Глава 2

Алгебраические структуры

Бинарные операции

Определение 2.1. *Бинарной операцией* на множестве X называется любое фиксированное отображение $\varphi : X \times X \to X$.

Согласно этому определению, при задании бинарной операции каждой упорядоченной паре $(a,b) \in X \times X$ ставится в соответствие однозначно определенный элемент $c = \varphi(a,b)$ множества X. Вместо $c = \varphi(a,b)$ иногда записывают $c = a\varphi b$, а еще чаще бинарную операцию обозначают каким-нибудь специальным символом, например, знаками $+$, $\oplus$, $\times$, $*$, $\circ$, $\otimes$ и тому подобное. При этом элемент $c = a * b$ могут назвать «произведением», а элемент $d = a \oplus b$ - «суммой» соответствующих элементов, хотя по своему характеру эти операции могут существенно отличаться от известных «обычных» операций на множестве действительных чисел. На любом множестве X могут быть заданы несколько бинарных операций. Желая выделить какую-либо из них, используют запись $(X, *)$, где $*$ есть некоторая бинарная операция, и тогда говорят, что опе-

рация $*$ задает на множестве X некоторую *алгебраическую структуру* $(X, *)$.

Пример 2.1. На множестве целых чисел $\boldsymbol{Z}$ определены естественные операции сложения и умножения. Помимо этих операций, можно ввести и другие операции, например, $m * n = m + n - m \cdot n$ или $m \circ n = -n - m$. В результате мы получим разные алгебраические структуры: $(\boldsymbol{Z}, +)$, $(\boldsymbol{Z}, \cdot)$, $(\boldsymbol{Z}, *)$, $(\boldsymbol{Z}, \circ)$.

В общем случае наряду с бинарными операциями можно ввести *n*-арные операции как отображения $\psi : X^n \to X$. Существуют и простейшие *унарные* операции. Примером такой операции может служить операция дополнения, заданная на элементах булеана $\mathcal{B}(X)$ некоторого множества X.

Полугруппы

Определение 2.2. Бинарная операция $*$ на множестве X называется *ассоциативной,* если $a * (b * c) = (a * b) * c$ для любых $a, b, c \in X$. Операция $*$ называется *коммутативной,* если $a * b = b * a$. Если операция $*$ ассоциативна (коммутативна), то такое же название присваивают и соответствующей алгебраической структуре $(X, *)$.

Пример 2.2. Рассмотрим множество $M_2(\boldsymbol{R})$ всех квадратных матриц второго порядка, элементами которых являются действительные

числа. Обычное произведение двух матриц A и B ассоциативно, но не коммутативно, поэтому структура $(M_2(\boldsymbol{R}), \cdot)$ только ассоциативна.

Пример 2.3. На множестве целых чисел $\boldsymbol{Z}$ операция, заданная правилом $m \circ n = -n - m$, коммутативна, но не ассоциативна. В самом деле,

$(-2) * ((-3) * 5) = (-2) * (+3 - 5) = (-2) * (-2) = 2 + 2 = 4$,

$((-2) * (-3)) * 5) = (+2 + 3) * 5 = 5 * 5 = -5 - 5 = -10$,

и поэтому $m * (n * k) \neq (m * n) * k$.

Определение 2.3. Элемент $e \in X$ называется *единичным* (или *нейтральным*) относительно бинарной операции $*$, если $e * x = x * e = x$ для любого элемента $x \in X$.

Отметим, что единичный элемент является единственным. Если мы предположим, что существует еще один единичный элемент $\tilde{e}$, то получим $\tilde{e} = \tilde{e} * e = e$.

Определение 2.4. Множество X с заданной на этом множестве ассоциативной операцией (т.е. алгебраическая структура $(X, *)$ с ассоциативной операцией) называется *полугруппой*.

Определение 2.5. Полугруппа с единичным элементом называется *полугруппой с единицей* или *моноидом*.

В условном обозначении моноида, как правило, указывают нейтральный элемент, используя запись $(X, *, e)$.

Пример 2.4. Пусть X – произвольное множество и $\mathcal{B}(X)$ его булеан. На элементах булеана рассмотрим две бинарные операции – объ-

единения и пересечения множеств. Обе операции ассоциативны. Поскольку для любого элемента A булеана $\varnothing \cup A = A$, пустое множество выполняет функции нейтрального элемента относительно операции объединения. Для операции пересечения в качестве нейтрального элемента выступает само множество X, так как $X \cap A = A$ для любого подмножества $A \subset X$. Таким образом, полугруппами с единицей являются обе алгебраические структуры $(\mathcal{B}(X), \cup, \varnothing)$ и $(\mathcal{B}(X), \cap, X)$. При этом оба моноида коммутативны.

Пример 2.5. Пусть $X = \{1, 2\}$. Рассмотрим множество $M_{\varphi}(X)$ всех функциональных отображений $\varphi : X \to X$. На рис. 2.1 приведены диаграммы всех возможных отображений, включая тождественное отображение e.

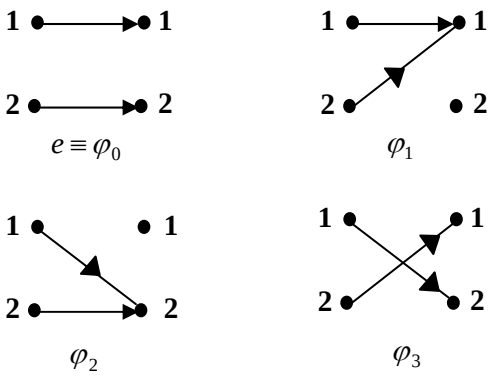


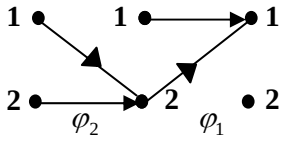
Рис. 2.1

В качестве бинарной операции на $M_{\varphi}(X)$ выберем композицию $\varphi \circ \psi$ любых двух перечисленных отображений[1]. Все возможные «произведения» отображений $e, \varphi_1, \varphi_2, \varphi_3$ полностью задаются таблицей 2.1, при этом в композиции $\varphi_i \circ \varphi_j$ отображение φ_i есть один из элементов первого столбца, а φ_j – один из элементов первой строки таблицы.

