Uvod v teorijo grup

Operacija na množici $S \neq \emptyset$

$\star : S \times S \longrightarrow S$

- $\star$ je asociativna ko $\forall a,b,c.\ (a \star b) \star c = a \star (b \star c)$
- $\star$ je komutativna $\forall a,b.\ a \star b = b \star a$

Definicija: $(S, \star)$ je ~~polgrupa~~, če je $\star$ asociativna

Definicija: Naj bo S množica z operacijo $\star$
Pravimo da je $e \in S$ ~~enota~~ oz. ~~nevtralni element~~, ko $\forall a.\ ea = ae = a$

Velja: če $\exists$ enota, potem je ena sama

Definicija: Polgrupa z enoto je ~~monoid~~

Definicija: S naj bo množica z operacijo $\star$ in enota e. Naj bo $x \in S$

a) $l \in S$ je levi inverz, če velja $lx = e$
b) $d \in S$ je desni inverz, če $x \star d = e$
c) $y \in S$ je inverz, če $x \star y = y \star x = e$

$$l = le = l(ed) = (l \star e) \star d = e \star d = d$$

Definicija: $x \in S$ je obrnljiv, če $\exists$ inverz za x

Definicija: Naj bo S z operacijo $\star$ monoid in je vsak element obrnljiv, potem je S ~~grupa~~
Če je $\star$ komutativna je ~~abelova~~

Zgledi:

1) $(\mathbb{Z}, +)$ abelova grupa

2) X neprazna množica

$Sim(X) = \{f : X \to\!\!\!\!\to X\}$ množica vseh bijektivnih preslikav

operacija: kompozitum $\circ$

asociativnost, enota, inverz

$(Sim(X), \circ)$ je simetrična grupa množice X

Poseben primer: X je končna $X = \{1, 2, \ldots, n\}$

$Sim(X) = Sim\{1, \ldots, n\} = S_n$

.... simetrična grupa reda n

Ponoviter o permutacijah

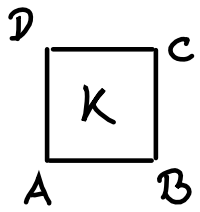
(elementi S_n)

- Vsaka permutacija je produkt (kompozitum) disjunktnih ciklov
- cikl: dolžine 2 je transpozicija
- vsaka permutacija $\sigma \in S_n$ je produkt transpozicij. Teh transpozicij je vedno sodo al: vedno liho mnogo

$$\operatorname{sgn} = \begin{cases} 1 : \sigma \text{ je produkt sodo mnogo transpozicij} \\ -1 \quad \sigma \text{ je produkt liho mnogo transpozicij} \end{cases}$$

- $\operatorname{sgn}(\sigma \circ \tau) = \operatorname{sgn}(\sigma) \cdot \operatorname{sgn}(\tau)$

Zgled: Simetrije kvadrata

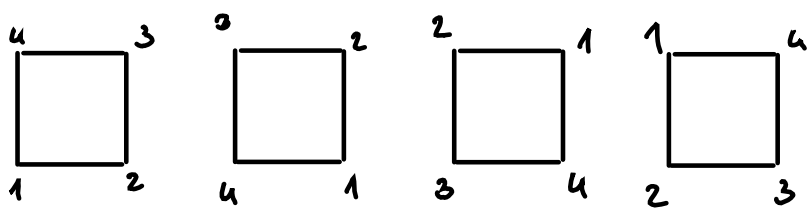


= izometrije $f: \mathbb{R}^2 \to \mathbb{R}^2$, da je $f_*(K) = K$

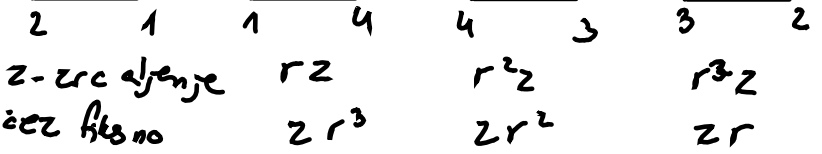
$f_{/K}: K \to K$ je bijekcija

Preverimo dobro množica simetrij grupa za kompozitum

Simetrija slika oglišča v oglišča
↳ permutacija oglišč



id = r^4 | r: rotacija za 90° okoli središča $(1\ 2\ 3\ 4)$ | r^2 | r^3



z - zrcaljenje čez fiksno os simetrije | rz | r^2z | r^3z
zr^3 | zr^2 | zr

$z^2 = id$

$(1\ 2)(3\ 4)$

$r^3z = zr$

$rzr = 1$

Torej vsak kompozitum r jev in z jev je oblike $r^n z^m$

$$\{id, r, r^2, r^3, rz, r^2z, r^3z\}$$

Trdimo: kvadratina ima ravno 8 simetrij

Simetrija je določena s sliko oglišča 1 in informacija ali smo naredili zrcaljenje ali ne

slika 1: 4 možnosti | zrcaljenje (da/ne) 2 možnosti

$4 \cdot 2 = 8$ manj kot 8 možnosti

$$D_{2\cdot 4} = \{id, r, r^2, r^3, zr, zr^2, zr^3\}$$

Diedrska grupa moči 8

Splošna simetracija:

r - rotacija za $\frac{2\pi}{n}$ okol: središča
z - zrcaljenje čez fiksno os simetrije

$$D_{2\cdot n} = \{1, r, \ldots r^{n-1}; z, zr^2, \ldots zr^{n-1}\}$$

Diedrska grupa moči $2n$

Velja $zr = r^{n-1}z$

če je $(S, \star)$ monoid naredim množico

$S^* := \{$ obrnljivi elementi iz $S\}$

S^* je grupa za $\star$

$e \in S^* \Rightarrow S^* \neq \emptyset$

Ali je S^* zaprta za operacijo

$x, y \in S^*$

$(x \star y)^{-1} = y^{-1} \star x^{-1}$ DN dokaži

$(x \star y) \star (y^{-1} \star x^{-1}) = x \star (e) \star (x^{-1}) = e$ ✓

Vsak $x \in S^*$ ima inverz $\in S^*$ ■

NPP: $S = (\mathbb{R}^{n \times n}, \cdot)$

$S^* = \{A \in \mathbb{R}^{n \times n}; \det A \neq 0\} = GL_n(\mathbb{R})$

splošna linearna grupa $n \times n$ matrik

Direktni produkt grup

$G_1, \ldots G_n$ naj bodo grupe z operacijami: $①, ②, ③ \ldots ⓝ$

$G_1 \times G_2 \times \ldots \times G_n$ vpeljemo operacijo $\star$

$(g_1, \ldots g_n) \star (h_1, \ldots, h_n) =$

$(g_1 ① h_1, g_2 ② h_2, \ldots g_n ⓝ h_n)$

DN: to je grupa

Oznake:	operacija	enota	inverz x	potenca x
grupa	$\cdot$	1	x^{-1}	x^n
abelova grupa	$+$	0	$-x$	nx

Podgrupe

Def: Naj bo G grupa, $H \subseteq G$ $H \neq \emptyset$

H je podgrupa grupe G, če je H grupa za isto operacijo

Trditev: Naslednje trditve so ekvivalentne

1) $H \leq G$
2) $\forall x, y \in H : xy^{-1} \in H$
3) H je zaprta za množenje in invertiranje

Dokaz:

$2 \Rightarrow 3$

$1 \in H$

- Izberemo $x \in H$ $y = x$

$xx^{-1} = 1 \in H$

Naj bo $x \in H$ poljuben

$x^{-1} \in H$

$1 \cdot x^{-1} \in H$

Izberemo $y \in H$

$y^{-1} \in H$

$x \cdot (y^{-1})^{-1} \in H \Rightarrow xy \in H$

Posledica: Naj bo G končna grupa
Naj bo $H \neq 0$ $H \subseteq G$

Potem je H podgrupa $\Leftrightarrow$ H je zaprta za množenje

Primer:
Določimo vse podgrupe v $(\mathbb{Z}, +)$

- $\{0\}$ trivialna podgrupa
- $\mathbb{Z}$

$H \leq \mathbb{Z}$ brez dodatnega zahtevnosti H ni trivialna
H gotovo vsebuje vsaj eno neravno število
Naj bo n najmanjše neravno število v H
Trdimo $H = n\mathbb{Z} = \{nk ; k \in \mathbb{Z}\}$
Ker je H zaprta za invertiranje, je $n\mathbb{Z} \subseteq H$
Vzemimo poljuben $m \in H$

$m = kn + r \qquad 0 \leq r < n$

$r = m - kn \in H \qquad r < n$
$\in H \quad \in H$

$\Rightarrow r = 0 \Rightarrow m = kn \Rightarrow m \in n\mathbb{Z}$

Primer

1) $GL_n(\mathbb{R})$ – obrnljive $n \times n$ matrike

je grupa za množenje matrik

$SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) : \det A = 1\}$ ... specialna linearna grupa

$SL_n(\mathbb{R})$

2) $O(n) = \{A \in GL_n(\mathbb{R}) : AA^T = A^TA = I\}$

3) $SO(n) = \{A \in O(n) : \det(A) = 1\}$

Trditev: Naj bosta $K, L \leq G$
Potem tudi $H \cap K \leq G$
Enako za preseke poljubnih družin podmnožic

Definicija: Naj bosta $HK \subseteq G$

$HK = \{h \cdot k : h \in H, k \in K\}$
produkt grup

Opomba:
HK ni vedno grupa

$G = S_3$
$H = \{id, (1,2)\}$
$K = \{id, (1,3)\}$

$HK = \{id, (1\,2), (1\,3), (1\,3\,2)\}$
$(1\,3\,2)\,(1\,3\,2) = (1\,2\,3) \notin HK$

Trditev: Naj bosta $H, K \leq G$. Če velja

$HK = KH$

potem je HK podgrupa

Dokaz:

$a, b \in HK$

$a = h_1 k_1 \quad h_1 \in H \; k_1 \in K$

$b = h_2 k_2 \quad h_2 \in H \; k_2 \in K$

$$ab^{-1} = h_1 k_1 (h_2 k_2)^{-1} = h_1 \underbrace{k_1 k_2^{-1}}_{\in K} \underbrace{h_2^{-1}}_{\in H} = h_1 h_3 k_3$$

$$\underbrace{\underbrace{k_1 k_2^{-1}}_{\in K} \underbrace{h_2^{-1}}_{\in H}}_{\in KH = HK} \qquad \underbrace{h_1 h_3}_{\in H} \underbrace{k_3}_{\in K} \in HK$$

✓

■

Trditev: Naj bo $H \leq G$, $a \in G$. Potem je

$$aHa^{-1} = \{aha^{-1}, h \in H\}$$

Potem je to tudi podgrupa

Dokaz: $x, y \in aHa^{-1}$

$$x = ah_1a^{-1} \quad y = ah_2a^{-1}$$

$$x \cdot y^{-1} = ah_1a^{-1}(ah_2a^{-1})^{-1} =$$

$$= ah_1a^{-1}a^{-1}h_2^{-1}a = a\underbrace{h_1h_2^{-1}}_{\in H}a$$

∎

DN: Naj bo G grupa

1) $Z(G) = \{g \in G : gx = xg \ \forall x \in G\}$

je podgrupa v G (center grupe G

2) Naj bo $a \in G$. Potem je $C_G(a) = \{g \in G; ga = ag\}$ podgrupa v G (centralizator elementa a v G)

Odsek podgrup in Lagrangeov izrek

Naj bo G grupa in H podgrupa G

Vpeljemo relacijo na G

$$a \sim b \Leftrightarrow a^{-1}b \in H$$

Trditev: relacija je ekvivalenca

Naj bo G končna grupa

G/H je tudi končna

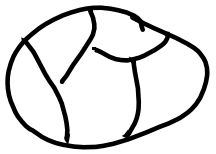
moč množice označimo z $|G:H|$ ← indeks podgrupe H v grupi G

Izrek: Če je G končna grupa in H podgrupa v G potem je $|G| = H \cdot |G:H|$

To je Lagrangeev izrek

Dokaz: $|G:H| = r$

$$G/H = \{a_1H, a_2H, \ldots, a_rH\}$$



$$|G| = |a_1H_1| + |a_2H_2| + \ldots + |a_rH|$$

Dokazati moramo, da je $|a;H| = |H|$

$$\varphi: H \longrightarrow a;H$$
$$h \longmapsto a;h$$

φ je očitno surjektivna

injektivnost

$$\varphi(h_1) = \varphi(h_2)$$
$$a;h_1 = a;h_2$$
$$a_i^{-1}/ \quad h_1 = h_2$$

■

Posledica: Naj bo G končna grupa in $H \leq G$. Potem $|H| \leq |G|$

Naj bo G abelova

Vpeljemo operacijo na G/H

$$(a+H)+(b+H)=(a+b)+H$$

Alije ta operacija dobro definirana

$a+H = a'+H$ $\quad a^{-1}a' \in H$ $\quad a'-a \in H$

$b+H = b'+H$ $\quad b^{-1}b' \in H$ $\quad b'-b \in H$

Dokazujemo $(a'+b')-(a+b) \in H$

komutativnost

$$a'+b'-a-b = (a'-a)-(b-b') \in H$$

G/H je abelova grupa za to operacijo

Generatorji grup, ciklične grupe

Definicija: Naj bo G grupa in X podmnožica v G. Potem označimo z $\langle X \rangle$ najmanjšo podgrupo, v G, ki vsebuje množico X.

Tej podgrupi pravimo podgrupa generirana z množico X

Zakaj je to smiselno?

$$\langle X \rangle = \bigcap_{X \subseteq A} A$$

Oznaka: če je $X = \{x_1, \ldots, x_n\}$ potem pišemo

$$\langle \{x_1, \ldots, x_n\} \rangle = \langle x_1, \ldots, x_n \rangle$$

če je $G = \langle x_1, \ldots, x_n \rangle$ potem je G končno generirana grupa.

če $\exists x \in G$. da je $G = \langle x \rangle$, pravimo da je G ciklična grupa

Kako izgledajo elementi $\langle X \rangle$?

$x_1, x_2 \in X \Rightarrow x_1^{-1} x_2 \in \langle X \rangle$

Očitno (DN)

$S = \{ x_{i_1}^{\pm 1} \cdot x_{i_2}^{\pm 1} \cdot \ldots \cdot x_{i_r}^{\pm 1} ; x_{i_j} \in X \} \subseteq \langle X \rangle$

Trditev: $\langle X \rangle = S$

Dokaz: $S \supseteq \langle X \rangle$

Naj bo $x \in \langle X \rangle$. $x = X \in S$

(Vzamemo produkt enega elementa x

$a, b \in S$

$a = x_{i_1}^{\pm 1} \cdot \ldots \cdot x_{i_r}^{\pm 1}$ $\quad x_{i_j} \in X$

$b = x_{k_1}^{\mp 1} \cdot \ldots \cdot x_{k_s}^{\pm 1}$ $\quad x_{i_j} \in X$

$a^{-1} \cdot b = x_{i_1}^{\mp 1} \cdot \ldots \cdot x_{i_r}^{\mp 1} \cdot x_{k_1}^{\pm 1} \cdot \ldots \cdot x_{k_s}^{\mp 1}$

Posledica: $a \in G$

$$\langle a \rangle = \{ a^n : n \in \mathbb{N} \}$$

Primeri:

$\mathbb{Z} = \langle 1 \rangle \quad n \in \mathbb{Z} \Rightarrow n = n \cdot 1$

$\mathbb{Z}_n = \langle 1 + n\mathbb{Z} \rangle$

Trdimo $\mathbb{Z} = \langle 2, 3 \rangle$

(Vseki dve tuji števil: generirata $\mathbb{Z}$

Def: Naj bo G grupa in $a \in G$.
Najmanjšemu naravnemu številu n, za katerega velja $a^n = 1$ pravimo red elementa a.
Če tak n ne obstaja pravimo, da ima a neskončen red

Primeri:

① $\mathbb{Z}$; 1 ima neskončen red $(n \cdot 1)$

② $\mathbb{Z}_n$ $1 + n\mathbb{Z}$ ima red n $k(1+n\mathbb{Z}) = k + n\mathbb{Z}$

Trditev: Naj bo G grupa, $a \in G$
Potem je red elementa a enak n
$\Leftrightarrow |\langle a \rangle| = n$

Dokaz:
$\Rightarrow$ Naj bo red $a = n$

Trdimo: $\langle a \rangle = \{1, a, a^2, \ldots, a^{n-1}\}$ in vsi naštetí elementi so paroma različni:

$\supseteq$ ok.

$\subseteq$ Naj bo $k \in \mathbb{Z}$ $k = mn + ost$ $0 \leq r \leq n-1$

$a^k = a^{mn+r} = (\underbrace{a^n}_{1})^m \cdot a^r = a^r$

Recimo da obstajata $0 \leq k < l \leq n-1$

$a^k = a^l \; / a^{-k}$

$1 = a^{l-k}$ $l-k < n$ ker je v prejšnjem

$\lightning$ predpostavko.

$\Leftarrow$ Recimo da $|\langle a \rangle| = n$

Potem ima a končen red

Po prejšnjem sklepu ima

$\langle a \rangle = \{1, a, \ldots, a^{m-1}\}$

Sledi: $m = n$

DN: $(\mathbb{Q}, +)$ ni končno generirana

Posledica: Naj bo G končna grupa

1) $\forall a \in G.$ red a deli $|G|$
2) $\forall a \in G.\ a^{|G|} = 1$
3) $|G|$ je praštevilo $\Rightarrow$ G je ciklična

Dokaz:

1) red $a = n$ ($n < \infty$ ker je G končna)

   $|\langle a \rangle| = n$. Po Lagrangevem izreku $n \mid |G|$

2) Naj bo red $a = n$

   Po 1) je $|G| = k \cdot n$

   $a^{|G|} = a^{kn} = (a^n)^k = 1$

3) Naj bo $|G| = p$, $a \in G - \{1\}$ po 2)

   $a^p = 1$

   red a deli p, red $a \neq 1$ Sledi $a = p \Rightarrow$

   $\langle a \rangle = \{1, \underbrace{\ldots, a^{p-1}}_{p}\}$

   Sledi $G = \langle a \rangle$

Uvod v teorijo kolobarjev, obsegov, polj in algebr

Def: Naj bo K neprazna množica z operacijama $+$ in $\cdot$.
Pravimo, da je K (oziroma $(K, +, \cdot)$) kolobar, če:

1) $(K, +)$ je abelova grupa
   (enota: 0 inverz a: $-a$)

2) $(K, \cdot)$ je monoid (kolobar ima vedno enoto za množenje: 1
   (enica kolobarja K))

3) $a(b+c) = ab + ac$ in $(a+b)c = ac + bc$
   za $\forall a, b, c \in K$

Če je $\cdot$ komutativna je K komutativen

Zgled:

- $(\mathbb{Z}, +, \cdot)$ komutativen kolobar
- $(2\mathbb{Z}, +, \cdot)$ (ni enote za množenje)
  komutativen kolobar (rng)
- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ so komutativni kolobarji
- $\mathbb{R}^{n \times n}$ je kolobar
- $X \subseteq \mathbb{R}$

  $\mathbb{R}^X = \{f : X \to \mathbb{R}\}$

  seštevanje in množenje po točkah

  $\mathbb{R}^X$ je komutativen kolobar

Homomorfizm:

Homomorfizem grup: $f(a)+f(b)=f(a+b)$

Homomorfizem kolobarjev:

$f(a)+f(b)=f(a+b)$

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

$f(1)=1$

zakaj moramo to definirati

$f:\mathbb{R}\longrightarrow\mathbb{R}^{2\times 2}$

$f(x)=\begin{bmatrix}x & 0\\ 0 & 0\end{bmatrix}$ $\quad f(x+y)=f(x)+f(y)$

$f(x\cdot y)=f(x)\cdot f(y)$

$f(1)$ ni enota v tem kolobarju

Homomorfizem algeber $f:A\longrightarrow B$

- f je homomorfizem kolobarjev in
- linearna preslikava

Opomba: če je $f: A \to B$ izomorfizem
potem je f^{-1} izomorfizem
potem $A \cong B$

a je fiksen
$\varphi(g) = aga^{-1}$ (konjugiranje)

φ je avtomorfizem grupe
notranji avtomorfizem

$\mathrm{Inn}\, G = \{ \varphi_a ;\ \varphi_a(g) = aga^{-1} \}$

K komutativen kolobar
$ev_a : K[x] \to K$ evaluacija
$p \mapsto p(a)$

$N \leq G$ je **Podgrupa edinka**, če

$\forall a \in G.\ aNa^{-1} \subseteq N$

$aNa^{-1} = \{ana^{-1};\ n \in N\}$

(Boljše ime bi bila normalna podgrupa)

Oznake: $N \triangleleft G$

Primeri:

$\{1\} \triangleleft G \qquad G \triangleleft G$

Grupe v katerih sta to edini edinki se imenujejo enostavne grupe

Če je G abelova je vsaka podgrupa edinka

(obstajajo tudi nekomutativne kjer to velja)

$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$

Vpeljemo množenje kvaternionov

Kvaternionska grupa. Vsaka grupa je edinka

Trditev: ekvivalentne

① $N \trianglelefteq G$

② $\forall a \in G \; aN \subseteq Na$

③ $\forall a \in G \; aN = Na$

④ $\forall a \in G \; aNa^{-1} = N$

1) $\Rightarrow$ 2)

$\forall a \in G, \forall n \exists k \in N. \; ana^{-1} = k$

$\Rightarrow \forall a \in G. \forall n \exists k \in N. \; an = ka \Rightarrow an \in Na \Rightarrow aN \subseteq Na$

2) $\Rightarrow$ 3

$\forall a \in G. \forall n \in N. \; an \in Na$

$\forall a \in G. \forall n \in N. \exists k \in N. \; an = ka$

$na^{-1} = a^{-1}k$

$na^{-1} \in a^{-1}N$

$Na^{-1} \subseteq a^{-1}N$

$Nb \subseteq bN \; \forall b$

3) $\Rightarrow$ 4): sledi

4) $\Rightarrow$ 1) analogno

Nazaj: $|G:H| = 2 \Rightarrow \exists aH, H$

$cH \in H \vee aH$

$cH = H \Rightarrow c \in H \Rightarrow Hc = H$

$cH = aH \Rightarrow a^{-1}c \in H \Rightarrow Ha^{-1}c = H \Rightarrow Ha^{-1} = Hc^{-1} \neq H$

$\Rightarrow Hc^{-1} = aH$

G grupa. Recimo $|G:H|=2$

Trdimo $H \lhd G$

↖ imamo dva leva odseka podgrupe H

$\forall a \in G \quad aH = Ha$

Bš zš $a \notin H$

$1 \cdot H = H$

$aH \neq H$

$G = H \cup aH$ disjunktna unija

$aH = G/H$

Desni odseki:

Lahko je v.deli, da imamo ~~same~~ natanko dva desna odseka

H in Ha

$G = H \cup Ha$ disjunktna unija

$Ha = G/H$

Torej $Ha = aH$

Primer

S_n,

A_n - {sode permutacije u S_n}

$A_n \leq S_n \quad |S_n : A_n| = 2 \Rightarrow A_n \trianglelefteq S_n$

② $D_{2n} = \{id, r, r^2 \dots r^{n-1}, z, rz, \dots r^{n-1}z\}$

$\langle r \rangle = \{id, r, \dots r^{n-1}\}$

$|D_{2n} : \langle r \rangle| = \frac{2n}{n} = 2$

$\langle r \rangle \trianglelefteq D_{2n}$

Trditev: Naj bo G grupa

(1) če je $H \leq G$ in $N \trianglelefteq G$

$HN = NH \leq G$

(2) če sta N, M podgrupi edinki v G

potem je $NM = MN \trianglelefteq G$

Dokaz:

1) $\forall h \in H$

$hN = Nh \Rightarrow HN = NH$ ~~ostalo~~

$HN = NH \Rightarrow$ je podgrupa (smo že dokazali)

2) NM je podgrupa

$g \in G$

$gNMg^{-1} \in NM$

$gNg^{-1}gMg^{-1} \in NM$

Izrek:

Naj bo G grupa $N \trianglelefteq G$

Potem je na G/N (← kvocientna/faktorska grupa) s predpisom

$$(aN)(bN) = (ab)N$$

dobro definirana operacija

s to operacijo postane množica G/N grupa

Preslikava $\pi: G \longrightarrow G/N$, dana s predpisom $\pi(g) = gN$ epimorfizem grup

$$\ker \pi = N$$

Dokaz:

dobra definiranost

če $aN = \hat{a}N$ in $bN = \hat{b}N \Rightarrow (ab)N = (\hat{a}\hat{b})N$

$$(ab)^{-1}(\hat{a}\hat{b}) = b^{-1}a^{-1}\hat{a}\hat{b} =$$

$$b^{-1}\underbrace{a^{-1}\hat{a}}_{\in N,\ \text{ker } aN = \hat{a}N} b\, b^{-1}\hat{b}$$

$\in N$

$\in N$, ker $bN = \hat{b}N$

$\in N$

G/N je grupa

asociativnost podeduje iz G

enota: $1 \cdot N = N$

inverz aN: $(aN)^{-1} = a^{-1}N$

π je homomorfizem

$$\pi(gh) = (gh)N = gN \cdot hN = \pi(g) \cdot \pi(h)$$

$g \in \ker \pi \Leftrightarrow \pi g = 1 \cdot N \Leftrightarrow gN = N \Leftrightarrow g \in N$

Izrek: (1. izrek o izomorfizmu)

Naj bo $\rho: G \to H$ homomorfizem grup.

