ОСА. Лекция

jdaslkda

15 октября 2024 г.

Def! Ассоциативное коммутативное кольцо K с единицей называется полем , если $\forall k \in K$ обратим

Examples 1) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ - числовые

2) $\mathbb{Z}_p$ - поле вычетов по mod p - конечное

3) ${}^{\mathbb{Z}_2[x]}/_{(x^2+x+1)}$ - поле из 4-х элементов

${}^{\mathbb{Z}_2[x]}/_{(x^3+x+1)}$ - поле из 8-и элементов

${}^{\mathbb{Z}_3[x]}/_{(x^2+1)}$ - поле из 9-и элементов

${}^{\mathbb{Z}_3[x]}/_{(x^3+x^2+2x+\overline{1})}$ - поле из 27-и элементов

4) $\mathbb{Q}(x) = \{\frac{f(x)}{g(x)} \mid 0 \neq g(x), f(x) \in \mathbb{Q}[x]\}$ - поле рациональных дробей

Доказывали:

F - поле, ${}^{F[x]}/_{(f(x))}$ – поле $\iff$ $f(x)$ непреводим над F

Характеристика поля

В любом поле есть $1 \neq 0$

min натуральное n $\mid 1 + \cdots + 1 = 0$ называется характеристикой поля K

обозн $charK = n$ ($\equiv charK$ порядок 1 в $(K, +)$)

Если $\nexists$ такого n, то $charK = 0$

$char\mathbb{Q} = 0$

$char\mathbb{Z}_p = p$

Предложение 1 Если $charK = n$, то $n = p$ - простое

Proof Пусть $n = n_1 \cdot n_2$ - не простое, $1 < n_1 < n,\ 1 < n_2 < n$

$$\implies (1 + \cdots + 1) \cdot (1 + \cdots + 1) \overset{\text{def}}{=} (n_1 \cdot 1)(n_2 \cdot 1) = n \cdot 1 = 0 \mid \cdot (n_1 \cdot 1)^{-1} \implies n_2 \cdot 1 = 0$$

Противоречие $charK = n,\ n_2 < n$

? $\exists \infty$ поле простой характеристики?

Предложение 2 1) $charK = 0 \implies K$ содержит подполе, изоморфное $\mathbb{Q}$

2) $charK = p \implies K$ содержит подполе, изоморфное $\mathbb{Z}_p$

Proof 1) $charK = 0$

Рассмотрим $\phi : \mathbb{Z} \to K : n \mapsto n \cdot 1$ - гомоморфизм колец

$$n \in \ker\phi \implies \phi(n) = n \cdot 1 = 0 \implies n = 0, \text{ т.к. } charK = 0 \implies \phi \text{ - иньективно} \implies \mathbb{Z} \hookrightarrow K \implies$$

$$\text{т.к. K поле, то } \forall 0 \neq a \in \phi(\mathbb{Z})\ \exists a^{-1} \in K \implies \text{ в K}\exists \text{ подполе } \cong \mathbb{Q}$$

2) $charK = p$

Рассмотрим $\phi : \mathbb{Z} \to K : n \mapsto n \cdot 1$ - гомоморфизм колец

$$\forall n \in \ker\phi \implies \phi(n) = n \cdot 1 = 0 \implies p \mid n \implies \ker\phi = p\mathbb{Z}$$

$$1 \text{ th iso} \implies \Im(\phi) \cong {}^{\mathbb{Z}}/_{p\mathbb{Z}} = \mathbb{Z}_p$$

Предложение Если $|k| < \infty$ и $charK = p \implies |k| = p^n$, где p - простое

Proof Предл 2 $\implies K$ содержит $\mathbb{Z}_p$

$$\implies K - \text{в.п. над } \mathbb{Z}_p$$

$$\text{Пусть } \{e_1, \ldots, e_n\} - \text{ базис K над } \mathbb{Z}_p \implies \forall a \in K\ \exists!\ \alpha_1, \ldots, \alpha_n \in \mathbb{Z}_p \mid a = \alpha_1 e_1 + \cdots + \alpha_n e_n$$

$$\implies |k| = p^n$$

Предложение 4 Пусть K - конечное поле, $charK = p \implies \phi : K \to K : x \mapsto x^p$ - автоморфизм(auto Фробениуса)

Proof

$$\phi(xy) = (xy)^p = x^p y^p = \phi(x)\phi(y)$$

$$\phi(x+y) = (x+y)^p \stackrel{?}{=} x^p + y^p = \phi(x) + \phi(y)$$

$$(x+y)^p = \sum_{i=0}^{p} C_p^i x^i y^{p-i} = x^p + y^p$$

$$C_p^i = \frac{p!}{i!(p-i)!}, \text{ кроме } i = 0,\ i = p$$

$$\forall x \in \ker\phi:\ \phi(x) = x^p = 0 \implies x = 0 \implies \phi - \text{иньективность} \stackrel{|K|<\infty}{\implies} \phi - \text{ сюрьективно}$$

Расширение полей

Def Поле K - расширение поля F, если $F \subset K$

Тогда K - векторное пространство над F, $\dim_F K \stackrel{df}{=} [K:F]$ - степень расширения

Ex 1) $\mathbb{R} \subset \mathbb{C} \implies [\mathbb{C}:\mathbb{R}] = 2$ с базисом $\{1, i\}$

2) $\mathbb{Q} \subset \mathbb{R} \implies [\mathbb{R}:\mathbb{Q}] = \infty$

Предл 5 $F \subset K \subset L$ - расширения полей $\implies [L:F] = [K:F] \cdot [L:K]$ (finite)

Если $[K:F] = \infty lor [L:K] = \infty \implies [L:F] = \infty$

Proof $[L:K] = m,\ [K:F] = n;\ \{e_1, \ldots, e_m\}$ б L над K; $\{f_1, \ldots, f_n\}$ - б K над F

$$1)\ L =_F < e_i f_i > \quad i = \overline{1,m},\ j = \overline{1,n}$$

$$\forall l \in L:\ l = k_1 e_1 + \cdots + k_m e_m,\ k \in K,\ i = \overline{1,m}$$

$$\forall i:\ k_i = \sum_{j=1}^{n} \alpha_{ij} f_i,\ \alpha_{ij} \in F$$

$$l = \sum_{i=1}^{m} \left(\sum_{j=1}^{n} \alpha_{ij} e_i f_j \right), \alpha_{ij} \in F \implies L =< e_i f_j >_F$$

2) лнз

$$\sum_{i=\overline{1,m}, j=\overline{1,n}} \implies \sum_{i=1}^{m} \left(\sum_{j=1}^{n} \alpha_{ij} f_j \right) e_i = 0 \implies \sum_{i=1}^{n} \alpha_{ij} f_j = 0 \implies \alpha_{ij} = 0 \implies \{e_i f_j\} - \text{ лнз над K}$$

$$1) \text{ и } 2) \implies \{e_i f_j\} \text{ - базис L над F} \implies [L:F] = n \cdot m$$