Доказательство.* Пусть  $\omega \in \Omega$ ,  $x \in G$ , тогда

$$\bar{\omega}\bar{x} = (\omega g)x^g = (\omega g)(g^{-1}xg) = (\omega x)g = \overline{\omega x}.$$

□

**Следствие 2.4.7.** Пусть  $\Omega$  —  $G$ -множество,  $\omega \in \Omega$ ,  $g \in G$ . Тогда  $G_{\omega g} = G_{\omega}^g$ .

*Доказательство.* В силу 2.4.6 и 2.4.5

$$G_{\omega g} = (G^g)_{\omega g} = \overline{G_{\bar{\omega}}} = \overline{G_{\omega}} = G_{\omega}^g.$$

□

**Пример 2.4.5.** Рассмотрим действие группы  $G$  правыми умножениями на множестве  $G/H$ ,  $H \leq G$ ,  $g \in G$ . Тогда стабилизатор точки  $Hg$  равен  $H^g$ .

Еще одним примером является следующая теорема.

**Теорема 2.4.8.** Пусть  $G$  — группа,  $H \leq G$ ,  $a, g \in G$ ,  $S \subseteq G$ . Тогда

$$C_H(a)^g = C_{H^g}(a^g),$$

$$C_H(S)^g = C_{H^g}(S^g),$$

$$N_H(S)^g = N_{H^g}(S^g).$$

Более общим образом:

**Теорема 2.4.9.** Пусть  $G$  — группа,  $H \leq G$ ,  $a \in G$ ,  $S \subseteq G$ ,  $\sigma \in \text{Aut}(G)$ . Тогда

$$C_H(a)^\sigma = C_{H^\sigma}(a^\sigma),$$

$$C_H(S)^\sigma = C_{H^\sigma}(S^\sigma),$$

$$N_H(S)^\sigma = N_{H^\sigma}(S^\sigma).$$

*Доказательство.* Здесь нужно рассмотреть действия групп  $H, H^\sigma$  на множестве  $\Omega$  всех подмножеств  $G$  сопряжениями и учесть, что  $\sigma$  можно рассматривать как изоморфизм  $(\Omega, H) \rightarrow (\Omega, H^\sigma)$ , после чего воспользоваться 2.4.5. □

**Предложение 2.4.10.** Если  $G$  — группа и  $S \subseteq_G G$  (то есть  $S$  — нормальное подмножество  $G$ ), то

$$C_G(S) \trianglelefteq G \text{ и } N_G(S) \trianglelefteq G.$$

*Доказательство.* Это следует из 2.4.8. □

**Определение 2.4.8.** Пусть  $\Gamma, \Delta$  —  $G$ -множества. Отображение  $\phi : \Gamma \rightarrow \Delta$  называется морфизмом, если  $(\gamma g)\phi = (\gamma\phi)g$  для всех  $g \in G, \gamma \in \Gamma$ .

**Замечание 2.4.11.** Очевидно, отображение  $\phi : \Gamma \rightarrow \Delta$  является морфизмом  $G$ -множеств тогда и только тогда, когда  $(\phi, \text{id}_G)$  является морфизмом  $(\Gamma, G) \rightarrow (\Delta, G)$ .

**Предложение 2.4.12.** Пусть  $\phi : \Omega \rightarrow \Omega'$  — морфизм  $G$ -множеств,  $\omega \in \Omega$ . Тогда  $\mathcal{O}_G(\omega)\phi = \mathcal{O}_G(\omega\phi)$ .

*Доказательство.* Очевидно. □

**Упражнение 2.4.13.**  $G$ -множества и их морфизмы образуют категорию. Морфизм этой категории является изоморфизмом тогда и только тогда, когда он биективен.

Изоморфизм перестановочных пар называется также перестановочным изоморфизмом, а пары, связанные перестановочным изоморфизмом, называются перестановочно изоморфными.

**Теорема 2.4.14.** Пусть  $\phi : \Omega \rightarrow \Omega'$  — изоморфизм  $G$ -множеств,  $\omega \in \Omega$ . Тогда  $G_\omega = G_{\omega\phi}$ .

*Доказательство.* Это следствие 2.4.5. □

**Лемма 2.4.15.** Пусть группа  $G$  действует на множестве  $\Omega$ ,  $\omega \in \Omega$ ,  $O := \omega G$ ,  $\phi : G \rightarrow O, g \mapsto \omega g$ . Тогда  $(\omega g)\phi^{-1} = G_\omega g$  для любого  $g \in G$ .

*Доказательство.*

$$h \in (\omega g)\phi^{-1} \Leftrightarrow h\phi = \omega g \Leftrightarrow \omega h = \omega g \Leftrightarrow \omega h g^{-1} = \omega \Leftrightarrow h g^{-1} \in G_\omega \Leftrightarrow h \in G_\omega g.$$

□

## 2.5 Транзитивные действия

**Определение 2.5.1.** Действие группы  $G$  на множестве  $\Omega$  называется транзитивным, если для любых точек  $a, b \in \Omega$  найдется элемент  $g \in G$  такой, что  $ag = b$ .

Транзитивность равносильна тому, что любые две точки  $\Omega$   $G$ -эквивалентны, то есть имеется единственная  $G$ -орбита.

**Предложение 2.5.1.** Пусть  $G$  действует на множестве  $\Omega$ ,  $\mathcal{O}$  — произвольная  $G$ -орбита. Тогда  $G$  транзитивно действует на  $\mathcal{O}$ .

*Доказательство.* В силу 2.2.2 все орбиты  $G$ -инвариантны, поэтому  $G$  действует на  $\mathcal{O}$ . Пусть  $u, v \in \mathcal{O}$ . По определению,  $\mathcal{O} = aG$  для некоторой точки  $a \in \Omega$ , следовательно,  $u = ag$ ,  $v = ah$  для некоторых  $g, h \in G$ . Так как

$$u(g^{-1}h) = ag(g^{-1}h) = ah = v,$$

то  $G$  транзитивно действует на  $\mathcal{O}$ . □

**Определение 2.5.2.** Не транзитивное действие группы на множестве называется интранзитивным.

**Пример 2.5.1.** Пусть  $G$  — группа вращений пространства вокруг точки  $O$ ,  $\Omega$  — произвольная сфера с центром в точке  $O$ , тогда  $G$  транзитивно действует на  $\Omega$  (вращениями). Очевидно, на всем пространстве  $E$  группа  $G$  действует интранзитивно, так как точки, удаленные от  $O$  на разные расстояния, не могут быть совмещены никаким вращением вокруг  $O$ .

**Пример 2.5.2.** Рассмотрим действие группы  $G$  правыми умножениями на множестве  $\Omega := G$ , то есть  $\omega.g := \omega g$  для всех  $\omega \in \Omega$ ,  $g \in G$ . Пусть  $a, b \in \Omega$ ,  $g = a^{-1}b$ . Тогда  $a.g = b$ , поэтому  $G$  транзитивно действует на  $\Omega$ .

**Пример 2.5.3.** Рассмотрим действие группы  $G$  правыми умножениями на множестве  $\Omega$  всех левых классов смежности  $G$  по подгруппе  $H \leq G$ , то есть  $\Omega = \{Ha : a \in G\}$  и  $Ha.g := Hag$  для всех  $a, g \in G$ . Пусть  $a, b \in G$ ,  $g = a^{-1}b$ . Тогда  $Ha.g = bH$ , поэтому  $G$  транзитивно действует на  $\Omega$ .

Очевидно, имеет место следующее утверждение.

**Предложение 2.5.2.** Действие группы  $G$  на множестве  $\Omega$  транзитивно тогда и только тогда, когда в  $\Omega$  имеется только одна  $G$ -орбита.

**Определение 2.5.3.** Действие группы  $G$  на множестве  $\Omega$  называется регулярным, если для любых точек  $a, b \in \Omega$  найдется ровно один элемент  $g \in G$  такой, что  $ag = b$ .

**Пример 2.5.4.** Действие группы  $G$  на множестве  $\Omega = G$  правыми умножениями, то есть  $(\omega, g) \mapsto \omega g$  — обычное произведение — регулярно. Действие  $G$  на  $\Omega = G$  левыми умножениями, то есть  $(\omega, g) \mapsto g^{-1}\omega$  тоже регулярно.

**Предложение 2.5.3.** Пусть группа  $G$  действует на множестве  $\Omega$ ,  $\omega \in \Omega$ . Данное действие регулярно тогда и только тогда, когда  $G$  транзитивно действует на  $\Omega$  и  $G_\omega = \{1\}$ .

*Доказательство.* Пусть  $G$  регулярно действует на  $\Omega$ . Очевидно, это действие транзитивно. По определению, существует ровно один элемент  $g \in G$  такой, что  $\omega g = \omega$ . Один такой элемент имеется — 1. Из единственности  $g$  следует, что  $g = 1$ , то есть  $G_\omega = \{1\}$ .

Обратно, предположим, что  $G$  транзитивно действует на  $\Omega$  и  $G_\omega = \{1\}$ . Пусть  $\alpha, \beta \in \Omega$ . Из транзитивности  $G$  следует, что существует  $g \in G$  такой, что  $\alpha g = \beta$ . Покажем, что такой элемент  $g$  единственен. Пусть  $g' \in G$  и  $\alpha g' = \beta$ . Так как  $G$  транзитивна, то  $\alpha = \omega h$  для некоторого  $h \in G$ .

$$\alpha g = \alpha g' \Rightarrow \alpha = \alpha g' g^{-1} \Rightarrow g' g^{-1} \in G_\alpha = G_{\omega h} = G_\omega^h = \{1\}^h = \{1\}.$$

Отсюда  $g' g^{-1} = 1$ , то есть  $g = g'$ . □

**Лемма 2.5.4.** Пусть группа  $G_i$  действует на множестве  $\Omega_i$ ,  $i \in \{1, 2\}$ ,  $(\Omega_1, G_1) \simeq (\Omega_2, G_2)$ . Если  $G_1$  транзитивно действует на  $\Omega_1$ , то и  $G_2$  транзитивно действует на  $\Omega_2$ .

*Доказательство.* Это очевидно. □

**Лемма 2.5.5.** Пусть группа  $G$  действует на множестве  $\Omega$ ,  $G' \leq G$ ,  $\Omega' \subseteq \Omega$  —  $G'$ -инвариантное подмножество,  $g \in G$ . Тогда  $(\Omega', G') \simeq (\Omega'g, (G')^g)$ . В частности, если  $G'$  транзитивно действует на  $\Omega'$ , то  $(G')^g$  транзитивно действует на  $\Omega'g$ .

*Доказательство.* Это следует из 2.4.6 и 2.5.4. □

**Определение 2.5.4.** Пусть  $H$  — подгруппа группы  $G$ . Тогда мы определяем подгруппу  $\text{Core}_G(H) := \bigcap_{g \in G} H^g$ .

**Теорема 2.5.6.** Пусть  $H$  — подгруппа группы  $G$ . Тогда выполняются следующие утверждения:

- 1)  $\text{Core}_G(H) \leq H$ ;
- 2)  $\text{Core}_G(H) = H \Leftrightarrow H \trianglelefteq G$ ;
- 3)  $\text{Core}_G(H) \trianglelefteq G$ ;
- 4) если  $A \leq H$  и  $A \trianglelefteq G$ , то  $A \leq \text{Core}_G(H)$ .

Можно сказать, что  $\text{Core}_G(H)$  — наибольшая подгруппа  $H$ , нормальная в  $G$ .

*Доказательство.* 1. Очевидно,  $\text{Core}_G(H) \leq H$ .

3. Пусть  $a \in G$ . Тогда

$$\text{Core}_G(H)^a = \left( \bigcap_{g \in G} H^g \right)^a = \bigcap_{g \in G} (H^g)^a = \bigcap_{g \in G} H^{ga} = \bigcap_{u \in G} H^u = \text{Core}_G(H),$$

следовательно  $\text{Core}_G(H) \trianglelefteq G$ . (4) Пусть  $A \leq H$  и  $A \trianglelefteq G$ . Тогда для произвольного  $u \in G$   $A = A^u \leq H^u$ , поэтому  $A \leq \bigcap_{u \in G} H^u = \text{Core}_G(H)$ . Утверждение 2 очевидным образом следует из уже доказанного.  $\square$

**Теорема 2.5.7.** Пусть группа  $G$  транзитивно действует на множестве  $\Omega$ ,  $\omega \in \Omega$ ,  $\rho : G \rightarrow \text{Sym}(\Omega)$  — ассоциированное перестановочное представление. Тогда

$$\ker(\rho) = \text{Core}_G(G_\omega).$$

*Доказательство.*

$$\begin{aligned} g \in \ker(\rho) &\Leftrightarrow \rho_g = 1_\Omega \Leftrightarrow x\rho_g = x \ \forall x \in \Omega \Leftrightarrow xg = x \ \forall x \in \Omega \Leftrightarrow g \in G_x \ \forall x \in \Omega \Leftrightarrow \\ &\Leftrightarrow g \in \bigcap_{x \in \Omega} G_x. \end{aligned}$$

Так как  $G$  транзитивно действует на  $\Omega$ , то

$$\bigcap_{x \in \Omega} G_x = \bigcap_{g \in G} G_{\omega g} = \bigcap_{g \in G} gG_\omega g^{-1} = \bigcap_{g \in G} G_\omega^g = \text{Core}_G(G_\omega).$$

$\square$

**Следствие 2.5.8.** Пусть  $H \leq G$ ,  $N := \text{Core}_G(H)$ ,  $\Omega = \{Ha : a \in G\}$ . Тогда  $G$  транзитивно действует на  $\Omega$  по правилу  $(Ha).g = Ha_d$  для всех  $a, g \in G$ . Стабилизатор точки  $H$  равен  $H$ . Ядро этого действия равно  $N$ .  $\overline{G}$  точно и транзитивно действует на  $\Omega$  по правилу  $\omega\bar{g} = \omega g$  для всех  $\omega \in \Omega$ ,  $g \in G$ , стабилизатор точки  $H$  в  $\overline{G}$  равен  $\overline{H}$  (черта — это естественный морфизм  $G \rightarrow G/N$ ).

*Доказательство.* Это следствие из 2.5.3, 2.4.1, 2.5.7, 2.1.16.  $\square$

**Теорема 2.5.9.** (Кэли) Пусть  $G$  — конечная группа порядка  $n$ . Тогда существует мономорфизм  $G \rightarrow S_n$ .

*Доказательство.* Рассмотрим действие группы  $G$  умножениями на множестве  $\Omega := G$  и ассоциированное перестановочное представление  $\rho : G \rightarrow \text{Sym}(\Omega)$ . Это действие транзитивно, и каждый стабилизатор точки тривиален, поэтому в силу 2.5.7  $\ker(\rho) = \{1\}$ , следовательно морфизм  $\rho$  инъективен. Так как  $\text{Sym}(\Omega) \simeq S_n$ , то теорема доказана.  $\square$

**Определение 2.5.5.**  $G$ -множество  $\Omega$  называется транзитивным, если  $G$  транзитивно действует на  $\Omega$ .

**Теорема 2.5.10.** Пусть  $\Gamma, \Delta$  —  $G$ -множества,  $\gamma \in \Gamma$ ,  $\delta \in \Delta$ . Тогда выполняются следующие утверждения:

- 1) если существует морфизм  $\phi : \Gamma \rightarrow \Delta$ , для которого  $\gamma\phi = \delta$ , то  $G_\gamma \leq G_\delta$ ;
- 2) если  $\Gamma$  транзитивно и  $G_\gamma \leq G_\delta$ , то существует, и только один, морфизм  $\phi : \Gamma \rightarrow \Delta$ , такой, что  $\gamma\phi = \delta$ ;
- 3) если  $\Gamma, \Delta$  транзитивны и  $G_\gamma = G_\delta$ , то существует, и только один, изоморфизм  $\phi : \Gamma \rightarrow \Delta$ , такой, что  $\gamma\phi = \delta$ .

*Доказательство.*

1. Пусть существует морфизм  $\phi : \Gamma \rightarrow \Delta$ , для которого  $\gamma\phi = \delta$ .

$$g \in G_\gamma \Rightarrow \gamma g = \gamma \Rightarrow (\gamma g)\phi = \gamma\phi \Rightarrow (\gamma\phi)g = \gamma\phi \Rightarrow \delta g = \delta \Rightarrow g \in G_\delta,$$

следовательно,  $G_\gamma \leq G_\delta$ .

2. Пусть  $\Gamma$  транзитивно и  $G_\gamma \leq G_\delta$ . Введем отображения  $\alpha : G \rightarrow \Gamma$ ,  $g\alpha = \gamma g$  для любого  $g \in G$ ,  $\beta : G \rightarrow \Delta$ ,  $g\beta = \delta g$ . Предположим, что  $g, h \in G$  таковы, что  $g\alpha = h\alpha$ .

$$\begin{aligned} g\alpha = h\alpha &\Rightarrow \gamma g = \gamma h \Rightarrow \gamma = \gamma h g^{-1} \Rightarrow h g^{-1} \in G_\gamma \leq G_\delta \Rightarrow h g^{-1} \in G_\delta \Rightarrow \\ &\Rightarrow \delta = \delta h g^{-1} \Rightarrow \delta g = \delta h \Rightarrow g\beta = h\beta. \end{aligned}$$

Мы доказали, что  $g\alpha = h\alpha \Rightarrow g\beta = h\beta$  для произвольных  $g, h \in G$ . Так как  $\alpha$  сюръективно (это следует из транзитивности действия  $G$  на  $\Gamma$ ), то мы находимся в ситуации теоремы об эпиморфизмах множеств 5.1.11, из которой вытекает, что

существует, и только одно отображение  $\phi : \Gamma \rightarrow \Delta$  такое, что  $\alpha\phi = \beta$ . Выберем произвольный элемент  $g \in G$ .

$$(\gamma g)\phi = (g\alpha)\phi = g(\alpha\phi) = g\beta = \delta g.$$

Таким образом,  $(\gamma g)\phi = \delta g$  для всех  $g \in G$ . Покажем, что  $\phi$  — морфизм  $G$ -множеств. Пусть  $g \in G$ ,  $\gamma' \in \Gamma$ . Так как  $G$  транзитивно действует на  $\Gamma$ , то  $\gamma' = \gamma h$  для некоторого  $h \in G$ .

$$(\gamma' g)\phi = (\gamma h g)\phi = \delta h g = (\gamma h)\phi g = (\gamma' \phi)g,$$

то есть  $\phi$  — морфизм. Покажем, что  $\phi$  единственно. Пусть  $\phi' : \Gamma \rightarrow \Delta$  — морфизм, для которого  $\gamma\phi' = \delta$ . Для любого  $g \in G$

$$g(\alpha\phi') = (g\alpha)\phi' = (\gamma g)\phi' = \gamma\phi'g = \delta g = g\beta,$$

следовательно,  $\alpha\phi' = \beta$ . В силу теоремы об эпиморфизмах множеств,  $\phi' = \phi$ .

3. В силу 2 существуют морфизмы  $\alpha : \Gamma \rightarrow \Delta$ ,  $\beta : \Delta \rightarrow \Gamma$  такие, что  $\gamma\alpha = \delta$ ,  $\delta\beta = \gamma$ . Тогда  $\alpha\beta : \Gamma \rightarrow \Gamma$  — морфизм и  $\gamma(\alpha\beta) = \gamma$ . С другой стороны,  $\text{id}_\Gamma : \Gamma \rightarrow \Gamma$  — тождественное отображение  $\Gamma$  — тоже морфизм, не сдвигающий  $\gamma$ . В силу (2)  $\alpha\beta = 1_\Gamma$ . Аналогично доказывается, что  $\beta\alpha = \text{id}_\Delta$ . Отсюда следует, что  $\alpha$  — изоморфизм.  $\square$

**Теорема 2.5.11.** Пусть  $\Gamma, \Delta$  — транзитивные  $G$ -множества,  $\gamma \in \Gamma$ ,  $\delta \in \Delta$ . Тогда  $\Gamma \simeq \Delta$  если и только если подгруппы  $G_\gamma, G_\delta$  сопряжены.

*Доказательство.* Пусть  $\Gamma \simeq \Delta$  и  $\phi : \Gamma \rightarrow \Delta$  — изоморфизм. Обозначим  $\delta' := \gamma\phi$ . В силу 2.4.14  $G_\gamma = G_{\delta'}$ . Так как  $\Delta$  — транзитивное  $G$ -множество, то  $\delta' = \delta g$  для некоторого  $g \in G$ , поэтому

$$G_\gamma = G_{\delta'} = G_{\delta g} = G_{\delta^g},$$

следовательно,  $G_\gamma, G_\delta$  сопряжены. Обратно, предположим, что  $G_\gamma, G_\delta$  сопряжены и  $G_\gamma = G_{\delta^g}$ ,  $g \in G$ . Тогда

$$G_\gamma = G_{\delta^g} = G_{\delta g} = G_{\delta'},$$

где  $\delta' = \delta g$ . В силу 2.5.10  $\Gamma \simeq \Delta$ .  $\square$

**Теорема 2.5.12.** Пусть  $\Omega$  — транзитивное  $G$ -множество,  $\omega \in \Omega$ . Тогда  $\Omega \simeq G/G_\omega$ .

*Доказательство.* Очевидно, стабилизатор точки  $\omega$  (равный  $G_\omega$ ) совпадает со стабилизатором точки  $G_\omega \in G/G_\omega$  (относительно действия правыми умножениями  $G$  на  $G/G_\omega$ ). Так как оба действия транзитивны, то, в силу теоремы 2.5.11,  $\Omega \simeq G/G_\omega$ .  $\square$

**Теорема 2.5.13.** (Длина орбиты) Пусть группа  $G$  транзитивно действует на множестве  $\Omega$ ,  $\omega \in \Omega$ . Тогда  $|\Omega| = [G : G_\omega]$ .

*Доказательство.* Так как  $\Omega \simeq G/G_\omega$ , то  $|\Omega| = |G/G_\omega| = [G : G_\omega]$ .  $\square$

**Теорема 2.5.14.** (Пуанкаре) Пусть  $G$  — группа,  $H \leq G$ ,  $[G : H] =: n < \infty$ . Тогда  $n \mid [G : \text{Core}_G(H)] \mid n!$ .

*Доказательство.* Рассмотрим действие  $G$  правыми умножениями на  $G/H =: \Omega$ , и ассоциированное перестановочное представление  $\rho : G \rightarrow \text{Sym}(\Omega)$ . Пусть  $N := \text{Core}_G(H)$  и  $- : G \rightarrow G/N$  — естественный морфизм. В силу 2.5.8  $\ker(\rho) = N$ , и  $\bar{G}$  точно и транзитивно действует на  $\Omega$ . Пусть  $n < \infty$ , тогда  $|\Omega| = n < \infty$ , следовательно  $\text{Sym}(\Omega)$  конечна, и так как  $G\rho \leq \text{Sym}(\Omega)$ , то и  $G\rho$  конечна. В силу 1.6.22  $G\rho \simeq \bar{G}$ , поэтому  $\bar{G}$  конечна. По формуле длины орбиты 2.5.13  $n = |\Omega| = [\bar{G} : \bar{H}] = \bar{G}/\bar{H}$ , поэтому  $n \mid |\bar{G}| = [G : N]$ . Так как  $\bar{G}$  вкладывается в  $\text{Sym}(\Omega)$ , то  $[G : N] = |\bar{G}| \mid |\text{Sym}(\Omega)| = n!$ .  $\square$

В частности, любая подгруппа конечного индекса содержит нормальную подгруппу конечного индекса.

**Теорема 2.5.15.** Пусть  $A, B$  — конечные подгруппы группы  $G$ . Тогда

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

*Доказательство.* Обозначим  $\Omega = \{Ab : b \in B\}$ . В силу 2.2.3, 2.3.1,

$$|AB| = \left| \bigcup_{C \in \Omega} C \right| = \sum_{C \in \Omega} |C| = \sum_{C \in \Omega} |A| = |\Omega||A|$$

и остается найти  $|\Omega|$ . Очевидно,  $B$  транзитивно действует на  $\Omega$  по правилу  $Ab.g = Abg$ . Поэтому, в силу 2.5.13,  $|\Omega| = [B : B_\omega]$ ,  $\omega = A$ . Согласно примеру 2.4.1,  $B_\omega = B \cap G_\omega = B \cap A$ .  $\square$

**Теорема 2.5.16.** Пусть  $G$  — группа,  $H \leq G$ ,  $a \in G$ . Тогда  $|a^H| = [H : C_H(a)]$ .

*Доказательство.* Группа  $H$  транзитивно действует сопряжениями на  $a^H$ , поэтому  $|a^H| = [H : H_a]$ . Так как  $H_a = C_H(a)$  (2.4.2), то теорема доказана.  $\square$

**Теорема 2.5.17.** Пусть  $G$  — группа,  $H \leq G$ ,  $S \subseteq G$ . Тогда  $|\{S\}^H| = [H : N_H(S)]$ .

*Доказательство.* Группа  $H$  транзитивно действует сопряжениями на  $\{S\}^H$ , поэтому  $|\{S\}^H| = [H : H_{\{S\}}]$ . Так как  $H_{\{S\}} = N_H(S)$  (2.4.3), то теорема доказана.  $\square$

Если  $a \in G$ , то, конечно,  $a \in a^G$ .

