§ 4. Универсальные алгебры и их основные типы

Б.М.Верников

Уральский федеральный университет,
Институт естественных наук и математики,
кафедра алгебры и фундаментальной информатики

4.1. Определение и примеры универсальных алгебр

Определение

Пусть S — непустое множество, а n — натуральное число. *n-арной алгебраической операцией* на множестве S называется отображение из множества S^n (т. е. n-й декартовой степени множества S) в S. При маленьких значениях n ($n = 1, 2, 3$) n-арные операции имеют специальные названия. При $n = 1$ n-арная операция называется *унарной*, при $n = 2$ — *бинарной*, при $n = 3$ — *тернарной*. 0-*арной операцией* на S называется выделение некоторого фиксированного элемента множества S.

В табл. 1 на следующем слайде приведены примеры операций на различных множествах.

Операции на множестве (примеры)

Табл. 1. Множества и операции на них

Множества	Операции		
	0-арные	унарные	бинарные
$\mathbb{N}$	1	$x+1$, $x!$	$x+y$, xy, x^y, $\min\{x,y\}$, $\max\{x,y\}$, НОД(x,y), НОК(x,y)
$\mathbb{Z}$	0, 1	$-x$, $\lvert x\rvert$	$x+y$, $x-y$, xy, $\min\{x,y\}$, $\max\{x,y\}$
$\mathbb{Q}$	0, 1	$-x$, $\lvert x\rvert$, $[x]$	$x+y$, $x-y$, xy, $\min\{x,y\}$, $\max\{x,y\}$
$\mathbb{R}$	0, 1	$-x$, $\lvert x\rvert$, $[x]$, $\sqrt[3]{x}$, e^x, $\sin x$, $\cos x$	$x+y$, $x-y$, xy, $\min\{x,y\}$, $\max\{x,y\}$
$\mathcal{B}(S)$	$\varnothing, S$	$\overline{A}$	$A\cup B, A\cap B, A\setminus B$
Множество всех отображений из S в S	ε	—	fg
Множество всех слов над алфавитом X (включая пустое)	λ (пустое слово)	—	**uv**

Аргументы и результат операции

В общем случае мы будем записывать n-арную алгебраическую операцию на некотором множестве в виде $f(x_1, x_2, \ldots, x_n)$. При этом элементы $x_1, x_2, \ldots, x_n$ называются *аргументами* операции f, а элемент $f(x_1, x_2, \ldots, x_n)$ (при фиксированных $x_1, x_2, \ldots, x_n$) — ее *результатом*. Как правило, мы будем опускать слово «алгебраическая» и называть алгебраические операции просто операциями.

Операции на множестве (комментарии)

Многие естественные и важные операции (в широком смысле этого слова) не являются алгебраическими. Это объясняется тремя причинами.

1) Результат n-арной операции должен быть определен для любой n-ки элементов основного множества. Поэтому не являются алгебраическими операции вычитания на множестве $\mathbb{N}$ (если $x < y$, то $x - y \notin \mathbb{N}$), деления на множествах $\mathbb{Q}$ и $\mathbb{R}$ (результат не определен, если делитель равен 0), извлечения квадратного корня на множестве $\mathbb{R}$ (если $x < 0$, то $\sqrt{x}$ не существует) и взятия обратного отображения (поскольку оно существует только для инъективных отображений).

2) Все аргументы операции должны принадлежать одному и тому же множеству. Поэтому не является алгебраической операцией произведение отображения из A в B на отображение из B в C (за исключением случая, когда $A = B = C$). По той же причине не является алгебраической операция умножения вектора на число, если рассматривать ее как операцию от двух аргументов (но операция умножения вектора на фиксированное число является унарной операцией на множестве всех векторов).

3) Результат операции должен принадлежать исходному множеству. Поэтому не является алгебраической операция скалярного произведения векторов, результатом которой является число.

Универсальные алгебры

Определение

Универсальной алгеброй (или просто *алгеброй*) называется совокупность непустого множества A и произвольного набора Ω заданных на A алгебраических операций. Такая алгебра обозначается через $\mathcal{A} = \langle A; \Omega \rangle$. Множество A называется *основным множеством* или *носителем* алгебры $\mathcal{A}$, а множество Ω — *сигнатурой* этой алгебры. В тех случаях, когда сигнатура будет ясна из контекста, мы часто будем отождествлять алгебру $\mathcal{A}$ с ее основным множеством A.

Универсальными алгебрами являются, например: множество $\mathbb{N}$ с бинарной операцией сложения чисел; то же самое множество с бинарными операциями сложения и умножения (таким образом, на одном и том же носителе могут существовать много различных алгебр); множество $\mathbb{Q}$ с бинарной операцией умножения чисел, унарной операцией взятия числа, обратного к данному, и 0-арной операцией 1; множество всех отображений некоторого множества в себя с операцией произведения отображений; булеан множества S с бинарными операциями объединения и пересечения и унарной операцией дополнения; множество всех векторов с бинарной операцией сложения векторов и набором всевозможных унарных операций умножения на число t, где t пробегает множество $\mathbb{R}$ и т.д. Последний пример показывает, что сигнатура алгебры может быть бесконечной.

4.2. Полугруппы и моноиды

Произвольная универсальная алгебра — это очень общее понятие. Мы будем рассматривать несколько частных случаев этого понятия.

Определение

Группоидом называется универсальная алгебра, сигнатура которой состоит из одной бинарной операции.

Группоидами являются, например, множество $\mathbb{Z}$ с операцией сложения, множество $\mathbb{R}$ с операцией умножения, множество $\mathcal{B}(S)$ с операцией разности множеств и т. д. Операцию в произвольном группоиде часто называют *умножением* и обозначают так же, как умножение чисел: точкой или отсутствием символа (т. е. $x \cdot y$ или xy).

Ассоциативность

Определение

Бинарная операция f, заданная на множестве A, называется *ассоциативной*, если $f\big(f(x,y),z\big) = f\big(x,f(y,z)\big)$ для любых $x,y,z \in A$. Если писать xy вместо $f(x,y)$, то ассоциативность операции означает, что $(xy)z = x(yz)$ для любых $x,y,z \in A$.

Если операция ассоциативна, то в записях вида $x_1 x_2 \cdots x_n$ скобок можно не ставить, так как результат операции от их расстановки не зависит.

