

1 Polja in Galoisova teorija

11. Ponovitev in dopolnitev algebri 2

2. oktober 2024

Ponovitev pojmov: algebraični element, algebraično število, transcendentni element, končna polja, minimalni polinom, algebraična razširitev,...

Izrek: Naj bo $f(x) \in F[x]$ nekonstanten. Potem obstaja razširitev K od F v kateri ima $f(x)$ ničlo.

Dokaz: $p(x) \stackrel{\text{nerazcep}}{\mid} f(x)$

$$K := F[x]/(p(x))$$

"
J max. ideal

$$F \xrightarrow{\text{vložimo}} K$$

$$\lambda \longmapsto \lambda + J$$

$$f(x + J) = \sum_{i=0}^n (\lambda_i + J)(x + J)^i$$

$$f(x) = \sum_{i=0}^n \lambda_i x^i \quad \Rightarrow \quad = \sum_{i=0}^n (\lambda_i x^i + J)$$

$$= \left(\sum_{i=0}^n \lambda_i x^i \right) + J$$

$$= f(x) + J$$

$$= 0 + J$$



$$p(x) \mid f(x) \Rightarrow f(x) \in J$$

$$f(x) - (x-a)g(x) \Rightarrow \text{postopek nachaljujemo} \dots$$

$\Rightarrow \exists$ polje v katerem polinom razpade

Razpadno polje polinoma $f(x)$ nad F je najmanjša razširitev F v kater $f(x)$ razpade.

$$\rightarrow F(\underbrace{a_1, \dots, a_n}_{\text{natanko vse ničle } f(x)})$$

Opomba: Razpadno polje je končna razširitev:

$$[F(a_1, \dots, a_n) : F] < \infty.$$

Opomba: Če je K razpadno polje polinoma $f(x) \in F[x]$ nad F , potem je K tudi razpadno polje $f(x)$ nad vsakim vmesnim poljem L : $F \subseteq L \subseteq K$.

$$L(a_1, \dots, a_n) = F(a_1, \dots, a_n) = K.$$

Polje K je algebraično zaprto, če ima vsak nekonstanten polinom iz $K[x]$ vsaj eno ničlo v K .

Primer: \mathbb{C} je algebraično zaprto

$A \dots$ polje algebraičnih števil

A je algebraično zaprto

A je algebraično zaprtje \mathbb{Q}

\mathbb{C} je algebraično zaprtje \mathbb{R}

Opomba 1: $F \subseteq K$ in $a \in K$ algebraičen nad F .
 $\exists \varepsilon$ označimo evalvaciski homomorfizem

$$\varepsilon: F[x] \longrightarrow F(a)$$

$$\varepsilon: f(x) \mapsto f(a)$$

To je homomorfizem kolobarjev.

ε je surjektiven, saj je a algebraičen

in $\ker \varepsilon = \{p(x) \mid p(x)g(x) \in F[x]\}$.
 minimalni polinom za a

Po izreku o izomorfizmu

$$F[x]/(p(x)) \xrightarrow{\cong} F(a)$$

\swarrow kanonični epimorfizem

$$\begin{array}{ccc} F[x] & \xrightarrow{\pi} & F[x]/(p(x)) \\ \varepsilon \searrow & & \downarrow \bar{\varepsilon} \\ & & F(a) \end{array}$$

$$\varepsilon = \bar{\varepsilon} \circ \pi$$

$$\bar{\varepsilon}(\lambda + (p(x))) = \lambda \quad \text{za } \lambda \in F$$

$$\bar{\varepsilon}(x + (p(x))) = a$$

$\bar{\varepsilon}$ je izomorfizem

Opomba 2: $f: F \rightarrow F'$ izomorfizem polj.

Za vsak $\underbrace{f(x)}_{\sim} \in F[x]$ definiramo:

$$\sum_{i=0}^n \lambda_i x^i \quad f_f(x) := \sum_{i=0}^n f(\lambda_i) x^i$$

Tako dobimo izomorfizem kolobarjev

$$\begin{aligned} F[x] &\longrightarrow F'[x] \\ f(x) &\longmapsto f_f(x) \end{aligned}$$

(Kot v dokazu Gaussove leme.)

$p(x)$ nerazcepna $\Rightarrow p_f$ nerazcepna

$f(x)$ razpadne v F (\Leftrightarrow) f_f razpadne v F'

Lema: Naj bosta F in F' polji, $f: F \rightarrow F'$ izomorfizem. Naj bo $p(x) \in F[x]$ nerazcepna. Naj bo $p(a) = 0$ za nek $a \in K \cong F$ in $p_{f^*}(a') = 0$ za nek $a' \in K' \cong F'$.

Potem obstaja natanko en izomorfizem $\Phi: F(a) \rightarrow F'(a')$, ki je razširitev preslikave f in slika $a \vee a'$.

Dokaz: $F[x]/(p(x)) \xrightarrow{\bar{\epsilon}} F(a)$

$$\begin{array}{ccc} & \downarrow \tilde{f} & \downarrow \Phi \\ F'[x]/(p_{f^*}(x)) & \xrightarrow{\bar{\epsilon}'} & F'(a') \end{array}$$

$$\tilde{f}(f(x) + (p(x))) = f_{\bar{\epsilon}}(x) + (p_{\bar{\epsilon}}(x))$$

Enoličnost je očitna, saj $F(a)$ sestoji iz elementov oblike $\sum \lambda_i a^i$.

9. oktober 2024

Obstoj: $\bar{\epsilon}'(x + (p_{\bar{\epsilon}}(x))) = a'$

$$\bar{\epsilon}'(\lambda + (p_{\bar{\epsilon}}(x))) = \lambda \quad \text{za } \lambda \in F'$$

$$\tilde{f}(f(x) + (p(x))) := f_{\bar{\epsilon}}(x) + (p_{\bar{\epsilon}}(x))$$

\tilde{f} je dobro definiran in je izomorfizem \leftarrow D.N.

$$\Phi := \bar{\epsilon}' \circ \tilde{f} \circ \bar{\epsilon}^{-1}$$

To je izomorfizem, saj je kompozitum izomorfizmov.

$$\begin{aligned} \Phi(a) &= a' \\ \Phi(\lambda) &= f(\lambda) \quad \text{za } \lambda \in F \end{aligned} \quad \left. \begin{array}{l} \text{glej} \\ \text{diagram} \end{array} \right\}$$

77

Izrek: Naj bo $\varphi: F \rightarrow F'$ izomorfizem polj in $f(x) \in F[x]$ nekonstanten. Naj bo K razpadno polje $f(x)$ nad F in K' razpadno polje $f_\varphi(x)$ nad F' . Potem lahko φ razširimo do izomorfizma $K \rightarrow K'$.

Opomba: Za $F = F'$ in $\varphi = \text{id}$ dobimo: Razcepno polje vsakega nekonstantnega polinoma $f(x) \in F[x]$ nad F je do izomorfizma natančno določeno.

Dokaz: Indukcija na $n := [K:F]$.

$$\begin{aligned} n=1: & \Rightarrow K=F \Rightarrow f(x) \text{ razpade nad } F \\ & \Rightarrow f_\varphi \text{ razpade nad } F'=K' \quad \checkmark \end{aligned}$$

$\leftarrow n \rightarrow n$:

$K \supsetneq F \Rightarrow \exists$ nerazcepni polinom $p(x) \in F[x]$ stopnje $m > 1$, ki deli $f(x)$

$$\Rightarrow p_\varphi \mid f_\varphi(x)$$

Naj bo $a \in K$ ničla $p(x)$ in $a' \in K$ ničla $p_\varphi(x)$.

Lema: obstaja izomorfizem $\Phi: F(a) \longrightarrow F'(a')$, ki razširi φ in a preslikava v a' .

Uporabimo indukcijsko predpostavko za Φ :

$$[K:F] = [K:F(a)] \underbrace{[F(a):F]}_{m>1}$$

$$\Rightarrow [K:F(a)] = \frac{n}{m} < n$$

Torej $\Phi: F(a) \rightarrow F'(a')$ lahko razširimo do izomorfizma iz K v K' . 

1.2 Polja s karakteristiko 0

Izrek: Naj bo F polje s karakteristiko 0 in $p(x) \in F[x]$ nerazcepni polinom. Potem ima $p(x)$ v vsaki razširitvi F same enostavne ničle.

Dokaz: $p(x) = (x-a)^2 \cdot h(x)$

$$p'(x) = 2(x-a) \cdot h(x) + (x-a)^2 h'(x)$$
$$\Rightarrow p'(a) = 0$$

$p(x)$ je minimalni polinom od a protišteje
 $\deg p'(x) = \deg p(x) - 1, \quad p'(a) = 0$

\uparrow
char = 0



Izrek: Naj bo F polje s karakteristiko 0, $f(x) \in F[x]$ nekonstanten polinom in K razpadno polje $F(x)$ nad F . Naj bo $\varphi: F \rightarrow F'$ izomorfizem polj in K' razpadno polje $f_\varphi(x)$ nad F' .

Potem obstaja natanko $[K:F]$ razširitev izomorfizma φ do izomorfizma iz K v K' .

Dokaz: Indukcija po $n = [K:F]$.

$n=1$: $K=F$ in $K'=F' \Rightarrow$ ena sama razširitev

$1, \dots, n-1 \rightarrow n$: Naj bo $p(x)$ nerazcepni polinom stopnje $m > 1$, ki deli $f(x)$.

$$\Rightarrow p_\varphi(x) \mid f_\varphi(x)$$

Naj bo $a \in K$ ničla $p(x)$. $p(a)=0$

Naj bo $\varphi: K \rightarrow K'$ nek izomorfizem, ki razširi φ .

$$p_\varphi(\varphi(a)) = ?$$

$$p(x) = \sum_{i=0}^m \lambda_i x^i$$

$$p_\varphi(\varphi(a)) = \sum_{i=0}^m \varphi(\lambda_i) \varphi(a)^i$$

$$\varphi \text{ razširitev } \varphi = \sum_{i=0}^m \varphi(\lambda_i) \varphi(a)^i$$

$$\varphi \text{ hom.} \rightarrow \sum_{i=0}^m \varphi(\lambda_i \cdot a^i)$$

$$= \varphi(p(a))$$

$$= 0$$

$\Rightarrow p_\varphi(x)$ ima natanko m nikel v K' (saj $\text{char} F = 0$)

Naj bodo a_1, \dots, a_m nicle $p_\varphi(x)$ in $a' \in \{a_1, \dots, a_m\}$.

Pokažimo, da obstaja natanko $\frac{n}{m}$ izomorfizmov, ki razširijo φ in slikajo $a \mapsto a'$.

Po lemi vemo, da obstaja natanko en izomorfizem $\Phi: F(a) \rightarrow F'(a')$, ki razširi φ in slikuje a v a' .

$$[K:F(a)] = \frac{[K:F]}{[F(a):F]} = \frac{n}{m} < n$$

I. P.: Obstaja točno $\frac{n}{m}$ izomorfizmov $K \rightarrow K'$, ki razširijo Φ .

Ker τ slika a v enega izmed a_i , sledi, da imamo $m \cdot \frac{n}{m} = n$ izomorfizmov $K \rightarrow K'$, ki razširijo f . \square

Definicija: Razširitev K/F je **enostavna**, če je $K = F(a)$ za nek $a \in K$.

Tak a imenujemo **primitivni element**.

Opozba: Primitivni element ni enolično določen.

Izrek: [O primitivnem elementu]: Vsaka končna razširitev polja s karakteristiko q je enostavna.

Dokaz: Naj bo K končna razširitev: $K = F(a_1, \dots, a_n)$.

Zadošča obravnavati $n=2$, saj je

$$K = F(a_1, \dots, a_{n-2})(a_{n-1}, a_n).$$

Zato privzemimo $n=2$. Torek $K = F(b, c)$.

$$\exists a \in K. K = F(a).$$

Kot elementa končne razširitve, sta b in c algebraična nad F .

$$F[x] \ni \begin{cases} p(x) := \text{minimalni polinom } b \text{ nad } F \\ q(x) := \text{minimalni polinom } c \text{ nad } F \end{cases}$$

Vzemimo K_1 : katerakoli razširitev K v kateri $p(x)$ in $q(x)$ razpadeta. (Recimo razpadno polje $p(x) \cdot q(x)$ nad K).

Naj bodo $b = b_1, \dots, b_r \in K_1$ ničle $p(x)$

in $c = c_1, \dots, c_s \in K$, ničle $g(x)$.

Polje F je neskončno (saj je $\text{char} F = 0$), zato lahko izberemo tak $\lambda \in F$, da velja

$$\forall j. \forall k \neq 1. \lambda \neq (b_j - b)(c - c_k)^{-1}$$

Definiramo: $a := b + \lambda c$

$$K = F(a)$$

$a \in F(b, c)$ očitno

$$\Rightarrow F(a) \subseteq F(b, c)$$

$$b, c \in F(a)$$

Zadostīca $c = F(a)$, saj $b = a - \lambda c$

Vpeljimo:

$$f(x) = p(a - \lambda x) \in F(a)[x]$$

$$f(c) = p(a - \lambda c) = p(b) = 0$$

↑
p minimalni polinom za b

$$g(c) = 0 \vee \text{in } g(x) \in F[x] \subseteq F(a)[x]$$

Naj bo $\tilde{g}(x) \in F(a)[x]$ minimalni polinom c nad $F(a)$.

$$\Rightarrow \tilde{g}(x) | f(x) \text{ in } \tilde{g}(x) | g(x)$$

Vsaka ničla $\tilde{g}(x)$ je tudi ničla $f(x)$ in $g(x)$.

Edine možne ničle $\tilde{g}(x)$ so torej $c = c_1, \dots, c_s$.

Recimo $\tilde{g}(c_k) = 0$ za $k \neq 1 \Rightarrow f(c_k) = 0$

$$\Rightarrow p(a - \lambda c_k) = 0 \Rightarrow a - \lambda c_k = b_j \text{ za nek } j$$

Tov je protislovje z izbirko λ .

Torej: c je edina ničla $\widehat{g}(x)$.

Polinom $\tilde{g}(x)$ je kot minimalni polinom nerazcep.

$\text{char } F = 0$

\Rightarrow same enostavne ničle

$$\Rightarrow \tilde{g}(x) = x - c$$

$$\tilde{g}(x) \in F(a)[x] \Rightarrow c \in F(a)$$



1.3. Galoisova teorija (motivacija) 16. oktober 2024

Dani sta polji $E \supseteq F$ s karakteristiko 0. Zanimajo nas vmesna polja med F in K ($F \subseteq L \subseteq K$).

Oznaka: $\mathcal{F} := \{\text{vmesna polja med } F \text{ in } K\}$

Galoisova teorija to poveže s teorijo grup.

$$G := \text{Aut}(\mathbb{K}/F) = \left\{ \sigma \in \text{Aut } \mathbb{K} \mid \forall \lambda \in F. \quad \sigma(\lambda) = \lambda \right\}$$

6 je grupa za kompozitum

Dogовор: $\mathfrak{f}^\sigma := \mathfrak{f} \circ \sigma$

$\text{id} =: 1$

$\mathcal{C} := \{\text{vse podgrupe } G\} \leftarrow \text{običajno je to končna grupa}$

Galois poveže F in G .