**Лемма 2.5.18.** Пусть  $G$  — группа,  $a \in G$ . Тогда  $a^G = \{a\}$  если и только если  $a \in Z(G)$ .

*Доказательство.* Пусть  $a \in Z(G)$ , тогда

$$a^G = \{g^{-1}ag : g \in G\} = \{ag^{-1}g : g \in G\} = \{a\}.$$

Обратно, пусть  $a^G = \{a\}$ . Тогда для любого  $g \in G$  мы имеем  $a^g = a$ , то есть  $g^{-1}ag = a$ , откуда следует, что  $ag = ga$  для всех  $g \in G$ , то есть  $a \in Z(G)$ .  $\square$

**Теорема 2.5.19.** Пусть  $G$  — конечная неабелева группа. В каждом неоднородном классе сопряженности  $G$  выберем по одному элементу и обозначим их  $a_1, \dots, a_l$ . Тогда

$$|G| = |Z(G)| + \sum_{i=1}^l [G : C_G(a_i)].$$

*Доказательство.* Пусть  $Z(G) = \{z_1, \dots, z_n\}$ , причем элементы  $z_i$  различны. Тогда

$$z_1, \dots, z_n, a_1, \dots, a_l$$

— система представителей классов сопряженности  $G$ , поэтому, в силу 2.2.4,

$$|G| = \sum_{i=1}^n |z_i^G| + \sum_{i=1}^l |a_i^G| = n + \sum_{i=1}^l [G : C_G(a_i)] = |Z(G)| + \sum_{i=1}^l [G : C_G(a_i)].$$

$\square$

**Теорема 2.5.20.** Пусть конечная группа  $G$  действует на конечном множестве  $\Omega$  и  $d$  делит порядок любой неоднородной орбиты. Тогда

$$|\Omega| \equiv |C_\Omega(G)| \pmod{d}.$$

*Доказательство.* Так как  $|\Omega|$  равен сумме порядков орбит, то  $|\Omega|$  сравним с количеством одноэлементных орбит по модулю  $d$ , то есть с количеством точек  $\Omega$ , неподвижных относительно  $G$ . Отсюда  $|\Omega| \equiv |C_\Omega(G)| \pmod{d}$ .  $\square$

**Теорема 2.5.21.** Пусть конечная группа  $P$  порядка  $p^n$ ,  $n \in \mathbb{Z}_{\geq 0}$ , действует на конечном множестве  $\Omega$ . Тогда  $|\Omega| \equiv |C_\Omega(P)| \pmod{p}$ .

*Доказательство.* Очевидно, если  $H < P$ , то  $p \mid [P : H]$ , поэтому  $p$  делит порядок каждой неоднородной орбиты. Остается применить 2.5.20.  $\square$

## 2.6 Характеры действий

**Определение 2.6.1.** Пусть группа  $G$  действует на конечном множестве  $\Omega$ . Характером этого действия назовем функцию  $\chi : G \rightarrow \mathbb{Z}_{\geq 0}$ ,  $g \mapsto |C_{\Omega}(g)|$ .

Таким образом,  $g\chi$  — это количество точек множества  $\Omega$ , неподвижных относительно  $g$ .

**Предложение 2.6.1.** Характеры изоморфных действий равны.

*Доказательство.* Пусть  $G$  — группа,  $\Omega \rightarrow \Omega'$  — изоморфизм  $G$ -множеств,  $\chi$  — характер  $\Omega$ ,  $\chi'$  — характер  $\Omega'$ ,  $g \in G$ . В силу 2.4.5 и замечания 2.4.11 (применяем соглашение о черте к изоморфизму  $\Omega \cup G \rightarrow \Omega' \cup G$ )

$$g\chi' = |C_{\Omega'}(g)| = |C_{\bar{\Omega}}(\bar{g})| = |\overline{C_{\Omega}(g)}| = |C_{\Omega}(g)| = g\chi.$$

□

**Предложение 2.6.2.** Пусть группа  $G$  действует на конечном множестве  $\Omega$ ,  $\chi$  — характер этого действия,  $n \in \mathbb{N}$ ,  $\Omega = \bigcup_{i=1}^n \Omega_i$ , причем  $\Omega_i \cap \Omega_j = \emptyset$  при  $i \neq j$  и множества  $\Omega_i$   $G$ -инвариантны. Обозначим  $\chi_i$  характер действия  $G$  на  $\Omega_i$ . Тогда  $\chi = \sum_{i=1}^n \chi_i$ .

*Доказательство.* Пусть  $g \in G$ , тогда  $C_{\Omega}(g) = \bigcup_{i=1}^n C_{\Omega_i}(g)$ , причем в данном объединении слагаемые попарно не пересекаются, поэтому

$$g\chi = |C_{\Omega}(g)| = \left| \bigcup_{i=1}^n C_{\Omega_i}(g) \right| = \sum_{i=1}^n |C_{\Omega_i}(g)| = \sum_{i=1}^n g\chi_i.$$

□

**Предложение 2.6.3.** Пусть группа  $G$  действует на конечных множествах  $\Omega_i$ ,  $i \in \{1, \dots, n\}$ ,  $n \in \mathbb{N}$ ,  $\Omega = \prod_{i=1}^n \Omega_i$ . Группа  $G$  действует на  $\Omega$ , как указано в 2.1.17. Обозначим  $\chi$  — характер действия  $G$  на  $\Omega$ ,  $\chi_i$  — характер действия  $G$  на  $\Omega_i$ . Тогда  $\chi = \prod_{i=1}^n \chi_i$ . В частности, если  $G$  действует на конечном множестве  $\Omega$  и  $\chi$  — характер этого действия,  $k \in \mathbb{N}$ , то характер действия  $G$  на  $\Omega^k$  равен  $\chi^k$ .

*Доказательство.* Пусть  $I = \{1, \dots, n\}$ . Если  $\omega = (\omega_i)_{i \in I} \in \Omega$ ,  $g \in G$ , то  $\omega g = \omega$  тогда и только тогда, когда  $\omega_i g = \omega_i$  для всех  $i \in I$ , следовательно,  $C_{\Omega}(g) = \prod_{i \in I} C_{\Omega_i}(g)$ , поэтому

$$g\chi = |C_{\Omega}(g)| = \left| \prod_{i \in I} C_{\Omega_i}(g) \right| = \prod_{i \in I} |C_{\Omega_i}(g)| = \prod_{i \in I} g\chi_i = g \prod_{i \in I} \chi_i.$$

□

**Лемма 2.6.4.** Пусть  $\phi : X \rightarrow Y$  — сюръективное отображение конечных множеств, причем для любого  $y \in Y$   $|y\phi^{-1}| = n$ . Тогда  $n|Y| = |X|$ .

*Доказательство.* Это очевидно.  $\square$

**Лемма 2.6.5.** Пусть  $H$  — подгруппа группы  $G$ ,  $\Omega = G/H$ ,  $G$  действует на  $\Omega$  стандартным образом (см. 2.1.5) и  $\chi$  — характер этого действия. Тогда для любого  $g \in G$

$$g\chi = \frac{|g^G \cap H| |C_G(g)|}{|H|}.$$

*Доказательство.* Обозначим  $\phi : G \rightarrow \Omega$ ,  $x \mapsto Hx$ . Очевидно,  $\phi$  сюръективно и если  $\omega \in \Omega$ ,  $a \in G$ ,  $a\phi = \omega$ , то  $\omega\phi^{-1} = Ha$  (см. 2.2.6). В частности, для любого  $\omega \in \Omega$   $|\omega\phi^{-1}| = |H|$ . Обозначим  $C_\Omega(g)\phi^{-1} =: A$  и заметим, что  $\phi$  можно рассматривать как сюръективное отображение  $A \rightarrow C_\Omega(g)$ . В силу 2.6.4

$$g\chi = |C_\Omega(g)| = \frac{|A|}{|H|}. \quad (2.6.1)$$

Согласно 1.4.2

$$\begin{aligned} A &= \{a \in G : Hag = Ha\} = \{a \in G : Haga^{-1} = H\} = \{a \in G : aga^{-1} \in H\} = \\ &= \{a \in G : aga^{-1} \in g^G \cap H\}. \end{aligned}$$

Рассмотрим отображение  $\psi : G \rightarrow g^G$ ,  $x \mapsto xgx^{-1}$ . Очевидно, отображение  $\psi$  сюръективно и по 2.4.15  $g^x\psi^{-1} = C_G(g)x$  и  $|g^x\psi^{-1}| = C_G(g)$ . Можно записать  $A = (g^G \cap H)\psi^{-1}$  и считать, что  $\psi$  — сюръективное отображение  $A \rightarrow g^G \cap H$ . В силу 2.6.4  $|A| = |g^G \cap H| |C_g(g)|$ . Используя 2.6.1, получаем, что

$$g\chi = \frac{|g^G \cap H| |C_G(g)|}{|H|}.$$

$\square$

**Теорема 2.6.6.** Пусть группа  $G$  транзитивно действует на множестве  $\Omega$ ,  $\omega \in \Omega$ ,  $\chi$  — характер данного действия. Тогда для любого  $g \in G$

$$g\chi = \frac{|g^G \cap G_\omega| |C_G(g)|}{|G_\omega|}.$$

*Доказательство.* В силу 2.5.12  $\Omega \simeq G/G_\omega$ , а из 2.6.1 следует, что  $\chi$  совпадает с характером стандартного действия  $G$  на  $G/G_\omega$ . Остальное следует из 2.6.5.  $\square$

В качестве следствия получаем следующие два утверждения.

**Пример 2.6.1.** Пусть  $\chi$  — характер действия группы  $G$  сопряжениями на классе сопряженности  $a^G$  элемента  $a \in G$ . Тогда для любого  $g \in G$

$$g\chi = \frac{|g^G \cap C_G(a)||C_G(g)|}{|C_G(a)|}.$$

**Пример 2.6.2.** Пусть  $\chi$  — характер действия группы  $G$  сопряжениями на классе сопряженности  $\{H\}^G$  подгруппы  $H \leq G$ . Тогда для любого  $g \in G$

$$g\chi = \frac{|g^G \cap N_G(H)||C_G(g)|}{|N_G(H)|}.$$

## 2.7 Лемма Бернсайда

**Лемма 2.7.1.** Пусть конечная группа  $G$  транзитивно действует на конечном множестве  $\Omega$ ,  $\chi$  — характер этого действия. Тогда

$$\frac{1}{|G|} \sum_{g \in G} g\chi = 1.$$

*Доказательство.* Введем отображение  $I : \Omega \times G \rightarrow \{0, 1\}$

$$(\omega, g)I = \begin{cases} 1, & \text{если } \omega g = \omega \\ 0, & \text{если } \omega g \neq \omega \end{cases}$$

и заметим, что  $g\chi = \sum_{\omega \in \Omega} (\omega, g)I$ .

$$\frac{1}{|G|} \sum_{g \in G} g\chi = \frac{1}{|G|} \sum_{g \in G} \sum_{\omega \in \Omega} (\omega, g)I = \frac{1}{|G|} \sum_{\omega \in \Omega} \sum_{g \in G} (\omega, g)I = \frac{1}{|G|} \sum_{\omega \in \Omega} |G_\omega|.$$

Возьмем  $a \in \Omega$ . В силу 2.4.7  $|G_\omega| = |G_a|$ , поэтому

$$\frac{1}{|G|} \sum_{\omega \in \Omega} |G_\omega| = \frac{1}{|G|} \sum_{\omega \in \Omega} |G_a| = \frac{1}{|G|} |\Omega| |G_a|.$$

Согласно 2.5.13  $|\Omega| = [G : G_a]$ , следовательно,

$$\frac{1}{|G|} |\Omega| |G_a| = \frac{1}{|G|} [G : G_a] |G_a| = \frac{1}{|G|} |G| = 1.$$

□

Если группа  $G$  действует на множестве  $\Omega$ , то количество  $G$ -орбит обозначим  $[\Omega : G]$ .

**Теорема 2.7.2.** (Лемма Бернсайда) Пусть конечная группа  $G$  действует на конечном множестве  $\Omega$ ,  $\chi$  — характер этого действия. Тогда

$$\frac{1}{|G|} \sum_{g \in G} g\chi = [\Omega : G].$$

*Доказательство.* Пусть  $n$  — количество орбит,  $\Omega_1, \dots, \Omega_n$  — все различные орбиты,  $a_i \in \Omega_i$ ,  $\chi_i$  — характер действия  $G$  на  $\Omega_i$ . Тогда на каждом множестве  $\Omega_i$   $G$  действует транзитивно, и в силу 2.7.1

$$\frac{1}{|G|} \sum_{g \in G} g\chi_i = 1.$$

В силу 2.6.2  $\chi = \sum_{i=1}^n \chi_i$ .

$$\frac{1}{|G|} \sum_{g \in G} g\chi = \frac{1}{|G|} \sum_{g \in G} \sum_{i=1}^n g\chi_i = \sum_{i=1}^n \frac{1}{|G|} \sum_{g \in G} g\chi_i = \sum_{i=1}^n 1 = n.$$

□

**Следствие 2.7.3.** Пусть конечная группа  $G$  действует на конечном множестве  $\Omega$ ,  $\chi$  — характер данного действия. Тогда это действие транзитивно если и только если

$$\frac{1}{|G|} \sum_{g \in G} g\chi = 1.$$

Если  $\Omega$  — множество и  $k \in \mathbb{N}$ , то обозначим  $\Omega^{(k)}$  множество всех строк  $(\omega_1, \dots, \omega_k) \in \Omega^k$ , в которых элементы не повторяются, то есть  $\omega_i \neq \omega_j$  для всех  $i \neq j$ .

**Определение 2.7.1.** Действие группы  $G$  на множестве  $\Omega$  называется  $k$ -транзитивным, если  $k \in \mathbb{N}$ ,  $k \leq |\Omega|$  и  $G$  транзитивно действует на  $\Omega^{(k)}$ .

Другими словами, группа  $G$  действует на множестве  $\Omega$   $k$ -транзитивно, если в  $\Omega$  найдутся  $k$  различных элементов, и если  $a_1, \dots, a_k \in \Omega$  — различные элементы, и  $b_1, \dots, b_k \in \Omega$  — различные элементы, то найдется  $g \in G$  такой, что  $a_i g = b_i$  для всех  $i \in \{1, \dots, k\}$ .

**Лемма 2.7.4.** Если  $k, l \in \mathbb{N}$ ,  $k \leq l$  и группа  $G$  действует на множестве  $\Omega$   $l$ -транзитивно, то  $G$  действует на  $\Omega$   $k$ -транзитивно.

*Доказательство.* Это очевидно.  $\square$

**Определение 2.7.2.** Пусть  $n \in \mathbb{N}$ . Количество всевозможных разбиений  $n$ -элементного множества называется  $n$ -м числом Белла и обозначается  $B_n$ .

Приведем несколько первых значений чисел Белла:

$$1, 2, 5, 15, 52, 203, 877, 4140, 21147, 115975, 678570, 4213597, 27644437, 190899322, \\ 1382958545, 10480142147, 82864869804, 682076806159, 5832742205057, \dots$$

**Лемма 2.7.5.** Пусть  $k \in \mathbb{N}$ , группа  $G$  действует на множестве  $\Omega$ ,  $k \leq |\Omega|$ . Группа  $G$   $k$ -транзитивно действует на множестве  $\Omega$  тогда и только тогда, когда

$$[\Omega^k : G] = B_k.$$

*Доказательство.* Без ущерба для понимания остальной части книги читатель может ограничиться случаем  $k = 2$ . Пусть  $\omega \in \Omega^k$ . Тогда  $\omega$  определяет отношение эквивалентности  $\rho_\omega$  на множестве  $I := \{1, \dots, k\}$ :

$$i\rho_\omega j \Leftrightarrow \omega_i = \omega_j.$$

Пусть  $g \in G$ .

$$(\omega g)_i = (\omega g)_j \Leftrightarrow \omega_i g = \omega_j g \Leftrightarrow \omega_i = \omega_j,$$

поэтому

$$\rho_{\omega g} = \rho_\omega$$

для всех  $\omega \in \Omega$ ,  $g \in G$ . Другими словами, если элементы  $\omega, \omega' \in \Omega^k$   $G$ -эквивалентны, то  $\rho_\omega = \rho_{\omega'}$ . Для произвольного  $\omega \in \Omega^k$  обозначим  $\gamma_\omega$  разбиение множества  $I$ , соответствующее отношению эквивалентности  $\rho_g$ . В силу сказанного ранее, для любых  $\omega \in \Omega^k$ ,  $g \in G$

$$\gamma_{\omega g} = \gamma_\omega. \quad (2.7.1)$$

Обозначим  $Y$  множество всех разбиений множества  $I$ . Мы имеем отображение  $\gamma : \Omega^k \rightarrow Y$ ,  $\omega \mapsto \gamma_\omega$ . Покажем, что это отображение сюръективно. Пусть  $P := \{P_1, \dots, P_l\}$  — разбиение множества  $I$ ,  $P_i \neq P_j$  при  $i \neq j$ . Тогда  $l \leq |\Omega|$ , поэтому найдутся различные  $a_1, \dots, a_l \in \Omega$ . Образует строку  $\omega \in \Omega^k$  так: На места в  $\omega$  с номерами из  $P_i$  запишем элемент  $a_i$ ,  $i \in I$ . Очевидно, получим строку  $\omega \in \Omega^k$ , причем  $\gamma_\omega = P$ . Таким образом, отображение  $\gamma : \Omega^k \rightarrow Y$  сюръективно.

$X$  — множество всех  $G$ -орбит множества  $\Omega^k$ ,  $\alpha : \Omega^k \rightarrow X$ ,  $\omega \mapsto \omega G$ . Очевидно,  $\alpha$  — сюръективное отображение, причем из 2.7.1 и 5.1.11 следует, что существует и единственно такое отображение  $\beta : X \rightarrow Y$ , что коммутативна диаграмма

$$\begin{array}{ccc} & X & \\ \alpha \nearrow & & \searrow \beta \\ \Omega^k & \xrightarrow{\gamma} & Y \end{array} .$$

Так как  $\gamma$  сюръективно, то и  $\beta$  сюръективно.

Предположим, что  $G$   $k$ -транзитивно действует на  $\Omega$  и докажем, что  $\beta$  — биекция. В силу 5.1.11 достаточно доказать, что если  $a, b \in \Omega^k$  и  $\gamma_a = \gamma_b$ , то  $a, b$  лежат в одной  $G$ -орбите. Пусть  $P := \{P_1, \dots, P_l\}$  — разбиение множества  $I$ ,  $P_i \neq P_j$  при  $i \neq j$ ,  $P = \gamma_a = \gamma_b$ . Выберем в каждом  $P_j$  по одному представителю  $i_j$ , тогда элементы  $a_{i_j}$ ,  $j \in \{1, \dots, l\}$  различны. Аналогично, элементы  $b_{i_j}$ ,  $j \in \{1, \dots, l\}$  различны. Так как  $l \leq k$ , то в силу 2.7.4 найдется такой элемент  $g \in G$ , что  $a_{i_j}g = b_{i_j}$  для всех  $j \in \{1, \dots, l\}$ . Но тогда и  $ag = b$ , что и требовалось доказать.

Обратно, пусть  $[\Omega^k : G] = B_k$ , тогда  $|X| = |Y|$ . Но тогда из сюръективности  $\beta$  следует инъективность, поэтому  $\beta$  — биекция, следовательно для любых  $a, b \in \Omega^k$  из  $\gamma_a = \gamma_b$  следует, что  $a\alpha = b\alpha$ , то есть  $a, b$   $G$ -эквивалентны. Докажем, что  $G$   $k$ -транзитивно действует на  $\Omega$ . Пусть  $a, b \in \Omega^k$  — строки, в каждой из которых элементы не повторяются. Тогда

$$\gamma_a = \gamma_b = \{\{i\} : i \in I\},$$

поэтому  $a, b$   $G$ -эквивалентны. □

**Теорема 2.7.6.** Пусть  $k \in \mathbb{N}$ , группа  $G$  действует на множестве  $\Omega$ ,  $k \leq |\Omega|$ ,  $\chi$  — соответствующий характер. Данное действие  $k$ -транзитивно тогда и только тогда, когда

$$\frac{1}{|G|} \sum_{g \in G} (g\chi)^k = B_k.$$

*Доказательство.* Пусть  $\chi$  — характер действия  $G$  на  $\Omega$ . В силу 2.7.5 действие  $k$ -транзитивно тогда и только тогда, когда  $[\Omega^k : G] = B_k$ . В силу 2.7.2 и 2.6.3

$$[\Omega^k : G] = \frac{1}{|G|} \sum_{g \in G} (g\chi)^k.$$

□

## 2.8 Действия и факторизации

Факторизацией группы  $G$  называется любая пара  $(A, B)$  ее подгрупп, такая, что  $G = AB$ . Первые наши факторизации были связаны с 1.6.25. В следующем утверждении снова возникает факторизация.

**Теорема 2.8.1.** (Аргумент Фраттини) *Пусть группа  $G$  транзитивно действует на множестве  $\Omega$ ,  $\omega \in \Omega$ ,  $A = G_\omega$ ,  $B \leq G$ . Равносильны условия:*

- 1)  $B$  транзитивно действует на  $\Omega$ ;
- 2)  $G = AB$ .

*Доказательство.* 1. Предположим, что  $B$  транзитивно действует на  $\Omega$ . Пусть  $g \in G$ . Так как  $B$  транзитивно действует на  $\Omega$ , то  $\omega g = \omega b$  для некоторого  $b \in B$ . Следовательно,  $\omega gb^{-1} = \omega$ , откуда  $gb^{-1} \in G_\omega = A$ . Отсюда получаем, что  $g \in Ab \subseteq AB$ . Следовательно,  $G \subseteq AB \subseteq G$ , откуда  $G = AB$ .

2. Предположим, что  $G = AB$ . Тогда  $\Omega = \omega G = (\omega A)B = \omega B$ , следовательно  $B$  транзитивно действует на  $\Omega$ .  $\square$

Отметим, что 1.6.25 следует из 2.8.1.

**Лемма 2.8.2.** *Пусть группа  $G$  действует на множествах  $\Gamma, \Delta$ ,  $\delta \in \Delta$ . Если  $G$  транзитивно действует на  $\Delta$  и  $G_\delta$  транзитивно действует на  $\Gamma$ , то  $G$  транзитивно действует на  $\Gamma \times \Delta$ .*

*Доказательство.* Пусть  $\delta' \in \Delta$ . Так как  $G$  транзитивно действует на  $\Delta$ , то  $\delta' = \delta g$  для некоторого  $g \in G$ . Тогда  $G_{\delta'} = G_{\delta g} = G_\delta^g$ . Так как  $G_\delta$  транзитивно действует на  $\Gamma$ , то в силу 2.5.5  $G_\delta^g$  тоже транзитивно действует на  $\Gamma$ , следовательно, для любой точки  $\delta' \in \Delta$  группа  $G_{\delta'}$  транзитивно действует на  $\Gamma$ .

Теперь докажем, что  $G$  транзитивно действует на  $E := \Gamma \times \Delta$ . Пусть  $\epsilon_1 = (\gamma_1, \delta_1)$ ,  $\epsilon_2 = (\gamma_2, \delta_2)$  — точки  $E$ . Так как  $G$  транзитивно действует на  $\Delta$ , то найдется элемент  $g_1 \in G$ , такой, что  $\delta_1 g_1 = \delta_2$ . Тогда

$$\epsilon_1 g_1 = (\gamma_1, \delta_1) g_1 = (\gamma_1 g_1, \delta_1 g_1) = (\gamma_1 g_1, \delta_2).$$

Так как  $G_{\delta_2}$  транзитивно действует на  $\Gamma$ , то найдется элемент  $g_2 \in G_{\delta_2}$ , такой, что  $\gamma_1 g_1 g_2 = \gamma_2$ . Тогда

$$\epsilon_1 g_1 g_2 = (\epsilon_1 g_1) g_2 = (\gamma_1 g_1, \delta_2) g_2 = (\gamma_1 g_1 g_2, \delta_2 g_2) = (\gamma_2, \delta_2) = \epsilon_2.$$

$\square$

Следующее утверждение связывает факторизации транзитивных действий с факторизациями группы.

**Теорема 2.8.3.** Пусть группа  $G$  действует на конечных множествах  $\Gamma, \Delta$ ,  $\gamma \in \Gamma$ ,  $\delta \in \Delta$ . Равносильны следующие утверждения:

- 1)  $G$  транзитивно действует на  $\Gamma \times \Delta$ ;
- 2)  $G$  транзитивно действует на  $\Gamma, \Delta$  и  $G = G_\gamma G_\delta$ .

*Доказательство.* Пусть  $G$  транзитивно действует на  $E := \Gamma \times \Delta$ ,  $A = G_\gamma$ ,  $B = G_\delta$ . Очевидно,  $G$  транзитивно действует на множествах  $\Gamma, \Delta$ .

