

Uvod v teorijo grup

Operacija na množici $S \neq \emptyset$

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

- \star je asociativna $\forall a, b, c. (a \star b) \star c = a \star (b \star c)$
- \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 .
Pravimode je $e \in S$ enota oz. neutralni element, ko $\forall a. e \star a = a \star e = a$

Velja: Če je enota, potem je ena sama

Definicija: Polgrupe z enoto je monoid.

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

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

$$l = l \star e = l \star (r \star d) = (l \star r) \star d = e \star d = d$$

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

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

Zagledi:

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

2) X neprazna množica

$\text{Sim}(X) = \{f: X \rightarrow X\}$ množica vseh
operacija: kompozitum \circ bijektičnih preiskov
asociativnost, enota, inverz

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

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

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

... simetrična grupa reda n

Ponovitev o permutacijah

(elementi S_n)

kompozitum

• Vsaka permutacija je produkt disjunktnih ciklov

• cikl dolzine 2 je transpozicija

• vsaka permutacija $\beta \in S_n$ je produkt transpozicij. Teh transpozicij je vedno sodo ali: vedno lahko mnogo

$$\operatorname{sgn}(\beta) = \begin{cases} 1 & \text{če } \beta \text{ je produkt sodo množ. transpozicij} \\ -1 & \text{če } \beta \text{ je produkt l.ho množ. transpozicij} \end{cases}$$

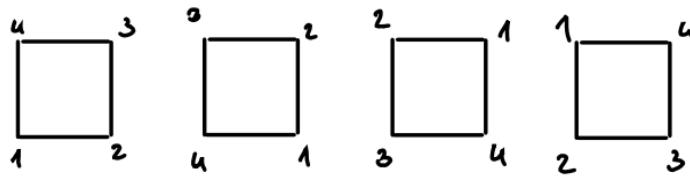
• $\operatorname{sgn}(\gamma \circ \delta) = \operatorname{sgn}(\gamma) \operatorname{sgn}(\delta)$

Zagled: Simetrije kvadrata

$$\begin{array}{c} D \\ \boxed{K} \\ A \quad B \end{array} \quad = \text{izometrije } f: \mathbb{R}^2 \rightarrow \mathbb{R}^2, \text{ da je } f_*(K) = K$$
$$f_K: K \rightarrow K \text{ je bijekcija}$$

Preverimo daje množica simetrij grupa za kompozicijo

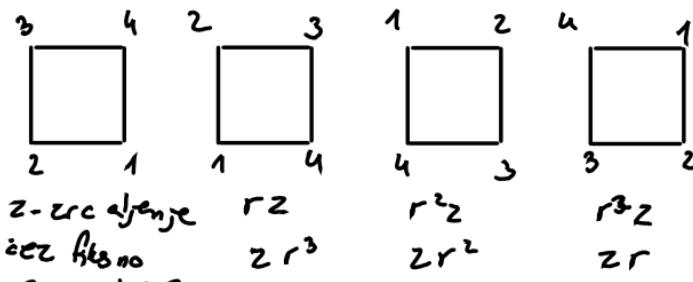
Simetrija slike ogljšča v ogljšča
↳ permutacija ogljšč



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

r^2

r^3



$$(1 \ 2)(3 \ 4) \quad r^3z = zr$$

$$rzr = 1$$

To je 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: kvadratima kažejo 8 simetrij

Simetrija jednolocena s sliko ogljšča 1 in informacijo ali smo naredili zrcaljenje ali ne

slike 1: 4 možnosti zrcaljenje (da/ne) 2 možnosti
 $4 \cdot 2 = 8$ manj kot 8 možnosti

$$D_{2,4} = \{id, r, r^2, r^3, rz, r^2z, r^3z\}$$

Diederska grupa mod 8

Splošna simetrija:

r - rotacija za $\frac{2\pi}{n}$ okoli središča
z - zrcaljenje čez akcen og simetrije

$$\mathcal{D}_{2n} = \{1, r, \dots, r^{n-1}; z, zr, \dots, zr^{n-1}\}$$

Diederska grupa moči $2n$
Velja $zr = r^{n-1}z$

$\bar{c}e j\in (S, \star)$ monoid naredim množico

$$S^* := \{ \text{obnjeni elementi iz } S \}$$

S^* je grupa za \star

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

Ali je S^* zaprta za operacijo

$$x, y \in S^*$$

$$(x \star y)^{-1} = y^{-1} \star x^{-1} \quad \text{DN dokaz}$$

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

Vsek $x \in S^*$ ima inverz $\in S^*$

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

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

↑
složna linearne
grupe $n \times n$ matrik

Direktni produkt grup

G_1, \dots, G_n nay bodo grupe =
operacijam: $\textcircled{1}, \textcircled{2}, \textcircled{3}, \dots, \textcircled{n}$

$G_1 \times G_2 \times \dots \times G_n$ vpeljemo operacijo *

$$(g_1, \dots, g_n) * (h_1, \dots, h_n) =$$

$$(g_1 \textcircled{1} h_1, g_2 \textcircled{2} h_2, \dots, g_n \textcircled{n} h_n)$$

DN: to je grupa

Oznake:	operacija	enota	inverz x	potenza x
grupa	•	1	x^{-1}	x^n
abstraktna 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

Trditve: 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:

$2 \Rightarrow 3$

$1 \in H$

Izbremo $x \in H$ $y = x$

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

Naj bo $x \in H$ poljuben

$x^{-1} \in H$

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

Izbremo $y \in H$

$y^{-1} \in H$

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

Posledica: Naj bo G končna grupa
Naj bo $H \neq \{0\} \leq G$

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 dodatek za splošnos H n: trivialna
 H gotovo vsebuje vsaj eno naravno število

Naj bo n najmanjše naravno število v H

Trdimo $H = n\mathbb{Z} = \{nk ; k \in \mathbb{Z}\}$

Ker je H zaprta za inverziranje, je $n\mathbb{Z} \subseteq H$

Vzemimo poluben $m \in H$

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

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

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

Primer

1) $GL_n(\mathbb{R})$ - obnjava n×n matrice

je grupa za množenje matrik

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

$SL_n(\mathbb{R})$

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

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

Trditev: Naj bo sta $K, K \leq G$

Potem tudi $H \cap K \leq G$

Iznaka za presek poljubnih dražin podmnogic

Definicija: Naj bo sta $H, K \leq G$

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

Opozame:

HK ni vedna grupa

$$G = S_3$$

$$H = \{\text{id}, (1, 2)\}$$

$$K = \{\text{id}, (1, 3)\}$$

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

$$(1, 3, 2) \cdot (1, 3, 2) = (1, 2, 3) \notin HK$$

Trditiv: Na; basta $H, K \leq G$. če velja

$$HK = KH$$

potem je HK podgrupa

Dokaz:

$$a, b \in HK$$

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

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

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

✓

4

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

$$aHa^{-1} = \{ah_1a^{-1} \mid h_1 \in H\}$$

Potem je to tudi podgrupa

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

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

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

$$= ah_1a^{-1} a^{-1} h_2^{-1} a = ah_1 h_2^{-1} a \\ \in H \quad \blacksquare$$

DN: Najbo G grupe

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

\Rightarrow podgrupa v G (center grupe G)

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

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 ekvivalenčna

Naj bo G končna grupa

G/H je tudi končna

moc množice označimo z $|G:H|$ grupi G

indeks podgrupe
 \downarrow
 H v

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

To je Lagrangev izrek

Dokaz: $|G:H|=r$

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



$$|G| = |a_1H| + |a_2H| + \dots + |a_rH|$$

Dokazati moramo, da je $|a_iH| = |H|$

$$\varphi: H \rightarrow a_iH$$

$$h \mapsto a_ih$$

φ je očitno slikektivna

injektivnost

$$\varphi(h_1) = \varphi(h_2)$$

$$a_i h_1 = a_i h_2$$

$$a_i^{-1} / \quad h_1 = h_2$$

Posledica: Naj bo G končna grupa

in $H \leq G$. Potem $|H| \leq |G|$

Naj bo G abelova

Vpeljemo operacijo na G/H

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

Ali je ta operacija dobro definirana

$$a+H = a' + H$$

$$\hat{a}\hat{a}' \in H$$

$$a'-a \in H$$

$$b+H = b' + H$$

$$\hat{b}' \hat{b} \in H$$

$$b'-b \in H$$

$$\text{Dokazjemo } (a'+b') - (a+b) \in H$$

komutativnost

$$a'+b' - a - b \stackrel{\text{komutativnost}}{=} (a'-a) - (b-b') = eH$$

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 podgrupu, v G , ki vsebuje množico X .