Potem je $\ker\rho \triangleleft G$. Velja

$$G/\ker\rho \cong \operatorname{im}\rho$$

Dokaz: $\ker\rho$ je podgrupa v G

Vzemimo $g \in G$, $x \in \ker\rho$

$gxg^{-1} \in \ker\rho$

$$\rho(gxg^{-1}) = \rho(g)\rho(x)\rho(g^{-1}) = 1$$

Definiramo $\psi: G/\ker\rho \to \operatorname{im}\rho$

$$\psi(g\ker\rho) := \rho(g)$$

Dobro definiranost

$g\ker\rho = g'\ker\rho$ želimo videti $\rho(g) = \rho(g')$

$\Downarrow$

$g^{-1}\cdot g' \in \ker\rho$

$\rho(g^{-1}\cdot g') = 1$

$\rho(g^{-1})\cdot\rho(g') = 1$

$\rho(g') = \rho(g)$

ψ je homomorfizem

$$\psi((g\ker\rho)(g'\ker\rho)) =$$

$$= \psi(gg'\ker\rho) = \rho(gg') = \rho(g)\cdot\rho(g') =$$

$$= \psi(g\ker\rho)\psi(g'\ker\rho)$$

ψ je očitno epimorfizem

ψ je monomorfizem

$g\ker\rho \in \ker\psi$

$\psi(g\ker\rho) = 1$

$\rho(g) = 1$

$g \in \ker\rho \Rightarrow 1\cdot\ker\rho$

$\ker\psi$ je trivialen dobeg

$\ker\psi = \{1\cdot\ker\rho\}$

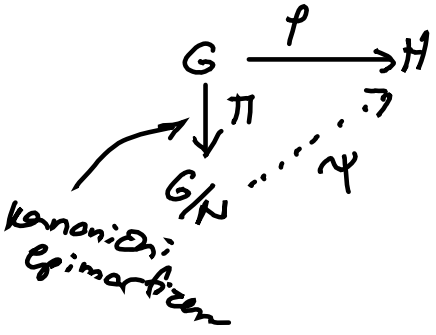
Opomba: Edinke so jedra
① homomorfizmov

② Naj bo $\rho: G \to H$ homomorfizem
Naj bo $N \trianglelefteq G$, recimo da
$N \subseteq \ker \rho$

Potem je $\psi: G/N \to H$ dana
s predpisom $\psi(gN) := \psi(g)$
dobro definiran homomorfizem grup

Pravimo da je ψ inducirana s ρ

shematično:



Ta diagram komutira

$$\psi \circ \pi(g) = \psi(\pi g) = \psi(gN) = \rho(g)$$

Izrek: (2. izrek o izomorfizmu)

Naj bo G grupa, $H \leq G$ $N \trianglelefteq G$

Potem je:

1) $N \cap H \trianglelefteq H$
2) $N \trianglelefteq HN$
3) $HN/N \cong H/N \cap H$

Ideja Dokaza:

1), 2) DN

3) Definiramo $f: H \to HN/N$

$f(h) := hN$

f je epimorfizem

$\ker f = H \cap N$

Uporabimo prvi izrek o izomorfizmu

$H/\ker f \cong \mathrm{im} f$

$H/N \cap H \cong HN/N$

Izrek (3. izrek o izomorfizmu)

Naj bo G grupa $N, M \trianglelefteq G$ $M \subseteq N$

1) $M \trianglelefteq N$
2) $N/M \trianglelefteq G/M$
3) $(G/M)/(N/M) \cong G/N$

Ideja dokaza

$\rho: G/M \longrightarrow G/N$

$\rho(gM) = gN$

ρ je dobro definiran epimorfizem

$\ker \rho = N/M$

Uporabimo 1. izrek o izomorfizmu

$$(G/M)/(N/M) = G/N$$

Lema: Naj bo $\varphi: G \to H$ homomorfizem grup

1) če je $K \leq G \Rightarrow \varphi_*(K) \leq H$

2) če je $K \trianglelefteq G$ in φ surjektiven $\Rightarrow \varphi_*(K) \trianglelefteq H$

3) $L \leq H \Rightarrow \varphi^*(L) \leq G$

4) $L \trianglelefteq H \Rightarrow \varphi^*(L) \trianglelefteq G$

Dokaz:

1) $\varphi(K) = \operatorname{im} \varphi|_K$ (zožitev φ na K) je podgrupa v H

2) $\varphi: G \to H$

$\varphi(K) \trianglelefteq H$

$x \in \varphi(K) \quad h \in H$

$hxh^{-1} \in \varphi(K)$

$x = \varphi(k) \; ; k \in K$

$h = \varphi(g) \; g \in G$ surjektivnost

$hxh^{-1} = \varphi(gkg^{-1}) \in \varphi(K)$

$\in K$

3) $x, y \in \varphi^*(L)$

$\exists a, b \in L. \; a = \varphi(x), \; b = \varphi(y)$

$ab^{-1} = \varphi(xy^{-1}) \in L$

$\in L \qquad \in \varphi^*(L)$

4) $x \in \varphi^*(L) \quad \exists a \in L : a = \varphi(x)$

$g \in G$

$gxg^{-1} \in \varphi^*(L)$

$\underbrace{\varphi(g) a \varphi(g^{-1})}_{\in L} = \varphi(\underbrace{gxg^{-1}}_{\in \varphi^*(L)})$

∎

Izrek: (korespondenčni izrek)

Naj bo G grupa in $N \trianglelefteq G$

a) Podgrupe v G/N so natanko oblike H/N kjer je $H \leq G$ $N \subseteq H$

b) Podgrupe edinke v G/N so natanko oblike K/N kjer je K $K \trianglelefteq G$ $N \subseteq K$

Dokaz a)

DN $H/N \leq G/N$

obratna smer

Naj bo L poljubna podgrupa v G/N

$\pi : G \longrightarrow G/N$ kanonični epimorfizem
$(g \mapsto gN)$

$H = \pi^*(L)$ je po lemi podgrupa v G

$N = \ker \pi \Rightarrow N \subseteq H$

$\pi_*(\pi^*(L)) = L$, ker je π surjektiven

Uporaba:

① G poljubna grupa, $a \in G$

$\langle a \rangle$

Trditev: $\langle a \rangle \cong \begin{cases} \mathbb{Z} & ; \text{reda} = \infty \\ \mathbb{Z}_n & \text{reda} = n \end{cases}$

Dokaz:

Recimo da reda $= \infty$

$\varphi : \mathbb{Z} \longrightarrow A$

$n \longmapsto a^n$

φ je homomorfizem

ker sur, je inj

$\ker \varphi = \{0\}$

Recimo da reda $= n$

$\varphi : \mathbb{Z}_n \longrightarrow \langle a \rangle$

$n \longmapsto a^n$

je ep: $\operatorname{im} \varphi = \langle a \rangle$

$m \in \ker \varphi \Leftrightarrow a^m = 1 \Leftrightarrow m \mid n$

$\ker \varphi = m\mathbb{Z}$

1. izrek o izomorfizmu $\mathbb{Z}/\ker \varphi \cong \operatorname{im} \varphi$

$\mathbb{Z}/m\mathbb{Z} \cong \langle a \rangle$

② Podgrupe v $\mathbb{Z}_n$

$$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$$

Po korespondenčnem izreku je $\forall$ podgrupa v $\mathbb{Z}_n$ oblike $H/n\mathbb{Z}$, kjer je $H \leq \mathbb{Z}$, $n\mathbb{Z} \subseteq H$

$H = k\mathbb{Z}$ $\quad k \mid n$ $\quad n = k \cdot d$

Podgrupe v $\mathbb{Z}_n$: $k\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_d$

Ideja dokaza: $\varphi : k\mathbb{Z} \xrightarrow{\text{DN}} \mathbb{Z}_d$ φ je epimorfizem in $\ker\varphi = n\mathbb{Z}$

③

Trditev: Naj bo G grupa netrivialna
G nima pravih netrivialnih podgrup
$\Leftrightarrow \exists p$ praštevilo, da je $G \cong \mathbb{Z}_p$

Dokaži

($\Leftarrow$) $H \subseteq \mathbb{Z}_p$ Lagrangeiveli: $|H| \mid |\mathbb{Z}_p|$

$|H| \mid p \Rightarrow |H| = 1$ ali $|H| = p$

$\Rightarrow H = \{\bar{0} + p\mathbb{Z}\}$ ali $H = \mathbb{Z}_p$

($\Rightarrow$) $a \in G$ arbitrarno

$\langle a \rangle$ je netrivialna grupa

Po predpostavki je $\langle a \rangle$ cela grupa.

G je ciklična

Dve možnosti: $G \cong \mathbb{Z}$ (ni res, ker ima $\mathbb{Z}$ veliko podgrup) ali: $G \cong \mathbb{Z}_n$

Po prejšnji trditvi (2) sledi: če je n sestavljeno število, potem ima G prave netrivialne podgrupe

Torej je n praštevilo

④ Izrek: (Cauchyjev izrek za abelove grupe)

Naj bo G končna abelova grupa.
Naj bo p praštevilo da $p \mid |G|$. $\Rightarrow$
Potem v G $\exists a \in G$. $\text{red}\, a = p$

Lema: Naj bo G grupa, $N \trianglelefteq G$, $a \in G$ reda n
Potem red $aN \in G/N$ deli n

Dokaz leme: $\pi : G \to G/N$

$$\pi(a^n) = \pi(a)^n = (aN)^n$$
$$\| \quad \|$$
$$1 \quad 1$$

Torej $\text{red}\, aN \mid n$ ∎

Dokaz: z indukcijo po moči $n = |G|$
baza indukcije:
$|G| = p \Rightarrow G \cong \mathbb{Z}_p$ $1 + p\mathbb{Z}$ ima red p

Recimo da $|G| > p$
po ③ ima G pravo netrivialno podgrupo
recimo N (ker je G abelova so vse podgrupe edinke)
$|G| = |N| \cdot |G/N|$ lagrange

$p \mid |N|$ ali: $p \mid |G/N|$

1. možnost $p \mid |N|$
po indukcijski predpostavki:
N vsebuje element reda $p \Rightarrow$
G vsebuje element reda p

2. možnost $p \mid |G/N|$
jetudi abelova in $|G/N| < |G|$
po indukcijski predpostavki:
G/N vsebuje aN reda p
$\text{red}\, aN \mid \text{red}\, a$

$$\text{red}\, a = p \cdot k$$
$$a^{pk} = 1$$
$$(a^k)^p = 1$$

Torej $\exists$ element de red $= p$ ∎

⑤ $\rho: S_n \longrightarrow (\{-1, 1\}, \cdot)$

$\rho(\pi) = \operatorname{sgn}(\pi)$

ρ je homomorfizem

$\ker \rho = \{\pi \in S_n ; \operatorname{sgn}\pi = 1\} = A_n \quad A_n \lhd S_n$

1. izrek o izomorfizmu $S_n/A_n = \mathbb{Z}_2$

⑥ F naj bo polje

$\rho: Gl_n(F) \longrightarrow F^*$

$\rho(A) = \det A$ je homomorfizem

$\ker \rho = \{A \in Gl_n(F) : \det A = 1\} = Sl_n(F)$

Torej $Sl_n(F) \lhd Gl_n(F)$

1. izrek o izomorfizmu $Gl_n(F)/Sl_n(F) \cong F^*$

(7.) G_1, G_2 grupi:

$G_1 \times G_2$ je tudi grupa

$(g_1, g_2)(h_1, h_2) = (g_1 h_1, g_2 h_2)$

$\tilde{G}_1 = \{(g_1, 1) : g_1 \in G_1\}$ je podgrupa v $G_1 \times G_2$

$\tilde{G}_1 \trianglelefteq G_1 \times G_2$

$(h_1, h_2)(g_1, 1)(h_1, h_2)^{-1} =$

$= (h_1 g_1, h_2)(h_1, h_2)^{-1} =$

$= (h_1 g_1 h_1^{-1}, 1) \in \tilde{G}_1$

$\tilde{G}_1 \cong G_1$

$(g_1, 1) \longmapsto g_1$

$G_1 \times G_2 / \tilde{G}_1 \cong G_2$

$\rho : G_1 \times G_2 \longrightarrow G_2$

$\rho : (g_1, g_2) \longmapsto g_2$ je epimorfizem

$\ker \rho = \tilde{G}_1$

(8) $\mathrm{Inn}\, G = \{ \rho_a : G \to G \; ; \rho_a(g) = aga^{-1} \}$

↓

konjugiranje z elementom a

(Notranji avtomorfizmi)

Opazimo: $(\rho_a)^{-1} = \rho_{a^{-1}}$

$\rho_a \circ \rho_b = \rho_{ab}$

Z drugimi besedami: imamo homomorfizem

$\Phi : G \to \mathrm{Inn}\, G$

$\Phi(a) = \rho_a$

Φ je surjektiven

Ker je Φ surjektiven je po 1. izreku o izomorfizmu $\mathrm{Inn}\, G \cong G / \ker \Phi$

$\ker \Phi = \{ a \in G : \rho_a = id_a \}$

$\rho_a = id_a \iff \rho_a(g) = g \quad \forall g \in G$

$\iff aga^{-1} = g \quad \forall g \in G$

$\iff ag = ga \quad \forall g \in G$

$\iff a \in Z(G)$

↑ center (elementi, ki komutirajo z vsemi)

Torej $G / Z(G) \cong \mathrm{Inn}\, G$

Opomba

$\mathrm{Inn}\, G$ je podgrupa v avtomorfizmih

DN: $\mathrm{Inn}\, G \trianglelefteq \mathrm{Aut}\, G$

$\mathrm{Out}\, G = \dfrac{\mathrm{Aut}\, G}{\mathrm{Inn}\, G}$ ... grupa zunanjih avtomorfizmov

(niso dejanski avtomorfizmi)

$\varphi \, \mathrm{Inn}\, G \, \varphi^{-1}(g) = \varphi(g) \rho_a(g) \varphi(g) =$

$\varphi(g) a g a^{-1} \varphi(g)^{-1} = \rho_{\varphi(g)a}$

Kvocientni kolobarji in algebre

K naj bo kolobar

Pozabimo na množenje

K za seštevanje je abelova grupa

Če je $I \leq K$ za seštevanje, lahko naredimo abelovo grupo K/I : $(a+I)$

operacija: $(a+I)+(b+I) = (a+b)+I$

na K/I bi radi vpeljali množenje

$(a+I)\cdot(b+I) = (ab+I)$

ali to deluje?

Definicija: Naj bo K kolobar in $I \subseteq K$, $I \neq \emptyset$. Pravimo da je I <u>ideal</u> če velja

a) $(I,+)$ je podgrupa v $(K,+)$
$\forall a,b \in I \quad a-b \in I$

b) $\forall a \in I . \forall x \in K . \; xa \in I$

c) $\forall a \in I . \forall x \in K . \; ax \in I$

Opomba:

① Pogoj b) lahko pišemo v obliki: $KI \subseteq I$
Prav tako pogoj c) $IK \subseteq I$

② Če I zadošča pogojema a) in b)
pravimo da je I levi ideal
če iz dodša a) in c) je desni ideal
Časti ideal/nom rečemo obojestranski ideal

Zgledi:

(1) Vsak kolobar ima vsaj dva ideala $\{0\}$, K sta vedno ideala

Kolobarjem ki imajo le tadva ideala pravimo enostavni kolobarji

K kolobar

I je <u>ideal</u> v K, če

I_1: $\forall a,b \in I.\ a-b \in I$ (je podgrupa za $+$)

I_2: $\forall a \in I\ \forall x \in K\ ax, xa \in I$

Zgled:

$aK = \{ax;\ x \in K$ je desni ideal v K

če je K komutativen, je $aK = Ka$ obojestranski ideal v K.

Pravimo mu <u>glavni ideal</u> v K generiran z a

(vsak ideal v K ki vsebuje a, vsebuje aK)

K nekomutativen: Najmanjši ideal, ki vsebuje a

$KaK = \{$vse končne vrste $\sum a_i a y_i$: $x_i, y_i \in K$

Ideal v $\mathbb{Z}$:

podgrupe: $n\mathbb{Z}$ vse avtomatično ideal.

$\mathbb{R}^{2\times 2}$

$\left\{\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix}, a,b \in \mathbb{R}\right\}$ je desni ideal, ni la.:

$\left\{\begin{bmatrix} a & 0 \\ b & 0 \end{bmatrix}; a,b \in \mathbb{R}\right\}$ je levi in ne desni ideal

DN: $\mathbb{R}^{n\times n}$ je enostaven ko lab-r

Opomba: Naj bo A algebra nad pdjem $\mathbb{F}$

Ideal: I_2, namesto I_1 podprostor v A-ju

Trdimo $I_1 + I_2 \Rightarrow$ podprostor v A

$\alpha \in \mathbb{F}$ $a \in I$

$$\alpha a = \alpha(1\cdot a) = (\alpha\cdot 1)\cdot a \in I$$
$$\in A \quad \in I$$

Namesto podprostor lahko rečemo abelova podgrupa

Trditev: Naj bo K kolobar in I ideal.
Potem je K/I z operacijama

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

$$(a+I)\cdot(b+I)=(a\cdot b)+I$$

je kolobar. Pravimo mu kvocientni (faktorski) kolobar.

Dokaz:
+ je dobro definirano (vemo iz grup)
• je dobro definirano

Recimo da $a+I=a'+I$ in $b+I=b'+I$
Dokazujemo $(ab)+I=(a'b')+I$

$$a-a'\in I \quad b-b'\in I$$

$$ab-a'b'=ab-a'b+a'b-a'b'=$$

$$=\underbrace{(a-a')}_{\in I}b+a'\underbrace{(b-b')}_{\in I}$$

$$\underbrace{\underbrace{(a-a')}_{\in I}b}_{\in I}+\underbrace{a'\underbrace{(b-b')}_{\in I}}_{\in I}$$

$$\in I$$

Lastnosti kolobarja izhajajo iz tega da je K kolobar.

Nicla v K/I : $0+I$

enica v K/I : $1+I$

Trditev: Najbo I ideal v K
če I vsebuje vsaj en obrnljiv element kolobarja K, potem $I = K$

Dokaz:

Recimo da je $u \in I$ obrnljiv. $x \in K$ poljuben

$$x = \underbrace{x u^{-1}}_{\in K} \cdot \underbrace{u}_{\in I} \in I$$

Torej $K = I$

Opomba: V prejšnji trditvi je dovolj da je I lev: (al: desni) ideal

Trditev: Naj bosta I, J ideala v K

a) $I \cap J$ je tudi ideal v K

b) $I \cdot J = \{$ vse končne vsote $\sum x_i y_i : x_i \in I \; y_j \in J\}$ je tudi ideal

c) $I + J$ je ideal

Dokaz:

a) DN

b) $\cdot$ IJ je očitno podgrupa za seštevanje

$\cdot \sum x_i y_i : x_i \in I \; y_i \in J$

$x \in K \quad x \sum x_i y_i = \sum \underset{\in I}{(x x_i)} \underset{\in J}{y_i} \in I \cdot J$

Izrek: (1. izrek o izomorfizmu)

Naj bo $\varphi : K \to L$ homomorfizem kolobarjev. Potem je $\ker\varphi$ ideal v K in velja $K/\ker\varphi \cong \operatorname{im}\varphi$

Dokaz:

$\ker\varphi \triangleleft K$

$(\ker\varphi, +)$ je podgrupa v $(K, +)$

$a \in \ker\varphi \quad x \in K$

$\varphi(ax) = \varphi(a)\varphi(x) = 0 \cdot \varphi(x) = 0 \Rightarrow ax \in \ker\varphi$

Podobno xa

$\psi : K/\ker\varphi \to \operatorname{im}\varphi$

$\psi(x + \ker\varphi) := \varphi(x)$

je dobro definiran izomorfizem kolobarjev

■

Izrek: (2. izrek o izomorfizmu)

Naj bosta I in J ideala v K. Potem je

$$(I+J)/J \cong I/(I \cap J)$$

Izrek: (3. izrek o izomorfizmu)

Naj bodo I, J, L ideali v K, $I \subseteq J \subseteq L$

$$(L/J)/(I/J) \cong L/I$$

Izrek: (korespondenčni izrek)

a) Podkolobarji v K/I so natanko oblike L/I, kjer je L podkolobar v K, ki vsebuje I

b) Ideali v K/I so natanko oblike J/I, kjer je J ideal v K, ki vsebuje I

Definicija: Naj bo $M \neq K$ ideal v kolobarju K. Pravimo da je M maksimalen ideal v K, če med M in K ni nobenega drugega ideala

$$I \trianglelefteq K,\ M \subseteq I \subseteq K \Rightarrow I = M \ \vee\ I = K$$

Izrek: Naj bo K komutativen kolobar, $M \trianglelefteq K$. Potem je M maksimalen ideal $\Leftrightarrow$ K/M je polje

Opomba: Komutativnost je nujna:

$\mathbb{R}^{2\times 2}$ (niceln: ideal je maksimalen kolobar)

Dokaz:

($\Rightarrow$) Izberemo poljuben $a+M \in K/M$ neničeln $a+M \neq 0+M$

$M + \underbrace{aK}_{\text{ideal, ker je } K \text{ komutativen}}$ je ideal (vsota dveh idealov je ideal DN

$M \subsetneq M + aK \subseteq K$

Zaradi maksimalnosti je $M + aK = K$

Med drugim $\exists k \in K.\ \exists m \in M.\ 1 = m + ak$

$1 - ak \in M$

$1 + M = ak + M = (a+M)(k+M)$

Torej je $(a+M)$ obrnljiv v K/M

($\Leftarrow$)

Naj bo $I \trianglelefteq K$ $\quad M \subsetneq I \subseteq K$

$\exists a \in I \setminus M$, ki ni v M

$a + M \neq 0 + M$

Po predpostavki je K/M polje, torej $\exists x \in K$

$(a+M)(x+M) = 1+M$

$$ax - 1 \in M \Rightarrow ax - 1 \in I$$
$$\in I$$

Sledi $1 \in I \Rightarrow I = K$

■

Izrek: Naj bo K poljubni kolobar
Potem je $\forall$ pravi ideal v K vsebovan
v nekem maksimalnem idealu

Dokaz uporabi: Zornova lemo:

X naj bo delno urejena množica

Veriga v X: $Y \subseteq X$. $\forall a,b \in Y$. $a \leq b \vee b \leq a$

Zgornja meja neke podmnožice Y:

$m \in X$. $y \leq m$. $\forall y \in M$

Maksimalen element množice X: tak $m \in X$, da
$\forall a \in X$. $m \not\leq a$

Zornova lema: Naj bo X delno urejena
množica: če ima $\forall$ veriga v X zgornjo mejo,
potem X vsebuje maksimalen element

Dokaz: $I \lhd K$, $I \neq K$

$\mathcal{J}$ naj bodo vsi: pravi ideali: v K, ki
vsebujejo I
$\mathcal{J} \neq 0$, ker $I \in \mathcal{S}$

$\mathcal{J}$ lahko delno uredimo z inkluzijo

Vzemimo poljubno verigo $\mathcal{V}$ v $\mathcal{J}$
$U = \bigcup_{J \in \mathcal{V}} J$ Trdimo $U \in \mathcal{J}$

U je ideal v K

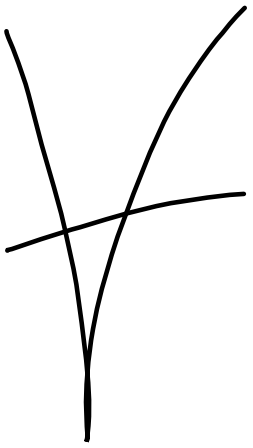
- $a,b \in U$. $\exists J_1, J_2 \in \mathcal{V}$. $a \in J_1$, $b \in J_2$
  BSZS. $J_1 \subseteq J_2$ (ker je $\mathcal{V}$ veriga)
  $a - b \in J_2 \subseteq U$
- $a \in U$, $x \in K$, $\exists J \in \mathcal{V}$. $a \in J$
  $ax, xa \in J \subseteq U$
- $U \neq K$
  če $U = K \Rightarrow 1 \in U \Rightarrow \exists J \in \mathcal{V}$. $1 \in J$. $\Rightarrow J = K$
  $\lightning$

Po zornovi lemi $\mathcal{J}$ vsebuje maksimalen element M
$M \lhd K$ $M \neq K$ $I \subseteq M$

M je maksimalen ideal v K

Recimo $\exists N \lhd K$. $M \subsetneq N \subsetneq K$. N je pravi ideal
v K, ki vsebuje I, torej $N \in \mathcal{J}$ $\lightning$

Zapiski od Vrške na discordu



Direktni produkt:

1) $G = N_1 \dots N_s$

2) $N_i \cap N_1 \cdots N_{i-1} \cdot N_{i+1} \cdots N_s = \{1\}$

Izrek:
Naj bo G grupa in $N_1, \dots N_s \trianglelefteq G$.
Potem je notranji direktni produkt $N_1 \dots N_s$ natanko tedaj, ko se da $\forall g \in G$ na enoličen način zapisati kot $g = n_1 \dots n_s$

Dokaz:

$\Rightarrow$ G je notranji direktni produkt

enoličnost zapisa:

$$n_1 \dots n_s = m_1 \dots m_s$$

$$\underbrace{m_1^{-1} n_1}_{\in N_1} = \underbrace{(m_2 \dots m_s)(n_2 \dots n_s)^{-1}}_{\in N_2 \cdot \dots N_s}$$

$N_1 \cap N_2 \dots N_s = 1 \Rightarrow m_1^{-1} n_1 = 1$

$\Rightarrow n_1 = m$

itd.

$\Leftarrow$ Recimo da se da $\forall g \in G$ enolično zapisati

1) Potem očitno $G = N_1 \cdot \dots N_s$

2) $n_i \in N_i$

$n_i = 1 \cdot \dots 1 \cdot n_i \cdot 1 \dots 1$

$P = N_1 \cdot \dots \cdot N_{i-1} \cdot N_{i+1} \dots N_s = \{ n_1 \dots n_s : n_j \in N_j \}$ (brez n_i)

$x \in N_i \cap P$

$x = 1 \dots n_i \dots 1 = n_1 \dots 1 \dots n_s \Rightarrow$

$n_1 \dots n_s = 1 = n_i$

komutator $[x,y] = xyx^{-1}y^{-1}$

$([x,y] = 1 \Leftrightarrow xyx^{-1}y^{-1} = 1 \Leftrightarrow xy = yx)$

lema: $M, N \trianglelefteq G$, $M \cap N = \{1\}$
elementi iz M komutirajo z elementi iz N.

Dokaz: $m \in M$, $n \in N$

$[m,n] = 1$ $\quad \underbrace{mnm^{-1}n^{-1}}_{\in N} \in N$

$\underbrace{mnm^{-1}n^{-1}}_{\in M} \in M \quad \Rightarrow = \{1\}$

Izrek: Naj bo G notranji direktni produkt edink. podgrup $N_1, \dots, N_s$.
Potem je $G \cong N_1 \times \dots \times N_s$

$\varphi: N_1 \times \dots \times N_s \longrightarrow G$

$(n_1, \dots, n_s) \longmapsto n_1 \cdots n_s$

inj, surj ✓

$(n_1, \dots, n_s)(m_1, \dots, m_s) = (n_1 m_1, \dots, n_s m_s) =$

$= n_1 m_1, \dots, n_s m_s$

$n_1 \cdots n_s \cdot m_1 \cdots m_s = n_1 m_1 n_2 \cdots n_s m_2 \cdots m_s =$

$= n_1 m_1 n_2 m_2 \cdots n_s m_s$

■

Klasifikacija končnih abelovih grup

Lema: $|G| = mn$, G abelova, m, n tuji:
$H = \{x \in G;\ mx = 0\}$, $K = \{x \in G;\ nx = 0\}$
Potem sta H in K podgrupi v G in
$G = H \oplus K$, $|H| = m$ $|K| = n$.

Dokaz: $H \leq G$

$a, b \in H \quad m(a-b) = ma - mb = 0 - 0 = 0$

m, n tuji $\Rightarrow \exists a, b \in \mathbb{Z}.\ am + bn = 1$

$x \in H \cap K$

$x = 1 \cdot x = a(mx) + b(nx) = a \cdot 0 + b \cdot 0 = 0$

$g \in G.\ g = mag - nbg = a\underbrace{mg}_{\in G} - b\underbrace{ng}_{\in H}$

$|H| = m$ $|K| = n$

$p \mid m \Rightarrow p \mid |H|$

$p \mid m \Rightarrow p \mid |G| \Rightarrow \exists a.\ pa = 0 = am = 0$

$\Rightarrow a \in H \Rightarrow \langle a \rangle \leq H \Rightarrow p \mid |H|$

Od zadnjič

$|G| = mn$ m, n sta s: tuj:

$H = \{x \in G;\ mx = 0\}$

$K = \{x \in G;\ nx = 0\}$

$G = H + K$

$\exists a, b \in \mathbb{Z}.\ am + bn = 1$

$x = 1 \cdot x = (am + bn)x = amx + bnx$

$m(bnx) = bmnx = 0$

$|G| \quad 0$

$\Rightarrow bnx \in H$

$\Rightarrow amx \in G \qquad G = H \oplus K$

$|H| = m \quad |K| = n$

$mn = |G| = |H| \cdot |K|$

Ker sta m in n tuji je dovolj premisliti

$\forall p \in \mathbb{P}.\ p \nmid m \Rightarrow p \nmid |H| \wedge p \nmid |K|$

Recimo da $p \mid m$ in recimo da $p \mid |H|$

Po cauchyjevem izreku

grupa H vsebuje element y reda p

$y \neq 0 \quad py = 0 \ ; \ my = 0$

m in p sta tuja. $\exists c, d \in \mathbb{Z}.$

$cm + dp = 1$

$y = 1y = (cm + dp)y = \underbrace{cmy}_{0} + \underbrace{dpy}_{0} = 0$

$\lightning$

Primer: G abelova grupa reda $6 = 2 \cdot 3$

$G = H \oplus K \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3$

$|H| = 2 \quad |K| = 3 \Rightarrow H \cong \mathbb{Z}_2 \wedge K \cong \mathbb{Z}_3$

Edina abelova grupa reda 6

DN: m, n tuji $\Rightarrow \mathbb{Z}_m \oplus \mathbb{Z}_n \cong \mathbb{Z}_{mn}$

opomba: $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \ncong \mathbb{Z}_4$, ker ima

$\mathbb{Z}_4$ element reda 4 $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ pa ne

Posledica: Naj bo G končna abelova

$$|G| = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k}$$

$$H_i := \{x \in G ; p_i^{e_i} x = 0$$

$$G = H_1 \oplus H_2 \oplus \ldots \oplus H_n$$

in $|H_i| = p_i^{e_i}$

Definicija: $|G| = p^n$: $p \in \mathbb{P}$ pravimo da je G <u>p-grupa</u>

Tavaj: $\forall$ končna abelova grupa je vsota p-grup (za različna praštevila)

Dovolj je torej obravnavati končne abelove p-grupe

Lema 1: Naj bo G netrivialna končna abelova p-grupa

Potem velja: G je ciklična $\Leftrightarrow$ G vsebuje natanko eno podgrupo moči p

Dokaz: $|G| = p^m$

($\Rightarrow$) če je G ciklična in ima moč p^m

$\Rightarrow G \cong \mathbb{Z}_{p^m}$

Podgrupe: $p^k \cdot \mathbb{Z}_{p^m}$; $k \leq m$

Edina, ki ima moč p je $p^{m-1} \cdot \mathbb{Z}_{p^m}$

($\Leftarrow$) indukcija po moči

$|G| = p$: očitno ima v tem primeru samo eno podgrupo

Recimo da ta trditev velja za vse p-grupe moči $< p^m$

Naj bo N edina podgrupa v G, ki ima moč p

$N = \{x \in G ; px = 0\}$

$N \subseteq \{\dots\}$ saj ima N moč p

če ima $x \in G$ red p je $\langle x \rangle$ podgrupa moči p

Zato je $N = \langle x \rangle$; torej $x \in N$

Oglejmo si

$\varphi: G \longrightarrow G$

$\varphi(x) = px$

φ je homomorfizem grup

$\ker \varphi = N$

$G/N \cong im\varphi$ je podgrupa v G

G/N je p-grupa netrivialna

ker jo lahko gledamo kot podgrupo v G
ima še vedno natanko eno podgrupo
moči p

Po indukcijski predpostavki je G/N ciklična

$G/N = \langle a+N \rangle \quad a \notin N$

$\forall x \in G. \exists k \in \mathbb{Z} \quad x+n = k(a+N) = ka+N$

$x - ka \in N$

$\exists n \in N \quad X = ka + n \quad n \in N$

$G = \langle a \rangle + N$

$\langle a \rangle$ je netrivialna ciklična p-grupa
to pa pomeni, da $\langle a \rangle$ vsebuje element reda p:

$\langle b \rangle$ ima moč $p \Rightarrow \langle b \rangle = N$

$\langle b \rangle \subseteq \langle a \rangle \Rightarrow N \subseteq \langle a \rangle$

$\Rightarrow G = \langle a \rangle$ ∎

Lema: Naj bo G končna abelova p-grupa. Naj bo C tista ciklična podgrupa v G, ki ima največjo možno moč.

