Алгоритмы в математике *(теория чисел)*

Михайлов Максим

11 марта 2022 г.

Оглавление

Лекция 1

3 марта

1 Алгебраическое тело

Определение. Алгебраическое тело — множество T с бинарными операциями $+$ и $\cdot$, такими, что:

1. $(T, 0, +)$ — абелева группа:
    - $\forall \alpha, \beta, \gamma \quad \alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$
    - $\exists 0 : \alpha + 0 = \alpha = 0 + \alpha$
    - $\forall \alpha \in T \;\; \exists (-\alpha) : \alpha + (-\alpha) = 0 = (-\alpha) + \alpha$
    - $\star$ $\forall \alpha, \beta \in T \quad \alpha + \beta = \beta + \alpha$
2. $((T \setminus \{0\}), 1, *)$ — группа:
    - $\alpha(\beta\gamma) = (\alpha\beta)\gamma$
    - $\exists 1 : \alpha \cdot 1 = \alpha = 1 \cdot \alpha$
    - $\forall \alpha \neq 0 \;\; \exists \alpha^{-1} : \alpha\alpha^{-1} = 1 = \alpha^{-1}\alpha$
    - $\star$ Если умножение не коммутативно, то T — тело, иначе — поле.
3. Дистрибутивность: $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma, (\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma$

Пример. $\mathbb{F}_p$ — поле вычетов по модулю p.

$$\mathbb{F}_p = \{0, 1, 2 \ldots p - 1\}$$

1. $\mathbb{F}_2 = \{0, 1\}$

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Таблица 1.1: Таблицы сложения и умножения в $\mathbb{F}_2$

Пусть есть поле $\mathbb{F}_k, k = n \cdot m, m \neq 0, n \neq 0$. Т.к. $n < k$ и $m < k$, то $n \cdot m = 0$. Таким образом, в поле есть делители нуля.

Примечание. Переход от $\mathbb{Q}$ к $\mathbb{R}$ — топологическая конструкция, поэтому будем рассматривать переход из $\mathbb{Q}$ в $\mathbb{C}$ над рациональными числами.

Определение. $\mathbb{C} \cong {}^{K[t]}\!/\!_{(t^2+1)K[t]}$

$\cdot$	1	i
1	1	i
i	i	-1

Теорема 1 (Фробениуса)**.** Дано тело T, такое что $T \supset \mathbb{R}$. Тогда:

1. Каждый элемент $\mathbb{R}$ коммутирует с каждым элементом T.
2. Каждый элемент T представим как:

$$x = x_0 + x_1 i_1 + x_2 i_2 + \cdots + x_n i_n$$

Из этого следует, что выполнено одно из:

1. T это $\mathbb{R}$
2. T это $\mathbb{C}$
3. T это $\mathbb{K}$

Если $i_1, i_2 \ldots i_n$ — базис $\mathbb{I}$, то $\dim \mathbb{I} \in \{0, 1, 3\}$

Лекция 2

11 марта

$\triangleleft \mathbb{I} = \{z \mid z^2 \in \mathbb{R}, z^2 \leq 0\}$

Примечание. $\mathbb{R} \cap \mathbb{I} = \{0\}$

Теорема 2. $\mathbb{R} \oplus \mathbb{I} = T$

Лемма 1. Если $z \in \mathbb{I}$, то $\forall \alpha \in \mathbb{R} \ \ \alpha z \in \mathbb{I}$.

Доказательство.

$$(\alpha z)^2 = \alpha^2 z^2 \leq 0 \Rightarrow \alpha z \in \mathbb{I}$$

□

Лемма 2. Если $z \in \mathbb{I}$ и z^{-1} существует, то $z^{-1} \in \mathbb{I}$, где z^{-1} это такой элемент $\mathbb{I}$, что $zz^{-1} = 1$.

Доказательство.

$$z^2(z^{-1})^2 = \underbrace{zz}_{<0} z^{-1}z^{-1} = 1 \Rightarrow z^{-1}z^{-1} < 0 \Rightarrow z^{-1} \in \mathbb{I}$$

□

Лемма 3. Всякий элемент x из T представим единственным образом в виде:

$$x \overset{!}{=} a + z, \quad a \in \mathbb{R}, z \in \mathbb{I}$$

Доказательство. $\triangleleft x \in T, \{x^0, x, x^2 \ldots x^{n+1}\}$ — линейно зависимые. Тогда $\exists \{\alpha_i\}_{i=0}^{n+1} \subset \mathbb{R}$, такие что:

$$\alpha_0 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_{n+1} x^{n+1} = 0$$

Не дописано

□

Лемма 4. Пусть $u, v \in \mathbb{I}, a, b \in \mathbb{R}$. Тогда $uv + vu = \xi \in \mathbb{R}$ и $au + bv = \eta \in \mathbb{I}$.

Доказательство. Положим, что $\{1, u, v\}$ линейно зависим, т.е. $\exists \alpha, \beta, \gamma : \alpha + \beta u + \gamma v = 0$.

$$\beta u = -\alpha - \gamma v \Rightarrow \alpha = 0 \Rightarrow u = -\frac{\gamma}{\beta} v$$

$$\sphericalangle uv + vu = -\frac{\gamma}{\beta} v^2 - \frac{\gamma}{\beta} v^2 = \frac{-2\gamma}{\beta} v^2 \in \mathbb{R}$$

$$-\frac{\alpha\gamma}{\beta} v + bv = \left(b - \frac{\alpha\gamma}{\beta}\right) v \in \mathbb{I}$$

Положим, что $\{1, u, v\}$ линейно независим.

$$\eta^2 = (\beta + z)^2 = (au + bv)^2 = a^2u^2 + b^2v^2 + ab(uv + vu)$$

$$(\beta + z)^2 = a^2u^2 + b^2v^2 + ab(\alpha + y)$$
$$\beta^2 + 2\beta z + z^2 = a^2u^2 + b^2v^2 + ab(\alpha + y)$$
$$2\beta z = ab(\alpha + y)$$

Если $z = 0$, то $\{1, u, v\}$ линейно зависим — противоречие.

$\sphericalangle z \neq 0, z = \frac{ab}{2\beta} y$

$$au + bv = \beta + \frac{ab}{2\beta} y$$

$$a^2u^2 + b^2v^2 = a'u + b'v = \beta' + \frac{a'b'}{2\beta} y$$

Не дописано $\square$

Лемма 5.

- $u, v \in \mathbb{I}$
- $u^2 = -1$
- $v^2 = -1$
- $w = u \cdot v$

Тогда:

$$u^2 = v^2 = w^2 = -1$$
$$uv = -vu = w$$
$$vw = -wv = u$$
$$wu = -uw = v$$