Primer: $\mathbb{F} = \mathbb{R}$, $\mathbb{K} = \mathbb{C}$

$$R \subseteq L \subseteq C$$

$$l \in L \setminus \mathbb{R} \Rightarrow l = a + bi; \quad a, b \in \mathbb{R}, \quad b \neq 0$$

$$\Rightarrow i = (b-a)b^{-1} \in L \Rightarrow L = \mathbb{C}$$

(Torej ne obstaja polje med \mathbb{R} in \mathbb{C})

$$\Rightarrow \mathcal{F} = \{\mathbb{R}, \mathbb{C}\}$$

$$\Rightarrow G = \{ \text{id}, \text{konjugiranje} \}$$

Naj bo řečen.

$$i^2 + 1 = 0 \rightarrow f(i^2) + f(1) = 0$$

$$\Rightarrow f(i) \in \{\pm i\}$$

Če je $f(i) = i \Rightarrow f = \text{id}.$

Če je $f(i) = -i \Rightarrow f = \text{konjugiranje}.$

$$\Rightarrow G = \{\{1\}, G\}$$

$\Rightarrow |\mathcal{G}| = |\mathcal{F}|$ izkaže se, da to velja za Galoisove razširitve

Za razširitev K polja F je ekvivalentno: ($\text{char}=0$)

1) E je razpadno polje nekega polinoma iz $F[x]$.

2) Če ima nerazcepni polinom $p(x) \in F[x]$ eno ničlo v $K \Rightarrow p(x)$ razpade v K .

3) $|G| = [K:F]$

V tem primeru je K Galoisova razširitev F .

Primer: $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{2})$

$$\mathcal{F} = \{\mathbb{Q}, \mathbb{Q}(\sqrt[3]{2})\} \quad (\text{ni vmesnih polj})$$

$$G = \{1, \sigma\}; \quad \sigma(\lambda + \mu\sqrt[3]{2}) = \lambda + \mu\sqrt[3]{2}$$

"konjugiranje"

$$\mathcal{G} = \{\{1\}, G\}$$

Spet velja $|\mathcal{F}| = |\mathcal{G}|$.

Primer: $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{2})$

$$\sigma \in G = \text{Aut}(K/F)$$

$$\sigma(\sqrt[3]{2}) = ?$$

$$\sigma(\sqrt[3]{2})^3 = \sigma(2) = 2$$

$$\Rightarrow \sigma(\sqrt[3]{2}) = \sqrt[3]{2} \quad (\text{zanimajo nas le rešitve v } K)$$

$$\Rightarrow \sigma = 1 \Rightarrow G = \{1\}$$

$$F = \{F, K\} \Rightarrow |F| \neq |G|$$

K ni Galoisova razširitev E (glej 2. pogoj)

Definicija: Za vsak $H \in \mathcal{G}$ definiramo

$$K^H := \{x \in K \mid \forall \sigma \in H. \sigma(x) = x\}$$

polje fiksnih točk podgrupe H

$$\text{Velja } K^{G^c} = K \quad \text{in} \quad K^G = F.$$

\nwarrow to ne velja v splošnem
(pri Gal. razširitvah pa)

Fundamentalni izrek Galoisove teorije:

Za Galoisovo razširitev K od F velja:

(a) $H \mapsto K^H$ je bijekcija $\mathcal{G} \rightarrow \mathcal{F}$

(b) $H \subseteq H' \Leftrightarrow K^{H'} \subseteq K^H$ (vsebovanosti se "obrnejo")

(c) $|H| = [K : K^H]$

Primer: $F = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3}) \xleftarrow{\text{baza nad } \mathbb{Q}} \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{3}, \sqrt[3]{6})$

K je razpadno polje za $(x^2 - 2)(x^2 - 3)$ nad \mathbb{Q}

$\Rightarrow K$ je Galoisova razširitev

$$\sigma \in G. \quad \sigma(\sqrt[3]{2})^2 = 2, \quad \sigma(\sqrt[3]{3})^2 = 3$$

$$\Rightarrow \begin{cases} \sigma(\sqrt{2}) = \pm \sqrt{2} \\ \sigma(\sqrt{3}) = \pm \sqrt{3} \end{cases} \Rightarrow \text{Največ 4 avtomorfizmi.} \Rightarrow |G| \leq 4$$

Elementi G:

- $\sqrt{2} \mapsto \sqrt{2}, \sqrt{3} \mapsto \sqrt{3} \dots \text{id}$
- $\sqrt{2} \mapsto \sqrt{2}, \sqrt{3} \mapsto -\sqrt{3} \dots \sigma$
- $\sqrt{2} \mapsto -\sqrt{2}, \sqrt{3} \mapsto \sqrt{3} \dots \rho$
- $\sqrt{2} \mapsto -\sqrt{2}, \sqrt{3} \mapsto -\sqrt{3} \dots \sigma\rho = \rho\sigma$

$$\begin{aligned} \sigma(\lambda_0 + \lambda_1\sqrt{2} + \lambda_2\sqrt{3} + \lambda_3\sqrt{6}) &= \dots \\ \rho(\dots) &= \dots \end{aligned} \Rightarrow \rho\sigma = \sigma\rho$$

$$|G| = [K:F] = 4$$

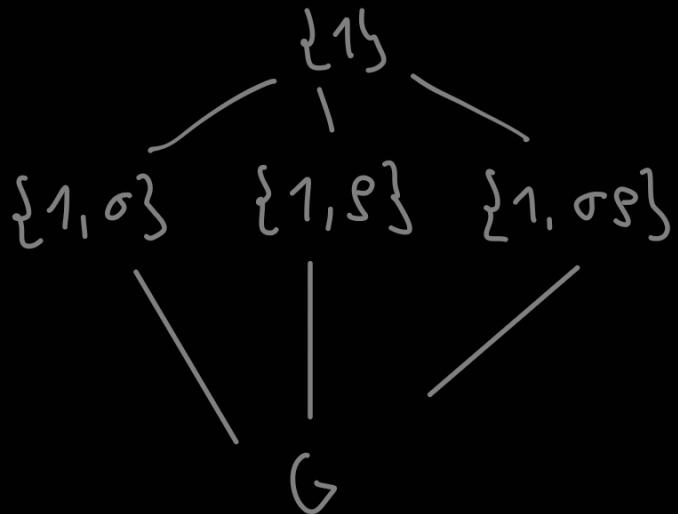
Imamo samo 4 možnosti za avtomorfizem.

$$\Rightarrow G = \{1, \sigma, \rho, \sigma\rho\} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

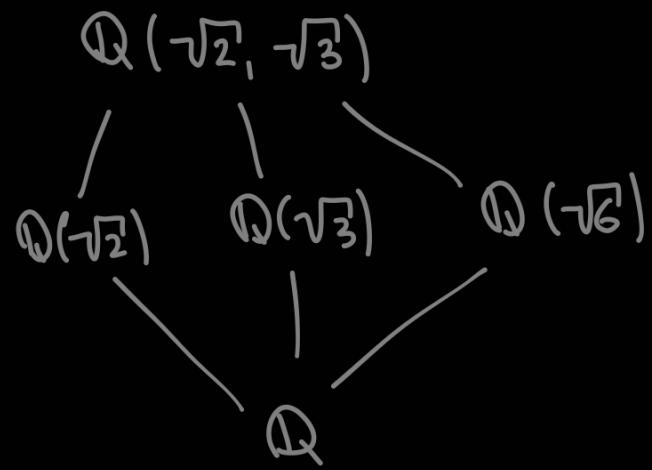
$\uparrow \quad \uparrow \quad \searrow \quad \uparrow$
vsi trije so reda 2

vse štiri
možnosti so
res avtomorfizmi

Podgrupe:



Vmesna polja:



Primer: $F = \mathbb{Q}$, $w := e^{\frac{2\pi i}{3}}$... primitivni 3. koren enste

$$K := F(\sqrt[3]{2}, w), \quad [K:F] = 6$$

K je razpadno polje za $x^3 - 2$ nad F

$$\Rightarrow |G| = 6$$

Minimalni polinom w je $x^2 + x + 1$. Ničli: w, w^2

Standardna baza K nad F :

$$\{1, \sqrt[3]{2}, \sqrt[3]{2}^2, w, \sqrt[3]{2}w, \sqrt[3]{2}^2w\}$$

$$\sigma \in G \Rightarrow \sigma(\sqrt[3]{2})^3 = 2$$

$$\sigma(\sqrt[3]{2}) \in \left\{ \sqrt[3]{2}, \sqrt[3]{2}w, \sqrt[3]{2}^2w \right\}$$

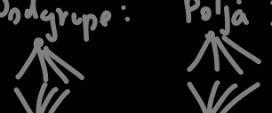
$\underbrace{\phantom{\sqrt[3]{2}}}_{-w-1}$

$$\sigma(w) \in \{w, w^2\}$$

$$w^2 + w + 1 = 0 \Rightarrow \sigma(w)^2 + \sigma(w) + 1 = 0$$

Avtomorfizmi: $w \mapsto 2$ možnosti }
 $\sqrt[3]{2} \mapsto 3$ možnosti } 6 avtomorfizmov

$$\left. \begin{array}{l} w \mapsto w, \sqrt[3]{2} \mapsto \sqrt[3]{2}w \\ \text{in } w \mapsto w^2, \sqrt[3]{2} \mapsto \sqrt[3]{2} \end{array} \right\} \text{ne komutirata!}$$

Podgrupe: 

G nekomutativna, $|G|=6 \Rightarrow G \cong S_3$

Galoisova teorija pove tudi:

- $H \triangleleft G \Leftrightarrow K^H$ je Galoisova razširitev F
- $G/H \cong \text{Aut}(K^H/F)$

(Na avtomorfizme lahko gledamo kot na permutacije ničel polinomov.)

1.4. Fundamentalni izrek Galoisove teorije

Lema Q: Naj bo $\sigma \in \text{Aut}(K/F)$. Če je $a \in K$ ničla $f(x) \in F[x]$, potem je tudi $f(\sigma(a)) = 0$.

Dokaz: $f(x) = \sum \lambda_i x^i \quad \lambda_i \in F$

$$0 = f(a) = \sum \lambda_i a^i$$

$$\Rightarrow 0 = \sigma(f(a)) = \sum \lambda_i \sigma(a)^i = f(\sigma(a)) \quad \square$$

Opomba: Naj bo K končna razširitev F in $\text{char } K = \text{char } F = 0$.

Po izreku o primitivnem elementu $K = F(a)$ za nek $a \in K$.

Naj bo $p(x) \in F[x]$ minimalni polinom za a .

Vsek $\sigma \in \text{Aut}(K/F)$ je enolično določen z delovanjem na a . Naj bo $m = \deg p(x)$. Ker je $p(a) = 0$, je $\sigma(a)$ ničla od $p(x)$. Ničle od $p(x)$ so a_1, a_2, \dots, a_m , (paroma različne, saj je karakteristika 0). a se lahko s σ preslikava v a_1, \dots, a_m , torej imamo največ m avtomorfizmov. Lema od zadnjič nam pove, da imamo točno m avtomorfizmov. Torej $|\text{Aut } K/F| = m = [K:F]$.

23. oktober 2024

$$H \leq G, [K:F] < \infty, \text{char } F = 0$$

Lema 1: Naj bo $a \in K$ in naj bodo $a = a_1, a_2, \dots, a_m$ različni elementi množice $\{\delta(a) \mid \delta \in H\}$. Potem je

$$p(x) = (x-a_1)(x-a_2) \cdots (x-a_m)$$

minimalni polinom a nad K^H .

Dokaz: $p(x)$ ima koeficiente iz K^H .

$$p_p(x) \quad p(x) = \sum d_i x^i$$

$$p \in H \quad p_p(x) = \sum p(d_i) x^i$$

$$\text{tudi } p_p(x) = (x - p(a_1)) \cdot (x - p(a_2)) \cdots (x - p(a_m))$$

Velja $a_i = \delta_i(a)$ za nek $\delta_i \in H$.

$$p(a_1) = \underbrace{\sum_{\sigma \in H} \sigma(p(a))}_{\in \{p(a)\}} \in \{\sigma(a) \mid \sigma \in H\} = \{a_1, \dots, a_m\}$$

$$p(a_1) \in \{a_1, \dots, a_m\}$$

$$p \text{ injektiven} \Rightarrow \{p(a_1), \dots, p(a_m)\} = \{a_1, \dots, a_m\}$$

$$\Rightarrow p_p(x) = p(x) \Rightarrow p(d_i) = d_i \quad \forall p \in H.$$

$$\Rightarrow d_i \in K^H.$$

Naj bo $f(x) \in K^H[x]$: $f(a) = 0$.

lema $\Rightarrow a_2, a_3, \dots, a_m$ so tudi nicle $f(x)$

$\Rightarrow p(x) | f(x) \Rightarrow p(x)$ minimalni polinom

□

Lema 2: $|H| = [K : K^H]$ in $[K : F] = |H| \cdot [K^H : F]$.

Dokaz: Izrek o primitivnem elementu: $K = F(a)$,

$$F \subseteq K^H \subseteq K$$

$$\Rightarrow K = K^H(a)$$

Zato: $[K : K^H] =$ st. m minimalnega polinoma
a nad K^H

Lema 1: $m = |\{\sigma(a) \mid \sigma \in H\}| = |H|$, saj različna
avtomorfizma iz H slikata a v različna
elementa (če bi bila avtomorfizma enaka v a ,
bi bila enaka na $K^H(a) = K$).

Druga formula trivialno sledi. □

Izrek: $[K : F] < \infty$, $\text{char } F = 0$

Naslednje trditve so ekvivalentne:

(i) $|\text{Aut}(K/F)| = [K : F]$

(ii) $K^{\text{Aut}(K/F)} = F$

(iii) Vsak nerazcepni polinom iz $F[X]$ z ničlo v K ,
razpade v K .

(iv) K je razpadno polje nekega nerazcepnega
polinoma iz $F[X]$.

(v) K je razpadno polje nekega polinoma iz $F[x]$.

Dokaz: (i) \Rightarrow (ii) $G = \text{Aut}(K/F)$.

Lema 2 za $H = G$: $[K : F] = |G| [K^G : F]$

$$\stackrel{(i)}{\Rightarrow} [K^G : F] = 1 \Rightarrow K^G = F$$

(ii) \Rightarrow (iii) $K^G = F$. Naj bo a ničla nekega nerazcepnega
polinoma $p(x) \in F[x]$.

BŠS: vodilni koeficient je 1 $\Rightarrow p(x)$ minimalni polinom
a nad F

Vporabimo lemo 1 za $H = G$ in vpoštevamo $K^G = F$:

$p(x) = (x - a_1) \cdots (x - a_m) \in F[x]$ je minimalni polinom
a = a_1 nad F. Torej $p(x)$ razpade.

(iii) \Rightarrow (iv): Izrek o primitivnem elementu: $K = F(a)$

Naj bo $p(x)$ minimalni polinom a nad F. Po
predpostavki razpade:

$$p(x) = (x - a)(x - a_2) \cdots (x - a_m)$$

Zato je K razpadno polje tega polinoma.

Razp. polje je po def: $F(a_1, \dots, a_m) \underset{a}{\supseteq} K = F(a)$

(iv) \Rightarrow (v): ✓

(v) \Rightarrow (i): Sledi iz izreka iz začetka: $K = K$ in $\text{id} = \text{id}$. ☐

Definicija: Končna razširitev K polja F, char F = 0,
se imenuje Galoisova razširitev, če ustreza
vsem pogojem zadnjega izreka.

Tedaj $\text{Aut}(K/F)$ označujemo tudi z $\text{Gal}(K/F)$.

Če je razpadno polje polinoma $f(x) \in F[x]$, potem
K imenujemo tudi Galoisova razširitev polinoma $f(x)$.

Opoomba: Splošneje te pojme vpeljemo za polja s
poljubno karakteristiko.

Galoisova razširitev je normalna in seperabilna
razširitev.