Potem $\exists$ podgrupa $K \leq G$, da je

$$G = C \oplus K$$

Dokaz: Če je G ciklična $\Rightarrow C = G$, $K = \{0\}$

Recimo da G ni ciklična. $|G| = p^m$, $m > 1$

Indukcija po moči $|G|$

Po prejšnji lem: ima G vsaj dve podgrup: moči p

C ima po prejšnji lem: natanko eno podgrupo moči p

Zato $\exists$ podgrupa moči p v G ki ni vsebovana v C. označimo $\mathbb{Z}_p \cong N$

Opazimo $C \cap N < N$ $|N| = p$

Torej $C \cap N = \{0\}$

2. izrek o izomorfizmu:

$$HN/N \cong H/N \cap H$$

$$\frac{C+N}{N} \cong \frac{C}{C \cap N} \cong C$$

$\frac{C+N}{N}$ je ciklična podgrupa v G/N

ima največjo moč med cikličnimi podgrupami grupe G/N in ima največjo moč med cikličnimi:

$$|G/N| < |G|$$

Po indukcijski predpostavki $\exists K \leq G$

$N \subseteq K$ da je

$$G/N = \frac{C+N}{N} \oplus \frac{K}{N} \quad *$$

$G = C \oplus K$

iz $*$ sledi:

$x \in G$: $x+N \in G/N$

$x+N = (y+N) + (k+N) =$ $y \in C+N$, $k \in K$

$= (y+k)+N =$

$= y+k+n$ $n \in N$

$y+n \in C+N$

$G = C+N+K \Rightarrow G = C+K$

$C \cap K = \{0\}$

$x \in C \cap K$ $x \neq 0$

$x \in N$ ker $C \cap N = \{0\}$

$x+N \in \frac{C+N}{N} \cap \frac{K}{N} = \{0\}^{+N}$, ker je

to dvoje direktna vsota

$\Rightarrow \not\exists x \in N$ $\lightning$

Posledica: V končna abelova p-grupa je direktna vsota cikličnih p-grup

Posledica: Vsaka končna abelova grupa je direktna vsota cikličnih grup katerih moči so potence praštevil

Kako vidimo ali: dva razcepa abelovih grup na direktne vsote ciklicnih p_i-grup predstavljata isto grupo do izomorfizma natanko

$G, \bar{G}$ končni abelovi grupi; $\varphi: G \to \bar{G}$ izomorfizem

$$|G| = |\bar{G}| = p_1^{e_1} \cdots p_k^{e_k}$$

$$G = H_1 \oplus \cdots \oplus H_k \qquad |H_i| = p_i^{e_i}$$
$$\bar{G} = \bar{H}_1 \oplus \cdots \oplus \bar{H}_k \qquad |\bar{H}_i| = p_i^{e_i}$$

$$H_1 = \{x \in G : p_1^{e_1} = 0\}$$
$$\bar{H}_1 = \{x \in G : p_1^{e_1} = 0\}$$

$$\varphi_{/H_1} : H_1 \longrightarrow \bar{H}_1$$

$x \in H_1 \quad p_1^{e_1} \varphi(x) = \varphi(p_1^{e_1} x) = 0$

ker $|H_1| = |\bar{H}_1|$ sledi $H_1 \cong \bar{H}_1$

Problem izomorfnosti končnih abelovih grup se često zreducira na to kdaj sta dve končni abelovi p-grupi izomorfni:

Izrek: Naj bosta G in $\tilde{G}$ končni abelovi p-grupi

$$G \cong \mathbb{Z}_{p^{k_1}} \oplus \mathbb{Z}_{p^{k_2}} \oplus \dots \oplus \mathbb{Z}_{p^{k_m}}$$

$$\tilde{G} \cong \mathbb{Z}_{p^{l_1}} \oplus \mathbb{Z}_{p^{l_2}} \oplus \dots \oplus \mathbb{Z}_{p^{l_n}}$$

Predpostavimo

$$k_1 \geq \dots \geq k_m$$
$$l_1 \geq \dots \geq l_n$$

Recimo da $G \cong \tilde{G} \Rightarrow k_i = l_i$ in $m = n$

Dokaz: $\varphi: G \to \tilde{G}$ $\quad |G| = |\tilde{G}|$

$$p^{k_1+k_2+\dots k_m} = p^{l_1+l_2+\dots l_n}$$

Torej $k_1+k_2+\dots k_m = l_1+l_2+\dots l_n$

Po indukciji na r

$G \cong \mathbb{Z}_p$ in $\tilde{G} = \mathbb{Z}_p$

Recimo da velja zveza grupe moči p^s skr

$pG = \{p \cdot g \cdot g \in G\}$

$\leq$ ubistvu podmn

$pG \leq G$ $\quad pg_1 \cdot pg_2 = p(g_1 \cdot g_2)$

izpostavljamo lahko ker je abelova

$\varphi/_{pG}: pG \longrightarrow p\tilde{G}$

$\varphi(pg) = p(\varphi g)$

$\varphi/_{pG}$ je izomorfizem

$$G = \underbrace{\mathbb{Z}_{p^{k_1}} \oplus \dots \oplus \mathbb{Z}_{p^{k_{m'}}}}_{k_j \geq 2} \oplus \underbrace{\mathbb{Z}_p \oplus \dots \oplus \mathbb{Z}_p}_{m-m'}$$

$$G = \mathbb{Z}_{p^{l_1}} \oplus \dots \mathbb{Z}_{p^{l_{m'}}} \oplus \underbrace{\mathbb{Z}_p \oplus \dots \oplus \mathbb{Z}_p}_{n-n'}$$

$$pG = p\mathbb{Z}_{p^{k_1}} \oplus \dots p\mathbb{Z}_{p^{k_{m'}}} \oplus \underbrace{p\mathbb{Z}_p \oplus \dots \oplus p\mathbb{Z}_p}_{=0,\ \text{ker } p \cdot n = 0 \vee \mathbb{Z}_p}$$

$$\cong \mathbb{Z}_{p^{k_1-1}} \oplus \dots \mathbb{Z}_{p^{k_{m'}-1}}$$

$$p\tilde{G} = \mathbb{Z}_{p^{l_1-1}} \oplus \dots \mathbb{Z}_{p^{l_{m'}-1}}$$

pG sta izomorfni in imata manjšo moč kot G

Po indukcijski predpostavki dobimo

$m' = n'$

$k_i - 1 = l_i - 1$

$k_i = l_i$

Torej

$$G = \mathbb{Z}_{p^{k_1}} \oplus \dots \mathbb{Z}_{p^{k_{m'}}} \oplus \underbrace{\mathbb{Z}_p \oplus \dots \oplus \mathbb{Z}_p}_{m-m'}$$

$$\tilde{G} = \mathbb{Z}_{p^{k_1}} \oplus \dots \mathbb{Z}_{p^{k_{m'}}} \oplus \underbrace{\mathbb{Z}_p \oplus \dots \oplus \mathbb{Z}_p}_{n-m'}$$

$$|G| = p^{k_1+k_2+\dots k_{m'}+m-m'}$$

$$|\tilde{G}| = p^{k_1+\dots k_{m'}+n-m'}$$

$\Rightarrow n = m$

Torej je izrek dokazan

Torej vsaka končna abelova grupa

Povzetek: Vsaka končna abelova grupa je izomorfna direktni vsoti cikličnih podgrup, ki so p-grupe za medsebojno različna praštevila

$G = \bigoplus_i \mathbb{Z}_{p_1^{k_i}} \bigoplus_j \mathbb{Z}_{p_1^{l_j}} \dots$

Zapis je enoličen do urstnega reda direktnih sumandov natanko



Use abelian group of order

$4032 = 2^4 \cdot 3^3$

2^4: $\mathbb{Z}_{2^4}$, $\mathbb{Z}_2^3 \oplus \mathbb{Z}_2$, $\mathbb{Z}_2^2 \oplus \mathbb{Z}_2^2$, $\mathbb{Z}_2^2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ — 5

3^3: $\mathbb{Z}_3^3$, $\mathbb{Z}_3^2 \oplus \mathbb{Z}_3$, $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$ — 3

So in 15

Maš podatke nečim lahko gene.

lahko generirane

končno generirane cikličke

abelove grupe

Izrek:

Naj bo G končno generirana abelova grupa. Potem je $G \cong \mathbb{Z}^n \oplus K$, pri čemer je K končna abelova grupa

Če je $G \cong \mathbb{Z}^n \oplus K \cong \mathbb{Z}^m \oplus L$

$\Rightarrow m = n \wedge K \cong L$

$(\mathbb{Z}^n = \underbrace{\mathbb{Z} \oplus \dots \oplus \mathbb{Z}}_{n})$

Ideja dokaza:

G abelova grupa z končno n rod

$T(G) = \{g \in G;\ |g| < \infty\}$

$T(G)$ je podgrupa v G

$mg = 0 \quad g, h \in T(G)$

$nh = 0$

$m \cdot n (g - h) = mng - mnh = 0 - 0 = 0$

$T(G)$... torzijska podgrupa v G

Za G pravimo da je brez torzije, če je $T(G) = \{0\}$

$G/T(G)$ je končno generirana abelova grupa brez torzij

$G = \langle x_1, \dots x_n \rangle \Rightarrow \frac{G}{T(G)} = \langle x_1 + T(G), \dots x_n + T(G) \rangle$

Recimo da $g + T(G)$ ima končen red $\Rightarrow g \in T(G)$

$(\forall g \in G/T(G).\ g + T(G) = 0 + T(G))$

$\Downarrow$

$\exists n.\ n(g + T(G)) = 0 + T(G)$

$ng + T(G) = 0 + T(G)$

Sledi $ng \in T(G) \Rightarrow$

$\exists m.\ m(ng) = 0$

$(mn) \cdot g = 0 \Rightarrow$ ima končen red, torej $g \in T(G)$

Izkaže se: če je G končno generirana abelova grupa brez torzije, potem je $G \cong \mathbb{Z}^n$ za neki n

Brez dokaza

Trditev: $\forall$ končno generirana abelova grupa je direktna vsota neke končnogenerirane abelove grupe brez torzije in neke končne abelove grupe

Dokaz: G naj bo končno generirana abelova $G/T(G)$ je k.g abelova brez torzije

$G/T(G) \cong \mathbb{Z}^n$

$e_i = (0, \dots 0, 1, 0, \dots 0) \in \mathbb{Z}^n$ (1 na i-tem mestu)

Vsak element $\mathbb{Z}^n$ lahko na enoličen način zapišemo kot

$\alpha_1 e_1 + \dots + \alpha_n e_n$ $\mathbb{Z}^n$ ima Bazo

Zato ima tudi $G/T(G)$ bazo

$f_1 + T(G), f_2 + T(G), \dots f_n + T(G)$

$f_i \in G \quad f_i \notin T(G)$

Naredimo $H = \langle f_1, f_2, \dots f_n \rangle$

Dokažemo lahko da so $f_1 \dots f_n$ baza za H

$H \longrightarrow \mathbb{Z}_n$

$f_i \longrightarrow e_i$ je izomorfizem grup

trdim da je $G = H \oplus T(G)$

Ker je $H \cong \mathbb{Z}_n$ nima elementov končnega reda. Zato je $H \cap T(G) = \{0\}$

$G = H + T(G)$

$g \in G \Rightarrow g + T(G) \in G/T(G)$

$g + T(G) = \alpha_1 (f_1 + T(G)) + \dots + \alpha_n (f_n + T(G)) \quad \alpha_i \in \mathbb{Z}$

$g + T(G) = \alpha_1 f_1 + \dots + \alpha_n f_n + T(G)$

Torej $g = \underbrace{\alpha_1 f_1 + \dots + \alpha_n f_n}_{\in H} + t \quad t \in T(G)$

Dokaz

Dokazati moramo še, da je

$T(G)$ končna grupa.

$G = H \oplus T(G)$

$T(G) \cong G/H$ ✓ abelova

G/H je kvocient končno generirane grupe

grupe je končno generirana

$T(G)$ je končno generirana grupa v kateri:

vsak element končen red

$T(G) = \langle t_1, \ldots, t_k \rangle \quad m_i t_i = 0$

$t \in T(G)$

$t = \alpha_1 t_1 + \ldots + \alpha_k t_k$ (ni baze, ampak uspemo lahko tako zapisemo (neenolično) ker je abelova

$0 \leq \alpha_i < m_i$

Za vse α_i imamo končno mnogo možnosti, zato imamo končno mnogo možnosti za t

$\Rightarrow T(G)$ končna

KONČNE GRUPE

delovanja grup

Definicija: Naj bo G grupa in X neprazna množica. Grupa G **DELUJE** na množici X ($G \curvearrowright X$), če $\exists$ preslikavo (**DELOVANJE**)

$$G \times X \longrightarrow X$$
$$(g, x) \longmapsto g \cdot x \quad \text{(samo oznaka)}$$

za katero veljata:

1) $g(h \cdot x) = (gh) \cdot x \quad \forall g, h \in G$

2) $1 \cdot x = x \quad 1 \in G$

Opomba: Definirali smo levo delovanje grupe G na X. Podobno lahko definiramo desno delovanje

$$X \times G \longrightarrow X$$
$$(x, g) \longmapsto x \cdot g$$

1') $(x \cdot h) \cdot g = x(h \cdot g)$

2') $x \cdot 1 = x$

Recimo da imamo levo delanje $G \curvearrowright X$ $(g, x) \mapsto g \cdot x$

Potem lahko definiramo desno delanje

$$X \times G \to X$$

$$(x, g) \mapsto g^{-1} x = x * g$$

Zakaj: 1) velja

$$(x * h) * g = g^{-1}(x * h) = g^{-1}(h^{-1} * x) =$$

$$= (g^{-1} \cdot h^{-1}) x = (h \cdot g)^{-1} x =$$

$$x * (h \cdot g)$$

$\square$

Opomba: Naj G deluje na X

$\mathrm{Sym}\, X = \{X \xrightarrow{\sim} X\}$

Delovanje poradi homomorfizem grup

$$\Phi : G \longrightarrow \mathrm{Sym}\, X$$

$$\Phi(g)(x) = g \cdot x \qquad g \mapsto (x \mapsto g \cdot x)$$

Φ je homomorfizem

$$\Phi(g \cdot h)(x) = (g \cdot h)x = g(h \cdot x) =$$

$$g \cdot \Phi(h)(x) = \Phi(g)(\Phi(h)(x)) =$$

$$\Phi(g)\,\Phi(h)(x)$$

Obratno: Če imamo homomorfizem

$\Phi : G \longrightarrow \mathrm{Sym}\, X$ potem $G \curvearrowright X$

s predpisom $g \cdot x = \Phi(g)(x)$

Opomba: Zakaj je $\varphi: X \to X$, $\varphi(x) = gx$ bijekcija?

surj:

$$\varphi(g^{-1}x) = g\,g^{-1}x = x$$

inj:

$$\varphi(x) = \varphi(y)$$

$$gx = gy$$

$$x = 1 \cdot x = g^{-1} \cdot g\,x = g^{-1}(gx) = g^{-1}(gy) = y$$

Recimo da imamo delovanje G na X

$$\Phi : G \longrightarrow Sym X$$

$\ker \Phi$ imenujemo jedro delovanja

Pravimo, da je delovanje <u>zvesto</u> če je jedro trivialno ($\ker \Phi = \{1\}$)

če je delovanje zvesto:

$$G/\ker \Phi \cong \operatorname{im} \Phi$$

$$\| \qquad\qquad \|$$

$$G \qquad\qquad \text{podgrupa } Sym X$$

G je izomorfna neki podgrupi $Sym X$

Pravimo da se G vloži v $Sym X$

Primeri delovanj

1) Trivialno delovanje

$g \cdot x = x$ za $\forall g \in G. \forall x \in X$

2) Grupa G deluje na G z levim množenjem

$$G \times G \longrightarrow G$$
$$(g,h) \longmapsto g \cdot h$$

imamo homomorfizem

$$\Phi : G \longrightarrow Sym\, G$$
$$\Phi(g)(h) = g \cdot h$$

$$g \in \ker \Phi \Leftrightarrow \Phi_g = id_G \Leftrightarrow \forall h \in G.\ g \cdot h = h$$

$$\Leftrightarrow g = 1$$

Cayleyjev izrek: ← levo regularno delovanje

Množenje z leve je tocij zvesto delovanje

$\Rightarrow$ $\forall$ grupa G se vloži v $Sym\, G$

V posebnem: G končna. $|G| = n$

G se vloži v $Sym\, G \cong Sym\{1,\dots,n\} = S_n$

3) G deluje na G

$$G \times G \longrightarrow G$$
$$(g,h) \longmapsto ghg^{-1}$$

DN: To je delovanje

$$g(h \cdot x) = g(hxh^{-1}) = ghxh^{-1}g^{-1}$$
$$(gh)x = ghx(gh)^{-1} = ghxh^{-1}g$$

4) $H \leq G$; G/H množica levih odsekov H v G

G deluje na G/H

$$G \times G/H \longrightarrow G/H$$
$$g \cdot (xH) = (gx)H$$

Dobra definiranost?

Recimo $xH = yH \Rightarrow gxH = gyH$

$\downarrow$

$x^{-1}y \in H$

Oglejmo si: $(gx)^{-1}gy = x^{-1}g^{-1}gy = x^{-1}y$

DN: To je delovanje $\in H$

5) Recimo da G deluje na X y nejbo neprazna množica

$$Y^X = \{f : X \to Y\}$$

G deluje na Y^X

$$G \times Y^X \to Y^X$$

$$(g, f) \longmapsto g \cdot f = (x \longmapsto f(g^{-1}x))$$

(izkaže se da je potrebno g^{-1} da deluje

Torej res deluje

~~(1,f)~~ a $1 \cdot f(x) = f(1^{-1}x) = f(x)$ ✓

$(g(hf))(x) = h \cdot f(g^{-1}x) =$

$f(h^{-1}g^{-1}x) = f((gh)^{-1}x) = (gh) \cdot f(x) + 1$

DN: $G \curvearrowright X \quad G \curvearrowright Y$

$(g, x) \to gx \quad (g, y) \mapsto gy$

Potem $G \curvearrowright Y^X$

$$(g \cdot f) = g \cdot f$$

$$gf(x) = g \cdot f(g^{-1}x)$$

6) V nejboa vektorski prostor

$GL(V)$ ....vsi avtomorfizmi prostora V

$$GL(V) \times V \longrightarrow V$$

$$(A, v) \mapsto Av$$

To je delovanje

7) K kemutativen kelabar z 1

$K[x_1, \ldots x_n]$

S_n deluje na $K[x_1 \ldots x_n]$

$\sigma \cdot p(x_1 \ldots x_n) = p(x_{\sigma(1)}, \ldots x_{\sigma(n)})$

to je delovanje

Orbite stabilizatorji, fiksne točke delovanj

Def: Naj grupa G deluje na množici X

1) Za $x \in X$ je ORBITA elementa x množica

$$G \cdot x = \{g \cdot x ; g \in G\}$$

2) Za $x \in X$ je stabilizator točke X množica $G_x = \{g \in G ; gx = x$

3) Za $g \in G$ je množica fiksnih točk

$$\text{g-ja} \quad X^g = \{x \in X ; gx = x\} = fix(g)$$

4) fiksne točke delovanja (invariante)

$$X^G = \bigcap_{g \in G} X^g = \{x \in X ; \forall g \in G . gx = x\}$$

Lema: Naj G deluje na X

Recimo da $g \cdot x = y$

Potem je $x = g^{-1} y$

Dokaz:

$$x = 1 \cdot x = g^{-1}(gx) = g^{-1} y$$

Trditev: Naj G deluje na X
Potem je $G_x \leq G$

Dokaz:

$1 \in G_x$ torej $G_x \neq \emptyset$

$g \cdot h \in G_x \qquad gx = x = hx$

$$(gh^{-1})x = g \cdot \underbrace{(h^{-1}x)}_{\text{lema}} = g \cdot x = x$$

■

Trditev: Naj G deluje na X. Na X vpeljemo relacijo $x,y \in X$: $x \sim y \Leftrightarrow \exists g \in G.\ y = gx$

Potem je $\sim$ ekvivalenčna relacija na X in ekvivalenčni razred elementa x je njegova orbita Gx

Dokaz

Refleksivnost $1x = 1$

simetričnost $gx = y \Rightarrow x = g^{-1}y$

tranzitivnost $gx = y \wedge hy = z \Rightarrow h \cdot gx = z$

Ekvivalenčni razred xa

$$[x] = \{y \in X : y \sim x\} = \{y \in X.\ \exists g \in G.\ y = gx\} =$$

$$= Gx$$

Oznaka: kvocientno množico po zg. relaciji označimo $X/G = X/\sim =$

$$= \{G \cdot x : x \in X\}$$

X/G je prostor orbit

Delovanju, ki ima eno samo orbito pravimo

<u>tranzitivno delovanje</u>

Zgled

1) Naj G deluje na G z levim množenjem

$$x \in G: \quad Gx = \{gx : g \in G\} = G$$

$$h \in G \Rightarrow h = h \cdot x^{-1} \cdot x$$

Tranzitivno delovanje

$$G_x = \{g \in G \cdot gx = x\} = \{1\}$$

$$\Downarrow$$

$$g = 1$$

$$G^g = \{x \in G : gx = x\} = \begin{cases} \emptyset & : g \neq 1 \\ G & : g = 1 \end{cases}$$

② G naj deluje na G s konjugiranjem

$$G \times G \longrightarrow$$
$$(g,h) \longmapsto g * h = ghg^{-1}$$

$x \in G$

$$G_x = \{g \in G;\ g*x = x\} = \{g \in G;\ gxg^{-1} = x\}$$
$$= \{g \in G,\ gx = xg\} =: C_G(x)$$

..., centralizator elementa x v G

orbita x-a $G*x = \{g*x;\ g \in G\} =$

$$= \underbrace{\{gxg^{-1} : g \in G\}}_{\text{konjugirani razred elementa } x \text{ v } G} = Cl_G(x)$$

$$G^g = \{x \in G.\ g*x = x\} = \{x \in G.\ gx = xg\} = C_G(g)$$

$$G^G = \bigcap_{g \in G} G^g = \bigcap_{g \in G} C_G(g) = Z(G)$$

3) $H \leq G$: G deluje na G/H

Orbita xH

$G(xH) = \{g \cdot xH;\ g \in G\} = G$

tranzitivna delovanja

Fiksne točke (invariante) delovanja

$K[x_1 \dots, x_n]^{S_n}$ = tisti polinomi, ki jih

$\{p : \forall \sigma \in S_n,\ \sigma \cdot p(x_1 \dots x_n) = p(x_1 \dots x_n)\} =$

$\{p(x_1 \dots x_n) : \forall \sigma \in S_n\ p(x_{\sigma(1)} \dots x_{\sigma(n)})\} =$

simetrični polinomi

$x_1 + x_2 + x_3$

$x_1x_2 + x_2x_3 + x_1x_3$

Izrek o orbiti in stabilizatorju

Naj grupa G deluje na množici X (orbita, indeks stabilizatorja)

a) $\forall x \in X.\ |G \cdot x| = |G : G_x|$ (deluje tudi za neskončne grupe)

b) G končna grupa $\Rightarrow |G| = |Gx| \cdot |G_x|$

Dokaz:

a) Iščemo bijekcijo med množicama Gx in G/G_x

$\alpha : Gx \longrightarrow G/G_x$

$\alpha : g \cdot x \mapsto gG_x$

Ali je α dobro definirana

$gx = hx \Rightarrow gG_x = hG_x$

$gx = hx$

$h^{-1}gx = x$

$h^{-1}g$ stabilizira $x \Rightarrow h^{-1}g \in G_x$

$\Rightarrow hG_x = gG_x$

α očitno surjektivna

α injektivna

$gG_x = hG_x \Rightarrow h^{-1}g \in G_x \Rightarrow$

$h^{-1}gx = x$

$gx = hx$ ✓

b) direktna posledica ■

Izrek

Naj grupa G deluje na X, X končna množica. Potem obstajajo elementi $x_1, \dots, x_r \in X - X^G$

↖ tisti x_i ki jih usi gji pustijo pri miru

$$|X| = |X^G| + \sum |G : G_{x_i}|$$

Dokaz: Množica X je disjunktna unija nekih orbit delovanja.

$x \in X^G \Rightarrow |Gx| = 1$

vsaka fiksna točka ima enoelementno orbito

Ostali: elementi imajo orbite večje od ~~ena~~

recimo da jih je r (ker je G končna)

Torej $|X| = |X^G| + |Gx_1| + \dots + |Gx_r|$

↖ vse ostale orbite

↗ orbite z 1 elementom

x_i: ji so predstavniki različnih orbit velikosti več kot 1

$$* \quad |X| = |X^G| + |G : G_{x_1}| + \dots |G : G_{x_r}| =$$

$$= |X^G| + \sum_{i=1}^{r} |G : G_{x_i}|$$

Posledica:

Naj bo G končna p-grupa, ki deluje na končni množici X.