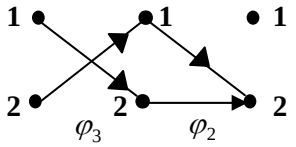
$\circ$	e	φ_1	φ_2	φ_3
e	e	φ_1	φ_2	φ_3
φ_1	φ_1	φ_1	φ_1	φ_1
φ_2	φ_2	φ_2	φ_2	φ_2
φ_3	φ_3	φ_2	φ_1	e

Табл. 2.1.

Поясним с помощью диаграмм, как работает композиция отображений. На следующем рис. 2.2 приведены диаграммы трех из шестнадцати возможных композиций

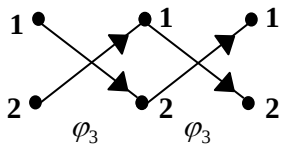


$\varphi_1 \circ \varphi_2 = \varphi_1$



$\varphi_2 \circ \varphi_3 = \varphi_2$

[1] Напомним, что в композиции отображений $\varphi \circ \psi$ сначала действует отображение ψ, а затем - отображение φ.



$\varphi_3 \circ \varphi_3 = e$

Рис. 2.2

Данные таблицы 2.1 позволяют сделать вывод о том, что структура $(M_\varphi(X), \circ, e)$ является некоммутативным моноидом.

Пример 2.6. Пусть $M_n(\boldsymbol{R})$ есть множество квадратных матриц порядка n с элементами из $\boldsymbol{R}$. Тогда $(M_n(\boldsymbol{R}), +, O)$ есть коммутативный моноид с нейтральным элементом O – нулевой матрицей и традиционной операцией сложения матриц.

Структура $(M_n(\boldsymbol{R}), \cdot, E)$ представляет собой некоммутативный моноид с единичной матрицей в качестве нейтрального элемента и обычной операцией умножения матриц.

Пример 2.7. Обозначим символом $m_0\boldsymbol{Z}$ множество целых чисел, кратных некоторому фиксированному целому числу $m_0 \neq 1$. Тогда $(m_0\boldsymbol{Z}, +, 0)$ – коммутативный моноид, а $(m_0\boldsymbol{Z}, \cdot)$ – коммутативная полугруппа.

Пример 2.8. Пусть $A = \{x, y, z\}$. Определим A^* как множество всевозможных последовательностей элементов из A. Тогда A^* содержит в качестве своих элементов, например, следующие последовательности символов (их еще называют *словами*):

x, xxy, $yyxz$, $zzzzx$ и т.д. На A^* определим операцию *конкатенации* (символ «○») следующим образом: если слова $a, b \in A^*$, то $a \circ b = ab$, где слово b записано сразу после слова a. Каждое слово из A^* имеет конечную длину $|a|$, равную числу символов слова. Например, длина $|xy| = 2$, $|xzzyz| = 5$. Наряду с «обычными» словами, введем *пустое* слово $\Lambda \in A^*$, имеющее длину $|\Lambda| = 0$ такое, что $\Lambda \circ a = a \circ \Lambda = a$ для любого слова a. Тогда структура $(A^*, \circ, \Lambda)$ является моноидом с нейтральным элементом[2] Λ.

Группы

Определение 2.6. *Обратным* к элементу x моноида $(X, *, e)$ называется элемент $y \in X$ такой, что $xy = yx = e$. Обратный элемент обозначают символом x^{-1}.

Определение 2.7. Моноид $(X, *, e)$, у которого для каждого элемента $x \in X$ существует обратный элемент $x^{-1} \in X$, называется *группой*.

Множество всех элементов группы называется *основным множеством* и обычно обозначается тем же символом, что и сама группа (т.е. алгебраическая структура). Произвольную группу и ее основное множество мы будем обозначать символом G.

---

[2] Отметим, что A^* представляет собой транзитивное замыкание отношения ρ конкатенации $\rho = \{(a, b) \mid b = a \circ x, \quad x \in A\}$.

Понятие группы является настолько важным в теории алгебраических структур, что мы снова перечислим все аксиомы, которым удовлетворяет группа.

Множество G называется *группой*, если:

1. На G определена бинарная операция $(x, y) \to x * y$.
2. Операция ассоциативна: $(x * y) * z = x * (y * z)$ для любых $x, y, z \in G$.
3. Структура $(G, *)$ содержит единичный (нейтральный) элемент $e \in G$ такой, что $e * x = x * e = x$ для любого $x \in G$.
4. Для каждого элемента $x \in G$ существует обратный элемент $x^{-1} \in G$: $x^{-1} * x = x * x^{-1} = e$.

В группе естественным образом определяются целые степени элементов с достаточно очевидными свойствами:

$$x^n = x * x * \ldots * x \quad (n \text{ раз}),$$

$$x^{-n} = x^{-1} * x^{-1} * \ldots * x^{-1} \quad (n \text{ раз}),$$

$$x^0 = e, \qquad x^n * x^m = x^{n+m}, \qquad (x^n)^m = x^{nm}, \qquad n, m \in \mathbf{Z}.$$

Если операция группы рассматривается как аналог умножения (обозначения $*$, $\circ$, $\otimes$, $\bullet$), то группу называют *мультипликативной*, вместо записи $x * y$ могут использовать запись xy, а единичный (нейтральный) элемент группы, по аналогии с операцией умножения, могут обозначить символом 1. Если же групповая операция рассматривается как аналог сложения (символы $+$, $\oplus$), то группу называют *аддитивной*. При этом нейтральный элемент груп-

пы могут обозначить символом 0, а элемент, обратный к элементу x, называют *противоположным*. В аддитивной группе вместо обозначения x^n используют запись nx.

