



# АЛГЕБРАИЧЕСКИЕ СИСТЕМЫ

Повторение.

# N-АРНАЯ АЛГЕБРАИЧЕСКАЯ ОПЕРАЦИЯ

Функция  $f:A^n \rightarrow B$  называется  $n$ -местной функцией из  $A$  в  $B$ .

Функция  $f:A^n \rightarrow A$  называется  $n$ -местной алгебраической операцией на  $A$ .

При  $n=1$  операция называется унарной.

При  $n=2$  операция называется бинарной.

При  $n=0$  операцию принято называть константой.

Очевидно, что  $n$ -местная операция на множестве  $A$  является  $(n+1)$ -местным отношением на том же множестве.

Если область значений операции лежит в  $A$ , то будем говорить, что операция  $f$  замкнута на  $A$ .

Сигнатурой называется совокупность предикатных и функциональных символов с указанием их местности.

# АЛГЕБРАИЧЕСКАЯ СИСТЕМА

Алгебраической системой  $(A; \Sigma)$  сигнатуры  $\Sigma$  называется непустое множество  $A$ , где каждому  $n$ -местному предикатному (функциональному) символу из  $\Sigma$  поставлен в соответствие  $n$ -местный предикат (операция), определенный на множестве  $A$ .

Множество  $A$  называется носителем или универсумом алгебраической системы  $(A; \Sigma)$ .

Мощностью а.с. называется мощность ее носителя.

А.с. называется алгеброй, если ее сигнатура состоит только из функциональных символов.

А.с. называется моделью, если ее сигнатура состоит только из предикатных символов.

# АЛГЕБРЫ С ОДНОЙ ОПЕРАЦИЕЙ

**Группоид** – алгебра  $(A, \cdot)$  с одной бинарной операцией. Помимо требования замкнутости множества относительно заданной на нём операции, других требований к операции и множеству не предъявляется.

**Полугруппа** – группоид с ассоциативной операцией (т.е. для всех  $x, y, z \in A$  верно  $(x \cdot y) \cdot z = x \cdot (y \cdot z)$  ).

Пример:  $(\mathbb{N}, +)$

Элемент  $e \in A$  такой, что  $e \cdot x = x \cdot e = x$  для всех  $x \in A$ , называется **единицей**.

**Моноид** – полугруппа с единицей.

Пример:  $(\mathbb{N}, \cdot)$

# ГРУППА

Элемент  $x^{-1} \in A$ , такой что для  $x \in A$   $x \cdot x^{-1} = x^{-1} \cdot x = e$ , называется **обратным** к  $x$ . Элемент  $x$  называется обратимым.

**Группа** – моноид  $(A, \cdot)$ , у которого для любого элемента существует обратный.

Пример:  $(\mathbb{Z}, +)$

**Абелева (коммутативная) группа** – группа  $(A, \cdot)$ , где операция  $\cdot$  коммутативна (т.е.  $x \cdot y = y \cdot x$  для всех  $x, y \in A$ ).

Пример:  $(\mathbb{Z}, +)$

# АЛГЕБРЫ С ДВУМЯ ОПЕРАЦИЯМИ

**Кольцо** — множество  $R$ , на котором заданы две бинарные операции:  $+$  и  $\times$  (называемые сложение и умножение), со следующими свойствами, выполняющимися для любых  $a, b, c \in R$ :

1.  $a + b = b + a$  — коммутативность сложения;
2.  $a + (b + c) = (a + b) + c$  — ассоциативность сложения;
3.  $\exists 0 \in R (a + 0 = 0 + a = a)$  — существование нейтрального элемента относительно сложения;
4.  $\forall a \in R \exists b \in R (a + b = b + a = 0)$  — существование противоположного элемента относительно сложения;
5.  $(a \times b) \times c = a \times (b \times c)$  — ассоциативность умножения;
6. 
$$\begin{cases} a \times (b + c) = (a \times b) + (a \times c) \\ (b + c) \times a = (b \times a) + (c \times a) \end{cases}$$
 — дистрибутивность.

Иными словами, кольцо — алгебра  $(R, +, \times)$ , являющаяся абелевой группой относительно сложения  $+$ , полугруппой относительно умножения  $\times$ , и обладающая двусторонней дистрибутивностью  $\times$  относительно  $+$ .

Пример:  $(\mathbb{Z}, +, \cdot)$ .

# ТЕЛО

**Кольцо с 1** – кольцо, содержащее нейтральный элемент  $e \in R$  относительно умножения ( $e \cdot x = x \cdot e = x$  для всех  $x \in R$ ).

**Тело** — кольцо с единицей, в котором каждый ненулевой элемент обратим (относительно умножения).

Иными словами, тело - это множество с двумя операциями (сложение и умножение), обладающее следующими свойствами:

образует абелеву группу относительно сложения;

все ненулевые элементы образуют группу относительно умножения;

имеет место дистрибутивность умножения относительно сложения.