Tej podgrupi pravimo podgrupa generirana z množico X

Zakaj je to smiselno?

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

Oznaka: Če je $X = \{x_1, \dots, x_n\}$ potem pišemo

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

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

če $\exists x \in G$ deje $G = \langle x \rangle$, 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)

$$S = \left\{ x_1^{\pm 1} \cdot x_2^{\pm 1} \cdot \dots \cdot x_n^{\pm 1} ; x_i \in X \right\} \subseteq \langle x \rangle$$

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 $\in S$

$$a = x_1^{\pm 1} \cdot \dots \cdot x_n^{\pm 1} \quad x_i \in X$$

$$b = x_{k_1}^{\pm 1} \cdot \dots \cdot x_{k_s}^{\pm 1} \quad x_j \in X$$

$$a^{-1} \cdot b = x_1^{\mp 1} \cdot \dots \cdot x_n^{\mp 1} \cdot x_{k_1}^{\pm 1} \cdot \dots \cdot x_{k_s}^{\pm 1}$$

Posledica: $a \in G$

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

Pimmer:

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

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

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

(Vsak dve tudi števili generirata \mathbb{Z})

Def: Nej bo G grupa in $a \in G$.

Najmanjšemu neskončnemu 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:

$$\Rightarrow \text{Naj bo red } a = n$$

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

\geq dok

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

$$a^k = a^{mn+r} = (\underbrace{a^n}_1)^m \cdot a^r = a^r$$

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

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

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

= predpostavko.

$$\Leftarrow \text{Rečimo da } |\langle a \rangle| = n$$

Potem ima a končen red

Po prejšnjem sledi pa ima

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

Sledi: $m = n$

DN: $(\mathbb{Q}, +)$ ni končna 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 prostovilo $\Rightarrow G$ je ciklična

Dokaz:

1) red $a = n$ (n co kerje 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 $a = p \Rightarrow$

$$\langle a \rangle = \underbrace{\{1, \dots, a^{p-1}\}}_p$$

sledi: $G = \langle a \rangle$

Uvod v teorijo kolobarjev, obsegov, polj in algebr

Def: Nej bo K neprazna množica z operacijama $+$.

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 enotu za množenje: 1
(enota kolobarja K))
- 3) $a(b+c) = ab+ac$ in $(a+b)c = ac+bc$
 $\forall a, b, c \in K$

Če je \cdot komutativna je K komutativen.

Zadaci:

- $(\mathbb{Z}, +, \cdot)$ komutativ kolobar
- $(2\mathbb{Z}, +, \cdot)$ (ni endet za množenje)
komutativen klbr (rng)
- $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ so komutativi kolobari;
- $\mathbb{R}^{n \times n}$ je kolobar
- $X \subseteq \mathbb{R}$

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

sestevanje in množenje po točkah

\mathbb{R}^X je komutativen kolobar

Homomorfizm:

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

Homomorfizem klobarjev :

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

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

$$f(1) = 1$$



takej morano to definisati:

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

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

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

$\rho(1)$ n: enota v tem klobarju

Homomorfizem algeber $\rho: A \rightarrow B$

- ρ je homomorfizem klobarjev in
- 'linearne preslikave'

Oponba: če je $f: A \rightarrow B$ izomorfizem
 potni je f^{-1} izomorfizem
 Potem $A \cong B$

a je člen
 $f(g) = aga^{-1}$ (konjugiranje)

f je automorfizem grup
 natančji automorfizem

$$\text{Inn } G = \{ f_a; f_a(g) = aga^{-1} \}$$

K konstantiven kolobar
 $e_v_a: K[x] \rightarrow X$ evalvacija
 $p \mapsto p(a)$

$N \leq G$ je Podgrupa edinke, os

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

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

(Baljše imo bi bile normalne podgrupe)

Oznaka: $N \triangleleft G$

Primeri:

$$\{1\} \triangleleft G \quad G \triangleleft G$$

Grupe v katerih sta to edini edinki se imenujejo enostavne grupe

če je G abelova je vsake podgrupe edinke

(obstajajo tudi nekomutativne kjer te velja)

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

Vsejemo mnogeje kvaternione

Kvaternionske grupe. Vseke grupe

je edinke

Trditer: ekvivalentne

$$\textcircled{1} \quad N \triangle G$$

$$\textcircled{2} \quad \forall a \in G \quad aN \subseteq Na$$

$$\textcircled{3} \quad \forall a \in G \quad aN = Na$$

$$\textcircled{4} \quad \forall a \in G \quad aNa^{-1} = N$$

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

Tvdimo $H \triangleleft G$

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

$\oplus \quad B\bar{S}Z\bar{S}$ $a \notin H$

imamo dva lave
odeska podgrupe H

$1 \cdot H = H$

$aH \neq H$

Desni odsack:

Lavke je v. deli, da
imamo ^{natural} same dva
desna odsacke

$$G = H \cup aH \text{ disjunktna}$$

unija

$$aH = G/H$$

$$H \in Ha$$

$$G = H \cup Ha \text{ disjunktna unija}$$

$$Ha = G/H$$

$$\text{Torej } Ha = aH$$

P_{permut}

S_n

$A_n = \{\text{sade permutacije } \cup S_n\}$

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

④ $D_{2n} = \{ \text{id}, r, r^2, \dots, r^{n-1}, z, rz, \dots, r^{n-1}z \}$

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

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

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

Trditve: Naj bo G grupa

① če je $H \leq G$ in $N \triangleleft G$

$$HN = NH \leq G$$

② če sta N, M podgrupe: dokazi $\forall g \in G$
potem je $NM = MN \triangleleft G$

Dokaz:

1) $\forall h \in H$

$$hN = Nh \Rightarrow HN = NH \quad \text{po definiciji}$$

$HN = NH \Rightarrow$ je podgrupa (samo že dokaz!)

2) NM je podgrupa

$g \in G$

$$\underline{g} \underline{N} \underline{M} \underline{g}^{-1} \in \underline{N} \underline{M}$$

$$\underline{g}^N \underline{g}^{-1} \underline{g}^M \underline{g}^{-1} \in N \cdot M$$

Izrek:

Naj bo G grupa $N \triangleleft G$

Potem je na G/N $\xleftarrow{\text{kvocientna/faktorska}} g^{-1}gN$ s predpisom

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

dobra definiranca operacija

s to operacijo postane množica G/N grupa

Preslikava $\Pi: G \longrightarrow G/N$, dana s predpisom

$$\Pi(g) = gN \quad \text{epimorfizem grup}$$

$$\ker \Pi = N$$

Dokaz:

dobra definiranost

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

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

$$b^{-1}\tilde{a}'\tilde{a}b b^{-1}\tilde{b}'$$

$$\underbrace{\qquad}_{\in N} \ker aN = \tilde{a}N$$

$$\underbrace{\qquad}_{\in N} \ker bN = b'N$$

$$\underbrace{\qquad}_{\in N}$$

G/N je grupa

asociativnost p. taja v G

$$\text{enota: } 1 \cdot N = N$$

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

Π je homomorfizem

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

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

Izrek: (1. izrek o izomorfizmu)

Naj bo $p: G \rightarrow H$ homomorfizem grup.