Potem velja

$$|X| \equiv |X^G| \bmod p$$

Dokaz:

Po prejšnjem izreku lahko napišemo

$$|X| = |X^G| + \sum_{i=1}^{r} |G : G_{x_i}| \quad x_i \text{ niso fiksne točke}$$

Ker x_i niso fiksne točke, $G_{x_i} \neq G$

G_{x_i} je prava podgrupa $|G : G_{x_i}| = \frac{|G|}{|G_{x_i}|}$

je deljiv s p

sledi $p \mid (|X| - |X^G|)$

∎

Izrek (Burnsidova lema)

Naj končna grupa G deluje na končno množico

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

Dokaz: Izračunamo moč množice $\{(g,x) \in G \times X ; gx = x\}$ na dva načina

$$|\{(g,x) \in G \times X : gx = x\}| =$$

$$= \sum_{x \in X} |\{g \in G ; gx = x\}| = \sum_{x \in X} |G_x| =$$

$$= \sum_{x \in X} \frac{|G|}{|Gx|} = |G| \cdot \sum_{x \in X} \frac{1}{|Gx|} =$$

$$= |G| \sum_{\sigma \in X/G} \sum_{x \in \sigma} \frac{1}{|G_x|} = |G| \cdot \sum_{\sigma \in X/G} \underbrace{\sum_{x \in \sigma} \frac{1}{|\sigma|}}_{1} =$$

(σ ... orbita)

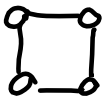
$$= |G| \cdot \sum_{\sigma \in X/G} 1 = |G| \cdot |X/G|$$

drugi način

$$|\{(g,x) \in G \times X ; gx = x\}| =$$

$$\sum_{g \in G} \{gx = x\} = \sum_{g \in G} |X^g|$$

Primer:

 barvamo oglišča z n barvami

 je isto barvanje

$\#$ barvanj glede na to identifikacijo

X .... množica vseh barv $\square$ z n barvami

$|X| = n^4$

r ... rotacija za $90°$

$G = \{id, r, r^2, r^3\}$

G deluje na X $|X/G| = ?$

$$|X/G| = \frac{1}{4}\left(|X^{id}| + |X^r| + |X^{r^2}| + |r^3|\right)$$

$|X^{id}| = |\{\text{vsa barvanja, ki jih } id \text{ pusti na miru}\}|$

$= |X| = n^4$

$|X^r| = |\{r \text{ za } 90° \text{ pusti na miru}\}| = n$ ← n barv

Podobno $|X^{r^3}| = n$

$|X^{r^2}| = n^2$

$$|X/G| = \frac{1}{4}\left(n^4 + 2n + n^2\right)$$

Razredna formula in Cauchyjev izrek

Posledica: Razredna formula

Naj bo G končna grupa
Potem obstajajo $x_1, \dots x_r \in X - Z(G)$
da velja $|G| = |Z(G)| + \sum_{i=1}^{r} |G : C_G(x_i)|$

$C_G(x_i) = \{ g \in G \mid gx_i = x_i g \}$

Dokaz: direktna uporaba splošne formule ko $G \curvearrowright G$ s konjugiranjem

$G \times G \longrightarrow G$
$(g, x) \longmapsto gxg^{-1}$

∎

Posledica: Naj bo G končna p-grupa.
Potem je $Z(G) \neq \{1\}$

Dokaz: BSZ G_n abelova

$\exists x_1 \dots x_r \in G - Z(G)$

$$|G| = |Z(G)| + \sum_{i=1} |G : C_G(x_i)|$$

$C_G(x_i) \neq G$, ker potem b_i:
x_i b_i-1 v centru

Zato $p \mid |G : C_G(x_i)|$

Torej mora biti: $p \mid |Z(G)|$

∎

Posledica: Naj bo G grupa moči p^2. Potem je G abelova

Dokaz: Naj bo G nekomutativna grupa moči p^2. Sledi $|Z(G)| = p$

$|G/Z(G)| = p$ torej je ciklična

$$G/Z(G) = \{1Z(G), xZ(G), \ldots x^{p-1}Z(G)\}$$

$$G = Z(G) \amalg xZ(G) \amalg \ldots \amalg x^{p-1}Z(G)$$

Vzemimo $a, b \in G$

$a \in x^i Z(G)$ $b \in x^j Z(G)$

$a = x^i \cdot z_1$ $b = x^j \cdot z_2$

$ab = x^i z_1 \cdot x^j z_2$ z_1 in z_2 sta v centru

torej $ab = x^i \cdot x^j z_1 \cdot z_2 = x^j x^i z_1 z_2 =$

$= x^j z_2 x^i z_1 = ba$ (↑ ker sta potenci iste ga elementa)

torej je G abelova ∎

Izrek (Cauchyjev izrek)

Naj bo G končna grupa in naj praštevilo p deli $|G|$. Potem v G obstaja element reda p.

Dokaz:

Za abelove grupe smo izrek že dokazali:

Indukcija po $|G|$

$|G|=p$: je ciklična torej ✓

Naj bo G grupa moči n in naj izrek velja za vse grupe manjših moči

BŠZS G ni abelova. Uporabimo razredno formulo

$$n=|G|=Z(G)+\sum_{i=1}^{r}|G:C_G(x_i)| \quad x_i \notin Z(G)$$

Recimo da $p \mid |Z(G)|$

(abelova grupa)

Potem po Cauchyjevem izreku za abelove grupe center vsebuje element reda p ✓

Lahko predpostavim da $p \nmid Z(G)$

Po razredni formuli

$\exists i: \; p \nmid |G:C_G(x_i)| = \frac{|G|}{|C_G(x_i)|}$

Sledi: $p \mid |C_G(x_i)|$

$C_G(x_i)$ je prava podgrupa in je manjša od $|G|$

po indukcijski predpostavki $C_G(x_i)$ vsebuje element red p

■

Izrek (i) Sylowa

Motivacija:

Lagrangeov izrek: G končna $H \leq G$

$\Rightarrow |H| \mid |G|$

Obrat? Recimo da $k \mid |G|$. Ali vedno obstaja $H \leq G$, $|H| = k$?

Ali nima podgrupe moči 6 ∴

Kaj če izberemo delitelj $|G|$ ki je potenca nekega praštevila?

Def: Naj bo G končna grupa. $H \leq G$

Pravimo da je H p-podgrupa Sylowa v G, če je

- $|H| = p^\alpha$
- $p^\alpha \mid |G|$
- $p^{\alpha+1} \nmid |G|$

(Največja podgrupa praštevila p moči)

Izrek Sylowa:

Naj bo G končna grupa $p \mid |G|$

a) če $p^l \mid |G|$ potem v G obstaja podgrupa moči p^l
(med drugim v $|G|$ obstaja vsaj ena p-podgrupa Sylowa)

b) Vsaka p-podgrupa v G je vsebovana v neki p-podgrupi Sylowa

c) Vse p-podgrupe Sylowa v G so konjugirane med sabo

d) Naj bo n_p število p-podgrup Sylowa v grupi G. Potem veljata dve zveze:
i) $n_p \mid |G|$
ii) $n_p \equiv 1 \bmod p$

Dokaz:

a) z indukcijo po moči $n = |G|$

$n = p$ očitno

Recimo da trditev za vse grupe moči $< n$

Dokazujemo za grupe moči n

Ločimo dve možnosti:

i) $p \mid |Z(G)| \Rightarrow Z(G)$ vsebuje element reda p

Naj bo Z podgrupa v $Z(G)$ generirana s tem elementom. Z je edinka v G

Oglejmo si G/Z

$$|G/Z| = \frac{n}{p}$$

če je $p^l \mid |G| \Rightarrow p^{l-1} \mid |G/Z|$

Po indukcijski predpostavki grupa G/Z vsebuje podgrupo moči p^{l-1}. Ta podgrupa je oblike H/Z kjer je $H \leq G$

$$|H| = |H:Z| \cdot |Z| = p^{l-1} \cdot p = p^l$$

ii) p ne deli $|Z(G)|$

Razredna enačba: $|G| = |Z(G)| + \sum_{i=1}^{k} |G : C_G(x_i)|$

$x_i \in G - Z(G)$

Po predpostavki $\exists i.\ p \nmid |G : C_G(x_i)|$

$$p^l \mid |G| = \underbrace{|G : C_G(x_i)|}_{p \nmid} \cdot \underbrace{|C_G(x_i)|}_{p^l \mid}$$

$p^l \mid |C_G(x_i)|$ ampak $|C_G(x_i)| < |G|$

(ker x_i ni v centru)

Po indukcijski predpostavki $C_G(x_i)$ vsebuje podgrupo moči p^l

b) Dokaz

Pomožen rezultat od zadnjic:

G končna p-grupa $G \curvearrowright X$ $(|X| < \infty)$

Potem $|X| \equiv |X^G| \bmod p$ ✱

Po a) točki v G obstaja vsaj ena p-podgrupa Sylowa S.

Naj bo sedaj $H \leq G$ p-podgrupa

$X = G/S = \{xS ; x \in G\}$

$H \curvearrowright X$ z levim množenjem

$a \in H : a \cdot (xS) = (ax)S$

Po ✱ $|X| \equiv |X^H| \bmod p$

$|X| = |G/S| = \frac{|G|}{|S|}$ zaradi maksimalnosti S je $|X|$ ni deljivo s p

potem $X^H \neq \emptyset$

$\exists x_S \in X^H$

$\forall a \in H . \; axS = xS$

$x^{-1}axS = S$

$x^{-1}ax \in S$ za $\forall a \in H$

$a \in xSx^{-1}$ za $\forall a \in H$

$H \leq xSx^{-1}$

$xSx^{-1} \in G$

$|xSx^{-1}| = |S|$ (konjugiranje je bijekcija)

Zato je xSx^{-1} tudi p-podgrupa Sylowa ki vsebuje H

c) Dokaz

S naj bo fiksna p-podgrupa Sylowa

H naj bo poljubna p-podgrupa Sylowa

Po b) $\exists x \in G.\ H \subseteq xSx^{-1}$

H in xSx^{-1} sta p-podgrupi Sylowa v G, torej imata isto moč. Zato $H = xSx^{-1}$

d) Dokaz

$X = Syl_p G = \{$ vse p-podgrupe Sylova $\}$

$= \{ xSx^{-1} : x \in G \}$

$n_p = |X|$

G naj deluje na X s konjugiranjem

$S \in X$: orbita S-ja glede na to delovanje

$\{ g \cdot S ; g \in G \} = \{ gSg^{-1} ; g \in G \} = X$

stabilizator S-ja: $\{ g \in G ; g \cdot S = S \} =$

$= \{ g \in G : gSg^{-1} = S \} = N_G(S)$

(normalizator S v G)

Izrek o orbiti in stabilizatorju:

moc orbite S = indeks stabilizerja v G

$|X| = |G : N_G(S)|$ $\quad n_p = |G : N_G(S)|$

deli $|G|$

Naj S deluje na X s konjugiranjem

Po $\clubsuit$ $|X| \equiv |X^S| \bmod p$

n_p //

Trdimo $X^S = \{S\}$

Gotovo velja $S \in X^S$

Naj bo $T \in X^S$

$\forall s \in S . sT = T$

$sTs^{-1} = T$ za $\forall s \in S$

Z drugimi besedami: $S \subseteq N_G(T)$

S je p-podgrupa Sylova v $N_G(T)$

Po c) sta T in S konjugirani v $N_G(T)$

$\exists y \in N_G(T) . \; S = yTy^{-1} = T$

$\uparrow$ $y \in N_G(T)$

Dobimo $n_p \equiv 1 \bmod p$

Opomba:

Iz dokaza sledi:

$n_p = |G : N_G(S)|$ S neka podgrupa Sylowa

$n_p = 1 \Leftrightarrow |G : N_G(S)| = 1$

$\Leftrightarrow \quad G = N_G(S) \Leftrightarrow S \trianglelefteq G$

"edina p-podgrupa Sylowa je edinka"

Primer:

$p, 2$ različni praštevili $p < q$

Kaj lahko povemo o grupah moči $p \cdot q$

$|G| = p \cdot q$

V G obstaja vsaj ena p-podgrupa Sylowa

P. $|P| = p$

V G obstaja vsaj ena q-podgrup Sylowa Q $|Q| = q$

$n_p \mid p \cdot q$ in $n_p \equiv 1 \bmod p$ $n_p \in \{1, q\}$

$n_q \mid p \cdot q$ in $n_q \equiv 1 \bmod q$ $n_q \in \{1\}$

(ker $\in$ bi bil p $p \equiv 1 \bmod q$ ampak $p < q$)

Torej Q je edina q-podgrupa Sylowa

$\Rightarrow Q \trianglelefteq G$ ($\Rightarrow G$ ni enostavna)

Opazimo: $|P \cap Q|$ deli p in q

$\Rightarrow |P \cap Q| = 1$. $P \cap Q = \{1\}$

Ker je Q edinka v G je $PQ \leq G$

$$|PQ| = \frac{|P| \cdot |G|}{|P \cap Q|} = p \cdot q = |G|$$

$PQ = G$

Glede n_p imamo dve možnosti:

① $n_p = 1 \Rightarrow P \trianglelefteq G$

$P, Q \trianglelefteq G$ $PQ = G$ $P \cap Q = \{1\}$

$G = P \times Q \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{p \cdot q}$

2) $n_p = q$

Lahko se zgodi: $|S_3| = 2 \cdot 3$

Ena 3-podgrupa Sylowa:

$Q = \langle (1\ 2\ 3) \rangle$

imamo 3 2-podgrupe Sylowa

$\langle (1\ 2) \rangle$, $\langle (1\ 3) \rangle$, $\langle (2,3) \rangle$

DN vse grupe moči 77

Končne enostavne grupe

Def: Grupa G je enostavna, če sta $\{1\}$ in G edini: edinki.

Kako zgledajo končne enostavne grupe?

Primer: G končna abelova grupa. Kdaj je enostavna

$\Leftrightarrow$

Abelova grupa z natanko dvema podgrupama

DN: $|G| = p \wedge G \cong \mathbb{Z}_p$

Primer:

$A_n \leq S_n \quad |S_n : A_n| = 2 \Rightarrow A_n$ je edinka

$A_3 \cong Z_3$ enostavna

A_4 ni enostavna

$N = \langle (12)(34), (13)(24) \rangle \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$

Kleinova četverka

DN:

$\forall \pi \in A_n. \quad \pi(12)(34)\pi^{-1} \in N$

$\pi(13)(24)\pi^{-1} \in N$

Izrek:
Če je $n \geq 5$ je A_n enostavna

Dokaz: $N \trianglelefteq A_n$. $N \neq \{1\}$

Dokazujemo da je $N = A_n$

① Recimo da N vsebuje vsaj en tricikel

BŠZS. $(1\,2\,3) \in N$

Vzemimo permutacijo

$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ a & b & c & * & \dots & * \end{pmatrix}$ poljubna soda permutacija

$\sigma(1\,2\,3)\sigma^{-1} \in N$

$\parallel$

$(a\ b\ c)$

Torej $(a\ b\ c) \in N$ za $\forall a,b,c$

A_n je generirana z vsemi 3-cikli

Torej $N = A_n$

② N ne vsebuje nobenega 3-cikla

Lačimo se več primerov

2.1 Recimo da H vsebuje π katere razcep na disjunktne cikle vsebuje cikel dolžine ≥ 4

$\pi = (a_1\ a_2\ a_3\ a_4 \dots)(\dots)\dots(\dots)$

Potem je

$\pi' = (a_1\ a_2\ a_3)\pi(a_1\ a_2\ a_3)^{-1} \in N$

$\pi' = (a_2\ a_3\ a_1\ a_4 \dots)(\dots)\dots(\dots)$

Potem je $\pi'\pi^{-1} \in N$

$\pi'\pi^{-1} = (a_2\ a_4\ a_1) \in N$

N vsebuje torej 3-cikel $\lightning$

(2.2) N ne vsebuje nobene permutacije katere razcep na disjunktne cikle bi vseboval cikel dolžine ≥ 4

(2.2.1) Recimo da imamo v N permutacijo oblike

$\pi = (a\ b\ c)(a'\ b'\ c')\dots$

Potem je tudi

$\pi' = (a'\ b'\ c')\pi(a'\ b'\ c')^{-1} \in N$

$\lightning$ ker v π

$\pi' = (a\ b\ a')(c\ c'\ b')\dots$

$\pi'\pi \in N$!

$\pi'\pi = (a\ a'\ c\ b\ c')$ Torej je cikel dolžine več kot 4 $\lightning$

(2.2.2) Recimo da je v N permutacija oblike $\pi = (a\ b\ c)\cdot\dots$ s sodim številom transpozicij

$\pi^2 \in N$

$\pi^2 = (a\,b\,c)^2 = (a\ c\ b)$ $\lightning$

(2.2.3) ostane še primer ko ima vsi elementi N produkt sodega števila transpozicij

Locirmo dve možnosti

(2.2.3.1) Recimo da je $(a,b)(a'\ b') \in N$

$(a\,c\,b)(a\,b)(a'\ b')(a\ c\ b)^{-1} \in N$ =

$= (a\ c)(a'\ b')$

opazimo:

$\underbrace{(a\ b)(a'\ b')}_{\in N}\ \underbrace{(a\ c)(a'\ b')}_{\in N} = (a\ c\ b) \in N$

$\lightning$

(2.2.3.2) $\forall$ elem $\in N$ je produkt ≥ 4 disjunktnih transpozicij

$\pi = \underbrace{(a_1\ b_1)(a_2\ b_2)}_{\in N}(a_3\ b_3)(a_4\ b_4)\dots \in N$

Potem je $\pi' = (a_3\ b_2)(a_2\ b_1)\pi(a_2\ b_1)(a_3\ b_2)$

$\pi' = (a_1\ a_2)(a_3\ b_1)(b_2\ b_3)(a_4\ b_4)\dots$

$\pi'\pi \in N$

$\pi'\pi = (a_1\ a_3\ b_2)\dots$ $\lightning$

$\blacksquare$

Izkaže se: (klasifikacija končnih enostavnih grup)

če je G končna enostavna grupa, potem sodi vsaj v eno od naslednjih kategorij:

1) $\mathbb{Z}_p$, $p \in \mathbb{P}$
2) A_n $n \geq 5$
3) grupe Lijevega tipa

npr: $SL_n(F)$

$$Z(SL_n(F)) = \{\lambda I ; \lambda^n = 1\}$$

$$PSL_n(F) = \frac{SL_n(F)}{Z(SL_n(F))} \dots \text{projektivna}$$

je enostavna (za skoraj vse n)

4) 26 sporadičnih grup

Največja med njimi: je POŠAST

Moonshine theory povezana s to grupo

Zakaj so enostavne grupe $\sum\sum$?

↖ sigma sigma

G končna grupa

Če G ni enostavna, potem $\exists M \trianglelefteq G$ ki ni:

vsebovana v nebenivečji edinki (maksimalna edinka)

G/M je enostavna grupa

Postopek nadaljujemo

$G \trianglerighteq M \trianglerighteq M_1 \trianglerighteq \dots \trianglerighteq M_k \trianglerighteq \{1\}$

$G/M \quad M/M_1 \quad \dots \quad M_{k-1}/M_k \quad M_k$ vse enostavne

To je kompozicijska vrsta grupe

M_k poznamo in M_{k-1}/M_k tudi poznamo



→ vse možnosti za M_{k-1}

Rešljive grupe

Grupa G je <u>rešljiva</u>, če obstaja končno zaporedje podgrup

$$\{1\} = G_0 \triangleleft G_1 \triangleleft G_2 \triangleleft \dots \triangleleft G_k$$

Vsaka je edinka večji za kakšna velja: G_{i+1}/G_i je abelova

Primeri:

1) Abelove so vse rešljive: $\{1\} \triangleleft G$

2) $A_4 \triangleright \langle (12)(34), (13)(24) \rangle \triangleright \{1\}$

- A_4: kvocient z $\mathbb{Z}_3$ je abelova
- $\langle (12)(34), (13)(24) \rangle \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$
- $\{1\}$: kvocient je tudi abelova

3) $S_4 \triangleright A_4 \triangleright \langle (12)(34), (13)(24) \rangle \triangleright \{1\}$

4) G je nekomutativna enostavna grupa

A_n za $n \geq 5$ niso rešljive

Trditev: Naj bo G rešljiva

1) $H \leq G$ je tudi rešljiva

2) $N \trianglelefteq G \Rightarrow G/N$ je rešljiva

Dokaz:

imamo $\{1\} = G_0 \trianglelefteq \dots \trianglelefteq G_k = G$

$\frac{G_{i+1}}{G_i}$ so abelove

1) Oglejmo si:

$\{1\} = G_0 \cap H \trianglelefteq \dots \trianglelefteq G_k \cap H$

↖ očitno ↑ enačnke ↗

$$\frac{G_{i+1} \cap H}{G_i \cap H} = \frac{G_{i+1} \cap H}{(G_{i+1} \cap G_i) \cap H} \cong$$

$$\cong \frac{(G_{i+1} \cap H)\, G_i}{G_i} \leq \frac{G_{i+1}}{G_i}$$

$\frac{H}{N \cap H} \cong \frac{HN}{N}$ abelova

$\frac{G_{i+1} \cap H}{G_i \cap H}$ podgrupa abelove je abelova

2) $$\frac{\frac{G_{i+1} N}{N}}{\frac{G_i N}{N}} \cong \frac{G_{i+1} N}{G_i N} = \frac{G_{i+1} G_i N}{G_i N} \cong$$

$$\cong \frac{G_{i+1}}{G_{i+1} \cap G_i N} \cong \frac{\left(\frac{G_{i+1}}{G_i}\right)}{\frac{G_{i+1} \cap G_i N}{G_i}}$$ ← abelova

kvocient abelove je abelova

Trditev:

Naj bo G grupa in $N \trianglelefteq G$
če sta N in G/N rešljivi
je tudi G rešljiva

Dokaz: $\{1\} = N_0 \trianglelefteq \dots \trianglelefteq N_k = N$

N_{i+1}/N abelova

$\{1\} = \frac{M_0}{N} \Rightarrow M_0 = N$

$$\frac{M_0}{N} \trianglelefteq \frac{M_1}{N} \trianglelefteq \dots \trianglelefteq \frac{M_l}{N} = \frac{G}{N}$$
$$= G$$

$\frac{M_{i+1}/N}{M_i/N}$ abelova $\cong \frac{M_{i+1}}{M_i}$ je abelova

Verska za G

$$\{1\} \trianglelefteq N_0 \trianglelefteq \dots \trianglelefteq N_k = M_0 \trianglelefteq M_1 \trianglelefteq \dots \trianglelefteq M_l = G$$

■

Opomba: Izkaže se da so vse grupe lihe moči rešljive

(Feit-Thompsonov izrek)

DN. G je končna p-grupa potem je rešljiva

Nasvet $Z(G) \neq \{1\}$. Indukcija po $|G|$

Kolobarj: polinomov (nad polji)

$\mathbb{F}$ bo vedno polje

Pravimo da je $p(x)$ stopnje n ko

$$p(x) = a_n x^n + \dots + a_0 \quad a_n \neq 0$$

Stopnja ničelnega polinoma je $-\infty$

Opazimo:

$$st(p(x) \cdot g(x)) = st(p(x)) + st(g(x))$$

(ker produkt dveh neničelnih ni nenič.)

Ker je $\mathbb{F}$ polje

Opomba: $\mathbb{Z}_4[x]$

$$p(x) = 2x^2 + 1$$
$$g(x) = 2x^3 + 1$$

$$st(p(x) \cdot g(x)) = 3 \neq st(p(x)) + st(g(x))$$

Posledica:

Kadarkoli $F[x]$ je brez deliteljev niča

Obrnljivi elementi $F[x]$ so natanko neničelni konstantni polinomi:

Dokaz: sledi iz formule za $st(p(x) \cdot g(x))$

Izrek: Osnovni izrek o deljenju polinomov

Za poljubna polinoma $f(x)$ in $g(x)$ iz $\mathbb{F}[x]$, $g(x) \neq 0$, obstajata enolično določena polinoma $k(x)$ in $r(x)$ da je

$$f(x) = k(x) \cdot g(x) + r(x)$$

$$st(r(x)) < st(g(x))$$

Dokaz: $f(x) = a_m x^m + \dots + a_0 \quad ; a_m \neq 0$

(BSZS $f(x) \neq 0$)

$g(x) = b_n x^n + \dots + b_0 \quad ; b_n \neq 0$

Indukcija po m

(BSZS $m \geq n$ (če $m < n$, potem $k(x) = 0$ in $r(x) = f(x)$))

Baza indukcije: $m = 0$

$$a_0 = (a_0 b_0)^{-1} \cdot b_0 \neq 0 \quad (\text{ker smo v } \mathbb{F})$$

Recimo da velja za vse polinome stopnje $< m$

$$a_m \cdot b_n^{-1} x^{m-n} \cdot g(x) = a_m x^m + \dots$$

$$f(x) - a_m b_n^{-1} x^{m-n} \cdot g(x) \quad \text{polinom stopnje } < m$$

$$f(x) - a_m b_n^{-1} x^{m-n} \cdot g(x) = k_1(x) \cdot g(x) + r(x)$$

$$f(x) = \underbrace{(k_1(x) + a_m b_n^{-1} x^{m-n})}_{k(x)} g(x) + r(x)$$

Enoličnost:

$$f(x) = k_1(x) g(x) + r_1(x) = k_2(x) g(x) + r_2(x)$$

$$st(r_1(x)) < st(g(x))$$
$$st(r_2(x)) < st(g(x))$$

$$(k_1(x) - k_2(x)) \cdot g(x) = r_2(x) - r_1(x)$$

Primerjamo stopnji:

$$st(r_2(x) - r_1(x)) < st g(x)$$

$$st((k_1(x) - k_2(x)) \cdot g(x)) \geq st(g(x)) \text{ če } k_1 - k_2 \neq 0$$

Torej $\Rightarrow k_1 = k_2 \Rightarrow r_2 = r_1$

■

Posledica: $\forall$ ideal v kolobarju $\mathbb{F}[x]$ je glavni: (generiran z enim elementom)

($I=(a)$ $I=\{ka; k\in K\}$ ker je K komutativen)

Dokaz:

$I \triangleleft F[x]$ poljuben ideal

$I=\{0\} \Rightarrow I=(0)$

$I=\mathbb{F}[x] \Rightarrow I=(1)$

$I \notin \{\{0\}, \mathbb{F}[x]\}$

V I lahko najdemo neničeln polinom $p(x)$ najnižje možne stopnje

Trdimo $I=(p(x))$

Vzemimo poljuben $f(x)\in I$

$$\underbrace{f(x)}_{\in I} = \underbrace{k(x)\cdot p(x)}_{\in I} + r(x) \Rightarrow r(x)\in I$$

$st(r(x)) < st(p(x))$

$\Rightarrow r(x)=0 \Rightarrow$

$f(x)=k(x)\cdot p(x)$

če $p(x) \in \mathbb{F}[x]$ $a \in \mathbb{F}$ $p(x) = \sum_{j=0}^{n} a_j x^j$

$p(a) = \sum_{j=0}^{n} a_j a^j \in \mathbb{F}$

a je ničla polinoma $p(x)$, če je $p(a) = 0$

Opomba: $p(x)$ ..... abstraktna vsota potenc x^j

Polinom lahko gledamo kot $p: \mathbb{F} \to \mathbb{F}$, $a \mapsto p(a)$

(polinomska funkcija)

Polinomov ne moremo identificirati s polinomskimi funkcijami:

$\mathbb{Z}_2[x]$

$p(x) = 0$ $\quad g(x) = x^{2025} + x$

različna polinoma

$p: \mathbb{Z}_2 \to \mathbb{Z}_2$

$0 \mapsto 0$

$1 \mapsto 0$

$g: \mathbb{Z}_2 \to \mathbb{Z}_2$

$0 \mapsto 0$

$1 \mapsto 0$

Trditev: $p(x) \in \mathbb{F}[x]$ $a \in \mathbb{F}$

a je ničla polinoma $p \Leftrightarrow$ polinom $(x-a)$ deli $p(x)$

Dokaz: $p(x) = k(x) \cdot (x-a) + r(x)$ ← konstanta

a ničla $p(x)$

$p(a) = k(a) \cdot 0 + r = 0$

$\Leftrightarrow r = 0$

∎

Posledica:

$p(x) \in \mathbb{F}[x]$ neničelen

potem je v $\mathbb{F}$ kvečjemu $st(p(x))$ ničel polinoma

Dokaz: indukcija po stopnji

nerazcepni polinomi

Def: Naj bo $p(x) \in \mathbb{F}[x]$ stopnje ≥ 1

Pravimo da je $p(x)$ nerazcepen nad $\mathbb{F}$, če iz enakosti $p(x) = g(x)h(x)$, $g(x), h(x) \in \mathbb{F}[x]$

sledi da je eden od $g(x)$ in $h(x)$ konstanten

Primeri:

$\mathbb{C}[x]$ nerazcepni polinomi so natanko linearni polinomi

$\mathbb{R}[x]$ linearni polinomi in kvadratni polinomi brez nicel

Trditev:

Naj bo $p(x) \in \mathbb{F}[x]$ stopnje ≥ 1

a) če $st(p(x)) = 1 \Rightarrow p(x)$ je nerazcepen

b) če je $st\,p(x) \geq 2$ in je $p(x)$ nerazcepen, potem $p(x)$ nima ničle v $\mathbb{F}$

c) če je $st(p(x)) = 2$ V $st(p(x)) = 3 \Rightarrow$ $p(x)$ je nerazcepen nad $\mathbb{F} \Leftrightarrow$ $p(x)$ nima ničle v $\mathbb{F}$

Od tu dalje gledamo $\mathbb{Q}[x]$

$p(x) \in \mathbb{Q}[x]$

Če $p(x)$ pomnožimo s skupnim menovalcem koeficientov dobimo polinom v $\mathbb{Z}[x]$

Def: $p(x) = a_n x^n + \dots + a_0 \in \mathbb{Z}[x]$ je primitiven polinom če so $a_0, a_1, \dots a_n$ tuja cela števila

Trditev: (Gaussova lema)
Produkt dveh primitivnih polinomov je spet primitiven polinom

Dokaz:
Naj bosta $p(x), g(x) \in \mathbb{Z}[x]$ primitivna

Recimo da $p(x) \cdot g(x)$ ni primitiven
zato obstaja neko praštevilo p, ki deli vse koeficiente polinoma $p(x) \cdot g(x)$

$p(x) \cdot g(x) \in p \cdot \mathbb{Z}[x] \lhd \mathbb{Z}[x]$

kaj je $\mathbb{Z}[x] / p\mathbb{Z}[x] \cong \mathbb{Z}_p[x]$

$\varphi : \mathbb{Z}[x] \longrightarrow \mathbb{Z}_p[x]$

$\sum a_j x^j \longmapsto \sum (a_j + p\mathbb{Z}) x^j$ je homomorfizem

je surjektiven

$\ker \varphi = p\mathbb{Z}[x]$

Torej $\mathbb{Z}[x] / p\mathbb{Z}[x] \cong \mathbb{Z}_p[x]$

$p(x)$ je primitiven $\Rightarrow p(x) \notin \ker \varphi$
$g(x)$ je primitiven $\Rightarrow g(x) \notin \ker \varphi$

$p(x) + p\mathbb{Z}[x]$ je neničeln element

$(p(x) + p\mathbb{Z}[x])(g(x) + p\mathbb{Z}[x]) =$

$p(x) \cdot g(x) + p\mathbb{Z}[x] = 0$

Torej $\mathbb{Z}[x] / p\mathbb{Z}[x]$ delitelje ničla torej
ima $\mathbb{Z}_p[x]$ delitelje ničla

Ker je $\mathbb{Z}_p[x]$ p-čje nima delitelja ničla $\lightning$

Izrek: Naj bo $f(x) \in \mathbb{Z}[x]$. Recimo da $f(x)$ ne moremo zapisati kot produkt dveh nekonstantnih polinomov v $\mathbb{Z}[x]$. Potem je $f(x)$ nerazcepen v $\mathbb{Q}[x]$.

