ГЛАВА 4

АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ НА МНОЖЕСТВАХ

Групповые по Бурбаки структуры на множествах чаще называют алгебраическими структурами (см., например, [43]), хотя понятие ***группа*** является более широким в сравнении с понятием ***алгебра***.

4.1. Внешние и внутренние законы композиции на множествах

Законом композиции или операций на множествах называют отображение произведений множеств в одно из множеств.

Так, сложение векторов $\bar{x}$ и $\bar{y}$ из множества A векторов трёхмерного пространства есть бинарная операция φ: $A \times A \to A$ ($\bar{x} + \bar{y} = \bar{z}$ - сложение по “правилу треугольника”), умножение вектора $\bar{x}$ на число α также является бинарной операцией ψ: $A \times \boldsymbol{R} \to A$, заданной формулой $\psi(\bar{x}, \alpha) = \alpha \times \bar{x}$. В первом случае *бинарная операция* называется *внутренней*, во втором случае говорят о *внешнем законе композиции*.

Свойства операций определяются аксиомами. Так, аксиомы унарной операции $\neg$ отрицание и бинарных отношений &,V, $\Rightarrow$ и $\Leftrightarrow$ (см. Глава 2, п. 2) записаны в форме истинностных таблиц. Внешний закон композиции всегда называют умножением, мы будем обозначать его символом $\circledast$, внутренние законы композиции называют и сложением, и умножением и обозначают символами $\oplus$ и $\otimes$, соответственно. Чем больше операций задано на множествах, тем богаче соответствующая этим операциям структура. Перечислим свойства и согласованность операций (см. Глава 2, п. 2).

1. *Ассоциативность*: $(a \otimes b) \otimes c = a \otimes (b \otimes c)$.

2. *Коммутативность*: $a \oplus b = b \oplus a$.

3. *Антикоммутативность*: $a \otimes b = -b \otimes a$.

4. *Дистрибутивность*: $\alpha \circledast (b \oplus c) = (\alpha \circledast b) \oplus (\alpha \circledast c)$.

5. Существование *нейтрального* относительно операции φ *элемента* e:

$$e \oplus a = a \;\; (0 + a = a), \;\; e \otimes b = b \;\; (1 \times b = b) \;\; e \circledast c = c \;\; (1 \times \bar{x} = \bar{x}).$$

6. Существование *обратного к элементу* a (*к элементу* b) относи-

тельно операции $\oplus$ (операции $\otimes$) *элемента* a^{-1}(*элемента* b^{-1}):

$$a \oplus a^{-1} = e(\overline{a} + (-\overline{a})) = \overline{0}\ b \otimes b^{-1} = e\ \ (b \cdot b^{-1}) = 1 .$$

Для аддитивных операций $\oplus$ нейтральный элемент e называют нулем, для мультипликативных операций $\otimes$– единицей. Для некоммутативных операций различают левый и правый нейтральные элементы.

4.2. Изоморфизм алгебраических структур

Пусть на множествах M и P заданы некоторые структуры, например с помощью внутренних бинарных операций $\otimes$ и $\oplus$, соответственно, т. е. $\otimes$: $M \times M \to M$ и $\oplus$: $P \times P \to P$. Множество со структурой мы будем обозначать соответствующей парой $(M, \otimes)$ и $(P, \oplus)$.

Определение 4.1. *Биекция* β: $M \to P$ *называется изоморфизмом структур* $(M, \otimes)$ *и* $(P, \oplus)$, *если из* $a \otimes b = c$ *на множестве M следует* $\beta(a) \oplus \beta(b) = \beta(c)$ *на множестве P, если же множество M совпадает с множеством P, то изоморфизм* β *называется автоморфизмом.*

При этом также говорят, что структуры (M, $\otimes$) и (P, $\oplus$) изоморфны. Отношение изоморфности на множестве $\{(M, \varphi)\}$ структур обладает свойствами (ср. п. 6 , Глава 3) рефлексивности, симметричности и транзитивности, которые гарантируются биекциями соответствующих множеств, и потому это отношение есть отношение эквивалентности. Теории изоморфных структур совпадают и не зависят ни от конкретной природы элементов изоморфных множеств, ни от способов задания структуры на множествах.

Пример 4.1. Пусть $\boldsymbol{R}^+ \stackrel{\Delta}{=} \{x\text{: } x \in \boldsymbol{R},\ x > 0\}$, $a \oplus b \stackrel{\Delta}{=} a + b$ и $a \otimes b \stackrel{\Delta}{=} a \times b$.

