Глава 1

Алгебраические структуры

Когда вы знакомитесь с новыми людьми, вы прежде всего запоминаете их имена и внешность. После этого, встречаясь с ними в разных ситуациях, вы постепенно узнаете их лучше и некоторые из них, может быть, становятся вашими друзьями.

В первой главе состоится лишь внешнее знакомство читателя со многими из алгебраических структур, рассматриваемых в этой книге. Более глубокое их понимание будет приходить в процессе дальнейшего чтения книги и решения задач.

§ 1. Введение

Если вообще можно четко определить предмет алгебры, то это изучение алгебраических структур — множеств с определенными в них операциями. Под операцией в множестве M понимается любое отображение

$$M \times M \to M,$$

т. е. правило, по которому из любых двух элементов множества M получается некоторый элемент этого же множества. Элементами множества M могут быть как числа, так и объекты другого рода.

Хорошо известными и важными примерами алгебраических структур являются следующие числовые множества с операциями сложения и умножения:

$\mathbb{N}$ — множество натуральных чисел,

$\mathbb{Z}$ — множество всех целых чисел,

$\mathbb{Z}_+ = \mathbb{N} \cup \{0\}$ — множество неотрицательных целых чисел,

$\mathbb{Q}$ — множество рациональных чисел,

$\mathbb{R}$ — множество всех вещественных (= действительных) чисел,

$\mathbb{R}_+$ — множество неотрицательных вещественных чисел.

Подчеркнем, что операции сложения и умножения определены далеко не на всяком числовом множестве. Например, в множестве отрицательных чисел не определена операция умножения, так как

произведение двух отрицательных чисел является положительным числом. В множестве иррациональных чисел не определены ни сложение, ни умножение, так как сумма и произведение двух иррациональных чисел могут быть рациональными.

Приведем примеры алгебраических структур, состоящих не из чисел.

Пример 1. Пусть M, N, P — какие-то множества и

$$f: N \to M, \quad g: P \to N$$

— какие-то отображения. *Произведением*, или *композицией*, *отображений* f и g называется отображение

$$fg: P \to M,$$

определяемое формулой

$$(fg)(a) = f(g(a)) \quad \forall a \in P,$$

т. е. результат последовательного выполнения сначала отображения g, а потом f. (Обычно, если это не может привести к недоразумению, произведение отображений записывают без какого-либо специального знака, т. е. пишут просто fg: ср. обозначение $\ln \sin x$ в анализе.) В частности, при $M = N = P$ мы получаем таким образом операцию на множестве всех отображений множества M в себя. Эта операция дает много важных примеров алгебраических структур, называемых группами. Так, например, согласно аксиоматике евклидовой геометрии, произведение двух движений плоскости есть также движение. Рассматривая в множестве всех движений плоскости операцию умножения, мы получаем алгебраическую структуру, называемую группой движений плоскости.

Пример 2. Множество векторов пространства с операциями сложения и векторного умножения является примером алгебраической структуры с двумя операциями. Кстати, отметим, что скалярное умножение векторов не является операцией в определенном выше смысле, так как его результат не есть элемент того же множества. Подобные более общие операции также рассматриваются в алгебре, но мы пока не будем об этом думать.

Все приведенные выше примеры являются естественными в том смысле, что они были открыты в результате изучения реального мира и внутреннего развития математики. В принципе можно рассматривать любые операции в любых множествах. Например, можно

рассматривать операцию в множестве $\mathbb{Z}_+$, ставящую в соответствие любым двум числам число совпадающих цифр в их десятичной записи. Однако лишь немногие алгебраические структуры представляют реальный интерес.

Следует уточнить, что алгебраиста интересуют только те свойства алгебраических структур и составляющих их элементов, которые могут быть выражены в терминах заданных операций. Этот подход находит свое выражение в понятии изоморфизма.

Определение 1. Пусть M — множество с операцией $\circ$, а N — множество с операцией $*$. Алгебраические структуры $(M, \circ)$ и $(N, *)$ называются *изоморфными*, если существует такое биективное отображение

$$f : M \to N,$$

что

$$f(a \circ b) = f(a) * f(b)$$

для любых $a, b \in M$. В этом случае пишут $(M, \circ) \simeq (N, *)$. Само отображение f называется *изоморфизмом* структур $(M, \circ)$ и $(N, *)$.

