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

1.1. 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,
$\mathbb{Z}_+ = \mathbb{N} \cup \{0\}$ — множество неотрицательных целых чисел,

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

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

$\mathbb{R}_+$ — множество неотрицательных действительных чисел,

$\mathbb{R}$ — множество всех действительных (= 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

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

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

$$fg\colon P \to M,$$

определяемое формулой

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

т. е. результат последовательного выполнения сначала g, а потом f. 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 $\mathbb{Z}_+$, сопоставляющую 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. Пусть M — множество с операцией $\circ$, а N — множество с операцией $*$. Алгебраические структуры $(M, \circ)$ и $(N, *)$ называются изоморфными, если существует такое биективное отображение

$$f\colon M \to N,$$

что

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

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

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

Пример 3. Отображение

$$a \mapsto 2^a$$

является изоморфизмом множества всех действительных 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 M — множество параллельных переносов плоскости на векторы, параллельные какой-либо фиксированной прямой. Для любого действительного числа a обозначим через t_a элемент множества M, представляющий собой перенос на вектор длины $|a|$ в одном из двух возможных направлений, определяемом знаком a. (Если $a = 0$, то t_a — это тождественное преобразование.) Легко видеть, что

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

где $\circ$ обозначает умножение (композицию) параллельных переносов. Следовательно, отображение $a \mapsto t_a$ является изоморфизмом алгебраических структур $(\mathbb{R}, +)$ и $(M, \circ)$.

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 не безразличен для фактического решения какой-либо задачи. Какая-то определенная модель может предоставить для этого наибольшее удобство. Например, если какая-то модель имеет геометрический характер, то она позволяет применить геометрические методы.

1.2. Абелевы группы

Сложение действительных 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 вычетания, обратной к сложению, означает, что для любых a, b уравнение

$$x + a = b$$

имеет единственное решение. Докажем это. 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 уравнение показывает, что $b + (-a)$ действительно является решением:

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

Умножение действительных 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) операции вычитания, будучи переведен на язык умножения, даст вывод из свойств (У1)–(У4) 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 действительных 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 действительными числами, а также вызывает полезные ассоциации.

Приведем вначале определение абелевой группы, использующее язык сложения.

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

1) $a + b = b + a \quad \forall a, b$ (коммутативность);

2) $(a + b) + c = a + (b + c) \quad \forall a, b, c$ (ассоциативность);

3) существует такой элемент 0 (нуль), что $a + 0 = a \quad \forall a$;

4) для любого a существует такой элемент $-a$ (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 $b - a$.

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 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 является 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 называется множество A с операцией умножения, обладающей следующими свойствами:

1) $ab = ba \quad \forall a, b$ (коммутативность);

2) $(ab)c = a(bc) \quad \forall a, b, c$ (ассоциативность);

3) существует такой элемент e (единица), что $ae = a \quad \forall a$;

4) для любого a существует такой элемент a^{-1} (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 $\dfrac{b}{a}$.

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.

1.3. Кольца и поля

В отличие от групп, кольца и поля — это алгебраические структуры с двумя операциями, называемыми обычно сложением и умножением. Их аксиомы, как и аксиомы абелевой группы, подсказаны свойствами операций над действительными 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 $(a + b)c = ac + bc \quad \forall a, b, c$ (дистрибутивность умножения относительно сложения).

Выведем некоторые следствия аксиом кольца, не входящие в число следствий аксиом аддитивной абелевой группы, перечисленных в §1.2.

1) $a0 = 0a = 0 \ \ \forall a$. 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) $a(-b) = (-a)b = -ab \quad \forall a, b$. В самом деле,

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

и, аналогично, $ab + (-a)b = 0$.

3) $a(b - c) = ab - ac$ и $(a - b)c = ac - bc \quad \forall a, b, c$. 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 (если такой существует) 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.

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:

$$a \times b + b \times a = 0 \quad \text{(антикоммутативность)},$$
$$(a \times b) \times c + (b \times c) \times a + (c \times a) \times b = 0 \quad \text{(тождество Якоби)}.$$

Антикоммутативность очевидна из определения векторного умножения. По поводу проверки тождества Якоби см. пример 8.2.

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

$$A \triangle B = (A \setminus B) \cup (B \setminus A)$$

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

Элемент a^{-1} кольца с единицей (если такой существует) 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. 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 действительных 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.)

В любом поле выполнено следующее важное свойство:

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

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 равенств:

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

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 подмножества X_1 и X_2 и положим

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

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^*.

1.4. Подгруппы, подкольца и подполя

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

$$a, b \in N \implies a \circ b \in N.$$

В этом случае операция $\circ$ определена в множестве N и превращает его в некоторую алгебраическую структуру. Если операция $\circ$ в M обладает некоторым свойством, имеющим характер тождественного соотношения (например, коммутативна или ассоциативна), 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, так как не содержит противоположных элементов ко всем своим элементам, кроме нуля.

Определение 1. Подмножество B аддитивной абелевой группы A называется подгруппой, если

1) B замкнуто относительно сложения;

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

3) $0 \in B$.

Замечание. 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 1. В аддитивной группе $\mathbb{R}$ имеется следующая цепочка подгрупп:

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

Пример 2. 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 1$'$. Подмножество B мультипликативной абелевой группы A называется подгруппой, если

1) B замкнуто относительно умножения;

2) $a \in B \implies a^{-1} \in B$;

3) $e \in B$.

Пример 3. В группе $\mathbb{R}^*$ имеется следующая цепочка подгрупп:

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

Соображения, с которых начинается этот параграф, могут быть распространены на алгебраические структуры с несколькими операциями. Таким образом мы приходим к следующим понятиям подкольца и подполя.

Определение 2. 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 4. Цепочка подгрупп аддитивной группы $\mathbb{R}$, приведенная в примере 1, является в то же время цепочкой подколец.

Пример 5. При любом $n \in \mathbb{Z}_+$ множество $n\mathbb{Z}$ является подкольцом кольца $\mathbb{Z}$. (Ср. задачу 1.)

Задача 2. Доказать, что все конечные подмножества множества M образуют подкольцо кольца 2^M из задачи 3.1.

Определение 3. Подмножество L поля K называется подполем, если

1) L является подкольцом кольца K;

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

3) $1 \in L$.

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

Пример 6. Поле $\mathbb{Q}$ является подполем поля $\mathbb{R}$.

Задача 3. 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 4. Доказать, что поле $\mathbb{Q}$ не имеет нетривиальных подполей (т. е. отличных от него самого).

1.5. Поле комплексных чисел

Подобно тому как невозможность деления в кольце целых чисел приводит к необходимости расширить его до поля рациональных чисел, невозможность извлечения квадратных корней из отрицательных чисел в поле действительных чисел приводит к необходимости расширить его до большего поля, называемого полем комплексных чисел.

Для того чтобы лучше понять, что такое поле комплексных чисел, нужно прежде подумать над тем, что такое поле действительных чисел. Строгое построение поля действительных чисел обычно приводится в курсе анализа. Мы не будем входить в его детали. Однако заметим, что имеется несколько определений действительных чисел: как бесконечных десятичных дробей, как сечений Дедекинда множества рациональных чисел и т. д. Формально говоря, при этом получаются различные поля. Какое из них является «настоящим» полем действительных чисел? Ответ на этот вопрос состоит в том, что все они изоморфны и их следует рассматривать просто как различные модели одного и того же объекта, называемого полем действительных чисел.