Normalna pomeni: algebraična razširitev, ki zadošča
(iii) iz izreka

Separabilna razširitev: vsak nerazcepni polinom je
separabilen, tj. vse njegove ničle so enostavne.

Opoomba: K Gal. razširitev F in L vmesno polje:
 $F \subseteq L \subseteq K$. Potem je K tudi Galoisova razširitev
L (saj je razpadno polje istega polinoma nad L
kot nad F). Zato govorimo o $\text{Gal}(K/L)$. L ni
nujno Galoisova razširitev F.

Izrek: Naj bo K Galoisova razširitev polja F, char F = q.
Označimo s \mathcal{F} množico vseh vmesnih polj med
F in K in naj bo \mathcal{G} množica vseh podgrup
grupe $G := \text{Gal}(K/F)$.

a) Preslikava $\alpha: \mathcal{G} \rightarrow \mathcal{F}$, $\alpha(H) = K^H$, je bijektivna
in njeni inverzni preslikavi je

$$\beta: \mathcal{F} \rightarrow \mathcal{G}, \beta(L) = \text{Gal}(K/L).$$

b) Če H ustrezata L, tj. $L = K^H$ ali ekvivalentno
 $H = \text{Gal}(K/L)$ – potem je $|H| = [K:L]$ in
 $[G:H] = [L:F]$.

c) Če H ustrezata L in H' ustrezata L', potem je
 $H \subseteq H' \Leftrightarrow L \supseteq L'$.

d) Če H ustreza L , potem je $H \triangleleft G \Leftrightarrow L$ je Galoisova razširitev F . V tem primeru $G/H \cong \text{Gal}(L/F)$.

Dokaz: (a) $\alpha \circ \beta = \text{id}_F$ in $\beta \circ \alpha = \text{id}_G$

$$\begin{aligned} \alpha(\beta(L)) &= L \\ \beta(\alpha(H)) &= H \end{aligned} \quad K_{\text{Gal}(K/L)} = L \quad \text{in } \text{Gal}(K/K^H) = H$$

K je Gal. razširitev L in zato iz izreka (ii)

Sledi: $K^{\text{Gal}(K/L)} = L$

$H \subseteq \text{Gal}(K/K^H)$ očitno.

Zato zadostiča dokazati, da imata grupe istired.

Lema 2: $|H| = [K : L]$ in po izreku (i) je

$$[K : L] = |\text{Gal}(K/L)|.$$

(b) $|H| = [K : L]$, kjer je $L = K^H$ je lema 2

$$[G : H] = [L : F]$$

$$[G : H] = \frac{|G|}{|H|} \xrightarrow{(i)} \frac{[K : F]}{[K : L]} = [L : F].$$

(d) $H \longleftrightarrow L \quad L = K^H \quad \text{in} \quad H = \text{Gal}(K/L)$

$$H \triangleleft G \Leftrightarrow \sigma \varphi \sigma^{-1} \in H \quad \forall \sigma \in G \quad \forall \varphi \in H$$

$$H = \text{Gal}(K/L)$$

$$\Leftrightarrow (\sigma^{-1} \varphi \sigma)(\ell) = \ell \quad \forall \sigma \in G, \forall \varphi \in H, \forall \ell \in L.$$

$$\Leftrightarrow \sigma(\sigma(\ell)) = \sigma(\ell) \quad -11-$$

$$\stackrel{L=K^H}{\Leftrightarrow} \sigma(\ell) \in L \quad \forall \ell \in L \quad \forall \sigma \in G$$

Torej: $H \circ G \Leftrightarrow \sigma(L) \subseteq L \quad (\Leftarrow) \quad \sigma(L) = L$

\uparrow
 na končnem razsežnem prostoru
 so inj. preslikave avtomatsko
 tudi surjektivne

Hzd6 vemo $\sigma(L) = L \quad \forall \sigma \in G$.

Def. $\varphi: G \longrightarrow \text{Aut}(L/F)$

$$\varphi(\sigma) = \sigma|_L$$

φ kom. Izrek o izom.

$$G/\ker \varphi \cong \text{Im } \varphi$$

"

$$\text{Gal}(K/L)$$

$$G/\underbrace{\text{Gal}(K/L)}_H \cong \text{Im } \varphi \leq \text{Aut}(L/F)$$

Za $G/H \cong \text{Aut}(L/F)$ zadostiča dokazati, da imata grupe isti red.

Iz leme 2 sledi: $|\text{Aut}(L/F)| \mid [L:F]$.

Iz (b) sledi: $[L:F] = [G:H] = |G/H|$.

\Rightarrow števili sta enaki.

Pogoj (i) iz izreku je izpoljen

$\Rightarrow L$ Galoisova razširitev F .

Naj bo L Galoisova razširitev F .

$$\sigma(L) \subseteq L \quad \forall \sigma \in G$$

L je razpadno polje $f(x) \in F[x]$,

$$L = F(a_1, \dots, a_m)$$

$$\sigma \in G \Rightarrow \sigma(L) \subseteq L$$

ažurnjanje

(c) domaća naloga



1.5. Rešljivost polinomskih enačb z radikali

30. oktober 2024

Primer: S_3 ni Abelova, je rešljiva

$$N = A_3 \triangleleft S_3$$

N Abelova, G/N Abelova

$$N \cong \mathbb{Z}_3 \quad G/N \cong \mathbb{Z}_2$$

Definicija: Grupa G je rešljiva, če obstajajo take edinice

$$N_0 = \{1\} \leq N_1 \leq N_2 \leq \dots \leq N_m = G,$$

da je N_{i+1}/N_i Abelova grupa za $i=0, \dots, m-1$.

Torej: S_3 je rešljiva grupa.

Primer: S_4 je rešljiva:

$$N_0 = \{1\} \leq N_1 \leq N_2 \leq N_3 = S_4$$

$\nearrow \nearrow$
preprasta vaja

Opomba: Nujno potrebujemo dve "imesni" grapi. Ena ne zadostira.

Izrek [Feit - Thompson]: Vsaka grupa lihega reda je rešljiva.

Dokaz na 250 straneh. \Downarrow

Nekomutativna enostavna grupa ne more biti rešljiva. (direktni iz definicije)

Primer: A_5 ni rešljiva

Trditev: (1) Podgrupa rešljive grupe je rešljiva.
(2) Naj bo $N \triangleleft G$. Potem je G rešljiva $\Leftrightarrow N$ in G/N sta rešljivi.

Dokaz izpustimo (pomanjkanje čusa).

Iz (1) sledi: S_n , $n \geq 5$, ni rešljiva (saj vsebuje A_5).

Lema: Naj bo F polje vsebovano v \mathbb{C} , $a \in F$. Potem je Galoisova grupa polinoma $f(x) = x^n - a$ n poljuben rešljiva

Dokaz: $K = F(a, w)$, $w = e^{\frac{2\pi i}{n}}$, $w^n = 1$

$F(w)$ je razpadno polje $x^n - 1$

$\sigma, \rho \in \text{Gal}(F(w)/F)$

σ in ρ sta določena z vrednostjo v w

Preslikata w v potenco w :

$$\sigma(w) = w^j, \quad \rho(w) = w^i$$

$$\rho\sigma(w) = \rho(w^j) = (w^i)^j = w^{ij}$$

$$\text{Podobno } \sigma\rho(w) = w^{ji} = w^{-ij}$$

$$\Rightarrow \rho \cdot \sigma = \sigma \cdot \rho$$

$\Rightarrow \text{Gal}(F(w)/F)$ je torej Abelova

$$\text{Gal}(K/F(w)), \quad K = F(a, w)$$

ρ_1, σ_1 avtomorfizma iz te grupe.

Določena sta z vrednostjo v a (w fiksirata)

$$\sigma_1(a) = aw^i \quad \rho_1(a) = aw^{i'}$$

$$\Rightarrow \sigma_1 \rho_1(a) = \rho_1 \sigma_1(a)$$

\Rightarrow Tudi $\text{Gal}(K/F(w))$ je torej Abelova.

$F(w)$ je Galoisova razširitev F , zato je

$$H := \text{Gal}(K/F(w)) \triangleleft G$$

$$\text{in } G/H \cong \text{Gal}(F(w)/F).$$

$$\text{in } G/H \cong \text{Gal}(F(w)/F)$$

Hin G/H sta Abelovi, torej je G rešljiva. \square

Definicija: Naj bo F polje. Polinom $f(x) \in F[x]$ je rešljiv z radikali nad F , če obstajajo takki elementi a_1, \dots, a_m iz neke razširitve F , da

(a) $f(x)$ razpade v $F(a_1, \dots, a_m)$.

(b) Obstajajo $n_1, n_2, \dots, n_m \in \mathbb{N}$, $a_1^{n_1} \in F$ in

$$a_i^{n_i} \in F(a_1, a_2, \dots, a_{i-1})$$

Neformalno: tu imamo korenjenje

Primer: $a, b, c \in \mathbb{C}$

$$f(x) = ax^2 + bx + c$$

$$F = \mathbb{Q}(a, b, c)$$

$f(x)$ je rešljiv z radikali nad F

$$\text{Ničli sta: } \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

$$a_1 = \sqrt{b^2 - 4ac}$$

(a) $f(x)$ razpade v $F(a_1)$

(b) $a_1^2 \in F$

Podobno polinomi stopenj 3 in 4.

Opomba: $a = a_1^{n_1} \in F$

$$a_1 = \sqrt[n_1]{a_1}$$

V $F(a_1)$ so torej elementi oblike

$$\sum \lambda_i \sqrt[n_1]{a_1^i}, \quad \lambda_i \in F$$

$$F(a_1) \leadsto B = a_2^{n_2}, \quad a_2 = \sqrt[n_2]{B}$$

Elementi v $F(a_1, a_2)$ so oblike

$$\sum f_j \sqrt[n_2]{B^j}, \quad f_j \in F(a_1)$$

itd.

Torej neformalna definicija res govori o korenih

Izrek: Naj bo $F \subseteq \mathbb{C}$ in $f(x) \in F[x]$. Če je $f(x)$ rešljiv z radikalni nad F , potem je Galoisova grupa $f(x)$ nad F rešljiva.

Zanimivost: velja natanko tedaj

Ideja dokaza: splošno situacijo zreduciramo na zgornjo kno.

Lema: Naj bo $p(x) \in \mathbb{Q}[x]$ nerazcepni polinom stopnje 5 z natanko tremi realnimi ničlami. Potem $p(x)$ ni rešljiv z radikalni nad \mathbb{Q} .

Dokaz: Zaradi nerazcepnosti ima 5 različnih ničel:

$$\underbrace{a_1, a_2, a_3}_{\mathbb{R}}, a_4, a_5$$

$$a_4 = \bar{a_5} \in \mathbb{C} \setminus \mathbb{R}$$

$K = \mathbb{Q}(a_1, a_2, a_3, a_4, a_5)$ razpadno polje

$G := \text{Gall}(K/\mathbb{Q})$ ni rešljiva.

Vsek $\sigma \in G$ je enolično določen z vrednostmi v a_1, \dots, a_5 in jih permutira.

$$\sigma \mapsto \sigma|_{\{a_1, \dots, a_5\}}$$

je vložitev G v S_5 .

$(z \mapsto \bar{z}) \in G$ (a_1, \dots, a_3 ohrani, $a_4 \leftrightarrow a_5$)

G torej vsebuje transpozicijo

Naj bo $a \in \{a_1, \dots, a_5\}$.

a je ničla nerazcepnega polinoma $p(x)$ stopnje 5

Torej je a algebraično število stopnje 5:

$$[\mathbb{Q}(a) : \mathbb{Q}] = 5, \quad \mathbb{Q} \leq \mathbb{Q}(a) \leq K$$

$$[K : \mathbb{Q}] = [K : \mathbb{Q}(a)] \cdot [\mathbb{Q}(a) : \mathbb{Q}]$$

$$\Rightarrow 5 \mid [K : \mathbb{Q}] \stackrel{\text{fundamentalni izrek}}{=} |G|$$

Po Cauchyjevem izreku G vsebuje element reda 5.

To pomeni: G vsebuje 5-cikel

Dejstvo: Če podgrupa S_5 vsebuje transpozicijo in 5-cikel, je enaka S_5 .

Torej je $G = S_5$ in ni rešljiva grupa. \square

Izrek: Obstajajo polinomi iz $\mathbb{Q}[x]$ stopnje 5, ki niso rešljivi z radikali.

Dokaz: $p(x) = x^5 - 3x^4 + 3 \in \mathbb{Q}[x]$.

Eisenstein \Rightarrow nerazcepnost.

$p(-1) < 0, p(0) > 0, p(2) < 0, p(3) > 0 \Rightarrow$ vsaj 3 realne ničle

$p'(x) = x^4 - 13x^3$ ima le dve ničli

Rolleov izrek \Rightarrow nimu 5 realnih ničel \square

2. Moduli

2.1. Vložitev kolobarja v kolobar endomorfizmov

M aditivna grupa

$\text{End}(M) := \{f: M \rightarrow M \mid f \text{ endomorfizem}\}$ postane kolobar, če

$$(f + \psi)(v) = f(v) + \psi(v)$$

$$(f \cdot \psi)(v) = f(\psi(v))$$

$$(f \cdot \psi = f \circ \psi)$$

To je enostavno preveriti.

$$1 = \text{id}_M$$

Izrek: Vsak kolobar lahko vložimo v kolobar endomorfizmov (neke) aditivne grupe.

Č Podobno kot Cayleyev izrek za grupe.

Dokaz: K kolobar

$\text{End}(K) = \text{kolobar endomorfizmov}$

$$(K, +)$$

Definiramo $f: K \rightarrow \text{End}(K)$

$$f(a) = l_a,$$

kjer $l_a = ax$, $l_a \in \text{End}(K)$.

$$f(a+b) = l_{a+b} = l_a + l_b = f(a) + f(b)$$

$$\varphi(a \cdot b) = \varphi_{a \cdot b} = \varphi_a \circ \varphi_b = \varphi(a) \cdot \varphi(b)$$

$$\varphi(1) = \varphi_1 = \text{id}_K = 1$$

Jedr φ : $\varphi(a) = 0 \Rightarrow \varphi_a = 0 \Rightarrow \varphi_a(1) = 0 \Rightarrow a = 0$
 \Rightarrow imamo vložitev □

Podobno:

Izrek: Vsako algebro $\xrightarrow{\text{nad } V}$ lahko vložimo v algebro endomorfizmov $\text{End}_F(V)$ (za neki v. pr. V).

Posledica: Vsako končno razsežno algebro lahko vložimo v $\text{End}_F(V) \cong M_n(F)$, kjer je V n-dim. vektorski prostor nad F .

Primer: Naj bo A n-razsežna realna algebra. Ali obstajata takšna $s, t \in A$, da je $st - ts = 1$.

Po posledici: Ali obstaja $S, T \in M_n(\mathbb{R})$:

$$ST - TS = I ?$$

$$0 = \text{tr}(ST - TS) \neq \text{tr}(I) = n.$$

2.2. Definicija modula

Definicija: Naj bo K kolobar. Množica M skupaj z binarno operacijo seštevanja $+$ in zunanjim binarnim operacijom $K \times M \rightarrow M$, $(a, u) \mapsto au$ (modulsko množenje ali včasih skalarno množenje), se imenuje modul nad K ali K -modul, če

- $(M, +)$ je Abelova grupa,
- $\forall a \in K, \forall u, v \in M. \quad a(u+v) = au+av,$
- $\forall a, b \in K. \forall u \in M. \quad (a+b)u = au+bu.$
- $\forall a, b \in K. \forall u \in M. \quad (ab)u = a(bu),$
- $\forall u \in M. \quad 1u = u.$

Opomba: Če je M K -modul, je $\varphi: K \rightarrow \text{End}(M)$,

$$\varphi(a)(u) = au.$$

homomorfizem kolobarjev.