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

$$G/\ker p \cong \text{im } p$$

Dokaz: ker p je podgrupa v G

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

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

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

Dekliniramo $\gamma: G/\ker p \rightarrow \text{im } p$

$$\gamma(g\ker p) := f(g)$$

Dobro dekliniranost

$$\underbrace{g\ker p = g'\ker p}_{\Downarrow} \quad \text{zato videti } \gamma(g) = p(g)$$

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

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

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

$$p(g') = f(g)$$

γ je homomorfizem

$$\gamma((g\ker p)(g'\ker p)) =$$

$$= \gamma(g \cdot g' \ker p) = p(g \cdot g') = p(g) \cdot p(g') =$$

$$= \gamma(g\ker p)\gamma(g'\ker p)$$

γ je ohranil zgornje množenje

γ je monomorfizem

$$g\ker p \in \ker \gamma$$

$$\gamma(g\ker p) = 1$$

$$p(g) = 1$$

$$g\ker p \Rightarrow 1\ker p$$

$\ker \gamma$ je trouvan doleg

$$\ker \gamma = \{1\ker p\}$$

Opomba: Edinke so jedra
① homomorfizmov

② Naj bo $\rho: G \rightarrow H$ homomorfizem

Naj bo $N \triangleleft G$, recimo da
 $N \subseteq \ker \rho$

Potem je $\gamma: G/N \rightarrow H$ dana

s predpisom $\gamma(gN) := \gamma(g)$

dobra definirata homomorfizem grup

Pravimo da je γ inducirana s f

shematicno:

$$\begin{array}{ccc} G & \xrightarrow{f} & H \\ \downarrow \pi & \nearrow \gamma & \\ G/N & & \end{array}$$

Ta diagram
kemutiira

$\gamma \circ \pi(g) = \gamma(\pi g) = \gamma(gN) = f(g)$

kanonidni
epimorfizem

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 Dokaži:

$$1), 2) DN$$

$$3) \text{Definiramo } f: H \rightarrow HN/N$$

$$f(h) := hN$$

f je epimorfizem

$$\ker f = H \cap N$$

Uporabimo prvi izrek o izomorfizmu

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

$$H_{N \cap H} \cong HN/N$$

Izrek (3. izrek o izomorfizmu)

Najbo G grupa $N, M \triangleleft G$ $M \subseteq N$

1) $M \triangleleft N$

2) $N/M \triangleleft G/M$

3) $(G/M)/_{(N/M)} \cong G/N$

Ideja dokaze

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

$$\rho(gM) = gN$$

ρ je dobro definiran epimorfizem

$$\ker \rho = N/M$$

Uparabimo 1. izrek o izomorfizmu

$$(G/M)/_{(N/M)} \cong G/N$$

Lema: Na; bo $\varphi: G \rightarrow H$ homomorfizam grup

$$1) \text{ Če je } K \leq G \Rightarrow \varphi^*(K) \leq H$$

$$2) \text{ Če je } K \triangleleft G \text{ in } \varphi \text{ surjektiven} \Rightarrow \varphi^*(K) \triangleleft H$$

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

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

Dokaz: \downarrow začít s φ na K

$$1) \varphi(K) = \text{im } \varphi|_K \quad \forall x \in \varphi(K) \quad \forall h \in H$$

$$2) \varphi: G \rightarrow H$$

$$\varphi(K) \triangleleft H$$

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

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

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

$$h = \varphi(g), g \in G \text{ surjektivnost}$$

$$h \times h^{-1} = \varphi(gk g^{-1}) \in \varphi(K)$$

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

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

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

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

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

$$g \in G$$

$$g \times g^{-1} \in \varphi(L)$$

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

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

Izrek: (Korespondencija izrek)

Naj bo G grupa in $N \trianglelefteq G$

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

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

Dokaz a)

$$\text{DN } H/N \leq G/N$$

Obiskatne smeri

Naj bo L pojavljajoča podgrupa $v G/N$

$\pi: G \longrightarrow G/N$ kanonična projekcija
 $(g \mapsto gN)$

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

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

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

Uporabna:

① G poljubna grupa, $a \in G$

$\langle a \rangle$

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

Dokaz:

Redimo da $\text{red } a = \infty$

$p: \mathbb{Z} \rightarrow A$ p je homomorfizem
 $n \mapsto a^n$ p je sur. je inj
 $\ker p = \{0\}$

Redimo da $\text{red } a = n$

$p: \mathbb{Z}_n \rightarrow \langle a \rangle$
 $n \mapsto a^n$

je $\text{cp}: \text{im } p = \langle a \rangle$

$m \in \ker p \Leftrightarrow a^m = 1 \Leftrightarrow m|n$

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

1: red o izomorfizmu $\mathbb{Z}/\ker p \cong \text{im } p$

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

② Podgrupe v \mathbb{Z}_n

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

Po korespondencijom izreke je H podgrupa v \mathbb{Z}_n oblike $H/n\mathbb{Z}$, kjer je $H \leq \mathbb{Z}$, $n \mathbb{Z} \leq H$

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

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

Ideja dokaz: $p: k\mathbb{Z} \xrightarrow{\text{Dž}} \mathbb{Z}_d$ p je epimorfizem
in $\ker p = n\mathbb{Z}$

(3)

Trditev: Nej bo G grupa ne trivialne
 G nima pravih ne trivialnih podgrup
 $\Leftrightarrow \exists p$ prostovilo, da je $G \cong \mathbb{Z}_p$

Dokazi:

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

$$|H| \mid p \Rightarrow |H| = 1 \text{ ali } |H| = p$$

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

(\Rightarrow)

$a \in G$ anti

$\langle a \rangle$ je ne trivialne grupe

Po predpostavki je $\langle a \rangle$ celo grupe.

G je ciklične

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

Po prejšnjem trditvi (2) sledi če je n sestavljen na stevil, potem ima G prave ne trivialne podgrupe

Torej je n prostovilo

④ Izrek: (Cauchyjev izrek za abelove grupe)

Naj bo G končna abelova grupa.

Naj bo p prstevilo de $p \mid |G|$. \Rightarrow

Potem $\forall G \exists a \in G$. red $a = p$

Lema: Naj bo G grupa, $N \triangleleft G$, $a \in G$ red $a = n$
Potem red $aN \leq G/N$ deli n

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

$$\pi(a^n) = \pi(a)^n = (aN)^n$$

1 1 To je red $aN \mid n$

Dokaz: z indukcijo po modi $n = |G|$
bazen indukcije:

$$|G|=p \Rightarrow G \cong \mathbb{Z}_p \quad 1+p\mathbb{Z} \text{ ima red } p$$

Rezimo da $|G| > p$

po ③ ima G pravu netrivialno podgrubo
rezimo N (ker je G abelova so vse
podgrupe edinke)

$$|G| = |N| \cdot |G/N| \quad \text{Lagrange}$$

$$p \mid |N| \text{ ali } p \mid |G/N|$$

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 abelove in $|G/N| < |G|$

po indukcijski predpostavki

G/N vsebuje aN reda p

red $aN \mid \text{reda}$

$$\text{reda} = p \cdot k$$

$$a^{pk} = 1$$

$$(a^k)^p = 1$$

To je \exists element de red $= p$

$$\textcircled{5} \quad p: S_n \rightarrow \{-1, 1\}, \quad \circ$$

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

p je homomorphismus

$$\ker p = \{\pi \in S_n : \operatorname{sgn} \pi = 1\} = A_n \quad A_n \triangleleft S_n$$

$$1. \text{ ist } \circ \text{ izomorfizmus } \quad S_n/A_n = \mathbb{Z}_2$$

$$\textcircled{6} \quad F \text{ naj bo polje}$$

$$p: GL_n(F) \rightarrow F^*$$

$$p(A) = \det A \text{ je homomorphismus } \Rightarrow$$

$$\ker p = \{A \in GL_n(F) : \det A = 1\} = SL_n(F)$$

$$1. \text{ ist } \circ \text{ izomorfizmus } \quad SL_n(F) \triangleleft GL_n(F)$$

$$GL_n(F)/SL_n(F) \cong F^*$$

(7.) G_1, G_2 grup:

$G_1 \times G_2$ 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 $G_1 \times G_2$

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

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

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

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

$\tilde{G}_1 \cong G_1$

$$(g_1, 1) \mapsto g_1$$

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

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

$$\rho: (g_1, g_2) \mapsto g_2 \quad \text{je operacija}$$

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

⑧ $\text{Inn } G = \{ f_a : G \rightarrow G \text{ : } f_a(g) = aga^{-1} \}$

↓

konjugiranje z elementom a
(Nekanj; automorfizmi)

$$\text{Opazimo: } (f_a)^{-1} = f_{a^{-1}}$$

$$f_a \circ f_b = f_{ab}$$

z drugimi besedami: imamo homomorfizem

$$\Phi: G \rightarrow \text{Inn } G \quad \Phi \text{ je surjektiven}$$

$$\Phi(a) = f_a$$

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

$$\ker \Phi = \{ a \in G : f_a = \text{id}_G \}$$

$$f_a = \text{id}_G \Leftrightarrow f_a(g) = g \quad \forall g \in G$$

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

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

$$\Leftrightarrow a \in Z(G)$$

↑ center (elementi, ki končno rajo
z ujemni)

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

Opomba
 $\text{Inn } G$ je podgrupa v automorfizmih

$$\text{DN: } \text{Inn } G \triangleleft \text{Aut } G$$

$$\text{Out } G = \frac{\text{Aut } G}{\text{Inn } G} \quad \dots \text{ grupa zunanjih
automorfizmov}$$

(niso dejanski automorfi)

Kocientni koldarji in algore

K naj bo koldar

Pozeljimo na množenje

K za sestavljanje je Abelova grupe

če je $I \leq K$ za sestavljanje, lahko naredimo
abelovo grupto $K/I : (a+I)$

$$\text{operacija: } (a+I) + (b+I) = (a+b)+I$$

$$\text{na } K_I \text{ bi radi vpeljeli množenje} \\ (a+I) \cdot (b+I) = (ab+I)$$

av te deluje?

