§ 4. Универсальные алгебры и их основные типы

Б.М.Верников

Уральский федеральный университет,
Институт математики и компьютерных наук,
кафедра алгебры и дискретной математики

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 $n = 1$ 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.

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 бинарных отношений на S	Δ_S, ∇_S	$\alpha^{-1}, \alpha^t, \alpha^r$	$\alpha\beta$
Множество всех векторов	$\vec{0}$	$-\vec{a}$	$\vec{a}+\vec{b}$

В общем случае мы будем записывать n-арную алгебраическую операцию на некотором множестве в виде $f(x_1, x_2, \dots, x_n)$ и называть $x_1, x_2, \dots, x_n$ *аргументами* операции f. Как правило, мы будем опускать слово «алгебраическая» и называть алгебраические операции просто операциями. Отметим, однако, что многие естественные и важные операции (в широком смысле этого слова) не являются алгебраическими. В самом деле, по определению n-арной операции, ее результат 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) и извлечения квадратного корня на множестве $\mathbb{R}$ (если $x < 0$, то $\sqrt{x}$ не существует). Результат операции должен быть определен однозначно (еще одна причина, по которой извлечение квадратного корня — не алгебраическая операция на $\mathbb{R}$). Все аргументы операции должны принадлежать исходному множеству. Поэтому не является алгебраической операция умножения вектора на число (см. § 10), если рассматривать ее как операцию от двух аргументов[1]. Наконец, результат операции должен принадлежать исходному множеству. Поэтому не является алгебраической операция скалярного произведения векторов (см. § 11), результатом которой является число.

[1] Но операция умножения вектора на фиксированное число является унарной операцией на множестве всех векторов.

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 операцией сложения чисел; множество $\mathbb{Q}$ с бинарной операцией умножения чисел, унарной операцией взятия числа, обратного к данному, и 0-арной операцией 1; множество всех векторов с бинарной операцией сложения векторов и набором всевозможных унарных операций умножения на число t, где t пробегает множество $\mathbb{R}$. Последний пример показывает, что сигнатура алгебры может быть бесконечной.

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).

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.

Определение

Полугруппой называется группоид, в котором сигнатурная бинарная операция ассоциативна.

Мы многократно встречались ранее с полугруппами — это любое из множеств $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ и $\mathbb{R}$ с любой из операций сложения и умножения, множество $\mathcal{B}(S)$ с любой из операций объединения и пересечения, множество $\mathrm{Eq}(S)$ с операцией произведения бинарных отношений, множество всех векторов с операцией сложения векторов, множество всех отображений произвольного непустого множества S в себя с операцией произведения отображений. Приведем еще один очень важный пример полугруппы. Для произвольного непустого множества X обозначим через X^+ множество всевозможных конечных последовательностей элементов из X. Элементы множества X^+ будем называть *словами* над *алфавитом* X. На множестве X^+ определим операцию *конкатенации* или *приписывания* слов: если $\alpha, \beta \in X^+$, то результат указанной операции — это слово $\alpha\beta$, получаемое приписыванием слова β к слову α справа. Очевидно, что операция приписывания ассоциативна, и потому множество X^+ с этой операцией является полугруппой. Эта полугруппа называется *свободной полугруппой над множеством* X.

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 $x \in S$. Если писать xy вместо $f(x, y)$, то нейтральность элемента e означает, что $xe = ex = x$ для любого $x \in A$.

Замечание о нейтральном элементе

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, $e_1 = e_2$. □

Определение

Моноидом называется универсальная операция, 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: $\langle \mathbb{Z}; \cdot, 1 \rangle$, $\langle \mathbb{Z}; +, 0 \rangle$, $\langle \mathcal{B}(S); \cup, \varnothing \rangle$, $\langle \mathcal{B}(S); \cap, S \rangle$, $\langle \mathrm{Eq}(S); \cdot, \nabla_S \rangle$, множество всех векторов относительно сложения векторов и выделения нулевого вектора, множество всех отображений данного множества в себя с операциями произведения отображений и выделения тождественного отображения. Для произвольного непустого множества X положим $X^* = X^+ \cup \{\varepsilon\}$, где ε — пустое слово, и распространим операцию конкатенации с множества X^+ на множество X^* правилом: $\alpha\varepsilon = \varepsilon\alpha = \alpha$ для любого слова $\alpha \in X^*$. Ясно, что X^* с операциями конкатенации и выделения пустого слова — моноид. Он называется *свободным моноидом над множеством* X.

Определение

Пусть A — моноид с бинарной операцией $\cdot$ и 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 об обратном элементе

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. Свойство 1) очевидно. Свойство 2) вытекает из следующих равенств: $(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xex^{-1} = xx^{-1} = e$. □

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.