Аналогичным образом определяется изоморфизм алгебраических структур с двумя или бóльшим числом операций.

Пример 3. Отображение

$$a \mapsto 2^a$$

является изоморфизмом множества всех вещественных чисел с операцией сложения и множества положительных чисел с операцией умножения, поскольку

$$2^{a+b} = 2^a 2^b.$$

Вместо основания 2 можно было бы взять любое положительное основание, отличное от 1. Это показывает, что между изоморфными алгебраическими структурами может существовать много различных изоморфизмов.

Пример 4. Пусть V — множество векторов плоскости, а T — множество параллельных переносов. Для любого вектора a обозначим через t_a параллельный перенос на вектор a. (Если $a = 0$, то t_a — это тождественное преобразование.) Легко видеть, что

$$t_a \circ t_b = t_{a+b},$$

где $\circ$ обозначает умножение (композицию) параллельных переносов, а $+$ обозначает сложение векторов (определяемое по прави-

лу параллелограмма). Следовательно, отображение $a \mapsto t_a$ является изоморфизмом алгебраических структур $(V, +)$ и $(T, \circ)$.

Ясно, что если две алгебраические структуры изоморфны, то любое утверждение, формулируемое только в терминах заданных операций, будет справедливым в одной из этих структур тогда и только тогда, когда оно справедливо в другой.

Например, операция $\circ$ в множестве M называется *коммутативной*, если

$$a \circ b = b \circ a$$

для любых $a, b \in M$. Если структура $(M, \circ)$ изоморфна структуре $(N, *)$ и операция $\circ$ в множестве M коммутативна, то и операция $*$ в множестве N коммутативна.

Таким образом, в принципе все равно, какую из изоморфных друг другу алгебраических структур изучать: все они являются различными моделями одного и того же объекта. Однако выбор модели может оказаться небезразличным для фактического решения какой-либо задачи. Определенная модель может представить для этого наибольшее удобство. Например, если какая-то модель имеет геометрический характер, то она позволяет применить геометрические методы.

§ 2. Абелевы группы

Сложение вещественных чисел обладает следующими свойствами:

(С1) $a + b = b + a$ (коммутативность);

(С2) $(a + b) + c = a + (b + c)$ (ассоциативность);

(С3) $a + 0 = a$;

(С4) $a + (-a) = 0$.

Из этих свойств чисто логическим путем могут быть получены и другие свойства, например, наличие операции вычитания, обратной к сложению. Это означает, что для любых a, b уравнение

$$x + a = b$$

имеет единственное решение. Докажем, что это так. Если c — решение данного уравнения, т. е. $c + a = b$, то

$$(c + a) + (-a) = b + (-a).$$

Пользуясь свойствами (С2)—(С4), получаем

$$(c+a)+(-a)=c+(a+(-a))=c+0=c.$$

Таким образом,

$$c=b+(-a).$$

Это показывает, что если решение существует, то оно единственно и равно $b+(-a)$. С другой стороны, подстановка $x=b+(-a)$ в рассматриваемое уравнение показывает, что $b+(-a)$ действительно является решением:

$$(b+(-a))+a=b+((-a)+a)=b+(a+(-a))=b+0=b.$$

Умножение вещественных чисел обладает аналогичными свойствами:

(У1) $ab=ba$ (коммутативность);

(У2) $(ab)c=a(bc)$ (ассоциативность);

(У3) $a1=a$;

(У4) $aa^{-1}=1$ при $a\neq 0$.

Свойства (У1)—(У4) лишь формой записи отличаются от свойств (С1)—(С4), с единственной оговоркой, что в (У4) мы предполагаем, что $a\neq 0$, в то время как в (С4) никаких ограничений на a нет. Поэтому приведенный выше вывод из свойств (С1)—(С4) наличия операции вычитания, будучи переведен на язык умножения, даст вывод из свойств (У1)—(У4) наличия операции деления, обратной к умножению. Более точно, таким путем доказывается, что для любого $a\neq 0$ и любого b уравнение $xa=b$ имеет единственное решение, равное ba^{-1}.