Наиболее удовлетворительным в подобной ситуации всегда является аксиоматический подход, при котором сначала формулируются в виде аксиом свойства, которыми должен обладать искомый объект, а затем доказывается, что этими свойствами он определяется однозначно с точностью до изоморфизма, и с помощью какой-либо конструкции доказывается его существование. В случае поля действительных чисел такими аксиомами (помимо аксиом поля) могут быть аксиомы порядка, аксиома Архимеда и аксиома непрерывности.

Замечание 1. Нетрудно доказать, что любые две модели поля действительных чисел не просто изоморфны, но между ними имеется единственный изоморфизм. (Доказательство сводится к тому, что всякий изоморфизм поля $\mathbb{R}$ на себя тождествен, и основано на соображении, что неотрицательные числа при любом изоморфизме должны переходить в неотрицательные, так как они и только они являются квадратами в поле $\mathbb{R}$.) Это означает, что каждый элемент поля $\mathbb{R}$ имеет свою индивидуальность, т. е. в любой модели могут быть идентифицированы числа 10, $\sqrt{2}$, π и т. д.

Дадим теперь аксиоматическое определение поля комплексных чисел.

Определение. Полем комплексных чисел называется всякое поле $\mathbb{C}$, обладающее следующими свойствами:

1) оно содержит в качестве подполя поле $\mathbb{R}$ действительных чисел;

2) оно содержит такой элемент i, что $i^2 = -1$;

3) оно минимально среди полей с этими свойствами, т. е. если $K \subset \mathbb{C}$ — какое-либо подполе, содержащее $\mathbb{R}$ и i, то $K = \mathbb{C}$.

Замечание 2. Из равенства $x^2 + 1 = (x - i)(x + i)$ следует, что уравнение $x^2 = -1$ имеет в $\mathbb{C}$ ровно 2 решения: i и $-i$. Если какое-либо подполе содержит одно из этих решений, то оно содержит и другое.

Теорема 1. Поле комплексных чисел существует и единственно с точностью до изоморфизма, переводящего все действительные числа в себя. Каждое комплексное число однозначно представляется в виде $a + bi$, где $a, b \in \mathbb{R}$, а i — (фиксированный) элемент, квадрат которого равен -1.

Доказательство. 1) Пусть $\mathbb{C}$ — какое-то поле комплексных чисел (если оно существует). Рассмотрим его подмножество

$$K = \{\, a + bi : a, b \in \mathbb{R} \,\}.$$

Из свойств операций в поле и соотношения $i^2 = -1$ следует, что

$$(a_1 + b_1 i) + (a_2 + b_2 i) = (a_1 + a_2) + (b_1 + b_2)i, \tag{1}$$

$$(a_1 + b_1 i)(a_2 + b_2 i) = (a_1 a_2 - b_1 b_2) + (a_1 b_2 + b_1 a_2)i. \tag{2}$$

Решая соответствующие уравнения, находим также, что

$$-(a + bi) = (-a) + (-b)i, \tag{3}$$

$$(a + bi)^{-1} = \frac{a}{a^2 + b^2} + \left(-\frac{b}{a^2 + b^2}\right) i \quad \text{при } a^2 + b^2 \neq 0. \tag{4}$$

Формулы (1)–(4) показывают, что K — подполе. Так как K, очевидно, содержит $\mathbb{R}$ и i, то $K = \mathbb{C}$.

Таким образом, каждый элемент поля $\mathbb{C}$ представляется в виде $a + bi$, где $a, b \in \mathbb{R}$. Докажем, что такое представление единственно. Пусть

$$a_1 + b_1 i = a_2 + b_2 i \quad (a_1, b_1, a_2, b_2 \in \mathbb{R}).$$

Тогда

$$a_1 - a_2 = (b_2 - b_1)i.$$

Возводя это равенство в квадрат, получаем

$$(a_1 - a_2)^2 = -(b_2 - b_1)^2,$$

откуда

$$a_1 - a_2 = b_2 - b_1 = 0,$$

что и требовалось доказать.

Если теперь $\mathbb{C}'$ — другое поле комплексных чисел и $i' \in \mathbb{C}'$ — такой элемент, что $(i')^2 = -1$, то поскольку формулы (1) и (2) остаются справедливыми при замене i на i', отображение

$$f\colon \mathbb{C} \to \mathbb{C}', \quad a + bi \mapsto a + bi' \quad (a, b \in \mathbb{R}),$$

является изоморфизмом поля $\mathbb{C}$ на поле $\mathbb{C}'$.

2) Предыдущее исследование подсказывает, как доказать существование поля комплексных чисел. Рассмотрим множество $\mathbb{C}$ пар (a, b), где $a, b \in \mathbb{R}$. Определим в нем сложение и умножение по формулам

$$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2),$$
$$(a_1, b_1)(a_2, b_2) = (a_1 a_2 - b_1 b_2, a_1 b_2 + b_1 a_2),$$

подсказанным формулами (1) и (2). Очевидно, что $\mathbb{C}$ является абелевой группой относительно сложения (ср. пример 2.3) и что умножение дистрибутивно относительно сложения и коммутативно. Непосредственной выкладкой проверяется ассоциативность умножения. Таким образом, $\mathbb{C}$ — коммутативное ассоциативное кольцо.

Так как

$$(a, b)(1, 0) = (a, b),$$

то элемент $(1, 0)$ — единица кольца $\mathbb{C}$. Формула (4) подсказывает, как должен выглядеть элемент, обратный к (a, b) при $a^2 + b^2 \neq 0$. И, действительно, непосредственная проверка показывает, что

$$(a, b)(a/(a^2 + b^2), -b/(a^2 + b^2)) = (1, 0).$$

Следовательно, $\mathbb{C}$ — поле.

Далее, имеем

$$(a_1, 0) + (a_2, 0) = (a_1 + a_2, 0),$$
$$(a_1, 0)(a_2, 0) = (a_1 a_2, 0),$$

т. е. операции над парами вида $(a, 0)$ сводятся к соответствующим операциям над их первыми компонентами. Условимся отождествлять пару $(a, 0)$ с действительным числом a. Тогда мы можем сказать, что построенное поле $\mathbb{C}$ содержит поле $\mathbb{R}$ в качестве подполя.

Положим $i = (0, 1)$; тогда

$$i^2 = (-1, 0) = -1,$$
$$a + bi = (a, b) \quad \text{при } a, b \in \mathbb{R}.$$

Таким образом, каждый элемент поля $\mathbb{C}$ (однозначно) представляется в виде $a + bi$, где $a, b \in \mathbb{R}$. Поэтому, если какое-либо подполе $K \subset \mathbb{C}$ содержит $\mathbb{R}$ и i, то $K = \mathbb{C}$. Следовательно, $\mathbb{C}$ — поле комплексных чисел.

Представление комплексного числа $c \in \mathbb{C}$ в виде $a + bi$ $(a, b \in \mathbb{R})$ называется его алгебраической формой; при этом число a называется действительной частью числа c и обозначается через $\operatorname{Re} c$, а число b называется мнимой частью числа c и обозначается через $\operatorname{Im} c$. Комплексные числа, не являющиеся действительными, называются мнимыми; числа вида bi, где $b \in \mathbb{R}$, называются чисто мнимыми.