Группа G с коммутативной бинарной операцией называется *коммутативной* (или *абелевой*) [3]. Символами $\mathrm{Card}\, G$ или $|G|$ обозначают число элементов (мощность) группы. Группа, содержащая только один элемент, называется *единичной* или *тривиальной*: $E = \{e\}$.

Определение 2.8. Пусть G – группа. Непустое подмножество $H \subset G$ называется *подгруппой* группы G, если:

для любых $h_1, h_2 \in H$ элемент $h_1 * h_2 \in H$;

для любого $h \in H$ элемент $h^{-1} \in H$.

Из определения следует, что любая подгруппа, очевидно, содержит единичный элемент $e = h * h^{-1}$.

Подгруппа H, отличная от E и G, называется *собственной подгруппой* группы G.

Пример 2.9. Структура ($\boldsymbol{Z}$, + , 0) представляет собой простейший пример аддитивной абелевой группы. Подгруппой этой группы является аддитивная группа всех четных целых чисел. В то же время не является подгруппой множество всех нечетных целых чисел с операцией сложения и нулем в качестве нейтрального элемента.

---

[3] Абель Нильс Хендрик (1802-1829) – норвежский математик, автор работ по алгебре, теории эллиптических функций, теории рядов, основатель теории интегралов от алгебраических функций.

Пример 2.10. Пусть $GL_n(\boldsymbol{R})$ есть множество всех квадратных матриц порядка n с действительными элементами и отличными от нуля определителями (множество *невырожденных* вещественных матриц порядка n). Покажем, что структура $(GL_n(\boldsymbol{R}), \cdot, E)$, где бинарная операция $\cdot$ представляет собой обычное произведение матриц, а E есть единичная матрица порядка n удовлетворяет аксиомам группы:

1) произведение любых двух невырожденных матриц $A, B \in GL_n(\boldsymbol{R})$ снова будет невырожденной квадратной матрицей порядка n с вещественными элементами, т.е. $A \cdot B \in GL_n(\boldsymbol{R})$;
2) в силу ассоциативности операции умножения матриц $A \cdot (B \cdot C) = (A \cdot B) \cdot C$ для любых $A, B, C \in GL_n(\boldsymbol{R})$;
3) единичная матрица $E \in GL_n(\boldsymbol{R})$ выполняет роль нейтрального элемента, поскольку $E \cdot A = A \cdot E = A$ для любой матрицы $A \in GL_n(\boldsymbol{R})$;
4) каждая матрица $A \in GL_n(\boldsymbol{R})$ является невырожденной, и, следовательно, существует обратная матрица $A^{-1} \in GL_n(\boldsymbol{R})$ – обратный к A элемент такой, что $A^{-1} \cdot A = A \cdot A^{-1} = E$.

Таким образом, структура $(GL_n(\boldsymbol{R}), \cdot, E)$ — мультипликативная группа, ее обозначают символом $GL_n(\boldsymbol{R})$ и называют *полной линейной группой степени n над* $\boldsymbol{R}$. Отметим, что $GL_n(\boldsymbol{R})$ не является абелевой (коммутативной) группой.

Пример 2.11. В группе $GL_n(\boldsymbol{R})$ выделим подмножество $SL_n(\boldsymbol{R})$ всех матриц с определителем, равным единице:

$SL_n(\boldsymbol{R}) = \{ A \mid \det A = 1,\ A \in GL_n(\boldsymbol{R})\}$.

Поскольку $\det E = 1$, единичная матрица $E \in SL_n(\boldsymbol{R})$. Кроме этого, если $\det A = 1$ и $\det B = 1$, то $\det(A \cdot B) = 1$ и $\det A^{-1} = 1$. Поэтому структура $(SL_n(\boldsymbol{R}), \bullet, E)$ также является группой. Эта группа представляет собой подгруппу группы $GL_n(\boldsymbol{R})$.

Симметрические группы

Прежде чем привести определение симметрической группы, рассмотрим простейшие примеры.

Пример 2.12. Пусть B_ψ есть множество всех биективных (взаимно однозначных) отображений множества $X = \{1,2,3\}$ в себя: $\psi : X \to X$. Элементы B_ψ мы можем представить в виде диаграмм (рис. 2.3).

Эти же отображения удобно записать в виде матриц размера 2×3, причем во второй строке матрицы расположены образы элементов первой строки, заданные данным отображением ψ_i:

$$e \equiv \psi_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \qquad \psi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \qquad \psi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

$$\psi_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \psi_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \psi_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Элементы ψ_i множества B_ψ иногда называют *перестановками* (или *подстановками*) на множестве $X = \{1, 2, 3\}$.

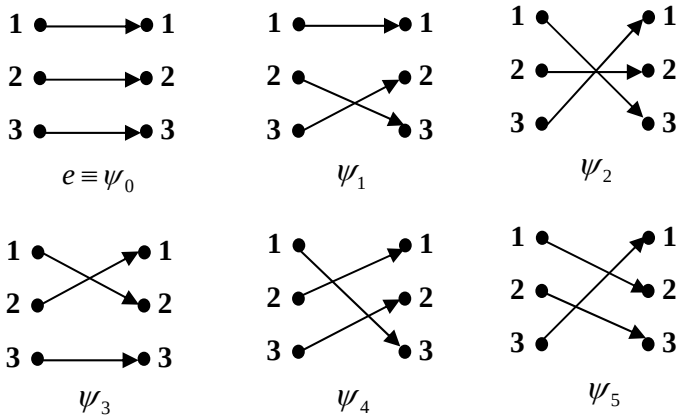


Рис. 2.3

В качестве бинарной операции на B_ψ введем композицию двух отображений $\psi_i \circ \psi_j$, и на следующем этапе покажем, как вычисляется такая композиция. Очевидно, тождественное отображение выполняет роль единичного элемента в композиции, например, $\psi_2 \circ e = \psi_2$ (сначала выполняется отображение e, а затем ψ_2):

$$\psi_2 \circ e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{matrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 2 & 1 \end{matrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \psi_2 .$$