Почти все упоминавшиеся выше бинарные операции ассоциативны. Этим свойством обладают, в частности, операции сложения и умножения чисел, объединения и пересечения множеств, сложения векторов, произведения отображений. Единственным исключением является операция разности множеств. О неассоциативности этой операции уже упоминалось в § 1. Еще одним примером неассоциативной бинарной операции является векторное произведение векторов, изучаемое в курсе аналитической геометрии.

Полугруппы

Определение

Полугруппой называется группоид, в котором сигнатурная бинарная операция ассоциативна.

Мы многократно встречались ранее с полугруппами — это, например:

- любое из множеств $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{Z}_n$ с любой из операций сложения и умножения;
- множество $\mathcal{B}(S)$ с любой из операций объединения и пересечения;
- множество всех отображений произвольного непустого множества S в себя с операцией произведения отображений;
- множество всех непустых слов X^+ или множество всех слов X^* над алфавитом X с операцией приписывания слов.

Нейтральные элементы

Важным частным случаем полугрупп являются моноиды. Чтобы дать соответствующее определение, нам понадобится одно новое понятие.

Определение

Пусть A — группоид с бинарной операцией f. Элемент $e \in A$ называется *нейтральным* относительно f, если $f(x, e) = f(e, x) = x$ для любого $x \in A$. Если писать xy вместо $f(x, y)$, то нейтральность элемента e означает, что $xe = ex = x$ для любого $x \in A$.

Замечание 4.1

Если группоид содержит нейтральный элемент, то этот элемент является единственным.

Доказательство. Пусть e_1 и e_2 — нейтральные элементы группоида A с операцией f. Тогда из нейтральности элемента e_1 вытекает, что $f(e_1, e_2) = e_2$, а из нейтральности e_2 — что $f(e_1, e_2) = e_1$. Следовательно, $e_1 = e_2$. □

Моноиды

Определение

Моноидом называется универсальная алгебра, сигнатура которой состоит из ассоциативной бинарной операции f и 0-арной операции, которая выделяет нейтральный относительно f элемент.

Иными словами, моноид — это полугруппа, на которой дополнительно задана 0-арная операция, выделяющая элемент, нейтральный относительно умножения. Нейтральный элемент в произвольном моноиде часто называется *единицей* и обозначается через 1.

Примерами моноидов являются следующие алгебры:

- $\langle \mathbb{Z}; \cdot, 1 \rangle$ и $\langle \mathbb{Z}; +, 0 \rangle$ (вместо $\mathbb{Z}$ здесь можно взять любое из множеств $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{Z}_n$, но не $\mathbb{N}$);
- $\langle \mathcal{B}(S); \cup, \varnothing \rangle$ и $\langle \mathcal{B}(S); \cap, S \rangle$;
- множество всех отображений данного множества в себя с операциями произведения отображений и выделения тождественного отображения;
- множество X^* (но не X^+) с операциями приписывания слов и выделения пустого слова.

4.3. Группы

Определение

Пусть A — моноид с нейтральным элементом e. Элемент $y \in A$ называется *обратным* к элементу $x \in A$, если $xy = yx = e$. Элемент, обратный к x, обозначается через x^{-1}. Элемент $x \in A$ называется *обратимым*, если существует элемент, обратный к x.

Лемма 4.1

Если элемент x моноида $\langle A; \cdot, e\rangle$ обратим, то обратный к x элемент является единственным.

Доказательство. Пусть y и z — элементы, обратные к x. Тогда $z = ez = (yx)z = y(xz) = ye = y$. □

Свойства обратных элементов

Если элементы x и y моноида $\langle A; \cdot, e\rangle$ обратимы, то:

1) *элемент x^{-1} обратим и $(x^{-1})^{-1} = x$;*
2) *элемент xy обратим и $(xy)^{-1} = y^{-1}x^{-1}$.*

Доказательство. 1) По определению обратного элемента, для всякого $x \in A$ выполнены равенства $x^{-1}x = xx^{-1} = e$. Это означает, что элемент x является обратным к x^{-1}. В частности, элемент x^{-1} обратим.

2) Заметим, что $(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xex^{-1} = xx^{-1} = e$. Аналогично проверяется, что $(y^{-1}x^{-1})xy = e$. Следовательно, элемент $y^{-1}x^{-1}$ является обратным к xy. В частности, элемент xy обратим. □

- Заметим, что мы не использовали в доказательстве свойства 1) ассоциативность операции $\cdot$. Таким образом, это свойство выполнено не только в моноиде, но и в произвольном группоиде с нейтральным элементом.

Группы (1)

Определение

Группой называется моноид, в котором все элементы обратимы.

Таким образом, группа — это универсальная алгебра, сигнатура которой состоит из ассоциативной бинарной операции, унарной операции взятия элемента, обратного к данному, и 0-арной операции выделения нейтрального элемента.

Приведем несколько примеров групп. Отметим, что для того, чтобы это сделать, достаточно указать основное множество и бинарную операцию, играющую роль умножения. Из определения этой операции, как правило, уже легко вытекает, какой элемент является нейтральным, и как «устроена» операция взятия обратного элемента.

Пример 1. Любое из множеств $\mathbb{Z}$, $\mathbb{Q}$ и $\mathbb{R}$ является группой относительно сложения. Очевидно, что нейтральным элементом в этих группах является число 0, а элементом, обратным к x, — число $-x$. Эти группы называют *аддитивными* группами целых, рациональных и действительных чисел соответственно.

Группы (2)

Пример 2. Множество всех ненулевых рациональных чисел, равно как и множество всех ненулевых действительных чисел, образует группу относительно умножения. Роль нейтрального элемента здесь играет число 1, а роль элемента, обратного к x, — число $\frac{1}{x}$. Эти группы называют *мультипликативными* группами рациональных и действительных чисел соответственно.

Пример 3. Группой является и множество всех векторов с операцией сложения векторов. Здесь нейтральный элемент — это $\vec{0}$, а элемент, обратный к $\vec{x}$, — вектор $-\vec{x}$.

Коммутативность. Абелевы группы

Укажем еще один важный тип бинарных операций.

Определение

Бинарная операция f, заданная на множестве A, называется *коммутативной*, если $f(x, y) = f(y, x)$ для любых $x, y \in A$. Если писать xy вместо $f(x, y)$, то коммутативность операции означает, что $xy = yx$ для любых $x, y \in A$.