Dokaz:

Recimo da $f(x) = g(x) \cdot h(x)$ $g(x), h(x) \in \mathbb{Q}[x]$

Dokazujemo: enod teh je konstanten

Znebimo se ulomkov:

k = skupni menovalec koeficientov $g(x)$

l = skupni — " — od $h(x)$

$k \cdot l \, f(x) = \underbrace{(kg(x))} \cdot \underbrace{(l \cdot h(f(x))}$

celi koeficienti $\in \mathbb{Z}[x]$

Dokaz (accesa)

$f(x) \in \mathbb{Z}[x]$

recimo $f(x) = g(x) \cdot h(x)$ ≈ skupni imenovalec l

↑ skupni imenovalec k

$$klf(x) = kg(x) \cdot l \cdot h(x)$$

d ... največji skupni delitelj koeficientov $f(x)$

d_1 ... -||- za $kg(x)$

d_2 ... -||- za $lh(x)$

$$kld f_0(x) = d_1 d_2 g_0(x) \cdot h_0(x)$$

primitivna

Po gaussovi lemi sta $g_0(x) \cdot h_0(x)$ primitivna.

Največji skupni koef $kld f_0(x) = kld$

-||- $d_1 d_2 g_0(x) h_0(x) = d_1 d_2$

Torej $d_1 d_2 = kld$

$f_0(x) = g_0(x) h_0(x)$

$f(x) = d f_0(x) = d g_0(x) h_0(x)$

Po predpostavki mora biti eden od polinomskih faktorjev konst

□

Izrek: (Eisenov kriterij)

Naj bo $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$

Naj bo p praštevila, za katero velja:

i) $p \nmid a_n$

ii) $p \mid a_{n-1}, \dots a_0$

iii) $p^2 \nmid a_0$

Potem je $f(x)$ nerazcepen nad $\mathbb{Q}[x]$

Dokaz:
Recimo da ton: res.
Po prejšnji trditvi: obstajata nekonstantna polinoma $g(x), h(x) \in \mathbb{Z}[x]$ da je

$f(x) = g(x) \cdot h(x)$

$g(x) = b_r x^r + \dots + b_0$

$h(x) = c_s x^s + \dots + c_0$

Primerjamo koeficiente

$b_0 \cdot c_0 = a_0$

ker $p \mid a_0$ in $p^2 \mid a_0 \Rightarrow p$ deli natanko enega od b_0, c_0. BSZS. $p \mid b_0$ $p \nmid c_0$

$a_n = b_r c_s$

ker $p \nmid a_n$ $p \nmid b_r, c_s$

Naj bo k najmanjši tak, da $p \mid b_0, \dots b_{k-1}$ in p ne deli b_k $k \leq r$

$$a_k = \underbrace{b_k \cdot c_0}_{\text{ni deljiv s } p} + \underbrace{b_{k-1} c_1 + \dots + b_0 c_k}_{\text{deljiv s } p}$$

$k < n \Rightarrow p \mid a_k$

$\times$

■

Primer:

p naj bo praštevilo

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \dots + x + 1 \in \mathbb{Z}[x]$$

Ta polinom ni razcepen nad $\mathbb{Q}$.

Eisensteinov kriterij ni uporaben. Ali pač?

Trik:

$$\Phi_p(x+1) = (x+1)^{p-1} + (x+1)^{p-2} + \dots + 1$$

Dovolj je pokazati, da je $\Phi_p(x+1)$ nerazcepen

$$(x-1)\,\Phi_p(x) = x^p - 1 \quad \text{premaknemo}$$

$$x\,\Phi_p(x+1) = (x+1)^p - 1$$

$$\Phi_p(x+1) = x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \dots + \binom{p}{p-2}x + \binom{p}{p-1}$$

$\binom{p}{1} \dots \binom{p}{p-1}$ so deljivi s p

1 ni deljiv s p

Po Eisensteinu je $\Phi_p(x+1)$ nerazcepen nad $\mathbb{Q}$, torej isto velja za $\Phi_p(x)$

Iz zveze $(x-1)\,\Phi_p(x) = x^p - 1$ vidimo

$$\Phi_p(x) = \prod_{k=1}^{p-1} (x - \omega_k)$$

$$\omega_k = \cos\frac{2k\pi}{p} + i\sin\frac{2k\pi}{p} = e^{i\frac{2k\pi}{p}}$$

↳ primitivni p-ti koreni enote

za splošen n:

$$\Phi_n(x) = \prod (x - \omega_k)$$

$$\omega_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} = e^{i\frac{2k\pi}{n}}$$

kjer sta k in n tuja

Izkaže se $\Phi_n(x)$ so tudi celoštevilski polinomi in so tudi nerazcepni nad $\mathbb{Q}$

$\Phi_n(x)$... ciklotomični polinom

Razširitve polj

Definicija. Naj bosta K in F polja: $F \subseteq K$.
Potem pravimo da je polje K razširitev polja F, oznaka K/F

Zgledi:

$\mathbb{R}/\mathbb{Q}$ $\mathbb{R}$ je razširitev polja $\mathbb{Q}$

$\mathbb{C}/\mathbb{R}$, $\mathbb{C}/\mathbb{Q}$

$\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2};\ ab \in \mathbb{Q}\}$ je polje

$\mathbb{Q}(\sqrt{2})/\mathbb{Q}$

Motivacija $\mathbb{R}/\mathbb{Q}$

Lepa iracionalna števila: $\sqrt{2}$

$\sqrt{2}$ je ničla polinoma $x^2 - 2 \in \mathbb{Q}[x]$

Grda iracionalna števila: π

π ni: ničla neničelnega polinoma v $\mathbb{Q}[x]$

Def: Naj bo K/F razširitev polj, $a \in K$.

Pravimo:

a) a je algebraičen, če obstaja polinom $p(x) \in F[x]$, da je $p(a) = 0$

b) a je transcendenten nad F, če ni algebraičen nad F

Primer:

$\sqrt{2}$ je algebraičen nad $\mathbb{Q}$ in π je transcendenten nad $\mathbb{Q}$

Definicija: Naj bo K/F razširitev polj

$a \in K$ naj bo algebraičen nad F

Polinom $p(x) \in F[x]$, ki ima vodilni koeficient 1 velja da je $p(a) = 0$ in je najmanjše stopnje med tistimi neničelnimi polinomi, ki imajo a za ničlo imenujemo **minimalni polinom** elementa a nad F

DN: minimalni polinom je enolično določen

Trditev:

Naj bo K/F razširitev polj, $a \in K$ naj bo algebraičen nad F. Naj bo $p(a)=0$. $p(x) \in F[x]$

Naslednje trditve so ekvivalentne:

i) $p(x)$ je minimalni polinom za a

ii) $p(x)$ je nerazcepen nad F

iii) $p(x)$ deli vsak polinom $f(x) \in F[x]$, za katerega je $f(a)=0$

Dokaz:

i) $\Rightarrow$ ii) če je $p(x)$ razcepen:

$p(x) = g(x) \cdot h(x)$ $g(x), h(x) \in F[x]$ nekonstantna

$p(a) = g(a) \cdot h(a) = 0 \Rightarrow$

$h(a)=0 \vee g(a)=0$

če na primer $g(a)=0$ je $g(x)$ polinom, ki ima nižjo stopnjo kot $p(x)$ in uniči a $\lightning$

ii) $\Rightarrow$ iii)

$I = \{ f(x) \in F[x] : f(a)=0 \}$

I ideal v $F[x]$. I je zato glavni ideal (ker je generiran zgolj z enim elementom)

$\exists p_1(x): I = (p_1(x)) = \{ k(x) p_1(x) : k(x) \in F[x] \}$

$p(x) \in I \Rightarrow p(x) = k(x) \cdot p_1(x)$ $\quad p_1(a)=0$

Zaradi nerazcepnosti je $k(x)$ konstanten zato $I = (p(x))$

Sledi da je $\forall f(x) \in I$ večkratnik $p(x)$

iii) $\Rightarrow$ i)

Če $p(x)$ ni minimalen polinom $\exists g(x) \in F[x]$ neničelen, $st(g(x)) < st(p(x))$ in $g(a)=0$

Po predpostavki $p(x) \mid g(x)$ $\lightning$ (stopnje

Def: K/F $a \in K$ naj bo alg nad F

$p(x)$ naj bo minimalen polinom a-ja nad F

če $st(p(x)) = n$ pravimo da je

a algebraičen stopnje n

Zgled:

① K/F alg. elementa stopnje 1 = ničle lin. polinoma $x-a$ $a \in F$

to so natanko elementi F

② $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$

$\sqrt{2}$ je ničla $x^2-2 \in \mathbb{Q}[x]$

to je minimalni polinom

$\sqrt{2}$ je algebraičen stopnje 2 nad $\mathbb{Q}$

③ $\mathbb{C}/\mathbb{R}$

i je ničla polinoma x^2+1

i je algebraičen stopnje 2 nad $\mathbb{R}$

Splošno je: $\forall z \in \mathbb{C}$ je algebraičen nad $\mathbb{R}$ stopnje 1 ali 2

z je ničla $x^2 - (z+\bar{z})x + z\bar{z} \in \mathbb{R}[x]$

$= (x-z)(x-\bar{z})$

④ $\mathbb{R}/\mathbb{Q}$ $\sqrt{2}+\sqrt{3}$ algebraičen nad $\mathbb{R}$?

$a = \sqrt{2}+\sqrt{3}$

$a^2 = 5 + 2\sqrt{6}$ $/\cdot 12$

$a^4 = 49 + 20\sqrt{6}$

$a^4 - 10a^2 + 1 = 0$

$\sqrt{2}+\sqrt{3}$ je ničla polinoma $x^4 - 10x^2 - 1 \in \mathbb{Q}[x]$

DN: to je minimalni polinom $\sqrt{2}+\sqrt{3}$ nad $\mathbb{Q}$

Končne razširitve polj

K/F naj bo razširitev polj

V K imamo seštevanje

Če elemente iz F imenujemo skalarji in elemente K-ja vektorji, imamo definirano množenje s skalarjem:

$$F \times K \longrightarrow K$$
$$(\alpha, k) \longmapsto \alpha k$$

K lahko gledamo kot vektorski prostor nad F

Def: <u>razširitev polj</u> K/F je <u>končna</u>, če je K končnorazsežen vektorski prostor nad F

Označimo:
$\dim_F K = [K:F]$ ... stopnja razširitve

Zgled:

- $\mathbb{C}/\mathbb{R}$:

  Baza $\mathbb{C}$ nad $\mathbb{R}$: $\{1, i\}$

  $[\mathbb{C}:\mathbb{R}] = 2$

- $[\mathbb{R}:\mathbb{Q}] = \infty$

  Recimo $[\mathbb{R}:\mathbb{Q}] < \infty$

  $\{r_1 \dots r_n\}$ baza $\mathbb{R}$ nad $\mathbb{Q}$

  $\forall r \in \mathbb{R}\ r = \underbrace{q_1 r_1 + \dots + q_m r_n}$

  samo števno neskončno možnosti

Trditev:

$F \subseteq L \subseteq K$ naj bodo Pdjs

Naj bosta L/F in K/L konen. razširitvi, Potem je K/F konč.

in velja $[K:F] = [K:L] \cdot [L:F]$

Dokaz: Baza L-ja kot vekt. prost. nad F: $\{a_1, \ldots, a_m\}$

Baza K-ja kot vek.pr. nad L: $\{b_1, \ldots, b_n\}$

$B = \{a_i b_j \; ; i \in \{1 \ldots m\}, j \in \{1, \ldots, n\}\}$ je baza K nad F

K lahko razvijemo po $b_1 \ldots b_n$ nad L

$k = \lambda_1 b_1 + \lambda_2 b_2 + \ldots + \lambda_n b_n \quad \lambda_i \in L$

$\lambda_i \in L \Rightarrow$ lahko razvijemo po a nad F

$\lambda_i = \rho_{i1} a_1 + \ldots + \rho_{im} a_m \quad \rho_{ij} \in F$

$k = \rho_{11} a_1 b_1 + \rho_{12} a_2 b_1 + \ldots + \rho_{nm} a_m b_n$

linearna neodvisnost:

$\sum \sum \rho_{ij} a_j b_i = 0 \quad \rho_{ij} \in F$

$\sum (\underbrace{\sum \rho_{ij} a_j}_{\in L}) b_i = 0$

$\Rightarrow \sum \rho_{ij} a_j = 0 \Rightarrow \rho_{ij} = 0$ za $\forall ij$

Def: Razširitev K nad F je **algebraična**, če je $\forall a \in K$, algebraičen nad K (je rešitev neke polinomske enačbe) in **transcendentna** če ni algebraična

Trditev: Vsaka končna razširitev K/F je algebraična

Dokaz: Recimo da $a \in K$ ni algebraična nad F
$1, a, a^2, \ldots$ so linearno neodvisni nad F
$\lightning$ ker je $\dim K/F$ končna

∎

Oznaka: $K/F \quad a \in K$

$F[a]$ = najmanjše podkolobar v K, ki vsebuje F in a = podkolobar v K generiran z F in a

$F[a] = \{p(a);\ p(x) \in F[x]\}$

$F(a)$ = podpolje v K generirano z F in a

$F(a) = \{xy^{-1};\ x \in F[a],\ y \in F[a] - \{0\}\}$

Podobno lahko definiramo

$F[a_1 \dots a_n]$, $F(a_1 \dots a_n)$

$F[a_1 \dots a_n] = F[a_1 \dots a_{n-1}][a_n]$

Def: Razširitev K/F je primitivna, če $\exists a \in K$. da je $K = F(a)$

Zgled: $\mathbb{Q}[\sqrt{2}] = \{\alpha + \beta\sqrt{2} ; \alpha, \beta \in \mathbb{R}\}$

$\mathbb{Q}(\sqrt{2})[\alpha + \beta\sqrt{2} ; \alpha, \beta \in \mathbb{R}\} = \mathbb{Q}[\sqrt{2}]$

Isto je, ker je $\sqrt{2}$ algebraična

Izrek: Naj bo K/F razširitev polj in naj bo $a \in K$ algebraičen nad F stopnje n. Potem je $F(a) = F[a]$ in velja $[F(a) : F] = n$

Dokaz:

Naj bo $p(x) \in F[x]$ minimalni polinom a-ja $st(p(x)) = n$

Dovolj je pokazati da je vsak neničeln element v $F[a]$ obrnljiv

$f(a) \neq 0 \quad f(x) \in F[x]$

Zaradi minimalnosti $p(x)$ sledi da sta $f(x)$ in $p(x)$ tuja polinoma

Zato obstajata polinoma $r(x)$ in $s(x)$ v $F[x]$ da

$$f(x)r(x) + p(x)\cdot s(x) = 1$$

(iz razširjenega evklidovega algoritma)

Izračunamo v a:

$$f(a)\cdot r(a) = 1$$

$r(a)$ je inverz $f(a)$-ja

še drugi del:

$$F(a) = \{ f(a) : f \in F[x] \}$$

$p(a) = a$

$p(x) = x^n + \alpha_{n-1}x^{n-1} + \dots \alpha_1 x + \alpha_0$

a^n je linearna kombinacija $1, a, a^2, \dots a^{n-1}$

$m \geq n \Rightarrow a^m$ tudi lin kombinacija $1, a \dots a^{n-1}$

$1, a, a^2, \dots a^{n-1}$ je ogrodje $F(a)$ nad F

Zaradi minimalnosti $p(x)$ so

$1, a, \dots a^{n-1}$ lin. neodvisni

Torej $\dim_F F(a) = n$ ∎

Posledica:

Če K/F in $a_1, \dots, a_n \in K$ naj bodo algebraični nad F. Potem velja $F(a_1, \dots, a_n) = F[a_1, \dots, a_n]$ in velja

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

Zgledi:

1) $\mathbb{Q}(\sqrt[n]{p})$ $p \in \mathbb{P}$

Polinom z racionalnimi koeficienti ki ima $\sqrt[n]{p}$: $X^n - p$

Po eisensteinovem kriteriju je ta polinom nerazcepen nad $\mathbb{Q}$, zato je minimalni polinom $\sqrt[n]{p}$ nad $\mathbb{Q}$

Zato je sto pnja tega razširitve $= n$

2) K/F $a \in K$

eval: $F[X] \to F[a]$

$f(X) \mapsto f(a)$

je surjektivna $\Rightarrow$ je epimorfizem kolobarjev

$\ker \text{eval} = ?$

- Če je a transcendenten nad $F \Rightarrow \ker \text{eval} = \{0\}$
  a ni: ničla nekonstantnega neničelnega polinoma

Če je a transcendenten: $F[X] \cong F[a]$

- Če je a algebraičen nad $F \Rightarrow$
  Naj bo $p(X) \in F[X]$ naj bo njegov minimalni polinom: $p(a) = 0$
  Če je $f(X) \in \ker \text{eval} \Leftrightarrow f(a) = 0 \Leftrightarrow$
  $p(X) \mid f(X)$
  $\ker \text{eval} =$ večkratniki $p(X) = (p(X))$

  Toej alg $\Rightarrow \dfrac{F[X]}{(p(X))} \cong F[a] = F(a)$

Izrek: Naj bo K/F razširitev

$L = \{a \in K;\ a \text{ je algebraičen nad } F\}$

Potem je L podpolje v K

Dokaz: $a, b \in L$; a, b sta algebraična nad F

$F(a,b)$ je po posledici končne razširitve F

Po izreku (enem prej) je $F(a,b)/F$ algebraična razširitev, torej $F(a,b)/F \subseteq L$

Med drugim $a \cdot b \in L$, $a - b \in L$ in $a^{-1} \in L$ če $a \neq 0$

∎

Obrat ne velja (obstaja algebraična rešitev ki ni končna)

Primer: algebraična razširitev $\mathbb{Q}$-je, ki ni končna.

$\mathbb{C}/\mathbb{Q}$

$L = \{ a \in A ; \exists p(x) \in \mathbb{Q}[X] . p(a) = 0 \}$

L je podpolje v $\mathbb{C}$

$L/\mathbb{Q}$ je algebraična razširitev

$[L : \mathbb{Q}] = \infty$

Recimo da bi bila končna $[L : \mathbb{Q}] = m$

$\sqrt[n]{2} \in L$

$\mathbb{Q}(\sqrt[n]{2}) \subseteq L$ za $\forall n$

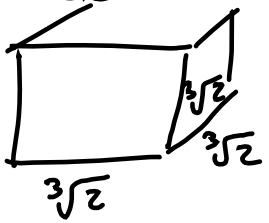
$$\underbrace{[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}]}_{= n} \mid [L : \mathbb{Q}] = m$$

m mora biti deljiv z vsakim naravnim številom

Konstrukcije z ravnilom in šestilom

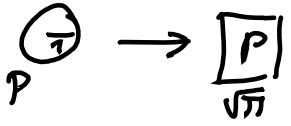


z ravnilom in šestilom narišemo kocko z 2x večjim volumnom



Podvojitev kocke

kvadratura kroga:



Ali lahko narišem kvadrat z isto ploščino

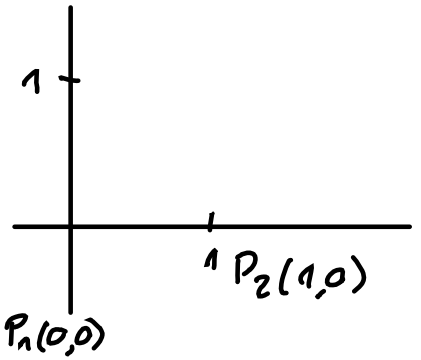
Trisekcija kota



Formulacja problema

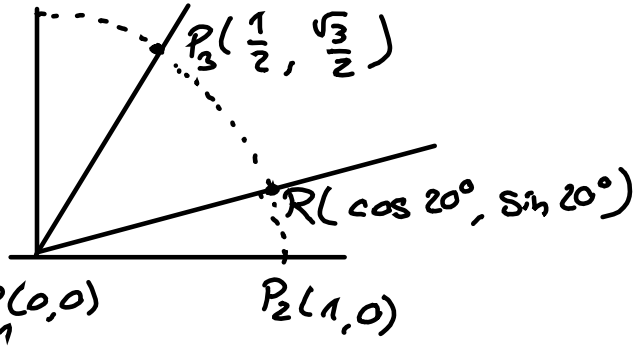
Motivacja





$\rightsquigarrow R(\sqrt[3]{2}, 0)$

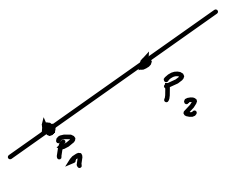
Trisekcja 60°



$P_1, P_2, \ldots, P_n \in \mathbb{R}^2$

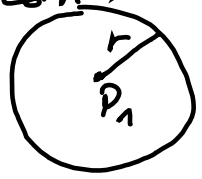
Konstrukcije:

- z ravnilom:



• cez dve tadi potegnemo premico

- s sestilom:





nove tocke: presecisca

Postopek

$\mathcal{P} = \{P_1, \ldots, P_n\}$

konstruiramo novo t. do A na enega od teh treh nacinov

$\mathcal{P} \leftarrow \mathcal{P} \cup \{A\}$

Ponovimo postopek

Izrek: Naj bo množica točk v $\mathbb{R}\times\mathbb{R}$

Recimo da je F podpolje v $\mathbb{R}$

da $\mathcal{P} \subseteq \mathbb{F}\times\mathbb{F}$

Recimo da je $A(a,b)$ konstruktibilna

s pomočjo točk iz $\mathcal{P}$

Potem sta ta dva elementa a, b algebraična

nad $\mathbb{F}$, s stopnjama razširitve, ki sta potenci

števila 2

Dokaz: Naj bo najprej $A(a,b)$ prva točka

v tej konstrukciji:

Trdimo: $[F(a,b):F] \in \{1,2\}$

(to je dovolj, ker potem se stopnja množi)

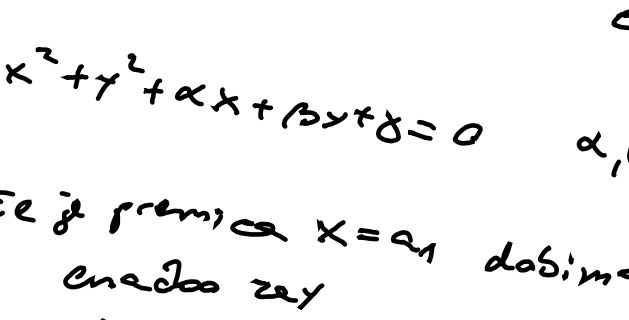
$[F(a,b)(c,d):F]$

uporej $([F(c,d):F(a,b)] \in \{1,2\} \Rightarrow \in \{1,2,4\}$

vtd

$A(a,b)$ smo dobili na enega od teh načinov

1) presečišče dveh premic



1. premica: $x=a_1$ ali: $y=k_1x+n_1$

2. premica: $x=a_2$ ali: $y=k_2x+n_2$

$a_2\ a_1 \in F$ $\quad k_1=\frac{y_2-y_1}{x_2-x_1} \in F$

$n_1=y_1-k_1x_1 \in F$

Presečišče dveh premic je rešitev linearnega

sistema enačb, ki imata koef. v $\mathbb{F}$

Rešitev $(a,b) \in \mathbb{F}\times\mathbb{F}$

$\Rightarrow [F(a,b):F]=1$

2) Presečišče premice in krožnice

premica: $x=a_1$ ali $y=k_1x+n_1$ $\quad a_1, k_1, n_1 \in F$

krožnica:



$$(x-x_1)^2 + (y-y_1)^2 = (x_3-x_2)^2 + (y_3-y_2)^2$$

x_1 ep, y_1 ep, desna stran ep

$$x^2+y^2+\alpha x+\beta y+\gamma=0 \qquad \alpha,\beta,\gamma \in F$$

Če je premica $x=a_1$ dobimo

enačbo za y

s koef. iz F

če je premica $y=k_1x+n_1$

dobimo kvadratno enačbo za x

s koef v F

$$\text{rešitev}_{1,2} = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$$

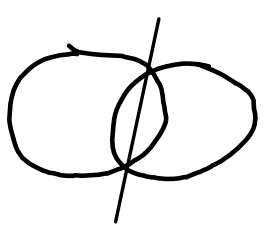
Rešitev je v $\mathbb{F}$, ki mu dodamo

ta korenček $(\sqrt{b^2-4ac})$

$\Rightarrow$ zato $[[F(a,b):F] = 2$ ali 1 (če kvadratni koren že v F)

3) 2 krožnici

-isto kot 2) ker



= presečišče krožnice in premice

Ponavljamo postopek

$\mathcal{P} \subseteq \mathbb{F}\times\mathbb{F}$

$A(a,b)$ konstruiramo $[F(a,b):F] \in \{1,2\}$

$\mathcal{P} \leftarrow \mathcal{P} \cup \{A\}$, $F \leftarrow F(a,b)$

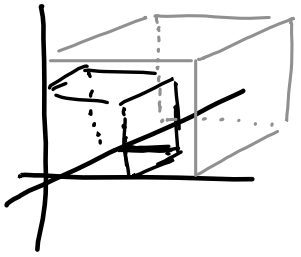
$B(c,d)$ $[F(a,b)(c,d):F(a,b)] \in \{1,2\}$

$[F(a,b)(c,d):F] =$

$[F(a,b)(c,d):F(a,b)] \cdot [F(a,b):F] \in \{1,2,4\}$

Posledica:

Kocke ne moremo podvojiti z ravnilom in šestilom

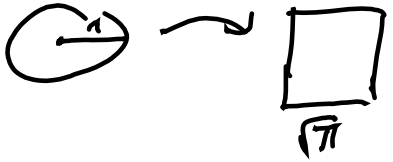


$P(0,0),\ P(1,0) \rightsquigarrow P_3(\sqrt[3]{2}, 0)$

$P_1, P_2 \in \mathbb{Q} \times \mathbb{Q}$

$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3 \neq 2^n$

Posledica: kvadratura kroga ni mogoča z ravnilom in šestilom



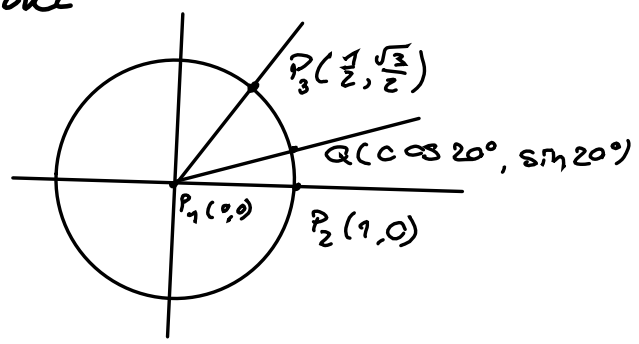
$P(0,0),\ P(1,0) \rightsquigarrow P_3(\sqrt{\pi}, 0)$

$[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}] = \infty$

π je transcendenten

Posledica: Kota $60°$ se ne more razdeliti na tri enake dele z ravn. in ščet.