Если в первой части доказательства теоремы в качестве $\mathbb{C}'$ взять то же поле $\mathbb{C}$, а в качестве i' — элемент $-i$, то мы получим, что отображение

$$c = a + bi \mapsto \overline{c} = a - bi \quad (a, b \in \mathbb{R}),$$

является изоморфизмом поля $\mathbb{C}$ на себя. Оно называется комплексным сопряжением. Вообще, изоморфизм какой-либо алгебраической структуры на себя называется ее автоморфизмом. Таким образом, комплексное сопряжение $c \mapsto \overline{c}$ есть автоморфизм поля комплексных чисел. Очевидно, что $\overline{\overline{c}} = c$.

Действительные числа характеризуются тем, что они совпадают со своими сопряженными. Отсюда следует, что для любого $c \in \mathbb{C}$ числа $c + \overline{c}$ и $c\overline{c}$ действительны. В самом деле,

$$\overline{c + \overline{c}} = \overline{c} + c = c + \overline{c}, \quad \overline{c\overline{c}} = \overline{c}c = c\overline{c}.$$

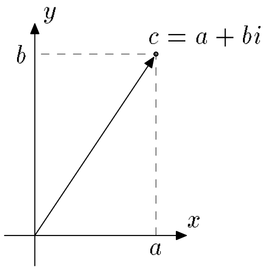

Рис. 1.

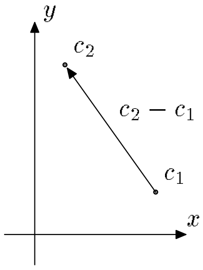

Рис. 2.

Легко видеть, что если $c = a + bi$ $(a, b \in \mathbb{R})$, то

$$c + \overline{c} = 2a, \quad c\overline{c} = a^2 + b^2. \tag{5}$$

Комплексные числа можно изображать точками или векторами на плоскости. А именно, число $c = a + bi$ изображается точкой или вектором с декартовыми координатами (a, b) (рис. 1). Иногда бывает удобнее представление комплексных чисел точками, иногда — векторами. При векторном представлении сложению комплексных чисел соответствует обычное сложение векторов по правилу параллелограмма (или эквивалентному ему правилу треугольника).

Отметим, что разность комплексных чисел c_2 и c_1 представляется вектором, соединяющим точки, изображающие c_1 и c_2 (рис. 2).

Вместо декартовых координат на плоскости иногда бывает удобно использовать полярные. Это приводит к следующим понятиям.

Модулем комплексного числа $c = a + bi$ называется длина вектора, изображающего это число. Модуль числа c изобра-

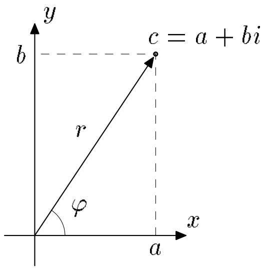

Рис. 3.

жается через $|c|$. Очевидно, что

$$|c| = \sqrt{a^2 + b^2}.$$

Аргументом комплексного числа называется угол, образуемый соответствующим вектором с положительным направлением оси абсцисс. Аргумент определен с точностью до прибавления целого кратного 2π. Аргумент числа 0 не определен. Аргумент числа c обозначается через $\arg c$.

Пусть r и φ — модуль и аргумент числа c (рис. 3).

Очевидно, что

$$a = r\cos\varphi,\ \ b = r\sin\varphi,$$

откуда

$$c = r(\cos\varphi + i\sin\varphi).$$

Такое представление комплексного числа называется его тригонометрической формой. Так как тригонометрическая форма данного комплексного числа определена однозначно с точностью до прибавления к φ целого кратного 2π, то при $r_1, r_2 > 0$

$$r_1(\cos\varphi_1 + i\sin\varphi_1) = r_2(\cos\varphi_2 + i\sin\varphi_2) \iff$$
$$\iff r_1 = r_2, \quad \varphi_1 = \varphi_2 + 2\pi k \quad (k \in \mathbb{Z}).$$

Тригонометрическая форма комплексных чисел хорошо приспособлена к таким операциям, как умножение, деление, возведение в степень и извлечение корня.

А именно, из формул для косинуса и синуса суммы двух углов следует, что

$$r_1(\cos\varphi_1 + i\sin\varphi_1)\cdot r_2(\cos\varphi_2 + i\sin\varphi_2) = \\ = r_1 r_2(\cos(\varphi_1+\varphi_2) + i\sin(\varphi_1+\varphi_2)),$$

т. е. при умножении комплексных чисел их модули перемножаются, а аргументы складываются. Отсюда вытекают следующие формулы для деления и возведения в степень:

$$\frac{r_1(\cos\varphi_1 + i\sin\varphi_1)}{r_2(\cos\varphi_2 + i\sin\varphi_2)} = \frac{r_1}{r_2}(\cos(\varphi_1-\varphi_2) + i\sin(\varphi_1-\varphi_2)),$$

$$[r(\cos\varphi + i\sin\varphi)]^n = r^n(\cos n\varphi + i\sin n\varphi) \quad \text{(формула Муавра).}$$

Извлечение корня n-й степени из комплексного числа $c = r(\cos\varphi + i\sin\varphi)$ есть решение уравнения $z^n = c$. Пусть $|z| = s$, $\arg z = \psi$; тогда $s^n = r$, $n\psi = \varphi + 2\pi k$ $(k \in \mathbb{Z})$. Следовательно,

$$s = \sqrt[n]{r} \quad \text{(арифметическое значение корня)},$$

$$\psi = \frac{\varphi + 2\pi k}{n}.$$

Окончательно получаем

$$z = \sqrt[n]{r}\left(\cos\frac{\varphi+2\pi k}{n} + i\sin\frac{\varphi+2\pi k}{n}\right).$$

Одинаковые значения z получаются по этой формуле тогда и только тогда, когда в качестве k берутся числа, сравнимые по модулю n. Отсюда следует, что при $c \neq 0$ уравнение $z^n = c$ имеет ровно n решений, получаемых, например, при $k = 0, 1, \ldots, n-1$. В геометрическом изображении эти числа располагаются в вершинах правильного n-угольника с центром в начале координат (см. рис. 4, где изображен случай $n = 6$).

1.6. Кольца вычетов

Расширения кольца целых чисел приводят к цепочке колец

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C},$$

в которую, как мы позже увидим, можно вставить и другие звенья (в том числе и продолжить ее вправо). Кольца вычетов определяются также на основе целых чисел, но идея их

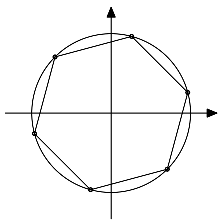

Рис. 4.

определения совершенно иная. Это часто используемый в математике прием «склейки» — образования фактормножества по отношению эквивалентности.

Пусть M — какое-нибудь множество. Всякое подмножество $R \subset M \times M$ называется отношением на множестве M. Если $(a, b) \in R$, то говорят, что элементы a и b находятся в отношении R, и пишут aRb.

Примеры отношений. 1. M — множество людей; aRb, если a знает b.

2. M — то же; aRb, если a и b знакомы.

3. M — то же; aRb, если a и b живут в одном доме.

4. $M = \mathbb{R}$; aRb, если $a \leqslant b$.

5. M — множество окружностей на плоскости; aRb, если окружности a и b равны, т. е. переводятся одна в другую движением.

Отношение R называется отношением эквивалентности, если выполняются следующие свойства:

1) aRa (рефлексивность);

2) $aRb \implies bRa$ (симметричность);

3) aRb и $bRc \implies aRc$ (транзитивность).