Obratno, če je $\varphi: K \rightarrow \text{End}(M)$ homomorfizem kolobarjev, postane M K -modul, če vpeljemo $au := \varphi(a)(u)$.

Primeri:

1) Vektorski prostor nad poljem F je F -modul.
(vektorski prostor \equiv modul nad poljem)

\Rightarrow Modul je posplošitev vektorskega prostora

2) Vsaka Abelova (aditivna) grupa je \mathbb{Z} -modul.

$$n\alpha = \underbrace{\alpha + \dots + \alpha}_{n\text{-krat}}$$

$$(-n)\alpha = \underbrace{-\alpha - \dots - \alpha}_{n\text{-krat}}$$

$$0 \cdot \alpha = 0$$

Obratno: \mathbb{Z} -modul je aditivna grupa.

3) Vsak kolobar K je K -modul, če za modulsko množenje vzamemo običajno množenje (v kolobarju).

4) Če je I levi ideal K , ga lahko obravnavamo kot $\overset{\uparrow}{K}$ -modul.

$$\underset{(levi)}{a \cdot u} \underset{\overset{\uparrow}{K}}{\in I}$$

5) Če je K' "večji" kolobar K , je K' K -modul.

$$\underset{K'}{\overset{\uparrow}{a u}} \in K'.$$

6) $K = M_n(F)$, $M = F^n$: M je K -modul za običajno množenje matrike s stolpcem.

Opomba: Definirali smo levi modul.

Desni modul: $\underset{\overset{\uparrow}{M}}{u \cdot a} \in M$

$$(u+v)a = ua + va, \text{ ostali aksiomi analogni}$$

Zakaj razlikujem? Levi ideal \rightsquigarrow Levi modul.

Če je K komutativen, vsak levi K -modul postane desni K -modul, če definiramo $ua := au$.

2.3. Osnovni pojmi teorije modulov

Podmoduli

Podmnožica N K -modula M se imenuje podmodul, če je za isti operaciji tudi sama K -modul.

Ekvivalentno: Za vse $a, b \in K$ in $u, v \in N$, je $au + bv \in N$.

Ekvivalentno:

- $\forall u, v \in N. u + v \in N$.
- $\forall a \in K. \forall u \in N. au \in N$.

Primeri:

1) Če je K polje, je podmodul = podprostор.

2) Če je $K = \mathbb{Z}$, je podmodul = podgrupa.

3) Podmoduli K -modula K so levi ideali.

Če sta N_1 in N_2 podmoduli, sta podmoduli tudi $N_1 + N_2 = \{v_1 + v_2 \mid v_i \in N_i\}$ in $N_1 \cap N_2$.

Vedno: $\{0\}$ in M sta podmoduli M .

Modul $M \neq \{0\}$, ki nima drugih podmodulov razen $\{0\}$ in M , se imenuje enostavni modul.

Primeri:

- 1) Če je $K = F$: enostavnii moduli so 1-razsežni prostori.
- 2) Če je $K = \mathbb{Z}$: \mathbb{Z}_p , p praštevilo.
- 3) $K = M_n(F)$ in $M = F^n$.

Naj bo $N \neq \{0\}$ podmodul M . Naj bo $x \in N$.

$$\forall y \in M. \exists A \in K. Ax = y \quad (\Rightarrow \text{ni pravega podmodula})$$

$\Rightarrow M$ je enostaven K -modul.

Homomorfizmi modulov

Naj bosta M in M' K -moduli. Preslikava $f: M \rightarrow M'$ je homomorfizem (modulov), če

- $f(u+v) = f(u) + f(v)$,
- $f(au) = a f(u)$.

Ekvivalentno: $f(au+bv) = af(u) + bf(v)$

Homomorfizmom modulov rečemo tudi linearne (K -linearne) preslikave.

Oznaka $M \cong M'$ pomeni, da sta M in M' izomorfna (\exists obstaja izomorfizem iz $M \rightarrow M'$).

Velja: $\circ f: M \rightarrow M'$ izomorfizem $\Rightarrow f^{-1}$ izomorfizem

• Kompozitum (produkt) homomorfizmov je homomorfizem.

Jedro: $\ker \varphi := \{ u \in M \mid \varphi(u) = 0 \}$

Slika: $\text{Im } \varphi := \varphi(M)$

Jedro in slika sta podmoduli.

Primeri:

1) K polje: "običajne" linearne preslikave

2) $K = \mathbb{Z}$: aditivne preslikave, torej homomorfizmi
aditivnih grup

3) $I^{(=n)}$ levi ideal K .

$c \in I$. $\varphi: I \rightarrow I$

$$\varphi(u) := uc \in I$$

$$\varphi(u+v) = \varphi(u) + \varphi(v)$$

$$\varphi(au) = (au)c = a(uc) = a\varphi(u)$$

Kolobarji endomorfizmov in Schurova lema

Naj bo M K -modul.

$\text{End}_K(M) =$ množica vseh endomorfizmov M

je kolobar za običajno sestevanje in komponiranjem
kot množenje.

Primera: F polje: $\text{End}_F(M)$

- M aditivna grupa

$$\text{End}(M) = \text{End}_{\mathbb{Z}}(M)$$

$\varphi \in \text{End}_K(M)$ je bijektivna $\Leftrightarrow \varphi$ je automorfizem
 $\Leftrightarrow \varphi$ je obrnljiv element $\text{End}_K(M)$.

Lema [Schur]: Če je M enostaven modul, je $\text{End}_K(M)$ obseg.

Dokaz: $\varphi \in \text{End}_K(M)$

$\text{Ker } \varphi, \text{Im } \varphi$ sta podmodula

$\varphi \neq 0 \Rightarrow \text{Ker } \varphi = \{0\}, \text{Im } \varphi = M$
enostaven modul

$\Rightarrow \varphi$ bijektiven



13. november 2024

Kvocientni moduli

Naj bo N podmodul K -modula M . Potem

$$M/N := \{u+N \mid u \in M\}$$

postane K -modul, če vpeljemo

$$(u+N) + (v+N) = (u+v)+N$$

$$a(u+N) = au+N$$

Imenujemo ga kvocientni modul.

$$\pi: M \rightarrow M/N, \pi(u) = u+N$$

je epimorfizem modulov (kanonični epimorfizem).

Za vsak hom. modulov $\varphi: M \rightarrow M'$ je

$$M/\ker \varphi \cong \text{Im } \varphi.$$

Primer: 1) $K = F$: kvoc. modul = kvoc. prostor

2) $K = \mathbb{Z}$: kvoc. modul = kvoc. grupa

3) Podmodul K -modula K je levi ideal I .

$$K/I = \{a \in I \mid a \in K\}$$

je aditivna grupa K/I z modulsko operacijo

$$a(b+I) = ab + I.$$

Direktne vsote modulov

Naj bodo N_1, \dots, N_s K -moduli. Potem $N_1 \times \dots \times N_s$ postane K -modul, če definiramo

$$(u_1, \dots, u_s) + (v_1, \dots, v_s) := (u_1 + v_1, \dots, u_s + v_s)$$

$$a(u_1, \dots, u_s) := (au_1, \dots, au_s).$$

Imenujemo ga zunanja direktna vsota modulov N_1, \dots, N_s ; oznaka: $N_1 \oplus \dots \oplus N_s$.

Primer: 1) $K = F$: direktna vsota vektorskih prostorov

2) $K = \mathbb{Z}$: direktna vsota aditivnih grup

3) K -modul K : $K^s := \underbrace{K \oplus \dots \oplus K}_{s\text{-krat}}$

Naj bodo N_1, \dots, N_s podmoduli K -modula M . Če velja

$$(a) M = N_1 + \dots + N_s = \{n_1 + \dots + n_s \mid n_i \in N_i\} \text{ in}$$

$$(b) N_i \cap (N_1 + \dots + N_{i-1} + N_{i+1} + \dots + N_s) = \{0\} \text{ za } i \in \{1, \dots, s\},$$

potem je M notranja direktna vsota podmodulov N_1, \dots, N_s .

Če je M notranja direktna vsota N_1, \dots, N_s , je

$$M \cong N_1 \oplus \dots \oplus N_s$$

\uparrow zunanjja direktna vsota

Izomorfizem:

$$\underbrace{N_1 + \dots + N_s}_{\text{točka a}} \xrightarrow{T} (N_1, \dots, N_s)$$

(b) \Rightarrow zapis angleščih \Rightarrow dobra definiranost

Tudi notranja direktna vsota zato označujemo z $N_1 \oplus \dots \oplus N_s$.

Definicija: Podmodul N modula M je **direktni sumand**, če obstaja tak podmodul N' , da je $M = N \oplus N'$.

$$(M = N + N' \text{ in } N \cap N' = \{0\})$$

Primer: 1) $K = F$: vsi podprostori so direktni sumandi
(posledams baze)

2) $K = \mathbb{Z}$: \mathbb{Z} -modul \mathbb{Z} nima pravih netrivialnih direktnih sumandov
(\mathbb{Z}_n včasih imata)

3) K kom. kuhbar. Izkuže se (dokaz v knjigi):

I podmodul K je direktni sumand $\Leftrightarrow I = eK$, $e = e^2$.

Generatorji modulov

Za vsak $u \in M$, kjer je M K -modul, je

$$Ku = \{au \mid a \in K\}$$

podmodul (generiran z u). Rečemo mu **ciklični podmodul**, generiran z u .

M je **ciklični modul**, če obstaja $u \in M$, da je $M = Ku$.

Velja: enostaven \Rightarrow cikličen. Obrat ne velja.

- Primeri:
- 1) $K = F$: cikl. podmodul = 1-razsežni podprostori ali $\{0\}$
 - 2) $K = \mathbb{Z}$: ciklični podmodul = ciklična podgrupa $(\mathbb{Z}, \mathbb{Z}_n)$.
 - 3) K komutativen kolobar: ciklični podmodul = glavni ideal
 - 4) I levi ideal K , K/I (kvocientni modul) je cikličen, saj je generiran $\in 1+I$

Naj bo M modul in $a \in M$. Definirajmo

$$\text{anihilator } \text{ann}_K(u) := \{a \in K \mid a \cdot u = 0\}.$$

To je levi ideal: $x \in K, a \in \text{ann}_K(u) \Rightarrow (xa)u = x(\underbrace{au})_u = 0$.

Lema: Za vsak $u \in M$ (kjer je M K -modul) je $Ku \cong K / \text{ann}_K(u)$.

Dokaz: $\varphi: K \rightarrow Ku$, $\varphi(a) = a \cdot u$ je epimorfizem modulov s $\ker \varphi = \text{ann}_K(u)$. Velja izrek o izomorfizmu. \blacksquare

Naj bo $X \subseteq M$ množica. Podmodul generiran $\in X$, je množica vseh vsot elementov oblike au , $a \in K$, $u \in X$.

$$a_1u_1 + \dots + a_nu_n, \quad a_i \in K, u_i \in X, n \in \mathbb{N}$$

Če je M končno generiran - tj. generiran je s končno podmnožico $\{u_1, \dots, u_n\}$ - je $M = Ku_1 + \dots + Ku_n$.

2.4. Baze modulov in prosti moduli

Definicija: Podmnožica B K -modula M je linearno neodvisna, če za vse različne elemente $e_1, \dots, e_s \in B$ in vse $a_1, \dots, a_s \in K$ velja:

$$a_1e_1 + \dots + a_se_s = 0 \Rightarrow \forall i. a_i = 0$$

Če je B linearno neodvisna in generira modul M , ji rečemo **baza** M .

Če je B baza, potem za vsak element $u \in M$ obstajajo takih elementov $e_1, \dots, e_s \in B$, da je

$$u = a_1 e_1 + \dots + a_s e_s$$

za neke (enolično določene) $a_i \in K$.

Poenostavljeno: $u = \sum_i a_i e_i$, $B = \{e_i\}_i$

Tu moramo razumeti, da je le končna množica a_i -jev lahko različnih od 0.

Primer: Končna (netrivialna) aditivna grupa nima baze, saj nima nepraznih linearnih neodvisnih podmnožic :

$$n \neq 0 \not\Rightarrow n = 0$$

(saj ima v končni grupi vsak element končen red).

Definicija: Modul, ki ima bazo, se imenuje prosti modul.

Primer: 1) K kolobar, $K^S = K \oplus \dots \oplus K$ je prost K -modul z bazo $\{(1, 0, \dots, 0), (0, 1, 0, \dots, 0), \dots, (0, \dots, 0, 1)\}$.

Če je M prost K -modul z bazo $\{e_1, \dots, e_s\}$, je $M \cong K^S$. ($a_1 e_1 + \dots + a_s e_s \mapsto (a_1, \dots, a_s)$)

2) K kolobar. $K[X]$ je K -modul in $\{1, X, X^2, \dots\}$ je baza. Torej je $K[X]$ prost K -modul.

Definicija: Prostemu \mathbb{Z} -modulu pravimo prosta Abelska grupa. (+ to ni isto kot prosta grupa)

Primer: \mathbb{Z}^S

Opozbe:

1) Podmodul prostega modula ni nujno prost.

Primer: $K = \mathbb{Z}_4$ je prost K -modul. Njegov podmodul $2\mathbb{Z}_4 = \{0, 2\}$ ni prost.

2) M prost in N podmodul $\Rightarrow M/N$ ni nujno prost.

Primer: $M = \mathbb{Z}$ (kot \mathbb{Z} -modul), $N = n\mathbb{Z}$ (tudi prost)
 $M/N = \mathbb{Z}_n$ ni prost \mathbb{Z} -modul.

3) Če ima prost modul bazo z n elementi, ni nujno res, da je vsaka linearne neodvisna podmnožica z n elementi tudi baza.

Primer: $\mathbb{Z}:$ Baza: • $\{1\}$ ali $\{-1\}$
• $\{2\}$ ni baza

4) Obstajači takši kolobarji K (nujno nekomutativni), da je $K^s \cong K^t$, $s \neq t$.

20. november 2024

Naj bo B poljubna množica, K kolobar

Npr. $B = \{e_1, \dots, e_s\}$

K -modul M nuj sestavlja formalne lin. komb.
 $a_1e_1 + \dots + a_se_s$, $a_i \in K$

Seštevanje in modulsko množenje vpeljemo na samoumeven način tako, da bo B baza.

Če je B poljubna, M sestoji iz formalnih vsot $\sum_{e \in B} a_e e$, pri čemer je le končno mnogo $a_e \neq 0$.

$\Rightarrow M$ je prosti modul z bazo B

Izrek: Za vsako množico B in kolobar K obstaja prosti K -modul z bazo B .

Izrek: Naj bo M prosti K -modul z bazo B in N poljuben K -modul. Vsako preslikavo $f: B \rightarrow N$ lahko enolično razširimo do homomorfizma $\ell: M \rightarrow N$.

Dokaz: Za vsak element iz $M: a_1e_1 + \dots + a_s e_s$ definiramo $\ell(a_1e_1 + \dots + a_s e_s) = a_1f(e_1) + \dots + a_s f(e_s)$.

ℓ je homomorfizem, ki se na bazi B ujemata z f . Homomorfizma, ki je ujemata na bazi sta enaka, torej je ℓ enolično določen.

Posledica: Vsak K -modul je homomorfna slika prostega K -modula.