Dokz



$\{P_1, P_2, P_3\} \subseteq \mathbb{Q}(\sqrt{3}) \times \mathbb{Q}(\sqrt{3})$

Če se Q da konstruirati potem

$[\mathbb{Q}(\sqrt{3}, \cos 20°) : \mathbb{Q}(\sqrt{3})] = 2^k$

$\cos 3\varphi = 4\cos^3\varphi - 3\cos\varphi \qquad \varphi = 20°$

$\cos 20° = a$

$\frac{1}{2} = 4a^3 - 3a$

$8a^3 - 6a - 1 = 0$

a je ničla polinoma $p(x) = 8x^3 - 6x - 1$

Trdimo da je $p(x)$ nerazcepen nad $\mathbb{Q}(\sqrt{3})$

Recimo da je razcepen nad $\mathbb{Q}(\sqrt{3})$.

Ker je stopnje 3 mora imeti neko ničlo v $\mathbb{Q}(\sqrt{3})$

$\alpha + \beta\sqrt{3}$ je ničla tega polinoma $\alpha, \beta \in \mathbb{Q}$

Tr.k: $(2x)^3 - 3 \cdot 2x - 1 = 0$

BSZS: $\alpha + \beta\sqrt{3}$ je ničla polinoma $y^3 - 3y - 1 = 0$

$(\alpha + \beta\sqrt{3}) - 3(\alpha + \beta\sqrt{3}) - 1 = 0$

$\alpha^3 + 3\alpha^2\beta\sqrt{3} + 9\alpha\beta^2 + 3\beta^3\sqrt{3} - 3\alpha - 3\beta\sqrt{3} - 1 = 0$

$\alpha^3 + 9\alpha\beta^2 - 3\alpha - 1 + \sqrt{3}(3\alpha^2\beta + 3\beta^3 - 3\beta) = 0$

Dob.mo $\alpha^3 + 9\alpha\beta^2 - 3\alpha - 1 = 0$ in

$\beta(3\alpha^2 + 3\beta^2 - 3) = 0$

1) $\beta = 0 \Rightarrow \alpha^3 - 3\alpha - 1 = 0$ nima racion. ničel!

2) $\alpha^2 + \beta^2 = 1 \Rightarrow$ vstavimo v prvo enačbo in dobimo enačbo 3 stopnje brez rac. reš.

Sklep: $p(x)$ je res nerazcepen nad $\mathbb{Q}(\sqrt{3})$

Torej je $[\mathbb{Q}(\sqrt{3}, \cos 20°) : \mathbb{Q}(\sqrt{3})] = 3$

Razpadna polja polinomov

Motivacija: $X^2-2 \in \mathbb{Q}[X]$ nima ničel v $\mathbb{Q}$

Če gledamo $x^2-2 \in \mathbb{R}[X]$ ga lahko razcepimo na linearne faktorje

Splošno: $f(x) \in F[X]$, naj obstaja neka razširitev K/F, da ima $f(x)$ neko ničlo $a \in K$

$f(x)$ lahko gledamo kot polinom v $K[X]$:

$$f(x) = (x-a) \cdot f_1(x) \quad ; \quad f_1(x) \in K[X]$$

Očitno: K/F, $f(x) \in F[X]$, $st f(x) = n \Rightarrow$

K vsebuje kvečjemu n ničel $f(x)$

Trditev: Naj bo $f(x) \in F[x]$ nekonst. polinom. Potem obstaja K/F, ki vsebuje vsaj eno ničlo polinoma $f(x)$

Dokaz:

Naj bo $p(x)$ nerazcepen $\in F[x]$ polinom, ki deli $f(x)$; stopnja $p(x) > 1$ BSZS

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

K je polje

$g(x) + (p(x)) \in F[x]/(p(x))$ neničeln element

$g(x) \notin (p(x))$. Ker je $p(x)$ nerazcepen, je največji skupni delitelj $g(x)$ in $p(x)$ enak 1

$a(x), b(x) \in F[x]$

$$g(x) \cdot a(x) + p(x) \cdot b(x) = 1$$

$$(g(x) + (p(x)))(a(x) + (p(x))) = g(x)a(x) + (p(x)) = 1 + (p(x))$$

$g(x) + (p(x))$ je obrnljiv

K vsebuje F, ker

$F \longrightarrow F[x]/(p(x))$

$\alpha \longmapsto \alpha + (p(x))$ je monomorfizem

$f(x) \in F[x]$ lahko gledamo kot polinom v $K[x]$

$f(x) = \sum a_k x^k \rightsquigarrow \sum (a_k + (p(x))) \cdot x^k$

Kateri element K je ničla tega polinoma

$x + (p(x)) \in K$

$$f(x + (p(x))) = \sum (a_k + (p(x)))(x^k + (p(x))) =$$

$$= \sum a_k x^k + (p(x)) = f(x) + (p(x)) = (p(x))$$

∎

Posledica: $f(x) \in F[x] \Rightarrow \exists$ polje $K \geq F$, da

$f(x) = c(x-a_1)(x-a_2)\cdots(x-a_n)$

$a_i \in K \quad c \in F$

Def: $f(x) \in F[x]$ <u>razpade</u> nad poljem K, če ga lahko v $K[x]$ lahko razstavimo na linearne faktorje

Def: za $f(x) \in F[x]$ je polje K <u>razpadno polje</u> če $f(x)$ razpade nad K in ne razpade nad nobenim manjšim poljem v K

Opomba: Razpadno polje polinoma vedno obstaja

Po posledici $\exists K$ ki vsebuje vse ničle $a_1 \ldots a_n$ polinoma $f(x) \in F[x]$

Razpadno polje je polje $F(a_1, \ldots a_n)$

Koliko je razpadnih polj

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

$\mathbb{Q}(\sqrt{2})$ je razpadno polje

$\mathbb{Q}[x] / (x^2 - 2) \cong \mathbb{Q}(\sqrt{2})$

Vsa razpadna polja so med seboj izomorfna

Opomba: Razpadno polje polinoma $f \in F[x]$ je končna razširitev polja F

Oznaka: Naj bosta F, F' polji:

$\varphi : F \to F'$ homomorfizem

$f(x) \in F[x] : f(x) = \sum_{k=1}^{n} a_k x^k \quad a_k \in F$

$F_\varphi[x] = \sum_{k=1}^{n} \varphi(a_k) x^k \in F'[x]$

Lema: $p(x) \in F[x]$ nerazcepen polinom

$a \in K$ nej bo nicla $p(x)$

$\varphi: F \longrightarrow F'$ nej bo izomorfizem polj

Polinom $p_\varphi(x) \in F'[x]$ nej ima neko nicla

$a' \in K'$

Potem dobimo natanko en izomorfizem

$\Phi: F(a) \longrightarrow F'(a')$ da

$\Phi_{/F} = \varphi$ in $\Phi(a) = a'$

Oblike so linearna kombinacija teh dveh

Dokaz: $p(x)$ je minimalni polinom a-ja

Ker je φ izomorfizem je $p_\varphi(x)$ minimalni polinom a'

$$\begin{array}{ccc} F[x]/(p(x)) & \xrightarrow{\tilde{\varepsilon}}_{\cong} & F(a) \\ \downarrow \pi & & \vdots \Phi \\ F'[x]/(p_\varphi(x)) & \xrightarrow[\cong]{\tilde{\varepsilon}} & F'(a') \end{array}$$

$\varepsilon: F[x] \to F(a)$ evaluacijski homomorfizem

Definirajmo $\Pi: F[x]/(p(x)) \longrightarrow F'[x]/(p_\varphi(x))$

$$f(x) + (p(x)) \longmapsto f_\varphi(x) + (p_\varphi(x))$$

DN: Π je izomorfizem polj

$\Phi = \tilde{\varepsilon} \circ \Pi \circ \tilde{\varepsilon}^{-1}$

Endiorost:

$\Phi(\sum \lambda_k a^k) = \sum \Phi(\lambda_k)\Phi(a^k) = \sum \varphi(\lambda_k) a'^k$

Recimo da imamo še en tak izomorfizem $\tilde{\Phi}$

$\tilde{\Phi}(\sum \lambda_k a^k) = \sum \tilde{\Phi}(\lambda_k)\tilde{\Phi}(a^k) = \sum \varphi(\lambda_k) a'^k$

Izrek: F, F' nej bosta polj:

$\varphi: F \xrightarrow{\sim} F'$ $f(x)$ nej bo nekonstanten polinom v $F(x)$ K nej bo razpadno polje $f(x)$ K' nej bo razpadno polje polinoma $f_\varphi(x) \in F'(x)$. Potem obstaja izomorfizem $\bar{\varphi}: K \to K'$

Posledica: Če je $f(x) \in F[x]$ nekonstanten polinom sta poljubni razpadni polji polinoma $f(x)$ izomorfni:

Dokaz: Uporabimo izrek za $F' = F$ $\varphi = id_F$

Dokaz:

Indukcija po $n = [K:F]$

$n = 1: K = F \overset{1:1}{\Rightarrow} K' = F'$

$n > 1$: $f(x)$ ne razpade na linearne faktorje nad F

Naj bo $p(x) \in F[x]$ nerazcepen polinom ki deli $f(x)$: $st(p(x)) > 1$

K vsebuje neko ničlo a polinoma $p(x)$, ker je razcepno polje $f(x)$

Podobno K' vsebuje ničlo a' polinoma $f_\varphi(x) \in F'[x]$

Po ker obstaja natanko en izomorfizem

$\bar{\Phi}: F(a) \to F'(a')$

$\bar{\Phi}_{/F} = \varphi$

$\bar{\Phi}(a) = a'$

K je razcepno polje $f(x)$ tudi nad $F(a)$

podobno je K' razcepno polje nad $f_\varphi(x)$ nad $F'(a')$

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

(p a minimalni polinom $p(x)$)

Po ind. pred. obstaja izomorfizem

$\bar{\Phi}^*: K \to K'$

$\bar{\Phi}^*_{/F(a)} = \bar{\Phi}$

$\bar{\Phi}^*_{/F} = \bar{\Phi}_{/F} = \varphi$

Normalne razširitve polj

Def: Naj bo K/F razširitev polj.
Pravimo, da je ta razširitev normalna, če za vsak nerazcepen polinom $p(x) \in F[x]$ velja ena od možnosti:

1) $p(x)$ ima vse ničle v K
2) $p(x)$ nima nobene ničle v K

Izrek: Naj bo K/F končna razširitev.

K/F je normalna razširitev $\Leftrightarrow$

$\Leftrightarrow$ K je razpadno polje nekega polinoma iz $F[X]$

Dokaz:

$\Rightarrow$ K/F naj bo normalna. $K = F(a_1 \dots a_n)$

Naj bo $p_i(x)$ minimalni polinom od a_i.

Po definiciji normalnosti K vsebuje vse ničle polinoma $p_i(x)$

$$f(x) := p_1(x)\, p_2(x) \dots p_m(x)$$

Naj bo L razpadno polje $f(x)$

$K = L$

$a_1 \dots a_n$ so ničle $f(x) \Rightarrow$

$a_1 \dots a_n \in L \Rightarrow F(a_1 \dots a_n) \subseteq L \Rightarrow K \subseteq L$

$L \subseteq K$

ker K vsebuje vse ničle $f(x)$, L pa je najmanjši tak, ki vsebuje vse ničle $f(x)$ po definiciji: $L \subseteq K$

$\Leftarrow$ K naj bo razpadno polje $f(x) \in F[x]$

Izberemo poljuben nerazcepen polinom $p(x) \in F[x]$.

Naj bo a ničla polinoma $p(x)$, ki leži v K. Naj bo b poljubna druga ničla polinoma $p(x)$

$b \in K$

$p(x)$ je minimalni polinom za a in b

Identično preslikavo $F \to F$ lahko razširimo do izomorfizma $\Phi: F(a) \xrightarrow{\sim} F(b)$

$$\Phi_{/F} = id \qquad \Phi(a) = b$$

K razp. polje $f(x)$

$p(x)$ nerazcepen z $a \in K$ ničlo

b poljuba ničla $p(x)$

Razpadno polje polinoma $f(x)$ nad

$F(a)$: $F(a, a_1, \dots, a_n) = K$

$\uparrow K$

nad $F(b)$: $F(b, a_1 \dots a_n) = K'$

Po izreku obstaja

$$\Phi^*: K \to K'$$

$$\Phi^*_{/F(a)} = \Phi$$

$$\Phi^*(a) = b$$

$a \in K = F(a_1, \dots a_b)$

$a =$ „polinom“ v $a_1, \dots a_n$

$b = \Phi^*(a) \Rightarrow b$ je polinom v $a_1 \dots a_n$ — ker ;d

Torej $b \in F(a_1 \dots a_n) = K$

Zgled:

① $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ je normalna, ker je

$\mathbb{Q}$ razpadno polje $x^2-2 \in \mathbb{Q}[x]$

② $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ ni normalna, ker

$\sqrt[3]{2}$ je nicla $x^3-2 \in \mathbb{Q}[x]$ nerazcepen

Toda $\mathbb{Q}(\sqrt[3]{2})$ ne vsebuje vseh nicel

x^3-2

③ p praštevilo, $\varepsilon = e^{\frac{2\pi i}{p}}$ (primitivna p-ta

koren enote)

$\mathbb{Q}(\varepsilon)/\mathbb{Q}$ je normalna, ker

$\mathbb{Q}(\varepsilon)$ razpadno polje x^p-1

↳ nicle tega polinoma

so $\varepsilon, \varepsilon^2, \ldots \varepsilon^{p-1}, 1$

Vse nicle živijo v $\mathbb{Q}(\varepsilon)$

Algebraično zaprtje polja

Def: A polje. Pravimo da je A **algebraično zaprto** če ima $\forall$ nekonst. polinom

$f \in A[x]$ vsaj eno ničlo

Ekvivalentno: $f(x) = c(x-a_1)\dots(x-a_n)$; $c, a_i \in A$

Lema: $F \subseteq L \subseteq K$ naj bodo polja, L/F algebraična. Naj bo $a \in K$ algebraičen nad L. Potem je a algebraičen nad F

Dokaz:

Po definiciji: $\exists\, p(x) \in L[x]$, $p(a) = 0$

$p(x) = \sum a_k x^k$ $\quad a_k \in L$

$\tilde{F} = F(a_1, \dots, a_n)$, $p(x) \in \tilde{F}[x] \Rightarrow$ a algebraičen nad $\tilde{F}$

$[\tilde{F}(a) : F]$ dovolj je dokazati da je to $< \infty$

$[\tilde{F}(a) : F] = \underbrace{[\tilde{F}(a) : \tilde{F}]}_{<\infty} \cdot [\tilde{F} : F]$

ker je a alg. nad $\tilde{F}$

L/F algebraična, $a_k \in L \Rightarrow a_k$ algebr nad F

$\Rightarrow [F(a_1 \dots a_n) : F] < \infty = [\tilde{F} : F] < \infty \Rightarrow$

$[\tilde{F}(a) : F] < \infty$ ∎

Def: Naj bo F polje. Algebraično zaprtje polja F je takšno algebraično zaprto polje $\bar{F}$, ki vsebuje F in je $\bar{F}/F$ algebraično

(DN: $\bar{F}$ je najmanjše algebraično zaprto polje, ki vsebuje F)

Opomba: Da se pokazati da je vsako polje vsebovano v nekem algebraičnem zaprtem polju.
Da se pokazati da algebraično zaprtje polja vedno obstaja in je do izomorfizma enolično določeno

Primer

$\mathbb{R}$:

$\mathbb{C}$ je alg zaprto

$\mathbb{R} \subseteq \mathbb{C}$ $\quad \mathbb{C}/\mathbb{R}$ je razširitev stopnje 2

$\Rightarrow \overline{\mathbb{R}} = \mathbb{C}$

$\mathbb{Q}$; $\quad \mathbb{C}/\mathbb{Q}$ ni algebraična $\quad \overline{\mathbb{Q}} \neq \mathbb{C}$

Izrek: Naj bo F vsebovano v nekem algebraičnem zaprtem polju A

$K := \{a \in A.\ a \text{ algebraičen nad } F\}$

Potem je $K = \overline{F}$

Dokaz: Dokazali smo že, da je K polje, ki vsebuje F. K/F je algebraična razširitev po def K. $\underbrace{F \subseteq K}_{\text{alg.}} \subseteq A$

Dokazati moramo še, da je K algebraično zaprto polje.

Naj bo $f(x) \in K[x]$ nek nekonst. polinom

Ker je A alg zaprto ima $f(x)$ ničlo $a \in A$

a je algebraičen nad K, K/F je alg. razširitev.

Po lemi je a algebraičen nad F.

Po definiciji $a \in K$

■

Zgled:

$\overline{\mathbb{Q}} = \{a \in \mathbb{C} : a \text{ je ničla nekega neničelnega polinoma iz } \mathbb{Q}[x]\} = \{\text{algebraična števila}\}$

Končna polja

Naj bo K končno polje
Potem je karakteristika tega polja
$\mathrm{char} K = p \quad p \in \mathbb{P}$.
Zato je $\mathbb{Z}_p$ podpolje v K. $K/\mathbb{Z}_p$

Trditev: $|K| = p^n$ za nek $n \in \mathbb{N}$

Dokaz: $K/\mathbb{Z}_p$ je končna razširitev.
K ima kot vek. prostor nad $\mathbb{Z}_p$ končno bazo $a_1, \ldots, a_n$
Vsak element K se da enolično zapisati kot $\underbrace{\alpha_1}_{p} a_1 + \underbrace{\alpha_2}_{p} a_2 + \ldots + \underbrace{\alpha_n}_{p} a_n \quad \alpha_k \in \mathbb{Z}_p$ možnosti.

Imamo torej natanko p^n možnosti za elemente K

∎

Lema: Naj bo K polje moči p^n.
Potem je K razpadno polje polinoma

$$X^{p^n} - X \in \mathbb{Z}_p[X]$$

Dokaz: $(K^*, \cdot)$ je grupa moči $p^n - 1$
Po Lagrangevem izreku

$$\forall a \in K^*: \; a^{p^n-1} = 1 \quad / \cdot a$$

$$\forall a \in K \quad a^{p^n} = a$$

Vsi elementi K so ničle polinoma $X^{p^n} - X$

Ker je $st(X^{p^n} - X) = p^n$ ima ta polinom $\leq p^n$ ničel v poljubni razširitvi
Ker K vsebuje vse ničle, ter nobena podpolje ne vsebuje vseh ničel, je K razpadno polje $X^{p^n} - X$

■

Lema:

Naj bo L razpadno polje $X^{p^n}-X$ nad $\mathbb{Z}_p$. Potem je $|L| = p^n$

Dokaz:

Naj bo K množica vseh ničel polinoma $f(X) = X^{p^n}-X$ v L

↙ zaradi minimalnosti L-ja

$K = L \Leftarrow K$ je polje

Frobenijusov endomorfizem:

$$\varphi : L \longrightarrow L$$
$$X \longmapsto X^p$$

$$K = \{a \in L ; a^{p^n} = a\} = \{a \in L ; \varphi^n(a) = a\}$$

$$x, y \in K : \varphi^n(x-y) = \varphi^n(x) - \varphi^n(y) = x - y \Rightarrow x-y \in K$$

Podobno $x \cdot y$, x^{-1} če $x \neq 0$

Torej je K polje $\Rightarrow K = L$

Za dokaz da je $|L| = p^n$ je dovolj da ima naš polinom $f(X)$ samo enostavne ničle

Ena ničla: $a = 0$

$$f(X) = (\underbrace{X^{p^n-1}-1}) X$$

0 ni ničla tega polinoma

$\Rightarrow$ 0 je enostavna ničla

Recimo da $a \neq 0$ ničla:

Iz prejšnjega dokaza $a^{p^n-1} = 1$

$$f(X) = (X^{p^n-1} - a^{p^n-1})X =$$
$$(x-a)x \underbrace{(X^{p^n-2} + aX^{p^n-3} + \ldots + a^{p^n-3}X + a^{p^n-2})}_{g(X)}$$

$$g(a) = a^{p^n-2} \cdot (p^n - 1) \neq 0$$

Torej je a enostavna ničla

Posledica: Za vsako praštevilo p in vsako $n \in \mathbb{N}$ dostaja natanko eno (do izomorfizma natanko) polje moči p^n

Oznake: $\mathbb{F}_{p^n}$, $GF(p^n)$

Opomba: Wedderburnov izrek:
Vsak končen obseg je polje

Trditev: Multiplikativna grupa končnega polja je vedno ciklična

Dokaz: Naj bo $G = (\mathbb{F}_{p^n}^*, \cdot)$

G je končna abelova grupa moči $p^n - 1$
v njej bo najmanjši skupni večkratnik redov elementov grupe G.
Iz klasifikacije končnih abelovih grup sledi (DN), da grupa G vsebuje element reda v
Po Lagrangeevem izreku $v \mid (p^n - 1)$ $v \leq p^n - 1$
Dovolj je videti da je $p^n - 1 \leq v$

$x^v - 1$ ima kvečjemu v ničel
ker je v skupni večkratnik redov elem. grupe G, za $\forall g \in G.\ g^v = 1$

$\Rightarrow \quad p^n - 1 \leq v \quad \Rightarrow v = p^n - 1$

Torej ima nek element a red $v = p^n - 1$

$\Rightarrow G = \langle a \rangle$

Separabilne razširitve

Def: Naj bo $p(x) \in F[x]$ nekonstanten polinom. Pravimo da je $p(x)$ **separabilen** če so njegove ničle v poljubni razširitvi polja F enostavne

Def: Naj bo K/F algebraična razširitev. Pravimo da je ta razširitev <u>separabilna</u> če je za $\forall a \in K$ minimalni polinom a-ja nad F separabilen

Izrek: Naj bo F polje s karakteristiko 0. Naj bo $p(x)$ poljuben nerazcepen polinom. Potem je poljubna ničla $p(x)$ v poljubni razširitvi K/F enostavna

Posledica: če je $\mathrm{char} F = 0$ je vsaka algebraična razširitev F separabilna

Dokaz: $p(x) \in F[x]$ nerazcepen ack ničla a je enostavna ničla

Recimo da $p(x) = (x-a)^2 k(x)$ $k(x) \in K[x]$

$p'(x) = 2(x-a)k(x) + (x-a)^2 k'(x)$

(Analiza pravi da to lahko naredimo

V karakteristiki p:

$f(x) = x^p$ $f'(x) = p x^{p-1} = 0$

V karakteristiki 0 $p'(x) \neq 0$ če je $p(x)$ nekonstanten polinom

$p'(a) = 0$

$p'(x)$ je minimalni nenični polinom, pravkar smo pa našli manjšega polinom ki tudi ubije a $\lightning$

∎

Primer razširitve, ki ni separabilna

$K = \mathbb{F}_p(X) = \{$racionalne funkcije $\frac{f(x)}{g(x)}$: $f(x), g(x) \in \mathbb{F}_p[X]\}$

$F = \mathbb{F}_p(X^p)$

če si ogledamo $a = X \in K$ je njegov minimalni polinom $P(y) = y^p - X^p = (y-x)^p$

Ta polinom nima enostavne ničle

Definicija K/F algebraična razširitev. To je enostavna razširitev, če $\exists a \in K.\ K = F(a)$

Izrek: (o primitivnem elementu)

Vsaka končna separabilna razširitev je enostavna.

Dokaz: K/F končna separabilna

1. F je neskončno polje

   Dovolj je dokazati $a,b \in K.\ \exists \lambda \in F.\ F(a,b) = F(a+\lambda b)$

   $p(x) \in F[x]$ naj bo minimalni polinom a-ja

   $q(x) \in F[x]$ naj bo minimalni polinom b-ja

   $\text{nič}\, p(x)$: $a_1 = a, a_2, \ldots a_m$ } enostavne ničle

   $\text{nič}\, q(x)$: $b_1 = b, b_2 \ldots b_n$ }

   L naj bo razpadno polje $p(x)q(x)$

   L torej vsebuje vse ničle $a_1 \ldots a_m$ in $b_1 \ldots b_n$

   Trik: Vzamemo $\lambda \in F - \left\{ \frac{a-a_i}{b_j-b} ;\ i \in [m], j \in \{2 \ldots n\} \right\}$

   ↖ Artinov trik

   (To deluje, ker je polje F neskončno)

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

   $f(b) = p(a) = 0$

   $f(x)$ ima vsaj eno skupno ničlo s $q(x)$.

   Ali ima še kakšno skupno ničlo?

   b_2 ; ali je ničla $f(x)$

   $f(b_2) = p(a+\lambda b - \lambda b_2)$ ali je kdaj

   $a + \lambda b - \lambda b_2 = a_i$ za nek i:

   $\lambda = \frac{a_i - a}{b - b_2}$ Tak λ ne dobimo

   ITD.

   b je torej edina skupna ničla $f(x)$ in $g(x)$

$\Rightarrow$ največji skupni delitelj $f(x)$ in $g(x)$ je $(x-b)$

$\Rightarrow \exists c(x), d(x) \in F(a+\lambda b)[x].\ (x-b) = \underbrace{c(x)f(x) + d(x)g(x)}_{\in F(a+\lambda b)[x]}$

$\Rightarrow x - b \in F(a+\lambda b)[x] \Rightarrow$ koeficienti tega polinoma

so v $F(a+\lambda b)[x] \Rightarrow 1, b \in F(a, \lambda b)$

$a = \underbrace{a+\lambda b}_{\in F(a+\lambda b)} - \underbrace{\lambda b}_{\text{smo ravnokar dokazali: da je notri}}$

$F(a,b) \subseteq F(a-\lambda b)$ dokazano

obratna inkluzija očitna

2. F končno polje $F = \mathbb{F}_{p^n}$

   K je tudi končno polje $K = \mathbb{F}_{p^m}$

   $K = F(c_1 \ldots c_r)$

   BSŽ: $c_i \neq 0$ $\quad c_i \in K^*$

   K^* je za množenje ciklična grupa

   generirana z c

   $c_i = c^{n_i}$

   $K = F(c_1 \ldots c_r) = F(c)$

Primer:

$\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$ je separabilna

$\mathbb{Q}(\sqrt{2},\sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$

$\sqrt{2}$ in $\sqrt{3}$ moramo izraziti kot racionalno funkcijo $\sqrt{2}+\sqrt{3}$

$$\sqrt{2}+\sqrt{3}+\frac{1}{\sqrt{2}+\sqrt{3}} = \sqrt{2}+\sqrt{3}+\frac{\sqrt{3}-\sqrt{2}}{1} = 2\sqrt{3}$$

$$\sqrt{3} = \frac{1}{2}\left(\sqrt{2}+\sqrt{3}+(\sqrt{2}+\sqrt{3})^{-1}\right)$$

$$\sqrt{2} = \sqrt{2}+\sqrt{3}-\sqrt{3}$$

Def: Polje F je <u>prfektno</u>, če je vsaka končna razširitev F separabilna

Primer: polja s $\mathrm{char}\, F = 0$ so prfektna

Trditev: Končna polja so prfektna

Dokaz:

F naj bo končno polje, K/F naj bo končna razširitev

Recimo da $\exists f(x) \in F[x]$ ki nima enostavnih ničel, ne razcepen

a naj bo večkratna ničla

$f'(a) = 0$

Zaradi minimalnosti $f(x)$ je $f'(x) \equiv 0$

$f(x)$ je torej oblike $f(x) = \sum a_k x^{pk}$

$a_k \in F = F_{p^n}$ = razpadno polje $x^{p^n} - x \Rightarrow a_k^{p^n} - a_k = 0$

$\Rightarrow a_k = a_k^{p^n} \Rightarrow$

$f(x) = \sum a_k^{p^n} x^{pk} = \left(\sum a_k^{p^{n-1}} x^k \right)^p$

To je razcep na p faktorjev $\lightning$

∎

Def: Normalnim separabilnim razširitvam pravimo Galoisjeve razširitve

Pomeni:

1) F karakteristike 0, K razpadno polje polinoma $f(x) \in F[x]$
$\Rightarrow$ K/F Galoisjeva razširitev

2) $\mathbb{Z}_p$. Vsaka končna razširitev $K/\mathbb{Z}_p$ je Galoisjeva

Ker $\mathbb{Z}_p$ prefektna $\Rightarrow$ $K/\mathbb{Z}_p$ separabilna
$\Rightarrow$ K je razpadno polje $X^{p^n} - X \in \mathbb{Z}_p[X]$
zato je $K/\mathbb{Z}_p$ normalna

Lema: $F \subseteq L \subseteq K$ naj bodo polja

1) Če je K/F končna razširitev $\Rightarrow$ K/L končna

2) K/F normalna $\Rightarrow$ K/L normalna

3) K/F separabilna $\Rightarrow$ K/L separabilna

Dokaz:

1) Enostavno

2) $f(x) \in L[x]$ ima eno ničlo $a \in K$ (nerazcepen)
Dokazujemo $\forall$ ničle $f(x) \in K$

Naj bo $p(x) \in F[x]$ minimalni polinom a nad F
$p(x)$ ima eno ničlo v K, K/F je normalna
$\Rightarrow$ $p(x)$ ima vse ničle v K
Trdimo: $f(x) \mid p(x)$
$d(x)$ največji skupni delitelj $f(x), p(x)$ $d(x) \in L(x)$
$d(x) = \frac{f(x)}{\quad}$.
$f(x), p(x)$ imata skupno ničlo $a \Rightarrow d(a) = 0$
$\Rightarrow d(x)$ ni konstanten, deli $f(x)$, ki je nerazcepen
$\Rightarrow d(x) = f(x) \Rightarrow f(x) \mid p(x) \Rightarrow$
$\Rightarrow$ ničle $f(x)$ so tudi ničle $p(x)$, torej $\in K$

3) $a \in K$, $p(x) \in L[x]$ minimalni polinom ga je nad L
Naj bo $g(x) \in F[x]$ minimalni polinom
ga je nad F
K/F separabilna $\Rightarrow$ $g(x)$ ima same enostavne ničle.
Isti dokaz kot v 2) pokaže $p(x) \mid g(x)$
Zato $p(x)$ nima večkratnih ničel

Opomba: $F \subseteq L \subseteq K$

a) K/F končna $\Rightarrow$ L/F končna

b) K/F separabilna $\Rightarrow$ L/F separabilna

c) K/F normalna $\not\Rightarrow$ L/F normalna

Primer c)

$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2}, \varepsilon_1)$

normalna

nenormalna

razpadno polje x^3-2 nad $\mathbb{Q}$

$x^3-2 = (x-\sqrt[3]{2})(x^2+\sqrt[3]{2}x+\sqrt[3]{4})$

$-\varepsilon_1 + \varepsilon_2 = -\sqrt[3]{2}$

nična

Galoisova grupa razširitve

Def: K/F naj bo razširitev. Naj bo $\alpha: K \to K$ avtomorfizem.