Определения

Группа G называется *абелевой*, если ее бинарная операция коммутативна (т. е. если $xy = yx$ для любых $x, y \in G$). Если бинарная операция в группе коммутативна, то ее часто называют *сложением* и обозначают символом $+$. Нейтральный элемент относительно такой операции обычно называется *нулем* и обозначается символом 0, а элемент, обратный к x относительно сложения, как правило, называется *противоположным* к x и обозначается через $-x$.

Все группы, указанные в примерах 1–3, абелевы. Чтобы привести пример неабелевой группы, введем одно новое понятие.

Определение

Пусть S — непустое множество. Взаимно однозначное отображение множества S на себя называется *подстановкой* на S.

Продолжим список примеров групп.

Пример 4. Произведение биективных отображений и отображение, обратное к биективному, биективны (см. замечания 1.2 и 1.3). Поэтому множество всех подстановок на данном множестве S образует группу относительно операции произведения отображений. Роль нейтрального элемента играет здесь тождественная подстановка, а роль подстановки, обратной к подстановке f, — отображение, обратное к f (отображение f^{-1} существует в силу того, что всякая подстановка взаимно однозначна — см. предложение 1.1). Группа подстановок на множестве X называется *симметрической группой* на X. Симметрическая группа на n-элементном множестве обозначается через $\mathbf{S}_n$.

Неабелевость группы $\mathbf{S}_n$ при $n > 2$

Если $n > 2$, то группа $\mathbf{S}_n$ неабелева. В самом деле, пусть $X = \{x_1, x_2, \ldots, x_n\}$ и $n > 2$. Определим подстановки α и β на X следующим образом: α отображает x_1 и x_2 друг в друга, оставляя остальные элементы на месте, а β отображает x_1 и x_3 друг в друга, оставляя остальные элементы на месте. Тогда

$$(\alpha\beta)(x_1) = \beta\big(\alpha(x_1)\big) = \beta(x_2) = x_2, \quad \text{а}$$
$$(\beta\alpha)(x_1) = \alpha\big(\beta(x_1)\big) = \alpha(x_3) = x_3.$$

Следовательно, $\alpha\beta \neq \beta\alpha$.

4.4. Кольца

Определение

Пусть f и g — бинарные операции на множестве S. Операция g называется *дистрибутивной относительно* f, если $g\big(f(x,y),z\big) = f\big(g(x,z),g(y,z)\big)$ и $g\big(x,f(y,z)\big) = f\big(g(x,y),g(x,z)\big)$ для любых $x,y,z \in S$.

Если заменить в этом определении $f(x,y)$ на $x+y$, а $g(x,y)$ на xy, и договориться о том, что, как обычно, умножение имеет приоритет перед сложением, то равенства из определения примут знакомый и привычный вид: $(x+y)z = xz+yz$ и $x(y+z) = xy+xz$.

Примерами дистрибутивности являются дистрибутивность умножения относительно сложения на всех числовых множествах, дистрибутивность объединения [пересечения] множеств относительно их пересечения [объединения].

Определение

Кольцом называется универсальная алгебра R, сигнатура которой состоит из двух бинарных операций (одну из которых мы будем называть *сложением* и обозначать через $x + y$, другую — *умножением* и обозначать через $x \cdot y$ или xy) таких, что выполнены следующие условия:

1) $\langle R; + \rangle$ — абелева группа;
2) умножение дистрибутивно относительно сложения.

Группа $\langle R; + \rangle$ называется *аддитивной группой кольца*, ее нейтральный элемент обозначается через 0 и называется *нулем*, а элемент, обратный к элементу $x \in R$, называется *противоположным* к x и обозначается через $-x$. Если умножение ассоциативно [коммутативно], то кольцо называется *ассоциативным* [соответственно *коммутативным*]. Если в кольце есть нейтральный элемент по умножению, то этот элемент называется *единицей* и обозначается (как правило) через 1, а кольцо называется *кольцом с* 1.

Примеры колец (1)

Пример 1. Множества $\mathbb{Z}$, $\mathbb{Q}$ и $\mathbb{R}$ являются ассоциативно-коммутативными кольцами с 1 относительно обычных операций сложения и умножения.

Пример 2. Пусть n — натуральное число такое, что $n > 1$. Положим $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ и определим на множестве $\mathbb{Z}_n$ операции сложения $\oplus$ и умножения $\otimes$ следующим образом: если $x, y \in \mathbb{Z}_n$, то $x \oplus y$ [соответственно $x \otimes y$] — это остаток от деления числа $x + y$ [соответственно xy] на n (здесь $x + y$ и xy — обычные сумма и произведение чисел x и y). Очевидно, что $\langle \mathbb{Z}_n; \oplus, \otimes \rangle$ — ассоциативно-коммутативное кольцо с 1 (противоположным к x является число $n - x$, если $x \neq 0$, и 0, если $x = 0$). Оно называется *кольцом вычетов по модулю* n.

Пример 3. Пусть S — произвольное множество. Булеан множества S с операциями симметрический разности (в роли сложения) и пересечения (в роли произведения) является ассоциативно-коммутативным кольцом с 1. Нулем в этом кольце является пустое множество, единицей — множество S, а элементом, противоположным к произвольному подмножеству A множества S, — само множество A.

Примеры колец (2)

Пример 4. Множество всех векторов с операциями сложения и векторного произведения является кольцом. Этот факт вытекает из свойств сложения и векторного произведения векторов, доказанных в курсе аналитической геометрии. Кольцо векторов некоммутативно, неассоциативно и не содержит единицы. Его некоммутативность вытекает из того, что, как показано в курсе аналитической геометрии, векторное произведение антикоммутативно. Докажем, что кольцо векторов неассоциативно. Пусть $(\vec{e}_1, \vec{e}_2, \vec{e}_3)$ — правый ортонормированный базис пространства. Тогда

$$(\vec{e}_1 \times \vec{e}_1) \times \vec{e}_2 = \vec{0} \times \vec{e}_2 = \vec{0}, \text{ но } \vec{e}_1 \times (\vec{e}_1 \times \vec{e}_2) = \vec{e}_1 \times \vec{e}_3 = -\vec{e}_2.$$

Таким образом, $(\vec{e}_1 \times \vec{e}_1) \times \vec{e}_2 \neq \vec{e}_1 \times (\vec{e}_1 \times \vec{e}_2)$. Докажем, наконец, отсутствие единицы в кольце векторов. Предположим, что $\vec{e}$ — нейтральный элемент этого кольца по умножению, т. е. что $\vec{x} \times \vec{e} = \vec{x}$ для любого вектора $\vec{x}$. Тогда $\vec{x} \perp \vec{x}$, откуда $\vec{x}^2 = 0$, и значит, $\vec{x} = \vec{0}$. Но это противоречит тому, что $\vec{x}$ — любой вектор.