Покажем, что  $G = AB$ . Пусть  $\gamma_1, \gamma_2 \in \Gamma$ . Так как  $G$  транзитивно действует на  $E$ , то  $(\gamma_1, \delta)g = (\gamma_2, \delta)$  для некоторого  $g \in G$ , откуда  $\delta g = \delta$ , то есть  $g \in B$  и  $\gamma_1 g = \gamma_2$ . Следовательно,  $B$  транзитивно действует на  $\Gamma$ . В силу аргумента Фраттини 2.8.1  $G = AB$ .

Обратно, пусть  $G$  транзитивно действует на  $\Gamma, \Delta$  и  $G = AB$ . Покажем, что  $G$  транзитивно действует на  $E$ . Из 2.8.1 следует, что  $B$  транзитивно действует на  $\Gamma$ . В силу 2.8.2  $G$  транзитивно действует на  $E$ .  $\square$

**Следствие 2.8.4.** Пусть  $G$  — группа,  $A, B \leq G$ ,  $G = AB$ ,  $g, h \in G$ . Тогда выполняются утверждения:

- 1)  $G = A^g B^h$ ;
- 2) если  $B$  сопряжена с  $A$ , то  $A = G$ ;
- 3) подгруппы  $A \cap B$ ,  $A^g \cap B^h$  сопряжены.

**Теорема 2.8.5.** Пусть  $G$  — произвольная группа, не обязательно конечная,  $A, B \leq G$ ,  $[G : A] < \infty$ ,  $[G : B] < \infty$ . Тогда имеют место следующие утверждения.

- 1)  $[G : A \cap B] \leq [G : A][G : B]$ ;
- 2)  $[G : A \cap B] = [G : A][G : B]$  тогда и только тогда, когда  $G = AB$ ;

*Доказательство.* 1. Пусть  $\Gamma = G/A$ ,  $\Delta = G/B$ ,  $E = \Gamma \times \Delta$ . Очевидно,  $E$  — конечное множество и  $|E| = |\Gamma||\Delta| = [G : A][G : B]$ . Так как  $|E| < \infty$ , то длина любой  $G$ -орбиты в множестве  $E$  конечна и не превосходит  $|E|$ . Кроме того, очевидно,  $G_{(A,B)} = A \cap B$ . Следовательно,

$$\infty > [G : A][G : B] = |E| \geq |(A, B)G| = [G : G_{(A,B)}] = [G : A \cap B].$$

2. Если  $[G : A][G : B] = [G : A \cap B]$ , то, в силу предыдущих соотношений,  $|E| = |(A, B)G|$ , поэтому  $E = (A, B)G$ , следовательно,  $G$  транзитивно действует на  $E$ . В силу леммы 2.8.3  $G = AB$ . Обратно, пусть  $G = AB$ . В силу 2.8.3  $G$  транзитивно действует на  $G/A \times G/B$ , следовательно,

$$[G : A][G : B] = |G/A \times G/B| = |(A, B)G| = [G : G_{(A,B)}] = [G : G_A \cap G_B] = [G : A \cap B].$$

□

**Теорема 2.8.6.** Пусть  $G$  — произвольная группа, не обязательно конечная,  $A_i \leq G$ ,  $[G : A_i] < \infty$  для  $i \in \{1, 2\}$  и  $([G : A_1], [G : A_2]) = 1$ . Тогда имеют место следующие утверждения.

- 1)  $[G : A_1 \cap A_2] = [G : A_1][G : A_2]$ ;
- 2)  $G = A_1 A_2$ .

*Доказательство.* Обозначим  $I = A_1 \cap A_2$ . В силу 2.8.5  $[G : I] \leq [G : A_1][G : A_2]$ . Покажем, что  $[G : I] \geq [G : A_1][G : A_2]$ . Пусть  $i \in \{1, 2\}$ . Тогда  $G \geq A_i \geq I$ . Заметим, что  $[A_i : I] \leq [G : I] < \infty$ , и  $[G : I] = [G : A_i][A_i : I]$ . Отсюда  $[G : A_i] \mid [G : I]$ . Так как  $([G : A_1], [G : A_2]) = 1$ , то  $[G : I]$  делится на  $[G : A_1][G : A_2]$ . Тем более  $[G : I] \geq [G : A_1][G : A_2]$ . Итак,  $[G : I] = [G : A_1][G : A_2]$ . В силу 2.8.5  $G = A_1 A_2$ . □

**Теорема 2.8.7.** Пусть группа  $G$  транзитивно действует на конечных множествах  $\Omega_1, \Omega_2$ , причем  $(|\Omega_1|, |\Omega_2|) = 1$ . Тогда  $G$  транзитивно действует на  $\Omega_1 \times \Omega_2$ .

*Доказательство.* Пусть  $x_i \in \Omega_i$ ,  $A_i = G_{x_i}$ ,  $i \in \{1, 2\}$ . Так как  $[G : A_i] = |\Omega_i|$ , то  $([G : A_1], [G : A_2]) = 1$ , и по 2.8.6  $G = A_1 A_2$ . Из 2.8.3 следует, что  $G$  транзитивно действует на  $\Omega_1 \times \Omega_2$ . □

## Глава 3

# Коммутаторы

**Определение 3.0.1.** Пусть  $G$  — группа,  $g, h \in G$ . Выражение  $g^{-1}h^{-1}gh$  называется коммутатором элементов  $g$  и  $h$  и обозначается  $[g, h]$ .

**Определение 3.0.2.** Пусть  $A, B \subseteq G$ . Группу  $\langle [a, b] : a \in A, b \in B \rangle$  назовем коммутатором множеств  $A, B$  и обозначим ее  $[A, B]$ . Если  $g \in G$ , то определим  $[g, A] := \langle [g, a] : a \in A \rangle$ .

**Определение 3.0.3.** Если  $n \in \mathbb{N}$  и  $A_1, \dots, A_n$  — элементы или подгруппы  $G$ , то по индукции определяем  $[A_1] := A_1$ , и при  $n > 1$   $[A_1, \dots, A_n] := [[A_1, \dots, A_{n-1}], A_n]$ .

В частности,  $[A, B, C] = [[A, B], C]$ .

**Предложение 3.0.1.** Пусть  $G$  — группа,  $x, y, z \in G$ . Тогда

- 1)  $[x, y] = 1$  если и только если  $xy = yx$ ;
- 2)  $[x, y]^{-1} = [y, x]$ ;
- 3)  $[x, y] = x^{-1}x^y$ ;
- 4)  $[xy, z] = [x, z]^y[y, z]$ ;
- 5)  $[xy, z] = [x, z][x, z, y][y, z]$ ;
- 6) если  $x_i, y_i \in G$  и  $[x_i, y_j] = 1$  для  $i, j \in \{1, 2\}$ , то  $[x_1y_1, x_2y_2] = [x_1, x_2][y_1, y_2]$ ;
- 7)  $[x, y^{-1}, z]^y[y, z^{-1}, x]^z[z, x^{-1}, y]^x = 1$  (тождество Ф. Холла).

*Доказательство.* Проверим лишь тождество Ф. Холла. Обозначим  $a = a(x, y, z) := xzx^{-1}yx$ ,  $b := a(y, z, x)$ ,  $c := a(z, x, y)$ . Тогда  $[x, y^{-1}, z]^y = a^{-1}b$ ,  $[y, z^{-1}, x]^z = b^{-1}c$ ,  $[z, x^{-1}, y]^x = c^{-1}a$ , и левую часть тождества можно записать как  $a^{-1}bb^{-1}cc^{-1}a = 1$ .  $\square$

Из тождества Ф. Холла вытекает важное следствие.

**Лемма 3.0.2.** *(о трех подгруппах) Пусть  $A, B, C \leq G$ ,  $N \trianglelefteq G$ . Если  $[A, B, C] \leq N$  и  $[B, C, A] \leq N$ , то и  $[C, A, B] \leq N$ .*

**Определение 3.0.4.** *Подмножества  $A, B$  группоиды  $G$  назовем поэлементно перестановочными, если любой элемент множества  $A$  перестановочен с любым элементом множества  $B$ .*

Очевидно, поэлементно перестановочные множества перестановочны, но обратное неверно.

**Теорема 3.0.3.** *Пусть  $A, B, C \leq G$ . Тогда*

- 1) *если  $A_1 \leq A$ ,  $B_1 \leq B$ , то  $[A_1, B_1] \leq [A, B]$ ;*
- 2)  *$[A, B] = [B, A]$ ;*
- 3) *если  $g \in G$ , то  $[A, B]^g = [A^g, B^g]$ ;*
- 4) *еёобще, если  $\sigma: G \rightarrow H$  — морфизм, то  $[A, B]^\sigma = [A^\sigma, B^\sigma]$ ;*
- 5)  *$[A, B] = \{1\}$  если и только если  $A, B$  поэлементно перестановочны;*
- 6)  *$[A, B] \leq A$  если и только если  $B \leq N_G(A)$ ;*
- 7) *если  $A, B \trianglelefteq G$ , то  $[A, B] \trianglelefteq G$  и  $[A, B] \leq A \cap B$ .*
- 8)  *$B \leq N_G([a, B])$  для всех  $a \in G$ ;*
- 9)  *$B \leq N_G([A, B])$ ;*
- 10)  *$[A, B] \trianglelefteq \langle A, B \rangle$ ;*
- 11) *если  $A_i, B_i \subseteq G$  для  $i \in \{1, 2\}$ , и  $[A_i, B_j] = \{1\}$ , то  $[A_1B_1, A_2B_2] \leq [A_1, A_2][B_1, B_2]$ .*
- 12) *Если  $B \leq N_G([A, C])$ , то  $[AB, C] = [A, C][B, C]$ . В аддитивной записи последнее тождество принимает вид:  $[A+B, C] = [A, C] + [B, C]$ . В частности, если  $A_1, \dots, A_n, B \trianglelefteq G$ , то  $[\prod_{i=1}^n A_i, B] = \prod_{i=1}^n [A_i, B]$ .*

$$13) [AB, G] = [A, G][B, G];$$

*Доказательство.*

6.

$$[A, B] \leq A \Leftrightarrow [a, b] \leq A \quad \forall a \in A, b \in B \Leftrightarrow a^{-1}a^b \in A \quad \forall a \in A, b \in B \Leftrightarrow$$

$$\Leftrightarrow a^b \in aA \quad \forall a \in A, b \in B \Leftrightarrow a^b \in A \quad \forall a \in A, b \in B \Leftrightarrow B \leq N_G(A).$$

7. Пусть  $A, B \trianglelefteq G$ . Если  $g \in G$ , то  $[A, B]^g = [A^g, B^g] = [A, B]$ , поэтому  $[A, B] \trianglelefteq G$ . Из  $A \trianglelefteq G$  следует, что  $B \leq N_G(A)$ , поэтому в силу 6)  $[A, B] \leq A$ . Аналогично,  $[A, B] \leq B$ . Так как  $[A, B] \leq A, B$ , то  $[A, B] \leq A \cap B$ .

8. Пусть  $x, y \in H \leq G, z \in G$ .  $[xy, z] = [x, z]^y[y, z] = [x^y, z^y][y, z]$ ,  $[x^y, z^y] = [xy, z][y, z]^{-1} \in [H, z][H, z] = [H, z]$ . Итак,  $[x^y, z^y] \in [H, z]$ . Если  $x$  пробегает  $H$ , то и  $x^y$  пробегает  $H$ , следовательно,  $[H, z]^y = [H, z^y] \leq [H, z]$ . Таким образом,  $H \leq N_G([H, z])$ . Так как  $[H, z] = [z, H]$ , то  $H \leq N_G([z, H])$ .

9. Заметим, что  $[A, B] = \langle [a, B] : a \in A \rangle$ . Так как  $B$  нормализует  $[a, B]$  для всех  $a \in A$ , то  $B$  нормализует  $[A, B]$ .

10. Очевидно, ввиду предыдущего.

11. Это следует из тождества 6).

12. Пусть  $a \in A, b \in B, c \in C$ . В силу 3.0.1,  $[ab, c] = [a, c]^b[b, c] \in [A, C]^b[B, C] = [A, C][B, C]$ . Ранее было доказано, что  $C \leq N_G([A, C])$ .  $B \leq N_G([A, C])$  по условию. Следовательно,  $[B, C] \leq \langle B, C \rangle \leq N_G([A, C])$ . Таким образом,  $[B, C]$  нормализует  $[A, C]$ , следовательно  $[A, C], [B, C]$  перестановочны. Отсюда  $[A, C][B, C] \leq G$ . Таким образом,  $[ab, c] \in [A, C][B, C] \leq G$ . Следовательно,  $[AB, C] \leq [A, C][B, C]$ .

С другой стороны, очевидно,  $[A, C] \leq [AB, C]$  и  $[B, C] \leq [AB, C]$ , следовательно,  $[A, C][B, C] \leq [AB, C]$ . Таким образом,  $[AB, C] = [A, C][B, C]$ .

13. Это следует из 12). □

**Предложение 3.0.4.** Пусть  $A, B$  — нормальные подгруппы группы  $G$ . Если  $A \cap B = \{1\}$ , то  $[A, B] = \{1\}$ .

*Доказательство.* В силу 7)  $[A, B] \leq A \cap B = \{1\}$ , поэтому  $[A, B] = \{1\}$ . □

**Определение 3.0.5.** Пусть  $G$  — группа. Полагаем

$$1) G^1 := G, G^{i+1} := [G^i, G] \text{ для всех } i \in \mathbb{Z}_{>0}, G^\infty := \bigcap_{i \in \mathbb{Z}_{>0}} G^i;$$

$$2) G^{(0)} := G, G^{(i+1)} := [G^{(i)}, G^{(i)}] \text{ для всех } i \in \mathbb{Z}_{>0}, G^{(\infty)} := \bigcap_{i \in \mathbb{Z}_{\geq 0}} G^{(i)}.$$

Таким образом,

$$\begin{aligned} G^1 &= G, G^2 = [G, G], G^3 = [G, G, G], \dots, \\ G^{(0)} &= G, G^{(1)} = [G, G], G^{(2)} = [G^{(1)}, G^{(1)}], \dots \end{aligned}$$

**Определение 3.0.6.** Группа  $G$  называется совершенной, если  $G^{(1)} = G$ .

**Определение 3.0.7.** Группа  $G$  называется артиновой, если в ней не существует строго убывающей бесконечной последовательности подгрупп.

Например, любая конечная группа артинова.

**Теорема 3.0.5.** Пусть  $i \in \mathbb{N} \cup \{\infty\}$ , и либо для любой группы  $X$   $F_i(X) = X^i$ , либо для любой группы  $X$   $F_i(X) = X^{(i)}$ . Пусть  $G$  — группа,  $A, B \leq G$ ,  $\sigma : G \rightarrow H$  — произвольный морфизм. Тогда выполняются следующие утверждения.

- 1)  $F_i(G)$  — вполне характеристическая подгруппа  $G$ ;
- 2)  $F_i(A) \geq F_j(A)$  при  $i \leq j$ ;
- 3) если  $A \leq B$ , то  $F_i(A) \leq F_i(B)$ ;
- 4)  $(F_i(G))\sigma = F_i(G\sigma)$ , если  $i < \infty$ ;
- 5)  $(F_\infty(G))\sigma = F_\infty(G\sigma)$  если  $\sigma$  инъективно или  $G$  артинова. В любом случае  $(F_\infty(G))\sigma \leq F_\infty(G\sigma)$ ;
- 6) если  $G = AB$ , причем  $[A, B] = \{1\}$ , то  $F_i(G) = F_i(A)F_i(B)$ . Если  $G = A \times B$ , то  $F_i(G) = F_i(A) \times F_i(B)$  (о прямых произведениях см. 4.1).

*Доказательство.* Упражнение. □

В частности, при  $i < \infty$   $F_i$  можно рассматривать как функтор из категории групп в ту же категорию. То же верно и для  $F_\infty$ , если ограничиться артиновыми группами.

**Теорема 3.0.6.** Пусть  $A, B \leq G$ ,  $C = [A, B]$ ,  $G = \langle A, B \rangle$ . Тогда

- 1)  $A$  и  $B$  нормализуют  $C$ ;
- 2)  $C \trianglelefteq G$ ;
- 3)  $BC = \text{nc}_G(B)$ ;

$$4) G = AB[A, B];$$

$$5) G^{(1)} = A^{(1)}B^{(1)}[A, B].$$

*Доказательство.* 1. Покажем, что  $A$  нормализует  $C$ . Пусть  $x, a \in A, b \in B$ . Покажем, что  $[a, b]^x \in C$ . В силу тождества 4 теоремы 3.0.1,  $[ax, b] = [a, b]^x[x, b]$ , откуда  $[a, b]^x = [ax, b][x, b]^{-1} \in C$ . Так как  $C = \langle [a, b] : a \in A, b \in B \rangle$ , то, в силу 1.5.6,  $A$  нормализует  $C$ . Так как  $[A, B] = [B, A]$ , то  $B$  нормализует  $C$ .

2. Очевидно.

3. Покажем сначала, что  $BC \trianglelefteq G$ . Так как  $B$  нормализует  $B$  и  $C$ , то  $B$  нормализует  $BC$ . Покажем, что  $A$  нормализует  $BC$ . Так как  $C \trianglelefteq G$ , то достаточно доказать, что  $B^a \leq BC$  для всех  $a \in A$ . Пусть  $a \in A, b \in B$ . Тогда  $b^a = a^{-1}ba = a^{-1}bab^{-1}b = [a, b^{-1}]b \in CB = BC$ . Мы доказали, что  $BC \trianglelefteq G$ .

Пусть  $B \leq N \trianglelefteq G$ .  $C = [B, A] \leq [N, A] \leq N$ , следовательно,  $C \leq N$  и  $B \leq N$ , откуда  $BC \leq N$ . Таким образом,  $BC$  — наименьшая нормальная подгруппа  $G$ , содержащая  $B$ . В силу 1.5.7, отсюда следует, что  $BC = \text{nc}_G(B)$ .

4.  $A \leq AC \trianglelefteq G, B \leq BC \trianglelefteq G$ , следовательно,  $AC, BC$  — перестановочные подгруппы и их произведение — подгруппа  $G$ .  $A, B \leq ACBC$ . Так как  $C \trianglelefteq G$ , то  $ACBC = ABCC = ABC$ . Таким образом,  $A, B \leq ABC \leq G$ , следовательно,  $G = \langle A, B \rangle \leq ABC \leq G$ , то есть  $G = ABC$ .

5. Пусть  $- : G \rightarrow G/C$  — естественный морфизм. Тогда  $\bar{G} = \overline{\langle A, B \rangle} = \langle \bar{A}, \bar{B} \rangle$  и  $[\bar{A}, \bar{B}] = \overline{[A, B]} = \bar{C} = 1$ . Из 1.4.13 следует, что  $\bar{G} = \bar{A}\bar{B}$ . В силу 11)  $\bar{G}^{(1)} = \bar{A}^{(1)}\bar{B}^{(1)} = \overline{A^{(1)}B^{(1)}}$ . Отсюда  $G^{(1)}C = A^{(1)}B^{(1)}C$ . Очевидно,  $C \leq G^{(1)}$ , следовательно,  $G^{(1)} = A^{(1)}B^{(1)}C$ .  $\square$

**Предложение 3.0.7.** *Группа  $G$  абелева тогда и только тогда, когда  $G^{(1)} = \{1\}$ .*

*Доказательство.* Это очевидно ввиду 3.0.1.  $\square$

**Лемма 3.0.8.** *Если  $G^{(1)} \leq H \leq G$ , то  $H \trianglelefteq G$ .*

*Доказательство.* Пусть  $- : G \rightarrow G/G^{(1)}$  — естественный морфизм. Тогда  $\bar{H}$  — подгруппа абелевой группы  $\bar{G}$ , поэтому  $\bar{H} \trianglelefteq \bar{G}$ , и в силу 1.6.29  $H \trianglelefteq G$ .  $\square$

**Лемма 3.0.9.** *Пусть  $H \trianglelefteq G$ . Тогда  $G/H$  абелева если и только если  $G^{(1)} \leq H$ .*

*Доказательство.* Пусть  $H \trianglelefteq G$  и  $- : G \rightarrow G/H$  — естественный морфизм.  $\bar{G}$  абелева тогда и только тогда, когда  $(\bar{G})^{(1)} = \{1\}$ . Так как  $(\bar{G})^{(1)} = \overline{G^{(1)}}$ , в силу 3.0.5, то это равносильно  $G^{(1)} \leq H$ .  $\square$

**Теорема 3.0.10.** Пусть  $G, H$  — группы,  $X = \text{Mor}(G/G^{(1)}, H)$ ,  $Y$  — множество морфизмов  $\phi : G \rightarrow H$ , таких, что  $G\phi$  — абелева группа,  $\nu : G \rightarrow G/G^{(1)}$  — естественный эпиморфизм. Тогда существует и единственна биекция  $\sigma : X \rightarrow Y$ , такая, что  $\phi\sigma = \nu\phi$  для всех  $\phi \in X$ .

*Доказательство.* Единственность очевидна, проверим, что отображение  $\sigma$  биективно. Пусть  $\alpha : G \rightarrow H$  — морфизм с абелевым образом. Тогда  $\{1\} = (G\alpha)^{(1)} = G^{(1)}\alpha$ , следовательно,  $G^{(1)} \leq \ker \alpha$ . В силу 1.6.19 существует и единствен морфизм  $\phi : G/G^{(1)} \rightarrow H$ , такой, что  $\alpha = \nu\phi = \phi\sigma$ . Таким образом,  $\sigma$  сюръективно и инъективно.  $\square$

**Теорема 3.0.11.** Пусть  $i, j \in \mathbb{N}$ ,  $G$  — группа. Тогда  $[G^i, G^j] \leq G^{i+j}$ .

*Доказательство.* Предположим, что неравенство неверно, и  $j$  — минимальное возможное при этом условии. Очевидно,  $j > 1$ , следовательно,  $G^j = [G^{j-1}, G]$ .

$$[G, G^i, G^{j-1}] = [G^i, G, G^{j-1}] = [G^{i+1}, G^{j-1}] \leq G^{i+1+j-1} = G^{i+j}, \text{ так как } j-1 < j.$$

$$[G^i, G^{j-1}, G] \leq [G^{i+j-1}, G] = G^{i+j}, \text{ так как } j-1 < j.$$

Итак,  $[G, G^i, G^{j-1}] \leq G^{i+j}$  и  $[G^i, G^{j-1}, G] \leq G^{i+j}$ . В силу леммы о трех подгруппах  $[G^{j-1}, G, G^i] \leq G^{i+j}$ . Так как  $[G^{j-1}, G, G^i] = [G^j, G^i] = [G^i, G^j]$ , то  $[G^i, G^j] \leq G^{i+j}$  — противоречие.  $\square$

Интуитивно, коммутатор веса  $n$  — это выражение, составленное только из коммутаторов и зависящее от  $n$  аргументов. Например,  $a$  — коммутатор веса 1,  $[a, b]$  — коммутатор веса 2,  $[[a, b], c]$  и  $[a, [b, c]]$  — коммутаторы веса 3. Точное определение опирается на индукцию.

**Определение 3.0.8.** Любой элемент группы  $G$  называется коммутатором веса 1. Если  $a, b \in G$  — коммутаторы весов  $\alpha, \beta$  соответственно, то мы называем  $[a, b]$  коммутатором веса  $\alpha + \beta$ .

**Теорема 3.0.12.** Пусть  $G$  — группа,  $n \in \mathbb{Z}_{>0}$ . Любой коммутатор веса  $n$  копий  $G$  содержится в  $G^n$ .

*Доказательство.* Индукция по  $n$ . Если  $n = 1$ , то теорема верна, так как коммутатор веса 1 это сама группа  $G$ . Пусть  $n > 1$  и теорема верна для всех коммутаторов весов, меньших  $n$ . Пусть  $C$  — произвольный коммутатор веса  $n$ . Тогда  $C = [A, B]$ , где  $A, B$  — коммутаторы весов  $i, j \geq 1$ ,  $i + j = n$ . Тогда  $i, j < n$  и, по предположению индукции,  $A \leq G^i$ ,  $B \leq G^j$ . Следовательно,  $[A, B] \leq [G^i, G^j]$ . В силу теоремы 3.0.11,  $[G^i, G^j] \leq G^{i+j} = G^n$ . Теорема доказана.  $\square$

**Следствие 3.0.13.** Если  $G$  — группа и  $n \in \mathbb{N}$ , то  $G^{(n)} \leq G^{2^n}$ .

## Глава 4

# Основные теоретико-групповые конструкции

### 4.1 Прямые произведения

**Определение 4.1.1.** Пусть  $(G_i)_{i \in I}$  — произвольное непустое семейство групп,  $G = \prod_{i \in I} G_i$  — их декартово произведение. Для  $g = (g_i)_{i \in I}, h = (h_i)_{i \in I} \in G$  мы полагаем

$$gh = (g_i h_i)_{i \in I}.$$

**Теорема 4.1.1.** Декартово произведение групп является группой.

*Доказательство.* Упражнение. □

**Теорема 4.1.2.** Пусть имеется семейство морфизмов групп  $\phi_i : G \rightarrow H_i, i \in I$  ( $I$  — произвольное непустое множество). Определим отображение  $\phi : G \rightarrow \prod_{i \in I} H_i$  следующим образом:  $g\phi = (g\phi_i)_{i \in I}$  для всех  $g \in G$ . Тогда  $\phi$  — морфизм групп, причем  $\ker(\phi) = \bigcap_{i \in I} \ker(\phi_i)$ .