Pravimo da je α F-avtomorfizem, če je $\alpha|_F = id_F$

Množici vseh avtomorfizmov polja K pravimo Galoisova grupa razširitve K/F

Opomba:

Avtomorfizmi polja K: $Aut(K)$

To je grupa za kompozitum

Galoisovo grupo razširitve bomo označili:

$Gal(K/F)$

$Gal(K/F)$ je podgrupa v $Aut(K)$

$\alpha, \beta \in Gal(K/F)$:

$x \in F$. $(\alpha\beta^{-1})(x) = \alpha(\beta^{-1}(x)) = \alpha(x) = x$

(β^{-1} na F = id)

Trditev: Naj bo $p(x) \in F[x]$ in $a \in K$ nicla tega polinoma

Za poljuben $\delta \in Aut(K/F)$ je tudi

$\delta(a)$ nicla polinoma $p(x)$

Dokaz:

$$p(x) = \sum_{k=0}^{n} a_k x^k \qquad a_k \in F$$

$$p(a) = 0$$

$$p(\delta(a)) = \sum a_k (\delta(a))^k = \sum a_k (\delta(a^k)) =$$

$$= \sum \delta(a_k) \cdot \delta(a^k) = \sum \delta(a_k a^k) =$$

($a_k \in F$, $\delta_{/F} = id$)

$$= \delta\left(\sum a_k a^k\right) = \delta(0) = 0$$

($p(a) = 0$)

∎

Komentar: V praksi bomo gledali primere ko je K/F končna separabilna.

$\exists a \in K.\ K = F(a)$ (Izrek o primitivnem elementu)

$\delta \in Gal(K/F)$ je natanko določen s sliko a-ja

$x \in K:\ x = \sum_{a_k \in F} a_k \cdot a^k \quad \delta(x) = \sum a_k \delta(a^k)$

Če je $p(x) \in F[x]$ minimalni polinom a-ja nad F, je $\delta(a)$ tudi ničla, ki leži v K

To pomeni $Gal(K/F)$ je končna grupa in

$|Gal(K/F)| \leq$ št ničel pol v K

V resnici velja enačaj:

$b \in K$ najbo poljubna ničla polinoma $p(x)$

Trdimo: $\exists\, \delta \in Gal(K/F)$, ki: a slika v b

a in b imata skupen minimalni polinom

Po neki trditvi: $\exists$ izomorfizem $\tilde{\delta}: F(a) \to F(b)$, $\tilde{\delta}|_F = id$ (pri tem $F(a) = K$, $F(b) = K$)

za V ničla imamo en avtomorfizem

Sklep: $|Gal(K/F)| =$ št ničel $p(x)$ v K

Posledica:

Če je G/F končna Galoisova razširitev, potem $|Gal(K/F)| = [K:F]$

Dokaz:

Ob označbah na prejšnji strani imamo pač vse ničle nad K zaradi normalnosti

$$|Gal(K/F)| = st\ pač = [K:F]$$

Opomba K/F končna separabilna $K = F(a)$

$p(x) \in F[x]$ minimalni polinom

$a_1, \ldots, a_n$ ničle pač ki so v K

$\delta \in Gal(K/F)$ zaradi bijektivnosti ↗

δ permutira ničle (slika ničle v ničla)

δ določa permutacijo S_n

DN: Imamo injektiven homomorfizem grup

$$Gal(K/F) \longrightarrow S_n$$

Primer:

- $Gal(\mathbb{C}/\mathbb{R})$

$\mathbb{C} = \mathbb{R}(i)$

$\delta \in Gal(\mathbb{C}/\mathbb{R})$ je določen s sliko i-ja

$p(x) = x^2+1$ minimalni polinom i-ja

$= (x-i)(x+i)$

$\delta(i)$ je ena od nicel ki leži v $\mathbb{C}$

$\delta \in \{id ; i \mapsto -i\}$

$\delta(a+bi) = a + b\delta(i) = a-bi$ konjugiranje

DN: str premislek za $Gal(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$

- $Gal(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ ← ni: normalna razširitev

$\delta \in Gal(\dots)$:

minimalni polinom $p(x) = x^3-2$

nicle: $\sqrt[3]{2}$, 2 kompleksni

Edina možnost $\delta(\sqrt[3]{2}) = \sqrt[3]{2} \Rightarrow id$ je edina

tak avtomorfizem $\Rightarrow Gal(\dots) = \{id\}$

- $Gal(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}) = ?$

Vsak a v $\mathbb{Q}(\sqrt{2},\sqrt{3})$ je oblike

$a \cdot 1 + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$

$(x^2-2)(x^2-3)$ uniči $\sqrt{2}$ in $\sqrt{3}$

Definirala $\sqrt{2}$: x^2-2 ga uniči:

δ slika $\sqrt{2}$ v eno od teh nicel

$\sqrt{2} \mapsto \pm\sqrt{2}$

enak premislek za $\sqrt{3}$

$\sqrt{3} \mapsto \pm\sqrt{3}$

Imamo 4 avtomorfizme

$|Gal(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q})| = 4$ $\not\cong \mathbb{Z}_4$ ali $\mathbb{Z}_2 \oplus \mathbb{Z}_2$

$\delta_1 : \sqrt{2} \mapsto \sqrt{2}, \sqrt{3} \mapsto \sqrt{3}$ $=: id$

$\delta_2 : \sqrt{2} \mapsto -\sqrt{2}, \sqrt{3} \mapsto \sqrt{3}$ red 2

$\delta_3 : \sqrt{2} \mapsto \sqrt{2}; \sqrt{3} \mapsto -\sqrt{3}$ red 2

$\delta_4 : \sqrt{2} \mapsto -\sqrt{2}; \sqrt{3} \mapsto -\sqrt{3}$ red 2

$\not\cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$

Def: Naj bo $f(x) \in F[x]$. Galoisova grupa polinoma $f(x)$ nad F je

$Gal_F f(x) = Gal(K/F)$ kjer je K razpadno polje polinoma $f(x)$ nad F

Opomba:

$K = F(a_1 \dots a_m)$ $a_1 \dots a_m$ ničle $f(x)$

$\delta \in Gal_F f(x)$ spet permutira $a_1 \dots a_m$

$Gal_F f(x) \longrightarrow S_m$

Primer:

$f(x) \in \mathbb{Q}[x]$ polinom stopnje 2

$Gal_{\mathbb{Q}} f(x) = ?$

a_1, a_2 ničli

$K = \mathbb{Q}(a_1, a_2)$

$f(x) = x^2 + px + q$

$a_1 + a_2 = -p$ po Vietovi formuli

$\Rightarrow \mathbb{Q}(a_1, a_2) = \mathbb{Q}(a_1)$

$\delta \in Gal_{\mathbb{Q}} F$ je določen z $\delta(a_1)$

1) $a_1 \in \mathbb{Q} \Rightarrow \delta(a_1) = a_1 \Rightarrow \delta = id \Rightarrow Gal(\dots) = \{id\}$

2) $a_1 \notin \mathbb{Q}$ ⇒ $f(x)$ je minimalni polinom a_1 z možnostmi:

$a_1 \mapsto a_1$

$a_2 \mapsto a_2$ $\quad \times \mathbb{Z}_2$

- $f(x) = x^3 + px^2 + qx + r \in \mathbb{Q}[x]$

a_1, a_2, a_3 naj bodo ničle

$K = \mathbb{Q}(a_1, a_2, a_3)$

Viet: $(x-a_1)(x-a_2)(x-a_3)$

$a_1 + a_2 + a_3 = -p$

$a_3 = -p - a_1 - a_2$

$K = \mathbb{Q}(a_1, a_2)$

Ločimo primere:

1) $a_1, a_2 \in \mathbb{Q} \Rightarrow \delta = id \Rightarrow Gal_{\mathbb{Q}} f(x) = \{id\}$

2) $a_1 \in \mathbb{Q}$, $a_2, a_3 \notin \mathbb{Q}$ (a ne razcepna)

$a_1 \mapsto a_1$

$a_2 \mapsto a_3$ $\quad Gal_{\mathbb{Q}} f(x) = \{id, (2,3)\}$

$a_3 \mapsto a_2$

$\times \mathbb{Z}_2$

3) $a_1, a_2, a_3 \notin \mathbb{Q}$ $\quad Gal$

Ločimo dve možnosti:

a) $a_2 \in \mathbb{Q}(a_1) \rightsquigarrow K = \mathbb{Q}(a_1)$

$f(x)$ je minimalni polinom a_1 nad $\mathbb{Q}$

$a_1 \mapsto a_1$ $\quad a_1 \mapsto a_2$ $\quad a_1 \mapsto a_3$ $\quad \times \mathbb{Z}_3$

3 možnosti

b) $a_2 \notin \mathbb{Q}(a_1)$

$f(x)$ je minimalni polinom a_1 in a_2 (in a_3)

$a_1 \mapsto$ ena od ničel $\quad 3$

$a_2 \mapsto$ ena od ničel -1 $\quad \cdot 2$

$a_3 \mapsto$ ničla ki ostane $\quad \cdot 1$ $\quad$ skupaj 6 možnosti

Dobimo vse permutacije indeksov ničel

$Gal \times S_3$

Primer

$$Gal_{\mathbb{Q}}((x^2-2)(x^2-3)) = Gal(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

$K = \mathbb{Q}(\sqrt{2},\sqrt{3})$

$Gal_{\mathbb{Q}}(x^5-1)$

$\varepsilon = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$

Rozpadno polje:

$K = \mathbb{Q}(\varepsilon)$

ničle: $1, \varepsilon, \varepsilon^2, \varepsilon^3, \varepsilon^4$

minimalni polinom ε: $(x-1)(x^4+x^3+x^2+x+1)$

minimalni polinom

ničle: $\varepsilon, \varepsilon^2, \varepsilon^3, \varepsilon^4$

$\sigma \in Gal_{\mathbb{Q}}(x^5-1)$

$\varepsilon \mapsto \varepsilon \quad \varepsilon \mapsto \varepsilon^2 \quad \varepsilon \mapsto \varepsilon^3 \quad \varepsilon \mapsto \varepsilon^4$

$id \qquad \sigma_1^2 \neq id$

$$Gal_{\mathbb{Q}}(x^5-1) \cong \mathbb{Z}_4$$

Fiksna podpolja

K/F naj bo razširitev

Naj bo H podgrupa $Gal(K/F)$

Fiksno podpolje polja K glede na H je

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

Očitno $F \subseteq K^H$

K^H podpolje v K

$x, y \in K \quad \sigma \in H$

$\sigma(x-y) = \sigma(x) - \sigma(y) = x - y \Rightarrow x - y \in K^H$

Podobno $xy \in K^H$, $x^{-1} \in K^H$ če $x \neq 0$

Lema: Naj bo K/F končna, $a \in K$

$H \leq Gal(K/F)$

Naj bo $\{\sigma(a); \sigma \in H\} = \{a = a_1, \dots, a_m\}$

Potem $p(x) = (x-a_1)(x-a_2)\dots(x-a_m)$
minimalni polinom a-ja nad K^H

Dokaz:

$p(x) \in K^H[x]$

$p(x) = \sum \alpha_k x^k$

$\varphi \in H$ poljuben

$$P_\varphi(x) = \sum \varphi(\alpha_k) x^k = (x-\varphi(a_1))\dots(x-\varphi(a_m))$$

$$= (x-\underbrace{\varphi(\sigma_1(a))}_{\in H = a_{j_1}})\cdot \dots \cdot (x-\underbrace{\varphi(\sigma_m(a))}_{\in H = a_{j_m}})$$

φ zaradi injektivnosti permutira $a_1 \dots a_m$

$p_\varphi(x)$ je do premešanja nelančno $p(x)$

$$p_\varphi(x) = p(x)$$

minimalnost:

$g(x) \in K^H[x]$, $g(a) = 0 \Rightarrow (x-a) \mid g(x)$ v $K[x]$

$\forall \sigma \in H$: $\sigma(a)$ je tudi ničla $g(x) \Rightarrow$

$(x-a_1) \mid g(x)$, $\dots$ $(x-a_m) \mid g(x)$

tuji so si med seboj

$\Rightarrow$ $p(x) \mid g(x)$

Lema: Naj bo K/F končna, separabilna (razširitev)
$H \leq Gal(K/F)$

a) $|H| = [K : K^H]$

b) $K^F = |H| \cdot [K^H : F]$
$[K:F]$??

Dokaz:

Po izreku o primitivnem elementu
$\exists a \in K,\ K = F(a)$

$K = K^H(a) = F(a)$ $\quad K = F(a) \subseteq K^H(a) \subseteq K$

$[K : K^H]$ = stopnja minimalnega polinoma a-ja nad K^H
$= |\{\sigma(a);\ \sigma \in H\}|$
po prejšnji lemi

Dovolj je videti da če imamo σ_1 in $\sigma_2 \in H$
$\sigma_1 \neq \sigma_2 \Rightarrow \sigma_1(a) \neq \sigma_2(a)$

$\sigma_1, \sigma_2 : K \to K$
$\sigma_1|_{K^H} = id = \sigma_2|_{K^H}$
ker $K = K^H(a)$, če bi veljalo
$\sigma_1(a) = \sigma_2(a)$ bi sledilo $\sigma_1 = \sigma_2$

■

Izrek:

Naj bo K/F končna separabilna raz.

NTSE

1) $|Gal(K/F)| = [K:F]$

2) $K^{Gal(K/F)} = F$

3) K/F je normalna

Dokaži

1) $\Rightarrow$ 2) Po prejšnji lemi

$$[K : K^{Gal(K/F)}] = |Gal(K/F)| = [K:F]$$

Po drugi strani: $[K:F] = [K : K^{Gal(K/F)}][K^{Gal(K/F)} : F]$

$\Rightarrow K^{Gal(K/F)} = F$ $\qquad$ $\| \; 1$

2) $\Rightarrow$ 3)

Naj bo $f(x) \in F[x]$ nerazc polinom, ki ima eno ničlo $a \in K$

$F = K^{Gal(K/F)}$

Uporabimo 1. lemo;

$f(x)$ je minimalni polinom a nad $K^{Gal(K/F)}$

$$f(x) = (x-a)(x-\sigma_1(a))\dots(x-\sigma_m(a))$$

Ostale ničle $f(x)$ so $\sigma(a)$; $\sigma \in Gal(K/F)$

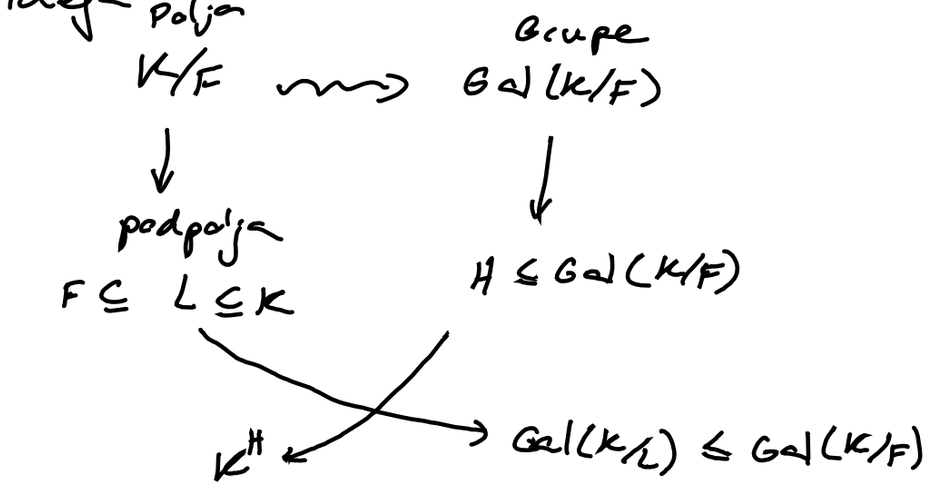
$\sigma(a) \in K$

$\Rightarrow$ ostale ničle so v K

3) $\Rightarrow$ 1) že dokazano

Fundamentalni izrek Galoisove teorije

Ideja:



Izrek: Naj bo K/F končna Galoisova razširitev

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

$\mathcal{G} = \{\text{podgrupe } Gal(K/F)\}$

Definirajmo

$\alpha : \mathcal{G} \to \mathcal{F}$, $H \mapsto K^H$ $\qquad$ $\beta : \mathcal{F} \to \mathcal{G}$, $L \mapsto Gal(K/L)$

a) α in β sta vzajemno inverzni preslikavi. Obstaja torej bijektivna korespondenca med vmesnimi polji razširitve K/F in podgrupami Galoisove grupe (K/F)

b) $|Gal(K/L)| = [K:L] \quad \forall F \subseteq L \subseteq K$

$[Gal(K/F) : Gal(K/L)] = [L:F]$

c) L, L' naj bosta vmesni polji, potem

$L \subseteq L' \iff Gal(K/L') \leq Gal(K/L)$

d) L/F je normalna raz. $\iff Gal(K/L) \trianglelefteq Gal(K/F)$

V tem primeru je $\dfrac{Gal(K/F)}{Gal(K/L)} \cong Gal(L/F)$

Opomba: $F \subseteq L \subseteq K$; končnost (normalnost, separabilnost) se iz K/F vedno podeduje na K/L

na L/F se podedujeta končnost in separabilnost, izrek pove kdaj se tudi normalnost

Dokaži:

K/L je Galoisova razširitev

a) $\alpha \circ \beta$: $L \overset{\beta}{\longmapsto} Gal(K/L) \longmapsto K^{Gal(K,L)} = L$

(pišemo: izrek)

$\beta \circ \alpha$: $H \longmapsto K^H \longmapsto Gal(K/K^H) = H$

$Gal(K/K^H) = [K : K^H] = |H|$

(normalnost)

Po definiciji: je $H \leq Gal(K/K^H)$

$\Rightarrow H = Gal(K/K^H)$ (podgrupa z istim številom elementov)

b)

Ker je K/L normalna je $|Gal(K/L)| = [K:L]$

$|Gal(K/F) : Gal(K/L)| = \frac{|Gal(K/F)|}{|Gal(K/L)|} = \frac{[K:F]}{[K:L]} =$

$= [L:F]$

c)

$(\Rightarrow)$ $\sigma \in Gal(K/L) \Rightarrow \sigma_{/L} = id \Rightarrow \sigma|_L = id \Rightarrow$

$\sigma \in Gal(K/L)$

$(\Leftarrow)$ $L = K^{Gal(K/L)}$

$L' = K^{Gal(K/L')}$ ker sta K/L in K/L' Galoisova;

$x \in L = K^{Gal(K,L)}$

$\Rightarrow \forall \sigma \in Gal(K/L).\ \sigma(x) = x$

$\Rightarrow \forall \sigma \in Gal(K/L').\ \sigma(x) = x \Rightarrow$

$x \in K^{Gal(K/L')} = L'$

d) Naj prej si ogledamo

$Gal(K/L) \triangleleft Gal(K/F) \iff$

$\forall \sigma \in Gal(K/F).\ \forall \tau \in Gal(K/L).\ \sigma^{-1}\tau\sigma \in Gal(K/L)$

$\iff \forall x \in L.\ \sigma^{-1}\tau\sigma(x) = x \quad \forall \sigma, \tau$

$\iff$

$\forall x, \tau, \sigma \quad \tau(\sigma(x)) = \sigma(x)$

$\iff$

$\forall x \in L.\ \sigma \quad \sigma(x) \in K^{Gal(K/L)} = L$

$\iff$

$\forall \sigma \in Gal(K/F).\ \sigma_*(L) \subseteq L$

$\iff$

$\forall \sigma^{-1} \in Gal(K/F)\ \ \sigma_*(L) = L$

Dokazimo ekvivalenco:

L/F je normalna

$(\Leftarrow)$ Naj bo $Gal(K/L) \triangleleft Gal(K/F)$

$\forall \sigma \in Gal(K/F) : \sigma_*(L) = L$

Naredimo preslikavo

$\Phi : Gal(K/F) \longrightarrow Gal(L/F)$

$\tau \longmapsto \tau|_L$

opomba: to je vredu ker $\tau_*(L) = L$

Φ je homomorfizem grup

$\sigma \in \ker\Phi \iff \sigma|_L = id \iff \sigma \in Gal(K/L)$

Zato je dovolj dokazati (1. izrek o izomorfizmu) da je Φ surj

$\Rightarrow$

$\Phi : Gal(K/F) \longrightarrow Gal(L/F)$

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

$\ker\Phi = Gal(K/F)$

1. izrek o: $\frac{Gal(K/F)}{Gal(K/L)} \cong \operatorname{im}\Phi \leq Gal(L/F)$

Med drugim:

$Gal(K/F) : Gal(K/L) \leq |Gal(L/F)$

$= [L : L^{Gal(L/F)}] \leq [L:F] = \frac{[K:F]}{[K:L]}$

(izrek)

$= \frac{|Gal(K/F)|}{|Gal(K/F)|} = [Gal(K/F) : Gal(K/L)]$

$\Rightarrow$ vse neenakosti tu so enačaji:

$|Gal(L/F) = [L:F]$ za končne separabilne razširitve, to pomeni: L/F je normalna

Serija neenakosti tudi implicira, da je Φ surjektiven

$(\Leftarrow)$ L/F je normalna. Torej je L razpadno polje nekega polinoma

$L = F(a_1 \dots a_n)$ $a_1 \dots a_n$ ničle $f(x)$

Izberimo poljuben $\sigma \in Gal(K/F)$

σ je določen s slikami: $a_1 \dots a_n$

$\sigma(a_i)$ je tudi ničla od $f(x)$

$\Rightarrow \sigma_*(L) \subseteq L$ (ker samo preuredi ničle

$\Rightarrow Gal(K/L) \triangleleft Gal(K/F)$

Primer

$$\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

$\sqrt{2} \longmapsto \pm\sqrt{2}$

$\sqrt{3} \longmapsto \pm\sqrt{3}$

elementi $\mathbb{Q}(\sqrt{2},\sqrt{3})$:

$$\{a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6};\ a,b,c,d \in \mathbb{Q}\}$$

id: $\sqrt{2} \longmapsto \sqrt{2}$, $\sqrt{3} \longmapsto \sqrt{3}$

σ: $\sqrt{2} \longmapsto -\sqrt{2}$, $\sqrt{3} \longmapsto \sqrt{3}$

τ: $\sqrt{2} \longmapsto \sqrt{2}$, $\sqrt{3} \longmapsto -\sqrt{3}$

$\sigma\circ\tau$: $\sqrt{2} \longmapsto -\sqrt{2}$, $\sqrt{3} \longmapsto -\sqrt{3}$

$$Gal(\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}) = \{id, \sigma, \tau, \sigma\circ\tau\}$$

Podgrupe:

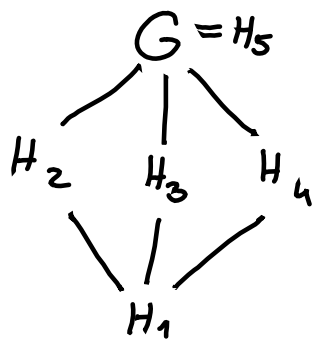
$H_1 = \{id\}$

$H_2 = \{id, \sigma\}$

$H_3 = \{id, \tau\}$

$H_4 = \{id, \sigma\tau\}$

$H_5 = G$



Fiksna podpolja: po fundamentalnem izreku so to natanko vsa vmesna polja med $\mathbb{Q}$ in $\mathbb{Q}(\sqrt{2},\sqrt{3})$

$K = \mathbb{Q}(\sqrt{2},\sqrt{3})$

$K^{H_1} = K^{\{id\}} = K$

$K^{H_2} = K^{\{id, \sigma\}}$:

$$\sigma(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}) =$$

$$= a-b\sqrt{2}+c\sqrt{3}-d\sqrt{6} = a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$$

$$b = 0 = d$$

$$K^{H_2} = \{a+c\sqrt{3};\ a,c \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{3})$$

$K^{H_3} = \mathbb{Q}(\sqrt{2})$

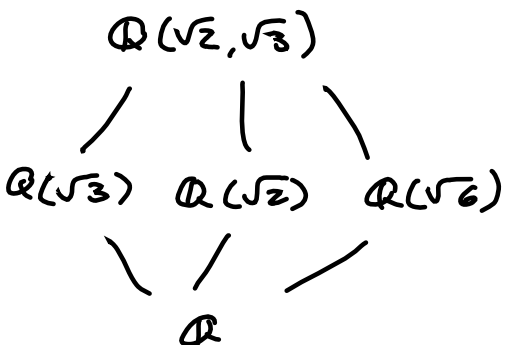
$K^{H_4} = \mathbb{Q}(\sqrt{6})$

$$\sigma(\tau(a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6})) =$$

$$a-b\sqrt{2}-c\sqrt{3}+d\sqrt{6} = a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$$

$$\Rightarrow K^{H_4} = \{a+d\sqrt{6} : a,d \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{6})$$

$K^{H_5} = \mathbb{Q}$



(NE) Rešljivost polinomskih enačb z radikali

Def: $f(x) \in F[x]$ je rešljiv z radikali, če $\exists a_1, \dots, a_k \in K$ (K razširitev F), za katere velja.

1) $f(x)$ razpade nad $F(a_1, \dots, a_k)$
2) $\exists n_1 \in \mathbb{N}.\ a_1^{n_1} \in F$
   $\exists n_2 \dots n_k \in \mathbb{N}.\ a_i^{n_i} \in F(a_1, \dots, a_{i-1})$

Kaj to pomeni?

1) ničle $f(x)$ so v $F(a_1, \dots, a_k)$
   $\Downarrow$
   ničle so rac. funkcije a_i-ja
2) $a_1 = \sqrt[n_1]{\alpha}$ $\alpha \in F$
   $a_2 = \sqrt[n_2]{\beta}$ $\beta \in F(a_1)$
   $= \sqrt[n_2]{\text{racionalna } F \text{ v } \sqrt[3]{\alpha}}$

Primer

$ax^2+bx+c \qquad a,b,c \in F$

$$x_{1,2} = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$$

$f(x)$ razpade nad $F(a_1) \qquad a_1^2 = b^2-4ac$

$a_1^2 \in F$

Polinom: stopnje 2 so rešljivi z radikali

pa dobro za 3 stopnje

Lema:

Naj bo $F \subseteq \mathbb{C}$, $\alpha \in F$ $n \in \mathbb{N}$.