Definicija: Naj bo k kolobar in $I \subseteq k$
 $I \neq \emptyset$. Pravimo da je I ideal če velja

a) $(I, +)$ je podgrupa v $(k, +)$

$$\forall a, b \in I \quad a - b \in I$$

b) $\forall a \in I \quad \forall x \in k \quad xa \in I$

c) $\forall a \in I \quad \forall x \in k \quad ax \in I$

Opomba:

① Pozej b) lahko pisemo v obliki $Ik \subseteq I$
Prav tako pozej c) $Ik \subseteq I$

② Če I zadaja pogojema a) in b)

pravimo da je I lan ideal

če iz določa a) in c) je dobiti ideal

Včasih idealnon recimo obujestranski ideal

Zgled:

- ① Vsak kelobar ima vsej dve ideale
{0}, ki sta vedno idealni

Kelobariji ki imajo le tisti dve ideali
pravimo enostavni kelobarji;

K kolobar

I je ideal u K , če

$I_1: \forall a, b \in I. a - b \in I$ (je podgrupa \mathbb{Z}^+)

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

Zgled:

$ak = \{ax; x \in K\}$ je lesni ideal u K

če je K komutativen, je $ak = ka$ obvezno ideal u K .

Pravimo mu glavní ideal u K generiran za
(vsek ideal u K ki vsebuje q vsebuje ak)

K nekomutativen: Nejmanjši ideal, ki vsebuje q

$ak = \{vse končne vrste \sum a_i x_i; a_i \in k\}$

Ideal v \mathbb{Z} :

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

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

$\left\{ \begin{bmatrix} ab & \\ 0 & 0 \end{bmatrix}, a, b \in \mathbb{R} \right\}$ je lesni ideal, nila.

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

DN: $\mathbb{R}^{n \times n}$ je enostaven kolobr

Opozba: Nejbo A algebra nad poljem FF

Ideal: I_2 , namesto I_1 , podprostor v A-ju

Trdimo $I_1 + I_2 \Rightarrow$ podprostor v A

$$\alpha \in I_1 \quad \alpha \in I_2$$

$$\alpha \cdot a = \alpha(1 \cdot a) = (\alpha \cdot 1) \cdot a \quad \underset{\alpha \in I_1}{\underset{\alpha \in I_2}{\in I}}$$

Nemesto podprostor lahko recemo
abelov podgrupe

Trditev: Nej bo k klobobar in I ideal.

Potem je $\frac{R}{I}$ z operacijama

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

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

je klobobar. Pravimo mu kvocientni:
(faktoršč.) klobobar.

Dokaz:

- + je dobro določljivano (venjo iz grup)
- je dobro določljivano

Rečimo da $a+I = a'+I$ in $b+I = b'+I$

Dokazujemo $(ab)+I = (a'b')+I$

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

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

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

Lastnosti klobbarja izhajajo iz tege da je k klobobar.

Ničlev $\frac{k}{I}$: $0+I$

enica v $\frac{k}{I}$: $1+I$

Trditev: Naj bo I ideal v K

če I vsebuje nek obrnljiv element kolobarja K , potem $I = K$

Dokaz:

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

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

Torej $K = I$

Opomba: V prejšnjih trditevih je dovolj da je I

lev: (ali: desni) ideal

Trditiv: Naj bosta I, J ideal v K

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

b) $I \cdot J = \{ \text{vsekakrone vsote } \sum_{i,j} x_i y_j : x_i \in I, y_j \in J \}$
je tudi ideal

c) $I + J$ je ideal

Dokaz:

a) DN

b) $I + J$ je očitno podgrupa za sestanje

$$\cdot \sum_{i,j} x_i y_j, x_i \in I, y_j \in J$$

$$x \in K \quad x \sum_{i,j} x_i y_j = \sum_{i \in I, j \in J} (x x_i) y_j \in I + J$$

Izrek: (1. izrek o izomorfizmu)

Naj bo $\varphi: k \rightarrow L$ homomorfizem
kolobarjev. Potem je $\ker\varphi$ ideal v k
in velja $k/\ker\varphi \cong \text{im } \varphi$

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 $x \in \ker\varphi$

$\psi: k/\ker\varphi \rightarrow \text{im } \varphi$

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

je dobro določen izomorfizem kolobarjev



Izrek: (2 izrek o izomorfizmu)

Naj boosta I in J idealni 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) Podkotlobarji v K/I so netanko oblike L/I , kjer je L podkotlobar v k, ki vsebuje I

b) Ideal v K/I so netanko oblike J/I , kjer je J ideal v k, k: vsebuje I

Definicija: Naj bo M ideal v kolobarju K . Pravimo da je M maksimalen ideal v K , če med M in K nima nobenega drugega idealja.

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

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

Opomba: Komutativnost je nujna:

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

Dokaz:

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

$M+aK$ je ideal (vsota dveh idealov je ideal, ker je K komutativen ideal DN)

$$M \subsetneq M+aK \subseteq K$$

Zrazi: 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 $(a + M)$ obrnjiv v K/M

(\Leftarrow)

Naj bo $I \triangleleft K$ $M \subsetneq I \subseteq K$

$\exists a \in I, k: n: v M$

$$a + M \neq 0 + M$$

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

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

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

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

Izrek: Naj bo K poljubni kolobar
Potem je \mathbb{V} pravi ideal v K vsebovan
v nekem maksimalnem idealu

Dokaz uporabi: Zornova lema:

X naj bo delno urejena množica

Verige v X : $y \subseteq X$. $\forall a, b \in y$. $a \leq b \vee b \leq a$

Zgornja meja neke podmnožice Y :

$$m \in X. y \subseteq m, \forall y \in M$$

Maksimalen element množice X : tak $m \in X$, da
 $\forall a \in X. m \leq a$

Zornova lema: Naj bo X delno urejena
množica: Če ima \mathbb{V} verige v X zgornjo mejo,
potem X vsebuje maksimalen element

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

\mathcal{J} naj bodo vsi pravi ideali v K , ki
vsebujejo I

$\mathcal{J} \neq \emptyset$, ker $I \in \mathcal{J}$

\mathcal{J} lahko delno uredimo z inkluzijo

Vzemimo poljubno verigo U v \mathcal{J}

$$U = \bigcup_{j \in U} J_j \quad \text{Trdimo } U \in \mathcal{J}$$

U je ideal v K

- $a, b \in U. \exists J_1, J_2 \in U. a \in J_1, b \in J_2$
BTSZS. $J_1 \subseteq J_2$ (ker je U veriga)

$$a - b \in J_2 \subseteq U$$

- $a \in U, x \in K, \exists J \in U. a \in J$
 $ax, x \in J \subseteq U$

$U \neq K$

$$\text{če } U = K \Rightarrow 1 \in U \Rightarrow \exists J \in U. 1 \in J \Rightarrow J = K$$