Из приведенных выше примеров отношений только третье и пятое являются отношениями эквивалентности: первое и четвертое не симметричны, а второе симметрично, но не транзитивно.

Отношение эквивалентности обычно записывается как $a \underset{R}{\sim} b$ или просто $a \sim b$.

Пусть R — отношение эквивалентности на множестве M. Для каждого $a \in M$ положим

$$R(a) = \{\, b \in M : a \underset{R}{\sim} b \,\}.$$

Из свойств отношений эквивалентности легко выводится, что $a \in R(a)$ и

$$R(a) \cap R(b) \neq \varnothing \implies R(a) = R(b).$$

Таким образом, подмножества $R(a)$ образуют разбиение множества M, т.е. покрывают его и попарно не пересекаются. Они называются классами эквивалентности R. Два элемента эквивалентны тогда и только тогда, когда они принадлежат одному классу.

Множество, элементами которого являются классы эквивалентности R, называется фактормножеством множества M по отношению эквивалентности R и обозначается через M/R. Отображение

$$M \to M/R, \quad a \mapsto R(a),$$

называется отображением факторизации.

Так, в третьем из приведенных выше примеров классы эквивалентности — это множества жильцов одного дома. Фактормножество отождествляется с множеством домов, а отображение факторизации — это отображение, сопоставляющее каждому человеку дом, в котором он живет. В пятом примере классы эквивалентности — это множества окружностей одного радиуса, фактормножество отождествляется с множеством положительных чисел, а отображение факторизации — это отображение, сопоставляющее каждой окружности ее радиус.

Пусть в множестве M задана некоторая операция $(x, y) \mapsto \mapsto x * y$. Отношение эквивалентности R в множестве M называется согласованным с операцией $*$, если

$$a \underset{R}{\sim} a',\ b \underset{R}{\sim} b' \implies a * b \underset{R}{\sim} a' * b'.$$

В этом случае на фактормножестве M/R также можно определить операцию $*$ по правилу

$$R(a) * R(b) = R(a * b). \tag{6}$$

В словесном выражении это определение выглядит так: чтобы произвести операцию над какими-либо двумя классами эквивалентности, надо выбрать из них произвольных представителей, произвести операцию над ними и взять тот класс, в котором будет лежать получившийся элемент. То, что этот класс не будет зависеть от выбора указанных представителей, как раз и обеспечивается согласованностью отношения эквивалентности с операцией.

Очевидно, что все свойства операции в M, имеющие характер тождества, например, коммутативность и ассоциативность, наследуются определенной таким образом операцией в M/R. То же самое можно сказать о наличии нуля (единицы) и противоположного (обратного) элемента. Более точно, если, скажем, операция в M называется сложением и в M имеется нулевой элемент 0 относительно этой операции, то $R(0)$ — нулевой элемент в M/R; если $-a$ — элемент, противоположный элементу a в M, то $R(-a)$ — элемент, противоположный элементу $R(a)$ в M/R.

Приступим теперь к построению колец вычетов. Пусть n — фиксированное натуральное число. Рассмотрим в множестве $\mathbb{Z}$ целых чисел следующее отношение сравнимости по модулю n: a сравнимо с b по модулю n (обозначение: $a \equiv b \pmod{n}$), если $a - b$ делится на n или, что равносильно, если a и b дают одинаковые остатки при делении на n.

Очевидно, что это отношение эквивалентности, причем классы эквивалентности могут быть занумерованы числами $0, 1, \ldots, n-1$ таким образом, что r-й класс состоит из всех целых чисел, дающих при делении на n остаток r.

Класс эквивалентности, содержащий целое число a, называется вычетом числа a по модулю n и обозначается через $[a]_n$ или просто через $[a]$, если ясно, какое n имеется в виду.

Фактормножество множества $\mathbb{Z}$ по отношению сравнимости по модулю n обозначается через $\mathbb{Z}_n$. Мы можем написать, что

$$\mathbb{Z}_n = \{[0]_n, [1]_n, \ldots, [n-1]_n\},$$

но следует понимать, что каждый элемент множества $\mathbb{Z}_n$ может быть обозначен по-разному. Так, элемент $[1]_n$ может быть с таким же успехом обозначен как $[2n+1]_n$, $[-(n-1)]_n$ и т. д.

Докажем теперь, что отношение сравнимости по модулю n согласовано с операциями сложения и умножения в $\mathbb{Z}$. Пусть

$$a \equiv a' \pmod{n}, \qquad b \equiv b' \pmod{n}.$$

Тогда

$$a + b \equiv a' + b \equiv a' + b' \pmod{n}$$

и, аналогично,

$$ab \equiv a'b \equiv a'b' \pmod{n}.$$

Таким образом, мы можем определить в множестве $\mathbb{Z}_n$ операции сложения и умножения по формулам

$$[a]_n + [b]_n = [a+b]_n, \quad [a]_n[b]_n = [ab]_n$$

(справедливым для любых $a, b \in \mathbb{Z}$). Тем самым $\mathbb{Z}_n$ превращается в коммутативное ассоциативное кольцо с единицей. Оно называется кольцом вычетов по модулю n.

Пример 6. Ниже приведены таблицы сложения и умножения в кольце $\mathbb{Z}_5$. При этом ради простоты квадратные скобки в обозначениях элементов этого кольца опущены.

$+$	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

$\times$	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

Мы видим, в частности, что элементы 2 и 3 взаимно обратны, а элемент 4 обратен сам себе.

Пример 7. Вычислим $[2]^{100}$ в кольце $\mathbb{Z}_{125}$:

$$\begin{aligned}
&[2]^7 = [128] = [3],\\
&[2]^{35} = ([2]^7)^5 = [3]^5 = [243] = [-7],\\
&[2]^{50} = [2]^{35}([2]^7)^2[2] = [-7][3]^2[2] = [-126] = [-1],\\
&[2]^{100} = ([2]^{50})^2 = [1].
\end{aligned}$$

Полученный результат означает, что

$$2^{100} \equiv 1 \pmod{125}.$$

Отсюда нетрудно вывести, что

$$2^{100} \equiv 376 \pmod{1000},$$

т.е. десятичная запись числа 2^{100} оканчивается на 376.

Кольцо $\mathbb{Z}_n$ обладает всеми свойствами поля, кроме, быть может, обратимости ненулевых элементов. Очевидно, что $\mathbb{Z}_2$ — поле из двух элементов, о котором шла речь в задаче 3.2.

Рассмотрение приведенной выше таблицы умножения в кольце $\mathbb{Z}_5$ показывает, что $\mathbb{Z}_5$ — также поле. С другой стороны, $\mathbb{Z}_4$ — не поле, так как элемент [2] в этом кольце не обратим.

Теорема 1. Кольцо $\mathbb{Z}_n$ является полем тогда и только тогда, когда n — простое число.

Доказательство. 1) Пусть n составное, т. е. $n = kl$, где $1 < k, l < n$. Тогда $[k]_n, [l]_n \neq 0$, но

$$[k]_n[l]_n = [kl]_n = [n]_n = 0.$$

Таким образом, в кольце $\mathbb{Z}_n$ имеются делители нуля и, значит, оно не является полем.