*Доказательство.* Упражнение. □

Используя данный факт и [1.6.22](#), приходим к следующей теореме.

**Теорема 4.1.3.** Пусть  $G$  — группа,  $(N_i)_{i \in I}$  — семейство нормальных подгрупп  $G$ . Тогда  $G / \bigcap_{i \in I} N_i$  вкладывается в  $\prod_{i \in I} (G / N_i)$ .

Семейство  $(g_i)_{i \in I}$  элементов  $g_i$  групп  $G_i$  назовем финитным, если множество

$$\{i \in I : g_i \neq 1\}$$

конечно. Множество всех финитных семейств из  $\prod_{i \in I} G_i$  обозначим  $\prod_{i \in I}^f G_i$  и назовем (внешним) прямым произведением семейства  $(G_i)_{i \in I}$ .

**Упражнение 4.1.4.** Докажите следующие утверждения:

- 1)  $\prod_{i \in I}^f G_i \leq \prod_{i \in I} G_i$ ;
- 2) если  $I$  конечно, то  $\prod_{i \in I}^f G_i = \prod_{i \in I} G_i$ .
- 3)  $\prod_{i \in I}^f G_i = \prod_{i \in I} G_i \Leftrightarrow$  множество  $\{i \in I : G_i \neq \{1\}\}$  конечно.

**Лемма 4.1.5.** Пусть  $I$  — непустое множество,  $(G_i)_{i \in I}$  — подгруппы  $G$ , причем  $[G_i, G_j] = \{1\}$  для  $i \neq j$ . Если  $(g_i)_{i \in I}, (h_i)_{i \in I} \in \prod_{i \in I}^f G_i$ , причем  $g = \prod_i g_i$ ,  $h = \prod_i h_i$ , то выполняются следующие утверждения:

- 1)  $gh = \prod_i g_i h_i$ ;
- 2)  $g^{-1} = \prod_i g_i^{-1}$ ;
- 3)  $g^k = \prod_i g_i^k \forall k \in \mathbb{Z}$ .

*Доказательство.* Упражнение. □

**Определение 4.1.2.** Говорят, что группа  $G$  является прямым произведением своих подгрупп  $(G_i)_{i \in I}$ , и пишут  $G = \times_{i \in I} G_i$ , если выполняются следующие условия:

- 1) для любого  $g \in G$  существует ровно одна строка  $(g_i)_{i \in I} \in \prod_{i \in I}^f G_i$  такая, что  $g = \prod_{i \in I} g_i$ ;
- 2) если  $i, j \in I$ ,  $i \neq j$ , то  $[G_i, G_j] = \{1\}$ .

Исходное определение прямого произведения подгрупп удобно слегка переформулировать.

**Пример 4.1.1.** Пусть  $G_1, G_2$  — подгруппы группы  $G$ . Тогда  $G = G_1 \times G_2$  если и только если  $[G_1, G_2] = \{1\}$ , и

$$(\forall g \in G)(\exists! g_1 \in G_1)(\exists! g_2 \in G_2) : g = g_1 g_2.$$

Аналогично, если  $n \in \mathbb{N}$ , и  $G_1, \dots, G_n \leq G$ , то  $G = G_1 \times \dots \times G_n$  тогда и только тогда, когда  $[G_i, G_j] = \{1\}$  при  $i \neq j$  и

$$(\forall g \in G)(\exists! g_1 \in G_1) \dots (\exists! g_n \in G_n) : g = g_1 \dots g_n.$$

**Предложение 4.1.6.** *Группа  $G$  является прямым произведением своих подгрупп  $(G_i)_{i \in I}$ , тогда и только тогда, когда выполняются следующие условия.*

- 1) *Для любого  $g \in G$  существует хотя бы одна строка  $(g_i)_{i \in I} \in \prod_{i \in I}^f G_i$  такая, что  $g = \prod_{i \in I} g_i$ .*
- 2) *Если  $i, j \in I$ ,  $i \neq j$ , то  $[G_i, G_j] = \{1\}$ .*
- 3) *Если  $(g_i)_{i \in I} \in \prod_{i \in I}^f G_i$  и  $\prod_{i \in I} g_i = 1$ , то все  $g_i = 1$ .*

*Доказательство.* Если  $G = \times_{i \in I} G_i$ , то, очевидно, все условия выполняются. Обратно, пусть выполнены условия 1, 2, 3. Нужно лишь доказать, что из  $\prod_i g_i = \prod_i g'_i$  и  $g_i, g'_i \in G_i$  для всех  $i$  следует, что  $g_i = g'_i$  для каждого  $i$ . Далее мы используем 4.1.5.

$$\prod_i g_i = \prod_i g'_i \Rightarrow 1 = \left(\prod_i g_i\right)^{-1} \prod_i g'_i = \left(\prod_i g_i^{-1}\right) \left(\prod_i g'_i\right) = \prod_i (g_i^{-1} g'_i).$$

Итак,  $\prod_i (g_i^{-1} g'_i) = 1$ . Из условия 3) следует, что  $(g_i^{-1} g'_i) = 1$  для всех  $i$ , поэтому  $g_i = g'_i$  для каждого  $i$ .  $\square$

Если  $(G_i)_{i \in I}$  — семейство попарно перестановочных подгрупп группы  $G$ , то  $\prod_{i \in I} G_i$  имеет очевидный смысл, когда  $I$  конечно. В общем случае мы определяем  $\prod_{i \in I} G_i$  как  $\cup_{S \in F} \prod_{i \in S} G_i$ , где  $F$  — множество всех конечных подмножеств  $I$ . Ясно, что эти два произведения совпадают, если  $I$  конечно, и  $\prod_{i \in I} G_i = \langle G_i : i \in I \rangle$ .

**Теорема 4.1.7.** *Группа  $G$  является прямым произведением своих подгрупп  $(G_i)_{i \in I}$  тогда и только тогда, когда выполняются следующие условия.*

- 1)  $G_i \trianglelefteq G$  для всех  $i$ ;
- 2)  $G = \prod_{i \in I} G_i$ ;
- 3)  $G_i \cap \prod_{j \neq i} G_j = \{1\}$  для всех  $i$ .

*Доказательство.* Пусть  $G = \times_{i \in I} G_i$ . Ясно, что  $G = \prod_{i \in I} G_i$ . Возьмем любой индекс  $i \in I$  и покажем, что  $G_i \trianglelefteq G$ . Очевидно,  $G_i \leq N_G(G_i)$ . Если  $I \ni j \neq i$ , то  $[G_i, G_j] = \{1\}$ , поэтому  $G_j \leq N_G(G_i)$ . Таким образом,  $G_j \leq N_G(G_i)$  для всех  $j$ , следовательно,  $G = \prod_{i \in I} G_i \leq N_G(G_i)$ , то есть  $G = N_G(G_i)$  и  $G_i \trianglelefteq G$ .

Теперь докажем, что  $G_i \cap \prod_{j \neq i} G_j = \{1\}$ . Рассмотрим произвольный элемент  $g \in G_i \cap \prod_{j \neq i} G_j$ . Обозначим  $g_i := g^{-1}$ . Так как  $g \in \prod_{j \neq i} G_j$ , то  $g = \prod_{j \neq i} g_j$  для некоторых  $g_j \in G_j$ ,  $j \neq i$ . В силу сказанного,  $g_i^{-1} = \prod_{j \neq i} g_j$ , откуда  $1 = g_i \prod_{j \neq i} g_j = \prod_j g_j$  (здесь

мы использовали перестановочность  $g_i$  и  $g_j$  при  $i \neq j$ ). С другой стороны,  $1 = \prod_{j \neq i} 1$ . В силу условия 1),  $g_j = 1$  для всех  $j$ , следовательно,  $g = 1$ . Мы доказали, что из  $G = \times_{i \in I} G_i$  следуют условия 1), 2), 3).

Обратно, пусть выполняются условия 1), 2), 3), и покажем, что  $G$  — прямое произведение подгрупп  $(G_i)_{i \in I}$ , для чего воспользуемся 4.1.6.

Пусть  $i, j \in I$ ,  $i \neq j$ . Убедимся, что  $[G_i, G_j] = \{1\}$ . Так как  $G_i \cap \prod_{k \neq i} G_k = \{1\}$ , и  $\prod_{k \neq i} G_k \geq G_j$ , то  $G_i \cap G_j = \{1\}$ . Кроме того,  $G_i, G_j \leq G$ , и в силу 3.0.4  $[G_i, G_j] = \{1\}$ .

Согласно 2) для любого  $g \in G$  найдется финитная строка  $(g_i)_{i \in I}$  такая, что  $g_i \in G_i$  для всех  $i \in I$ , и  $g = \prod_{i \in I} g_i$ . Остается проверить условие 3). Пусть  $\prod_i g_i = 1$ , где  $g_i \in G_i$  для всех  $i$ . Покажем, что  $g_i = 1$  для каждого  $i \in I$ . При  $i \in I$

$$G_i \ni g_i^{-1} = \prod_{j \neq i} g_j^{-1} \in \prod_{j \neq i} G_j,$$

и в силу 3)  $g_i^{-1} = 1$ , откуда  $g_i = 1$ . □

**Пример 4.1.2.** Пусть  $G_1, G_2$  — подгруппы группы  $G$ . Тогда  $G = G_1 \times G_2$  если и только если выполняются следующие условия:

- 1)  $G = G_1 G_2$ ;
- 2)  $G_1, G_2 \leq G$ ;
- 3)  $G_1 \cap G_2 = \{1\}$ .

Аналогично, если  $n \in \mathbb{N}$ , и  $G_1, \dots, G_n \leq G$ , то  $G = G_1 \times \dots \times G_n$  тогда и только тогда, когда

- 1)  $G = G_1 \dots G_n$ ;
- 2)  $G_i \leq G$  для всех  $i$ ;
- 3)  $G_i \cap \prod_{j \neq i} G_j = \{1\}$ .

**Теорема 4.1.8.** Пусть  $(G_i)_{i \in I}$  — семейство подгрупп группы  $G$ ,  $H = \prod_{i \in I}^f G_i$ ,  $\phi : H \rightarrow G$  — такое отображение, что  $(g_i)_{i \in I} \phi = \prod_{i \in I} g_i \ \forall (g_i)_{i \in I} \in H$ . Тогда  $G = \times_{i \in I} G_i$  если и только если  $\phi$  — изоморфизм.

*Доказательство.* Предположим, что  $G$  является прямым произведением подгрупп  $G_i$  и покажем, что  $\phi$  — изоморфизм. Пусть  $g = (g_i)_{i \in I} \in H$ ,  $h = (h_i)_{i \in I} \in H$ .

$$(gh)\phi = (g_i h_i)_{i \in I} \phi = \prod_{i \in I} (g_i h_i),$$

$$(g\phi)(h\phi) = \left( \prod_{i \in I} g_i \right) \left( \prod_{i \in I} h_i \right).$$

Из 4.1.5 следует, что  $(\prod_{i \in I} g_i)(\prod_{i \in I} h_i) = \prod_{i \in I} (g_i h_i)$ , то есть  $(gh)\phi = (g\phi)(h\phi)$ , следовательно,  $\phi$  — морфизм. В силу 1)  $\phi$  инъективно и сюръективно.

Обратно, пусть  $\phi$  — изоморфизм. Биъективность  $\phi$  означает, что для каждого  $g \in G$  имеется ровно одна строка  $(g_i)_{i \in I} \in H$  такая, что  $g = \prod_{i \in I} g_i$ . Пусть  $i, j \in I$ ,  $i \neq j$ , и  $a \in G_i$ ,  $b \in G_j$ . Покажем, что  $ab = ba$ . Для каждого  $k \in I$  и  $x \in G_k$  обозначим  $x^*$  строку из  $H$ ,  $k$ -й элемент которой равен  $x$ , а остальные элементы равны 1. Очевидно,  $x = x^* \phi$ .

$$ab = (a^* \phi)(b^* \phi) = (a^* b^*) \phi = (b^* a^*) \phi = (b^* \phi)(a^* \phi) = ba.$$

□

**Теорема 4.1.9.** Пусть  $(G_i)_{i \in I}$  — семейство групп,  $G = \prod_{i \in I}^f G_i$ , для произвольных  $i \in I$ ,  $a \in G_i$   $a^*$  — такое семейство  $(g_j)_{j \in I}$ , что  $g_i = a$ , и  $g_j = 1$  при  $j \in I \setminus \{i\}$ , а  $G_i^* = \{a^* : a \in G_i\}$ . Тогда  $G = \times_{i \in I} G_i^*$ .

*Доказательство.* Упражнение. □

**Теорема 4.1.10.** Пусть группа  $G$  является прямым произведением своих подгрупп  $(G_i)_{i \in I}$ , и каждая подгруппа  $G_i$  является прямым произведением своих подгрупп  $(G_{i,j})_{j \in J_i}$ . Тогда  $G$  — прямое произведение подгрупп  $G_{i,j}$ ,  $i \in I$ ,  $j \in J_i$ .

*Доказательство.* Упражнение. □

**Теорема 4.1.11.** Пусть группа  $G$  является прямым произведением своих подгрупп  $G_i$ ,  $i \in I$ , и  $H_i \trianglelefteq G_i$  для всех  $i \in I$ . Тогда  $(\times_{i \in I} G_i) / (\times_{i \in I} H_i) \simeq \times_{i \in I} (G_i / H_i)$ .

*Доказательство.* Упражнение. □

**Теорема 4.1.12.** Если группа  $G$  является произведением своих периодических нормальных подгрупп  $G_1, \dots, G_n$ ,  $n \in \mathbb{N}$  таких, что  $(G_i \pi) \cap (G_j \pi) = \emptyset$  для всех  $i \neq j$ , то  $G$  — прямое произведение данных подгрупп.

*Доказательство.* Допустим, что теорема неверна и  $n$  — минимальный контрпример. Очевидно,  $n > 1$ . Обозначим  $H = G_1 \dots G_{n-1}$ . Ясно, что  $H \trianglelefteq G$ . Так как подгруппы  $G_i$ ,  $i < n$ , нормальны в  $G$ , то они нормальны и в  $H$ . Так как  $(G_i\pi) \cap (G_j\pi) = \emptyset$  при  $i \neq j$ ,  $i, j < n$  и  $n-1 < n$ , то  $H = G_1 \times \dots \times G_{n-1}$ , поэтому  $H\pi = \cup_{i=1}^{n-1} G_i\pi$  и, следовательно,  $(H\pi) \cap (G_n\pi) = \emptyset$ . Отсюда  $H \cap G_n = \{1\}$ . Так как  $G = HG_n$  и  $H, G_n \trianglelefteq G$ , то  $G = H \times G_n$ . В силу 4.1.10  $G = G_1 \times \dots \times G_n$ .  $\square$

Если  $G = \times_{i \in I} G_i$ , то для каждого элемента  $g \in G$  существует единственная финитная строка  $(g_i)_{i \in I}$  такая, что  $g_i \in G_i$  для всех  $i$ , и  $g = \prod_{i \in I} g_i$ . Мы можем определить отображение  $\phi : G \rightarrow G_i$ , полагая  $g\phi = g_i$ . Это отображение называется проекцией  $G$  на  $G_i$ . Очевидно, каждая проекция является эпиморфизмом.

**Теорема 4.1.13.** Пусть группа  $G$  является прямым произведением некоторых своих периодических подгрупп  $G_1, \dots, G_n$  таких, что  $(G_i\pi) \cap (G_j\pi) = \emptyset$  для всех  $i \neq j$ . Если  $H \leq G$ , то  $H = \times_{i=1}^n H\phi_i$ , где  $\phi_i$  — проекция  $G \rightarrow G_i$ .

*Доказательство.* Сначала рассмотрим случай  $n = 2$ . Обозначим  $H_i := H\phi_i$ . Очевидно,  $H_1H_2 = H_1 \times H_2$  и  $H \leq H_1 \times H_2$ . Покажем, что  $H \geq H_1 \times H_2$ , для этого достаточно убедиться, что  $H_1, H_2 \leq H$ . Пусть  $a_1 \in H_1$ , тогда найдется  $a \in H$  такой, что  $a_1 = a\phi_1$ . Пусть  $a_2 := a\phi_2$ , тогда  $a = a_1a_2$  и  $a_1a_2 = a_2a_1$ . Обозначим  $n_2 = |a_2|$ , тогда  $a^{n_2} = a_1^{n_2}$ . Так как  $n_2\pi \subseteq G_2\pi$ ,  $|a_1|\pi \subseteq G_1\pi$  и  $(G_1\pi) \cap (G_2\pi) = \emptyset$ , то  $(n_2\pi) \cap (|a_1|\pi) = \emptyset$ , то есть  $(n_2, |a_1|) = 1$ . Отсюда

$$\langle a_1 \rangle = \langle a_1^{n_2} \rangle = \langle a^{n_2} \rangle \leq \langle a \rangle,$$

следовательно,  $a_1 \in \langle a_1 \rangle \leq \langle a \rangle \leq H$ . Таким образом,  $H_1 \leq H$ . Аналогично доказывается, что  $H_2 \leq H$ . Рассмотрим общий случай. Пусть теорема доказана для  $n = m > 2$ . Докажем ее при  $n = m + 1$ . Обозначим  $A = G_1$ ,  $B = G_2 \times \dots \times G_n$ , тогда  $G = A \times B$  и  $(A\pi) \cap (B\pi) = \emptyset$ . Как доказано ранее,  $H = V_1 \times V$  для некоторых  $V_1 \leq A$ ,  $V \leq B$ . По предположению индукции,  $V = V_2 \times \dots \times V_n$  для некоторых подгрупп  $V_i \leq G_i$ ,  $i \geq 2$ . Тогда  $H = V_1 \times V_2 \times \dots \times V_n$ . Так как  $V_i \leq G_i$  при  $1 \leq i \leq n$ , то  $V_i = H\phi_i$  для всех  $i$ .  $\square$

**Теорема 4.1.14.** Пусть группа  $G$  является прямым произведением конечного семейства  $(G_i)_{i \in I}$  своих подгрупп,  $H \trianglelefteq G$ .

- 1) Если  $H$  — совершенная группа, то  $H = \times_{i \in I} (H \cap G_i)$ .
- 2) Если все  $G_i$  — простые неабелевы группы, то  $H = \times_{j \in J} G_j$ , где

$$J = \{i \in I : H \cap G_i \neq \{1\}\}.$$

*Доказательство.* 1. Пусть  $H$  совершенна. Из нормальности подгрупп  $G_i, H$  и 12) следует, что

$$H = [H, H] \leq [G, H] = [\prod_{i \in I} G_i, H] = \prod_{i \in I} [G_i, H] \leq \prod_{i \in I} (G_i \cap H) \leq H,$$

откуда  $H = \prod_{i \in I} (H \cap G_i)$ . Так как  $G = \times_{i \in I} G_i$ , то  $H = \times_{i \in I} (H \cap G_i)$ .

2. Предположим, что все  $G_i$  — простые неабелевы группы. Сначала докажем, что  $H$  совершенна. Воспользуемся индукцией по числу  $\ell(G)$  композиционных факторов  $G$ . Очевидно,  $\ell(G) = |I|$ . Если  $\ell(G) = 1$ , то  $G$  — простая неабелева группа. Так как  $H \trianglelefteq G$ , то  $H = \{1\}$  или  $H = G$ , и в обоих случаях  $H$  совершенна. Пусть совершенность  $H$  доказана для  $\ell(G) = n$ , и допустим, что  $\ell(G) = n + 1$ . Если  $J = I$ , то (в силу 4.2.1)  $H$  содержит все  $G_i$ , и тогда  $H = G$  — совершенная группа. Пусть  $J \subset I$ , и  $i_0 \in I \setminus J$ . Тогда  $G_{i_0} \cap H = \{1\}$ . Рассмотрим естественный эпиморфизм  $- : G \rightarrow G/G_{i_0}$ . Очевидно,  $\bar{G} = \times_{i \neq i_0} \bar{G}_i$ , группы  $\bar{G}_i$  — простые неабелевы при  $i \neq i_0$ ,  $H \trianglelefteq G$  и  $\ell(\bar{G}) = n$ . По предположению индукции  $\bar{H}$  — совершенная группа, то есть  $\bar{H}^{(1)} = \bar{H}$ . Отсюда  $H^{(1)} = \bar{H}$ , и в силу 1.6.29  $H^{(1)}G_{i_0} = HG_{i_0}$ . Очевидно,  $HG_{i_0} = H \times G_{i_0}$ . Так как  $H \geq H^{(1)}$ , то  $H = H^{(1)}$  (использовали 1.4.15). В силу доказанного в (1)

$$H = \times_{i \in I} (H \cap G_i) = \times_{j \in J} G_j.$$

□

**Упражнение 4.1.15.** Докажите следующие утверждения:

- 1)  $\mathbb{R}^* = S^0 \times \mathbb{R}_{>0}$ , где  $S^0 = \{\pm 1\}$  — 0-мерная сфера;
- 2)  $\mathbb{C}^* = S^1 \times \mathbb{R}_{>0}$ , где  $S^1 = \{z \in \mathbb{C} : |z| = 1\}$  — окружность — 1-мерная сфера;
- 3)  $\mathbb{H}^* = S^3 \times \mathbb{R}_{>0}$ , где  $S^3 = \{q \in \mathbb{H} : |q| = 1\}$  — 3-мерная сфера.

**Упражнение 4.1.16.** Если векторное пространство  $V$  является прямой суммой своих подпространств  $V_i$ , то абелева группа  $V$  является прямой суммой своих подгрупп  $V_i$ .

**Упражнение 4.1.17.** Пусть  $X$  — множество,  $n \in \mathbb{N}$ ,  $(X_i)_{i=1}^n$  — разбиение  $X$ ,  $G$  — множество всех  $\phi \in \text{Sym}(X)$  таких, что  $X_i\phi = X_i$  для всех  $i$ ,  $G_i$  — множество всех  $\phi \in G$  таких, что  $\phi|_{X_j} = \text{id}_{X_j}$  для всех  $j \neq i$ . Тогда  $G = \times_{i=1}^n G_i$ .

**Упражнение 4.1.18.** Пусть  $D$  — тело,  $V$  — векторное пространство,  $n \in \mathbb{N}$ ,  $V = \oplus_{i=1}^n V_i$ ,  $G$  — множество всех  $\phi \in \text{GL}(V)$  таких, что  $V_i\phi = V_i$  для всех  $i$ ,  $G_i$  — множество всех  $\phi \in G$  таких, что  $\phi|_{V_j} = \text{id}_{V_j}$  для всех  $j \neq i$ . Тогда  $G = \times_{i=1}^n G_i$ .

**Упражнение 4.1.19.** Пусть  $G$  — группа обратимых диагональных матриц  $n \times n$  над кольцом  $R$ . Разложите  $G$  в прямое произведение подгрупп, изоморфных  $R^*$ .

**Упражнение 4.1.20.** Пусть  $G$  — произвольная группа,  $\iota : G \rightarrow G$ ,  $g\iota = g^{-1}$  для всех  $g \in G$ . Докажите следующие утверждения:

- 1) если  $G$  абелева, то  $\iota \in Z(\text{Aut}(G))$ ;
- 2) если  $G$  неабелева, то  $\text{Aut}^+(G) = \text{Aut}(G) \times \langle \iota \rangle$ , причем  $\langle \iota \rangle = \{\text{id}_G, \iota\}$ .

**Упражнение 4.1.21.** Обозначим  $\pi$  множество всех простых чисел. Как известно, для любого целого ненулевого числа  $z$  найдется единственный элемент  $u \in \{\pm 1\}$  и единственная строка  $\alpha \in \prod_{p \in \pi}^f \mathbb{Z}_{\geq 0}$  такие, что  $z = u \prod_{p \in \pi} p^{\alpha_p}$ . Используя данный факт, докажите, что  $\mathbb{Q}^* = \{\pm 1\} \times \prod_{p \in \pi} \langle p \rangle$ .

**Упражнение 4.1.22.** После ознакомления с понятием порядка элемента и циклическими группами докажите, что если  $G$  — группа всех комплексных корней из единицы, и для  $p \in \pi$   $G_p$  —  $p$ -группа Прюфера (см. 1.2.1), то  $G = \times_{p \in \pi} G_p$ .

**Упражнение 4.1.23.** Докажите, что в теоремах 4.1.12, 4.1.13 требование конечности семейства  $G_i$  несущественно.

## 4.2 Минимальные нормальные подгруппы

**Определение 4.2.1.** Подгруппа  $H$  группы  $G$  называется минимальной нормальной, если

- 1)  $H \neq \{1\}$ ;
- 2)  $H \trianglelefteq G$ ;
- 3) не существует  $A \trianglelefteq G$  такой, что  $\{1\} < A < H$ .