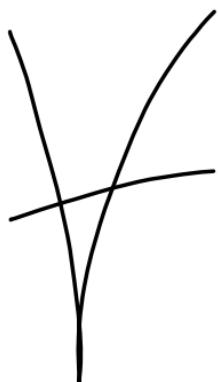


Po zornovi lemi \mathcal{J} vsebuje maksimalen element M
Mak $M \neq K$ ICM

M je maksimalen ideal v K

Rečimo $\exists N \triangleleft K. M \subset N \subsetneq K$. N je pravi ideal
v K , ki vsebuje I , torej $N \in \mathcal{J}$ *

Zapiski od Urske na
discordu



Od zadnječ

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

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

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

$$\underline{G} = H + K$$

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

$$x = 1 \cdot x = (am + bn)x = amx + bnx \quad \text{---}$$

$$\cancel{amx} + bnx = \cancel{bnx} = 0$$

" " 0
 $|G|$

$$\Rightarrow bnx \in H$$

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

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

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

ker sta min n tuj: je dovolj premisliti

$$\forall p \in P, p \neq 0 \Rightarrow p \nmid |H| \wedge p \nmid |K|$$

Rečimo da $p \nmid m$ in rečimo da $p \mid |H|$

Po cauchyjevi izrekvi

grupa H vsebuje element y reda p

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

m: n p sta tuj: $\exists c, d \in \mathbb{Z}$.

$$cm + dp = 1$$

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

X

Primer: G abelova grupe modi $6 = 2 \cdot 3$

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

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

Edine abelove grupe modi 6

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

Oponba: $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \not\cong \mathbb{Z}_4$, kerime

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

Posledica: Naj bo \$G\$ končna abelovska

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

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

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

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

Definicija: $|G| = p^n$; $p \in \mathbb{P}$ pravim o
da je G p -grupe

Torej: V končne abelove grupe je
vsota p -grup (za razloge pravilnosti)

Davalj 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 mod p

Dokaz: $|G| = p^m$

(\Rightarrow) Če je G ciklična in ima mod p^m
 $\Rightarrow G \cong \mathbb{Z}_{p^m}$

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

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

(\Leftarrow) indukcija po mod

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

Recimo da te trdite velja za vse grupe mod $< p^m$

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

$$N = \{x \in G; p \cdot x = 0\}$$

$$N \subseteq \{ \dots \} \text{ saj ima } N \text{ mod } p$$

če ima $x \in N$ red p je $\langle x \rangle$ podgrupa mod p
zato je $N = \langle x \rangle$; to je $x \in N$

Oglejmo si

$$\varphi: G \rightarrow G$$

$$\varphi(x) = px$$

φ je homomorfizem grup

$$\ker \varphi = N$$

$$G/N \cong \text{im } \varphi \text{ je podgrupa v } G$$

G/N je p-grupa nekrivalne

ker je lahko sledenje kaj podgrupov G
ime je vedno nekakšno eno podgrupo
moci p

Po indukcijski predpostavki je G/N ciklična

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

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

$$x-ka \in N$$

$$\forall a \in N \quad x = ka + n \quad n \in N$$

$$G = \langle a \rangle + N$$

$\langle a \rangle$ je nekrivalne ciklične p-grupa

torej $\langle a \rangle$ vsebuje element reda p ;

$$\langle b \rangle \text{ ima mno\v{c} p} \Rightarrow \langle b \rangle = N$$

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

$$\Rightarrow G = \langle a \rangle$$

Lema: Maj bo G končna abelova

podgrupa $N \leq G$ tisti ciklione podgrupe v G , ki ima največjo moč 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 n: ciklione. $|G| = p^m$

Indukcija po mapi $|G|$

Po prejšnji tem: ima G vsaj dve podgrupe moči p

C ima po prejšnji tem: natančno eno podgrupu moči p

Zato \exists podgrupa moči p v G ki n: vsakovrstna v C . označimo jo $\mathbb{Z}N$

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

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

2. zreda o izrekovanju:

$$\frac{HN}{N} \cong \frac{H}{N \cap H}$$

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

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

ima največjo moč med ciklonskimi podgrupami grupe G/N in ima največjo moč med ciklonskimi.

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

Po indukcijski predpostavki $\exists K \leq G$

$N \leq K$ da je

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

$$G = C \oplus K$$

* sledi

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

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

$$= (y + k) + N = k \in K$$

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

$$y + n \in C + N$$

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

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

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

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

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

+ v drugi direktni vsoti

$$\Rightarrow x \in N \quad *$$

Postedica: Vsi končni abelove p-grupe
je direktna vsota cikličnih p-grup

Postedica: Vsaka končna abelova grupa
je direktna vsota cikličnih grup
katerih moči se podariti prostovoljno.

Kako vidimo ali dva razcega abelovih grup na direktni vsoti ciklacionih p-
grup predstavljata isto grupo
da izomorfizma načinoma

G, \bar{G} kononi abelovi grupi: $\varphi: G \rightarrow \bar{G}$
izomorfizem

$$|G| = |G| = p_1^{e_1} \dots p_n^{e_n}$$

$$G = H_1 \oplus \dots \oplus H_k \quad |H_i| = p_i^{c_i}$$

$$\bar{G} = \bar{H}_1 \oplus \dots \oplus \bar{H}_n \quad |\bar{H}_i| = p_i^{c_i}$$

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

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

$$\varphi_{|H_1}: H_1 \rightarrow \bar{H}_1$$

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

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

Problem izomorfosti kononih abelovih grup se zato zreducira na to da je steve kononi abelovi p-grupi; i.e. merni:

Izrek: Nej boste G in \tilde{G} kononi abelovi p-grupi; tencirati:

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

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

Predpostavimo

$$k_1 \geq \dots \geq k_m$$

$$l_1 \geq \dots \geq l_n$$

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

$$\text{Dokaz: } f: G \rightarrow \tilde{G} \quad |G| = |\tilde{G}|$$

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

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

Po indukciji na r

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

Recimo da velja za vse grupe modri p's ker

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

Kubistna potenca

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

izpostavljam latice ker je abelova

$$\varphi_{pG}: pG \rightarrow p\tilde{G}$$

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

φ_{pG} je izomorfija

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

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

$$\cong \mathbb{Z}_p^{k_1-1} \oplus \dots \oplus \mathbb{Z}_p^{k_{m-1}-1} \quad = 0, \text{ ker } p \cdot n = 0 \text{ v } \mathbb{Z}_p$$

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

pG je izomorfija in imata manjšo moč kot G

Po induktivnosti prepreostale

dovemo

$$m' = n'$$

$$k_{i-1} = l_{i-1}$$

$$k_i = l_i$$

Torej

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

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

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

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

$$\Rightarrow n = m$$

Torej je izrek dokazen

Torej vsake abelove abelove

grupe

Ponsetek: Vseke končne abelove grupe je izomorfna direktni vsotji cikloških podgrup, ki so p-grupe za male razlike približno

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

Zg: s je enačbo je vrstnega reda direktnih sumandov natančno



use abelian type mod 14002

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

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

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

Grp jn 15

Na podoben način lahko generira.

lahko generira

končno generiran abelova

abelova grupa

Izrek:

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

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

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

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

ideja dokaza:

G abelova grupa \Leftrightarrow končna red

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

$T(G)$ je podgrupa v G

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

$$nh = 0$$

$$m \cdot n (g^{-1}h) = mn g - mn h = 0 - 0 = 0$$

$T(G)$... torzijske podgrupe v G

za G pravimo da je brez torzije,

$$\text{če je } T(G) = \{0\}$$

$G/T(G)$ je končno generirana

abelova grupa brez torzije

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

Rečimo da $g + T(G)$ ima končen

red $\Rightarrow g \in T(G)$

$$\left(\forall g \in \frac{G}{T(G)}, g + T(G) = 0 + T(G) \right)$$

\Downarrow

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

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

glede na $ng \in T(G) \Rightarrow$

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

$$(m) \cdot g = 0 \Rightarrow g \text{ je končen}$$

red ter je $g \in T(G)$

Izhaja se: če je G končna generirana abelova grupe brez torzije, potem je $G \cong \mathbb{Z}^n$ za nek n

Brez dokaza

Trditev: V končno generirane abelove grupe je direktno vsebuje neke končno generirane 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

$$G/T(G) \cong \mathbb{Z}^n \quad ; \\ e := (0, \dots, 0, 1, 0, \dots, 0) \in \mathbb{Z}^n$$