Все эти рассуждения приведены здесь не для того, чтобы читатель узнал что-либо новое о вещественных числах, а чтобы подвести его к важной для алгебры идее. Эта идея есть аксиоматический метод в алгебре. Он состоит в одновременном изучении целых классов алгебраических структур, выделяемых теми или иными аксиомами, представляющими собой какие-то свойства операций в этих структурах. При этом совершенно не важно, как в каждом конкретном случае эти операции определяются. Коль скоро выполнены аксиомы, справедлива и любая теорема, полученная логическим путем из этих аксиом.

Конечно, лишь немногие системы аксиом действительно интересны. Невозможно придумать «из головы» такую систему аксиом,

которая привела бы к содержательной теории. Все системы аксиом, рассматриваемые в современной алгебре, имеют длительную историю и являются результатом анализа алгебраических структур, возникших естественным путем. Таковы системы аксиом группы, кольца, поля, векторного пространства и другие, с которыми читатель познакомится в этом курсе.

Свойства (С1)—(С4), а также (У1)—(У4) являются по сути дела системой аксиом абелевой группы. Перед тем как привести точные формулировки этих аксиом, скажем несколько слов о терминологии. Названия и обозначения операций в алгебраических структурах не имеют принципиального значения, однако чаще всего они называются сложением или умножением и обозначаются соответствующим образом. Это позволяет использовать разработанную терминологию и систему обозначений, относящиеся к операциям над вещественными числами, а также вызывает полезные ассоциации.

Приведем вначале определение абелевой группы, использующее язык сложения.

Определение 1. (*Аддитивной*) *абелевой группой* называют множество A с операцией сложения, обладающей следующими свойствами:

1) $a+b=b+a$ для любых $a, b \in A$ (*коммутативность*);

2) $(a+b)+c=a+(b+c)$ для любых $a, b, c \in A$ (*ассоциативность*);

3) в A существует такой элемент 0 (*нуль*), что $a+0=a$ для любого $a \in A$;

4) для любого элемента $a \in A$ существует такой элемент $-a \in A$ (*противоположный элемент*), что $a+(-a)=0$.

Выведем некоторые простейшие следствия из этих аксиом.

1) Нуль единствен. В самом деле, пусть 0_1 и 0_2 — два нуля. Тогда

$$0_1 = 0_1 + 0_2 = 0_2.$$

2) Противоположный элемент единствен. В самом деле, пусть $(-a)_1$ и $(-a)_2$ — два элемента, противоположных a. Тогда

$$(-a)_1 = (-a)_1 + (a + (-a)_2) = ((-a)_1 + a) + (-a)_2 = (-a)_2.$$

3) Для любых a, b уравнение $x+a=b$ имеет единственное решение, равное $b+(-a)$. Доказательство см. выше. Это решение называется *разностью* элементов b и a и обозначается $b-a$.

Из свойства ассоциативности нетрудно вывести (попробуйте сделать это), что сумма произвольного числа (а не только трех) элементов не зависит от расстановки скобок. Пользуясь этим, скобки обычно вообще опускают.

Пример 1. Числовые множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ являются абелевыми группами относительно обычной операции сложения.

Пример 2. Множество векторов (плоскости или пространства) является абелевой группой относительно обычного сложения векторов.

Пример 3. Последовательность из n чисел назовем *строкой* длины n. Множество всех строк длины n, составленных из вещественных чисел, обозначим через $\mathbb{R}^n$. Определим сложение строк по правилу

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

Очевидно, что множество $\mathbb{R}^n$ является абелевой группой относительно этой операции. Ее нулем служит *нулевая строка*

$$0 = (0, 0, \ldots, 0).$$

Пример 4. Множество всех функций, определенных на заданном подмножестве числовой прямой, является абелевой группой относительно обычного сложения функций.

Приведем теперь определение абелевой группы, использующее язык умножения.