Пример 5. Пусть $\langle R; + \rangle$ — абелева группа с нейтральным элементом 0. Положим $x * y = 0$ для любых $x, y \in R$. Очевидно, что $\langle R; +, * \rangle$ — ассоциативно-коммутативное кольцо. Такие кольца называются *кольцами с нулевым умножением*.

Понятие матрицы

Все кольца, указанные на двух предыдущих слайдах, коммутативны. Чтобы привести пример некоммутативного кольца, введем понятие, которое является одним из важнейших в нашем курсе.

Определение

Пусть R — произвольное ассоциативно-коммутативное кольцо с 1. *Матрицей* над кольцом R называется прямоугольная таблица, составленная из элементов этого кольца, которые мы будем называть *скалярами*. Если матрица содержит m строк и n столбцов, то будем говорить, что она имеет *размер* $m \times n$ (читается: «m на n»). Множество всех матриц размера $m \times n$ над кольцом R обозначается через $R^{m\times n}$. Если число строк матрицы равно числу ее столбцов, то матрица называется *квадратной*. В этом случае вместо термина «матрица размера $n \times n$», как правило, употребляется термин *квадратная матрица порядка* n. Скаляры, из которых составлена матрица, называются *элементами* матрицы. При рассмотрении матриц над кольцом R мы иногда будем называть R *кольцом скаляров*.

- В дальнейшем мы для краткости будем, как правило, опускать упоминание о том, что кольцо скаляров ассоциативно-коммутативно и содержит единицу.

Запись произвольной матрицы

Элемент матрицы обозначается буквой с двумя индексами, при этом первый индекс означает номер строки, а второй — номер столбца, в которых стоит данный элемент. Произвольная матрица размера $m \times n$ записывается следующим образом:

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

Кратко эта матрица записывается в виде $A = (a_{ij})$.

Сложение матриц

Определение

Пусть $A = (a_{ij})$ и $B = (b_{ij})$ — матрицы размера $m \times n$ над кольцом R. *Суммой* матриц A и B называется матрица $C = (c_{ij}) \in R^{m \times n}$ такая, что $c_{ij} = a_{ij} + b_{ij}$ для всех $i = 1, 2, \ldots, m$ и $j = 1, 2, \ldots, n$. Эта матрица обозначается через $A + B$.

- Если матрицы A и B имеют различные размеры, то их сумма не определена.
- Очевидно, что *множество $R^{m \times n}$ с операцией сложения матриц является абелевой группой*. Нейтральным элементом этой группы является матрица, все элементы которой равны 0. Эта матрица называется *нулевой* и обозначается буквой O. Матрицей, противоположной к матрице $A = (a_{ij})$, является матрица $-A = (-a_{ij})$.

Умножение матриц

Введем теперь операцию умножения матриц.

!! *Произведение двух матриц над одним и тем же кольцом определено лишь в случае, когда число столбцов первого сомножителя равно числу строк второго.*

Иными словами, если A и B — матрицы над кольцом R, A имеет размер $k \times \ell$, а B — размер $r \times m$, то произведение AB существует тогда и только тогда, когда $\ell = r$.

Определение

Пусть $A = (a_{ij}) \in R^{k\times\ell}$, а $B = (b_{ij}) \in R^{\ell\times m}$. Тогда *произведением* AB матриц A и B называется матрица $C = (c_{ij}) \in R^{k\times m}$ такая, что

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{i\ell}b_{\ell j}$$

для всех $i = 1, 2, \ldots, k$ и $j = 1, 2, \ldots, m$. Иными словами, c_{ij} есть сумма произведений элементов i-й строки матрицы A на соответствующие элементы j-го столбца матрицы B.

Для краткости правило вычисления элементов произведения матриц часто формулируют так:

- *элемент c_{ij} равен произведению i-й строки матрицы A на j-й столбец матрицы B.*

Единичная матрица

Определения

Если $A = (a_{ij})$ — квадратная матрица порядка n, то элементы $a_{11}, a_{22}, \ldots, a_{nn}$ образуют ее *главную диагональ*. В следующей матрице элементы, расположенные на главной диагонали, выделены красным цветом:

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \ldots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \ldots & a_{2n} \\ a_{31} & a_{32} & a_{33} & \ldots & a_{3n} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & a_{n3} & \ldots & a_{nn} \end{pmatrix}.$$

Квадратная матрица, в которой все элементы на главной диагонали равны 1, а все остальные элементы равны 0, называется *единичной* и обозначается буквой E.

Таким образом, единичная матрица выглядит следующим образом:

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

Свойства произведения матриц (1)

Свойства произведения матриц.

Пусть A, B и C — матрицы над одним и тем же кольцом R. Тогда:

1) $(AB)C = A(BC)$ (*умножение матриц ассоциативно*);
2) $(A+B)C = AC + BC$ (*умножение матриц дистрибутивно справа* относительно сложения);
3) $A(B+C) = AB + AC$ (*умножение матриц дистрибутивно слева* относительно сложения);
4) $AE = A$ *и* $EA = A$.

Во всех четырех свойствах имеется в виду, что размеры матриц таковы, что все операции, возникающие в данном свойстве, выполнимы.