Vsih element \mathbb{Z}^n lahko na enakovreden način napisimo kot

$\alpha_1, \dots, \alpha_n$ elementi \mathbb{Z}^n ima Baza zato ima tudi $G/T(G)$ baza $f_1 + T(G), f_2 + T(G), \dots, f_n + T(G)$

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

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

Dokazemo lahko da so f_1, \dots, f_n baza \mathbb{Z}^n

$$H \rightarrow \mathbb{Z}_n$$

$f_i \rightarrow e_i$ jo izomorfizem grup

izrazim de je $G = H \oplus T(G)$

Ker je $H \cong \mathbb{Z}_n$ njene elemente končne redne. Zato je $H \cap T(G) = \{0\}$

$$\underline{G = H + T(G)}$$

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

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

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

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

~~Dokaz~~

Dokazati moemo je, da je

$T(G)$ končna grupe.

$$G = H \oplus T(G)$$

$$T(G) \cong G_H$$

G_H je kvocient končne generirane

grupe je končno generirana

$T(G)$ je končno generirana grupa v letor:
ime & element končen red

$$T(G) = \langle t_1, \dots, t_m \rangle \quad m; t_i \neq 0$$

$$t \in T(G)$$

$$t = \alpha_1 t_1 + \dots + \alpha_m t_m$$

$$0 \leq \alpha_i < m:$$

Za vsi α_i imamo

končno-množje možnosti, zato imamo
končno-množje možnosti $\alpha_1 + \dots + \alpha_m$

$$\Rightarrow T(G) \text{ končna}$$

KONCNE GRUPE

delovanje grup

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

če \exists preslikave (DELOVANJE)

$$G \times X \longrightarrow X$$

$$(g, x) \longmapsto g \cdot x \quad (\text{samо} \quad \text{členke})$$

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

$$X \times G \longrightarrow X$$

$$(x, g) \longmapsto x \cdot g$$

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

$$2) x \cdot 1 = x$$

Recimo de meama leva

definije $G \curvearrowright X$ ($g \cdot x \mapsto g \cdot x$)

Potem tako b definiramo desna definanje

$$X \times G \rightarrow X$$

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

zakoj : 1) $\underline{\underline{vol}}$ -

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

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

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

◻

Opoomba: Maj G deluje na X

$$\text{Sym } X = \{X \rightarrow \rightarrow X\}$$

Delovanje poradi homomorfizem
grup

$$\phi: G \longrightarrow \text{Sym } X$$

$$\phi(g)(x) = g \cdot x \quad g \mapsto (x \mapsto g \cdot x)$$

ϕ je homomorfizem

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

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

$$\phi(g) \phi(h)(x)$$

Obretna: Če imamo homomorfizem

$$\phi: G \longrightarrow \text{Sym } X \text{ potem } G \rtimes X$$

$$\text{S predpisom } g \cdot x = \phi(g)(x)$$

Oponba: Zekoji je $f: X \rightarrow X$, $f(x) = g \cdot x$
b: jek c: j?

Sarj:

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

inj: $f(x) = f(y)$
 $gx = gy$

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

Recimo da imamo delovanje G na X

$$\Phi: G \longrightarrow \text{Sym } X$$

$\ker \Phi$ imenujemo jedro delovanja

Pravimo, da je delovanje nesto če
je jedra trivialno ($\ker \Phi = \{1\}$)

Če je delovanje nesto:

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

$$\begin{matrix} \text{im} \\ G \end{matrix}$$

G je izomorfna neki podgrupi $\text{Sym } X$

Pravimo da se G vloži v $\text{Sym } X$

Primeri delovanja

1) Trivialno delovanje

$$g \cdot x = x \quad \forall g \in G, \forall x \in X$$

2) Grupa G deluje na G z levim množenjem

$$G \times G \longrightarrow G$$

$$(g, h) \longmapsto g \cdot h$$

Imamo homomorfizem

$$\Phi : G \longrightarrow \text{Sym } G$$

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

$$g \in \ker \Phi \Leftrightarrow \Phi g = \text{id}_G \Leftrightarrow \forall h \in G, g \cdot h = h$$

$$\Leftrightarrow g = 1$$

Cayleyjev : zek: \downarrow levo regularno
množenje z leve je torej zvesto delovanje

\Rightarrow vsaka grupa G se vloži v $\text{Sym } G$

V posebnem: G končna. $|G| = n$

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

3) G deluje na G

$$G \times G \longrightarrow G$$

$$(g \cdot h) \mapsto ghg^{-1}$$

DN: To je delovanje

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

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

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

G deluje na G/H

$$G \times G/H \longrightarrow G/H$$

$$g \cdot (xH) = (gx)H$$

Dobra definiranost?

$$\text{Reamo } xH = yH \Rightarrow \underline{g} \underline{x} \underline{H} = \underline{g} \underline{y} \underline{H}$$



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

$$\text{Ogleđenost: } (gx)^{-1}gy = x^{-1}g^{-1}gy = x^{-1}y$$

DN: To je delovanje

$$\in H$$

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

$$y^X = \{f : X \rightarrow Y\}$$

G deluje na y^X

$$G \times y^X \rightarrow y^X$$

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

Izreže se da je potrebno g^{-1} da deluje

To nij res delovanje

$$\text{ZRF} \quad 1 \cdot f(\bar{x}) \quad f(1^{-1}x) = f(x) \quad \checkmark$$

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

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

$$DN: \begin{array}{ccc} G \curvearrowright X & G \curvearrowright Y \\ (g, x) \mapsto gx & (g, y) \mapsto gy \end{array}$$

Potom $G \curvearrowright Y^X$

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

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

6) V nejbo vektorski prostor

$GL(V)$ vsi automorfizmi prostora V

$$GL(V) \cdot V \longrightarrow V$$

$$(R, v) \mapsto Rv$$

To je delovanje

?) K komutativen kôlôbar $\Rightarrow 1$

$$K[x_1, \dots, x_n]$$

S_n deluje na $K[x_1, \dots, x_n]$

$$\delta \cdot p(x_1, \dots, x_n) = p(x_{\delta(1)}, \dots, x_{\delta(n)})$$

to je delovanje

Orbite stabilizatorji, fiksne točke delovanja

Def.: Nej 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

$$\text{množica } G_x = \{g \in G : gx = x\}$$

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

$$g \cdot j^g \quad X^g = \{x \in X : gx = x\} = \text{fix}(g)$$

4) fiksne točke delovanja (invariante)

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

Lemaj: Nej G deluje na X

Recimo da $g \cdot x = y$

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

Dokaz:

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

Traditer: Nagj. G deluje na X
Potem je $G_x \leq G$

Dokaz:

$$1 \in G_x \text{ tarej } G_x \neq \emptyset$$

$$g, h \in G_x \quad gx = x = hx$$

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

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

Potem je \sim ekvivalentne relacija na X in ekvivalenčni razred elemente x jo njegeva orbita Gx

Dokaz

Refleksivnost $\forall x \in X$

Simetričnost $\forall x,y \in X. y = g \cdot x \Rightarrow x = g^{-1} \cdot y$

tranzitivnost $\forall x,y,z \in X. y = g \cdot x \wedge z = h \cdot y \Rightarrow z = h \cdot g \cdot x = h \cdot y = z$

Ekvivalenčni razredi x_G

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

Oznake: koncentrično 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

tranzitivno delovanje

Zájed

1) Naj G deluje na G = levim množením.