2) Пусть, напротив, n — простое число и $[a]_n \neq 0$, т. е. a не делится на n. Будем искать элемент, обратный к $[a]_n$, подбором, т. е. умножая $[a]_n$ по очереди на все элементы кольца. Получим элементы

$$[0]_n, [a]_n, [2a]_n, \ldots, [(n-1)a]_n. \tag{7}$$

Докажем, что все они различны. В самом деле, если $[ka]_n = [la]_n$ $(0 \leqslant k < l \leqslant n-1)$, то $[(l-k)a]_n = 0$, т. е. $(l-k)a$ делится на n, что невозможно, так как ни $l-k$, ни a на n не делятся. (Здесь мы использовали то, что n простое.) Следовательно, в ряду элементов (7) встречаются все элементы кольца $\mathbb{Z}_n$, в том числе $[1]_n$, а это и означает, что элемент $[a]_n$ обратим.

В полях вычетов мы встречаемся с новым явлением, не имевшим места в числовых полях. А именно, в поле $\mathbb{Z}_n$ (n простое) выполняется равенство

$$\underbrace{1 + 1 + \ldots + 1}_{n} = 0. \tag{8}$$

(Конечно, это верно и в кольце $\mathbb{Z}_n$ при любом n.) Это приводит к некоторым особенностям алгебраических преобразований в этом поле, о которых мы скажем ниже.

Пусть, вообще, K — произвольное поле. Наименьшее натуральное n, для которого в поле K выполняется равенство (8), называется характеристикой этого поля; если такого n не существует, то говорят, что K — поле нулевой характеристики. Таким образом, $\mathbb{Z}_n$ (n простое) — поле характеристики n, а числовые поля имеют нулевую характеристику. Характеристика поля K обозначается через $\operatorname{char} K$.

Если $\operatorname{char} K = n$, то для любого $a \in K$ имеем

$$\underbrace{a + a + \ldots + a}_{n} = (\underbrace{1 + 1 + \ldots + 1}_{n})a = 0a = 0.$$

Характеристика поля, если она положительна, всегда является простым числом. В самом деле, пусть $\operatorname{char} K = n = kl$ $(1 < k, l < n)$. Тогда

$$\underbrace{1 + 1 + \ldots + 1}_{n} = (\underbrace{1 + 1 + \ldots + 1}_{k})(\underbrace{1 + 1 + \ldots + 1}_{l}) = 0$$

и, значит, либо $\underbrace{1 + 1 + \ldots + 1}_{k} = 0$, либо $\underbrace{1 + 1 + \ldots + 1}_{l} = 0$, что противоречит определению характеристики.

Большинство формул элементарной алгебры справедливы в любом поле, так как при их выводе используются только те свойства операций сложения и умножения, которые входят в число аксиом поля или являются их следствием. Особенность полей положительной характеристики проявляется только в тех формулах, которые содержат умножение или деление на натуральные числа.

Рассмотрим, например, формулу

$$(a + b)^2 = a^2 + 2ab + b^2.$$

Она справедлива в любом поле, если понимать $2ab$ как $ab + ab$. Однако в поле характеристики 2 она принимает более простой вид

$$(a + b)^2 = a^2 + b^2.$$

Более общо, в поле характеристики n справедливо тождество

$$(a + b)^n = a^n + b^n.$$

В самом деле, по формуле бинома Ньютона

$$(a + b)^n = \sum_{k=0}^{n} C_n^k a^{n-k} b^k.$$

Однако при $0 < k < n$

$$C_n^k = \frac{n(n-1)\cdots(n-k+1)}{k!}$$

(число сочетаний из n по k), очевидно, делится на n. Следовательно, все слагаемые формулы бинома Ньютона, кроме первого и последнего, в рассматриваемом случае равны нулю.

Задача. Вывести отсюда, что в поле $\mathbb{Z}_n$ (n простое) $a^n = a$ для любого a. (Другое доказательство последнего факта, называемого малой теоремой Ферма, будет дано в §4.4.)

Хуже обстоит дело, когда приходится делить на натуральное число, например, когда мы находим выражение для ab из выписанной выше формулы квадрата суммы. Для того чтобы придать смысл этому делению в любом поле, можно рассматривать умножение на натуральное число k как умножение на элемент $\underbrace{1+1+\ldots+1}_{k}$ данного поля; тогда деление на k можно понимать как деление на этот элемент. Однако если k делится на характеристику поля, то этот элемент равен нулю и деление невозможно.

Так, формула для решения квадратного уравнения, содержащая деление на 2, применима в указанном смысле в любом поле характеристики $\neq 2$, но в поле характеристики 2 она не работает.

Пример 8. Решим квадратное уравнение

$$x^2 + x - 1 = 0$$

в поле $\mathbb{Z}_{11}$. По обычной формуле находим:

$$x_{1,2} = \frac{[-1] \pm \sqrt{[5]}}{[2]}.$$

Так как $[5] = [16] = [4]^2$, то можно считать, что $\sqrt{[5]} = [4]$ (одно из значений квадратного корня). Следовательно,

$$x_1 = \frac{[-1]+[4]}{[2]} = \frac{[3]}{[2]} = \frac{[14]}{[2]} = [7],$$

$$x_2 = \frac{[-1]-[4]}{[2]} = \frac{[-5]}{[2]} = \frac{[6]}{[2]} = [3].$$

1.7. Векторные пространства

Векторы, рассматриваемые в элементарной геометрии, можно не только складывать, но и умножать на числа. Анализ свойств этих двух операций приводит к понятию векторного пространства.

Прежде чем мы дадим определение, необходимо отметить, что здесь мы выходим за рамки того понимания операции на множестве, которое принималось до сих пор. Умножение вектора на число не есть операция над двумя элементами одного и того же множества. Это операция, которая каждой паре (число, вектор) сопоставляет вектор. В общем определении векторного пространства дело обстоит так же, но действительные числа заменяются элементами произвольного (но фиксированного) поля.

Определение 1. Векторным пространством над полем K называется множество V с операциями сложения и умножения на элементы поля K, обладающими следующими свойствами:

1) относительно сложения V есть абелева группа;
2) $\lambda(a+b) = \lambda a + \lambda b \;\; \forall \lambda \in K,\; a, b \in V$;
3) $(\lambda + \mu)a = \lambda a + \mu a \;\; \forall \lambda, \mu \in K,\; a \in V$;
4) $(\lambda\mu)a = \lambda(\mu a) \;\; \forall \lambda, \mu \in K,\; a \in V$;
5) $1a = a \;\; \forall a \in V$.

Элементы векторного пространства называются векторами. Элементы поля K, в отличие от векторов, мы будем иногда, допуская вольность речи, называть числами, даже если K не есть числовое поле (т.е. подполе поля комплексных чисел).

Векторы в смысле элементарной геометрии мы будем отныне называть геометрическими векторами. Операции над ними удовлетворяют всем аксиомам векторного пространства, что, собственно, и послужило основой для данного выше определения. Пространство геометрических векторов евклидовой плоскости (соотв. трехмерного евклидова пространства) мы будем обозначать через E^2 (соотв. через E^3). Подчеркнем, что это векторное пространство над полем $\mathbb{R}$. Приведем другие важные примеры векторных пространств.