Доказательство. Свойства 2)–4) проверяются простыми вычислениями, основанными на определениях операций над матрицами. Докажем свойство 1). Пусть $A = (a_{ij})$, $B = (b_{ij})$ и $C = (c_{ij})$, причем $A \in R^{m\times n}$ для некоторых m и n. Из существования матриц AB и BC вытекает, что $B \in R^{n\times r}$ и $C \in R^{r\times s}$ для некоторых r и s. Положим $AB = D = (d_{ij})$ и $BC = F = (f_{ij})$. Ясно, что $D \in R^{m\times r}$ и $F \in R^{n\times s}$. Отсюда вытекает, что матрицы $(AB)C$ и $A(BC)$ существуют и лежат в $R^{m\times s}$. Положим $(AB)C = (g_{ij})$ и $A(BC) = (h_{ij})$. Требуется доказать, что $g_{ij} = h_{ij}$ для всех $i = 1, 2, \ldots, m$ и $j = 1, 2, \ldots, s$. В самом деле, используя ассоциативность кольца скаляров, имеем:

$$g_{ij} = \sum_{k=1}^{r} d_{ik}c_{kj} = \sum_{k=1}^{r}\Big[\Big(\sum_{\ell=1}^{n} a_{i\ell}b_{\ell k}\Big)\cdot c_{kj}\Big] = \sum_{k=1}^{r}\sum_{\ell=1}^{n} a_{i\ell}b_{\ell k}c_{kj} =$$

$$= \sum_{\ell=1}^{n}\sum_{k=1}^{r} a_{i\ell}b_{\ell k}c_{kj} = \sum_{\ell=1}^{n}\Big[a_{i\ell}\cdot\Big(\sum_{k=1}^{r} b_{\ell k}c_{kj}\Big)\Big] = \sum_{\ell=1}^{n} a_{i\ell}f_{\ell j} = h_{ij}.$$

Свойство 1) доказано. □

Некоммутативность произведения матриц

Произведение матриц некоммутативно. Иными словами, равенство $AB = BA$ выполняться не обязано. Во-первых, одно из произведений AB и BA может существовать, а другое нет. Например, если матрица A имеет размер 3×5, а B — размер 5×2, то произведение AB существует и имеет размер 3×2, а произведения BA не существует.

Во-вторых, произведения AB и BA могут существовать, но иметь разные размеры. Например, если матрица A имеет размер 2×4, а B — размер 4×2, то произведения AB и BA существуют, но первое из них имеет размер 2×2, а второе — 4×4.

Но даже если произведения AB и BA существуют и имеют одинаковые размеры, равенство $AB = BA$ может не выполняться (и, более того, выполняется крайне редко). Легко понять, что матрицы AB и BA существуют и имеют одинаковые размеры тогда и только тогда, когда A и B — квадратные матрицы одного и того же порядка. Но если написать наугад, например, две квадратных матрицы второго порядка, то их произведения в разных порядках почти наверняка не совпадут. Конкретный пример квадратных матриц одного и того же порядка A и B таких, что $AB \neq BA$, будет приведен на следующем слайде.

Кольцо квадратных матриц

Теперь мы уже можем привести обещанный выше пример некоммутативного кольца. Мы продолжаем при этом начатую ранее нумерацию примеров колец.

Пример 6. Из свойств сложения и умножения матриц вытекает, что множество $R^{n\times n}$ (т. е. множество всех квадратных матриц одного и того же порядка n над одним и тем же кольцом R) с операциями сложения и умножения является ассоциативным кольцом с единицей, роль которой играет единичная матрица порядка n. Это кольцо называется *кольцом квадратных матриц порядка* n или просто *кольцом матриц*.

Если $n > 1$, а кольцо R неодноэлементно, то кольцо матриц $R^{n\times n}$ некоммутативно. Чтобы убедиться в этом, обозначим через A квадратную матрицу порядка n над R, в которой в первой строке и первом столбце стоит 1, а все остальные элементы равны 0, а через B — квадратную матрицу порядка n над R, в которой в первой строке и втором столбце стоит 1, а все остальные элементы равны 0. Непосредственная проверка показывает, что $AB = B$, а $BA = O$. В частности, $AB \neq BA$.

Договоренность о терминологии

Почти все кольца, упоминавшиеся выше, ассоциативны. Единственным исключением является кольцо векторов из примера 4, которое относится больше к геометрии, чем к алгебре. Все кольца, которые будут появляться в дальнейшем в нашем курсе, также будут ассоциативными. Поэтому

! *всюду в дальнейшем, если явно не оговорено противное, слово «кольцо» означает «ассоциативное кольцо».*

Простейшие свойства умножения в кольцах

Если R — кольцо и $x \in R$, то

$$x \cdot 0 = 0 \cdot x = 0. \tag{1}$$

В самом деле, $x \cdot 0 = x(x - x) = x^2 - x^2 = 0$. Равенство $0 \cdot x = 0$ проверяется аналогично.

Если R — кольцо, $x \in R$, а n — натуральное число, то мы будем писать

$$nx = \underbrace{x + \cdots + x}_{n \text{ слагаемых}}.$$

Подчеркнем, что nx — это не произведение числа n на x (*операции произведения натурального числа на элемент кольца не существует!*), а просто обозначение для суммы n экземпляров элемента x. Если $x, y \in R$, а $n \in \mathbb{N}$, то

$$n(xy) = (nx)y, \tag{2}$$

поскольку

$$n(xy) = \underbrace{xy + xy + \cdots + xy}_{n \text{ слагаемых}} = (\underbrace{x + x + \cdots + x}_{n \text{ слагаемых}})y = (nx)y.$$

Делители нуля

Определение

Элемент x кольца R называется *делителем нуля*, если $x \neq 0$ и существуют ненулевые элементы $y, z \in R$ такие, что $xy = 0$ и $zx = 0$.

Делители нуля есть в кольце $\mathbb{Z}_n$ при условии, что n — составное число: если $n = km$, где $1 < k, m < n$, то k и m — делители нуля, так как $k \otimes m = m \otimes k = 0$. Очевидные равенства

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ -1 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \text{ и } \begin{pmatrix} -1 & 1 \\ -1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

показывают, что матрица

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$$

является делителем нуля в кольце $R^{2\times 2}$, где R — произвольное кольцо с 1.

Области целостности

В кольце с нулевым умножением любой ненулевой элемент является делителем нуля. Еще одним примером кольца с таким свойством является кольцо векторов из примера 4, поскольку, как известно, $\vec{x} \times \vec{x} = \vec{0}$ для всякого вектора $\vec{x}$. Но для дальнейшего основной интерес представляет противоположная «крайность» — кольца, не содержащие делителей нуля.

Определение

Ассоциативно-коммутативное кольцо с 1, не содержащее делителей нуля, называется *областью целостности* или *целостным кольцом*. Примерами областей целостности являются кольца $\mathbb{Z}$, $\mathbb{Q}$ и $\mathbb{R}$.

4.5. Поля

Введем новое понятие, которое будет играть очень важную роль в дальнейшем.

Определение

Неодноэлементное ассоциативно-коммутативное кольцо с 1, в котором все ненулевые элементы обратимы (относительно умножения), называется *полем.*

Покажем, что всякое поле является областью целостности.