В любой группе можно определить операцию *деления* элементов правилом $x/y = xy^{-1}$.

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 $x, y \in A$.

Определение

Группа G называется *абелевой*, если ее бинарная операция коммутативна (т. е. если $xy = yx$ для любых $x, y \in G$).

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.

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 $-\vec{x}$.

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.

Пример 4. 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, в смысле определения обратного отображения, данного в § 1 (отображение f^{-1} существует в силу того, что всякая подстановка взаимно однозначна — см. критерий существования обратного отображения в § 1). Группа подстановок на множестве X называется *симметрической группой на* X. Симметрическая группа на n-элементном множестве обозначается через $\mathbf{S}_n$.

Неабелевость группы $\mathbf{S}_n$

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

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

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

Если бинарная операция 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 $-x$. Такой способ представления операций называется *аддитивным*, поскольку он возник по аналогии со сложением чисел, в отличие от изложенного выше более употребительного *мультипликативного* способа, возникшего по аналогии с умножением чисел.

Определение

Пусть f и g — бинарные операции на множестве S. Операция g называется *дистрибутивной относительно* f, если $g(f(x,y),z) = f(g(x,z),g(y,z))$ и $g(x,f(y,z)) = f(g(x,y),g(x,z))$ 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], дистрибутивность прямого произведения множеств относительно их объединения и пересечения, дистрибутивность умножения вектора на данное число (рассматриваемое как унарная операция над векторами) относительно сложения векторов.

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 (эта группа называется *аддитивной группой кольца*, ее нейтральный элемент обозначается через 0 и называется *нулем*, а элемент, обратный к элементу $x \in A$, называется *противоположным* к x обозначается через $-x$);
2) умножение дистрибутивно относительно сложения.

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.

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 $x \otimes n$] — 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 (если $x \neq 0$, то противоположным к x является число $n - x$). Оно называется *кольцом вычетов по модулю* n.

Пример 3. Пусть $\langle R; + \rangle$ — абелева группа с нейтральным элементом 0. Положим $xy = 0$ для любых $x, y \in R$. Очевидно, что $\langle R; +, \cdot \rangle$ — ассоциативно-коммутативное кольцо. Такие кольца называются *кольцами с нулевым умножением*.

Пример 4. Пусть K — множество всех функций от одной переменной из $\mathbb{R}$ в $\mathbb{R}$. На множестве K определим операции сложения и умножения функций «поточечно»: если $f, g \in K$, а $x \in \mathbb{R}$, то $(f + g)(x) = f(x) + g(x)$ и $(fg)(x) = f(x) \cdot g(x)$. Ясно, что $\langle K; +, \cdot \rangle$ — ассоциативно-коммутативное кольцо. Нейтральным элементом по сложению является функция h такая, что $h(x) = 0$ для всякого $x \in \mathbb{R}$. Это кольцо называется *кольцом функций*.

В дальнейшем у нас будут возникать важные примеры некоммутативных колец. Но почти все кольца, которые будут появляться в дальнейшем, будут ассоциативными. Поэтому

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

Если R — кольцо, $x \in R$, а n — натуральное число, то мы будем писать $nx = \underbrace{x + \dots + x}_{n \text{ раз}}$.

Замечание о свойствах сложения в кольцах

Если R — кольцо, $x, y \in R$, а k и m — натуральные числа, то выполнены равенства:

$$k(xy) = (kx)y, \tag{1}$$

$$(kx)(my) = (km)xy. \tag{2}$$

Доказательство. В самом деле,

$$k(xy) = \underbrace{xy + \dots + xy}_{k \text{ раз}} = (\underbrace{x + \dots + x}_{k \text{ раз}})y = (kx)y \quad \text{и}$$

$$(kx)(my) = (\underbrace{x + \dots + x}_{k \text{ раз}})(\underbrace{y + \dots + y}_{m \text{ раз}}) = \underbrace{xy + \dots + xy}_{km \text{ раз}} = (km)xy,$$

что и требовалось доказать. □

Если x — произвольное натуральное число, то nx делится на n. Поэтому

- *для всякого $x \in \mathbb{Z}_n$ в кольце $\mathbb{Z}_n$ выполнено равенство $nx = 0$.*

Во всяком кольце можно определить *разность* $x - y$ элементов x и y правилом: $x - y = x + (-y)$.

Замечание о свойствах умножения в кольцах

Для произвольных элементов x, y, z произвольного кольца R выполнены равенства:

1) $(x - y)z = xz - yz$ *и* $x(y - z) = xy - xz$ (*умножение дистрибутивно относительно вычитания*);
2) $x \cdot 0 = 0 \cdot x = 0$.