# ПОЛЕ

**Поле** - множество  $F$  с введёнными на нём алгебраическими операциями сложения  $+$  и умножения  $*$  ( $+$  :  $F \times F \rightarrow F$  ,  $*$  :  $F \times F \rightarrow F$ , для которого выполняются следующие аксиомы:

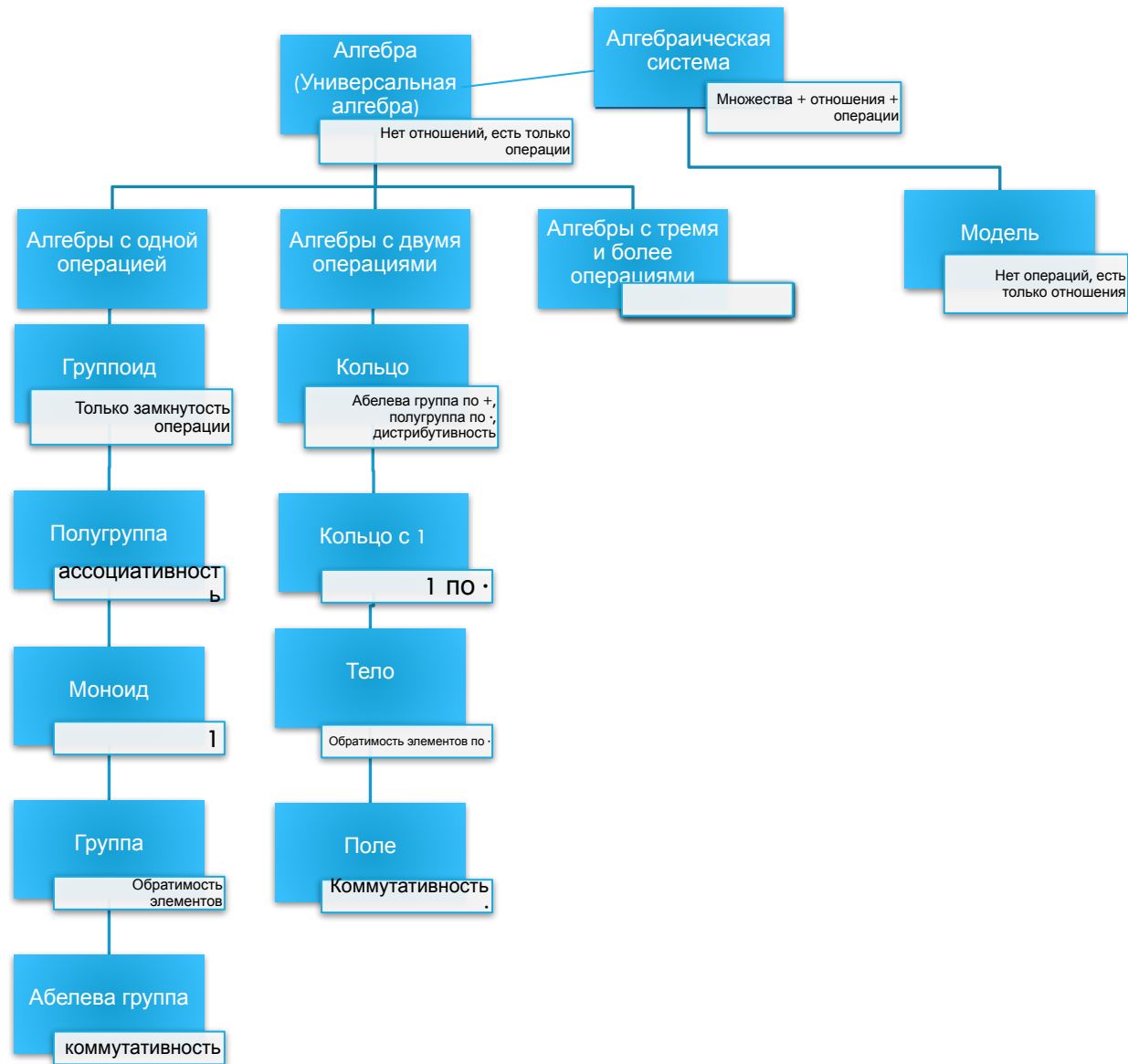
1. Коммутативность сложения:  $\forall a, b \in F \quad a + b = b + a$ .
2. Ассоциативность сложения:  $\forall a, b, c \in F \quad (a + b) + c = a + (b + c)$ .
3. Существование нулевого элемента:  $\exists \mathbf{0} \in F: \forall a \in F \quad a + \mathbf{0} = a$ .
4. Существование противоположного элемента:  $\forall a \in F \exists (-a) \in F: a + (-a) = \mathbf{0}$ .
5. Коммутативность умножения:  $\forall a, b \in F \quad a * b = b * a$ .
6. Ассоциативность умножения:  $\forall a, b, c \in F \quad (a * b) * c = a * (b * c)$ .
7. Существование единичного элемента:  $\exists e \in F \setminus \{\mathbf{0}\}: \forall a \in F \quad a * e = a$ .
8. Существование обратного элемента для ненулевых элементов:  $(\forall a \in F: a \neq \mathbf{0}) \exists a^{-1} \in F: a * a^{-1} = e$ .
9. Дистрибутивность умножения относительно сложения:  $\forall a, b, c \in F \quad (a + b) * c = (a * c) + (b * c)$ .