Dokaz: Naj bo N K -modul in B množica generatorjev N . Naj bo M prosti K -modul z bazo B in naj bo $f: M \rightarrow N$ homomorfizem: $f(e) = e$. Im f vsebuje vsi $e \in B$, ti elementi pa generirajo N .

Definicija: Modul nad obsegom D se imenuje vektorski prostor nad D . (balj natančno: (levi) v.p.)

Primer: $\mathbb{H}^S = \mathbb{H} \times \dots \times \mathbb{H}$ je vektorski prostor nad \mathbb{H} .

Izrek: Naj bo V vektorski prostor nad obsegom D . Za vsako linearно neodvisno podmnožico T prostora V obstaja baza B , ki T vsebuje.

Posledica: Vsak vektorski prostor nad obsegom D ima bazo.

Zornova lema: Če ima V neprazni delno urejeni množici S vsaka veriga zgornjo mejo, ima S maksimalni element.

Dokaz izreka: T linearно neodvisna množica

$S :=$ množica vseh linearne neodvisnih množic,
ki vsebujejo T

$T \in S \Rightarrow S \neq \emptyset$. Imamo delno urejenost S z inkluzijo.

Naj bo $\mathcal{V} \subseteq S$ veriga in \mathcal{Z} unija vseh elementov iz \mathcal{V} .

$\mathcal{Z} \in S$:

Naj bo $z_1, \dots, z_n \in \mathcal{Z}$. $z_1 \in A_1 \in \mathcal{V}, \dots, z_n \in A_n \in \mathcal{V}$

Ker je V veriga, obstaja množica A_i , npr. A_1 , ki vsebuje vse druge A_j . $z_1, \dots, z_n \in A_1$, A_1 lin. neodvisna

Zornova lema: obstaja maksimalni element B v S

B je baza:

B je lin. neodvisna, saj je $v \in S$. $T \subseteq B$.

$v \in V$. v je lin. kombinacija elementov iz B .

$B \subseteq S$ $v \notin B$. $B \cup \{v\}$ zaradi maksimalnosti B ni linearne neodvisna.

$\exists a_0, a_1, \dots, a_k : a_0 v + a_1 e_1 + \dots + a_s e_s = 0$ za neke $a_i \in K, e_i \in B$

$$a_0 \neq 0 \Rightarrow v = - (a_0^{-1} a_1) e_1 + \dots + (-a_0^{-1} a_s) e_s$$

Definicija: rang modula = kardinalnost baze

Torej: moduli nad obsegom so vedno prosti.

2.5. Eksaktна zaporedja

Definicija: Zaporedje modulskih homomorfizmov

$$M_0 \xrightarrow{\varphi_1} M_1 \xrightarrow{\varphi_2} \dots \xrightarrow{\varphi_k} M_k$$

je eksaktne, če je $\text{Im } \varphi_i = \text{Ker } \varphi_{i+1}$ za $i = 1, \dots, k$.

Primeri: (1) $\{0\} = 0 \longrightarrow L \xrightarrow{\varphi} M$ je eksaktne
 $\Leftrightarrow \varphi$ injektiven

(2) $M \xrightarrow{\varphi} N \longrightarrow 0$ je eksaktnej ($\Rightarrow \varphi$ surjektiven)

(3) $0 \longrightarrow L \xrightarrow{\varphi} M \longrightarrow 0$ je eksaktnej
 $\Leftrightarrow \varphi$ bijektiven

(4) Kratko eksaktne zaporedje (KEZ)

$$0 \longrightarrow L \xrightarrow{\varphi} M \xrightarrow{\gamma} N \longrightarrow 0$$

je eksaktnej $\Leftrightarrow \varphi$ inj., γ sur. in $\text{Im } \varphi = \text{Ker } \gamma$.
 $\hookrightarrow \gamma \circ \varphi = 0$

Primera: (1) Naj bo L podmodul M .

$$0 \longrightarrow L \xrightarrow{\text{id}_L} M \xrightarrow{\pi} M/L \longrightarrow 0$$

V splošnem: $\text{Im } \varphi = \varphi(L) = \text{Ker } \gamma$

$$N \cong M/\text{Im } \varphi$$

(2) L, N modula

$$0 \longrightarrow L \xrightarrow{i_L} L \oplus N \xrightarrow{\pi_N} N \longrightarrow 0$$

$\ell \mapsto (\ell, 0)$ projekcija

Definicija: KEZ $0 \longrightarrow L \xrightarrow{\varphi} M \xrightarrow{\gamma} N \longrightarrow 0$ je razpadno kratko eksaktne zaporedje, če obstaja tak izomorfizem $\sigma : M \longrightarrow L \oplus N$, da diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & L & \xrightarrow{\varphi} & M & \xrightarrow{\gamma} & N \longrightarrow 0 \\ & & \downarrow & & \downarrow \sigma & & \downarrow \\ 0 & \longrightarrow & L & \longrightarrow & L \oplus N & \longrightarrow & N \longrightarrow 0 \end{array}$$

komutira.

To pomeni: $\sigma \varphi = \text{id}_L$ in $\pi_N \sigma = \gamma$ ali

$$\sigma(\varphi(t)) = (t, v) \quad \forall t \in L \quad \text{in} \quad \gamma(\sigma^{-1}(t, v)) = v \quad \forall v \in N.$$

Primer: Vsako KEZ ni razpadno:

$$0 \longrightarrow \mathbb{Z} \xrightarrow{x \mapsto nx} \mathbb{Z} \longrightarrow \mathbb{Z}_n \longrightarrow 0.$$

\mathbb{Z} -modul \mathbb{Z} ni enak direktni vsoti dveh svojih podmodulov

Izrek: Za KEZ $0 \rightarrow L \xrightarrow{\varphi} M \xrightarrow{\pi} N \rightarrow 0$ so naslednje trditve ekvivalentne:

(i) Zaporedje je razpadno.

(ii) Obstaja tak homomorfizem $\varphi': M \rightarrow L$, da je $\varphi' \varphi = \text{id}_L$.

(iii) Obstaja tak homomorfizem $\pi': N \rightarrow M$, da je $\pi' \pi = \text{id}_N$.

Dokaz: (i) \Rightarrow (ii) in (iii): $\sigma: M \rightarrow N \oplus L$

$$\varphi := \pi_L \sigma \Rightarrow \varphi' \varphi = \text{id}_L$$

$$\pi' := \sigma^{-1} \iota_N \Rightarrow \pi' \pi = \text{id}_N$$

(ii) \Rightarrow (i): $\varphi': M \rightarrow L$, $\varphi' \varphi = \text{id}_L$

$$\sigma: M \rightarrow L \oplus N, \quad \sigma(u) = (\varphi'(u), \pi(u))$$

$$\sigma \varphi = \iota_L \checkmark \quad \pi_N \sigma = \pi \checkmark$$

• σ -inj: $u \in \ker \sigma \Rightarrow u \in \ker \varphi$ in $u \in \ker \pi = \text{Im } \varphi$

$$u = \varphi(t)$$

$$\varphi'(u) = 0 \Rightarrow \varphi'(\underbrace{\varphi(t)}_t) = 0 \Rightarrow t = 0 \Rightarrow u = 0$$

• σ -sur: $(t, v) \in L \oplus N$

$$(t, v) = \sigma(u): v = \pi(u_0) \text{ za neki } u_0 \in M$$

$$\nexists f = 0 \Rightarrow r = \tau(u_0 + f(k)) \quad \forall k \in L$$

$\tau'(u_0 + f(k)) = t$ Edina možna izbira:

$$f(u_0) + k = t \Rightarrow k = t - f(u_0)$$

(iii) \Rightarrow (i): Izpustimo.

□

2.6. Projektivni moduli

27. november 2024

$$\begin{array}{ccc} & \varphi \cdots & P \\ & \downarrow & \downarrow \varphi \\ M & \xrightarrow{\quad \tau \quad} & N \end{array}$$

Definicija: Modul P je projektivni modul, če za vsak homomorfizem $\varphi: P \rightarrow N$ in vsak epimorfizem $\tau: M \rightarrow N$ obstaja tak homomorfizem $\psi: P \rightarrow M$, da je $\varphi = \tau \psi$.

Lema: Vsak prosti modul je projektiven.

Dokaz: Naj bo P prosti modul z bazo B .

$$\begin{array}{ccc} & \varphi \cdots & P \\ & \downarrow & \downarrow \varphi \\ M & \xrightarrow{\quad \tau \quad} & N \end{array} \quad e \in B \Rightarrow \varphi(e) = \tau(m_e) \text{ za nek } m_e \in M$$

Ker je B baza obstaja tak $\psi: P \rightarrow M$, da $\psi(e) = m_e$. Očitno je $\varphi = \tau \psi$ (soj se ujemata na B).

Izrek: Za modul P so naslednje trditve ekvivalentne:

(i) P je projektiven

(ii) Vsake KEZ $O \rightarrow L \xrightarrow{f} M \xrightarrow{\pi} P \rightarrow O$ razpade.

(iii) Obstaja tak modul L , da je $P \oplus L$ prosti modul.

Dokaz: (i) \Rightarrow (ii):

$$\begin{array}{ccccc} & & P & & \\ & \swarrow \varphi & \downarrow id_P & & \\ M & \xrightarrow{\pi} & N & \longrightarrow & O \end{array} \quad \pi \circ \varphi = id_P$$

Izrek od zadnjic: to KEZ razpade.

(ii) \Rightarrow (iii): $O \rightarrow L \rightarrow M \rightarrow N \rightarrow O$ vedno razpade

Vemo: Obstaja prosti modul M : P je njegova hom. sliku
($f: M \rightarrow P$ epimorfizem)

$$L = \ker \pi : O \rightarrow L \xrightarrow{\iota} M \xrightarrow{\pi} P \rightarrow O$$

Ker razpade, je $M \cong P \oplus L$. M prost $\Rightarrow P \oplus L$ prost.

(iii) \Rightarrow (i):

$$\begin{array}{ccccc} & & P & & \\ & \swarrow \varphi & \downarrow \pi & & \\ M & \xrightarrow{\pi} & N & \longrightarrow & O \end{array}$$

$P \oplus L$ prost \Rightarrow proj.

$$\varphi := \Theta \iota_P$$

$$\pi \circ \varphi = \pi \circ \Theta \iota_P = f \circ \pi \circ \iota_P = f \circ id_P = f$$

$$\begin{array}{ccccc} & & P \oplus L & & \\ & \swarrow \Theta & \downarrow \pi_P & & \\ & \swarrow \varphi & \downarrow f & & \\ M & \xrightarrow{\pi} & N & \longrightarrow & O \end{array}$$

Primer: Naj komutativni kohbar vsebuje idempotent $e \neq 0, 1$. eK je K -modul in je direktni sumand prostega K -modula K , torej je projektiven.

Ni prost, ker nisena njegova neprazna podmnožica ni linearne neodvisna.

$$(1-e) \cdot ex = 0$$

K_1, K_2 hom.

$$K := K_1 \times K_2 \quad e = (1, 0)$$

$$\mathbb{Z}_6 \cong \mathbb{Z}_3 \times \mathbb{Z}_2$$

$K = D$ obseg : vsi moduli so prosti in zato projektivni.

Posledica: Vsaka KEZ vektorskih prostorov je razpadna.

2.7. Tenzorski produkt modulov nad komutativnim kolobarjem

Motivacija:

U, V vektorska prostora nad F

$$\dim U = n, \dim V = m$$

$$\dim U \otimes V = m \cdot n$$

$\{e_1, \dots, e_n\}$ baza U

$\{f_1, \dots, f_m\}$ baza V

$\{e_i \otimes f_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ baza $U \otimes V$

$\{e'_i \otimes f'_j\}$ tudi baza

Definicija: Naj bosta M in N K -modula, kjer je K komutativni kolobar.

Naj bo \tilde{F} prost modul $\not\cong$ bazo $M \times N$.

Tu $M \times N$ obravnavamo kot množico.

$$\underbrace{(0,0)}_{\text{elementa množice}}, \underbrace{(u+u', v)}_{\text{vsota dveh baznih elementov}}, \underbrace{(u, v) + (u', v')}_{(u, v) + (u', v')}$$

→ Modul \mathbb{F} ima torej zelo veliko bazo.

Modula M in N sta "bistveno manjša" od \mathbb{F} .

Z \mathcal{N} označimo podmodul \mathbb{F} generiran z elementi oblike $(au+a'u', v) = a(u, v) - a'(u', v')$
 $(u, av+a'v') = a(u, v) - a'(u, v')$

za vse $u \in M, v \in N, a, a' \in K$.

Definicija: Naj bosta M in N K -modula. Kvocientni modul \mathbb{F}/\mathcal{N} imenujemo **tenzorski produkt** M in N in označujemo $M \otimes N$ ozziroma $M \otimes_K N$.

Definicija: Preslikava $\Phi: M \times N \rightarrow L$ je bilinearna, če $\Phi(au+a'u', v) = a\Phi(u, v) + a'\Phi(u', v)$ in $\Phi(u, av+a'v') = a\Phi(u, v) + a'\Phi(u, v')$.

Primeri: (1) Skalarni produkt: $\mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}$

(2) Vektorski produkt: $\mathbb{R}^3 \times \mathbb{R}^3 \rightarrow \mathbb{R}^3$

(3) V vsaki algebri je $(a, b) \mapsto ab$ bilinearna preslikava.

(4) Množenje matrik.

(5) $(z, w) \mapsto \bar{z}w$ je \mathbb{R} -bilinearna

Izrek [univerzalna lastnost tenzorskega produkta]:
Naj bosta M in N K -modula. Potem obstaja bilinearna preslikava $\otimes : M \times N \rightarrow M \otimes N$, $(u, v) \mapsto u \otimes v$, ki ima naslednjo lastnost:

- Za vsako bilinearno preslikavo $\Phi : M \times N \rightarrow L$ obstaja enolično določena preslikava $\varphi : M \otimes N \rightarrow L$ z lastnostjo $\varphi(u \otimes v) = \Phi(u, v)$ za vse $u \in M$ in $v \in N$.

Z obstojem bilinearne preslikave s to lastnostjo, je $M \otimes N$ enolično določen.

Dokaz: $M \otimes N = \mathcal{F}/\mathcal{N}$

$$u \otimes v = (u, v) + \mathcal{N} \in M \otimes N$$

Bilinearnost \otimes sledi iz definicije \mathcal{N} .

Elementi v $M \otimes N$ so linearne kombinacije $(u, v) + \mathcal{N} = u \otimes v$

Vsi so torej vsote elementov $u \otimes v$. ($a(u \otimes v) = (au) \otimes v$)

$$\Phi : M \times N \rightarrow L$$

Vzemimo linearne preslikave $F : \mathcal{F} \rightarrow L$, $F((u, v)) = \Phi(u, v)$

Ker je F linear, ker F vsebuje vse generatorje modula \mathcal{N} .

Definiramo: $\varphi : M \otimes N \rightarrow L$, $\varphi(x + \mathcal{N}) = F(x) \quad \forall x \in \mathcal{F}$.

Dobra definiranost: $x + \mathcal{N} = y + \mathcal{N} \Rightarrow x - y \in \mathcal{N} \Rightarrow F(x - y) = 0 \Rightarrow F(x) = F(y)$

φ je linear, saj je F linear

$$\varphi(u \otimes v) = \varphi(u, v) + \mathcal{N} = F(u, v) - \Phi(u, v)$$

Ker je vsak element vsota elementov $u \otimes v$,
je p enolično določena.