Покажем, как вычисляются и некоторые другие композиции.

$$\psi_2 \circ \psi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{matrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 3 & 2 \\ \downarrow & \downarrow & \downarrow \\ 3 & 1 & 2 \end{matrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \psi_4 ,$$

$$\psi_3 \circ \psi_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{matrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 1 & 2 \\ \downarrow & \downarrow & \downarrow \\ 3 & 2 & 1 \end{matrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \psi_2 .$$

Отметим, что бинарная операция некоммутативна, так как

$$\psi_1 \circ \psi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \psi_5 \neq \psi_2 \circ \psi_1 .$$

Результаты этих и других аналогичных вычислений всех возможных композиций отображений приведены в таблице 2.2. Из таблицы 2.2 следует, что композиция отображений удовлетворяет следующим условиям:

1) для любых трех отображений $\psi_i, \psi_j, \psi_k \in B_\psi$

$$(\psi_i \circ \psi_j) \circ \psi_k = \psi_i \circ (\psi_j \circ \psi_k),$$

и поэтому операция композиции ассоциативна;

2) единичный элемент представлен тождественным отображением: $e \circ \psi_i = \psi_i \circ e = \psi_i$ для любого $\psi_i \in B_\psi$;

3) для каждого элемента $\psi_i \in B_\psi$ существует обратный элемент $\psi_i^{-1} \in B_\psi$ такой, что $\psi_i^{-1} \circ \psi_i = \psi_i \circ \psi_i^{-1} = e$. Так, обратными к элементам e, ψ_1, ψ_2, ψ_3 являются эти же элементы соответственно. Элементы ψ_4, ψ_5 взаимно обратные, т.е. $\psi_4^{-1} = \psi_5$ и $\psi_5^{-1} = \psi_4$.

$\circ$	e	ψ_1	ψ_2	ψ_3	ψ_4	ψ_5
e	e	ψ_1	ψ_2	ψ_3	ψ_4	ψ_5
ψ_1	ψ_1	e	ψ_5	ψ_4	ψ_3	ψ_2
ψ_2	ψ_2	ψ_4	e	ψ_5	ψ_1	ψ_3
ψ_3	ψ_3	ψ_5	ψ_4	e	ψ_2	ψ_1
ψ_4	ψ_4	ψ_2	ψ_3	ψ_1	ψ_5	e
ψ_5	ψ_5	ψ_3	ψ_1	ψ_2	e	ψ_4

Табл. 2.2

Таким образом, структура $(B_\psi, \circ, e)$ является некоммутативной группой. Эта группа обозначается символом S_3 и называется *симметрической группой степени* 3.

Таблица «умножения» элементов любой группы называется *таблицей Кэли*. Такую таблицу можно составить для любой конечной группы G. Для групп таблица Кэли имеет важную особенность: каждый ее столбец (строка) содержит все элементы группы. Действительно, если мы предположим, что какой-то элемент a_k встречается дважды в $j-$ом столбце, например, во 2-ой и 4-ой строках, получим $a_2 a_j = a_4 a_j$. Умножая обе части на a_j^{-1} справа, придем к равенству $a_2 = a_4$, которое невозможно, так как все элементы группы различны. Если группа абелева (коммутативна), то ее таблица Кэли будет симметричной относительно главной диагонали.

Пример 2.13. Если внимательно посмотреть на таблицу 2.1 композиции отображений, то нетрудно заметить, что в ней «спрятаны» таблицы меньшего размера, «замкнутые» относительно некоторых отображений (таблицы 2.3, 2.4, 2.5, 2.6).

Перечисленные таблицы задают собственные *подгруппы* группы S_3: $H_1 = \{e, \psi_1\}$, $H_2 = \{e, \psi_2\}$, $H_3 = \{e, \psi_3\}$, $H_4 = \{e, \psi_4, \psi_5\}$.

Помимо перечисленных подгрупп, группа S_3 имеет и две несобственные подгруппы — одна из них единичная $E = \{e\}$, а другая совпадает с S_3.

$\circ$	e	ψ_1
e	e	ψ_1
ψ_1	ψ_1	e

Табл. 2.3

$\circ$	e	ψ_2
e	e	ψ_2
ψ_2	ψ_2	e

Табл. 2.4

$\circ$	e	ψ_3
e	e	ψ_3
ψ_3	ψ_3	e

Табл. 2.5

$\circ$	e	ψ_4	ψ_5
e	e	ψ_4	ψ_5
ψ_4	ψ_4	ψ_5	e
ψ_5	ψ_5	e	ψ_4

Табл. 2.6

Замечание. Название *симметрическая* группа связано с тем, что совокупность элементов группы может служить характеристикой свойств симметрии некоторого правильного многоугольника. Группа S_3 тесно связана с *группой совмещений* T_3 правильного треугольника, вершины которого пронумерованы цифрами 1, 2 и 3. Элементы группы совмещений переводят правильный треугольник в конгруэнтный правильный треугольник с тем же расположением вершин, но с другой нумерацией. Так, например, элементу $\psi_1 \in S_3$ соответствует преобразование симметрии относительно прямой l_1, проходящей через вершину 1 треугольника (рис. 2.4).