**Предложение 4.2.1.** Пусть  $G$  — группа,  $A \leq G$  — минимальная нормальная подгруппа.

- 1) Если  $B \trianglelefteq G$ , то либо  $A \cap B = \{1\}$ , либо  $A \leq B$ .
- 2) Если  $A$  — абелева,  $B \leq G$  и  $G = \langle A, B \rangle$ , то либо  $A \cap B = \{1\}$ , либо  $A \leq B$ .
- 3) Если  $\phi : G \rightarrow H$  — эпиморфизм, то  $A\phi = \{1\}$  или  $A\phi$  — минимальная нормальная подгруппа  $H$ .

*Доказательство.* 1. Так как  $A, B \trianglelefteq G$ , то  $A \cap B \trianglelefteq G$ . Кроме того,  $A \cap B \leq A$ . Так как  $A$  — минимальная нормальная подгруппа, то  $A \cap B = \{1\}$  или  $A \cap B = A$ . В последнем случае  $A \leq B$ .

2. Заметим, что  $A \cap B \trianglelefteq G$ . Действительно, так как  $A$  — абелева, то  $A \leq N_G(A \cap B)$ . Если  $b \in B$ , то  $(A \cap B)^b = A^b \cap B^b = A \cap B$ , поэтому  $B \leq N_G(A \cap B)$ . Из  $A, B \leq N_G(A \cap B)$  следует, что  $G = \langle A, B \rangle \leq N_G(A \cap B)$ , то есть  $A \cap B \trianglelefteq G$ . Так как  $A$  — минимальная нормальная подгруппа и  $A \cap B \leq A$ , то  $A \cap B = \{1\}$  или  $A \cap B = A$ . В последнем случае  $A \leq B$ .

3. Допустим, что  $B \trianglelefteq H$  и  $\{1\} < B < A\phi$ . Тогда найдется такой элемент  $a \in A \setminus \{1\}$ , что  $a\phi \in B$ . Следовательно,  $\{1\} < B\phi^{-1} \cap A \trianglelefteq G$ . Так как  $B\phi^{-1} \cap A \leq A$ , то либо  $B\phi^{-1} \cap A = \{1\}$ , что невозможно, либо  $B\phi^{-1} \cap A = A$ , и тогда  $A \leq B\phi^{-1}$ , что означает  $A\phi \leq B$ , откуда следует, что  $A\phi = B$  — противоречие.  $\square$

**Предложение 4.2.2.** Пусть  $G$  — группа,  $A \trianglelefteq G$ ,  $(M_i)_{i \in I}$  — конечное семейство минимальных нормальных подгрупп  $G$ ,  $M = \prod_{i \in I} M_i$ . Тогда выполняются следующие утверждения.

1) Найдется такое подмножество  $J \subseteq I$ , что  $AM = A \times (\times_{j \in J} M_j)$ .

2) Найдется такое подмножество  $J \subseteq I$ , что  $M = \times_{j \in J} M_j$ .

*Доказательство.* (1) Для подмножества  $S \subseteq I$  обозначим  $M_S := \prod_{i \in S} M_i$ . Пусть  $J$  — максимальное подмножество  $I$ , для которого  $AM_J = A \times (\times_{j \in J} M_j)$ . Допустим, что  $AM_J < AM$ . Тогда найдется такой элемент  $i \in I$ , что  $M_i \not\leq AM_J$ . Очевидно,  $i \notin J$ , и из минимальной нормальности  $M_i$  следует, что  $M_i \cap (AM_J) = \{1\}$ .

$$AM_{J \cup \{i\}} = AM_J M_i = (AM_J) \times M_i = A \times (\times_{j \in J \cup \{i\}} M_j)$$

— противоречие с максимальностью  $J$ .

Утверждение (2) следует из (1) при  $A = \{1\}$ .  $\square$

**Теорема 4.2.3.** Пусть  $M$  — минимальная нормальная подгруппа группы  $G$ ,  $N$  — минимальная нормальная подгруппа  $M$ , причем класс сопряженности  $\{N\}^G$  группы  $N$  конечен. Тогда  $N$  проста и найдутся  $N_1, \dots, N_k \in \{N\}^G$  такие, что  $M = N_1 \times \dots \times N_k$ .

*Доказательство.* Если  $g \in G$ , то из  $N \leq M \trianglelefteq G$  следует, что  $N^g \leq M^g = M$ , то есть все подгруппы  $G$ , сопряженные с  $N$ , содержатся в  $M$ . Отсюда следует, что  $\text{pc}_G(N) \leq M$ . Так как  $\{1\} < N \leq \text{pc}_G(N) \trianglelefteq G$  и  $\text{pc}_G(N) \leq M$ , то  $\text{pc}_G(N) = M$ . Если  $g \in G$ , то  $N^g$  — минимальная нормальная подгруппа  $G$ . В силу 4.2.2 найдутся

$N_1 = N, \dots, N_k \in \{N\}^G$  такие, что  $M = N_1 \times \dots \times N_k$ . Если  $\{1\} < H \trianglelefteq N$ , то  $H \trianglelefteq M$  и из минимальной нормальности  $N$  в  $M$  следует, что  $H = N$ , поэтому  $N$  — простая группа.  $\square$

**Теорема 4.2.4.** *Если  $M$  — абелева минимальная нормальная подгруппа конечной группы  $G$ , то найдется такое простое число  $p$ , что  $M$  является прямым произведением нескольких своих подгрупп, изоморфных  $C_p$ .*

*Доказательство.* Это следует из 4.2.3 и того, что абелева группа  $G$  проста тогда и только тогда, когда  $G$  — циклическая группа простого порядка.  $\square$

Другими словами, минимальная нормальная подгруппа конечной группы  $G$  — элементарная абелева.

**Теорема 4.2.5.** *Пусть  $M$  — неабелева минимальная нормальная подгруппа конечной группы  $G$ ,  $K$  — множество всех минимальных нормальных подгрупп  $M$ . Тогда выполняются следующие утверждения.*

- 1) Все элементы  $K$  — неабелевы простые группы и сопряжены в  $G$ .
- 2) Если  $N \trianglelefteq M$ ,  $K(N) := \{S \in K : S \leq N\}$ , то  $N = \times_{S \in K(N)} S$ .
- 3)  $M = \times_{S \in K} S$ .

*Доказательство.* Пусть  $A \in K$ . Очевидно, все сопряженные с  $A$  подгруппы  $G$  принадлежат  $K$ . В силу 4.2.3  $A$  проста и найдутся такие  $A_1 = A, \dots, A_n \in \{A\}^G$ , что  $M = \times_{i=1}^n A_i$ . Так как  $M$  неабелева, то не все  $A_i$  абелевы. Все  $A_i$  изоморфны, поэтому все они — неабелевы простые группы. Пусть  $N \trianglelefteq M$ . В силу 4.1.14  $N = \times_{j \in J} A_j$ , где  $J = \{i \in I : N \geq A_i\}$ . Если  $N \in K$ , то  $J \neq \emptyset$  и из  $N \geq A_i$  следует, что  $N = A_i$ , поэтому  $K \subseteq \{A_i\}_{i=1}^n$ . Так как любая неединичная нормальная подгруппа  $M$  содержит одну из подгрупп  $A_i$ , то  $K \supseteq \{A_i\}_{i=1}^n$ , поэтому  $K = \{A_i\}_{i=1}^n$ . Отсюда следует, что  $N = \times_{S \in K(N)} S$ . Наконец, полагая  $N = M$ , получаем, что  $M = \times_{S \in K} S$ .  $\square$

**Определение 4.2.2.** Цоколем  $\text{Soc}(G)$  конечной группы  $G$  называется подгруппа  $G$ , порожденная всеми минимальными нормальными подгруппами  $G$ .

**Предложение 4.2.6.** *Пусть  $G$  — конечная группа. Выполняются следующие утверждения:*

- 1) если  $G \neq \{1\}$ , то и  $\text{Soc}(G) \neq \{1\}$ .
- 2) если  $\{1\} < N \trianglelefteq G$ , то  $N \cap \text{Soc}(G) > \{1\}$ .

3)  $Soc(G)$  является прямым произведением некоторых минимальных нормальных подгрупп  $G$ .

4)  $Soc(G) \text{ char } G$ .

*Доказательство.* 1 следует из 2.

2. Если  $\{1\} < N \trianglelefteq G$ , то  $N$  содержит некоторую минимальную нормальную подгруппу  $H \leq G$ , и тогда  $H \leq N$  и  $H \leq Soc(G)$ , откуда следует, что  $\{1\} < H \leq N \cap Soc(G)$ .

3. Это следует из 4.2.2.

4. Это очевидно. □

В частности,  $Soc(G)$  является прямым произведением некоторых простых субнормальных подгрупп  $G$ .

**Теорема 4.2.7.** Пусть  $G$  — конечная группа,  $S \trianglelefteq G$ . Тогда  $Soc(G) \leq N_G(S)$ .

*Доказательство.* Предположим, что теорема неверна, и  $G$  — минимальный контрпример. Так как  $Soc(G) \not\leq N_G(S)$ , то найдется минимальная нормальная подгруппа  $M$  группы  $G$ , не нормализующая  $S$ . Очевидно,  $S \not\trianglelefteq G$ . Так как  $S \trianglelefteq G$ , то  $S \trianglelefteq N \triangleleft G$  для некоторой  $N$ . В силу 4.2.1  $M \cap N = \{1\}$  или  $M \leq N$ . Если  $M \cap N = \{1\}$ , то из 3.0.4 следует, что  $[M, N] = \{1\}$  и, в частности,  $M$  нормализует  $S$  — противоречие, следовательно,  $M \leq N$ . Так как  $|N| < |G|$  и  $S \trianglelefteq N$ , то  $Soc(N) \leq N_G(S)$ . Заметим, что  $Soc(N) \text{ char } N \triangleleft G$ , и в силу 1.7.9  $Soc(N) \triangleleft G$ . Кроме того, в силу 4.2.6  $M \cap Soc(N) \neq \{1\}$ . Так как  $M$  — минимальная нормальная подгруппа  $G$ , то по 4.2.1  $M \leq Soc(N)$ , поэтому  $M \leq N_G(S)$  — противоречие. □

## 4.3 Действия групп на группах

Пусть  $A, G$  — группы,  $G$  записывается аддитивно, и группа  $A$  действует на множестве  $G$ . Это действие называется действием на группе  $G$ , если  $(g_1 + g_2)a = g_1a + g_2a$  для всех  $g_1, g_2 \in G$ ,  $a \in A$ . Аналогично определяется левое действие  $A$  на группе  $G$ : левое действие группы  $A$  на множестве  $G$  называется левым действием на группе  $G$ , если  $a(g_1 + g_2) = ag_1 + ag_2$  для всех  $g_1, g_2 \in G$ ,  $a \in A$ . Если группа  $G$  записывается мультипликативно, то для действия  $A$  на группе  $G$  обычно используют экспоненциальную запись — для  $g \in G$ ,  $a \in A$  вместо  $ga$  пишут  $g^a$ . Если при этом  $A$  действует на группе  $G$  слева, то вместо  $ag$  пишут  ${}^a g$ . Таким образом, в данной ситуации (левое) действие  $A$  на множестве  $G$  называется (левым) действием на группе  $G$ , если для всех  $g_1, g_2 \in G$  и  $a \in A$  выполняется равенство  $(g_1 g_2)^a = g_1^a g_2^a$  (равенство

${}^a(g_1g_2) = ({}^ag_1)({}^ag_2)$ ). Заметим, что отражение левого (правого) действия группы  $A$  на группе  $G$  является правым (левым) действием на группе  $G$ . Кроме того, если  $A$  действует на группе  $G$  слева (справа), то ассоциированное правое (левое) действие на множестве  $G$  является одноименным действием на группе  $G$ .

Представлением группы  $A$  на группе  $G$  называется любой морфизм  $\rho : A \rightarrow \text{Aut}(G)$ . Очевидно, если  $A$  действует на группе  $G$ , то ассоциированное перестановочное представление  $A$  на множестве  $G$  является также представлением  $A$  на группе  $G$ . Обратно, если имеется представление  $A$  на группе  $G$ , то его можно рассматривать как перестановочное представление  $A$  на множестве  $G$ , и действие  $A$  на множестве  $G$ , ассоциированное с ним, является действием  $A$  на группе  $G$ . Применяя теорему 2.1.8, заключаем, что имеет место следующее утверждение.

**Теорема 4.3.1.** Пусть  $A, G$  — группы,  $X$  — множество действий  $A$  на группе  $G$ ,  $Y$  — множество всех представлений  $A$  на группе  $G$ , отображение  $\phi : X \rightarrow Y$  каждому действию  $A$  на группе  $G$  сопоставляет ассоциированное представление  $A$  на группе  $G$ . Тогда  $\phi$  — биекция.

Рассуждая аналогично и применяя 2.1.11, получаем похожую теорему для левых действий на группе.

**Теорема 4.3.2.** Пусть  $A, G$  — группы,  $X$  — множество левых действий  $A$  на группе  $G$ ,  $Y$  — множество всех представлений  $A^\circ$  на группе  $G$ , отображение  $\phi : X \rightarrow Y$  каждому левому действию  $A$  на группе  $G$  сопоставляет представление  $A^\circ$  на группе  $G$ , ассоциированное с его отражением. Тогда  $\phi$  — биекция.

Таким образом, понятие левого действия группы  $A$  на группе  $G$  равносильно понятию антиморфизма  $A \rightarrow \text{Aut}(G)$ .

**Пример 4.3.1.** Пусть  $G$  — группа,  $N \trianglelefteq G$ , тогда (в силу 1.5.1)  $G$  действует на группе  $N$  по правилу  $(x, g) \mapsto x^g$ , где  $x^g = g^{-1}xg$ . Мы называем это действие действием сопряжениями  $G$  на  $N$ . Ему соответствует ассоциированное представление  $G \rightarrow \text{Aut}(N)$ . Аналогично,  $G$  действует слева на группе  $N$  по правилу  $(g, x) \mapsto {}^gx$ , где  ${}^gx = gxg^{-1}$ .

Еще один пример появится в 4.5.2.

## 4.4 Полупрямые произведения

Нередко встречается ситуация, когда в группе  $G$  имеются подгруппы  $A \leq G$ ,  $B \trianglelefteq G$ , причем  $G = AB$  и  $A \cap B = \{1\}$ . Тогда говорят, что  $G$  — полупрямое произведение  $A$

и  $B$ , и пишут  $G = A \ltimes B$  или  $G = B \rtimes A$ . В силу 1.4.15 для каждого элемента  $g \in G$  существует единственная пара  $(a, b) \in A \times B$  такая, что  $g = ab$ . Допустим, мы имеем два элемента  $a_1b_1, a_2b_2$  группы  $G$ , где  $a_1, a_2 \in A, b_1, b_2 \in B$ . Тогда

$$(a_1b_1)(a_2b_2) = a_1a_2(a_2^{-1}b_1a_2)b_2 = a_1a_2b_1^{a_2}b_2.$$

Нами доказана

**Лемма 4.4.1.** Пусть  $G = A \ltimes B, a_1, a_2 \in A, b_1, b_2 \in B$ . Тогда  $(a_1b_1)(a_2b_2) = a_1a_2b_1^{a_2}b_2$ .

Теперь предположим, что  $A, B$  — произвольные группы, причем задано действие  $A$  на группе  $B$ , и  $\phi : A \rightarrow \text{Aut}(B)$  — ассоциированное представление. Составим декартово произведение  $G := A \times B$  и определим на нем операцию так, как подсказывает 4.4.1:

$$(a_1, b_1)(a_2, b_2) := (a_1a_2, b_1^{a_2}b_2)$$

для всех  $(a_1, b_1), (a_2, b_2) \in G$ . Полученный группоид обозначим  $A \ltimes_\phi B$  и назовем полупрямым произведением  $A$  на  $B$  относительно  $\phi$ .

**Теорема 4.4.2.** Пусть  $A, B$  — группы,  $A$  действует на группе  $B$ ,  $\phi : A \rightarrow \text{Aut}(B)$  — ассоциированное представление,  $G = A \ltimes_\phi B$ . Тогда  $G$  — группа.

*Доказательство.* Пусть  $a_i \in A, b_i \in B$  для всех  $i \in \{1, 2, 3\}$ .

$$(a_1, b_1)((a_2, b_2)(a_3, b_3)) = (a_1, b_1)(a_2a_3, b_2^{a_3}b_3) = (a_1a_2a_3, b_1^{a_2a_3}b_2^{a_3}b_3),$$

$$((a_1, b_1)(a_2, b_2))(a_3, b_3) = (a_1a_2, b_1^{a_2}b_2)(a_3, b_3) = (a_1a_2a_3, (b_1^{a_2}b_2)^{a_3}b_3) = (a_1a_2a_3, b_1^{a_2a_3}b_2^{a_3}b_3),$$

следовательно, операция умножения на  $G$  ассоциативна. Пусть  $a \in A, b \in B$ .

$$(1, 1)(a, b) = (1a, 1^ab) = (a, b), (a, b)(1, 1) = (a1, b^11) = (a, b),$$

поэтому  $(1, 1)$  — единица  $G$ .

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

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

Следовательно, каждый элемент  $(a, b) \in G$  имеет обратный элемент  $(a^{-1}, (b^{a^{-1}})^{-1})$ .  $\square$

Попутно мы доказали следующую теорему.

**Теорема 4.4.3.** Пусть  $A, B$  — группы,  $A$  действует на группе  $B$ ,  $\phi : A \rightarrow \text{Aut}(B)$  — ассоциированное представление,  $G = A \ltimes_{\phi} B$ ,  $(a, b) \in G$ . Тогда

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

Если  $A, B$  — конечные группы, то, очевидно,  $|A \ltimes_{\phi} B| = |A||B|$ .

**Теорема 4.4.4.** Для  $a \in A$ ,  $b \in B$  обозначим  $\bar{a} := (a, 1)$ ,  $\bar{b} := (1, b)$ . Тогда выполняются следующие утверждения.

- 1) Отображение  $a \mapsto \bar{a}$  является изоморфизмом  $A \rightarrow \bar{A}$ .
- 2) Отображение  $b \mapsto \bar{b}$  является изоморфизмом  $B \rightarrow \bar{B}$ .
- 3)  $G = \bar{A} \ltimes \bar{B}$ .
- 4)  $\bar{b}^{\bar{a}} = \bar{b}^a$  для всех  $a \in A$ ,  $b \in B$ .

*Доказательство.* Пусть  $a_1, a_2 \in A$ . Тогда

$$\bar{a}_1 \bar{a}_2 = (a_1, 1)(a_2, 1) = (a_1 a_2, 1^{a_2} 1) = (a_1 a_2, 1),$$

следовательно, отображение  $a \mapsto \bar{a}$  является морфизмом  $A \rightarrow \bar{A}$ . Очевидно, это изоморфизм. Теперь пусть  $b_1, b_2 \in B$ .

$$\bar{b}_1 \bar{b}_2 = (1, b_1)(1, b_2) = (1 \cdot 1, b_1^1 b_2) = (1, b_1 b_2),$$

следовательно, отображение  $b \mapsto \bar{b}$  является морфизмом  $B \rightarrow \bar{B}$ . Очевидно, это изоморфизм. Если  $a \in A$ ,  $b \in B$ , то

$$\bar{a} \bar{b} = (a, 1)(1, b) = (a 1, 1^1 b) = (a, b).$$

Отсюда следует, что  $G = \bar{A} \bar{B}$ . Очевидно,  $\bar{A} \cap \bar{B} = \{1\}$ . Так как  $G = \bar{A} \bar{B}$ , то  $\bar{B} \trianglelefteq G$  тогда и только тогда, когда  $\bar{A} \leq N_G(\bar{B})$ . Достаточно установить тождество  $\bar{b}^{\bar{a}} = \bar{b}^a$  для всех  $a \in A$ ,  $b \in B$ . Пусть  $a \in A$ ,  $b \in B$ .

$$\bar{b}^{\bar{a}} = \bar{a}^{-1} \bar{b} \bar{a} = (a, 1)^{-1} (1, b) (a, 1) = (a^{-1}, 1) (1, b) (a, 1) = (a^{-1}, b) (a, 1) = (1, b^a) = \bar{b}^a.$$

□

Таким образом, мы можем считать, что  $\bar{a} = a$ ,  $\bar{b} = b$  для всех  $a \in A$ ,  $b \in B$ , и тогда  $\bar{A} = A$ ,  $\bar{B} = B$ ,  $G = A \ltimes B$ , причем  $b^a = b(a\phi)$  для всех  $a \in A$ ,  $b \in B$ , то есть действие  $A$  на  $B$  становится в  $A \ltimes_\phi B$  действием сопряжениями  $A$  на  $B$ . Если ясно, какое действие  $A$  на  $B$  подразумевается, то в формуле  $A \ltimes_\phi B$  можно не писать  $\phi$ . В силу высказанных замечаний, так как  $(a, b) = (a, 1)(1, b)$ , то при желании вместо  $(a, b)$  можно писать  $ab$ .

**Пример 4.4.1.** Пусть  $G = \{\pm 1\}$ , тогда  $G$  — группа по умножению. Возьмем любую абелеву группу  $A$  и будем записывать ее аддитивно. Очевидно,  $G$  действует на  $A$  по правилу  $(a, \epsilon) \mapsto a\epsilon$ , поэтому мы можем сконструировать соответствующее полупрямое произведение  $G \ltimes A$ . Данная группа называется обобщенной диэдральной группой с ядром  $A$ , и мы обозначим ее  $D(A)$ . Из сказанного ранее следует, что  $D(A) = \{\pm 1\} \times A$ , причем

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

для всех  $(a_1, b_1), (a_2, b_2) \in D(A)$ . Если  $(a, b) \in D(A)$ , то в силу 4.4.3

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

В теории конечных групп наиболее часто встречается случай, когда  $A$  — конечная циклическая группа порядка  $n$  (то есть  $G \simeq C_n$ ), тогда группа  $D(A)$  обозначается  $D_{2n}$  и называется диэдральной группой порядка  $2n$ . Иногда эта же группа обозначается  $D_n$ , но мы не будем так делать.

**Пример 4.4.2.** Пусть  $n \in \mathbb{N}$ ,  $n \geq 4$ ,  $R = \mathbb{Z}_{2^{n-1}}$ ,  $- : \mathbb{Z} \rightarrow R$  — естественный эпиморфизм. Обозначим  $i = 2^{n-2} - 1$ . Заметим, что  $2(n-2) \geq n-1$  и

$$i \not\equiv 1 \pmod{2^{n-1}},$$

$$i^2 = (2^{n-2} - 1)^2 = 2^{2(n-2)} + 2^{n-1} + 1 \equiv 1 \pmod{2^{n-1}},$$

поэтому  $\bar{i}^2 = \bar{1}$ , откуда  $\bar{i} \in R^*$ . Так как  $\bar{i} \neq 1$ , то  $|\bar{i}| = 2$ , то есть  $\bar{i}$  — инволюция в  $R^*$ . Обозначим  $G = \langle \bar{i} \rangle = \{\bar{1}, \bar{i}\}$ . Группа  $G$  действует на группе  $R^+$  по правилу  $(r, g) \mapsto rg$ , следовательно, мы имеем право образовать полупрямое произведение  $G \ltimes R^+$ . Эта группа называется полудиэдральной, или квазидиэдральной группой порядка  $2^n$ , и мы обозначим ее  $SD_{2^n}$ . Таким образом,

$$SD_{2^n} = \{\bar{1}, \bar{i}\} \times R,$$

причем пары  $(a_1, b_1), (a_2, b_2) \in SD_{2^n}$  умножаются по правилу

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

Как и в предыдущем примере, если  $(a, b) \in SD_{2^n}$ , то

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

Допустим, что  $G$  — множество, и для некоторых пар  $(a, b) \in G^2$  определено произведение  $ab \in G$ , тогда назовем  $G$  частичным группоидом. Например, если  $G$  — группа и  $A, B \leq G$ , то  $A \cup B$  — частичный группоид, если считать определенными лишь произведения, в которых оба сомножителя принадлежат одной из подгрупп  $A, B$ . Если  $G, H$  — частичные группоиды, то морфизмом  $G \rightarrow H$  назовем любое отображение  $\sigma : G \rightarrow H$ , такое, что если  $a, b \in G$ , и их произведение определено, то определено и произведение  $(a\sigma)(b\sigma)$ , и  $(ab)\sigma = (a\sigma)(b\sigma)$ .

**Предложение 4.4.5.** Пусть  $G = A \ltimes B$ ,  $H$  — группа, и  $- : A \cup B \rightarrow H$  — произвольный морфизм частичных группоидов. Данный морфизм имеет не более одного продолжения до морфизма  $G \rightarrow H$ . Продолжение существует тогда и только тогда, когда  $\overline{b^a} = \overline{b^a}$  для всех  $a \in A$ ,  $b \in B$ , и в этом случае  $\overline{ab} = \overline{a}\overline{b}$  для всех  $a \in A$ ,  $b \in B$ .