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

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

Transitivno delovanje

$$Gx = \{g \in G : gx = x\} = \begin{cases} 1 \\ \downarrow \\ g = 1 \end{cases}$$

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

② G nej deluje na G s kanjugáciou

$$G \times G \longrightarrow$$

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

$$x \in G$$

$$G_x = \{g \in G; g * x = x\} = \{g \in G; g * g^{-1} = x\}$$

$$= \{g \in G, g * x = x * g\} =: C_G(x)$$

..., centralizator elementu $x \in G$

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

$$= \underbrace{\{g * g^{-1}; g \in G\}}_{\text{kanjugáciu rázred elementu } x \in G} = C_G(x)$$

kanjugáciu rázred elementu $x \in G$

$$G^G = \{x \in G; g * x = x\} = \{x \in G, g * x = x * g\} = C_G(G)$$

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

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

Orbitor xH

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

transitívne delovanie

Fikone točke (invariantne) delovacie

$$K[x_1, \dots, x_n]^{S_n} = \text{tieto polinomy, kde jih}$$
$$\left\{ \begin{array}{l} \forall \delta \in S_n, \delta \cdot p(x_1, \dots, x_n) = p(x_{\delta(1)}, \dots, x_{\delta(n)}) \end{array} \right\} =$$
$$\{ p(x_1, \dots, x_n) : \forall \delta \in S_n, p(x_{\delta(1)}, \dots, x_{\delta(n)}) \} =$$

symetrické polinomy

$$x_1 + x_2 + x_3$$

$$x_1 x_2 + x_2 x_3 + x_1 x_3$$

Izrek o orbiti in stabilizatorju

Naj grupa G deluje na množici X
orbita \leftarrow indeks stabilizatorja

- a) $\forall x \in X. |G \cdot x| = |G : G_x|$ (deluje tudi
na nekončne grupe)
- b) G končna grupa $\Rightarrow |G| = |Gx| \cdot |G_x|$

Dokaz:

a) Izsemam bijekcijo med množicama
 Gx in G/G_x

$$\alpha: Gx \longrightarrow G/G_x$$

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

Ali je α dobro definirana

$$gx = hx \Rightarrow g \cdot G_x = h \cdot G_x$$

$$gx = hx$$

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

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

$$\Rightarrow h \cdot G_x = g \cdot G_x$$

α je surjektivna

α injektivna

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

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

$$gx = hx$$

✓

b) direktna posledica

Izrek

Nej grupa G deluje na X , X konena množica. Potem obstajajo elementi

$$x_1, \dots, x_r \in X - X^G$$

\nwarrow kisti x_i ki jih vse gji postopoma

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

Dokaz: Množica X je disjunktna unija nekih orbit delovanja.

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

Vsake akra točke ima enoelementno orbit

Ostali elementi in jih je r (ker je G konena)
recimo da jih je r (ker je G konena)

$$\text{To je } |X| = |X^G| + |Gx_1| + \dots + |Gx_r|$$

\uparrow \nwarrow vsi ostale
orbiti z 1 elementom orbiti

x_i : jih se predstavijo reči o teh orbit velikosti več kot 1

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

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

Posledica:

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

Potem velja

$$|X| \equiv |X^G| \pmod{p}$$

Dokaz:

Po prejšnjem izreku lahko napišemo

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

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

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

$$\text{Sledi: } p \mid (|X| - |X^G|)$$



Izrek (Burnsideova lema)

Naj končna grupe 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 dve načine

$$\begin{aligned} & |\{(g, x) \in G \times X; gx = x\}| = \\ &= \sum_{x \in X} |\{g \in G; gx = x\}| = \sum_{x \in X} |G_x| = \\ &= \sum_{x \in X} \frac{|G|}{|G_x|} = |G| \cdot \sum_{x \in X} \frac{1}{|G_x|} = \\ &= |G| \sum_{\substack{\sigma \in X/G \\ \text{orbit}}} \underbrace{\sum_{x \in \sigma} \frac{1}{|G_x|}}_{\text{orbite}} = |G| \cdot \underbrace{\sum_{\substack{\sigma \in X/G \\ \text{orbit}}} \frac{1}{|\sigma|}}_1 = \\ &= |G| \cdot \sum_{\sigma \in X/G} 1 = |G| \cdot |X/G| \end{aligned}$$

drugi način

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

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

Primer:



barvamo ogljisca z n barvami;



je isto barvanje

st barvanj glede nato identifikacija

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 $|X/G| = ?$

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

$$|X^{id}| = |\{\text{kakšna barvanja, ki jih id pusti nemeno}\}| = |X| = n^4$$

$$|X^r| = |\{x \text{ za } 90^\circ \text{ pusti nemeno}\}| = \underbrace{n}_{\text{barva}}^n$$

$$\text{Podobno } |X^{r^2}| = n$$

$$|X^{r^3}| = n^2$$

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

Razredna formula in Cauchyjev izrek

Posledica: Razredna formula

Naj bo G končna grupa

Potem obstajajo $x_1, \dots, x_r \in X - Z(G)$

de 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 s posebnimi

formule ko $G \curvearrowright G$ s konjugiranjem

$$G \times G \longrightarrow G$$

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

Posledica: Maj ba G končna grupa.

Potem je $Z(G) \neq \{1\}$

Dokaz: $B\bar{S} \geq S^G_n$; abelova

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

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

\nearrow
 $C_G(x_i) \neq G$, ker potem b:
 $x_i \in b : 1 \cup \text{centri}$

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

Tamp mora bit: $p \mid |Z(G)|$

■

Posledica: Naj bo G grupa mod p^2 .

Potem je G abelova

Dokaz: Naj bo G nekomutativna grupa

mod p^2 . Sledi: $|Z(G)| = p$

$|G/Z(G)| = p$ torej je ciklična

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

$$G = Z(G) \sqcup xZ(G) \sqcup \dots \sqcup x^{p-1}Z(G)$$

Vzemimo $a, b \in G$

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

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

$$ab = x^i z_1 \cdot x^j z_2 \quad z_1, z_2 \text{ sta v centru}$$

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

$$= x^j z_2 x^i z_1 = ba$$

torej je G abelova

ker sta potencije iste glede elemente



Izrek (Cauchyjev izrek)

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

Dokaz:

Za abelove grupe smo izrek že dokazali:

Indukcija po $|G|$

$|G|=p$: je cikločna točka ✓

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

Beszs G n: abelova. Uporabimo razredno formulo

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

Rečimo da $p \mid |Z(G)|$

\Downarrow
abelova grupa

Potem po Cauchyjevu 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:

Lagrangev izrek: G končna $H \leq G$
 $\Rightarrow |H| \mid |G|$

Obraz? Recimo da $k \mid |G|$. At: vedno obstaja $H \leq G$, $|H|=k$?

An nima podgrupe modi 6 :=
Kaj če izberemo delitelj $|G|$ ki je potenza nekega prastevila?

Def: Maj bo G končna grupa, $H \leq G$

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

- $|H|=p^{\alpha}$

(Naj večji p -delitelj
prastevila
pa modi)

- $p^{\alpha} \mid |G|$

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

Trek Sylowa:

Naj bo G končna grupa $p \mid |G|$

- a) Če $p^e \mid |G|$ potem v G obstaja podgrupa modi p^e
(med drugim v $|G|$ obstaja vsaj ena p -podgrupa Sylowa)
- b) Vsake 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 agrupi G . Potem veljata dve zvezni
- $n_p \mid |G|$
 - $n_p \equiv 1 \pmod{p}$

Dokaz:

a) z indukcijo po moci $n=|G|$

$$n=p \quad \text{ocitra}$$

Rečimo da trditev za vse grupe moci $< n$

Dokazujemo za grupe moci n

Locimo 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

$$|G/Z| = \frac{n}{p} \quad \text{v}^n$$

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

Po indukcijski predpostavki grupa G/Z vsebuje podgrupo moci p^{e-1} . Ta podgrupa je oblike H/Z ker je $H \subseteq G$

$$|H| = |H/Z| \cdot |Z| = p^{e-1} \cdot p = p^e$$

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

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

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

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

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

(ker x_i ni v centru)

Po indukcijski predpostavki $C_G(x_i)$ vsebuje podgrupo moci p^e

b) Dokaž

Pomožen rezultat od zadnjic:

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

Tonem $|X| \equiv |X^G| \pmod{p}$

Po a) tacki v G obstaja vsajena p-podgrupa Sylowa S .