Замечание 4.2

Поле не содержит делителей нуля.

Доказательство. Все ненулевые элементы поля обратимы относительно умножения. Поэтому достаточно установить, что обратимый (относительно умножения) элемент произвольного ассоциативного кольца с 1 не является делителем нуля. В самом деле, предположим, что элемент x обратим и $xy = 0$ для некоторого $y \in R$. Используя (1), имеем:

$$y = 1 \cdot y = (x^{-1}x)y = x^{-1}(xy) = x^{-1} \cdot 0 = 0.$$

Следовательно, x не является делителем нуля.

Поля (2)

Примерами полей являются кольца $\mathbb{Q}$ и $\mathbb{R}$ с обычными операциями сложения и умножения. Следующее утверждение дает еще один пример поля.

Лемма 4.2

Кольцо вычетов по модулю n является полем тогда и только тогда, когда n — простое число.

Доказательство. *Необходимость.* Как уже отмечалось выше, кольцо $\mathbb{Z}_n$ при составном n содержит делители нуля. Остается учесть замечание 4.2.

Достаточность. Пусть $n = p$ — простое число. Достаточно проверить, что каждый ненулевой элемент кольца $\mathbb{Z}_p$ имеет обратный элемент по умножению. Пусть $s \in \mathbb{Z}_p \setminus \{0\}$, т. е. $1 \leqslant s \leqslant p-1$. Рассмотрим числа $1 \otimes s$, $2 \otimes s$, $\ldots$, $(p-1) \otimes s$. Требуется доказать, что одно из них равно 1. Пусть $k \in \{1, 2, \ldots, p-1\}$. Очевидно, $0 \leqslant k \otimes s \leqslant p-1$. Из того, что $k, s < p$, а p — простое число, вытекает, что p не делит ks. Следовательно, $k \otimes s \neq 0$. Далее, если $k \otimes s = \ell \otimes s$ для некоторых $1 \leqslant k < \ell \leqslant p-1$, то $(\ell - k) \otimes s = 0$ вопреки сказанному выше. Следовательно, все числа $1 \otimes s$, $2 \otimes s$, $\ldots$, $(p-1) \otimes s$ попарно различны. Иными словами, $1 \otimes s$, $2 \otimes s$, $\ldots$, $(p-1) \otimes s$ — это упорядоченные каким-то образом числа $1, 2, \ldots, p-1$. Следовательно, одно из них равно 1, что и требовалось доказать. □

Поля (3)

Определение

Если p — простое число, то поле $\mathbb{Z}_p$ называется *полем вычетов* по модулю p. Для этого поля, наряду с $\mathbb{Z}_p$, часто используется обозначение $\mathbf{GF}(p)$. Это обозначение объясняется тем, что конечные поля (в частности, поля вычетов) часто называют *полями Галуа*.

Определение

Пусть F — произвольное поле. Если существует натуральное число n такое, что $nx = 0$ для всякого $x \in F$, то минимальное n с таким свойством называется *характеристикой* поля F; если такого n не существует, то характеристика поля F полагается равной 0. Характеристика поля F обозначается через $\operatorname{char} F$.

Очевидно, что $\operatorname{char} \mathbb{Q} = \operatorname{char} \mathbb{R} = 0$, а $\operatorname{char} \mathbf{GF}(p) = p$.

Лемма 4.3

Характеристика любого поля равна либо нулю, либо простому числу.

Доказательство. Пусть F — поле, $\operatorname{char} F = n$ и $n = km$ для некоторых k и m таких, что $1 < k, m < n$. Обозначим единицу поля F через e и положим $y = ke$ и $z = me$. Если $y = 0$, то, в силу замечания 2.2б), $\operatorname{char} F = n$ делит k, что неверно. Следовательно, $y \neq 0$. Аналогично проверяется, что $z \neq 0$. Но $yz = (ke)(me) = (km)e^2 = ne = 0$. Таким образом, y и z — делители нуля, которых в поле быть не может. Противоречие. □

Замечание 4.3

Пусть F — поле, а n — натуральное число. Если $na = 0$ для некоторого $a \in F \setminus \{0\}$, то:

а) *$nx = 0$ для всякого $x \in F$;*

б) *характеристика поля F делит n.*

Доказательство. а) Обозначим единицу поля F через e. Пусть $x \in F$. Используя (1) и (2), имеем:

$$nx = n(ex) = n(aa^{-1}x) = (na)(a^{-1}x) = 0 \cdot a^{-1}x = 0.$$

б) Пусть $k = \operatorname{char} F$. Ясно, что $k \neq 0$, так как в противном случае не могло бы выполняться равенство $na = 0$. Предположим, что k не делит n, и обозначим через d наибольший общий делитель k и n. Тогда $d < k$. В силу известного свойства наибольшего общего делителя чисел, существуют натуральные числа u и v такие, что $d = uk + vn$. Пусть $x \in F$. Тогда $nx = 0$ в силу п. а) и $kx = 0$ по определению характеристики поля, откуда

$$dx = (uk + vn)x = ukx + vnx = 0 + 0 = 0.$$

Итак, $dx = 0$ для всякого $x \in F$. Но это невозможно, так как $d < k = \operatorname{char} F$. □

4.6. Подалгебры и гомоморфизмы

В заключение параграфа введем некоторые важные понятия, относящиеся к произвольным универсальным алгебрам.

Определение

Пусть $\langle A; \Omega \rangle$ — универсальная алгебра, а f — n-арная операция из Ω. Непустое подмножество B множества A называется *замкнутым относительно* f, если для любых $x_1, x_2, \ldots, x_n \in B$ имеет место включение $f(x_1, x_2, \ldots, x_n) \in B$. Подмножество B называется *подалгеброй* в A, если оно замкнуто относительно всех операций из Ω.