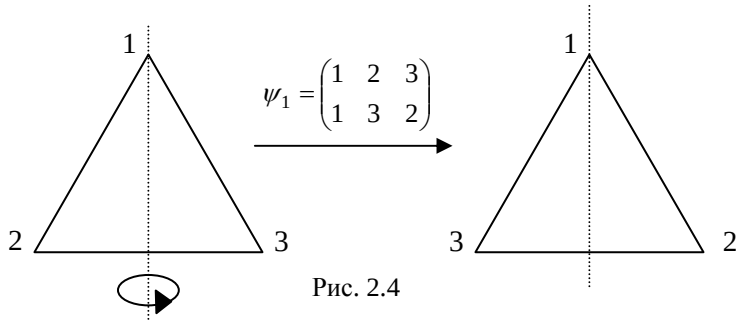


Рис. 2.4

Отображению ψ_5 соответствует поворот треугольника против часовой стрелки на угол 120^0 вокруг точки O - центра треугольника (рис. 2.5).

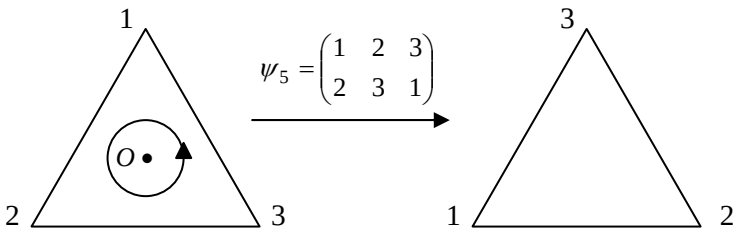


Рис. 2.5

Теперь приведем общее определение симметрической группы.

Определение 2.9. Пусть X есть конечное множество, содержащее n элементов. *Симметрической группой* S_n называется множество всех биективных отображений множества X на себя, снабженное бинарной операцией композиции отображений.

Отметим без доказательства, что $\operatorname{Card} S_n = n!$. Отметим также, что именно симметрическая группа лежала у истоков общей теории групп, созданной более 150 лет назад Эваристом Галуа[4].

Циклические группы

Пусть G есть некоторая мультипликативная группа, a - фиксированный элемент этой группы. Степенью m элемента a называется m-кратное произведение $a^m = a * a * \ldots * a$ (m раз). Если групповой

[4] Галуа Эварист (1811-1832) –французский математик, заложивший основы современной алгебры.

операцией является операция сложения (аддитивная группа), то «степенью» m элемента a называют m-кратную сумму $ma = a + a + \ldots + a$ (m раз).

Определение 2.10. *Циклической группой,* порожденной элементом a, называется группа G, любой элемент которой имеет вид a^n, $n \in \boldsymbol{Z}$.

Иными словами, циклическая группа содержит все возможные целые степени одного и того же элемента a. Для циклической группы часто используют обозначение $G =< a >$.

Предположим, что существует некоторое натуральное число n такое, что $a^n = e$. Тогда говорят, что элемент a имеет *конечный порядок* n, и, очевидно,

$$a^{n+1} = a,\ \ a^{n+2} = a^2,\ \ \ldots,\ a^{2n-1} = a^{n-1},\ \ a^{2n} = a^n = e,$$

$$a^{n-1} = a^n \cdot a^{-1} = e \cdot a^{-1} = a^{-1},$$

$$a^{n-2} = a^{-2},\ \ a^{n-n} = a^{-n} = (a^n)^{-1} = e^{-1} = e\ .$$

В этом случае можно считать, что циклическая группа содержит только элементы e, a, $a^2, \ldots, a^n$, и такую циклическую группу называют *конечной* (Card $G = n$). Если же для любого натурального n все степени a^n различны, то G называется *бесконечной* циклической группой.

Пример 2.14. Множество целых чисел $\boldsymbol{Z}$, снабженное традиционной операцией сложения, т.е. структура ($\boldsymbol{Z}$, + , 0), представляет со-

бой бесконечную циклическую абелеву группу, порожденную степенями элемента $a = 1$:

$Z = \{\ldots, 1-1-1-1,\ 1-1-1,\ 1-1,\ 1,\ 1+1,\ 1+1+1, \ldots\}$.

Пример 2.15. Рассмотрим множество вращений правильного треугольника вокруг точки O – центра треугольника. Пусть элемент φ_1 этого множества представляет собой поворот треугольника на угол 120^0 вокруг точки O против часовой стрелки. При таком повороте треугольник совмещается с исходным треугольником, но его вершины меняются местами (рис. 2.6).

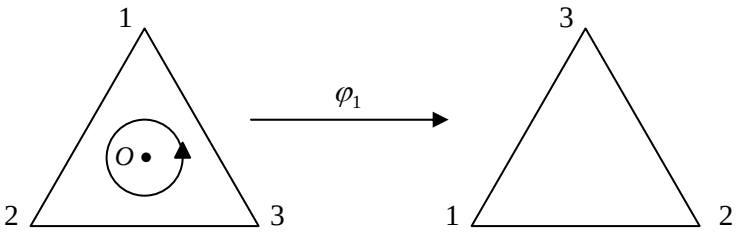


Рис. 2.6

Следующий поворот еще на 120^0 против часовой стрелки снова соответствует элементу φ_1 , но в то же время по отношению к исходному положению треугольника итоговый поворот φ_2 на 240^0 мы можем рассматривать как композицию двух последовательных поворотов на 120^0 : $\varphi_2 = \varphi_1 \circ \varphi_1 = \varphi_1^2$ (рис. 2.7).

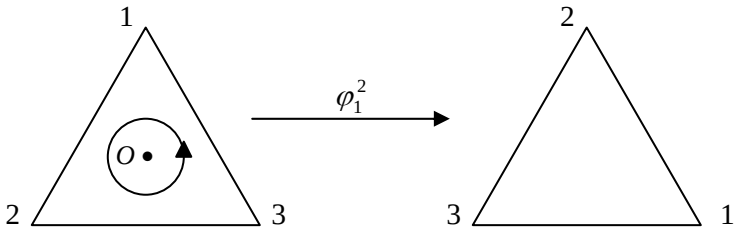


Рис. 2.7

Наконец, третий поворот еще на 120^0 возвращает треугольник в исходное положение, т.е. $\varphi_1^2 \circ \varphi_1 = \varphi_1^3 = e$; поэтому элемент φ_1 имеет конечный порядок 3.