Определение 1′. (*Мультипликативной*) *абелевой группой* называют множество A с операцией умножения, обладающей следующими свойствами:

1) $ab = ba$ для любых $a, b \in A$ (*коммутативность*);

2) $(ab)c = a(bc)$ для любых $a, b, c \in A$ (*ассоциативность*);

3) в A существует такой элемент e (*единица*), что $ae = a$ для любого $a \in A$;

4) для любого элемента $a \in A$ существует такой элемент $a^{-1} \in A$ (*обратный элемент*), что $aa^{-1} = e$.

Единица мультипликативной абелевой группы иногда обозначается символом 1.

Простейшие следствия аксиом абелевой группы, полученные выше на аддитивном языке, на мультипликативном языке выглядят следующим образом.

1) Единица единственна.

2) Обратный элемент единствен.

3) Для любых a, b уравнение $xa = b$ имеет единственное решение, равное ba^{-1}. Оно называется *частным* от деления b на a (или *отношением* элементов b и a) и обозначается $\frac{b}{a}$ (или b/a).

Пример 5. Числовые множества $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$ и $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ являются абелевыми группами относительно обычной операции умножения.

В дальнейшем мы познакомимся с общим понятием группы (не обязательно абелевой), которое не включает требования коммутативности операции.

Читатель, наверное, заметил, что некоторые из рассмотренных выше абелевых групп содержатся в других, причем операция в «маленькой» группе определяется так же, как в «большой». Это приводит нас к понятию подгруппы.

Вообще, пусть M — множество с операцией $\circ$ и N — какое-либо его подмножество. Говорят, что N *замкнуто относительно операции* $\circ$, если

$$a, b \in N \;\Rightarrow\; a \circ b \in N.$$

В этом случае операция $\circ$ определена в множестве N и превращает его в некоторую алгебраическую структуру. Если операция $\circ$ в M обладает каким-то свойством, имеющим характер тождественного соотношения (например, свойством коммутативности или ассоциативности), то она, очевидно, обладает этим свойством и в N. Однако другие свойства операции $\circ$ могут не наследоваться подмножеством N.

Так, подмножество аддитивной абелевой группы, замкнутое относительно сложения, не обязано быть абелевой группой, так как оно может не содержать нуля или элемента, противоположного какому-либо его элементу. Например, подмножество $\mathbb{Z}_+$ замкнуто относительно сложения в абелевой группе $\mathbb{Z}$, но не является абелевой группой (и вообще группой), так как не содержит противоположного элемента ни к одному своему элементу, кроме нуля.

Определение 2. Подмножество B аддитивной абелевой группы A называется *подгруппой*, если

1) B замкнуто относительно сложения;

2) $a \in B \Rightarrow -a \in B$;

3) $0 \in B$.

Замечание 1. Легко видеть, что если B непусто, то из первых двух условий вытекает третье. Поэтому третье условие может быть заменено условием непустоты.

Очевидно, что всякая подгруппа аддитивной абелевой группы сама является абелевой группой относительно той же операции.

Пример 6. В аддитивной группе $\mathbb{R}$ имеется следующая цепочка подгрупп:

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}.$$

Пример 7. В аддитивной группе векторов пространства множество векторов, параллельных заданной плоскости или прямой, является подгруппой.

В любой аддитивной абелевой группе имеются две «тривиальные» подгруппы: вся группа и подгруппа, состоящая только из нуля.

Задача 1. Доказать, что всякая подгруппа группы $\mathbb{Z}$ имеет вид $n\mathbb{Z}$, где $n \in \mathbb{Z}_+$ (решение этой задачи можно найти в § 4.3).

Приведем мультипликативный вариант предыдущего определения.

Определение 2. Подмножество B мультипликативной абелевой группы A называется *подгруппой*, если

1) B замкнуто относительно умножения;
2) $a \in B \Rightarrow a^{-1} \in B$;
3) $e \in B$.