Naj bo T modul, ki ima enako (univerzalno) lastnost:

$$\odot: M \times N \rightarrow T \text{ bilinearna}$$

$$T \cong M \otimes N$$

Zaradi univerzalne lastnosti obstaja

$$\varphi: T \rightarrow M \otimes N. \quad \varphi(u \otimes v) = u \otimes v \text{ in podobno}$$

$$\psi: M \otimes N \rightarrow T. \quad \psi(u \otimes v) = u \otimes v$$

$$(\psi \varphi)(u \otimes v) = u \otimes v \stackrel{\text{enol.}}{\Rightarrow} \psi \varphi = \text{id}_T$$

$$\text{Podobno } \varphi \psi = \text{id}_{M \otimes N}.$$

□

Povzetek:

(1) $M \otimes N$ je K -modul z elementi oblike

$$u_1 \otimes v_1 + \dots + u_m \otimes v_m$$

$u \otimes v \dots$ enostavni tenzor

$$(u+u') \otimes v = u \otimes v + u' \otimes v$$

$$a(u \otimes v) = (au) \otimes v = u \otimes (av)$$

$$u \otimes (v+v') = u \otimes v + u \otimes v'$$

$$(2) \quad M \times N \xrightarrow{\odot} M \otimes N$$

$$\underline{\text{Opomba}}: u = \sum a_i u_i, \quad v = \sum b_j v_j$$

$$u \otimes v = \sum (a_i b_j) u_i \otimes v_j$$

$$\varphi(u \otimes v) = \bar{\varphi}(u, v)$$

$$\varphi(\sum \lambda_i u_i \otimes v_i) = \sum \lambda_i \bar{\varphi}(u_i, v_i)$$

$$\begin{array}{l} \varphi: M \rightarrow M' \\ \psi: N \rightarrow N' \end{array} \left. \begin{array}{c} \\ \end{array} \right\} \text{linearni}$$

$(u, v) \mapsto \varphi(u) \otimes \psi(v)$ je bilin., zato obstaja lin. pres.

$$\varphi \otimes \psi: M \otimes N \rightarrow M' \otimes N'$$

$$(\varphi \otimes \psi)(u \otimes v) = \varphi(u) \otimes \psi(v)$$

tenzorski produkt φ in ψ

$$\underline{\text{Lastnosti}}: (\varphi + \varphi') \otimes \psi = \varphi \otimes \psi + \varphi' \otimes \psi$$

$$\varphi \otimes (\psi + \psi') = \varphi \otimes \psi + \varphi \otimes \psi'$$

$$a(\varphi \otimes \psi) = a\varphi \otimes \psi = \varphi \otimes a\psi$$

$$(\varphi \otimes \psi)(\varphi' \otimes \psi') = \varphi \varphi' \otimes \psi \psi'$$

$$\varphi, \psi \text{ izom.} \Rightarrow \varphi \otimes \psi \text{ izom.}$$

4. december 2024

Izrek: Naj bodo M, N, R K -moduli. Potem velja

$$(a) M \otimes N \cong N \otimes M$$

$$(b) (M \otimes N) \otimes R \cong M \otimes (N \otimes R)$$

$$(c) (M \otimes N) \otimes R \cong (M \otimes R) \otimes (N \otimes R) \quad (c') R \otimes (M \otimes N) \cong (R \otimes M) \otimes (R \otimes N)$$

$$(d) M \otimes K \cong M$$

$$(d') K \otimes M \cong M$$

Dokaz: (a): $\varphi: M \otimes N \rightarrow N \otimes M$

$$\varphi(u \otimes v) = v \otimes u$$

je linearne, saj je $(u, v) \mapsto v \otimes u$ bilinearne

$$\psi: N \otimes M \rightarrow M \otimes N$$

$$v \otimes u \mapsto u \otimes v$$

$$\Rightarrow \varphi \psi = id_{N \otimes M}, \quad \psi \varphi = id_{M \otimes N}$$

$\Rightarrow \varphi$ je izomorfizem, saj smo našli inverz

(b) $\varphi: (M \otimes N) \otimes R \rightarrow M \otimes (N \otimes R)$

$$\sum x_i \otimes w_i$$

$$\sum (u_{ij} \otimes v_{ij}) \otimes w_i$$

$$(u \otimes v) \otimes w \mapsto u \otimes (v \otimes w)$$

(c) $u \otimes a = au \otimes 1$

$$u \otimes a \xrightarrow{\varphi} au$$

$$u \xrightarrow{\quad} u \otimes 1$$

Oznaka: $M^{\otimes n} = \underbrace{M \otimes \dots \otimes M}_{n\text{-krat}}$

Primer: m, n tiji

$\mathbb{Z}_m, \mathbb{Z}_n \mathbb{Z}$ -modula

$$\mathbb{Z}_m \otimes_{\mathbb{Z}} \mathbb{Z}$$

$$rm + sn = 1 \quad \text{za neka } r, s \in \mathbb{Z}$$

$$\begin{aligned} u \otimes v &= 1u \otimes v = (rm + sn)u \otimes v \\ &= r(mu) \otimes v + s(u \otimes nv) \end{aligned}$$

$$= 0$$

$$0 \otimes v = (0+0) \otimes v = 0 \otimes v + 0 \otimes v = 0$$

$$\Rightarrow \mathbb{Z}_m \otimes_{\mathbb{Z}} \mathbb{Z}_n = \{0\}$$

Izrek: Naj bo M prost in N poljuben K -modul.
 Če je $\{e_i | i \in I\}$ baza M , potem lahko vsak element iz $M \otimes N$ na en sam način zapišem kot $\sum_{i \in I} e_i \otimes v_i$, $v_i \in N$.

Dokaz: $u \in M$, $v \in N$

$$u \otimes v = (\sum a_i e_i) \otimes v = \sum e_i \otimes a_i v$$

$$(se prenese na \sum_{i \in I} u_i \otimes v_i)$$

Enoličnost: zadostca $\sum_{i \in I} e_i \otimes v_i = 0 \Rightarrow v_i = 0 \quad \forall i$
 $(\sum_{i \in I} e_i \otimes v_i = \sum_{i \in I} e_i \otimes w_i \Rightarrow \sum_{i \in I} e_i \otimes (v_i - w_i) = 0)$

$$\sum e_i \otimes v_i = 0$$

$$i_0 \in I. \quad v_{i_0} = 0.$$

Definiramo linearno preslikavo $\varphi: M \rightarrow K$

$$\varphi(e_i) = 0, \quad i \neq i_0$$

$$\varphi(e_{i_0}) = 1$$

$$\exists \psi: M \otimes N \rightarrow N$$

$$\psi(u \otimes v) = \varphi(u)v$$

$$M \times N \rightarrow N$$

$$(u, v) \mapsto \underbrace{\varphi(u)}_K v$$

$$\psi\left(\sum_{i \in I} e_i \otimes v_i\right) = \psi(0) = 0$$

$$\sum_{i \in I} \psi(e_i \otimes v_i) = \sum \varphi(e_i) v_i = v_{i_0}$$



Pomembno: Enak izrek velja, če je N prost. $\sum u_j \otimes f_j$

Izrek: Naj bosta M in N prosta k -modula. Potem je tudi $M \otimes N$ prost. Še več, če je $\{e_i \mid i \in I\}$ baza M in $\{f_j \mid j \in J\}$ baza N , je $\{(e_i \otimes f_j) \mid i \in I, j \in J\}$ baza $M \otimes N$.

Dokaz: Vzemimo $u \otimes v \in M \otimes N$.

$$u = \sum_{i \in I} a_i e_i, \quad v = \sum_{j \in J} b_j f_j$$

$$u \otimes v = \sum_{i,j} (a_i b_j) e_i \otimes f_j$$

• linearna neodvisnost:

$$\sum_{i,j} \underset{k}{\underset{\uparrow}{a_{i,j}}} e_i \otimes f_j = 0$$

$$\sum_i a_i \otimes \left(\sum_j a_{ij} f_j \right) = 0 \quad \{f_j \mid j \in J\} \text{ baza}$$

$$\Rightarrow \sum_j a_{ij} f_j = 0 \quad \stackrel{\downarrow}{\Rightarrow} a_{ij} = 0 \quad \blacksquare$$

Posledica: Vektorski prostori so prosti moduli, zato:
Naj bosta U in V vektorska prostora nad F , $\dim U = m$, $\dim V = n$. Potem je $\dim U \otimes V = mn$.

Opomba: $\dim V < \infty$

$$V \otimes V^* \cong \text{End}_F(V)$$

$$(u \otimes f)v = f(v)u$$

2.8. Tenzorski produkt algeber

4. december 2024

Definicija: Algebra nad komutativnim kolobarjem (ali K -algebra) je definirana enako kot algebra nad poljem:

- kolobar
- K -modul
- $a(xy) = (ax)y = x(ay)$

Primeri: (1) Vsak kolobar je \mathbb{Z} -algebra.

(2) Če je komutativen kolobar in K podkolobar
če lahko obravnavamo kot algebro nad K

(3) $\text{End}_K(M)$, M K -modul

$$(a \cdot f)(u) = a f(u)$$

Izrek: Naj bosta A in B K -algebri. Potem K -modul $A \otimes B$ postane algebra, če definiramo $(u \otimes v)(z \otimes w) = u z \otimes v w$.

Opomba: Izrek pove, da je $(\sum_i u_i \otimes v_i)(\sum_j z_j \otimes w_j) = \sum_{i,j} u_i z_j \otimes v_i w_j$ dobro definirano (modulsko) množenje.

Dokaz: $f_z(x) = xz$. f_z je linearne preslikave iz algebre vase
za $z \in A$ in $w \in B$: $f_z \otimes f_w : A \otimes B \rightarrow A \otimes B$

$$f_z \otimes f_w \in \text{End}_K(A \otimes B)$$

$$A \times B \longrightarrow \text{End}_K(A \otimes B)$$

$(z, w) \longmapsto f_z \otimes f_w$ je bilinearna

$$\Rightarrow \exists \text{ lin. } \varphi : A \otimes B \rightarrow \text{End}_K(A \otimes B)$$

$$\varphi(z \times w) = \varphi_z \oplus \varphi_w$$

Za $r, s \in A \otimes B$ definiramo $r \cdot s = \varphi(s)(r)$.

Posebni primer: $r = u \otimes v$, $s = z \otimes w$

$$(u \otimes v)(z \otimes w) - \varphi(z \otimes w)(u \otimes v) = (\varphi_z \otimes \varphi_w)(u \otimes v) = uz \otimes vw. \quad \square$$

Izrek: A, B, C K -algebре

$$(a) A \otimes B \cong B \otimes A$$

$$(b) (A \otimes B) \otimes C \cong A \otimes (B \otimes C)$$

$$(c) (A \times B) \otimes C \cong (A \otimes C) \times (B \otimes C)$$

$$(d) A \otimes K \cong A$$

Dokaz: Kot prej.

Primer 1: $K[x]$ je K -algebra (ne le kolobar)

$$a(a_0 + a_1x + \dots + a_nx^n) = aa_0 + (aa_1)x + \dots + (aa_n)x^n$$

Kot K -modul je $K[x]$ prost z bazo $\{1, x, x^2, \dots\}$

A K -algebra

$$A \otimes K[x] \cong A[x]$$

Kot vemo lahko vsak element v $A \otimes K[x]$ pišemo kot

$$\sum_i a_i \otimes x^i \text{ in to na en sam način.}$$

$\sum_i a_i \otimes x^i \mapsto \sum_i a_i x^i$ je izomorfizem algeber

$$(a \otimes x^i)(b \otimes x^j) \mapsto ab x^{i+j}$$

$$\begin{matrix} \downarrow \\ ax^i \end{matrix}$$

$$\begin{matrix} \downarrow \\ bx^i \end{matrix}$$

$$K[y] \otimes K[x] \cong K[y][x] = K[x,y]$$

$$(K[x])^{\otimes n} \cong K[x_1, \dots, x_n]$$

$$f(x) \otimes g(y) \mapsto f(x)g(y)$$

$$(f \otimes g)(x,y) = f(x)g(y)$$

11. december 2024

Primer 2: A algebra nad K

$$\text{Trdimo: } M_n(K) \otimes A \cong M_n(A)$$

E_{ij} matrične enote

Vsak element v $M_n(K)$ lahko torej enolično zapisemo kot:

$$\sum_{i,j=1}^n E_{ij} \otimes u_{ij}$$

Izomorfizem iz $M_n(K) \otimes A$ v $M_n(A)$ je:

$$\sum_{i,j=1}^n E_{ij} \otimes u_{ij} \mapsto [u_{ij}]_{i,j}$$

$$\text{Npr. } A = M_n(K)$$

$$M_m(K) \otimes M_n(K) \cong M_m(M_n(K))$$

$$M_m(M_n(K)) \cong M_{mn}(K)$$

$$S \otimes T = \sum_{i,j} s_{ij} E_{ij} \otimes T = \sum_{i,j} E_{ij} \otimes s_{ij} T \mapsto \begin{bmatrix} s_{11}T & \dots & s_{1m}T \\ \vdots & & \vdots \\ s_{m1}T & \dots & s_{mm}T \end{bmatrix}$$

Primer 3: A naj bo realna algebra, $\dim A = n$

$\{e_1, \dots, e_n\}$ baza A

$$e_i \cdot e_j = \sum_{k=1}^n d_{ijk} e_k$$

A_C naj bo \mathbb{C} -prostor z bazo $\{e_1, \dots, e_n\}$, ki postane algebra z isto multiplikativno tabelo

$$A = M_n(\mathbb{R}) \Rightarrow A_C \cong M_n(\mathbb{C})$$

$$A = \mathbb{H} \Rightarrow \mathbb{H}_C \cong M_n(\mathbb{C})$$

Primer 4: K komutativen kolobar, A K -algebra
 C komutativen kolobar, ki vsebuje K kot podkolobar

$$A_C := C \underset{\substack{\hookrightarrow \\ K\text{-algebra}}}{\otimes_K} A$$

Ta K -algebra postane C -algebra z

$$c \cdot y = (c \otimes 1)y \quad \forall c \in C, \forall y \in A_C$$

$$c(d \otimes a) = cd \otimes a$$

Če je $\{e_i \mid i \in I\}$ baza A , je $\{1 \otimes e_i \mid i \in I\}$ baza A_C .

$$\sum c_i \otimes e_i = \sum c_i (1 \otimes e_i)$$

\hookrightarrow vsak element enškriv zapišemo tako

$$1 \otimes e_i \cdot 1 \otimes e_j = \sum_{k=1}^n d_{ijk} 1 \otimes e_k$$

C, K polji: A_C = algebra, dobiljena z razširitvijo skalarjev
razširitev skalarjev

2.9. Končno generirane Abelove grupe

$$\mathbb{Z}^s \cong \mathbb{Z}^t \Rightarrow s = t$$

$\underbrace{\mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_s$

Naj bo M K -modul. $I \triangleleft K$. $IM = \{0\}$ ($\overset{I \subseteq M}{\text{UW=0}}$)

Potem M postane K/I -modul $\ni (x+I)m := xm$. (*)

Lema: Naj bo $K \neq \{0\}$ komutativen kolobar. Če je $K^s \cong K^t$, potem je $s = t$.

Dokaz: Naj bo I maksimalni ideal K . K/I je polje.

Za vsak $n \in \mathbb{N}$ definiramo:

$$M_n := K/I \otimes_K K^n$$

\uparrow K modul $a(b+I) = ab + I$

$$IM_n = \{0\}$$

$$u((a+I) \otimes m) = \overbrace{u(a+I)}^{ua+I=0} \otimes m = 0$$

Zato M_n postane K/I -modul \ni (*); pravzaprav vek. prostor.