В результате мы получили группу вращений правильного треугольника: $V_3 = \{e, \varphi_1, \varphi_1^2\}$. Очевидно, группа V_3 является циклической. Составим для нее таблицу Кэли (табл. 2.7) и запишем рядом для сравнения таблицу Кэли подгруппы H_4 симметрической группы S_3 (пример 2.13, табл. 2.6).

$\circ$	e	ψ_4	ψ_5
e	e	ψ_4	ψ_5
ψ_4	ψ_4	ψ_5	e
ψ_5	ψ_5	e	ψ_4

Табл. 2.6

$\circ$	e	φ_1	φ_1^2
e	e	φ_1	φ_1^2
φ_1	φ_1	φ_1^2	e
φ_1^2	φ_1^2	e	φ_1

Табл. 2.7

Нетрудно заметить, что обе таблицы совпадают с точностью до обозначений, и этот факт связан с понятием, которое математики называют *изоморфизмом*. Подробнее об изоморфизме групп мы расскажем в следующем разделе.

Пример 2.16. При обсуждении отношения эквивалентности и фактор-множества по заданному отношению мы вводили понятие сравнения по модулю 5 (глава I, пример 1.45, стр.66). Аддитивная группа классов вычетов по модулю m представляет собой важнейший пример циклической группы. Элементы a и b множества целых чисел $\boldsymbol{Z}$ находятся в отношении сравнения по модулю m (запись $a \equiv b (\mathrm{mod}\, m)$), если разность $a - b$ кратна числу m (делится на m без остатка). Сравнение по модулю m является отношением эквивалентности, фактор-множество $\boldsymbol{Z}/_{\equiv m}$ (другое обозначение – $\boldsymbol{Z}_m$) содержит m элементов: [0], [1], [2], …, $[m-2]$, $[m-1]$, каждый из которых называется *классом вычетов по модулю* m и представляет собой один из классов эквивалентности. На множестве классов вычетов $\boldsymbol{Z}_m = \{ [0], [1], [2], \ldots, [m-2], [m-1] \}$ зададим бинарную операцию «сложение по модулю m» следующим образом: $[n] \oplus [k] = [s]$, где s есть остаток от деления суммы чисел $n + k$ на m. Действие этой бинарной операции проиллюстрируем на примере фактор-множества $\boldsymbol{Z}_5 = \{ [0], [1], [2], [3], [4] \}$ (табл. 2.8). В этой таблице оперируют с классами вычетов, но для того, чтобы выраже-

ния были менее громоздкими, обычно квадратные скобки в обозначении классов «снимают».

$\oplus$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Табл. 2.8

Из таблицы 2.8 следует, что фактор-множество $\boldsymbol{Z}_5$, снабженное операцией сложения по модулю 5, является аддитивной группой. Кроме этого, группа $\boldsymbol{Z}_5$ – циклическая, поскольку порождается «степенями» элемента $[1]$:

$[1]^1 = [1]$,

$[1]^2 = [1] \oplus [1] = [2]$,

$[1]^3 = [1] \oplus [1] \oplus [1] = [2] \oplus [1] = [3]$,

$[1]^4 = [1] \oplus [1] \oplus [1] \oplus [1] = [3] \oplus [1] = [4]$,

$[1]^5 = [1] \oplus [1] \oplus [1] \oplus [1] \oplus [1] = [4] \oplus [1] = [0]$.

Пример 2.17. Отдельного внимания заслуживает аддитивная циклическая группа классов вычетов по модулю $m = 2$. В этом случае множество $\boldsymbol{Z}_2 = \{[0],[1]\}$, а таблица 2.9 представляет таблицу Кэли группы $\boldsymbol{Z}_2$.

$\oplus$	0	1
0	0	1
1	1	0

Табл. 2.9

Бинарная операция $\oplus$ на $\boldsymbol{Z}_2$ называется *сложением по модулю* 2 (или *двоичным сложением*). Отметим, что сложение по модулю 2 отличается от «логического» сложения – дизъюнкции. Это отличие хорошо заметно, если выписать рядом результаты двух операций (табл. 2.10 и 2.11).

a	b	$a \oplus b$
0	0	0
0	1	1
1	0	1
1	1	0

Табл. 2.10

p	q	$p \vee q$
0	0	0
0	1	1
1	0	1
1	1	1

Табл. 2.11.

Изоморфизм групп

Предположим, что заданы две группы $(G, *)$ и $(H, \circ)$.

Определение 2.11. Группы G и H называются *изоморфными* (обозначение $G \prec H$), если существует биективное отображение $f : G \to H$, «сохраняющее» групповую операцию, т.е.

$$f(x * y) = f(x) \circ f(y). \qquad (2.1)$$

Термин «изоморфны» идентичен словам «имеют одну и ту же форму», и поэтому можно ожидать, что изоморфные группы обладают одинаковыми алгебраическими свойствами. Нетрудно про-

верить, что изоморфизм является отношением эквивалентности на множестве групп, поэтому в абстрактной теории групп к изоморфным группам относятся как к совершенно одинаковым объектам. В результате можно исследовать свойства операций какой-либо алгебраической структуры, а затем распространить соответствующие выводы на изоморфную алгебраическую структуру.