*Доказательство.* Если продолжение существует, то оно единственно, так как  $G = \langle A, B \rangle$ , и в силу 1.6.18, кроме того, в силу морфности продолжения,  $\overline{ab} = \overline{a}\overline{b}$  и  $\overline{b^a} = \overline{b^a}$  для всех  $a \in A$ ,  $b \in B$ . Обратно, пусть  $\overline{b^a} = \overline{b^a}$  для всех  $a \in A$ ,  $b \in B$ . Определим отображение  $- : G \rightarrow H$  следующим образом:  $\overline{ab} := \overline{a}\overline{b}$  для произвольных  $a \in A$ ,  $b \in B$ . Покажем, что мы получили морфизм. Пусть  $a_i \in A$ ,  $b_i \in B$ ,  $i \in \{1, 2\}$ .

$$\overline{(a_1 b_1)(a_2 b_2)} = \overline{a_1 a_2 b_1^{a_2} b_2} = \overline{a_1 a_2 b_1^{a_2} b_2} = \overline{a_1} \overline{a_2} \overline{b_1^{a_2}} \overline{b_2} = (\overline{a_1} \overline{b_1}) (\overline{a_2} \overline{b_2}) = (\overline{a_1 b_1}) (\overline{a_2 b_2}).$$

□

Предположим, что группа  $B$  действует слева на группе  $A$ , и  $\phi : B^\circ \rightarrow \text{Aut}(A)$  — ассоциированное представление. Тогда удобно определить  $A \rtimes_\phi B$  как множество  $G := A \times B$ , наделенное операцией умножения  $G^2 \rightarrow G$ , такой, что для всех  $a_1, a_2 \in A$ ,  $b_1, b_2 \in B$

$$(a_1, b_1)(a_2, b_2) = (a_1({}^{b_1}a_2), b_1 b_2).$$

Обозначим  $\iota : B \rightarrow B$ ,  $b \mapsto b^{-1}$ . Убедимся в том заранее очевидном факте, что отображение  $\sigma : A \rtimes_\phi B \rightarrow B \ltimes_{\iota\phi} A$ ,  $(a, b) \mapsto (b^{-1}, a^{-1})^{-1}$  является изоморфизмом.

$$\begin{aligned} ((a_1, b_1)(a_2, b_2))\sigma &= (a_1({}^{b_1}a_2), b_1 b_2)\sigma = ((b_1 b_2)^{-1}, (a_1({}^{b_1}a_2))^{-1})^{-1} = (b_2^{-1} b_1^{-1}, {}^{b_1}(a_2^{-1}) a_1^{-1})^{-1} = \\ &= ((b_2^{-1} b_1^{-1})^{-1}, ({}^{b_1}(a_2^{-1}) a_1^{-1})^{-1}) = (b_1 b_2, (a_1({}^{b_1}a_2))^{b_1 b_2}) = (b_1 b_2, (a_1(a_2^{b_1^{-1}}))^{b_1 b_2}) = \end{aligned}$$

$$\begin{aligned}
&= (b_1 b_2, a_1^{b_1 b_2} a_2^{b_2}), \\
&= ((a_1, b_1)\sigma)((a_2, b_2)\sigma) = (b_1^{-1}, a_1^{-1})^{-1}(b_2^{-1}, a_2^{-1})^{-1} = (b_1, ((a_1^{-1})^{b_1})^{-1})(b_2, ((a_2^{-1})^{b_2})^{-1}) = \\
&= (b_1, a_1^{b_1})(b_2, a_2^{b_2}) = (b_1 b_2, (a_1^{b_1})^{b_2} a_2^{b_2}) = (b_1 b_2, a_1^{b_1 b_2} a_2^{b_2}).
\end{aligned}$$

Таким образом,  $((a_1, b_1)(a_2, b_2))\sigma = ((a_1, b_1)\sigma)((a_2, b_2)\sigma)$ , то есть  $\sigma$  — морфизм. Биективность  $\sigma$  очевидна. Итак,  $\sigma : A \rtimes_\phi B \rightarrow B \ltimes_\phi A$  — изоморфизм, поэтому все сказанное о  $B \ltimes_\phi A$  очевидным образом переносится на  $A \rtimes_\phi B$ . Например,  $G$  — группа, и если для  $a \in A$ ,  $b \in B$  обозначить  $\bar{a} := (a, 1)$ ,  $\bar{b} := (1, b)$ , то имеет место

**Теорема 4.4.6.**

- 1) *Отображение  $a \mapsto \bar{a}$  является изоморфизмом  $A \rightarrow \bar{A}$ .*
- 2) *Отображение  $b \mapsto \bar{b}$  является изоморфизмом  $B \rightarrow \bar{B}$ .*
- 3)  $G = \bar{A} \rtimes \bar{B}$ .
- 4)  ${}^{\bar{b}}\bar{a} = \bar{{}^b a}$  для всех  $a \in A$ ,  $b \in B$ .

Поэтому можно считать, что  $\bar{a} = a$ ,  $\bar{b} = b$  для всех  $a \in A$ ,  $b \in B$ , и тогда  $\bar{A} = A$ ,  $\bar{B} = B$ ,  $G = A \rtimes B$ , причем  ${}^b a = a(b\phi)$  для всех  $a \in A$ ,  $b \in B$ , то есть левое действие  $B$  на группе  $A$  становится в  $A \rtimes_\phi B$  левым действием сопряжениями  $B$  на  $A$ .

Очевидно, всегда можно ограничиться лишь полупрямыми произведениями типа  $A \rtimes B$ , но иногда это приводит к усложнениям формул, как в случае со сплетением, к которому мы сейчас переходим.

## 4.5 Сплетения

Пусть  $G, H$  — группы,  $\rho : G \rightarrow \text{Sym}(\Omega)$  — перестановочное представление группы  $G$  на множестве  $\Omega$ .

**Лемма 4.5.1.** *Пусть  $\Psi, \Omega$  — множества,  $H$  — группа, записываемая аддитивно,  $\alpha \in \text{Mor}(\Psi, \Omega)$ ,  $\beta, \gamma \in \text{Mor}(\Omega, H)$ . Тогда  $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$  или, в мультипликативной записи,  $\alpha(\beta\gamma) = (\alpha\beta)(\alpha\gamma)$ .*

*Доказательство.* Пусть  $x \in \Psi$ .

$$x(\alpha(\beta + \gamma)) = (x\alpha)(\beta + \gamma) = (x\alpha\beta) + (x\alpha\gamma) = x(\alpha\beta + \alpha\gamma).$$

□

**Лемма 4.5.2.** *стандартное левое действие группы  $G$  на множестве  $B := \text{Mor}(\Omega, H)$  (см. 2.1.14) является также левым действием группы  $G$  на группе  $B$ .*

*Доказательство.* Пусть  $g \in G$ ,  $b_1, b_2 \in B$ . Тогда

$$g(b_1 + b_2) = (g\rho)(b_1 + b_2) = (g\rho)b_1 + (g\rho)b_2 = gb_1 + gb_2.$$

□

Итак,  $G$  действует на группе  $B$  (слева), следовательно, мы можем составить полупрямое произведение  $W := B \rtimes_\phi G$ , где  $\phi$  — представление группы  $G$  на группе  $B$ , ассоциированное со стандартным действием  $G$  на  $B$ . Группа  $W$  называется сплетением  $H$  и  $G$  относительно перестановочного представления  $\rho : G \rightarrow \text{Sym}(\Omega)$ , и оно обозначается  $H \wr_\rho G$ , или  $H \wr_\rho G$ , или просто  $H \wr G$ , если ясно, как действует  $G$  на  $\Omega$ . Нередко обозначают  $W$  через  $H \wr_\Omega G$ . Группа  $B$  называется базовой группой сплетения  $W$ , или просто базой. Если  $\Omega = G$  и  $G$  действует на  $\Omega$  правыми умножениями (см. 2.1.4), то  $W$  называется стандартным сплетением  $H$  и  $G$ . По умолчанию  $H \wr G$  означает стандартное сплетение. По определению,  $W$  состоит из всевозможных пар вида  $((h_\omega)_{\omega \in \Omega}, g)$ , где  $(h_\omega)_{\omega \in \Omega} \in H^\Omega$  — произвольное семейство элементов из  $H$ , снабженных индексами из  $\Omega$ ,  $g \in G$ . Найдем формулу для умножения в  $W$ . Пусть  $(h_\omega)_{\omega \in \Omega} \in B$ ,  $h' = (h'_\omega)_{\omega \in \Omega} \in B$ ,  $g, g' \in G$ .

$${}^g(h'_\omega)_{\omega \in \Omega} = {}^g h' = g\rho h' = (h'_{\omega(g\rho)})_{\omega \in \Omega} = (h'_{\omega g})_{\omega \in \Omega},$$

$$\begin{aligned} ((h_\omega)_{\omega \in \Omega}, g)((h'_\omega)_{\omega \in \Omega}, g') &= ((h_\omega)_{\omega \in \Omega}({}^g(h'_\omega)_{\omega \in \Omega}), gg') = ((h_\omega)_{\omega \in \Omega}(h'_{\omega g})_{\omega \in \Omega}, gg') = \\ &= ((h_\omega h'_{\omega g})_{\omega \in \Omega}, gg'). \end{aligned}$$

Окончательно,

$$((h_\omega)_{\omega \in \Omega}, g)((h'_\omega)_{\omega \in \Omega}, g') = ((h_\omega h'_{\omega g})_{\omega \in \Omega}, gg'), \quad (4.5.1)$$

$${}^g(h_\omega)_{\omega \in \Omega} = (h_{\omega g})_{\omega \in \Omega}. \quad (4.5.2)$$

Далее мы установим связь между сплетениями и матрицами. Пусть  $R$  — коммутативное кольцо,  $RH$  — групповая  $R$ -алгебра группы  $H$ .

Пусть  $T$  — любое кольцо (например  $RH$ ) и  $M$  — свободный левый  $T$ -модуль с базисом  $e = (e_\omega)_{\omega \in \Omega}$ . Если  $a = (a_\omega)_{\omega \in \Omega} \in T^\Omega$ , то диагональную матрицу  $\text{diag}(a) \in M_\Omega(T)$ , в которой на месте  $(\omega, \omega)$  стоит  $a_\omega$ , будем обозначать  $[a]$ , или  $[a_\omega]_{\omega \in \Omega}$ . Если  $\sigma \in \text{Sym}(\Omega)$ , то  $[\sigma] := (\delta_{\omega', \omega\sigma})_{\omega, \omega' \in \Omega}$  — матрица перестановки  $\sigma$  ( $\delta$  — символ Кронекера). Если  $S \subseteq T^\Omega$  или  $S \subseteq \text{Sym}(\Omega)$ , то  $[S] := \{[s] : s \in S\}$ .

**Пример 4.5.1.** Пусть  $n \in \mathbb{N}$ ,  $\Omega = \{1, \dots, n\}$ . Тогда мы считаем, что  $T^\Omega = T^n$ . Пусть  $a = (a_1, \dots, a_n) \in T^n$ . Договоримся, что неописанные элементы матрицы — нули. Тогда

$$[a] = \begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{pmatrix}.$$

Пусть  $n = 5$ ,  $\sigma \in S_5$ ,

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}.$$

Тогда

$$[\sigma] = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

**Лемма 4.5.3.** Пусть  $(a_\omega)_{\omega \in \Omega}, (b_\omega)_{\omega \in \Omega} \in T^\Omega$ . Тогда

$$[a_\omega]_{\omega \in \Omega} [b_\omega]_{\omega \in \Omega} = [a_\omega b_\omega]_{\omega \in \Omega}.$$

В частности,  $[a_\omega]_{\omega \in \Omega} \in \text{GL}_\Omega(T)$  тогда и только тогда, когда все  $a_\omega \in T^*$ . Если  $D \leq (T^*)^\Omega$ , то  $[D] \leq \text{GL}_\Omega(T)$ .

*Доказательство.* Это очевидно. □

В частности,  $[B] \leq \text{GL}_\Omega(RH)$ .

**Пример 4.5.2.** Пусть  $n \in \mathbb{N}$ ,  $a_1, \dots, a_n, b_1, \dots, b_n \in T$ . Тогда

$$[a_1, \dots, a_n][b_1, \dots, b_n] = [a_1 b_1, \dots, a_n b_n],$$

или, в развернутой записи

$$\begin{pmatrix} a_1 & & \\ & \ddots & \\ & & a_n \end{pmatrix} \begin{pmatrix} b_1 & & \\ & \ddots & \\ & & b_n \end{pmatrix} = \begin{pmatrix} a_1 b_1 & & \\ & \ddots & \\ & & a_n b_n \end{pmatrix}.$$

**Лемма 4.5.4.** Если  $a, b \in \text{Sym}(\Omega)$ , то  $[ab] = [a][b]$ . В частности, если  $S \leq \text{Sym}(\Omega)$ , то  $[S] \leq \text{GL}_\Omega(T)$ .

*Доказательство.* Пусть  $\alpha = [a]^e$ ,  $\beta = [b]^e$ ,  $\gamma = [ab]^e$ . Для любого  $\omega \in \Omega$

$$e_\omega \alpha \beta = e_{\omega a} \beta = e_{\omega ab} = e_\omega \gamma,$$

поэтому  $\alpha \beta = \gamma$ , следовательно,  $\alpha_e \beta_e = \gamma_e$ , откуда  $[a][b] = [ab]$ . Остальное следует из 2.1.4.  $\square$

**Лемма 4.5.5.** Пусть  $\phi \in \text{Sym}(\Omega)$ ,  $(h_\omega)_{\omega \in \Omega} \in T^\Omega$ . Тогда

$$[\phi][h_\omega]_{\omega \in \Omega}[\phi]^{-1} = [h_{\omega\phi}]_{\omega \in \Omega}.$$

В частности,  $[\text{Sym}(\Omega)]$  нормализует  $[B]$ .

*Доказательство.* Пусть  $\omega \in \Omega$ .

$$\begin{aligned} e_\omega([\phi][h_\omega]_{\omega \in \Omega}[\phi]^{-1})^e &= e_\omega[\phi]^e[h_\omega]_{\omega \in \Omega}^e[\phi^{-1}]^e = e_{\omega\phi}[h_\omega]_{\omega \in \Omega}^e[\phi^{-1}]^e = \\ &= h_{\omega\phi}e_{\omega\phi}[\phi^{-1}]^e = h_{\omega\phi}e_\omega = e_\omega[h_{\omega\phi}]_{\omega \in \Omega}^e, \end{aligned}$$

следовательно, доказываемое равенство верно.  $\square$

**Пример 4.5.3.** Пусть  $\sigma$  — перестановка из 4.5.1,  $h = (h_i)_{i=1}^5 \in T^5$ . Тогда

$$[\sigma][h][\sigma]^{-1} = [h_{1\sigma}, h_{2\sigma}, h_{3\sigma}, h_{4\sigma}, h_{5\sigma}] = [h_2, h_3, h_1, h_5, h_4].$$

Если  $S \leq \text{Sym}(\Omega)$ , то  $[S]$  нормализует  $[B]$ . Кроме того,  $[B] \cap [S] = \{1\}$ , поэтому  $[B][S] \leq \text{GL}_\Omega(RH)$ , причем  $[B][S] = [B] \rtimes [S]$ .

**Определение 4.5.1.** Матрицу  $M \in M_\Omega(T)$  назовем мономиальной над множеством  $E \subseteq T$ , если в ней можно так отметить элементы, что в каждой строке и любом столбце матрицы  $M$  имеется ровно один отмеченный элемент, все неотмеченные элементы — нулевые, а все отмеченные элементы принадлежат  $E$ . Схемой мономиальной матрицы  $M$  над  $E$  назовем такое отображение  $\sigma : \Omega \rightarrow \Omega$ , что для  $i \in \Omega$   $i\sigma$  — номер отмеченного элемента  $i$ -й строки. Из условий, определяющих разметку, следует, что  $\sigma \in \text{Sym}(\Omega)$ . Диагональю мономиальной матрицы  $M \in M_\Omega(T)$  назовем матрицу  $[M_{i,i\sigma}]_{i \in \Omega}$ . Очевидно, диагональ не зависит от выбора разметки.

**Пример 4.5.4.** Пусть  $\Omega = \{1, \dots, 5\}$ ,  $a_1, \dots, a_5 \in T$ ,  $a = (a_1, \dots, a_5)$ ,

$$h = \begin{pmatrix} 0 & a_1 & 0 & 0 & 0 \\ 0 & 0 & a_2 & 0 & 0 \\ a_3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & a_4 \\ 0 & 0 & 0 & a_5 & 0 \end{pmatrix},$$

тогда  $h$  — мономиальная матрица над множеством  $\{a_1, \dots, a_5\}$  со схемой

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$$

и диагональю

$$[a] = \begin{pmatrix} a_1 & 0 & 0 & 0 & 0 \\ 0 & a_2 & 0 & 0 & 0 \\ 0 & 0 & a_3 & 0 & 0 \\ 0 & 0 & 0 & a_4 & 0 \\ 0 & 0 & 0 & 0 & a_5 \end{pmatrix}.$$

**Лемма 4.5.6.** Пусть  $(h_{\omega, \omega'})_{(\omega, \omega') \in \Omega^2} \in M_\Omega(T)$  — мономиальная матрица со схемой  $\sigma \in \text{Sym}(\Omega)$ . Тогда

$$(h_{\omega, \omega'})_{(\omega, \omega') \in \Omega^2} = [h_{\omega, \omega\sigma}]_{\omega \in \Omega} [\sigma]. \quad (4.5.3)$$

Таким образом, любая мономиальная матрица  $h$  является произведением своей диагонали и матрицы схемы  $h$ .

*Доказательство.* Пусть  $\omega \in \Omega$ .

$$e_\omega((h_{\omega, \omega'})_{(\omega, \omega') \in \Omega^2})^e = h_{\omega, \omega\sigma} e_{\omega\sigma},$$

$$e_\omega([h_{\omega, \omega\sigma}]_{\omega \in \Omega} [\sigma])^e = e_\omega([h_{\omega, \omega\sigma}]_{\omega \in \Omega})^e [\sigma]^e = h_{\omega, \omega\sigma} e_\omega [\sigma]^e = h_{\omega, \omega\sigma} e_{\omega\sigma},$$

поэтому равенство 4.5.3 верно.  $\square$

Из 4.5.6 и 1.1.11 следует, что мономиальная матрица  $M \in M_\Omega(T)$  обратима тогда и только тогда, когда в каждой ее строке и столбце имеется ровно один ненулевой элемент, и этот элемент обратим.

**Пример 4.5.5.** В силу 4.5.6 получаем разложение матрицы  $h$  из 4.5.4 в произведение ее диагонали  $[a_1, \dots, a_5]$  и матрицы  $[\sigma]$  ее схемы  $\sigma$ :

$$h = [a][\sigma] = \begin{pmatrix} a_1 & 0 & 0 & 0 & 0 \\ 0 & a_2 & 0 & 0 & 0 \\ 0 & 0 & a_3 & 0 & 0 \\ 0 & 0 & 0 & a_4 & 0 \\ 0 & 0 & 0 & 0 & a_5 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

**Определение 4.5.2.** Пусть  $S \leq \text{Sym}(\Omega)$ . Группу  $[H^\Omega] \rtimes [S]$  обозначим  $\text{Mon}(H, S)$ .

В силу 4.5.6  $\text{Mon}(H, S)$  состоит из всех мономиальных матриц  $M \in M_\Omega(RH)$  над  $H$  со схемами из  $S$ .

**Следствие 4.5.7.** *Отображение  $- : B \cup G \rightarrow \text{GL}_\Omega(RH)$ , такое, что  $\bar{b} = [b]$ ,  $\bar{g} = [g\rho]$  для всех  $b \in B$ ,  $g \in G$ , является частичным морфизмом, причем  $\bar{g}\bar{b} = \overline{gb}$  для всех  $b \in B$ ,  $g \in G$ .*

*Доказательство.* Это следует из 4.5.3, 4.5.4, 4.5.5.  $\square$

**Теорема 4.5.8.** *Существует и единственен эпиморфизм  $\phi : H \wr_\rho G \rightarrow \text{Mon}(H, [G\rho])$ , такой, что  $b\phi = [b]$ ,  $g\phi = [g\rho]$  для всех  $b \in B$ ,  $g \in G$ . Его ядро равно  $\ker(\rho)$ . Если  $G$  точно действует на  $\Omega$ , то  $\phi$  — изоморфизм.*

*Доказательство.* Первое утверждение следует из 4.5.7 и 4.4.5. Пусть  $b \in B$ ,  $g \in G$ . Воспользуемся соглашением о черте для  $\phi$ .

$$\bar{bg} = 1 \Leftrightarrow 1 = \bar{b}\bar{g} \Leftrightarrow 1 = [b][g\rho] \Leftrightarrow 1 = [b] = [g\rho] \Leftrightarrow b = 1 \text{ и } g\rho = 1.$$

$\square$

Найденный нами эпиморфизм  $\phi : H \wr_\rho G \rightarrow \text{Mon}(H, [G\rho])$  будем называть естественным, или каноническим. Обратный морфизм, если он существует, тоже назовем каноническим.

**Пример 4.5.6.** Пусть  $\Omega = \{1, \dots, 5\}$ ,  $S_5$  обычным образом действует на  $\Omega$ ,  $a = (a_1, \dots, a_5) \in B = H^5$ ,  $\sigma$  — перестановка из 4.5.1. Тогда  $(a, \sigma) \in H \wr S_5$ , и в силу 4.5.5

$$(a, \sigma)\phi = (a\sigma)\phi = (a\phi)(\sigma\phi) = [a][\sigma] = \begin{pmatrix} 0 & a_1 & 0 & 0 & 0 \\ 0 & 0 & a_2 & 0 & 0 \\ a_3 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & a_4 \\ 0 & 0 & 0 & a_5 & 0 \end{pmatrix}.$$

**Лемма 4.5.9.** Пусть  $e = (e_i)_{i \in I}$  — левая трансверсаль группы  $G$  по ее подгруппе  $H$ . Тогда  $e$  — базис левого  $RH$ -модуля  $RG$ .

*Доказательство.* Обозначим  $L$   $RH$ -линейную оболочку семейства  $e$ . Пусть  $g \in G$ , тогда найдется единственная пара  $(i, h) \in I \times H$  такая, что  $g = he_i$ . В частности,  $g \in L$ , следовательно,  $G \subseteq L$ . Отсюда следует, что  $L$  содержит  $R$ -линейную оболочку

$G$ , то есть  $L \supseteq RG$ , поэтому  $L = RG$ . Пусть  $(\alpha_i)_{i \in I}$  — такое семейство элементов  $RH$ , что  $\sum_{i \in I} \alpha_i e_i = 0$ . Покажем, что все  $\alpha_i = 0$ . Пусть  $\alpha_i = \sum_{h \in H} \alpha_{i,h} h$ ,  $\alpha_{i,h} \in R$ . Тогда

$$0 = \sum_{i \in I} \alpha_i e_i = \sum_{i \in I} \left( \sum_{h \in H} \alpha_{i,h} h \right) e_i = \sum_{(i,h) \in I \times H} \alpha_{i,h} h e_i = 0.$$

Если  $(i, h)$  пробегает без повторений  $I \times H$ , то  $h e_i$  без повторений пробегает  $G$ . В силу линейной независимости  $G$  над  $R$  и последнего равенства все коэффициенты  $\alpha_{i,h}$  нулевые, следовательно, все  $\alpha_i = 0$ .  $\square$

**Лемма 4.5.10.** *Для каждого элемента  $g \in G$  определим отображение  $\phi_g : RG \rightarrow RG$ ,  $x \mapsto xg$ . Пусть  $S$  — любое подкольцо в  $RG$ , тогда можно рассматривать  $RG$  как левый  $S$ -модуль  $M$ . Выполняются следующие утверждения.*

- 1)  $\phi_g \in \text{GL}_S(M)$  для всех  $g \in G$ .
- 2) Отображение  $G \ni g \mapsto \phi_g \in \text{GL}_S(M)$  является морфизмом  $G \rightarrow \text{GL}_S(M)$ .
- 3)  $\phi : G \rightarrow \text{GL}_S(M)$  — вложение.

*Доказательство.* Очевидно,  $\phi_g \in \text{End}_S(M)$  для любого  $g \in G$  (здесь используется то, что  $M$  — именно левый  $S$ -модуль, правый модуль бы не подошел, а  $\phi_g$  действует на  $M$  умножением на  $g$  именно справа). Заметим, что  $\phi_{ab} = \phi_a \phi_b$  для всех  $a, b \in G$  и  $1\phi = \text{id}_M$ , поэтому из 2.1.4 следует, что  $\phi_g \in \text{GL}_S(M)$ . Следовательно, мы получили морфизм  $\phi : G \rightarrow \text{GL}_S(M)$ ,  $g\phi = \phi_g$  для всех  $g \in G$ . Ясно, что  $\ker(\phi) = \{1\}$ , поэтому в силу 1.6.16  $\phi$  — вложение.  $\square$

В силу 2.1.5 если  $H \leq G$ , то  $G$  действует на  $\Omega$  по правилу  $(Ha, g) \mapsto Hag$ .