Тогда β: $\boldsymbol{R}^+ \to \boldsymbol{R}$, где $\beta(x) \stackrel{\Delta}{=} \ln x$, есть изоморфизм, так что структуры ($\boldsymbol{R}^+$, $\times$) и ($\boldsymbol{R}$, +) изоморфны. Этот изоморфизм позволяет операцию умножения чисел заменить менее *трудоемкой* операцией сложения их логарифмов. Подробности см. в [5], [27] и в [45].

4.3. Структура группы на множестве

Определение 4.2. *Группой называется множество* G *с такой бинарной операцией* $\otimes$: $G \times G \to G$, *что*

1) $\otimes$ *ассоциативна*: $a \otimes (b \otimes c) = (a \otimes b) \otimes c$,

2) *существует* $e \in G$ (*нейтральный элемент по отношению к опе-*

рации $\otimes$): $\forall g \in G \;\; e \otimes g = g \otimes e = g$,

3) $\forall a, a \in G, \exists b \in G$: $a \otimes b = b \otimes a = e$, *элемент b называют обратным* (*противоположным*) *элементом элементу a относительно операции* $\otimes$.

Пример 4.2. Множество $\boldsymbol{Z}$ целых чисел с операцией сложения образует аддитивную коммутативную группу, при этом нейтральным элементом служит число 0, а обратным элементом для $z \in \boldsymbol{Z}$ является противоположное число $-z$: $-z+z=0$.

Упражнение 4.1. Показать, что если в определении группы постулировать существование таких левого и правого (e и e^*) нейтральных элементов и левого и правого обратных (b и b^*) элементов к элементу a, что $e \otimes a = a \otimes e^* = a$ и $b \otimes a = a \otimes b^* = e$, то $e = e^*$ и $b = b^*$.

Упражнение 4.2. Показать, что множество $\boldsymbol{R}^+$ положительных чисел с операцией $\otimes$, определяемой формулой $a \otimes b = a^b$, не образует группу.

Упражнение 4.3. Показать, что множество *G* параллельных переносов плоскости и множество ϕ вращений плоскости с центром в некоторой точке О образуют группу параллельных переносов и, соответственно, группу вращений.

Замкнутость групповой операции $\otimes$ группы *G* определяется тем, что:

1) отображение $\otimes: G \times G \to G$ задано для всех пар $(a,\, b) \in G \times G$ и, кроме того,

2) это отображение есть сюръекция, так что в группе *G* уравнение $a \otimes x = b$ разрешимо при любых *a* и *b* из *G*.

$$\bullet\; a \otimes x = b \Rightarrow a^{-1} \otimes (a \otimes x) = a^{-1} \otimes b \Rightarrow (a^{-1} \otimes a) \otimes x = a^{-1} \otimes b \Rightarrow$$
$$\Rightarrow e \otimes x = a^{-1} \otimes b \Rightarrow x = a^{-1} \otimes b. \blacksquare$$

Определение 4.3. *Подмножество* $\widetilde{G}$ *группы G, являющееся группой с законом композиции* $\otimes$ *группы G, называется подгруппой группы* G.

Так, в группе ϕ поворотов плоскости множество $\phi_k = \{\varphi_{k,m}\}$, $k \in \boldsymbol{Z}$, где $\varphi_{k,m}$ – поворот плоскости на угол $\alpha_{k,\,m} = \dfrac{\pi m}{k}$, $m \in \boldsymbol{Z}$, является подгруппой группы ϕ. Нейтральным элементом здесь является $\varphi_{k,0}$ – поворот плоскости на 0 радиан, обратным элементом для $\varphi_{k,m}$ будет поворот $\varphi_{k,-m}$ и элемент $\varphi_{k,p} \otimes \varphi_{k,q} = \varphi_{k,p+q}$ есть поворот на угол $\alpha_{k,p} + \alpha_{k,q} = \dfrac{\pi(p+q)}{k}$.

Очевидно, что всякая подгруппа $\widetilde{G}$ группы G содержит нейтральный элемент e группы G и $\forall a \in \widetilde{G}\ \exists a^{-1} \in \widetilde{G}$. Назовем три подгруппы:

1) $\widetilde{G}_0 \triangleq \{e\}$,

2) $\widetilde{G}_1 \triangleq \{e, a\}$, где $a \otimes a = e$, т. е. $a^{-1} = a$,

3) $\widetilde{G}_n \triangleq \{e, a_1, ..., a_n\}$, где $a_k = a_{k-1} \otimes a_1$, $k \le n$, $a_n \otimes a_1 = e \triangleq a_0$.

Группа $\widetilde{G}_n$ называется циклической группой, порождённой элементом a_1, для элементов a_p и a_q такой группы

$$a_p \otimes a_q = a_r, \text{ где } p+q \equiv r \bmod(n+1) \text{ и } (a_p)^{-1} = a_{n+1-p}.$$

Конкретной реализацией группы $\widetilde{G}_1$ является множество $\{1, -1\}$, где $e \triangleq 1$, $a \triangleq -1$ и законом композиции служит умножение из множества $\boldsymbol{R}$: $(-1) \otimes 1 \triangleq 1 \times (-1) = -1$.