Пример 2.18. Группа самосовмещений правильного треугольника T_3 изоморфна симметрической группе S_3. Напомним, что T_3 содержит шесть элементов – три вращения $\varphi_0, \varphi_1, \varphi_2$ вокруг центра треугольника на углы $0^0, 120^0$, 240^0 соответственно и три преобразования симметрии τ_1, τ_2, τ_3 относительно осей симметрии l_1, l_2, l_3 (рис. 2.8). Пронумеруем вершины треугольника и зададим биективное отображение $f : T_3 \to S_3$ следующим образом:

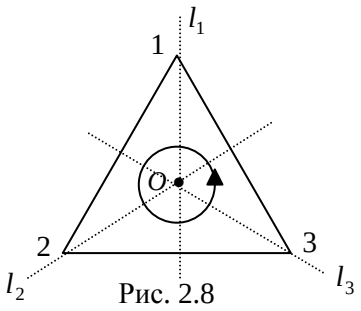


Рис. 2.8

$$\varphi_0 \to e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \tau_1 \to \psi_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \tau_2 \to \psi_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$

$$\tau_3 \to \psi_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \varphi_1 \to \psi_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \varphi_2 \to \psi_4 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Из геометрических соображений следует, что условие (2.1) выполняется, например,

$$f(\varphi_1 * \varphi_2) = f(\varphi_0) = e = \psi_5 \circ \psi_4 = f(\varphi_1) \circ f(\varphi_2).$$

В результате группы T_3 и S_3 изоморфны. Естественно, эти группы имеют одинаковые (с точностью до обозначений) таблицы Кэли – табл. 2.12 и 2.13.

Группа T_3

$*$	φ_0	τ_1	τ_2	τ_3	φ_2	φ_1
φ_0	φ_0	τ_1	τ_2	τ_3	φ_2	φ_1
τ_1	τ_1	φ_0	φ_1	φ_2	τ_3	τ_2
τ_2	τ_2	φ_2	φ_0	φ_1	τ_1	τ_3
τ_3	τ_3	φ_1	φ_2	φ_0	τ_2	τ_1
φ_2	φ_2	τ_2	τ_3	τ_1	φ_1	φ_0
φ_1	φ_1	τ_3	τ_1	τ_2	φ_0	φ_2

Табл. 2.12

Группа S_3

$\circ$	e	ψ_1	ψ_2	ψ_3	ψ_4	ψ_5
e	e	ψ_1	ψ_2	ψ_3	ψ_4	ψ_5
ψ_1	ψ_1	e	ψ_5	ψ_4	ψ_3	ψ_2
ψ_2	ψ_2	ψ_4	e	ψ_5	ψ_1	ψ_3
ψ_3	ψ_3	ψ_5	ψ_4	e	ψ_2	ψ_1
ψ_4	ψ_4	ψ_2	ψ_3	ψ_1	ψ_5	e
ψ_5	ψ_5	ψ_3	ψ_1	ψ_2	e	ψ_4

Табл. 2.13

Пример 2.19. Аддитивная группа классов вычетов $\boldsymbol{Z}_3$ по модулю 3 изоморфна циклической группе порядка 3, порожденной элементом a (сравните таблицы Кэли 2.14 и 2.15).

Группа $\boldsymbol{Z}_3$

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Табл. 2.14

Группа $G = < a >$

$*$	e	a	a^2
e	e	a	a^2
a	a	a^2	e
a^2	a^2	e	a

Табл. 2.15

Пример 2.20. Пусть $(\boldsymbol{R}_+, \cdot)$ есть мультипликативная группа положительных действительных чисел, снабженная обычной операцией умножения, а $(\boldsymbol{R}, +)$ – аддитивная группа всех действительных чисел. Биективное отображение

$$f : \boldsymbol{R}_+ \to \boldsymbol{R}, \quad f(x) = \ln x, \quad x \in \boldsymbol{R}_+$$

устанавливает изоморфизм двух групп, поскольку

$$f(x \cdot y) = \ln(x \cdot y) = \ln x + \ln y = f(x) + f(y).$$

Теперь мы перечислим некоторые свойства изоморфизма.

Пусть две группы $(G, *)$ и $(H, \circ)$ изоморфны.

1. При изоморфизме образом единичного элемента $e \in G$ является единичный элемент $\tilde{e} \in H$.
2. Для любого элемента $x \in G$ образ обратного элемента $f(x^{-1})$ является обратным к элементу $f(x) \in H$.

3. Обратное отображение $f^{-1}: H \to G$ также является изоморфизмом.

Докажем, например, свойства 1 и 2.

Доказательство свойства 1.

► Для любого элемента $x \in G$, $e * x = x$, поэтому $f(e * x) = f(x)$. В силу изоморфизма $f(e * x) = f(e) \circ f(x) = f(x)$, и, следовательно, элемент $f(e)$ является единичным элементом $\tilde{e}$ в группе H.◄

Доказательство свойства 2.

► Если $x * x^{-1} = e$, то $f(x * x^{-1}) = f(x) \circ f(x^{-1}) = \tilde{e}$, поэтому элемент $f(x^{-1})$ является обратным к элементу $f(x)$ в группе H.◄

Следующие две теоремы, которые мы приводим без доказательства, позволяют понять, почему понятие изоморфизма играет важную роль в теории групп.

Теорема 2.1. (Кэли). Любая конечная группа порядка n изоморфна некоторой подгруппе симметрической группы S_n.

Теорема 2.2. Любая циклическая группа порядка m изоморфна группе $\mathbf{Z}_m$ классов вычетов по модулю m.

С учетом того, что отношение изоморфизма есть отношение эквивалентности, можно считать, что все циклические группы одного и того же порядка изоморфны.

Кольца и поля

Определение 2.12. Пусть K есть непустое множество, на котором заданы две бинарные операции: + (сложение) и • (умножение), удовлетворяющие следующим условиям:

1) структура (K , +) является абелевой (коммутативной) группой;
2) структура (K , •) есть полугруппа;
3) операции сложения и умножения связаны законом дистрибутивности:

$$(a+b)\cdot c = a\cdot c + b\cdot c \quad \text{и} \quad c\cdot(a+b) = c\cdot a + c\cdot b$$

для любых $a,b,c \in K$.

