IPMPFMF2025-04-08 zamudil 15 minut

Izrek: a.) Vsaka končna razširitev je algebraična.

b.) $K \leq F$, $A \subseteq F$ algebraični nad K. Potem je $K(A)$ algebraična razširitev K.

c.) F alg. razš. K, E alg. razš. F, potem E alg. raz. K.

$K \leq F \leq E$

alg alg

$\Rightarrow$ alg.

Dokaz: a.) $[F:K] = n$, $x \in F$. $1, x, x^2, \dots, x^n$ so lin. odvisni $\rightarrow \exists k_1, \dots, k_n$, ki niso vsi 0 t.: $k_0 + k_1 x^1 + \dots + k_n x^n = 0$ ν x je ničla polinoma v K.

b.) Vsak element $K(A)$ je oblike:

za $a_i \in A$, p, q polinoma v $K[x_1, \dots, x_n]$

$$\frac{p(a_1, \dots, a_n)}{q(a_1, \dots, a_n)}$$

$\frac{a_1 + a_3^2}{a_2 + a_4} \in K(a_1, \dots, a_n)$, ki je končna razš.

$K \rightarrow$ algebraična

c.) $a \in E$, $f_0, f_1, \dots, f_n \in F$.

$f_0 + f_1 \cdot a + f_2 a^2 + \dots + f_n a^n = 0 \Rightarrow$

$\Rightarrow$ a je alg. nad $K(f_0, \dots, f_n)$.

$$K \leq K(f_0, \dots, f_n) \leq K(f_0, \dots, f_n, a)$$

končna končna

končna.

$\Rightarrow$ a je alg. nad K.

[Razpadni obseg]

$K \leq \mathbb{C}$ $\quad p(x) \in K[x]$. $\quad \underbrace{\{a_1, \dots, a_n\}}_{\subseteq \mathbb{C}}$ so ničle $p(x)$

$K \leq K(a_1, \dots, a_n) \leq \mathbb{C}$

$p(x)$ v $\mathbb{C}$ razpade na lin. faktorje $p(x) = (x-a_1)\cdots(x-a_n)$

najmanjša razširitev s to lastnostjo

naj bo sedaj $p(x) \in \mathbb{Z}_p[x]$, specifično $x^2+x+1 \in \mathbb{Z}_2[x]$.

ta ireducibilen, je nerazc. ⇐ dokaži?

$$\left[\mathbb{Z}_2[x] / (x^2+x+1) : \mathbb{Z}_2 \right] = 2$$

$K :=$ ideal, ki ga generira ta nerazc. polinom.

obseg

$x + (x^2+x+1) \in K$

elementi, ki dajo ostanek x pri deljenju z x^2+x+1 v $\mathbb{Z}_2$.

etv. razred v

naj bo $I := (x^2+x+1)$.

$$(x+I)^2 + (x+I) + 1 + I = x^2 + I + x + I = (x^2+x+1) + I = 0 + I$$

Torej x^2+x+1 razpade na linearne faktorje v

$$\mathbb{Z}_2[x]/(x^2+x+1) \cong \mathbb{Z}_2$$

$$a := x+(x^2+x+1) \qquad p(a) = a^2+a+1$$

$\Rightarrow$ elementi/predstavniki so:

$$0,\ 1,\ x,\ x+1$$

$\cdot$	0	1	x	$1+x$
0	0	0	0	0
1	0	1	x	$1+x$
x	0	x	$x^2 \bmod x^2+x+1 = x+1$	$x+x^2 \bmod x^2+x+1 = 1$
$1+x$	0	$1+x$	1	$1+2x+x^2 = 1+x^2 \equiv x \pmod{x^2+x+1}$

$+$	0	1	x	$1+x$
0	0	1	x	$1+x$
1		0	$1+x$	x
x	tovrst		0	1
$1+x$				0

Kaj pa poljuben obseg in poljuben polinom?

Let $p(x) \in K[x]$. nične ima lahko v K in izven K.

case vse ničle so elementi K: ✓ polinom je popolnoma razcepen nad K.

case obstaja ničle izven K: ima vsaj en nelinearen nerazcepen faktor.

Let $q(x)$ nerazcepen nelinearen faktor $p(x)$.

$$\Rightarrow \quad K[x]/(q(x)) \supseteq K$$

Let $a := x+(q(x))$

$q(a) = q(x)+(q(x)) = 0+q(x)$

$\hookrightarrow$ v tej razširitvi K je $x+(q(x))$ ničla od $p(x)$.

to delfonje $K[x]$ povarjamo, najprej n-krat (za vsako ničlo). na koncu dobimo razširitev F za K, ki vsebuje vse ničle $p(x)$ — v F $p(x)$ razpade na linearne faktorje.

