Алгебра. I Семестр

Лектор: Вавилов Николай Александрович
Автор конспекта: Буглеев Антон

2022

1 Некоторые бинарные операции

Операции над векторами

Сложение и умножение векторов:

$$(x_1, ..., x_n) + (y_1, ..., y_n) = (x_1 + y_1, ..., x_n + y_n)$$

$$(x_1, ..., x_n)(y_1, ..., y_n) = (x_1 y_1, ..., x_n y_n)$$

Комплексное умножение:

$$(a, b)(c, d) = (ac - bd, ad + bc)$$

Векторное умножение в $\mathbb{R}^3$:

$$(x_1, x_2, x_3) \times (y_1, y_2, y_3) = (x_2 y_3 - x_3 y_2, -x_1 y_3 + x_3 y_1, x_1 y_2 - x_2 y_2)$$

Операции над матрицами

Сложение матриц:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} e & b \\ g & h \end{pmatrix} = \begin{pmatrix} a + c & b + f \\ c + g & d + h \end{pmatrix}$$

Умножение матриц:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix} = \begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + ch \end{pmatrix}$$

2 Структуры

Основные структуры

$X \neq \emptyset$
$* : X \times X \to X$
$(x, y) \mapsto x * y$

Аксиомы:

1. $\forall\, x, y, z \in X : x * (y * z) = (x * y) * z$ (Ассоциативность)

2. $\exists\, e \in X : e * x = x = x * e$ (нейтральный элемент)

3. $\forall\, x \in X, \exists\, x' : x * x' = x' * x = e$ (обратный элемент)

4. $\forall\, x, y \in X : a * b = b * a$ (коммутативность)

Def. Полугруппа (Semigroup) - множество X с операцией, удовлетворяющее аксиоме 1

Примеры: $(\mathbb{N}, +)$

Def. Моноид (Monoid) - множество X с операцией *, удовлетворяющее аксиомам 1-2

Примеры: $(\mathbb{N}_0, +)$, $(\mathbb{N}, *)$, $(X, \cup)$

Def. Группа (Group) - множество X с операцией *, удовлетворяющее аксиомам 1-3

Def. Абелева (коммутативная) группа (Abelian group) - множество X с операцией *, удовлетворяющее аксиомам 1-4

Некоторые полезные леммы и определения

Def. Элемент $z \in X$ называется **регулярным**, если $\forall\, x, y \in X$:

$$\begin{cases} x * z = y * z \Rightarrow x = y \text{ (Регулярный справа)} \\ z * x = z * y \Rightarrow x = y \text{ (Регулярный слева)} \end{cases}$$

Def. Элемент $z \in X$ называется **обратимым**, если $\exists\, z' \in X$:

$$\begin{cases} z * z' = e \text{ (Обратимый слева)} \\ z' * z = e \text{ (Обратимый справа)} \end{cases}$$

Lemma. *Элемент $z \in X$ обратим слева/справа $\Rightarrow$ z регулярен слева/справа*

Proof. ... $\square$

Lemma. *В группе G есть левое и правое деление:*

$\forall\, h, g \in G\ \exists!\, x, y \in G, (hx = g) \wedge (yh = g) \Rightarrow (x = h^{-1}g) \wedge (y = gh^{-1})$

Proof. Докажем, что $hx = g \Rightarrow x = h^{-1}g$

$$\begin{aligned}
hx &= g \mid \text{домножим на } h^{-1} \\
h^{-1}(hx) &= h^{-1}g \\
(h^{-1}h)x &= h^{-1}g \\
ex &= h^{-1}g \\
x &= h^{-1}g
\end{aligned}$$

Аналогичное доказательство утверждения $yh = g \Rightarrow y = gh^{-1}$ $\square$

Def. $H \subset G$ называется **Подгруппой в** G, если

$$\forall\, x, y \in H,\ xy^{-1} \in H \Leftrightarrow \begin{cases} xy \in H \\ y^{-1} \in H \end{cases}$$

Примеры:

1. $\mathbb{R}_{>0} < \mathbb{R}^*$ значит, что $\mathbb{R}_{>0}$ - подгруппа $\mathbb{R}^*$
2. $\mathbb{Q}_{>0} < \mathbb{Q}^*$ значит, что $\mathbb{R}_{>0}$ - подгруппа $\mathbb{R}^*$

Def. Операция **возведения в степень в моноиде.** Пусть X - моноид с нейтральным e, $x \in X,\ n \in \mathbb{N}_0$. Тогда:

$$x^0 = e,\ x^n = \begin{cases} \left(x^{\frac{n}{2}}\right)^2,\ 2 \mid n \ (2 \text{ - делитель } n) \\ x^{n-1} \cdot x,\ 2 \nmid n \ (2 \text{ - не делитель } n) \end{cases}$$

Def. Операция **возведения в степень в группе** определяется аналогично, только показатель $n \in \mathbb{Z}$

Def. Группа G называется **конечной**, если её порядок $|G|$ конечен

Def. **Симметрическая группа** множества X:

$$S_X = \text{биекция } X \to X$$

3 Кольца и поля

Def. *Кольцом* называется множество K с операцией сложения и умножения, обладающая следующими свойствами:

1. Относительно сложения существует абелева группа.

2. Выполняется дистрибутивность: $\forall\, a, b, c \in K : a(b + c) = ab + ac \wedge (b + c)a = ba + ca$.

Следствия аксиом кольца:

1. $\forall\, a \in K : a0 = 0a = 0$

2. $\forall\, a, b \in K : a(-b) = (-a)b = -ab$

3. $\forall\, a, b, c \in K : a(b - c) = ab - ac$

Def. Кольцо K называется *коммутативным*, если выполнено $\forall\, a, b \in K : ab = ba$

Def. Кольцо K называется *ассоциативным*, если выполнено $\forall\, a, b, c \in K : (ab)c = a(bc)$

Def. Кольцо с единицей называется *унитальным*.

Два важных замечания:

1. Если $1 = 0$, то
$$\forall\, a \in K : a = a1 = a0 = 0$$
То есть кольцо K состоит только из нуля. Если кольцо содержит более одного элемента, то $1 \neq 0$

2. При наличии коммутативности умножения из двух тождеств дистрибутивности можно оставить только одно.

Примеры колец:

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

2. $2\mathbb{Z}$ является коммутативным ассоциативным кольцом без единицы.

3. Множество векторов пространства с операциями сложения и векторного умножения является некоммутативным неассоциативным кольцом. Однако выполнены другие тождества:

   (a) $a \times b + b \times a = 0$ (антикоммутативность)

   (b) $(a \times b) \times c + (b \times c) \times a + (c \times a) \times b = 0$ (тождество Якоби)

Def. Элемент a' кольца с единицей называется *обратным* к элементу a, если выполнено $a'a = aa' = 1$.
Элемент, имеющий обратный, называется *обратимым*

Def. *Телом* называется унитальное ассоциативное кольцо, у которого $\forall\, x \in R \backslash 0\ \exists\, x' : xx' = x'x = 1$

Def. *Полем* называется коммутативное ассоциативное кольцо с единицей, в котором каждый ненулевой элемент обратимым.
Примером полей являются $\mathbb{R}$ и $\mathbb{Q}$, но $\mathbb{Z}$ не является полем (т.к. обратимы только ± 1)

Важное свойство поля:

$$ab = 0 \Rightarrow a = 0 \vee b = 0$$

Кольцо $\mathbb{Z}$ также обладает этим свойством. Такие кольца называют *кольцами без делителей нуля.*
В кольце без делителей нуля имеет место:

$$ac = bc \wedge c \neq 0 \Rightarrow a = b$$

Def. Операция $\circ$ называется *самодистрибутивной (слева/справа)*, если

$$x \circ (y \circ z) = (x \circ y) \circ (x \circ z)$$

Например, конъюнкция и дизъюнкция являются *самодистрибутивными*

Цитата Великого: *"К некоммутативности привыкаешь за семестр, к неассоциативности - никогда"*.