Пример 1. Множество K^n строк длины n с элементами из поля K является векторным пространством над K относительно операций, определенных формулами

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

Пример 2. Множество $F(X, K)$ всех функций на множестве X со значениями в поле K является векторным пространством относительно обычных операций над функциями:

$$(f+g)(x) = f(x) + g(x),$$
$$(\lambda f)(x) = \lambda f(x).$$

Пример 3. Пусть K — подполе поля L. Тогда L можно рассматривать как векторное пространство над K, определив умножение элементов из L на элементы из K просто как умножение в L. В частности, поле $\mathbb{C}$ есть в этом смысле векторное пространство над $\mathbb{R}$.

Укажем некоторые следствия аксиом векторного пространства, не являющиеся следствием только аксиом абелевой группы. Все они доказываются аналогично похожим на них следствиям аксиом кольца (см. §1.3). Символом 0 обозначается как нуль поля K, так и нулевой вектор, т. е. нуль аддитивной группы V; читатель увидит, что это не приводит к путанице.

1) $\lambda 0 = 0 \ \ \forall \lambda \in K$ (здесь 0 — нулевой вектор).
2) $\lambda(-a) = -\lambda a \ \ \forall \lambda \in K,\ a \in V$.
3) $\lambda(a-b) = \lambda a - \lambda b \ \ \forall \lambda \in K,\ a, b \in V$.
4) $0a = 0 \ \ \forall a \in V$ (здесь 0 слева — число, справа — вектор).
5) $(-1)a = -a \ \ \forall a \in V$.
6) $(\lambda - \mu)a = \lambda a - \mu a \ \ \forall \lambda, \mu \in K,\ a \in V$.

Определение 2. Подмножество U векторного пространства V называется подпространством, если

1) U является подгруппой аддитивной группы V;
2) $a \in U \implies \lambda a \in U \ \ \forall \lambda \in K$.

Замечание. В определении подгруппы требуется, чтобы

$$a \in U \implies -a \in U.$$

При наличии условия 2) это свойство выполняется автоматически, так как $-a = (-1)a$.

Подпространство векторного пространства само является векторным пространством относительно тех же операций.

Пример 4. В пространстве E^3 множество векторов, параллельных заданной плоскости или прямой, является подпространством.

Пример 5. В пространстве $F(X, \mathbb{R})$ всех функций на заданном промежутке X числовой прямой множество непрерывных функций является подпространством.

В каждом векторном пространстве V есть два «тривиальных» подпространства: само пространство V и нулевое подпространство (состоящее из одного нулевого вектора). Последнее мы будем обозначать символом 0.

Определение 3. Векторные пространства V и U над полем K называются изоморфными, если существует такое биективное отображение

$$f\colon V \to U,$$

что

1) $f(a+b) = f(a) + f(b) \quad \forall a, b \in V$;

2) $f(\lambda a) = \lambda f(a) \quad \forall \lambda \in K,\ a \in V$.

Само отображение f называется при этом изоморфизмом пространств V и U.

Как мы увидим в §2.2, описание векторных пространств с точностью до изоморфизма весьма просто. В частности, все так называемые конечномерные векторные пространства, с которыми мы в основном и будем иметь дело в этом курсе, изоморфны пространствам K^n. Ключевым понятием этой теории является понятие базиса.

Всякое выражение вида

$$\lambda_1 a_1 + \lambda_2 a_2 + \ldots + \lambda_n a_n \quad (\lambda_1, \lambda_2, \ldots, \lambda_n \in K)$$

называется линейной комбинацией векторов $a_1, a_2, \ldots, a_n \in V$. Говорят, что вектор b линейно выражается через векторы $a_1, a_2, \ldots, a_n$, если он равен некоторой их линейной комбинации.

Определение 4. Система векторов $\{e_1, e_2, \ldots, e_n\} \subset V$ называется базисом векторного пространства V, если каждый вектор $a \in V$ единственным образом линейно выражается через $e_1, e_2, \ldots, e_n$. Коэффициенты этого выражения называются координатами вектора a в базисе $\{e_1, e_2, \ldots, e_n\}$.

Пример 6. Из геометрии известно, что любые два неколинеарных вектора e_1, e_2 составляют базис пространства E^2 (рис. 5). Аналогично, любые три некомпланарных вектора составляют базис пространства E^3.

Пример 7. Единичные строки

$$\begin{array}{l} e_1 = (1, 0, \ldots, 0), \\ e_2 = (0, 1, \ldots, 0), \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ e_n = (0, 0, \ldots, 1) \end{array}$$

составляют базис пространства K^n. Координатами строки

$a = (a_1, a_2, \ldots, a_n)$ в этом базисе служат числа $a_1, a_2, \ldots, a_n$. Конечно, в пространстве K^n имеются и другие базисы.

Пример 8. В качестве базиса поля $\mathbb{C}$ как векторного пространства над $\mathbb{R}$ (см. пример 3) можно взять $\{1, i\}$. Координатами комплексного числа в этом базисе служат его действительная и мнимая части.

Предложение 1. Всякое векторное пространство V над полем K, имеющее базис из n векторов, изоморфно пространству K^n.

Доказательство. Пусть $\{e_1, e_2, \ldots, e_n\}$ — базис пространства V. Рассмотрим отображение

$$f\colon V \to K^n,$$

сопоставляющее каждому вектору строку из его координат в базисе $\{e_1, e_2, \ldots, e_n\}$. Очевидно, что это биективное отображение. Далее, если

$$a = a_1e_1 + a_2e_2 + \ldots + a_ne_n,$$
$$b = b_1e_1 + b_2e_2 + \ldots + b_ne_n,$$

то

$$a + b = (a_1 + b_1)e_1 + (a_2 + b_2)e_2 + \ldots + (a_n + b_n)e_n,$$
$$\lambda a = (\lambda a)e_1 + (\lambda a_2)e_2 + \ldots + (\lambda a_n)e_n.$$

Отсюда следует, что f — изоморфизм.

Пример 9. Пространство E^2 (соотв. E^3) изоморфно $\mathbb{R}^2$ (соотв. $\mathbb{R}^3$).

1.8. Алгебры

Ввиду крайней простоты своего строения векторные пространства не интересны сами по себе, но они служат необ-

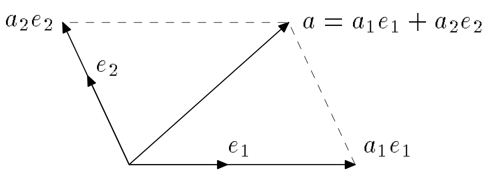

Рис. 5.

ходимым фоном для многих алгебраических (и не только алгебраических) теорий. Так, комбинируя понятия векторного пространства и кольца, мы приходим к важному понятию алгебры.

Определение. Алгеброй над полем K называется множество A с операциями сложения, умножения и умножения на элементы поля K, обладающими следующими свойствами:

1) относительно сложения и умножения на элементы поля A есть векторное пространство;

2) относительно сложения и умножения A есть кольцо;

3) $(\lambda a)b = a(\lambda b) = \lambda(ab) \quad \forall \lambda \in K,\ a, b \in A$.

Замечание. Термин «алгебра», употреблявшийся нами до сих пор только как название одного из разделов математики, в этом определении имеет, естественно, другой смысл.

Пример 1. Всякое поле L, содержащее K в качестве подполя, можно рассматривать как алгебру над K. В частности, поле $\mathbb{C}$ есть алгебра над $\mathbb{R}$.

Пример 2. Пространство E^3 есть алгебра относительно операции векторного умножения.