Алгебраическая структура (K , + , •), подчиненная требованиям 1-3, называется *кольцом* . При этом структура (K , +) называется аддитивной группой кольца, а структура (K , •) называется его мультипликативной полугруппой.

Если (K , •) есть полугруппа с единицей (моноид), то кольцо называют *кольцом с единицей*.

Кольцо называется *коммутативным*[5], если $a\cdot b = b\cdot a$ для любых $a,b \in K$.

Пример 2.21. Структура ($\boldsymbol{Z}$, + , •) является коммутативным кольцом целых чисел с традиционными операциями сложения и умножения. Другой пример коммутативного кольца представляет кольцо

[5] В отличие от групп коммутативное кольцо не называют абелевым.

$m\boldsymbol{Z}$ целых чисел, кратных некоторому фиксированному числу m. Это кольцо коммутативно (без единицы, если $m>1$).

Пример 2.22. Пусть $M_n(\boldsymbol{R})$ есть множество всех квадратных матриц порядка n с вещественными элементами. Тогда структура $(M_n(\boldsymbol{R}),\ +,\ \bullet)$, где $+$ и $\bullet$ есть операции сложения и умножения матриц, представляет собой кольцо с единичной матрицей E в качестве единицы кольца. $M_n(\boldsymbol{R})$ называется *кольцом матриц порядка n над $\boldsymbol{R}$*. Это кольцо не является коммутативным.

Пример 2.23. Рассмотрим множество $\boldsymbol{Z}_m$ всех классов вычетов по модулю m:

$$\mathrm{Z}_m=\{[0],[1],\ldots,[m-1]\}.$$

Сумму и произведение элементов из $\boldsymbol{Z}_m$ определим как сложение и умножение по модулю m, т.е.

$$[n]\oplus[k]=[s],\qquad [n]\odot[k]=[l],[n]\oplus[k]=[s]$$

где s и l есть остатки от деления суммы $n+k$ и произведения $n\cdot k$ на m. Например, на множестве $\boldsymbol{Z}_4=\{[0],[1],[2],[3]\}$

$$[2]\oplus[3]=[1],\qquad [2]\odot[3]=[2],$$

а на множестве $\mathrm{Z}_7=\{[0],[1],[2],[3],[4],[5],[6]\}$

$$[3]\oplus[5]=[1],\quad [6]\oplus[1]=[0],\quad [6]\oplus[5]=[4],$$

$$[3]\odot[5]=[1],\quad [6]\odot[2]=[5],\quad [6]\odot[5]=[2].$$

Часто в указанных обозначениях (для упрощения формы записи) отказываются от кружочков в обозначениях операций и от квадрат-

ных скобок для классов вычетов. В этом случае множество элементов $\{0,1,\ldots,m\}$ называют *приведенной системой вычетов по модулю* m (за этим множеством сохраняют обозначение $\boldsymbol{Z}_m$), и в таких более простых обозначениях удобно записывать таблицы сумм и произведений элементов (табл. 2.16 – 2.21).

$Z_2 = \{0,1\}$

+	0	1
0	0	1
1	1	0

Табл. 2.16

•	0	1
0	0	0
1	0	1

Табл. 2.17

$Z_3 = \{0,1,2\}$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Табл. 2.18

•	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Табл. 2.19

$Z_4 = \{0,1,2,3\}$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Табл. 2.20

•	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Табл. 2.21

Отметим, что любая структура $(\boldsymbol{Z}_m, \oplus, \odot)$ является коммутативным кольцом с единицей.

Определение 2.13. Кольцо $(K, +, \cdot)$ называется *полем,* если выполняются следующие условия:

1) структура $(K, +, 0)$ – абелева группа;
2) структура $(K \setminus \{0\}, \cdot, 1)$ – коммутативная группа;
3) выполняется закон дистрибутивности

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

для любых $a, b, c \in K$.

Любое поле, по сути дела, представляет собой гибрид двух абелевых групп – аддитивной и мультипликативной, связанных законами дистрибутивности.

Среди широко известных полей следует отметить поле рациональных чисел $\boldsymbol{Q}$, поле действительных чисел $\boldsymbol{R}$, поле комплексных чисел $\boldsymbol{C}$.

В дискретной математике важнейшую роль играют *конечные поля,* т.е. поля, содержащие конечное число элементов. Структуру конечного поля описывает следующая теорема.

Теорема 2.3. Кольцо классов вычетов $(\mathbf{Z}_m, +, \cdot)$ тогда и только тогда является полем, когда m есть простое число.

Так, например, полю $\boldsymbol{Z}_5$ отвечают таблицы 2.22 и 2.23 сложения и умножения элементов.

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

Табл. 2.22

•	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Табл. 2.23

Из симметрии таблицы умножения элементов множества $\boldsymbol{Z}_5 \setminus \{0\}$ следует, что структура $(\boldsymbol{Z}_5 \setminus \{0\}, \bullet)$ действительно является абелевой группой: каждый из элементов множества $\boldsymbol{Z}_5 \setminus \{0\}$ имеет обратный, и операция умножения коммутативна.

В то же время, например, структура $(\boldsymbol{Z}_4, +, \bullet)$ полем не является. Достаточно посмотреть на таблицу 2.21 умножения элементов $\boldsymbol{Z}_4 \setminus \{0\}$ и заметить, что элемент 2 не имеет обратного элемента по умножению.

В заключение этого раздела отметим, что конечные поля $\boldsymbol{Z}_p$, где p - простое число, играют важную роль в теории передачи и кодирования информации. С помощью таких полей конструируют так называемые *коды*, исправляющие ошибки при передаче информации.