Пример 8. В группе $\mathbb{R}^*$ имеется следующая цепочка подгрупп:

$$\{\pm 1\} \subset \mathbb{Q}^* \subset \mathbb{R}^*.$$

§ 3. Кольца и поля

В отличие от групп ко́льца и поля́ — это алгебраические структуры с двумя операциями, называемыми обычно сложением и умножением. Их аксиомы, как и аксиомы абелевой группы, подсказаны свойствами операций над вещественными числами. При этом аксиомы кольца — это разумный минимум требований относительно свойств операций, позволяющий охватить и другие важные примеры алгебраических структур, из которых мы пока можем привести только уже упоминавшееся множество векторов пространства с операциями сложения и векторного умножения.

Определение 1. *Кольцом* называется множество K с операциями сложения и умножения, обладающими следующими свойствами:

1) относительно сложения K есть абелева группа (называемая *аддитивной группой кольца* K);

2) $a(b+c)=ab+ac$ и $(a+b)c=ac+bc$ для любых $a,b,c\in K$ (*дистрибутивность умножения относительно сложения*).

Выведем некоторые следствия аксиом кольца, не входящие в число следствий аксиом аддитивной абелевой группы, перечисленных в § 2.

1) $a0=0a=0$ для любого $a\in K$. В самом деле, пусть $a0=b$. Тогда

$$b+b=a0+a0=a(0+0)=a0=b,$$

откуда

$$b=b-b=0.$$

Аналогично доказывается, что $0a=0$.

2) $a(-b)=(-a)b=-ab$ для любых $a,b\in K$. В самом деле,

$$ab+a(-b)=a(b+(-b))=a0=0$$

и, аналогично, $ab+(-a)b=0$.

3) $a(b-c)=ab-ac$ и $(a-b)c=ac-bc$ для любых $a,b,c\in K$. В самом деле,

$$a(b-c)+ac=a(b-c+c)=ab$$

и, аналогично, $(a-b)c+bc=ac$.

Кольцо K называется *коммутативным*, если умножение в нем коммутативно, т. е.

$$ab=ba\quad\forall a,b,$$

и *ассоциативным*, если умножение в нем ассоциативно, т. е.

$$(ab)c=a(bc)\quad\forall a,b,c.$$

Элемент 1 кольца называется *единицей*, если

$$a1=1a=a\quad\forall a.$$

Так же, как в случае мультипликативной абелевой группы, доказывается, что в кольце не может быть двух различных единиц (но может не быть ни одной).

Замечание 1. Если $1 = 0$, то для любого a имеем

$$a = a1 = a0 = 0,$$

т. е. кольцо состоит из одного нуля. Таким образом, если кольцо содержит более одного элемента, то $1 \neq 0$.

Замечание 2. При наличии коммутативности из двух тождеств дистрибутивности, входящих в определение кольца, можно оставить лишь одно. Аналогичное замечание относится к определению единицы.

Пример 1. Числовые множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ являются коммутативными ассоциативными кольцами с единицей относительно обычных операций сложения и умножения.

Пример 2. Множество $2\mathbb{Z}$ четных чисел является коммутативным ассоциативным кольцом без единицы.

Пример 3. Множество всех функций, определенных на заданном подмножестве числовой прямой, является коммутативным ассоциативным кольцом с единицей относительно обычных операций сложения и умножения функций.

Пример 4. Множество векторов пространства с операциями сложения и векторного умножения является некоммутативным и неассоциативным кольцом. Однако в нем выполняются следующие тождества, которые в некотором смысле заменяют коммутативность и ассоциативность:

$$a \times b + b \times a = 0 \qquad (\textit{антикоммутативность}),$$

$$(a \times b) \times c + (b \times c) \times a + (c \times a) \times b = 0 \qquad (\textit{тождество Якоби}).$$

Антикоммутативность очевидна в силу определения векторного умножения. По поводу проверки тождества Якоби см. пример 7.5.

Задача 1. Пусть X — какое-либо множество и 2^X — множество всех его подмножеств. Доказать, что 2^X — кольцо относительно операций симметрической разности

$$M \triangle N = (M \setminus N) \cup (N \setminus M)$$

и пересечения, взятых в качестве сложения и умножения соответственно. Доказать, что это кольцо коммутативно, ассоциативно и обладает единицей.