$\varphi: K^s \rightarrow K^t$ izomorfizem K -modulov

$\Phi = \text{id}_{K/I} \otimes \varphi$ je izomorfizem K -modulov iz M_s v M_t .

Dejansko je Φ K/I -linearna preslikava.

M_s je s -dimensionalen vek. pr. nad K/I
 M_t je t -dim. vek. pr. nad K/I

$$\left. \begin{array}{c} \text{lin. alg.} \\ \hline \end{array} \right\} \Leftrightarrow s = t$$

Definicija: $(G, +)$ je torzijsko prosta, če imajo vsi od 0 različni elementi neskončen red.

$$na = 0 \Rightarrow a = 0$$

Lema: Končno generirana torzijsko prosta Abelova grupa H je prosta Abelova grupa.

Dokaz: Denimo, da to ni res. Nobena množica, ki jo generira, ni linearno neodvisna.

Naj bo, $m \in \mathbb{N}$: H naj ima množico generatorjev z m elementi, ne pa manj kot m .

Izmed vseh množic, ki generirajo H , izberemo $\{h_1, \dots, h_m\}$: $a_1h_1 + \dots + a_mh_m = 0$ in $\sum_{i=1}^m |a_i|$ najmanjša. k_1, \dots, k_m : $b_1k_1 + \dots + b_mk_m = 0$: $\sum |a_i| \leq \sum |b_j|$

$h_i \neq 0 \Rightarrow a_i h_i \neq 0$, če $a_i \neq 0$

Vsa j dva a_i sta neničelna.

BSS $|a_1| \geq |a_2| > 0$ in $a_2 > 0$

$$a_1 = q a_2 + r, \quad r = a_1 - q a_2 \in \{0, \dots, a_2 - 1\}$$

$$(a_1 - q a_2)h_1 + a_2(h_2 + q h_1) + a_3h_3 + \dots + a_mh_m = 0$$

$\{h_1, h_2 + q h_1, h_3, \dots, h_m\}$ generira H

$$|a_1 - q a_2| < |a_2| \leq |a_1| \quad \times$$



$(G, +)$. $T =$ množica elementov v G s končnim redom

T je podgrupa: $nu = 0$, $mb = 0 \Rightarrow mn(a-b) = 0$

T je torzijska podgrupa

G/T je torzijsko-prosta.

$$m(a+I) = 0 \Rightarrow na \in T \Rightarrow m(na) = 0 \Rightarrow a \in T$$

Izrek: Naj bo G končna generirana Abelova grupa. Potem je njena torzijska podgrupa T končna in obstaja tako enolično določeno število $s \geq 0$, da je $G \cong \mathbb{Z}^s \oplus T$.

Dokaz: G/T je torzijsko prosta, zato prostu in $G/T \cong \mathbb{Z}^s$ za nek enolično določen s .

$$0 \rightarrow T \longrightarrow G \longrightarrow G/T \rightarrow 0$$

G/T je prosta grupa, zato projektivna in zaporedje razpade, torej $G \cong G/T \oplus T$

$T \cong ((G/T) \oplus T) / (G/T) \Rightarrow T$ končno generirana
 L končno generiranu

t_1, \dots, t_m generatorji

Vsak element iz T je oblike $m_1t_1 + \dots + m_mt_m$.

Vsak t_i ima končen red zaradi teh elementov končnih. \square

Vemo: $T \cong \mathbb{Z}_{n_1} \oplus \dots \oplus \mathbb{Z}_{n_r}$, $n_i = p_i^{k_i}$

Osnovni izrek o končno generiranih Abelovih grupah:

Vsaka končna generirana Abelova grupa je končna direktna vsota neskončnih cikličnih grup in cikličnih p -podgrup.

Ta zapis je enoličen v smislu: če je

$G = C_1 \oplus \dots \oplus C_m$ (C netrivialne, ciklične, neskončne ali p -podgrupe) in

$G = D_1 \oplus \dots \oplus D_n$ (D netrivialne, ciklične, neskončne ali p -podgrupe),

potem lahko s permutacijo indeksov dosežemo $\forall i. C_i \cong D_i$ in $n = m$.

Posplošitev na module nad glavnim kolaborjem K :

$$M \cong K^s \oplus K/(p_1^{k_1}) \oplus \dots \oplus K/(p_r^{k_r})$$

3. KATEGORIJE

18. december 2024

Definicija: Kategorijo \mathcal{K} sestavljajo:

- (a) Razred objektov.
- (b) Množice $\text{Hom}(A, B)$, ki obstajajo za vsak par objektov A in B . Njihove elemente imenujemo morfizmi in jih označujemo $f: A \rightarrow B$ ali f .
splošneje: razredi
- (c) Preslikave $\text{Hom}(B, C) \times \text{Hom}(A, B) \rightarrow \text{Hom}(A, C)$, ki vsakemu paru morfizmov $g: B \rightarrow C$ in $f: A \rightarrow B$ privedijo morfizem $g \circ f: A \rightarrow C$, imenovan kompozitum morfizmov f in g . Ob tem velja:
 - Za vse $f: A \rightarrow B$, $g: B \rightarrow C$, $h: C \rightarrow D$ je $(h \circ g) \circ f = h \circ (g \circ f)$.
 - Za vsak objekt A obstaja tak morfizem $1_A: A \rightarrow A$, da je $F \circ 1_A = f$ in $1_A \circ g = g$ za vse $f: A \rightarrow B$ in $g: B \rightarrow A$, ki ga imenujemo enotski morfizem (ali identiteta).

Primer: 1) Monsid $(M, *)$ porodi kategorijo z enim samim objektom σ in $\text{Hom}(\sigma, \sigma) = M$, kompozitum b in a pa je $b * a$.

2) Kategorija množic:

- objekti množice
- morfizmi so preslikave med njimi
- običajno kompozitum, $1_A = \text{id}_A$

3) Kategorija topoloških prostorov
 \rightsquigarrow morfizmi = zvezne funkcije

4) Kategorija delno urejenih množic:
 $x \leq y \Rightarrow f(x) \leq f(y)$
morfizmi

5) Kategorija grup

6) Kolobarjev

7) Monoidov

8) Vektorskih prostorov nad F (F fiksni)

9) K -modulov (K fiksni)

10) K -algeber (K fiksni komutativen kolobar)

Majhna kategorija: razred objektov je množica

Lokalna majhna: množice Hom (namesto razredi)

Podkategorija P kategorije K

Primeri: • Kategorija Abelovih grup je podkategorija kategorije grup.

• končne množice \sim množice

• polja \sim kolobarji

Dualna kategorija kategorije K : K°

• isti objekti

• morfizmom obrnemo puščice

$$f: A \rightarrow B \rightsquigarrow f': B \rightarrow A$$

Primer: $(M, *)$

Dualna kategorija (M^o, \circ) : $a \circ b := b * a$

Funktor iz $\mathcal{K} \vee \mathcal{K}'$ je preslikava, ki vsakemu objektu $A \in \mathcal{K}$ priredi objekt $F(A) \in \mathcal{K}'$ in vsakemu morfizmu $f: A \rightarrow B$ priredi morfizem $F(f): f(A) \rightarrow f(B)$ takš, da velja

$$\bullet F(g \circ f) = F(g) \circ F(f).$$

$$\bullet F(1_A) = 1_{F(A)}$$

Primera: 1) Pozabljivi Funktor

$$F(G) = \text{množica } G$$

$$F(f) = \text{preslikava } f$$

"pozabi na strukturo, grepe"

2) $F: \mathcal{K} \rightarrow \mathcal{K}'$

\mathcal{K} = kat. množic

\mathcal{K}' = kat. K -modulov

Mn. $X \rightarrow$ prosti K -modul $F(X) \ni$ baze X

$$\begin{matrix} F(X) &= F(X) \\ \uparrow & \uparrow \\ \text{funktor} & \text{prost: modul} \end{matrix}$$

$\uparrow F(f) = \text{enolično dobičeni homomorfizem } \bar{F}$

Kovariantni funkтор

Kontravariantni funktor: $F(g \circ f) = F(f) \circ F(g)$

Morfizem $f: A \rightarrow B$ je izomorfizem, če obstaja tak morfizem $g: B \rightarrow A$, da je $g \circ f = \text{id}_A$ in $f \circ g = \text{id}_B$. g ... inverz f

- Primeri:
- 1) $(M, *)$: izomorfizmi so obrnljivi elementi
 - 2) \mathcal{K} = kategorija množic : bijekcije
 - 3) \mathcal{K} = kategorija grup : "običajni" izomorfizmi

Univerzalna lastnost

Definicija: Produkt družine objektov $\{A_i \mid i \in I\}$ kategorije \mathcal{K} je objekt P skupaj z družino morfizmov $\{\pi_i : P \rightarrow A_i \mid i \in I\}$, tako da za vsak objekt B in vsako družino morfizmov $\{f_i : B \rightarrow A_i\}$ obstaja natanko en tak morfizem $f: B \rightarrow P$, da je $f_i = \pi_i \circ f$ za vse $i \in I$.

$$\begin{array}{ccc} & P & \\ f: & \swarrow & \downarrow \pi_i \\ B & \xrightarrow{f_i} & A_i \end{array}$$

Primeri: 1) Kategorija množic: $P = \prod_{i \in I} A_i$ $(a_i), a_i \in A_i$

$$\pi_j : (a_j) \longmapsto a_j$$

$$f_i: B \rightarrow A_i \quad f(b) = (f_i(b))$$

$$f_i = \pi_i \circ f$$

2) Produkt $\{G_i \mid i \in I\}$ v kategoriji grup
 ~ direktni produkt grup

3) Produkt $\{K_i \mid i \in I\}$ v kategoriji kolobarjev

~> direktni produkt kolobarjev

4) Moduli:

5) Produkt polj F_1 in F_2 v kategoriji polj:

Če imata F_1 in F_2 različni karakteristiki, potem homomorfizma Π_1 in Π_2 sploh ne moreta obstajati.

Ta definicija je univerzalna.

Naj bo P in $\{\Pi_i\}$ kot v definiciji.

Recimo: tudi Q in $\{\sigma_i \mid i \in I\}$ zadostu istemu pogoju.

P in Q sta izomorfnia

$$\begin{array}{ccc} P & & \\ \downarrow \pi_i & \swarrow g & \\ A_i & \xleftarrow{\sigma_i} & Q \\ & \uparrow f & \\ Q & \xrightarrow{\sigma_i} & A_i \end{array}$$

$$f \circ g : P \longrightarrow P$$

$$\pi_i \circ f \circ g = \sigma_i \circ g = \pi_i$$

$$\pi_i \circ (f \circ g) = \pi_i$$

$$\begin{array}{ccc} P & \xrightarrow{f \circ g} & P \\ & \downarrow \pi_i & \\ P & \xrightarrow{\pi_i} & A_i \end{array} \Rightarrow \begin{array}{l} f \circ g = 1_P \\ g \circ f = 1_Q \end{array}$$

Definicija: Koprodukt družine objektov $\{A_i \mid i \in I\}$ kategorije \mathcal{K} je objekt S skupaj z družino morfizmov $\{\iota_i : A_i \rightarrow S \mid i \in I\}$, tako da za vsak objekt B in vsako družino morfizmov $\{g_i : A_i \rightarrow B\}$ obstaja natanko en tak morfizem $g : S \rightarrow B$, da je $g_i = g \circ \iota_i$ za vse $i \in I$.

$$\begin{array}{ccc} & S & \\ \iota_i \downarrow & \vdots & \uparrow \iota_i \\ B & \xleftarrow{g_i} & A_i \end{array}$$

Oznaka: $\coprod A_i$, $A_1 \coprod A_2$

Tudi ta definicija je univerzalna.

Primeri: 1) Koprodukt v kategoriji množic je disjunktna unija.

$$\{A_i \mid i \in I\}$$

$$S = \bigcup \{(a, i) \mid a \in A_i\}$$

$$\iota_i(a) = (a, i)$$

$$g_i : A_i \rightarrow B \quad g : S \rightarrow B$$

$$g((a, i)) = g_i(a)$$

2) Kategorija Abelovih grup $\{A_i \mid i \in I\}$

Koprodukt je direktna vsota:

podgrupa direktnega produkta, ki sestoji iz (a_i) : vsi razen končnih mnogovstev a_i so 0.

Opomik: I končna \rightsquigarrow isto kot direktni produkt

$$g((a_i)) = \sum_{i \in I} g_i(a_i)$$

3) Moduli : podobno

4) Kategorija K -algeber :

$$A_1 \amalg A_2 = A_1 \otimes A_2$$

Prosti objekti

Konkretna kategorija: objekti so množice, morfizmi preslikave (neformalno)

Definicija: Naj bo P objekt v konkretni kategoriji \mathcal{K} . Naj bo X množica in $i: X \rightarrow P$. P je prosti objekt na množici X , če za vsak objekt A in preslikavo $f: X \rightarrow A$ obstaja natanko in preslikava $\bar{f}: P \rightarrow A$ obvezna, da velja $\bar{f} \circ i = f$.

$$\begin{array}{ccc} X & \xrightarrow{i} & P \\ & \searrow F & \downarrow \bar{f} \\ & & A \end{array} \quad \begin{array}{c} \uparrow \\ \text{univerzalna} \\ \text{lastnost} \end{array}$$

Primer: V kategoriji K -modulov so prosti moduli prosti objekti (na bazi).

Proste grupe in reprezentacija grup

Prosta grupa na $\{x, y\}$ sestoji iz „zaporedij“

$$1, x, y, xy, yx, x^{-1}, x^2y^{-3}x, \dots$$

$$x^{-1}y^3 \cdot xy^{-3}x^2 = x^{-1}y^3xy^{-3}x^2$$

$$xy^{-3}x^2 \cdot x^{-2}y^3 = x$$

Naj bo X poljubna množica

$$\cdot X = \emptyset . \quad F_X = \{1\}$$

$$\cdot X \neq \emptyset . \quad F_X = ?$$

$$|X| = |X^{-1}|$$

$$x \mapsto x^{-1}$$

$$X = \{x_1, x_2, \dots\}$$

$$X^{-1} = \{x_1^{-1}, x_2^{-1}, \dots\}$$

Beseda na X je zaporedje iz $X \cup X^{-1} \cup \{1\}$

$$(x_1, x_2, \dots, x_n, 1, 1, \dots), \quad x_i \in X \cup X^{-1} \cup \{1\}$$

Reducirana beseda:

(1) Če je $x_i = 1$, je tudi $x_{i+1} = x_{i+2} = \dots = 1$.

(2) x in x^{-1} ali x^{-1} in x ne nasposta zaporedoma

Poenskrivitev zapisa: $x_1 x_2 x_3 \cdots x_n, \quad 1 = (1, 1, 1, \dots)$

Dogovor: $xy^{-1}y^{-1}yx = xy^{-3}x^2$

Množico vseh reduciranih besed na X , označimo jo s

F_X , postane grupa, če vpeljemo

Brešar UVA 22

Poučuje 6.6.

Verzija 2025-01-12

$$x_1 \dots x_m \cdot y_1 \dots y_n = \begin{cases} x_1 \dots x_m y_1 \dots y_n, & \text{če } x_m \neq y_n^{-1} \\ x_1 \dots x_{m-1} y_2 \dots y_n = \begin{cases} \dots & x_{m-1} \neq y_n^{-1} \\ \dots & = \end{cases} \end{cases}$$

F_X ... prosta grupa na X

Izrek: Prosta grupa F_X je prosti objekt v kategoriji grup na množici F_X .