**Теорема 4.5.11.** *Пусть  $H \leq G$ ,  $\Omega = G/H$ ,  $\rho : G \rightarrow \text{Sym}(\Omega)$  — представление, ассоциированное с действием  $G$  на  $\Omega$  умножениями. Тогда  $G$  вкладывается в  $\text{Mon}(H, G\rho)$ .*

*Доказательство.* Обозначим  $\rho : G \rightarrow \text{Sym}(\Omega)$  — перестановочное представление, ассоциированное со стандартным действием  $G$  на  $\Omega$  (см. 2.1.5),  $W := \text{Mon}(H, G\rho)$ ,  $M$  — кольцо  $RG$ , рассматриваемое как левый  $RH$ -модуль. Далее мы воспользуемся обозначениями из 4.5.10, а в качестве  $S$  возьмем  $RH$ . Выберем произвольную левую трансверсаль  $G$  по  $H$   $e = (e_\omega)_{\omega \in \Omega}$ ,  $e_\omega \in \omega$  для всех  $\omega \in \Omega$ , и докажем, что  $(G\phi)_e \leq W$ . Пусть  $\omega \in \Omega$ . Так как  $e_\omega \in \omega$ , то  $e_\omega g \in \omega g \ni e_{\omega g}$ , поэтому  $e_\omega g = h_{\omega, \omega g} e_{\omega g}$  для некоторого  $h_{\omega, \omega g} \in H$ . Отсюда следует, что  $(g\phi)_e = (h_{\omega, \omega'})_{(\omega, \omega') \in \Omega^2}$ , где  $h_{\omega, \omega'} = h_{\omega, \omega g} \delta_{\omega g, \omega'}$ . В силу 4.5.6  $(g\phi)_e = [h_{\omega, \omega g}]_{\omega \in \Omega} [g\rho] \in W$ . Итак, мы нашли вложение  $\chi : G \rightarrow W$ ,  $g\chi = (g\phi)_e \in W$ .  $\square$

Построенное вложение  $\chi : G \rightarrow \mathrm{GL}_\Omega(RH)$  назовем стандартным, соответствующим левой трансверсали  $e$   $G$  по  $H$ . Это вложение неоднократно послужит нам. С помощью него мы получим теоремы 4.5.12, 4.5.13 о вложении расширения группы в сплетение, оно позволит нам построить индуцированные представления и характеры. Кроме того, с помощью данного вложения можно определить морфизм перемещения.

Вернемся к ситуации 4.5.11. В силу 2.5.8 ядро  $N$  действия  $G$  на  $\Omega$  совпадает с  $\mathrm{Core}_G(H)$ , и если  $\sim : G \rightarrow G/N$  — естественный морфизм, то  $\tilde{G}$  точно действует на  $\Omega$  умножениями по правилу  $(\omega, \tilde{g}) \mapsto \omega g$  для всех  $\omega \in \Omega$ ,  $g \in G$ . Если  $\rho : G \rightarrow \mathrm{Sym}(\Omega)$ ,  $\tilde{\rho} : \tilde{G} \rightarrow \mathrm{Sym}(\Omega)$  — соответствующие ассоциированные представления, то  $G\rho = \tilde{G}\tilde{\rho}$ .

**Теорема 4.5.12.** Пусть  $H \leq G$ ,  $N := \mathrm{Core}_G(H)$ ,  $\Omega = G/H$ . Тогда  $G$  вкладывается в  $H \wr_{\tilde{\rho}} (G/N)$ , где  $\tilde{\rho} : G/N \rightarrow \mathrm{Sym}(\Omega)$  — представление, ассоциированное со стандартным действием  $G/N$  на  $\Omega$  (см. 2.1.5).

*Доказательство.* В терминах 4.5.11 мы нашли вложение  $\chi : G \rightarrow W$ ,  $W = \mathrm{Mon}(H, G\rho)$ . Так как  $G\rho = \tilde{G}\tilde{\rho}$ , то  $W = \mathrm{Mon}(H, \tilde{G}\tilde{\rho})$ . В силу 4.5.8 имеется канонический изоморфизм  $\theta : W \rightarrow H \wr_{\tilde{\rho}} (G/N)$ , поэтому  $\chi\theta : G \rightarrow H \wr_{\tilde{\rho}} (G/N)$  — вложение.  $\square$

Построенное вложение  $\psi : G \rightarrow H \wr_{\tilde{\rho}} (G/N)$  действует так:

$$g\psi = g(\chi\theta) = (g\chi)\theta = ([h_{\omega, \omega g}]_{\omega \in \Omega} [g\rho])\theta = ([h_{\omega, \omega g}]_{\omega \in \Omega} [\tilde{g}\tilde{\rho}])\theta = ((h_{\omega, \omega g})_{\omega \in \Omega}, \tilde{g}),$$

где  $\sim : G \rightarrow G/N$  — естественный морфизм. Окончательно,

$$g\psi = ((h_{\omega, \omega g})_{\omega \in \Omega}, \tilde{g}).$$

Назовем это вложение каноническим, соответствующим трансверсали  $e$ . Если в 4.5.12  $H \trianglelefteq G$ , то получим

**Следствие 4.5.13.** Пусть  $H \trianglelefteq G$ . Тогда  $G$  вкладывается в стандартное сплетение  $H \wr (G/H)$ .

Посмотрим, что произойдет, если в 4.5.11 изменить трансверсаль. Выберем любую левую трансверсаль  $e' = (e'_\omega)_{\omega \in \Omega}$   $G$  по  $H$  и обозначим  $\chi'$  соответствующее вложение  $G \rightarrow W$ . Тогда  $e, e'$  — базисы  $M$ , поэтому они связаны матрицей перехода  $T := T_{e' \leftarrow e}$ . В силу известной формулы,

$$g\chi' = (g\phi)_{e'} = T(g\phi)_e T^{-1} = T(g\chi)T^{-1}.$$

Итак,

$$g\chi' = T(g\chi)T^{-1}$$

для всех  $g \in G$ . Используя канонический изоморфизм

$$\theta : \text{Mon}(H, G\rho) \rightarrow H \wr_{\bar{\rho}} (G/N),$$

из 4.5.8 получаем, что для всех  $g \in G$

$$g\psi' = g(\chi'\theta) = (g\chi')\theta = (T(g\chi)T^{-1})\theta = (T\theta)(g\chi\theta)(T\theta)^{-1} = (T\theta)(g\psi)(T\theta)^{-1}.$$

В итоге получаем соотношение

$$g\psi' = (T\theta)(g\psi)(T\theta)^{-1}.$$

Далее мы обобщим конструкцию сплетения, построив некоторые его подгруппы. Предположим, что имеется некоторая группа  $G_0$ , действующая на множестве  $\Omega$  и на группе  $H$ , причем  $(\omega g_0)g = (\omega g)g_0$  для всех  $g_0 \in G_0$ ,  $g \in G$  и  $\omega \in \Omega$ . Обозначим  $B_0 := \text{Mor}_{G_0}(\Omega, H)$ .

**Лемма 4.5.14.**  $B_0 \leq B$ .

*Доказательство.* Пусть  $\omega \in \Omega$ ,  $g_0 \in G_0$ , тогда  $(\omega g_0)1_B = 1$ , и  $(\omega 1_B)^{g_0} = 1^{g_0} = 1$ , поэтому  $1_B \in B_0$ . Пусть  $b_1, b_2 \in B_0$ .

$$(\omega g_0)(b_1 + b_2) = (\omega g_0)(b_1) + (\omega g_0)(b_2) = (\omega b_1)^{g_0} + (\omega b_2)^{g_0} = (\omega b_1 + \omega b_2)^{g_0} = (\omega(b_1 + b_2))^{g_0},$$

следовательно,  $B_0$  замкнуто по сложению. Пусть  $b \in B_0$ .

$$(\omega g_0)(-b) = -((\omega g_0)b) = -((\omega b)^{g_0}) = (-(\omega b))^{g_0} = (\omega(-b))^{g_0}.$$

Следовательно,  $B_0$  замкнуто по обращению. □

**Лемма 4.5.15.**  $B_0$   $G$ -инвариантна.

*Доказательство.* Пусть  $\omega \in \Omega$ ,  $g_0 \in G_0$ ,  $g \in G$ ,  $b \in B_0$ . Тогда

$$\begin{aligned} (\omega g_0)(gb) &= (\omega g_0)(g\rho b) = ((\omega g_0)(g\rho))b = ((\omega g_0)g)b = ((\omega g)g_0)b = ((\omega g)b)^{g_0} = \\ &= ((\omega(g\rho))b)^{g_0} = ((\omega(gb))^{g_0}). \end{aligned}$$

□

Таким образом,  $G$  действует слева на  $B_0$ , поэтому мы можем составить полупрямое произведение  $B_0 \rtimes G$  относительно этого действия. Полученная группа называется скрученным сплетением  $H$  и  $G$  и обозначается  $H \text{ twr } G$ . Очевидно,  $H \text{ twr } G \leq H \wr G$ , поэтому умножение в  $H \text{ twr } G$  задается тем же законом 4.5.1. Если  $G_0$  тривиально действует на  $\Omega$  и  $H$ , то  $B_0 = B$  и тогда  $H \text{ twr } G = H \wr G$ .

## 4.6 Действия сплетений на множествах

Здесь мы построим два важных действия сплетения на множествах.

**Определение 4.6.1.** Пусть  $\Omega$  — множество,  $G_1 \leq G_2$  — группы. Действия  $\cdot_i : \Omega \times G_i \rightarrow \Omega$ ,  $i \in \{1, 2\}$  назовем согласованными, если для любых  $\omega \in \Omega$ ,  $g_1 \in G_1$  выполняется равенство  $\omega \cdot_1 g_1 = \omega \cdot_2 g_1$ .

Обозначим  $\rho_i$  перестановочное представление  $G_i \rightarrow \text{Sym}(\Omega)$ , ассоциированное с действием  $\cdot_i$ ,  $i \in \{1, 2\}$ . Очевидно, согласованность действий  $\cdot_i$  равносильна следующему условию:  $g_1 \rho_1 = g_1 \rho_2$  для всех  $g_1 \in G_1$ . Это равносильно совпадению отображений  $\rho_i$  на  $G_1$ .

**Определение 4.6.2.** Пусть  $\Omega$  — множество,  $G_0$  — группа,  $G_1, G_2 \leq G_0$ ,  $G_0 = \langle G_1, G_2 \rangle$ . Действия  $\cdot_i : \Omega \times G_i \rightarrow \Omega$ ,  $i \in \{1, 2\}$  назовем согласованными, если существует действие  $\cdot_0 : \Omega \times G_0 \rightarrow \Omega$ , согласованное с действиями  $\cdot_i$ ,  $i \in \{1, 2\}$ .

Пусть  $\rho_i : G_i \rightarrow \text{Sym}(\Omega_i)$  — перестановочное представление, ассоциированное с действием  $\cdot_i$ ,  $i \in \{0, 1, 2\}$ . Тогда ясно, что действие  $\cdot_0$  согласовано с действиями  $\cdot_i$ ,  $i \in \{1, 2\}$  тогда и только тогда, когда  $\rho_0, \rho_i$  совпадают на  $G_i$  для всех  $i \in \{1, 2\}$ . Отсюда и из 1.6.18 следует, что если существует действие  $G_0$  на  $\Omega$ , согласованное с действиями групп  $G_i$ ,  $i \in \{1, 2\}$ , то только одно.

**Лемма 4.6.1.** Пусть  $\Omega$  — множество,  $G$  — группа,  $A, B \leq G$ ,  $G = A \rtimes B$ ,  $A, B$  действуют на  $\Omega$ . Равносильны следующие условия.

- 1) Действия  $A, B$  на  $\Omega$  согласованы.
- 2)  $((\omega b)a)b^{-1} = \omega(ba)$  для любых  $\omega \in \Omega$ ,  $a \in A$ ,  $b \in B$ .

*Доказательство.* Применим соглашение о черте к перестановочным представлениям  $\alpha : A \rightarrow \text{Sym}(\Omega)$ ,  $\beta : B \rightarrow \text{Sym}(\Omega)$ , ассоциированным с соответствующими действиями  $A, B$  на  $\Omega$ . В силу 4.4.5 действие  $G$  на  $\Omega$ , согласованное с действиями  $A, B$  существует тогда и только тогда, когда  $\bar{b}a = \overline{ba}$ . Последнее равенство эквивалентно второму условию доказываемого утверждения.  $\square$

Далее в настоящем разделе  $\Gamma, \Delta$  — множества,  $A, B$  — группы, действующие соответственно на  $\Gamma, \Delta$ . Мы построим некоторые стандартные действия сплетения  $W := A \wr_{\Delta} B$  на множествах  $\Gamma \times \Delta$  и  $\Gamma^{\Delta}$ .

### 4.6.1 Действие сплетения на парах

Обозначим  $\Omega := \Gamma \times \Delta$  и построим действие  $W$  на  $\Omega$ . Вспомним, что  $W = A^\Delta \rtimes B$  и что имеются естественные действия  $A^\Delta, B$  на  $\Omega$ , описанные в 2.1.19 и 2.1.20 соответственно. Чтобы доказать согласованность этих действий, в силу 4.6.1 достаточно убедиться, что

$$(((\gamma, \delta)b)(a_\delta)_{\delta \in \Delta})b^{-1} = (\gamma, \delta)(^b(a_\delta)_{\delta \in \Delta}) \quad (4.6.1)$$

для всех  $(\gamma, \delta) \in \Omega$ ,  $(a_\delta)_{\delta \in \Delta} \in A^\Delta$ ,  $b \in B$ .

$$(((\gamma, \delta)b)(a_\delta)_{\delta \in \Delta})b^{-1} = ((\gamma, \delta b)(a_\delta)_{\delta \in \Delta})b^{-1} = (\gamma a_{\delta b}, \delta b)b^{-1} = (\gamma a_{\delta b}, \delta),$$

Согласно 4.5.2

$$(\gamma, \delta)(^b(a_\delta)_{\delta \in \Delta}) = (\gamma, \delta)(a_{\delta b})_{\delta \in \Delta} = (\gamma a_{\delta b}, \delta).$$

Итак, действия  $A^\Delta, B$  на  $\Omega$  согласованы, поэтому существует и единственно действие  $W$  на  $\Omega$ , согласованное с данными действиями. Легко видеть, что для любых  $(\gamma, \delta) \in \Omega$ ,  $(a_\delta)_{\delta \in \Delta} \in A^\Delta$ ,  $b \in B$

$$(\gamma, \delta)((a_\delta)_{\delta \in \Delta}b) = ((\gamma, \delta)(a_\delta)_{\delta \in \Delta})b = (\gamma a_\delta, \delta)b = (\gamma a_\delta, \delta b).$$

Итак,  $W$  действует на  $\Omega$  по правилу

$$(\gamma, \delta)((a_\delta)_{\delta \in \Delta}b) = (\gamma a_\delta, \delta b).$$

Мы доказали следующую теорему.

**Теорема 4.6.2.** Пусть  $\Gamma, \Delta$  — множества,  $A, B$  — группы, действующие соответственно на  $\Gamma, \Delta$ ,  $W := A \wr_\Delta B$ . Тогда существует и единственно действие группы  $W$  на множестве  $\Gamma \times \Delta$ , такое, что для всех  $(\gamma, \delta) \in \Gamma \times \Delta$ ,  $(a_\delta)_{\delta \in \Delta} \in A^\Delta$ ,  $b \in B$  выполняется равенство

$$(\gamma, \delta)((a_\delta)_{\delta \in \Delta}b) = (\gamma a_\delta, \delta b).$$

### 4.6.2 Действие сплетения на функциях

Обозначим  $\Omega := \Gamma^\Delta$  и построим действие  $W$  на  $\Omega$ . Мы имеем стандартное действие  $A^\Delta$  на  $\Omega$ , описанное в 2.1.18. Кроме того,  $B$  действует на  $\Omega$  слева, как указано в 2.1.14. Используя 2.1.1, мы можем преобразовать это левое действие в правое действие так:

$$(\gamma_\delta)_{\delta \in \Delta}b := b^{-1}(\gamma_\delta)_{\delta \in \Delta} = (\gamma_{\delta b^{-1}})_{\delta \in \Delta}$$

для всех  $(\gamma_\delta)_{\delta \in \Delta} \in \Omega$ ,  $b \in B$ . Окончательно,

$$(\gamma_\delta)_{\delta \in \Delta} b = (\gamma_{\delta b^{-1}})_{\delta \in \Delta}.$$

Итак,  $A^\Delta$  и  $B$  действуют на  $\Omega$ , и  $W = A^\Delta \rtimes B$ , поэтому в силу 4.6.1 достаточно убедиться, что

$$(((\gamma_\delta)_{\delta \in \Delta} b)(a_\delta)_{\delta \in \Delta})b^{-1} = (\gamma_\delta)_{\delta \in \Delta}(^b(a_\delta)_{\delta \in \Delta}) \quad (4.6.2)$$

для всех  $(\gamma_\delta)_{\delta \in \Delta} \in \Omega$ ,  $(a_\delta)_{\delta \in \Delta} \in A^\Delta$ ,  $b \in B$ .

$$(((\gamma_\delta)_{\delta \in \Delta} b)(a_\delta)_{\delta \in \Delta})b^{-1} = ((\gamma_{\delta b^{-1}})_{\delta \in \Delta}(a_\delta)_{\delta \in \Delta})b^{-1} = (\gamma_{\delta b^{-1}}a_\delta)_{\delta \in \Delta}b^{-1} = (\gamma_\delta a_{\delta b})_{\delta \in \Delta}.$$

В силу 4.5.2

$$(\gamma_\delta)_{\delta \in \Delta}(^b(a_\delta)_{\delta \in \Delta}) = (\gamma_\delta)_{\delta \in \Delta}(a_{\delta b})_{\delta \in \Delta} = (\gamma_\delta a_{\delta b})_{\delta \in \Delta}.$$

Мы доказали равенство 4.6.2, поэтому существует и единственно действие  $W$  на  $\Gamma^\Delta$ , согласованное с действиями  $A, B$  на  $\Gamma, \Delta$  соответственно. Очевидно, для всех  $(\gamma_\delta)_{\delta \in \Delta} \in \Omega$ ,  $(a_\delta)_{\delta \in \Delta} \in A^\Delta$ ,  $b \in B$  это действие работает так:

$$(\gamma_\delta)_{\delta \in \Delta}((a_\delta)_{\delta \in \Delta}b) = ((\gamma_\delta)_{\delta \in \Delta}(a_\delta)_{\delta \in \Delta})b = (\gamma_\delta a_\delta)_{\delta \in \Delta}b = (\gamma_{\delta b^{-1}}a_{\delta b^{-1}})_{\delta \in \Delta}.$$

Окончательно,

$$(\gamma_\delta)_{\delta \in \Delta}((a_\delta)_{\delta \in \Delta}b) = (\gamma_{\delta b^{-1}}a_{\delta b^{-1}})_{\delta \in \Delta}.$$

Мы доказали следующую теорему.

**Теорема 4.6.3.** Пусть  $\Gamma, \Delta$  — множества,  $A, B$  — группы, действующие соответственно на  $\Gamma, \Delta$ ,  $W := A \wr_\Delta B$ . Тогда существует и единственно действие группы  $W$  на множестве  $\Gamma^\Delta$ , такое, что для всех  $(\gamma_\delta)_{\delta \in \Delta} \in \Gamma^\Delta$ ,  $(a_\delta)_{\delta \in \Delta} \in A^\Delta$ ,  $b \in B$  выполняется равенство

$$(\gamma_\delta)_{\delta \in \Delta}((a_\delta)_{\delta \in \Delta}b) = (\gamma_{\delta b^{-1}}a_{\delta b^{-1}})_{\delta \in \Delta}.$$

# Глава 5

## Приложение

### 5.1 Декартовы произведения

Пусть  $n \in \mathbb{N}$  и  $a_1, \dots, a_n$  — некоторые множества. Множество  $S$ , состоящее из элементов  $a_1, \dots, a_n$ , обозначается  $\{a_1, \dots, a_n\}$ . Высказывание « $S = \{a_1, \dots, a_n\}$  и элементы  $a_1, \dots, a_n$  различны» сокращенно записывается так:  $S = {}^\circ\{a_1, \dots, a_n\}$ .

**Определение 5.1.1.** Пусть  $a, b$  — множества. Множество  $\{\{a\}, \{a, b\}\}$  обозначается  $(a, b)$  и называется упорядоченной парой. Элемент  $a$  называется первым элементом пары  $(a, b)$ , элемент  $b$  — вторым элементом пары  $(a, b)$ .

**Теорема 5.1.1.** Пусть  $a, b, c, d$  — множества. Тогда  $(a, b) = (c, d)$  если и только если  $a = c$  и  $b = d$ .

**Определение 5.1.2.** Пусть  $X, Y$  — множества. Множество всех упорядоченных пар  $(x, y)$ , где  $x \in X$ ,  $y \in Y$  называется декартовым произведением множеств  $X$  и  $Y$  и обозначается  $X \times Y$ .

**Определение 5.1.3.** Пусть  $X$  — множество. Декартово произведение  $X \times X$  называется декартовым квадратом множества  $X$  и обозначается  $X^2$ .

Определим понятие упорядоченной тройки, четверки и, вообще, упорядоченной  $n$ -ки для любого  $n \in \mathbb{N}$ .

**Определение 5.1.4.** При  $n = 2$  определение упорядоченной пары уже имеется. Предположим, определено понятие упорядоченной  $(n - 1)$ -ки. Тогда упорядоченную  $n$ -ку  $(a_1, \dots, a_n)$  определяем как  $((a_1, \dots, a_{n-1}), a_n)$ .

**Теорема 5.1.2.**  $(a_1, \dots, a_n) = (a'_1, \dots, a'_n)$  тогда и только тогда, когда  $a_i = b_i$  для всех  $i \in \{1, \dots, n\}$ .

**Определение 5.1.5.** Декартовым произведением множеств  $X_1, \dots, X_n$  называется множество  $X$  всевозможных упорядоченных  $n$ -ок  $(x_1, \dots, x_n)$ , где  $x_i \in X_i$  для всех  $1 \leq i \leq n$ . Декартово произведение  $X$  обозначается  $X_1 \times \dots \times X_n$  или  $\bigtimes_{i=1}^n X_i$ .

Количество элементов множества  $X$  мы обозначаем  $|X|$ .

**Теорема 5.1.3.** Если множества  $X_1, \dots, X_n$  конечны, то  $|\bigtimes_{i=1}^n X_i| = \prod_{i=1}^n |X_i|$ .

**Определение 5.1.6.** (Неформальное) Отображением множества  $X$  в множество  $Y$  называют любое правило  $f$ , сопоставляющее каждому элементу  $a \in X$  некоторый (один) элемент  $b \in Y$ . Высказывание « $f$  — отображение  $X$  в  $Y$ » записывают следующим образом:  $f : X \rightarrow Y$ . Множество  $X$  называют областью определения  $f$ ,  $Y$  — областью значений. Если элементу  $a \in X$  отображение  $f$  сопоставляет элемент  $b \in Y$ , то пишут  $b = af$ , или  $f : a \mapsto b$ , или просто  $a \mapsto b$ . Графиком  $f$  называют множество  $\{(a, b) \in X \times Y : af = b\}$ .

**Определение 5.1.7.** (Формальное) Пусть  $X, Y$  — множество. Отображением  $X$  в  $Y$  называют любую упорядоченную тройку  $f = (X, Y, g)$ , где  $g \subseteq X \times Y$ , причем для каждого  $a \in X$  найдется ровно один элемент  $b \in Y$ , такой, что  $(a, b) \in g$ .  $X$  называют областью определения  $f$ ,  $Y$  — областью значений,  $g$  — графиком  $f$ . Если  $(a, b) \in g$ , то пишут  $b = af$ .

**Определение 5.1.8.** Множество всех отображений  $Y$  в  $X$  обозначается  $X^Y$ .

Если  $f : I \rightarrow X$  — отображение, то бывает удобным элементы  $I$  считать индексами, вместо  $f(i)$  писать  $f_i$  и представлять себе  $f$  как «строку», элементы которой индексируются индексами из  $I$  и в которой на  $i$ -м месте стоит элемент  $f_i$ . В таком случае мы называем  $f$  индексированным семейством и записываем  $f$  как  $(f_i)_{i \in I}$ . Если  $I$  бесконечно, то такая «строка» имеет бесконечную длину. Можно также рассматривать  $f$  как некоторую последовательность элементов  $X$ , занумерованных элементами из  $I$ . Мы получили обобщение понятия строки, или упорядоченной  $n$ -ки. Но тогда у нас возникает возможность обобщить конструкцию декартова произведения конечного семейства множеств до декартова произведения любого семейства множеств.

**Определение 5.1.9.** Пусть  $I$  — множество, и  $(A_i)_{i \in I}$  — семейство множеств. Декартовым произведением  $\prod_{i \in I} A_i$  называется множество всевозможных отображений  $I \rightarrow \bigcup_{i \in I} A_i$  таких, что  $f(i) \in A_i$  для всех  $i \in I$ .

Другими словами,  $\prod_{i \in I} A_i$  — это множество всевозможных индексированных семейств  $(a_i)_{i \in I}$  таких, что  $a_i \in A_i$  для всех  $i \in I$ .