Элемент a^{-1} кольца с единицей называется *обратным* к элементу a, если

$$aa^{-1}=a^{-1}a=1.$$

(В коммутативном кольце достаточно требовать, чтобы $aa^{-1}=1$.) Так же, как в случае мультипликативной абелевой группы, доказывается, что в ассоциативном кольце с единицей никакой элемент не может иметь двух различных обратных элементов (но может не иметь ни одного). Элемент, имеющий обратный, называется *обратимым*.

Определение 2. *Полем* называется коммутативное ассоциативное кольцо с единицей, в котором всякий ненулевой элемент обратим.

Замечание 3. Кольцо, состоящее из одного нуля, не считается полем.

Примерами полей служат поле рациональных чисел $\mathbb{Q}$ и поле вещественных чисел $\mathbb{R}$. Кольцо $\mathbb{Z}$ не является полем: в нем обратимы только ± 1.

Задача 2. Доказать, что существует поле, состоящее из двух элементов. (Очевидно, что один из этих элементов должен быть нулем поля, а другой — его единицей.)

Любое поле обладает следующим важным свойством:

$$ab=0 \;\Rightarrow\; a=0 \text{ или } b=0.$$

В самом деле, если $a\neq 0$, то, умножая обе части равенства $ab=0$ на a^{-1}, получаем $b=0$.

Существуют и другие кольца, обладающие этим свойством, например, кольцо $\mathbb{Z}$. Они называются *кольцами без делителей нуля*. В кольце без делителей нуля возможно сокращение:

$$\{ac=bc \text{ (или } ca=cb) \text{ и } c\neq 0\} \;\Rightarrow\; a=b.$$

В самом деле, равенство $ac=bc$ может быть переписано в виде $(a-b)c=0$, откуда при $c\neq 0$ получаем $a-b=0$, т. е. $a=b$.

Приведем пример коммутативного ассоциативного кольца с делителями нуля.

Пример 5. В кольце функций на подмножестве X числовой прямой (см. пример 3) есть делители нуля, если только X содержит более одной точки. В самом деле, разобьем X на два непустых под-

множества X_1 и X_2 и положим при $i = 1, 2$

$$f_i(x) = \begin{cases} 1 & \text{при } x \in X_i, \\ 0 & \text{при } x \notin X_i. \end{cases}$$

Тогда $f_1, f_2 \neq 0$, но $f_1 f_2 = 0$.

Отсутствие делителей нуля в поле означает, что произведение любых двух ненулевых элементов также является ненулевым элементом. Ненулевые элементы поля K образуют абелеву группу относительно умножения. Она называется *мультипликативной группой поля* K и обозначается через K^*.

Аналогично понятию подгруппы абелевой группы вводится понятие подкольца.

Определение 3. Подмножество L кольца K называется *подкольцом*, если

1) L является подгруппой аддитивной группы кольца K;

2) L замкнуто относительно умножения.

Очевидно, что всякое подкольцо само является кольцом относительно тех же операций. При этом оно наследует такие свойства, как коммутативность и ассоциативность.

Пример 6. Цепочка подгрупп аддитивной группы $\mathbb{R}$, приведенная в примере 1, является в то же время цепочкой подколец.

Пример 7. При любом $n \in \mathbb{Z}_+$ множество $n\mathbb{Z}$ является подкольцом кольца $\mathbb{Z}$. (Ср. задачу 2.1.)

Задача 3. Доказать, что все конечные подмножества множества X образуют подкольцо кольца 2^X из задачи 1.

Определение 4. Подмножество L поля K называется *подполем*, если

1) L является подкольцом кольца K;

2) $a \in L, a \neq 0 \Rightarrow a^{-1} \in L$;

3) $1 \in L$.

Очевидно, что всякое подполе является полем относительно тех же операций.

Пример 8. Поле $\mathbb{Q}$ является подполем поля $\mathbb{R}$.

Задача 4. Доказать, что подмножество L поля K является подполем тогда и только тогда, когда

1) L замкнуто относительно вычитания и деления;

2) $L \ni 0, 1$.

Задача 5. Доказать, что поле $\mathbb{Q}$ не имеет нетривиальных (т. е. отличных от него самого) подполей.