Dokaz: $\begin{array}{ccc} X & \xrightarrow{i} & F_X \\ & \searrow f & \downarrow \tilde{f} \\ & & G \end{array}$ $i(x) = x$
 $\tilde{f}(x_1^{e_1} x_2^{e_2} \dots x_m^{e_m}) = f(x_1)^{e_1} \dots f(x_m)^{e_m}$ \square

Posledica: Vsaka grupa je homomorfna slika kakršne proste grupe.

Dokaz: G ; naj bo $X \subseteq G$ poljubna množica, ki jo generira

$$f: X \rightarrow G, f(x) = x$$

\exists hom. $\tilde{f}: F_X \rightarrow G$, ki je surjektiven, saj njegova slika vsebuje X

$$G \cong F_X / \underbrace{\ker \tilde{f}}_{N \triangleleft F_X}$$

Definicija: Naj bo X množica in R množica reduciranih besed na množici X . Pravimo, da je grupa G definirana z generatorji $x \in X$ in relacijami $r=1, r \in R$, če je G izomorfna grapi F_X/N_R , kjer je N_R edinka, generirana z R . Rečemo, da je par $\langle X | R \rangle$ reprezentacija grupe G .

$$r = x_1^{\epsilon_1} \cdots x_m^{\epsilon_m} \in R$$

$$x_1 N_{\ell}, \dots, x_n N_R \in F_x / N_R$$

$$(x_1 N)^{\epsilon_1} \cdots (x_m N)^{\epsilon_m} = 1$$

$$x_1, x_2, x_1^{-1}, x_2^{-1} \in R$$

Končno prezentirana grupa: $|X|, |R| < \infty$

$$\langle x_1, \dots, x_n \mid r_1 = \dots = r_n = 1 \rangle \quad (= \langle X | R \rangle)$$

Primeri: (1) $F_x: \langle x \mid \emptyset \rangle$

(2) $\mathbb{Z}_n: \langle x \mid x^n = 1 \rangle$

(3) $\langle x, y \mid xy = yx \rangle \cong \mathbb{Z} \oplus \mathbb{Z}$

$$\underbrace{xyx^{-1}y^{-1}}_r = 1$$

(4) $D_{2n}: r, z, \quad r^n = z^2 = (rz)^2 = 1$

$$\langle x, y \mid x^n = y^2 = (xy)^2 = 1 \rangle \cong D_{2n}$$

Dokaz: Naj bo G katerakoli grupa generirana z u in v :

$$u^n = v^2 = (uv)^2 = 1$$

1. primer: D_{2n}

2. primer: $F_{\{x, y\}} / N$, N je generirana z $x^n, y^2, (xy)^2$
 $(u = xN, v = yN)$

(a) G je homeomorna slika $F_{\{x, y\}} / N$

(b) $|G| \leq 2n$

(a) $\Rightarrow \exists$ epimorfizem iz $F_{\{x, y\}} / N \rightarrow D_{2n}$

$$(b) \Rightarrow |F_{\{x,y\}}/N| \leq 2n$$

$$\text{zato } F_{\{x,y\}}/N \cong D_{2n}$$

(a) \exists epimorfizem $\ell: F_{\{x,y\}} \longrightarrow G$, $x \mapsto u$, $y \mapsto v$

$$x^h \in \ker \ell, \quad y^2, (xy)^2 \in \ker \ell$$

$$\ker \ell \geq N$$

Definiramo $F_{\{x,y\}}/N \longrightarrow G$

$$w_n \longmapsto w \ker \ell$$

$$(b) uvuv^{-1} = 1$$

$$vuv^{-1} = u^{-1}$$

$$\Rightarrow \langle u \rangle \triangleleft G$$

$$|G/\langle u \rangle| \leq 2 \quad |\langle u \rangle| \leq n \quad \Rightarrow |G| \leq 2n$$

Proste algebre in prezentacije algeber

Algebre polinomov nad poljem F so prosti objekti v kategoriji komutativnih algeber.

$$F[x,y]$$

A nad F

$$f: \{x,y\} \rightarrow A$$

$$f(x) = a$$

$$f(y) = b$$

$$\bar{f}(f(x,y)) = f(a,b)$$

$$X = \{x,y\}$$

$$1, x, y, xy, yx, xy - yx, \dots$$

$$(xy - x)(yx + x) = xy^2x - x^2$$

$$(yx + x)(xy - x) = yx^2y - x^2y - yx^2 + x^2$$

Prosta algebra na X: $F\langle x \rangle$

$$A \cong F\langle x \rangle / I$$

$$F\langle x_1, \dots, x_m | f_1(x_1, \dots, x_n) = \dots = f_n(x_1, \dots, x_n) = 0 \rangle$$

Primeri: (1) $F\langle x_1, x_2 | x_1x_2 = x_2x_1 \rangle = F[x_1, x_2]$

(2) $\mathbb{H} \cong \mathbb{R}\langle x, y | x^2 = y^2 = -1, xy + yx = 0 \rangle$

(3) $M_2(\mathbb{R}) \cong \mathbb{R}\langle x, y | x^2 = y^2 = 0, xy + yx = 1 \rangle \quad (E_{12}, E_{21})$

(4) $F\langle x, y | xy = 1 \rangle$

Bresčar UVA 22

Pozdravljenje 6.7

verzija 2025-01-12

Wedderburn - Artinov izrek

15. januar 2025

Nekomutativni obseg: \mathbb{H} } nekomutativna kolobarja
Matrke nad $S : M_n(S)$ }

1. Enostavni kolobarji: $R \neq \{0\}$ je enostaven, če sta $\{0\}$ in R edina idealna.

Primeri: (1) obsegi

(2) $M_n(D) \dots D$ obseg

E_{ij} standardne matrične enote

$$A = (a_{ij}) \quad E_{ij} A E_{kj} = a_{jk} E_{ij}$$

$\rightsquigarrow \dots \Rightarrow$ res enostaven kolobar

2. Prakolobarji: R je pradeal, če za vsaka idealna $I, J \triangleleft R$:

$$IJ = \{0\} \Rightarrow I = \{0\} \text{ ali } J = \{0\}$$

enostaven \Rightarrow pradeal


Lema: Za R so naslednji pogoji ekvivalentni:

(i) R je prakolobar.

(ii) $\forall a, b \in R. \quad aRb = \{0\} \Rightarrow a=0 \text{ ali } b=0$

(iii) Za vsaka leva idealna I in J . $IJ = \{0\} \Rightarrow I = \{0\} \text{ ali } J = \{0\}$.

Dokaz: (i) \Rightarrow (ii):

$$aRb = \{0\} \Rightarrow \overbrace{(RaR)R(RbR)}^{\sum x_i a y_i} \subset \{0\} \Rightarrow \begin{cases} RaR = \{0\} \\ \text{ali} \\ RbR = \{0\} \end{cases} \Rightarrow \begin{cases} a=0 \\ \text{ali} \\ b=0 \end{cases}$$

(ii) \Rightarrow (iii): $a \in I, b \in J \Rightarrow aRb = \{0\} \Rightarrow a=0$ ali $b=0$

□

(iii) \Rightarrow (i): trivialno

Artinski kolobarji

Definicija: Kolobar R je levi artinski kolobar, če za vsake verige levih idealov I_j velja:

$$I_1 \supseteq I_2 \supseteq \dots \Rightarrow \exists n \in \mathbb{N}. I_n = I_{n+1} = \dots$$

Primeri: (1) Končno razsežne algebreski (levi) artinski kolobarij nad poljem
To sledi iz dimenzij.

(2) $M_n(D)$ obseg; levi ideali so podprostori nad D
 \rightarrow ponovno gledamo dimenzije
 $\dim_D M_n(D) = n^2$

Idempotenti: $e \in R$ je idempotent, če je $e^2 = e$.

Idempotentna e, f sta ortogonalna idempotentna, če je $ef = fe = 0$.

Primeri: (1) 1, 0

(2) $e, 1-e$ je par ortogonalnih idempotentov

(3) E_1, \dots, E_n so paroma ortogonalni idempotentni

Lema: Če sta e in $f \neq 0$ ortogonalna idempotentna, je $R(1-e) \not\supseteq R(1-e-f)$.

Dokaz: $(1-e-f)(1-e) = 1-e-f$

$$\Leftrightarrow x(1-e-f)e \in R(1-e)$$

$$f = f(1-e) \in R(1-e)$$

Recimo $f = \chi(1-e-f)$

$$0 = f(1-f) < \chi(1-e-f)(1-f) \\ = \chi(1-e-f) : f$$

* ✓

Opozba: Če so e_1, \dots, e_m paroma ortogonalni idempotenti, je $e_1 + \dots + e_m$ idempotent. Če je f ortognalen na $e_1 + \dots + e_f$, je $fe_i = e_i f = 0 \quad \forall i$.

$$0 = f(e_1 + \dots + e_m) / e_i \\ \Rightarrow fe_1 = 0$$

eRe je kolobar z enoto e kastni kolobar

Lema: (a) Če je R levi artinski, je tudi eRe tak.
(b) Če je R prakolobar, je tudi eRe .

Dokaz: (a) $L_1 \supseteq L_2 \supseteq \dots$ L_i levi ideal eRe

$$RL_1 \supseteq RL_2 \supseteq \dots \Rightarrow$$

$$RL_n = RL_{n+1} = \dots$$

$$eReeL_n = eReeL_{n+1} = \dots$$

$$\begin{matrix} \text{..} & \text{..} \\ L_n & L_{n+1} \end{matrix}$$

(b) $(eae - e)R(e - ebe) = \{0\}$

$$eae - e = 0 \text{ ali } eebe = 0$$

✓

Minimalni levi ideal: L je minimalni levi ideal R , če iz $\{0\} \subseteq J \subseteq L \Rightarrow \{0\} = J$ ali $J = L$

Lema: Naj bo L minimalni levi ideal R : $L \neq \{0\}$.

Potem obstaja tak idempotent $e \in R$, da je $L = Re$ in eRe je obseg.

Primer: $M_n(D)$, $e = E_{11}$

$$RE_{11} = \left\{ \begin{bmatrix} * & & \\ & 0 & \\ & & \end{bmatrix} \right\}$$

$$eRe = \left\{ \begin{bmatrix} * & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & & 0 \\ 0 & & & \end{bmatrix} \right\} \tilde{=} D$$

Dokaz: Vzemimo $y \in L$: $Ly \neq \{0\}$

$$0 \neq Ly \subseteq L \Rightarrow Ly = L. \text{ Za } \exists z \in L \quad e y = y;$$

$$J = \{z \in L \mid zy = 0\}$$

$$J \text{ je levi ideal in } \subseteq L \Rightarrow J = \{0\}$$

$$e^2 y = ey = 0 \Rightarrow (e^2 - e)y = 0 \Rightarrow e^2 = e$$

$$\{0\} \neq Re \subseteq L \Rightarrow L = Re$$

eRe - obseg

$$eae \neq 0$$

$$\emptyset \neq Reae \subseteq L \Rightarrow Reae = L$$

$$e = beae$$

$$e = ebe eae$$

ebe ima tudi levi inverz

Lema: Levi artinski kolobar ima minimalni levi ideal.

Dokaz: $L_1 \supseteq L_2 \supseteq \dots$ na neki točki dobimo minimalni ideal \square

Matrične enote: $\{e_{ij} \mid 1 \leq i \leq j \leq n\}$ je množica $n \times n$ matričnih enot, če $e_{ij} e_{kl} = \delta_{jk} e_{il}$ in $e_{11} + e_{22} + \dots + e_{nn} = 1$.

Primer: $\{E_{ij}\} \subseteq M_n(S)$

Lema: Če je $\{e_{ij}\}$ množica $n \times n$ matričnih enot v R , je $R \cong M_n(e_{11} R e_{11})$.

Dokaz: $a \in R$

$$a_{ij} = e_{1i} a e_{j1} = e_{11}(a_{ij})e_{11} \in e_{11} R e_{11}$$

$$\varphi: R \rightarrow M_n(e_{11} R e_{11})$$

$$\varphi(a) = (a_{ij}) \text{ je izom.} \quad \square$$

Lema: Če R vsebuje paroma ortogonalne idempotence e_{11}, \dots, e_{nn} z $\sum_{i=1}^n e_{ii} = 1$ in take elemente $e_{1i} \in e_{11} R e_{11}$ in $e_{ii} \in e_{11} R e_{11}$, da je $e_{1i} e_{i1} = e_{11}$ in $e_{ii} e_{1i} = e_{ii}$, potem lahko to množico dopolnimo do množice matričnih enot.

Dokaz: $i \neq j$ $e_{ij} := e_{1i} e_{1j} \dots$ to res zadostia ... \square

Lema: Če sta e in f taka ortogonalna idempotentna v R , da sta eRe in fRf obseg, potem obstajata taka $u \in eRe$ in $v \in fRf$, da je $uv = e$ in $vu = f$.

Dokaz: 3a. $eaf \neq 0$

3b. $\underbrace{eafbe}_{eRe} \neq 0$

$\exists c \in R. eafbe \cdot ece = e$

$$(e \circ f)(f \circ e) = e$$

!! !!

\bar{u} \bar{v}

$$\nabla u = F$$

$$(\nabla u)^2 - \underbrace{\nabla u \cdot \nabla u}_{\bar{e}} = \nabla u \quad \nabla u \in FRf \text{ obseg}$$

$$\Rightarrow \nabla u = 0 \quad \times$$

$$\cdot \nabla \overset{\text{a:}}{u} = f$$

□

Lema: Če ima prakolobar R take paroma ortogonalne idempotente e_1, \dots, e_n , da je $e_1 + \dots + e_n = 1$ in je $e_i R e_i$ obseg za vsaki, potem je $R \cong M_n(e_i R e_i)$.

Dokaz: $u \nabla = e_1 \quad u \in e_1 R e_2$
 $v \nabla = e_2 \quad v \in e_2 R e_1$

$$\begin{array}{l} e_{11} := u \\ e_{21} := v \\ \vdots \\ e_{nn} \end{array} \quad \left. \begin{array}{l} e_{12}, e_{31} \\ \vdots \\ e_{nn} \end{array} \right\} \text{analogno}$$

→ predzadnja lemu.

□

Izrek [Wedderburn-Artin]:

Kolobar R je levi artinski prakolobar (posebej: enostaven) natanko tedaj, kadar obstajata $n \in \mathbb{N}$ in obseg D , da velja $R \cong M_n(D)$.

Dokaz: R levi artinski $\Rightarrow \exists$ minimalni levi ideal L

$L^2 \neq \{0\}$, ker R prakolobar

\exists idempotent e_1 . $e_1 R e_1$ obseg in $L = R e_1$

• $e_1 = 1 \checkmark$

• $e_1 \neq 1 \quad R \cong R(1-e_1)$

$(1-e_1)R(1-e_1)$ je levi artinski prakolobar

\exists idempotent $e_2 \in (1-e_1)R(1-e_1)$

e_2Re_2 je obseg $e_2e_1 = e_1e_2 = 0$

$R(1-e_1) \supsetneq R(1-e_1-e_2)$, ker $e_2 \neq 0$ (soj $e_1 \neq 1$)

$(1-e_1-e_2)R(1-e_1-e_2)$ je levi artinski prakolobar

če je tak 0 , je $e_1+e_2=1$ in uporabimo

zadnjo leme, sicer nadaljujemo s postopkom

$\exists e_3 \dots$ ortognanen na e_1 in e_2

$e_3Re_3 = e_3(1-e_1-e_2)R(1-e_1-e_2)e_3$ je obseg

$$e_1+e_2+e_3=1 \quad \checkmark$$

:

Postopek se ustavi zaradi leve artinskoosti

□