Поле - алгебра  $(F, +, \times)$ , являющаяся абелевой группой по сложению, все его ненулевые элементы образуют абелеву группу по умножению, и выполняется свойство дистрибутивности.



# ПРИМЕРЫ ПОЛЯ

- $\mathbb{Q}$  – рациональные числа,
- $\mathbb{R}$  – вещественные числа,
- $\mathbb{C}$  – комплексные числа,
- $\mathbb{Z}_p$  – поле вычетов по модулю  $p$ , где  $p$  – простое число.
- $\mathbb{F}_q$  – конечное поле из  $q = p^k$  элементов, где  $p$  – простое число,  $k$  – натуральное.



Алгебраическая система

Одноосновная  
я  
(односортная)

Многоосновная  
я  
(многосортная)

# МНОГООСНОВНАЯ АЛГЕБРА

**Многоосновной алгеброй** (многоосновной универсальной алгеброй) называется  $(A_1, A_2, \dots, A_n, \Sigma)$ , где  $A_1, A_2, \dots, A_n$  – произвольные непустые множества (основы алгебры) и  $\Sigma$  – множество полиморфных операций на указанных основах (в общем случае различной ариности) – сигнатура многоосновной алгебры.

Отличие полиморфных операций от алгебраических состоит в том, что аргументы такой операции могут выбираться в нескольких основах, а результат (значение) может принадлежать любой из основ (может быть не имеющей никакого отношения к тем основам, откуда выбирались аргументы).

Аналогично определяются многоосновные модели и многоосновные АС.

# ВЕКТОРНОЕ ПРОСТРАНСТВО

**Линейное, или векторное, пространство  $V(F)$  над полем  $F$  — это упорядоченная четвёрка  $(V, F, +, \cdot)$ , где**

$V$  — непустое множество элементов произвольной природы, которые называются векторами.

$F$  — поле, элементы которого называются скалярами.

Определена операция сложения векторов  $V \times V \rightarrow V$ , сопоставляющая каждой паре элементов  $x, y \in V$  единственный элемент множества  $V$ , называемый их суммой и обозначаемый  $x + y$ .

Определена операция умножения векторов на скаляры  $F \times V \rightarrow V$ , сопоставляющая каждому элементу  $\lambda$  поля  $F$  и каждому элементу  $x$  множества  $V$  единственный элемент множества  $V$ , обозначаемый  $\lambda \cdot x$ .

Заданные операции должны удовлетворять следующим аксиомам — аксиомам линейного (векторного) пространства:

1.  $\mathbf{x} + \mathbf{y} = \mathbf{y} + \mathbf{x}$  для любых  $\mathbf{x}, \mathbf{y} \in V$  (коммутативность сложения);
2.  $\mathbf{x} + (\mathbf{y} + \mathbf{z}) = (\mathbf{x} + \mathbf{y}) + \mathbf{z}$  для любых  $\mathbf{x}, \mathbf{y}, \mathbf{z} \in V$  (ассоциативность сложения);
3. существует такой элемент  $\mathbf{0} \in V$ , что  $\mathbf{x} + \mathbf{0} = \mathbf{0} + \mathbf{x} = \mathbf{x}$  для любого  $\mathbf{x} \in V$  (существование нейтрального элемента относительно сложения);
4. для любого  $\mathbf{x} \in V$  существует такой элемент  $-\mathbf{x} \in V$ , что  $\mathbf{x} + (-\mathbf{x}) = \mathbf{0}$ , называемый вектором, **противоположным** вектору  $\mathbf{x}$ ;
5.  $\alpha(\beta\mathbf{x}) = (\alpha\beta)\mathbf{x}$  (ассоциативность умножения на скаляр);
6.  $1 \cdot \mathbf{x} = \mathbf{x}$  (унитарность: умножение на нейтральный (по умножению) элемент поля  $F$  сохраняет вектор).
7.  $(\alpha + \beta)\mathbf{x} = \alpha\mathbf{x} + \beta\mathbf{x}$  (дистрибутивность умножения вектора на скаляр относительно сложения скаляров);
8.  $\alpha(\mathbf{x} + \mathbf{y}) = \alpha\mathbf{x} + \alpha\mathbf{y}$  (дистрибутивность умножения вектора на скаляр относительно сложения векторов).

Таким образом, операция сложения задаёт на множестве  $V$  структуру абелевой группы.

Пример: множество пар действительных чисел  $\mathbb{R}^2$  - двумерное векторное пространство над полем действительных.