Пример 3. Множество $F(X, K)$ функций на множестве X со значениями в поле K (см. пример 7.2) является алгеброй над K относительно обычных операций сложения и умножения функций и умножения функции на число. Эта алгебра коммутативна, ассоциативна и обладает единицей (каковой является функция, тождественно равная единице).

Задача. Доказать, что кольцо 2^M из задачи 3.1 превращается в алгебру над полем $\mathbb{Z}_2$, если определить в нем умножение на элементы этого поля по правилам

$$0A = \varnothing, \quad 1A = A \quad \forall A \in 2^M.$$

Предположим, что алгебра A обладает базисом $\{e_1, e_2, \ldots, e_n\}$ как векторное пространство над K, и пусть

$$a = a_1e_1 + a_2e_2 + \ldots + a_ne_n = \sum_{i=1}^{n} a_ie_i,$$

$$b = b_1e_1 + b_2e_2 + \ldots + b_ne_n = \sum_{i=1}^{n} b_ie_i$$

— два произвольных элемента этой алгебры. Тогда из дистрибутивности умножения относительно сложения и свойства 3) в определении алгебры следует, что

$$ab = \sum_{i=1}^{n} a_i(e_i b) = \sum_{i=1}^{n} a_i \left(\sum_{j=1}^{n} b_j(e_i e_j) \right) = \sum_{i,j=1}^{n} a_i b_j (e_i e_j).$$

Это показывает, что умножение в алгебре A полностью определяется произведениями базисных векторов.

Если умножение базисных векторов коммутативно, т. е.

$$e_i e_j = e_j e_i \quad \forall i, j,$$

то и умножение в алгебре A в целом коммутативно. В самом деле, для любых $a, b \in A$ мы тогда в предыдущих обозначениях получаем:

$$ab = \sum_{i,j} a_i b_j (e_i e_j) = \sum_{i,j} b_j a_i (e_j e_i) = ba.$$

Аналогично доказывается, что если умножение базисных векторов ассоциативно, т. е.

$$(e_i e_j) e_k = e_i (e_j e_k) \quad \forall i, j, k,$$

то и умножение в алгебре A в целом ассоциативно.

С другой стороны, если V — какое-то векторное пространство с базисом $\{e_1, e_2, \ldots, e_n\}$ и e_{ij} $(i, j = 1, 2, \ldots, n)$ — произвольные векторы этого пространства, то мы можем определить операцию умножения в V по правилу

$$ab = \sum_{i,j} a_i b_j e_{ij}$$

и тем самым превратить V в алгебру.

Пример 4. Поле $\mathbb{C}$ как алгебра над $\mathbb{R}$ задается следующей таблицей умножения базисных векторов:

$\times$	1	i
1	1	i
i	i	-1

Проверка коммутативности и ассоциативности умножения в $\mathbb{C}$ сводится к тривиальной проверке коммутативности и ассоциативности умножения элементов 1 и i.

Пример 5. В ортонормированном (т. е. состоящее из ортогональных единичных векторов) базисе $\{i, j, k\}$ пространства E^3 таблица векторного умножения выглядит следующим образом:

$\times$	i	j	k
i	0	k	$-j$
j	$-k$	0	i
k	j	$-i$	0

Это умножение антикоммутативно и удовлетворяет тождеству Якоби (см. пример 3.4). Последнее тождество достаточно проверить для базисных векторов, что не составляет труда (проделайте это!).

Пример 6. Алгебра кватернионов $\mathbb{H}$ задается базисом $\{1, i, j, k\}$ со следующей таблицей умножения:

$\times$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

Эта алгебра ассоциативна (проверьте это!), но не коммутативна. Она содержит в качестве подалгебры (см. определение ниже) алгебру комплексных чисел. Позже мы увидим, что в алгебре $\mathbb{H}$, как в поле, всякий ненулевой элемент обратим. Таким образом, это «некоммутативное поле».

Подмножество алгебры называется подалгеброй, если оно одновременно является подпространством и подкольцом. Отображение алгебр называется изоморфизмом, если оно одновременно является изоморфизмом векторных пространств и колец.

1.9. Алгебра матриц

Матрицей размера $m \times n$ над полем K называется прямоугольная таблица из элементов поля K, имеющая m строк и n столбцов. В буквенной записи элементы матрицы обычно обозначаются одной и той же буквой с двумя индексами, первый из которых есть номер строки, а второй — номер столбца:

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}.$$

Иногда ради краткости мы будем писать просто $A = (a_{ij})$.

Суммой матриц $A = (a_{ij})$ и $B = (b_{ij})$ одинакового размера называется матрица

$$A + B = (a_{ij} + b_{ij}).$$

Произведением матрицы $A = (a_{ij})$ на элемент $\lambda \in K$ называется матрица

$$\lambda A = (\lambda a_{ij}).$$

Относительно этих двух операций все матрицы размера $m \times n$ образуют векторное пространство, которое мы будем обозначать $K^{m \times n}$. По сути дела оно не отличается от пространства строк K^{mn}. Специфика матриц проявляется при определении их умножения.

Произведением матрицы $A = (a_{ij})$ размера $m \times n$ и матрицы $B = (b_{jk})$ размера $n \times p$ называется матрица $AB = (c_{ik})$ размера $m \times p$, элементы которой находятся по формулам

$$c_{ik} = \sum_{j=1}^{n} a_{ij} b_{jk}.$$

(Смысл этого определения выяснится в §2.3)

Подчеркнем, что произведение двух матриц определено только тогда, когда их размеры согласованы, а именно, когда число столбцов первой матрицы равно числу строк второй.

Пример 1.

$$\begin{pmatrix} 1 & 0 & 2 \\ 0 & -1 & 3 \end{pmatrix} \begin{pmatrix} 2 & -1 \\ 0 & 5 \\ 1 & 1 \end{pmatrix} =$$

$$= \begin{pmatrix} (1 \cdot 2 + 0 \cdot 0 + 2 \cdot 1) & (1 \cdot (-1) + 0 \cdot 5 + 2 \cdot 1) \\ (0 \cdot 2 + (-1) \cdot 0 + 3 \cdot 1) & (0 \cdot (-1) + (-1) \cdot 5 + 3 \cdot 1) \end{pmatrix} =$$

$$= \begin{pmatrix} 4 & 1 \\ 3 & -2 \end{pmatrix}.$$

Пример 2.

$$\begin{pmatrix}\cos\alpha & -\sin\alpha\\ \sin\alpha & \cos\alpha\end{pmatrix}\begin{pmatrix}\cos\beta & -\sin\beta\\ \sin\beta & \cos\beta\end{pmatrix}=$$
$$=\begin{pmatrix}\cos\alpha\cos\beta-\sin\alpha\sin\beta & -\cos\alpha\sin\beta-\sin\alpha\cos\beta\\ \sin\alpha\cos\beta+\cos\alpha\sin\beta & -\sin\alpha\sin\beta+\cos\alpha\cos\beta\end{pmatrix}=$$
$$=\begin{pmatrix}\cos(\alpha+\beta) & -\sin(\alpha+\beta)\\ \sin(\alpha+\beta) & \cos(\alpha+\beta)\end{pmatrix}.$$

Умножение матриц ассоциативно в том смысле, что

$$(AB)C=A(BC), \tag{9}$$

если только размеры матриц A, B, C согласованы таким образом, что указанные произведения имеют смысл.