Potem je $Gal_F(x^n - \alpha)$ rešljiva grupa

Opomba: Lastnosti rešljivih grup

1) Podgrupa rešljive grupe je rešljiva
2) Kvocient rešljive je rešljiva
3) Na G $\wedge$ G/N rešljivi $\Rightarrow$ G rešljiva

Dokaz:

K = razpadno polje $x^n - \alpha$ nad F

Naj bo a neka ničla $x^n - \alpha$

Vse ničle: $a, aw, aw^2, \ldots aw^{n-1}$ $\quad w = e^{\frac{2\pi i}{n}}$

$K = F(a, w) \Rightarrow F(a,w)/F$ je normalna razširitev. zaradi karakteristike 0 je Galoisova)

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

$F(w)/F$ Galoisova

$F \subseteq F(w) \subseteq F(a,w)$

(normalna)

Po fundamentalnem izreku:

$Ga(F(a,w)/F(w)) \lhd Gal(F(a,w)/F)$

Velja še: $\dfrac{Gal(F(a,w)/F)}{Gal(F(a,w)/F(w))} \cong Gal(F(w)/F)$

(za to dokazujemo da je rešljiva)

Dokazal: bomo da sta $Gal(F(w)/F)$ in $Gal(F(a,w)/F(w))$ abelovi

$Gal(F(w)/F))$: $\sigma, \tau \in Gal(F(w)/F)$

σ, τ sta določeni s sliko w

$\sigma(w) = w^i \quad \tau(w) = w^j$

$\sigma\tau(w) = w^{ji} = w^{ij} = \tau\sigma(w)$

$\Rightarrow \sigma\tau = \tau\sigma$

Podobno za $Gal(F(a,w)/F(w))$

Po 3) iz opombe sledi rezultat

Izrek: $F \subseteq \mathbb{C}$, $f(x) \in F[x]$

naj bo $F[x]$ rešljiv z radikali nad F

$\Rightarrow$ Galvajeva grupa $f(x)$ nad F je vedno rešljiva

Opomba $p(x) \in \mathbb{Q}[x]$ nerazcepen nad $\mathbb{Q}$ st. 5

če ima $p(x)$ natanko 3 realne ničle

$\Rightarrow$ Galvajeva grupa $p(x)$ nad $\mathbb{Q} \cong S_5$

S_5 ni rešljiva $\Rightarrow$ $p(x)$ ni rešljiv z radikali nad $\mathbb{Q}$ $\Rightarrow$ ni formule :-

(ampak nad $\mathbb{R}$ se da)

Primer: $p(x) = x^5 - 3x^4 + 3$

Dokaz: $\exists a_1, \dots, a_m$. $f(x)$ razpade nad $F(a_1, \dots a_m)$

$a_1^{n_1} \in F$

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

$K_f :=$ razpadno polje $f(x)$ nad F

Dokazujemo $Gal(K_f/F)$ rešljiva

$K_\alpha :=$ razpadno polje $x^{n_1} - \alpha$ nad F $\alpha = a_1^{n_1}$

$K :=$ razpadno polje $f(x)$ nad K_α

$a_1 \in K_\alpha$

$F \subseteq K_\alpha \subseteq K$

$F \subseteq K_f \subseteq K$

K je tudi razpadno polje $f(x)(x^{n_1} - \alpha)$ nad F

$\Rightarrow K/F$ je galoisova razširitev

Vemo že K_α/F in K_f/F sta tudi Galoisovi

Po prvi. izreku je

$Gal(K/K_f) \trianglelefteq Gal(K/F)$

in $\dfrac{Gal(K/F)}{Gal(K/K_f)} \cong \underbrace{Gal(K_f/F)}_{\text{dokazujemo da je to rešljiva}}$

Dovolj je dokazati da je $Gal(K/F)$ rešljiva

indukcija po m

$m = 1$: $f(x)$ razpade nad $F(a_1)$, $a_1^{n_1} \in F$

Ker je $a_1 \in K_\alpha$ je $F(a_1) \subseteq K_\alpha$

zato je $K = K_\alpha$

$Gal(K/F) = Gal(K_\alpha/F)$ je po lem: rešljiva

$m > 1$:

$a_1 \in K(\alpha)$

$f(x)$ razpade nad $K_\alpha(a_2, \dots a_n)$

po ind. predpostavki je $Gal(K/K_\alpha)$ rešljiva

K_α/F je normalna

zato je $Gal(K/K_\alpha) \trianglelefteq Gal(K/F)$

$$\frac{Gal(K/F)}{\underbrace{Gal(K/K_\alpha)}_{\text{rešljiva}}} \cong \underbrace{Gal(K_\alpha/F)}_{\text{rešljiva po lemi}} \Rightarrow Gal(K/F) \text{ rešljiva}$$

Kategorije

Definicija: **kategorija** je struktura $\mathcal{C}$,

ki jo sestavljata:

1) Razred objektov: $Ob\,\mathcal{C}$

2) Za objekta $A, B \in Ob\,\mathcal{C}$ imamo množico morfizmov $\mathcal{C}(A,B)$

Oznake za morfizem: f $A \xrightarrow{f} B$

$$A \xrightarrow{f} B \xrightarrow{g} C$$

$$A \xrightarrow{g \circ f} C$$

Pdleg tega imamo definirano preslikavo $\mathcal{C}(B,C) \times \mathcal{C}(A,B) \longrightarrow \mathcal{C}(A,C)$

$$(g, f) \longmapsto g \circ f$$

(f, g nista nujno preslikavi)

za katera velja

a) $f \circ (g \circ h) = (f \circ g) \circ h$ za $\forall$ $h \in \mathcal{C}(A,B)$ $g \in \mathcal{C}(B,C)$ $f \in \mathcal{C}(C,D)$ za vse $A, B, C, D \in Ob\,\mathcal{C}$

b) $\forall A \in Ob\,\mathcal{C}$. $\exists$ morfizem $1_A \in \mathcal{C}(A,A)$ identični morfizem da velja

$f \circ 1_A = f$ za $\forall f \in \mathcal{C}(A,B)$ za $\forall B \in \mathcal{C}$

$1_A \circ g = g$ za $\forall g \in \mathcal{C}(B,A)$ za $\forall B \in \mathcal{C}$

Primeri:

1)
Set: objekti: množice
set(A,B) = {vse preslikave $A \to B$}

2) GRP: objekti: grupe
morfizmi med A,B:
homomorfizmi: $A \to B$
o: običajni kompozitum

3) Ring: kategorija kolobarjev z enoto
objekti: kolobarji
Mor: = homomorfizmi kolobarjev
kompozitum: običajni kompozitum

4) Vec_K: objekti: vek. prostori nad poljem K
morfizmi: linearne preslikave

5) $Vec_{\mathbb{Z}}$ = Ab ... kategorija abelovih grup

6) Top
objekti = top. prostori
morfizmi: zvezne preslikave

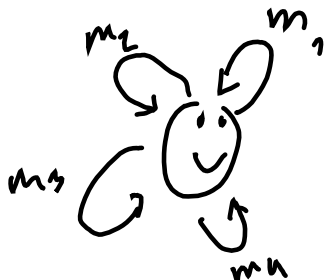
7) Naj bo M delno urejena množica $\leq$
(refl, antisim, tranz)
objekti: elementi množice M
morfizmi: $a, b \in M$
$M(a,b) = \begin{cases} \{(a,b)\} & a \leq b \\ \emptyset & \text{sicer} \end{cases}$

kompozitum: a, b, c
$a \to b \to c$
$a \leq b \quad b \leq c$
morfizmi: $(a,b) \quad (b,c)$

$(b \circ c) \circ (a,c) = (a,c)$
$\circ$ ... kompozitum morfizmov

identični morfizem:
$a \in M \quad a \leq a$
(a,a)

8) $(M, \cdot)$ naj bo monoid
Mon_M: monoidna kategorija
objekti: $\odot$ en sam objekt
morfizmi: elementi množice M



$m_1 \circ m_2 = m_1 \cdot m_2$

Def:

Pravimo da je f izomorfizem objekta A in B, če obstaja $g \in \mathcal{C}(A,B)$ da velja

$$g \circ f = 1_A$$
$$f \circ g = 1_B$$

objekta A in B sta izomorfna če obstaja izomorfizem $f \in \mathcal{C}(A,B)$

Morfizmu g pravimo inverz f

Zgled

set: Dve sedeži sta izomorfna če ∃ bijekcija

$\Leftrightarrow$ ista kardinalnost

Def: Naj bo kategorija $F \in \mathcal{C}(A,B)$

1) F je prerez, če ima levi inverz
$\exists g \in \mathcal{C}(B,A) . \; g \circ F = 1_A$

2) F je retrakt če ima desni inverz
$\exists g \in \mathcal{C}(B,A) . \; f \circ g = id_B$

3) F je monomorfizem če za
$\forall g,h \in \mathcal{C}(C,A) . \; f \circ g = f \circ h \Rightarrow g = h$

4) F je epimorfizem če
$\forall g,h \in \mathcal{C}(B,C) \; g \circ f = h \circ f \Rightarrow g = h$

V kategoriji epimorfizmi ravno surjektivne preslikave

$i : \mathbb{Z} \hookrightarrow \mathbb{Q}$

Vzemimo f,g poljubna, ki sta morfizma $Ring(\mathbb{Q},R)$ za katera $g \circ i = f \circ i \Rightarrow g/\mathbb{Z} = f/\mathbb{Z}$

$\mathbb{Q}$ je polje ulomkov

$g/\mathbb{Z}$ in $f/\mathbb{Z}$ lahko na dva različna načina razširimo do

$g/\mathbb{Q}$ in $f/\mathbb{Q}$

$f\left(\frac{a}{b}\right) = f(a) \cdot f(b)^{-1}$

Top: $i : \mathbb{Q} \to \mathbb{R}$

i je monomorfizem in epimorfizem ni pa izomorfizem

DN: monomorfizmi v Top so ulaganja

f je epimorfizem, ampak $\mathbb{Q}$ in $\mathbb{R}$ nista izomorfna

Vsak prerez je monomorfizem
Vsak retrakt je epimorfizem

Def: $\mathcal{C}$ naj bo kategorija

a) Objekt Z je začetni objekt kategorije $\mathcal{C}$, če za $\forall$ objekt C iz $\mathcal{C}$ velja

$$|\mathcal{C}(Z, C)| = 1$$

(obstaja natanko en morfizem iz Z v C)

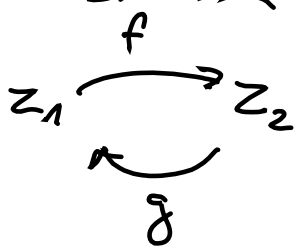
b) Objekt K je končni objekt kategorije $\mathcal{C}$, če za $\forall$ objekt C iz $\mathcal{C}$

$$|\mathcal{C}(C, K)| = 1$$

Trditev: Če v kategoriji $\mathcal{C}$ obstaja začetni objekt je do izomorfizma natančno določen

Dokaz: Z_1, Z_2 začetna objekta kategorije $\mathcal{C}$

$\mathcal{C}(Z_1, Z_2)$ ima moč ena $\Rightarrow f: Z_1 \to Z_2$



Dokazujemo: $f \circ g = 1_{Z_2}$

$g \circ f = 1_{Z_1}$

$f \circ g : \mathcal{C}(Z_2, Z_2)$

↖ ↖ začetni objekt

to je edini morfizem in identiteta smerij obstaja

$\Rightarrow f \circ g = 1_{Z_2}$

Podobno za končni objekt

Podobno za končne objekte

Primeri:

Set: $\emptyset$ je začetni

$\mathbb{N}$ je končen.

Grup: $\{1\}$ je začetna in končna

Monoid:

Mon_M 

$|M| = 1 \Rightarrow$  je začetn. in končni objekt

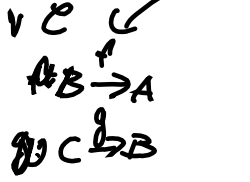
Svet Mon_M nima začetnega ali končnega

Def: Naj bo $\mathcal{C}$ kategorija. **Dualna (nasprotna) kategorija** kategorije $\mathcal{C}$ je kategorija $\mathcal{C}^{opp}$, za katero velja:

- $Ob\,\mathcal{C}^{opp} = Ob\,\mathcal{C}^{opp}$
- $\mathcal{C}^{opp}(A,B) = \mathcal{C}(B,A)$
- kompozitum:

$f \in \mathcal{C}^{opp}(A,B)$ $g \in \mathcal{C}^{opp}(D,C)$

$g * f := fog$



Primer:

Konec: objekt $\mathcal{C}$ = začetek: objekt $\mathcal{C}^{opp}$

Funktorji in naravne transpozicije

Def: Naj bosta $\mathcal{C}$ in $\mathcal{D}$ kategoriji.
Funktor F med $\mathcal{C}$ in $\mathcal{D}$ je predpis, ki

- Vsakemu objektu C iz $\mathcal{C}$ priredi objekt $F(C)$ v $\mathcal{D}$
- za vsaka objekta A, B iz $\mathcal{C}$ imamo preslikavo $\mathcal{C}(A,B) \longrightarrow \mathcal{D}(F(A), F(B))$
  $f \longmapsto F(f)$

  ki zadošča zahtevama:
  1) $\forall A \in Ob\mathcal{C} . F(1_A) = 1_{F(A)}$
  2) $F(f \circ g) = F(f) \circ F(g)$

Primeri

① F iz Grp v Set

$grp\ G \longmapsto G$ množica

$f: G \to H \longmapsto f: G \to H$
homom. preslikava

F je pozabljivi funktor

② Grupa

$[x,y] = xyx^{-1}y^{-1}$ komutator

$G' = \langle [x,y]; x,y \in G \rangle$ komutatorska podgrupa

$F: Grp \to Grp$

$G \longmapsto G'$

$f: G \to H \longmapsto G' \to H'$
homo.

Pod-bnc

$Grp \longrightarrow Grp$

$G \longmapsto Z(G)$

$f: G \to H \longrightarrow f_{|Z(G)}: Z(G) \to Z(H_1)$?

Ne, ker

$\mathbb{Z}_2 \longrightarrow S_3$

$Z(\mathbb{Z}_2) = \mathbb{Z}_2 \quad Z(S_3) = \{1\}$

③ $\mathcal{C}$ kategorija

Fiksirano $A \in Ob\mathcal{C}$

F iz $\mathcal{C}$ v Set

$C \in Ob\mathcal{C} \quad C \longmapsto \mathcal{C}(A,C)$

$f \in \mathcal{C}(B,C)$

$F(f): \mathcal{C}(A,B) \longrightarrow \mathcal{C}(A,C)$

$g \longmapsto f \circ g$

DN to je funktor

Def: Naj bosta $\mathcal{C}$ in $\mathcal{D}$ kategoriji

kofunktor iz $\mathcal{C}$ v $\mathcal{D}$ je predpis:

a) objektu $c \in Ob\mathcal{C}$ priredimo $F(c) \in Ob(\mathcal{D})$

b) morfizmu $f \in \mathcal{C}(A,B)$ priredimo morfizem $F(f) \in \mathcal{D}(F(B), F(A))$ pri čemer velja:

$F(1_A) = 1_A$

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

Zgled:

F je Vec_k v Vec_k (linearne preslikave med $V \to V$ nad k)

V objekt, $F(V) = V^* = \mathcal{L}_{in}(V, k)$

$A: U \to V$ linearna $\longrightarrow F(A): V^* \to U^*$

$F(A) := A^d$

$\varphi \in V^*$

$$\begin{array}{ccc} V & \xrightarrow{\varphi} & k \\ A \uparrow & \nearrow & \\ U & & \end{array}$$

$A^d(\varphi) = \varphi \circ A$

$F(id_V) = id_{V^*}$, ker $I^d = I$

$(A \circ B)^d = B^d \circ A^d$

DN:

$F: V \to V^{**}$ je funktor

$\mathcal{C}$, fiksiramo $A \in Ob\mathcal{C}$

F iz $\mathcal{C}$ v set

objekti: $C \mapsto \mathcal{C}(C, A)$

morfizmi:

$f \in \mathcal{C}(B, C) \dots F(f): \mathcal{C}(C, A) \to \mathcal{C}(B, A)$

$g \mapsto g \circ f$

$$\begin{array}{ccc} C & \xrightarrow{g} & A \\ f \uparrow & & \\ B & & \end{array}$$

to je kofunktor

Def. Naj bosta $\mathcal{C}$ in $\mathcal{D}$ kategoriji,
F in G naj bosta funktorja iz $\mathcal{C}$ v $\mathcal{D}$

Naravna transformacija med F in G
("$\mu : F \to G$") je nabor morfizmov

$$\mu_C : F(C) \longrightarrow G(C)$$

↖ ups, puščice

Bolj prav: $\mu_C \in \mathcal{D}(F(C), G(C))$

za katerega velja:
za $f \in \mathcal{C}(A,B)$ pojdeš en velja:

$$\begin{array}{ccc} F(A) & \xrightarrow{F(f)} & F(B) \\ \downarrow{\scriptstyle \mu_A} & & \downarrow{\scriptstyle \mu_B} \\ G(A) & \xrightarrow[G(f)]{} & G(B) \end{array}$$

$$G(f) \circ \mu_A = \mu_B \circ F(f) \quad \forall A, B, f$$

Zgledi

Dva funktorja iz Grp v Grp

1. funktor: identični funktor

2. funktor: Abelizacija

$$Ab: G \longmapsto G^{ab} = G/G'$$

↖ komutatorska ab grupa

$$f: G \to H \longmapsto f^{ab}: G^{ab} \to H^{ab}$$

$$f^{ab}(xG') = f(x)H'$$

Naredimo naravno transformacijo med Id in Ab

G grupa

$$\mu_G: G \longrightarrow G^{ab}$$
$$g \longmapsto gG'$$

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ {\scriptstyle \mu_G}\downarrow & & \downarrow{\scriptstyle \mu_H} \\ G^{ab} & \xrightarrow[f^{ab}]{} & H^{ab} \end{array} \qquad x \in G$$

$$(\mu_H \circ f)(x) = \mu_H(f(x)) = f(x)H' =$$
$$= f^{ab}(xG') = f^{ab}(\mu_G(x)) = (f^{ab} \circ \mu_G)(x)$$

Produkti, koprodukti, prosti objekti

Def: Naj bo $\mathcal{C}$ kategorija, I naj bo indeksna množica, $A_i; i \in I$ naj bo družina objektov iz $\mathcal{C}$. **Produkt** družine objektov A_i je objekt P skupaj z morfizmi $\Pi_i : P \to A_i ; i \in I$, da velja

za $\forall$ objekt X in vsak nabor morfizmov $f_i : X \to A_i$ obstaja natanko en morfizem $f : X \to P$, da

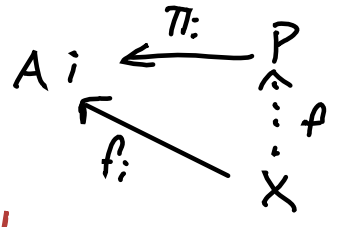


diagram komutira za $\forall i \in I$

(P je univerzalen

strukturni morfizmi

Zgled:

set A, B množici

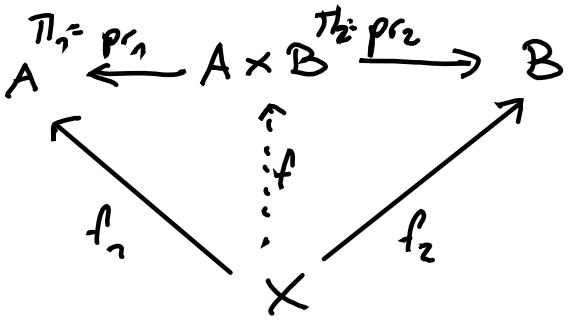
$A \times B$ je produkt A in B

$$A \xleftarrow{\pi_1 := pr_1} A \times B \xrightarrow{\pi_2 := pr_2} B$$

X poljubna množica

$f_1 : X \to A$

$f_2 : X \to B$



Recimo da f obstaja:

$\pi_1 \circ f = f_1 \qquad \pi_2 \circ f = f_2$

$f(x) = (a_x, b_x)$

$\pi_1 \circ f(x) = \pi_1(a_x, b_x) = a_x = f_1(x)$

$\pi_1 \circ f(x) = b_x = f_2(x)$

če f obstaja, mora veljati $f(x) = (f_1(x), f_2(x))$

(to je dokaz enoličnosti)

obstoj: definiramo $f = (f_1, f_2)$

(zgoraj tudi dokaz da komutira)

- Poljubna družina množic $A_i \in I$
  produkt je kartezični produkt
  $f = (f_1, \dots, f_n)$ sklopaj s projekcijami na i-ti faktor

- Grp:
  produkt = kartezični produkt z operacijo po komponentah

- Top: isto
- Ring: isto
- Vec_K: isto

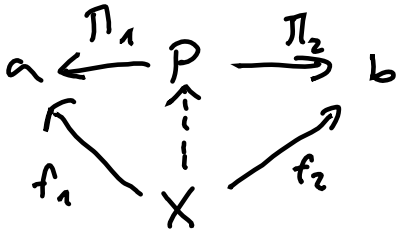
- Field (kategorija polj)
  $F_1 \longrightarrow F_2$ neničeln homomorfizem
  $\ker f \lhd f_1 \Rightarrow \ker f = \{0\}$
  f mora biti injektiven
  F_1 in F_2 morata biti iste karakteristike

kartezični produkt ne more biti polje
(delitelji: niča $(a,0)\cdot(0,b)$)

Produkt polj mora biti kvadi produkt kolobarjev, če imamo enoličnost torej mora biti kartezični produkt to pa ne gre

DN kategorija dobljena iz delno urejene množice $(M, \leq)$

Produkt a in $b \in M$, če obstaja



$\pi_1 = (P, a)$ $\quad p \leq a$

$\pi_2 = (P, b)$ $\quad p \leq b$

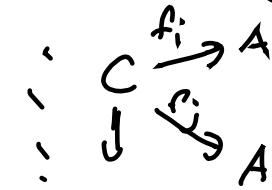
če $x \leq a$, $x \leq b$, potem $x \leq p$

p bi moral biti $\inf(a, b)$, če obstaja.

Trditev: Naj bo A_i ; $i \in I$ družina objektov v kategoriji $\mathcal{C}$. Naj bosta $(P, \pi_i)_{i \in I}$ in $(Q, \sigma_i)_{i \in I}$ produkta objektov A_i. Potem sta P in Q izomorfna

Dokaz:

Naredimo novo kategorijo: $\mathcal{D}$

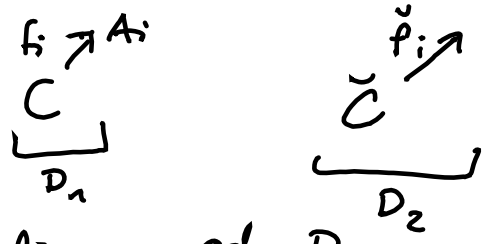
Objekti: 

C objekt v $\mathcal{C}$

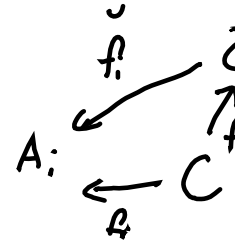
če ne obstaja pol n: produkta

$(C, z$ nekimi morfizmi $f_i : C \to A_i)$

Morfizem med dvema takima objektoma



Morfizem med D_1 in D_2 je morfizem med C in $\check{C}$ v $\mathcal{C}$



za katerega ta diagram komutira (če obstaja) za $\forall i \in I$

Produkt v $\mathcal{C}$ je natanko končni objekt v $\mathcal{D}$ (sa enolično določeni)

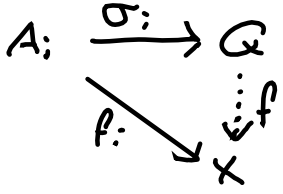
Def: Naj bodo $A_i : i \in I$ objekti kategorije $\mathcal{C}$

koprodukt objektov A_i je produkt teh objektov v $\mathcal{C}^{op}$.

Natančneje to je objekt Q skupaj z morfizmi:

$\sigma_i : A_i \to Q$, da velja:

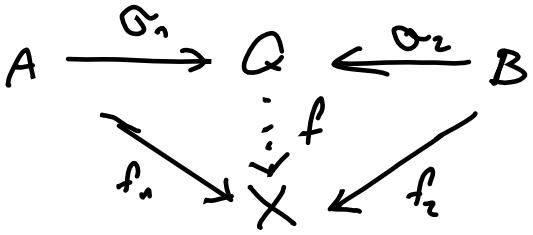
za $\forall$ objekt X in za vse $f_i : A_i \to X$ obstaja natanko en morfizem $f : Q \to X$, da vs. diagram:



komutirajo

Primer:

set: A, B množici, $Q = ?$



↙ disjunktna unija

$Q = A \sqcup B$

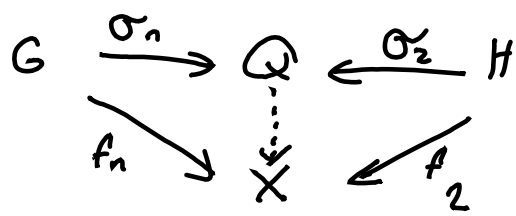
Če imamo X in f_1, f_2:

$f: Q \longrightarrow X$

$f(a) = f_1(a)$

$f(b) = f_2(b)$

Grp: G, H grupi:



$Q = G * H$ ... prosti produkt G in H

↓ formalno: produkt

$d = g_1 h_1 g_2 h_2 \dots g_k h_k$

$g_i, h_i \in H \quad k \geq 0$

$\sigma_1: G \longrightarrow G * H$

$g \longmapsto g \cdot 1$

$\sigma_2: H \longrightarrow G * H$

$h \longmapsto 1 \cdot h$

To je koprodukt v Grp:

$f(g) := f_1(g)$

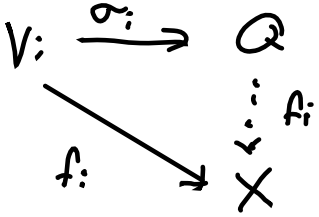
$f(h) := f_2(h)$

$f(g_1 h_1 \dots g_k h_k) = f(g_1) f(h_1) \dots f(g_k) f(g_k)$

(n: nujno da se začne s h jem in konča z g jem ↑ haha dodajamo

Vec_K : V_i vektorski prostori

kopreduld: Q



Definiramo $Q = \{(v_i)_{i \in I} : v_i \in V_i,$ le

končno mnogo $v_i \neq 0\}$

$Q = \bigoplus_{i \in I} V_i$ direktna vsota V_i-jev

$\sigma_i : V_i \longrightarrow \bigoplus_{i \in I} V_i$

$f : (v_i)_{i \in I} \longmapsto \sum f_i(v_i)$

Def: $\mathcal{C}$ je konkretna kategorija

če lahko na objekte gledamo kot na množice in na morfizme kot preslikave na množice



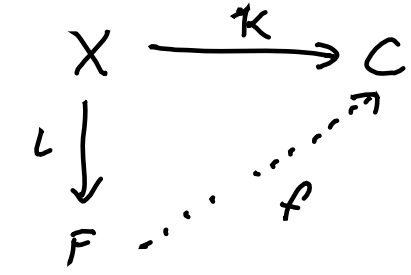
ni: konkretna kategorija

Def: Naj bo $\mathcal{C}$ konkretna kategorija

Naj bo X neprazna množica

Prosti objekt nad množico X je objekt P skupaj s preslikavo $\iota: X \to F$ da velja:

za $\forall$ objekt C in $\forall$ preslikavo $K: X \to C$ $\exists$ natanko en morfizem iz F v C, da komutira



Trditev: Prosti objekt, če obstaja je do izomorfizma natanko določen

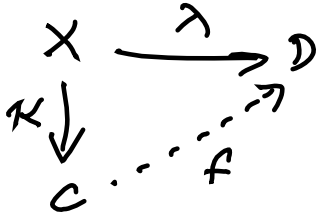
Dokaz: kategorija $\mathcal{D}$

objekti: $X \xrightarrow{\kappa} C$; C objekt v $\mathcal{C}$

Morfizem med $X \xrightarrow{\kappa} C$ in $X \xrightarrow{\lambda} D$

$=$

morfizem f med C in D, da



Prosti objekt kategorije $\mathcal{C}$ je ravno začetni objekt v $\mathcal{D}$

∎

Zgled:

1) Vec_K

X poljubna množica: $F = \mathcal{L}in\, X =$

$= \{ \alpha_1 x_1 + \ldots + \alpha_k x_k, \; k \geq 0 \; x_i \in X \; \alpha_i \in K \}$

formalne vsote

2) Mon:

X poljubna množica

$F = \{ x_1 x_2 \ldots x_k ; \; x_i \in X \}$ → prosti monoid nad X

produkt = sklop besed

3) Grp: $F = \{ x_1 \ldots x_k \quad x_i \in X \cup X^{-1}$

↑ formalni inverzi $\{x^{-1} ; x \in X\}$

produkt = „sklop" + krajšanje

$x_1 x_2^{-1} x_3 \cdot x_3^{-1} x_4 x_5 =$

$= x_1 x_2^{-1} x_4 x_5$

(tehnične komplikacije: robimo grupo reduciranih besed)

→ prosta grupa nad X