**Определение 5.1.10.** Пусть  $A \xrightarrow{\alpha} B \xrightarrow{\beta} C$ . Отображение  $A \rightarrow C$ , каждой точке  $a \in A$  сопоставляющее элемент  $(a\alpha)\beta$ , называется произведением  $\alpha$  и  $\beta$  и обозначается  $\alpha\beta$ .

**Определение 5.1.11.** Пусть  $X$  — множество. Отображение  $X \rightarrow X$ , каждой точке  $a \in X$  сопоставляющее точку  $a$ , называется единичным, или тождественным отображением  $X$  и обозначается  $\text{id}_X$  или  $1_X$ .

**Теорема 5.1.4.** Пусть  $f : X \rightarrow Y$ . Тогда  $1_X f = f$ ,  $f 1_Y = f$ .

**Теорема 5.1.5.** Пусть  $A \xrightarrow{\alpha} B \xrightarrow{\beta} C \xrightarrow{\gamma} D$ . Тогда  $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ .

**Определение 5.1.12.** Пусть  $f : X \rightarrow Y$ ,  $S \subseteq X$ . Множество  $\{af : a \in S\}$  называется  $f$ -образом  $S$  и обозначается  $Sf$ .

**Определение 5.1.13.** Пусть  $f : X \rightarrow Y$ ,  $X' \subseteq X$ ,  $Y' \subseteq Y$ , причем  $X'f \subseteq Y'$ . Тогда отображение  $X' \rightarrow Y'$ , каждой точке  $x' \in X'$  сопоставляющее точку  $x'f \in Y'$ , обозначим  $f|_{X', Y'}$ . Если  $X = Y$ ,  $X' = Y'$ , то мы обозначаем  $f|_{X', Y'} =: f|_{X'}$  и называем  $f|_{X'}$  сужением  $f$  на  $X'$ .

**Определение 5.1.14.** Пусть  $f : X \rightarrow Y$ ,  $S \subseteq Y$ . Множество  $\{a \in X : af \in S\}$  называется  $f$ -прообразом  $S$  и обозначается  $Sf^{-1}$ .

Если  $S = \{a\}$ , то вместо  $\{a\}f^{-1}$  пишут  $af^{-1}$ .

**Определение 5.1.15.** Отображение  $f : X \rightarrow Y$  называется инъективным, если для любых  $a, b \in X$  из  $a \neq b$  следует  $af \neq bf$ .

Высказывание «отображение  $f : X \rightarrow Y$  инъективно» иногда сокращенно записывают так:  $f : X \rightarrowtail Y$ .

**Определение 5.1.16.** Отображение  $f : X \rightarrow Y$  называется сюръективным, если  $Xf = Y$ .

**Определение 5.1.17.** Отображение  $f : X \rightarrow Y$  называется сюръективным, если для любого  $y \in Y$  найдется  $x \in X$  такой, что  $xf = y$ .

Высказывание «отображение  $f : X \rightarrow Y$  сюръективно» сокращенно записывают так:  $f : X \twoheadrightarrow Y$ .

**Определение 5.1.18.** *Отображение  $f : X \rightarrow Y$  называется биекцией, если  $f$  сюръективно и инъективно.*

**Определение 5.1.19.** *Биекция  $f : X \rightarrow X$  называется перестановкой множества  $X$ , или перестановкой элементов  $X$ .*

**Теорема 5.1.6.** *Пусть  $A \xrightarrow{\alpha} B \xrightarrow{\beta} C$  — отображения. Тогда выполняются следующие утверждения.*

- 1) *Если  $\alpha, \beta$  инъективны, то и  $\alpha\beta$  — инъективное отображение.*
- 2) *Если  $\alpha, \beta$  сюръективны, то и  $\alpha\beta$  — сюръективное отображение.*
- 3) *Если  $\alpha, \beta$  биекции, то и  $\alpha\beta$  — биекция.*

**Определение 5.1.20.** *Пусть  $\alpha : A \rightarrow B$ . Отображение  $\beta : B \rightarrow A$  назовем обратным к  $\alpha$ , если  $\alpha\beta = 1_A$ ,  $\beta\alpha = 1_B$ .*

**Теорема 5.1.7.** *Любое отображение имеет не более одного обратного отображения.*

**Определение 5.1.21.** *Отображение  $\alpha : A \rightarrow B$ , имеющее обратное, будем называть обратимым.*

**Определение 5.1.22.** *Если отображение  $\alpha : A \rightarrow B$  обратимо, то обратное к нему обозначается  $\alpha^{-1}$ .*

**Предложение 5.1.8.** *Пусть  $\alpha : A \rightarrow B$ ,  $\beta : B \rightarrow A$  — обратное к  $\alpha$  отображение. Тогда  $\alpha$  — обратное к  $\beta$  отображение.*

**Определение 5.1.23.** *Обратимое отображение  $\alpha : A \rightarrow B$  называется изоморфизмом (множеств).*

**Предложение 5.1.9.** *Если  $\alpha : A \rightarrow B$  — изоморфизм,  $\beta : B \rightarrow A$  — обратное к  $\alpha$  отображение, то  $\beta$  — изоморфизм.*

**Теорема 5.1.10.** *Пусть  $f : X \rightarrow Y$  — отображение. Равносильны следующие утверждения:*

- 1)  *$f$  — биекция;*
- 2)  *$f$  — обратимое отображение;*

3)  $f$  — изоморфизм.

**Теорема 5.1.11.** (О сюръективном отображении) Пусть  $\alpha : A \twoheadrightarrow B$  — сюръективное отображение,  $\gamma : A \rightarrow C$  — такое отображение, что  $x\alpha = y\alpha \Rightarrow x\gamma = y\gamma$  для любых  $x, y \in A$ . Тогда существует и единственно отображение  $\beta : B \rightarrow C$  такое, что коммутативна следующая диаграмма.

$$\begin{array}{ccc} & B & \\ \alpha \nearrow & & \searrow \beta \\ A & \xrightarrow{\gamma} & C \end{array} .$$

Если  $\gamma$  сюръективно, то и  $\beta$  сюръективно. Если  $x\alpha = y\alpha \Leftrightarrow x\gamma = y\gamma$  для любых  $x, y \in A$ , то  $\beta$  инъективно.

*Доказательство.* Покажем, что существует не более одного отображения  $\beta : B \rightarrow C$ , удовлетворяющего условию  $\alpha\beta = \gamma$ . Пусть  $\beta, \beta' : B \rightarrow C$  — отображения такие, что  $\alpha\beta = \gamma$ ,  $\alpha\beta' = \gamma$ ,  $b \in B$ . Так как отображение  $\alpha$  сюръективно, то найдется  $a \in A$  такое, что  $b = a\alpha$ .

$$b\beta = (a\alpha)\beta = a(\alpha\beta) = a\gamma,$$

$$b\beta' = (a\alpha)\beta' = a(\alpha\beta') = a\gamma.$$

Следовательно, для любого  $b \in B$ ,  $b\beta = b\beta'$ , откуда вытекает равенство  $\beta = \beta'$ .

Докажем, что существует отображение  $\beta : B \rightarrow C$  такое, что  $\alpha\beta = \gamma$ . Определим отображение  $\beta : B \rightarrow C$  следующим образом: Пусть  $b \in B$  и  $a \in A$ , причем  $b = a\alpha$ . Тогда полагаем  $b\beta = a\gamma$ . Это определение нуждается в проверке корректности. Необходимо убедиться, что если  $a' \in A$  и  $b = a'\alpha$ , то  $a\gamma = a'\gamma$ . Так как  $a\alpha = a'\alpha$ , то, по условию,  $a\gamma = a'\gamma$ . Корректность доказана.

Докажем, что  $\alpha\beta = \gamma$ . Пусть  $a \in A$ .

$$a\alpha\beta = (a\alpha)\beta = \gamma(a).$$

Таким образом, отображения  $\alpha\beta$  и  $\gamma$  совпадают в любой точке  $A$ , следовательно, они равны.

Пусть  $x\alpha = y\alpha \Leftrightarrow x\gamma = y\gamma$  для любых  $x, y \in A$ . Покажем, что  $\beta$  инъективно. Пусть  $b_1, b_2 \in B$  и  $b_1\beta = b_2\beta$ . Докажем, что  $b_1 = b_2$ . Из сюръективности  $\alpha$  вытекает существование элементов  $a_1, a_2 \in A$  таких, что  $b_1 = a_1\alpha$ ,  $b_2 = a_2\alpha$ . В силу коммутативности диаграммы,  $b_1\beta = (a_1\alpha)\beta = a_1(\alpha\beta) = a_1\gamma$ . Аналогично,  $b_2\beta = a_2\gamma$ . Так как  $b_1\beta = b_2\beta$ , то  $a_1\gamma = a_2\gamma$ . Отсюда  $a_1\alpha = a_2\alpha$ , то есть  $b_1 = b_2$ . Инъективность доказана.

Пусть  $\gamma$  сюръективно. Покажем, что  $\beta$  сюръективно. Рассмотрим произвольный элемент  $c \in C$ . Так как  $\gamma$  сюръективно, то  $c = a\gamma$  для некоторого  $a \in A$ . Но  $a\gamma = (a\alpha)\beta$ , поэтому  $c = (a\alpha)\beta$ .  $\square$

## 5.2 Отношения эквивалентности

В настоящем разделе  $X$  — произвольное множество. Интуитивно, отношение  $\rho$  на множестве  $X$  — это произвольное «правило», сопоставляющее любой паре  $(a, b) \in X^2$  какое-либо одно логическое значение, — «истину» или «ложь». Таким образом, отношение — не что иное, как отображение  $X^2 \rightarrow \{true, false\}$ . Очевидно, однако, что такое отношение  $\rho$  полностью определяется тем, каким парам из  $X^2$  сопоставлено значение «истина». Можно сказать, что  $\rho$  полностью определено некоторым множеством  $T$  пар из  $X^2$ . С другой стороны, имея произвольное подмножество  $T \subseteq X^2$ , можно построить отношение (в интуитивном смысле)  $\rho$  так, чтобы парам из  $T$  соответствовала бы «истина», а остальным парам из  $X^2$  — ложь. Очевидно, получаем биекцию между отношениями на  $X$  и подмножествами  $X^2$ . Мы видим, что можно отождествлять отношения на  $X$  и подмножества  $X^2$ . Так как понятие подмножества проще понятия отображения, то мы принимаем следующее определение.

**Определение 5.2.1.** *Отношением на  $X$  называют любое подмножество  $\rho \subseteq X^2$ .*

Далее,  $\rho$  — отношение на  $X$ . Для  $a, b \in X$  высказывание « $(a, b) \in \rho$ » будем сокращать так:  $arb$ .

**Пример 5.2.1.** *Отношение  $\rho = \{(a, a) : a \in X\}$  называется отношением равенства на  $X$ . Высказывание  $arb$  означает, что  $a = b$ .*

**Пример 5.2.2.** *Если  $f : X \rightarrow Y$  — отображение, то возникает отношение  $\rho = \{(a, b) \in X^2 : af = bf\}$ . Высказывание  $arb$  означает, что  $af = bf$ .*

**Пример 5.2.3.** *Отношение  $\rho = \{(a, b) \in X^2 : a \neq b\}$  называется отношением неравенства на  $X$ . Высказывание  $arb$  означает, что  $a \neq b$ .*

**Пример 5.2.4.** *Пусть  $X \subseteq \mathbb{R}$ , и  $\rho = \{(a, b) \in X^2 : a \leq b\}$ . Тогда  $\rho$  — это обычное отношение  $\leq$  на числовом множестве  $X$ , и высказывание  $arb$  означает, что  $a \leq b$ .*

**Пример 5.2.5.** *Аналогично, пусть  $X \subseteq \mathbb{R}$ , и  $\rho = \{(a, b) \in X^2 : a < b\}$ . Тогда  $\rho$  — это обычное отношение  $<$  на числовом множестве  $X$ . Высказывание  $arb$  означает, что  $a < b$ .*

Множество всех подмножеств множества  $X$  обозначим  $P(X)$ . Очевидно, высказывание  $A \subseteq P(X)$  означает, что множество  $A$  состоит из некоторых подмножеств  $X$ .

**Пример 5.2.6.** *Пусть  $\Omega$  — множество, и  $X \subseteq P(\Omega)$ , тогда отношение  $\rho$  включения на  $X$  может быть записано как  $\rho = \{(a, b) \in X^2 : a \subseteq b\}$ . Высказывание  $arb$  означает, что  $a \subseteq b$ .*

**Пример 5.2.7.** Мы можем взять любое множество  $X$  и произвольное подмножество  $\rho \subseteq X^2$ , тогда  $\rho$  — отношение на  $X$ . Например, если  $X = \mathbb{R}$ , то  $X^2$  — это координатная плоскость, и любое ее подмножество — это отношение на  $X$ . В частности, в качестве  $\rho$  можно взять какую-нибудь окружность или прямую на плоскости  $X^2$ .

**Определение 5.2.2.** Отношение  $\rho$  называется

- 1) рефлексивным, если  $a \rho a$  для любого  $a \in X$ ,
- 2) симметричным, если  $a \rho b \Rightarrow b \rho a$  для всех  $a, b \in X$ ,
- 3) транзитивным, если  $a \rho b$  и  $b \rho c$  влечет  $a \rho c$  для всех  $a, b, c \in X$ ,
- 4) отношением эквивалентности, если  $\rho$  рефлексивно, симметрично и транзитивно.

**Пример 5.2.8.** Рассматривая описанные выше примеры отношений и описывая их свойства, мы получаем следующую таблицу (в первом столбце указаны номера примеров, «-» означает «не всегда»).

| $\rho$ | Рефлексивно | Симметрично | Транзитивно | Отн. экв-ти |
|--------|-------------|-------------|-------------|-------------|
| 5.2.1  | +           | +           | +           | +           |
| 5.2.2  | +           | +           | +           | +           |
| 5.2.3  | -           | +           | -           | -           |
| 5.2.4  | +           | -           | +           | -           |
| 5.2.5  | -           | -           | +           | -           |
| 5.2.6  | +           | -           | +           | -           |

**Определение 5.2.3.** Разбиением множества  $X$  называется произвольное множество  $P$  некоторых подмножеств  $X$ , удовлетворяющее условиям:

- 1)  $\emptyset \notin P$ ;
- 2) Любые два элемента  $P$  либо совпадают, либо не пересекаются;
- 3)  $\cup P = X$ .

**Определение 5.2.4.** Пусть  $X$  — множество,  $\rho$  — отношение эквивалентности на  $X$ ,  $x \in X$ . Классом эквивалентности  $[x]$  элемента  $x$  относительно  $\rho$  называется множество  $\{y \in X : x \rho y\}$ . Множество всех классов эквивалентности обозначим  $X/\rho$ .

Если  $a, b \in X$ , то  $[a] = [b] \Leftrightarrow a \sim b$ . В частности, если  $a \in [b]$ , то  $[a] = [b]$ .

**Теорема 5.2.1.** Пусть  $X$  — непустое множество,  $\rho$  — отношение эквивалентности на  $X$ . Тогда  $X/\rho$  является разбиением  $X$ .

### 5.3 Отношения порядка

**Определение 5.3.1.** Отношение  $\rho$  на множестве  $X$  называется *антисимметричным*, если из  $x\rho y$  и  $y\rho x$  следует  $x = y$ .

**Определение 5.3.2.** Рефлексивное, транзитивное и антисимметричное отношение  $\rho$  на множестве  $X$  называется *порядком*, а множество вместе с некоторым порядком называется *упорядоченным*.

Например, если  $\Omega$  — множество, а  $X$  — множество, состоящее из некоторых подмножеств  $\Omega$ , то  $X$  упорядочено отношением включения.

**Определение 5.3.3.** Мы говорим, что элементы  $a, b$  упорядоченного множества  $X$  *сравнимы*, если  $a \leq b$  или  $b \leq a$ .

**Определение 5.3.4.** Подмножество  $C$  упорядоченного множества  $X$  называется *цепью*, если любые два элемента  $C$  сравнимы.

**Определение 5.3.5.** Элемент  $a$  упорядоченного множества  $X$  называется

- 1) *максимальным*, если не существует элемента  $b \in X$  такого, что  $a < b$ ,
- 2) *минимальным*, если не существует элемента  $b \in X$  такого, что  $a > b$ ,
- 3) *наибольшим*, если  $a \geq b$  для всех  $b \in X$ ,
- 4) *наименьшим*, если  $a \leq b$  для всех  $b \in X$ .

Очевидно, наибольший и наименьший элементы единственны, если они есть. Максимальных и минимальных элементов может быть несколько. Ясно, что наибольший элемент является максимальным, но обратное не верно. То же касается наименьших и минимальных элементов.

## 5.4 Категории

**Определение 5.4.1.** Граф  $G$  состоит из

- 1) произвольного класса  $V$ , элементы которого называются вершинами графа  $G$ ,
- 2) любого класса  $A$ , элементы которого мы представляем как стрелки, каждая из которых ведет из одной вершины в другую, возможно, совпадающую с исходной.
- 3) любого отображения  $\text{dom} : A \rightarrow V$ , которое сопоставляет каждой стрелке из  $A$  ее начало = область определения — некоторую вершину из  $V$ ,
- 4) произвольного отображения  $\text{cod} : A \rightarrow V$ , которое сопоставляет любой стрелке ее конец = область значений, = кообласть — какую-то вершину из  $V$ .

Например, следующий граф  $G$  состоит из множества вершин  $V = \{A, B, C, D\}$ , множества стрелок  $A = \{e, f, g, h\}$ , отображений  $\text{dom}, \text{cod} : V \rightarrow A$ ,  $\text{dom}(e) = \text{cod}(e) = A$ ,  $\text{dom}(f) = A$ ,  $\text{cod}(f) = B$ ,  $\text{dom}(g) = A$ ,  $\text{cod}(g) = B$ ,  $\text{dom}(h) = B$ ,  $\text{cod}(h) = C$ .

$$e \begin{array}{c} \curvearrowright \\ \curvearrowleft \end{array} A \begin{array}{c} \xrightarrow{f} \\ \xrightarrow{g} \end{array} B \xrightarrow{h} C \quad D . \quad (5.4.1)$$

**Определение 5.4.2.** Если  $a, b$  — вершины графа  $G$ , то множество стрелок графа  $G$  из  $a$  в  $b$  обозначим  $G(a, b)$ , или  $\text{Mor}_G(a, b)$ , или  $\text{Mor}(a, b)$ , если ясно, о каком графе идет речь.

Например, в графе  $G$  из 5.4.1  $G(A, A) = \{e\}$ ,  $G(A, B) = \{f, g\}$ ,  $G(A, C) = \emptyset$ ,  $G(C, D) = \emptyset$ .

Если стрелка  $f$  имеет начало  $a$  и конец  $b$ , то мы пишем  $f : a \rightarrow b$ , или  $a \xrightarrow{f} b$ . Множество вершин графа  $G$  обозначим  $\text{Ob}(G)$ .

Можно считать, что множество вершин графа и множество его ребер не пересекаются.

**Определение 5.4.3.** Пусть  $G, H$  — графы. Морфизмом  $G \rightarrow H$  назовем любое отображение  $\phi : V(G) \cup A(G) \rightarrow V(H) \cup A(H)$  такое, что  $(V(G))\phi \subseteq V(H)$  (т. е. вершины  $G$  переходят в вершины  $H$ ),  $(A(G))\phi \subseteq A(H)$  (т. е. ребра  $G$  переходят в ребра  $H$ ), и если  $a, b \in V(G)$ ,  $f \in \text{Mor}_G(a, b)$ , то  $f\phi \in \text{Mor}_H(a\phi, b\phi)$  (т. е. из  $f : a \rightarrow b$  следует  $f\phi : a\phi \rightarrow b\phi$ ).

**Определение 5.4.4.** Категория — это граф  $\mathcal{C}$ , в котором для произвольных вершин  $A, B, C$  задано произведение  $\text{Mor}(A, B) \times \text{Mor}(B, C) \rightarrow \text{Mor}(A, C)$ , причем выполняются следующие условия.

- 1) Для вершин  $A, B, C, D$  и  $f \in \text{Mor}(A, B)$ ,  $g \in \text{Mor}(B, C)$ ,  $h \in \text{Mor}(C, D)$  выполняется закон ассоциативности  $(fg)h = f(gh)$ .
- 2) Для каждой вершины  $A$  найдется  $e \in \text{Mor}(A, A)$  такой, что для любой вершины  $B$  и  $f \in \text{Mor}(A, B)$ ,  $g \in \text{Mor}(B, A)$  выполняются равенства  $ef = f$  и  $ge = g$ .

Вершины категории  $\mathcal{C}$  называются ее объектами и класс всех объектов категории  $\mathcal{C}$  обозначим  $\text{Ob}(\mathcal{C})$ . Если  $X, Y \in \text{Ob}(\mathcal{C})$ , то элементы  $\text{Mor}(X, Y)$  называются морфизмами  $X$  в  $Y$ , или морфизмами  $X \rightarrow Y$ . Если  $\alpha \in \text{Mor}(X, Y)$ , то мы пишем  $\alpha : X \rightarrow Y$ , или  $X \xrightarrow{\alpha} Y$ . Морфизм  $e : A \rightarrow A$  из аксиомы 2 называется *тождественным*, или *единичным* морфизмом объекта  $A$ . Морфизмы вида  $A \rightarrow A$  называются эндоморфизмами объекта  $A$ .

**Пример 5.4.1.** Множества вместе со всеми их отображениями образуют категорию — категорию множеств.

**Пример 5.4.2.** Все однотипные математические структуры, вместе с их гомоморфизмами, образуют категорию. Так возникают категории групп, абелевых групп, колец, модулей над фиксированным кольцом, топологических пространств и их непрерывных отображений, графов и их морфизмов, и.т.д.

**Пример 5.4.3.** Допустим, что  $X$  — *упорядоченное множество*, тогда можно рассматривать  $X$  как категорию  $\mathcal{C}$ , в которой  $\text{Ob}(\mathcal{C}) = X$  и для  $a, b \in \text{Ob}(\mathcal{C})$

$$\text{Mor}(a, b) = \begin{cases} \{(a, b)\}, & \text{если } a \leq b \\ \emptyset, & \text{если } a \not\leq b. \end{cases}$$

Если  $\alpha : a \rightarrow b$ ,  $\beta : b \rightarrow c$  морфизмы в  $\mathcal{C}$ , то мы определяем их композицию  $\alpha\beta := (a, c)$ . Очевидно, для  $a \in X$  тождественным морфизмом будет пара  $(a, a)$ . Обычно мы отождествляем  $X$  и  $\mathcal{C}$ .

**Лемма 5.4.1.** Каждый объект категории  $\mathcal{C}$  имеет единственный тождественный морфизм.

*Доказательство.* Пусть  $A \in \text{Ob}(\mathcal{C})$ ,  $e, e'$  — тождественные морфизмы  $A$ . Тогда  $e'e = e'$  и  $e'e = e$ , то есть  $e = e'$ .  $\square$

По этой причине мы имеем право обозначить этот единственный элемент  $\text{id}_A$ .

**Определение 5.4.5.** Пусть  $A, B \in \text{Ob}(\mathcal{C})$ ,  $f : A \rightarrow B$ ,  $g : A \leftarrow B$ . Мы называем морфизм  $g$  обратным к  $f$ , если  $fg = \text{id}_A$  и  $gf = \text{id}_B$ . Если  $f$  имеет обратный морфизм, то  $f$  называется изоморфизмом, или обратимым морфизмом.

**Лемма 5.4.2.** Для любого морфизма существует не более одного обратного морфизма.

*Доказательство.* Пусть  $A, B \in \text{Ob}(\mathcal{C})$ ,  $f : A \rightarrow B$ ,  $g, g' : A \leftarrow B$  — обратные к  $f$  морфизмы. Тогда

$$g = g \text{id}_A = g(fg') = (gf)g' = \text{id}_B g' = g'.$$

□

Если морфизм  $f$  имеет обратный морфизм  $g$ , то мы обозначаем  $g =: f^{-1}$ .

**Лемма 5.4.3.** Пусть  $f, g$  — изоморфизмы категории  $\mathcal{C}$ , и существует произведение  $gf$ . Тогда  $gf$  — изоморфизм, и  $(gf)^{-1} = f^{-1}g^{-1}$ .

*Доказательство.* Очевидно.

□

*Учебное издание*

**Волочков Александр Андреевич**

# **КОНЕЧНЫЕ ГРУППЫ**

## **ВВЕДЕНИЕ В ТЕОРИЮ**

### **Часть 1**

Учебное пособие

Редактор *Н. И. Стрекаловская*

Компьютерная верстка: *А. А. Волочков*

Техническая подготовка материалов: *Л. С. Нечаева*

---

Подписано к использованию 31.08.2018

Объем данных – 1 Мб

---

Размещено в открытом доступе  
на сайте [www.psu.ru](http://www.psu.ru)  
в разделе НАУКА / Электронные публикации  
и в электронной мультимедийной библиотеке ELiS

Издательский центр  
Пермского государственного  
национального исследовательского университета.  
614990, г. Пермь, ул. Букирева, 15