Циклической группой $\widetilde{G}_n$ является множество

$$Z_n = \{\{m_k\} : m_k \equiv k(\bmod n),\ 0 \le k \le n-1,\ m_k \in \boldsymbol{Z}\},\ n \ge 2\},$$

классов $\{m_k\}$ эквивалентности по модулю числа n во множестве $\boldsymbol{Z}$ целых чисел, когда закон композиции $\otimes$ группы Z_n определяется формулой $k \triangleq p \otimes q \triangleq (p+q) \equiv k(\bmod n)$, $p, q \in \boldsymbol{Z}$.

При этом по определению $m_k \otimes m_s \equiv (k+c)(\bmod n)$ и аддитивной единицей, нулём группы, служит класс $\{m_0\} = \{0, n, 2n, ...\}$ (см. Пример 3.4, Глава 3).

Очевидно, что не каждая группа G имеет циклические подгруппы.

В качестве упражнений читателю мы предлагаем проверить следующие утверждения:

1. Если G_1 и G_2 являются подгруппами группы G, то подмножество $G_1 \cap G_2$ также является подгруппой.

2. Все подгруппы данной группы G пересекаются по подгруппе $G_0 = \{e\}$.

Понятие подгруппы позволяет изучать свойства группы G на некоторой, не слишком малой, её подгруппе. Но следует заметить, что если G группа, то множество $G \setminus \{a\}$, $a \in G$, уже группой не является, если при этом $a \neq a^{-1}$. Подробности см. в [27], [43], [45], [57], [82] и др.

4.4. Кольца и поля

Структура группы не позволяет описать даже простейшие во многих математических дисциплинах *линейные операции*, т. е. отображение $l: M \times A \to M$ со свойствами:

$$l(x, \alpha + \beta) = l(x, \alpha) \oplus l(x, \beta) \text{ и } l(x \oplus y, \alpha) = l(x, \alpha) \oplus l(y, \alpha).$$

Здесь $\oplus$ и $+$ суть знаки законов композиции в M и в A, соответственно.

Определение 4.4. *Кольцом называется коммутативная группа К с операцией* $\oplus$, *если на ней определена вторая бинарная операция* $\otimes$: $K \times K \to K$ *и операции* $\oplus$ *и* $\otimes$ *согласованы дистрибутивностью*:

$$a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c),\ (b \oplus c) \otimes a = (b \otimes a) \oplus (c \otimes a).$$

Кольцо K называется коммутативным, если операция $\otimes$ коммутативна, и кольцом с единицей, если в K существует нейтральный элемент относительно второй операции $\otimes$.

Операции $\oplus$ и $\otimes$ обычно называют сложением и, соответственно, умножением, нейтральный элемент относительно $\oplus$ обозначают через 0 и называют нулём, обратный для a элемент обозначают символом $-a$ и называют противоположным a, нейтральный элемент относительно операции $\otimes$ называют единицей.

Ближайший пример – множество $\boldsymbol{Z}$ целых чисел с операциями $\times$ и $+$ есть коммутативное кольцо с единицей. Второй пример некоммутативного кольца с единицей даёт множество $K_n=\{A,B,C,...\}$ квадратных матриц порядка n.

Пример 4.3. Множество $K_2=\{A,B,C,...\}$ квадратных матриц порядка 2 (при n=2) образует некоммутативное кольцо с единицей:

$$B \triangleq (b_{ij}) \triangleq \begin{pmatrix} b_{11} b_{12} \\ b_{21} b_{22} \end{pmatrix},\ 0 \triangleq \begin{pmatrix} 0\,0 \\ 0\,0 \end{pmatrix},\ e \triangleq E \triangleq \begin{pmatrix} 1\,0 \\ 0\,1 \end{pmatrix},$$

$$A \oplus B = (a_{ij}) \oplus (b_{ij}) \triangleq \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix},$$

$$A \otimes B = (a_{ij}) \otimes (b_{ij}) \triangleq \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}.$$

Здесь предполагается, что элементы a_{ij}, b_{ij}, ... матриц A, B,... из кольца K_n сами являются элементами некоторого кольца K_0 с операциями + и × $(b \times a = a \times b)$, и если K_0 =$\boldsymbol{Z}$, то K_1=$\boldsymbol{Z}$. Так что кольцо K_n квадратных матриц порядка n есть обобщение кольца $\boldsymbol{Z}$ целых чисел.