Доказательство. 1) В самом деле,

$$(x - y) + y = \big(x + (-y)\big) + y = x + \big((-y) + y\big) = x + 0 = x,$$

т. е. $(x - y) + y = x$. Умножая обе части этого равенства на z справа и используя дистрибутивность умножения относительно сложения, имеем $xz = \big((x - y) + y\big)z = (x - y)z + yz$, т. е. $xz = (x - y)z + yz$. Вычитая из обеих частей этого равенства элемент yz, получаем $xz - yz = (x - y)z + yz - yz = (x - y)z$. Следовательно, $(x - y)z = xz - yz$. Равенство $x(y - z) = xy - xz$ проверяется аналогично.

2) Используя п. 1), имеем $x \cdot 0 = x(x - x) = x^2 - x^2 = 0$. Аналогично проверяется, что $0 \cdot x = 0$.

Определение

Элемент x кольца R называется *делителем нуля*, если $x \neq 0$ и $xy = 0$ для некоторого ненулевого элемента $y \in R$.

В кольце с нулевым умножением все ненулевые элементы являются делителями нуля. Делители нуля есть также в кольце $\mathbb{Z}_n$ при условии, что n — составное число (если $n = km$, где $1 < k, m < n$, то $k \otimes m = 0$).

Замечание о делителях нуля

Обратимый (относительно умножения) элемент произвольного кольца с 1 не является делителем нуля.

Доказательство. Если элемент x обратим и $xy = 0$, то

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

Следовательно, x не является делителем нуля. □

Определение

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

Ясно, что если R — кольцо с 1, то множество всех его обратимых (относительно умножения) элементов образует группу, которая обозначается через R^*. Если R — поле, то $R^* = R \setminus \{0\}$ и группа R^* абелева.

Определение

Если $\langle F; +, \cdot \rangle$ — поле, то группа $\langle F^*; \cdot \rangle$ называется *мультипликативной группой* этого поля.

Из замечания о делителях нуля вытекает, что

- *поле не может содержать делителей нуля.* $\square$

Примерами полей являются кольца $\mathbb{Q}$ и $\mathbb{R}$ с обычными операциями сложения и умножения. На следующем слайде приведен еще один пример поля.

Лемма о кольце вычетов по простому модулю

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

Доказательство. Достаточность. Пусть $n = p$ — простое число. Достаточно проверить, что каждый ненулевой элемент кольца $\mathbb{Z}_p$ имеет обратный элемент по умножению. Пусть $1 \leqslant s \leqslant p-1$. Для произвольного натурального числа m будем обозначать через $\overline{m}$ остаток от деления m на p. Рассмотрим числа

$$\overline{s}, \overline{2s}, \ldots, \overline{(p-1)s}. \tag{3}$$

Пусть $k \in \{1, 2, \ldots, p-1\}$. Очевидно, $0 \leqslant \overline{ks} \leqslant p-1$. Из того, что $s \not\equiv 0 \pmod{p}$, а p — простое число, вытекает, что $ks \not\equiv 0 \pmod{p}$. Следовательно, все числа (3) отличны от 0. Далее, если $\overline{ks} = \overline{\ell s}$ для некоторых $1 \leqslant k < \ell \leqslant p-1$, то $\overline{(\ell - k)s} = 0$ вопреки сказанному выше. Следовательно, все числа (3) попарно различны. Иными словами, (3) — это (возможно, переставленные) числа $1, 2, \ldots, p-1$. Следовательно, существует $t \in \{1, 2, \ldots, p-1\}$ такое, что $\overline{ts} = 1$. Это означает, что $t \in \mathbb{Z}_p$ и $t \otimes s = 1$. Иными словами, элемент t обратен к s по умножению.

Необходимость. Как уже отмечалось выше, кольцо $\mathbb{Z}_n$ при составном n содержит делители нуля, а в поле делителей нуля нет. □

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 $\operatorname{char} \mathbb{Z}_p = p$.

Предложение о характеристике поля

Характеристика всякого поля равна либо нулю, либо простому числу.

Доказательство. Будем обозначать нейтральный элемент поля по умножению не через 1, как обычно, а через e. Пусть F — поле и $\operatorname{char} F = n \neq 0$. Ясно, что $n \neq 1$, так как, по определению поля, $1 \cdot e = e \neq 0$. Предположим, что $n = km$ для некоторых $1 < k, m < n$. Положим $x = ke$ и $y = me$. Если $x = 0$, то, в силу (1), для любого $z \in F$ выполнены равенства $kz = k(ez) = (ke)z = xz = 0 \cdot z = 0$. Но это противоречит равенству $n = \operatorname{char} F$. Таким образом, $x \neq 0$. Аналогично проверяется, что $y \neq 0$. Но $xy = (ke)(me) = (km)e^2 = (km)e = ne = 0$ в силу (2). Таким образом, x и y — делители нуля. Однако, как отмечалось выше, делителей нуля в поле нет.