Примеры подалгебр

Приведем некоторые примеры подалгебр. Любая алгебра A является подалгеброй в самой себе. Единица произвольной группы G образует подгруппу в G, а нуль произвольного кольца R — подкольцо в R. Полугруппа $\langle \mathbb{N}; + \rangle$ является подполугругруппой в полугруппах $\langle \mathbb{Z}; + \rangle$, $\langle \mathbb{Q}; + \rangle$ и $\langle \mathbb{R}; + \rangle$, а кольцо $\langle \mathbb{Z}; +, \cdot \rangle$ — подкольцом в кольцах $\langle \mathbb{Q}; +, \cdot \rangle$ и $\langle \mathbb{R}; +, \cdot \rangle$. Если R — произвольное кольцо, то каждый из следующих пяти наборов матриц является подкольцом в кольце $R^{2\times 2}$:

$$\left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| \, a, b, c \in R \right\}; \quad \left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \middle| \, a, b, c \in R \right\};$$

$$\left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \middle| \, a, b \in R \right\}; \quad \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \middle| \, a \in R \right\}; \quad \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \middle| \, a, b \in R \right\}.$$

В то же время, кольцо вычетов $\langle \mathbb{Z}_n; \oplus, \otimes \rangle$ не является подкольцом кольца $\langle \mathbb{Z}; +, \cdot \rangle$, потому что может оказаться, что сумма (в обычном смысле этого слова) элементов из $\mathbb{Z}_n$ больше, чем $n-1$, и потому не лежит в $\mathbb{Z}_n$.

Гомоморфизмы

Определение

Пусть $\mathcal{A} = \langle A; \Omega \rangle$ и $\mathcal{B} = \langle B; \Omega \rangle$ — две универсальных алгебры с одной и той же сигнатурой Ω. *Гомоморфизмом* из $\mathcal{A}$ в $\mathcal{B}$ называется отображение $f : A \longrightarrow B$ такое, что

$$f\big(\omega(x_1, x_2, \ldots, x_n)\big) = \omega\big(f(x_1), f(x_2), \ldots, f(x_n)\big)$$

для любой операции $\omega \in \Omega$ и любых $x_1, x_2, \ldots, x_n \in A$, где n — арность операции ω.

Гомоморфизмы (рисунок)

Иллюстрацией к понятию гомоморфизма служит рис. 1.

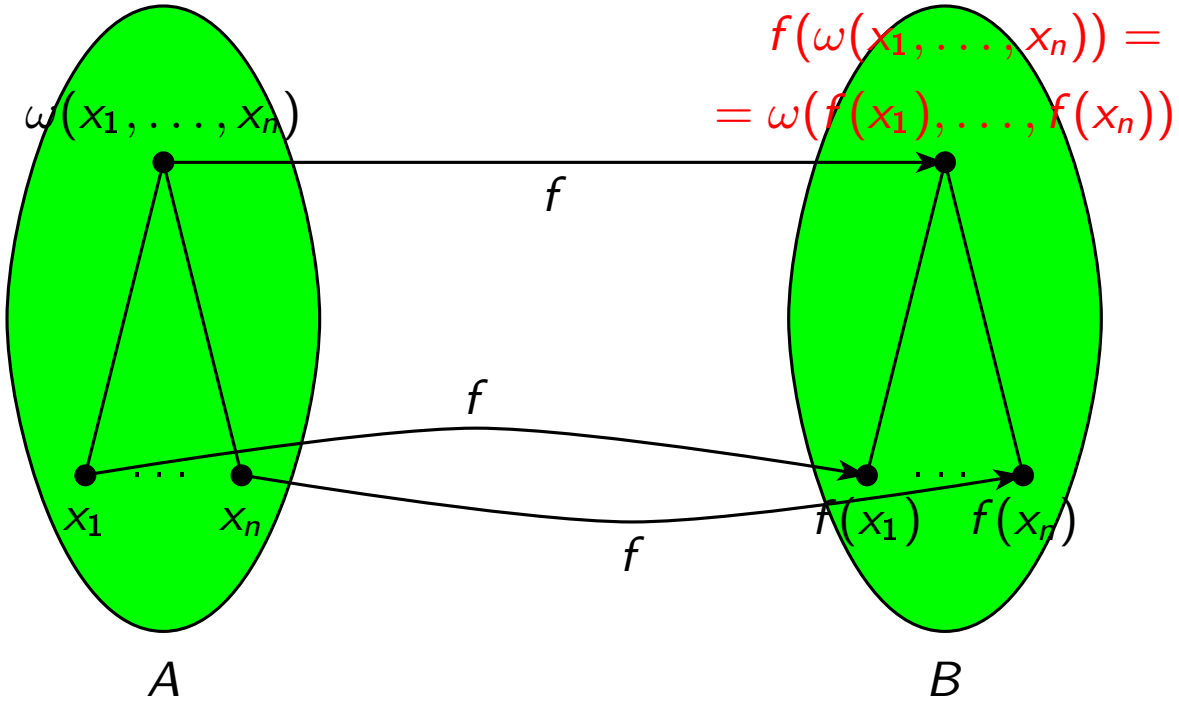

Рис. 1. Гомоморфизм

Изоморфизмы, изоморфные вложения, эндоморфизмы, автоморфизмы

Определения

Пусть $\mathcal{A} = \langle A; \Omega \rangle$ и $\mathcal{B} = \langle B; \Omega \rangle$ — две универсальных алгебры с одной и той же сигнатурой Ω и существует гомоморфизм из $\mathcal{A}$ в $\mathcal{B}$. Если этот гомоморфизм биективен, то он называется *изоморфизмом*, а если он инъективен, то он называется *изоморфным вложением* или просто *вложением*. Если существует изоморфизм из $\mathcal{A}$ на $\mathcal{B}$, то говорят, что алгебры $\mathcal{A}$ и $\mathcal{B}$ *изоморфны*, а если существует изоморфное вложение $\mathcal{A}$ в $\mathcal{B}$, то говорят, что $\mathcal{A}$ *изоморфно вложима* (или просто *вложима*) в $\mathcal{B}$. Гомоморфизм алгебры в себя называется *эндоморфизмом*, а изоморфизм алгебры на себя — *автоморфизмом*.

«Содержательный смысл» понятий изоморфизма и изоморфного вложения

Неформально говоря, существование изоморфизма алгебры $\mathcal{A} = \langle A; \Omega \rangle$ на алгебру $\mathcal{B} = \langle B; \Omega \rangle$ означает, что мы можем «переименовать» элементы из A (элемент x переименовывается в $f(x)$, где f — изоморфизм), после чего все операции над элементами алгебры $\mathcal{B}$ выполняются точно так же, как они выполнялись в $\mathcal{A}$, но под «новыми именами». Иначе говоря, изоморфные алгебры отличаются «внутренней природой» элементов, но неразличимы с точки зрения действия алгебраических операций. Поэтому в алгебре, как правило, отождествляют изоморфные алгебры, считая их одной и той же алгеброй (или различными «реализациями» одной и той же алгебры).