Пример 4.4. Интересный пример кольца даёт множество $\boldsymbol{Z}$ целых чисел, у которого операции $\oplus$ и $\otimes$ определены как сложение и умножение по модулю числа p. Например, при p=6 (см. Пример 3.4 Главы 3) $s \equiv k(\mathrm{mod}\, 6)$ означает, что $\exists m \in \boldsymbol{Z}: \left(\frac{s}{6}\right) = m + \left(\frac{k}{6}\right)$, где $0 \le k \le 5$. В этом кольце при $a \otimes b = 0$ не всегда $q \equiv a(\mathrm{mod}\, 6) \cdot p \equiv b(\mathrm{mod}\, 6) = 0$. Например, $3 \otimes 8 = 0$, ибо $3 \cdot 8 = 24 \equiv 0(\mathrm{mod}\, 6)$ в то время как $3 \equiv 3(\mathrm{mod}\, 6)$, $8 \equiv 2(\mathrm{mod}\, 6)$ и $3 \cdot 2 = 6$.

Ненулевые элементы p и q кольца K называются делителями нуля, если $p \otimes q = 0$.

Упражнение 4.4. Показать, что в кольце K без делителей нуля равенство $a \otimes b = a \otimes c$ имплицирует равенство $b = c$ (здесь $a \ne 0$).

Введём ещё одну алгебраическую структуру на M, необходимую нам для описания (в Главе 5) множества $\boldsymbol{R}$ действительных чисел.

Определение 4.5. *Коммутативное кольцо F с единицей называется полем, если для* $\forall a \in F \setminus \{0\}$ *существует в F такой элемент b, обозначаемый через* a^{-1}, *что* $a \otimes b = 1$.

Так что в поле F уравнение $a \otimes x = b$ разрешимо для всех b и $a \ne 0$ (во множестве $\boldsymbol{Z}$, например, уравнение $ax = b$ не разрешимо при b=1 и $a \ne 1$).

Примеры поля дают множества: $\boldsymbol{Q}$ – рациональных чисел, $\boldsymbol{R}$ – действительных чисел, $\boldsymbol{C}$ – комплексных чисел.

Упражнение 4.5. Показать, что множество $P(A)$ всех подмножеств множества A с операциями $\cup$ и $\cap$ в качестве $\oplus$ и $\otimes$, соответственно, не образует поля.

Пример 4.5. Интересный пример поля даёт множество Z_p целых чисел, имеющее в качестве операций $\oplus$ и $\otimes$ сложение и умножение по модулю простого числа *p*. Здесь, например, при $p = 3$ равенство $2 \otimes x = 1$ означает, что $2 \times x \equiv 1(\mathrm{mod}\,3)$, и поэтому

$$2 \cdot \left(\frac{x}{3}\right) = z + \left(\frac{1}{3}\right), \text{ т. е. } x = 0{,}5 \cdot (3z + 1) \text{ и } x \in \boldsymbol{Z} \text{ при нечётном } z.$$

Упражнение 4.6. Показать на примере q=4, что множество Z_q не образует поля, если q не является простым числом.

Последний пример и упражнения оправдывают следующие два понятия. Число n называют аддитивным порядком ненулевого элемента a поля F, если $a \otimes n = 0$ и $\forall r: 0 < r < n \ \ a \otimes r \neq 0,\ \ n, r \in \boldsymbol{N}$.

Определение 4.6. *Говорят, что поле F имеет характеристику n, если все ненулевые элементы поля F имеют аддитивный порядок n, в противном случае говорят, что поле имеет характеристику* 0.

Так, например, поле $\boldsymbol{Q}$ рациональных чисел имеет характеристику 0.

Общее утверждение таково: поле характеристики 0 бесконечно, и характеристика каждого конечного поля есть простое число p.

Структура поля на множестве M позволяет ввести отношение порядка на M, то есть упорядочить поле F, введя следующее ниже определение.

Определение 4.7. *Поле F называется упорядоченным, если оно содержит такое непустое подмножество* F^**, замкнутое относительно операций сложения и умножения, что*

$$\forall x \in F\backslash\{0\} \text{ либо } x \in F^*, \text{ либо } -x \in F^*.$$

Если $1 \in F^*$, то F^* называется множеством всех положительных элементов из F. При этом с изложением Главы 3 более согласуется условие $0 \notin F^*$ (по Определению 4.7 допустимо и $0 \in F^*$). Далее пишем a>0, если $a \in F^*$ и b<0, если в $b \in F\backslash(\{0\} \cup F^*)$, т. е. если $-b \in F^*$.

Теперь можно показать, что отношение < асимметрично и транзитивно, т. е. является отношением порядка на F.

Замечание 4.1. Из аксиом поля F не следует по необходимости существование подмножества F^* из Определения 4.7.

Упражнение 4.7. Записать аксиомы поля.