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

Определение

Пусть $\langle A; \Omega\rangle$ — универсальная алгебра. Непустое подмножество B множества A называется *подалгеброй* в A, если для любой операции $f \in \Omega$ и любых $x_1, x_2, \ldots, x_n \in B$, где n — арность операции f, имеет место включение $f(x_1, x_2, \ldots, x_n) \in B$.

Иначе говоря, подалгебра алгебры A — это ее подмножество, замкнутое относительно всех сигнатурных операций. Очевидно, что подалгебра алгебры A сама является алгеброй той же сигнатуры, что и A. Заметим еще, что

- *любая алгебра A является подалгеброй в самой себе.*

Приведем некоторые примеры подалгебр. Полугруппа $\langle \mathbb{N}; +\rangle$ является подполугругруппой в полугруппах $\langle \mathbb{Z}; +\rangle$, $\langle \mathbb{Q}; +\rangle$ и $\langle \mathbb{R}; +\rangle$, а кольцо $\mathbb{Z}_n$ — подкольцом кольца $\mathbb{Z}_{n^2}$. В то же время, $\mathbb{Z}_n$ не является подкольцом в кольца $\mathbb{Z}$ с обычными операциями сложения и умножения, 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 $\mathbb{Z}_n$. Отметим еще, что единица произвольной группы G образует подгруппу в G, а нуль произвольного кольца R — подкольцо в R.

Определение

Пусть $\langle A;\Omega\rangle$ и $\langle B;\Omega\rangle$ — две универсальных алгебры одной и той же сигнатуры. Отображение $f\colon A\longrightarrow B$ называется *гомоморфизмом*, если $f\big(\omega(x_1,x_2,\ldots,x_n)\big)=\omega\big(f(x_1),f(x_2),\ldots,f(x_n)\big)$ для любой операции $\omega\in\Omega$ и любых $x_1,x_2,\ldots,x_n\in A$, где n - арность операции ω. Если, при этом, отображение f биективно, то оно называется *изоморфизмом*. Если существует изоморфизм из A на B, то говорят, что алгебры A и B *изоморфны* и пишут $A\cong B$. Если алгебра A изоморфна некоторой подалгебре алгебры B, то говорят, что A *изоморфно вложима в* B. Гомоморфизм алгебры A в себя называется *эндоморфизмом*, а изоморфизм A на себя — *автоморфизмом*.

Неформально говоря, существование изоморфизма алгебры A на алгебру B означает, что можем «переименовать» элементы алгебры A (элемент $a\in A$ «переименовывается» в $f(a)$, где f — изоморфизм), после чего все операции над элементами алгебры B выполняются точно так же, как они выполнялись в 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).

Пример 1. Пусть n — натуральное число, $n > 1$. Определим отображение f из кольца $\mathbb{Z}$ в кольцо $\mathbb{Z}_n$ правилом: если $x \in \mathbb{Z}$, то $f(x)$ — остаток от деления x на n. Поскольку, очевидно, остаток суммы равен сумме остатков, а остаток произведения — произведению остатков, отображение f является гомоморфизмом. Очевидно, что это отображение не инъективно и потому не является изоморфизмом.

Пример 2. Отображение f множества $\mathbb{Z}$ в себя, заданное правилом $f(x) = 2x$ для всякого $x \in \mathbb{Z}$ является эндоморфизмом полугруппы $\langle \mathbb{Z}; + \rangle$, но не является ее автоморфизмом (поскольку оно не сюръективно). Задаваемое тем же равенством $f(x) = 2x$ отображение f множества $\mathbb{R}$ в себя является уже автоморфизмом полугруппы $\langle \mathbb{R}; + \rangle$. Заметим, что эти отображения не являются гомоморфизмами колец $\langle \mathbb{Z}; +, \cdot \rangle$ и $\langle \mathbb{R}; +, \cdot \rangle$ соответственно, поскольку если $x, y \neq 0$, то $2x \cdot 2y \neq 2xy$.

Пример 3. Положим $\mathbb{R}_+ = \{x \in \mathbb{R} \mid x > 0\}$. Ясно, что множество $\langle \mathbb{R}_+; \cdot \rangle$ является полугруппой. 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 полугруппы $\langle \mathbb{R}; + \rangle$ в полугруппу $\langle \mathbb{R}_+; \cdot \rangle$. 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.*

Пример 4. Определим отображение f из кольца $\mathbb{Z}$ в кольцо $\mathbb{Q}$ правилом: $f(n) = \frac{n}{1}$ для всякого $n \in \mathbb{Z}$. Очевидно, что f — изоморфное вложение.