Def: razpadni obseg za $p(x) \in K[x]$ (nad K) je minimalna razširitev K, v kateri $p(x)$ razpade na linearne faktorje.

Izrek: Razpadni obseg $p(x) \in K[x]$ nad K obstaja in je enolično do izomorfizma. NE RABIMO DOKAZATI

Poljubna razpadna obsega sta izomorfna.

Poprej konstruktivno dokazano.

Primer: $x^2 - 2 \in \mathbb{Q}[x]$.

Lahko vzamemo

- $\mathbb{Q}(\sqrt{2})$, kjer razpade na $(x-\sqrt{2})(x+\sqrt{2})$
- $\mathbb{Q}[x]/(x^2-2)$, kjer razpade na $(x-a)(x+a)$ za $a := x + (x^2-2)$

ta dva obsega sta izomorfna.

ODMOR

let K končen obseg $\Rightarrow \operatorname{char} K = p$ v končno praštevil

$K \supseteq \mathbb{Z}_p$, $n = [K : \mathbb{Z}_p] \Rightarrow K$ ima p^n elementov.

$(K^\times = K \setminus \{0\}, \cdot)$ ... grupa s $p^n - 1$ elementi.

V vsaki grupi G velja $\forall a \in G: a^{|G|} = 1$.

torej $\forall a \in K \setminus \{0\}: a^{(p^n-1)} = 1$

$\Rightarrow$ vsak $a \neq 0$ je ničla polinoma $x^{(p^n-1)} - 1$.

$\Rightarrow$ vsi elementi K so ničle polinoma $x(x^{(p^n-1)} - 1) = x^{(p^n)} - x \Rightarrow x^{p^n} - x = \prod_{a_i \in K} (x - a_i)$

<u>Trditev:</u> če je K končen obseg, je K razpadni obseg polinoma $x^{|K|} - x$ nad $\mathbb{Z}_p$, kjer $p = \text{char } K$.

<u>Primer:</u> če ima K 27 elementov, je K razpadni obseg polinoma $x^{27} - x$ nad $\mathbb{Z}_3$.

<u>Trditev:</u>

Vzemimo p^n za p praštevilo in $n \in \mathbb{N}$.

Let $K :=$ razpadni obseg $x^{p^n} - x$ nad $\mathbb{Z}_p$
↳ minimalno velik

Let $K' \subseteq K$ ∋: $K = (\text{množica ničel } x^{p^n} - x)$.

TEDAJ VELJA K' je obseg in $|K'| = p^n$.

<u>Dokaz:</u> <u>$x^{p^n} - x$ nima večkratnih ničel</u>

če ima polinom $p(x)$ večkratne ničle, so te ničle stopnje $\geq p'(x)$. (odvodom).

$(x^{p^n}-x)' = p^n x^{p^n-1} - 1 \equiv -1 \pmod p$ ✓

$\Rightarrow K'$ ima p^n elementov.

<u>K' je zaprta za $+,-,\cdot,/$ (je obseg)</u>

vzemimo $a, b \in K'$ (velja, da $a^{p^n} = a$ in $b^{p^n} = b$).

$$ab = a^{p^n} b^{p^n} = (ab)^{p^n}$$

(komut.)

$$\frac{a}{b} = \frac{a^{p^n}}{b^{p^n}} = \left(\frac{a}{b}\right)^{p^n}$$

$$(a+b)^{p^n} = a^{p^n} + \underbrace{\binom{p^n}{1} a^{p^n-1} b + \cdots + \binom{p^n}{p^n-1} a b^{p^n-1}}_{=0,\ \text{ker so vsi koef. deljivi s } p \text{ in zato v mod } p = 0} + b^{p^n}$$

$$= a^{p^n} + b^{p^n}$$

$$(a-b)^{p^n} = \cdots = a^{p^n} - b^{p^n}$$

□

<u>Izrek:</u> $\forall p \in \mathbb{P},\ n \in \mathbb{N}\ \exists$ do na izomorfizmo natanko določen obseg, ki ima p^n elementov. Standardno ga označimo $\underbrace{GF(p^n)}_{\text{Galois-Field}}$. Dobimo ga tot razpadni obseg polinoma $x^{p^n} - x$ nad $\mathbb{Z}_p$.

<u>Primer:</u> Za opis $GF(p^n)$ je dovolj, če najdemo nerazcepni polinom $p(x)$ stopnje n nad $\mathbb{Z}_p$ (tak vselej obstaja -- kje bomo dokazali), potem je $GF(p^n)$ izomorfen

$\mathbb{Z}_p[x]/(p(x))$.

Primer: $GF(4) = \mathbb{Z}_2[x]/(x^2+x+1)$

$GF(27) = \mathbb{Z}_3[x]/(x^3+2x+1)$

Za K končen teloben brez deliteljev niča velja

$$K \cong GF(|K|)$$