

Алгоритмы в математике (*теория чисел*)

Михайлов Максим

6 марта 2022 г.

Оглавление

Лекция 1	3 марта	2
1	Алгебраическое тело	2

Лекция 1

3 марта

1 Алгебраическое тело

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

1. $(T, 0, +)$ — абелева группа:

- $\forall \alpha, \beta, \gamma \quad \alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$
- $\exists 0 : \alpha + 0 = \alpha = 0 + \alpha$
- $\forall \alpha \in T \quad \exists (-\alpha) : \alpha + (-\alpha) = 0 = (-\alpha) + \alpha$
- ★ $\forall \alpha, \beta \in T \quad \alpha + \beta = \beta + \alpha$

2. $((T \setminus \{0\}), 1, *)$ — группа:

- $\alpha(\beta\gamma) = (\alpha\beta)\gamma$
- $\exists 1 : \alpha \cdot 1 = \alpha = 1 \cdot \alpha$
- $\forall \alpha \neq 0 \quad \exists \alpha^{-1} : \alpha\alpha^{-1} = 1 = \alpha^{-1}\alpha$
- ★ Если $\alpha\beta \neq \beta\alpha$, то T — тело, иначе — поле.

3. $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma, (\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma$

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

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

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

+	0	1	·	0	1
0	0	1	0	0	0
1	1	0	1	0	1

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

·	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:

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

Из этого следует, что выполнено одно из:

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

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