Если же алгебра A вложима в алгебру B, то в B существует подалгебра C, изоморфная A. Алгебры A и C часто отождествляют и считают, что A — подалгебра в B.

Пример гомоморфизма

Пример 1. Положим $\mathcal{A} = \langle \mathbb{Z}; +, \cdot \rangle$ и $\mathcal{B} = \langle \mathbb{Z}_n; \oplus, \otimes \rangle$. Определим отображение f из $\mathbb{Z}$ в $\mathbb{Z}_n$ правилом: если k — целое число, то $f(k)$ — остаток от деления k на n. Легко проверяется, что для любых $k, m \in \mathbb{Z}$ выполнены равенства $f(k+m) = f(k) \oplus f(m)$ и $f(km) = f(k) \otimes f(m)$. Следовательно, f является гомоморфизмом из $\mathcal{A}$ в $\mathcal{B}$. Изоморфизмом это отображение не является, так как оно не инъективно.

Формально говоря, в этом примере сигнатуры алгебр $\mathcal{A}$ и $\mathcal{B}$ различны. Но мы можем «отождествить» операции $+$ и $\oplus$, считая, что это одна и та же операция, обозначенная двумя разными способами. Аналогичное соглашение относится к операциям $\cdot$ и $\otimes$. Важно лишь то, что в каждом из этих случаев обе операции имеют одну и ту же арность.

Пример изоморфизма

Пример 2. Положим $\mathbb{R}_+ = \{x \in \mathbb{R} \mid x > 0\}$. Обозначим через $\mathcal{A}$ полугруппу $\langle \mathbb{R}; + \rangle$, а через $\mathcal{B}$ — полугруппу $\langle \mathbb{R}_+; \cdot \rangle$. Зафиксируем произвольное положительное число $a \neq 1$ и определим отображение $f : \mathbb{R} \longrightarrow \mathbb{R}_+$ правилом: $f(x) = a^x$ для всякого $x \in \mathbb{R}$. Поскольку $a^{x+y} = a^x \cdot a^y$, отображение f является гомоморфизмом из $\mathcal{A}$ в $\mathcal{B}$. Очевидно, что это отображение инъективно (если $x \neq y$, то $a^x \neq a^y$) и сюръективно (если $y \in \mathbb{R}_+$, то $y = f(x)$, где $x = \log_a y$). Следовательно, f — изоморфизм. Таким образом, *полугруппа действительных чисел по сложению изоморфна полугруппе положительных действительных чисел по умножению*.

Как и в примере 1, формально полугруппы $\langle \mathbb{R}; + \rangle$ и $\langle \mathbb{R}_+; \cdot \rangle$ имеют разные сигнатуры, но операции, из которых они состоят, имеют одну и ту же арность, что позволяет нам отождествить эти операции.

Уточнение определения гомоморфизма

Два приведенных примера показывают, что определение гомоморфизма (а значит и всех остальных определенных выше понятий — изоморфизма, изоморфного вложения и т. д.) можно уточнить. А именно, можно считать, что алгебры $\mathcal{A}$ и $\mathcal{B}$ имеют разные сигнатуры, скажем, Ω и Ψ соответственно, но существует биекция Ω на Ψ, отображающая всякую операцию $\omega \in \Omega$ в операцию $\omega^\star \in \Psi$, такая, что операции ω и $\omega^\star$ имеют одну и ту же арность для любой операции $\omega \in \Omega$. Ключевое равенство из определения гомоморфизма при этом имеет вид

$$f\big(\omega(x_1, x_2, \ldots, x_n)\big) = \omega^\star\big(f(x_1), f(x_2), \ldots, f(x_n)\big).$$

Но обычно этого не делают из-за громоздкости этого определения, а просто отождествляют операции ω и $\omega^\star$ для всякой $\omega \in \Omega$.

Примеры изоморфного вложения

Пример 3. Определим отображение f из кольца $\langle \mathbb{Z}; +, \cdot \rangle$ в кольцо $\langle \mathbb{Q}; +, \cdot \rangle$ правилом: $f(n) = \frac{n}{1}$ для всякого $n \in \mathbb{Z}$. Очевидно, что f — изоморфное вложение.

Пример 4. Пусть m и n — натуральные числа, причем $m < n$. Определим отображение f из группы $\mathbf{S}_m$ в группу $\mathbf{S}_n$ правилом: если $\sigma \in \mathbf{S}_m$, то $f(\sigma)$ — подстановка из $\mathbf{S}_n$ такая, что

$$(f(\sigma))(i) = \begin{cases} \sigma(i), & \text{если } 1 \leqslant i \leqslant m, \\ i, & \text{если } m+1 \leqslant i \leqslant n. \end{cases}$$

Легко понять, что f — изоморфное вложение. Это позволяет считать, что $\mathbf{S}_m$ — подгруппа в $\mathbf{S}_n$.

Пример 5. Пусть R — ассоциативно-коммутативное кольцо с 1, а n — натуральное число такое, что $n > 1$. Очевидно, что отображение f из кольца R в кольцо $R^{n \times n}$, задаваемое правилом: если $a \in R$, то

$$f(a) = \begin{pmatrix} a & 0 & 0 & \dots & 0 \\ 0 & a & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & a \end{pmatrix},$$

является изоморфным вложением. Таким образом, всякое кольцо можно рассматривать как подкольцо кольца матриц над собой.

Примеры эндоморфизма и автоморфизма

Пример 6. Пусть S — одно из множеств $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ и $\mathbb{R}$. Определим отображение f из полугруппы $\langle S; + \rangle$ в себя правилом: $f(x) = 2x$ для всякого $x \in S$. Очевидно, что f — инъективный эндоморфизм. Если $S \in \{\mathbb{N}, \mathbb{Z}\}$, то f не является автоморфизмом, так как не сюръективно. Если же $S \in \{\mathbb{Q}, \mathbb{R}\}$, то f — автоморфизм.

Пример 7. Пусть G — произвольная абелева группа. Определим отображение f из G в себя правилом: $f(x) = x^{-1}$ для всякого $x \in G$. Используя абелевость группы G, имеем $(xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1}$. Следовательно, f — эндоморфизм. Кроме того, легко проверяется, что это отображение биективно. Следовательно, f — автоморфизм.