В самом деле, пусть

$$(AB)C=(u_{il}),\quad A(BC)=(v_{il}).$$

Имеем тогда:

$$u_{il}=\sum_k\left(\sum_j a_{ij}b_{jk}\right)c_{kl}=\sum_{j,k}a_{ij}b_{jk}c_{kl},$$
$$v_{il}=\sum_j a_{ij}\left(\sum_k b_{jk}c_{kl}\right)=\sum_{j,k}a_{ij}b_{jk}c_{kl},$$

так что $u_{il}=v_{il}$.

Матрица размера $n\times n$ называется квадратной матрицей порядка n. Квадратная матрица имеет две диагонали. Одна из них, ведущая из левого верхнего угла в правый нижний, называется главной диагональю, или просто диагональю, а другая — побочной диагональю. Квадратная матрица называется диагональной, если все ее элементы, находящееся вне (главной) диагонали, равны нулю. Умножение на диагональные матрицы выглядит особенно просто:

$$\begin{pmatrix}a_1 & & & 0\\ & a_2 & & \\ & & \ddots & \\ 0 & & & a_n\end{pmatrix}\begin{pmatrix}b_{11} & b_{12} & \ldots & b_{1p}\\ b_{21} & b_{22} & \ldots & b_{2p}\\ \ldots & \ldots & \ldots & \ldots\\ b_{n1} & b_{n2} & \ldots & b_{np}\end{pmatrix}=\begin{pmatrix}a_1b_{11} & a_1b_{12} & \ldots & a_1b_{1p}\\ a_2b_{21} & a_2b_{22} & \ldots & a_2b_{2p}\\ \ldots & \ldots & \ldots & \ldots\\ a_nb_{n1} & a_nb_{n2} & \ldots & a_nb_{np}\end{pmatrix}.$$

(каждая строка второй матрицы умножается на соответствующий диагональный элемент первой матрицы) и, аналогично,

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} \begin{pmatrix} b_1 & & & 0 \\ & b_2 & & \\ & & \ddots & \\ 0 & & & b_n \end{pmatrix} = \begin{pmatrix} a_{11}b_1 & a_{12}b_2 & \dots & a_{1n}b_n \\ a_{21}b_1 & a_{22}b_2 & \dots & a_{2n}b_n \\ \dots & \dots & \dots & \dots \\ a_{m1}b_1 & a_{m2}b_2 & \dots & a_{mn}b_n \end{pmatrix}$$

(каждый столбец первой матрицы умножается на соответствующий диагональный элемент второй матрицы).

Диагональная матрица вида

$$E = \begin{pmatrix} 1 & & & 0 \\ & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix}$$

называется единичной матрицей. Из предыдущих формул следует, что для любой матрицы A размера $m \times n$

$$AE = A, \quad EA = A, \tag{10}$$

где E в первом случае обозначает единичную матрицу порядка n, а во втором — единичную матрицу порядка m.

Следующие очевидные свойства связывают операцию умножения матриц с другими операциями:

$$A(B + C) = AB + AC, \quad (A + B)C = AC + BC, \tag{11}$$

$$(\lambda A)B = A(\lambda B) = \lambda(AB) \quad \forall \lambda \in K. \tag{12}$$

(Как и в свойстве ассоциативности, здесь предполагается, что размеры матриц согласованы таким образом, что все указанные действия имеют смысл.)

Сумма и произведение квадратных матриц одного и того же порядка n определены и также являются квадратными матрицами порядка n. Свойства (9)–(12) показывают, что все квадратные матрицы порядка n образуют ассоциативную алгебру с единицей. Мы будем обозначать ее $L_n(K)$.

Отметим некоторые «отрицательные» свойства алгебры $L_n(K)$ при $n \geqslant 2$. (Алгебра $L_1(K)$ есть поле K.)

1) Алгебра $L_n(K)$ не коммутативна. При $n = 2$ это можно продемонстрировать на следующем примере:

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

Аналогичные примеры можно привести и при $n > 2$.

2) Алгебра $L_n(K)$ имеет делители нуля. Это показывает, например, второе из приведенных выше равенств. Более того, существуют такие ненулевые матрицы, квадрат которых равен нулю, например,

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

3) Не всякий ненулевой элемент алгебры $L_n(K)$ обратим. Это следует из наличия делителей нуля и того факта, что делитель нуля не может быть обратим (см. доказательство отсутствия делителей нуля в поле, данное в §1.3). Так, например, матрицы $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ и $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ необратимы в $L_2(K)$.

Задача 1. Матрица E_{ij}, у которой на (i, j)-м месте стоит 1, а на остальных местах — нули, называется матричной единицей (не путать с единичной матрицей!). Матричные единицы E_{ij} $(i, j = 1, \ldots, n)$ образуют базис векторного пространства $L_n(K)$. Выписать таблицу умножения алгебры $L_n(K)$ в этом базисе.

Задача 2. Матрицы вида λE $(\lambda \in K)$ называются скалярными. Очевидно, что всякая скалярная матрица перестановочна со всеми квадратными матрицами того же порядка. Доказать обратное: всякая квадратная матрица, перестановочная со всеми квадратными матрицами того же порядка, скалярна.

Задача 3. Доказать, что в алгебре $L_2(\mathbb{R})$ матрицы вида

$$\begin{pmatrix} a & -b \\ b & a \end{pmatrix}, \quad a, b \in \mathbb{R},$$

образуют подалгебру, изоморфную алгебре комплексных чисел.

Задача 4. Доказать, что в алгебре $L_2(\mathbb{C})$, рассматриваемой как алгебра над $\mathbb{R}$, матрицы вида

$$\begin{pmatrix} a & -\overline{b} \\ b & \overline{a} \end{pmatrix}, \quad a, b \in \mathbb{C},$$

образуют подалгебру, изоморфную алгебре кватернионов (см. пример 8.6).

Для каждой матрицы

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \multicolumn{4}{c}{\dotfill} \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

определим транспонированную матрицу

$$A^T = \begin{pmatrix} a_{11} & a_{21} & \dots & a_{m1} \\ a_{12} & a_{22} & \dots & a_{m2} \\ \multicolumn{4}{c}{\dotfill} \\ a_{1n} & a_{2n} & \dots & a_{mn} \end{pmatrix},$$

строками которой служат столбцы матрицы A, а столбцами — строки матрицы A. Если (i,j)-й элемент транспонированной матрицы обозначить через a_{ij}^T, то

$$a_{ij}^T = a_{ji}.$$

Очевидно, что

$$(A^T)^T = A.$$

Очевидно также, что

$$(A+B)^T = A^T + B^T,$$
$$(\lambda A)^T = \lambda A^T \quad \forall \lambda \in K.$$

Докажем, что

$$(AB)^T = B^T A^T.$$

В самом деле, пусть $AB = C = (c_{ik})$; тогда

$$c_{ki}^T = c_{ik} = \sum_j a_{ij} b_{jk} = \sum_j b_{kj}^T a_{ji}^T,$$

откуда видно, что $C^T = B^T A^T$.

Замечание. Читатель может проследить, что все построения последних трех параграфов проходят без изменений, если в качестве K взять произвольное коммутативное ассоциативное кольцо с единицей, например, кольцо целых чисел или кольцо вычетов. Единственное отличие является терминологическим: вместо термина «векторное пространство» в этой более общей ситуации употребляется термин «модуль».