Naj bo sedež $H \leq G$ p-podgrupa

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

$H \curvearrowright X$ z levim množenjem

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

Po \star $|X| \equiv |X^H| \pmod{p}$

$$|X| = |G/S| = \frac{|G|}{|S|} \quad \text{zarač množinskega faktora}$$

po tem $|X^H| \neq \emptyset$ $|X|$ ni deljivo s p

$$\exists x_0 \in X^H$$

$$x_0^{-1} x_0 S = S$$

$$x_0^{-1} a x_0 S = S$$

$$x_0^{-1} a x_0 \in S \Rightarrow a \in H$$

$$a \in x_0 S x_0^{-1} \Rightarrow x_0^{-1} a x_0 \in H$$

$$H \leq x_0 S x_0^{-1}$$

$$x_0 S x_0^{-1} \leq G$$

$$|x_0 S x_0^{-1}| = |S| \quad (\text{koneciranje je bijekcija})$$

Zato je $x_0 S x_0^{-1}$ tudi p-podgrupa Sylowa

ki vsebuje H

c) Dokaž

S naj bo fiksna p -podgrupa Sylova

H naj bo poljubna p -podgrupa Sylova

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

H in xSx^{-1} sta p -podgrupe Sylova v G , torej imata isto množ. Zato $H = xSx^{-1}$

d) Dokaz

$X = \text{Syl}_p G = \{\text{vse } p\text{-podgrupe Sylowa}\}$

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

$$n_p = |X|$$

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_{sa} : $\{g \in G; g \cdot S = S\} =$

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

(normalizator S v G)

ljud o orbiti in stabilizatorju:

mod orbite $S = \text{indeks stabilizatorja v } G$

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

deli $|G|$

Naj S deluje na X s konjugiranjem

$$P_0 \nmid |X| = |X^S| \text{ mod } p$$

n_p''

$$\text{Trdimo } X^S = \{SS^{-1}\}$$

Gotovo velja $S \in X^S$

Naj bo $T \in X^S$

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

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

z drugim: besedami $S \subseteq N_G(T)$

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

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

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

Dobimo $n_p \equiv 1 \pmod{p}$

Opomba:

Iz dokaza sledi:

$$n_p = |G:N_G(S)| \quad S \text{ neke podgrupa sylowa}$$

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

$$\Leftrightarrow G = N_G(S) \Leftrightarrow S \triangleleft G$$

"edina p-podgrupa sylowa je edinka"

Primer:

p, g različni prostovlni $p < g$

Kaj lahko pavema o grafih modi $p \cdot g$

$$|G| = p \cdot g$$

$\forall G$ obstaja vsaj ena p -podgrupa Sylowa

$$P, |P|=p$$

$\forall G$ obstajajo vsajene g -podgrupe
Sylowa $Q, |Q|=g$

$n_p | p \cdot g$ in $n_p \equiv 1 \pmod{p}$ $n_p \in \{1, g\}$

$n_g | p \cdot g$ in $n_g \equiv 1 \pmod{g}$ $n_g \in \{1\}$

(ker je \exists biljek $p \pmod{g}$ $p \equiv 1 \pmod{g}$
ampak $p < g$)

Torej Q je edina g -podgrupa Sylowa

$$\Rightarrow Q \trianglelefteq G (\Rightarrow G \text{ ni enostavna})$$

Opazimo: $|P \cap Q|$ deli $p = n_g$

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

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

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

$$PQ = G$$

Glede n_p imamo dve možnosti:

$$\textcircled{1} \quad n_p = 1 \Rightarrow P \trianglelefteq G$$

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

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

$$\textcircled{2} \quad n_p = g$$

$$\text{Lahko se razdi: } |S_3| = 2 \cdot 3$$

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 modi ??

Končne enostavne grupe

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

Kako razgledajo končne enostavne grupe?

Primer: G končna abelova grupa. Kdaj je
enostavna

"
Abelova grupa z natančno določenimi podgrupami

$$DN: |G|=p \wedge G \cong \mathbb{Z}_p$$

Primer:

$$A_n \leq S_n \quad |S_n : A_n| = 2 \Rightarrow A_n \text{ je edinko}$$

$A_3 \cong \mathbb{Z}_3$ en estorne

A_n ni en estorne

$$N = \langle (12)(34), (13)(24) \rangle \cong \underbrace{\mathbb{Z}_2 * \mathbb{Z}_2}$$

Kleinova
cetverka

DN:

$$\forall \pi \in A_n, \pi(12)(34)\pi^{-1} \in N$$

$$\pi(13)(24)\pi^{-1} \in N$$

Izrek:

Ce je $n \geq 5$ je A_n enostavna

Dokaz: $N \neq A_n$. $N \neq S_3$

Dokazemo da je $N = A_n$

(1) Recima de N vsebuje vsaj en tričikel

$B\bar{S}ZS.$ $(123) \in N$

Vremo poskusiti

$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ a & b & c & \dots & t \end{pmatrix}$ naj bo sode
permute

$\sigma(123)\sigma^{-1} \in N$

$\begin{pmatrix} a & b & c \\ 1 & 2 & 3 \end{pmatrix}$

Torej $(a \ b \ c) \in N$ za vsa a, b, c

Anje generirane z usemimi 3-cikli

Torej $N = A_n$

(2) N ne vsebuje nobenega 3-cikla

Lactimo se vec primer

2.1 Recima de Π , vsebuje Π katerih
razcep na disjunktni cikel vsebuje
cikel dolzine ≥ 4

$\Pi = (a_1 \ a_2 \ a_3 \ a_4 \ \dots) \ (\dots) \ \dots \ (\dots)$

Potenje

$\Pi' = (a_1 \ a_2 \ a_3) \Pi (a_1 \ a_2 \ a_3)^{-1} \in N$

$\Pi' = (a_2 \ a_3 \ a_1 \ a_4 \ \dots) \ (\dots) \ \dots \ (\dots)$

Potenje $\Pi' \Pi'^{-1} \in N$

$\Pi' \Pi'^{-1} = (a_2 \ a_4 \ a_1) \in N$

N vsebuje tudi 3-cikel \rightarrow

(2.2) pi ne vsebuje nobene permutacije

katerih razcep na disjunktni cikli

bi vseboval cikel dolzine ≥ 4

(2.2.1) Recima de imenuje v N
permutacija oblike

$\Pi = (a \ b \ c) (a' \ b' \ c') \dots$

Potenje tudi

$\Pi' = (a' \ b' \ c) \Pi (a' \ b' \ c)^{-1} \in N$

$\Pi' = (a \ b \ a') (c \ c' \ b') \dots$

$\Pi' \Pi \in N$

$\Pi' \Pi = (a \ a' \ c \ b \ c') \quad$ Torej je
cikel dolzine vec kot 4 \rightarrow

(2.2.2) Recima de je v N permutacija

oblike $\Pi = (a \ b \ c) \dots$ sodskrivljena transpozicija

$\Pi^2 \in N$

$\Pi^2 = (abc)^2 = (acb)$ \rightarrow

(2.2.3) ostane se primer kje je vsi

elementi N produkt sodega stevila
transpozicij

Lactimo da je možnost

(2.2.3.1) Recima de je $(a, b) (a' b')$ v N

$(acb)(a'b)(a'b')(acb)^{-1} \in N$

$= (a \ c) (a' \ b')$

Opazimo:

$\underbrace{(a \ b)}_{\in N} \underbrace{(a' b')}_{\in N} \underbrace{(a \ c)}_{\in N} \underbrace{(a' b')}_{\in N} = (a \ c \ b) \in N$

\rightarrow

(2.2.3.2) V elementu N je produkt ≥ 4

disjunktnih transpozicij

$\Pi = (a_1 \ b_1) (a_2 \ b_2) (a_3 \ b_3) (a_4 \ b_4) \dots \in N$

Potenje $\Pi' = (a_3 \ b_2) (a_2 \ b_1) \Pi (a_2 \ b_1) (a_3 \ b_2)$

$\Pi' = (a_1 \ a_2) (a_3 \ b_1) (b_2 \ b_3) (a_4 \ b_4) \dots$

$\Pi' \Pi \in N$

$\Pi' \Pi = (a_1 \ a_3 \ b_2) \dots$ \rightarrow

Izberite se: (klasifikacija končnih enostavnih grup)

če je G končna enostavna grupa, potem sodi veno od naslednjih kategorij:

1) \mathbb{Z}_p , $p \in \mathbb{P}$

2) A_n $n \geq 5$

3) grupe L : jevnega tipa

npv: $SL_n(F)$

$$Z(SL_n(F)) = \{\lambda I, \lambda^n = 1\}$$

$$PSL_n(F) = \frac{SL_n(F)}{Z(SL_n(F))} \dots \text{projektivna}$$

je enostavna
(zakrov) vseh n)

4) 26 sporadičnih grup

Največja med njimi: je POŠAST
Moonshine theory ponovno s to grupo

Zakej so enostavne grupe $\Sigma \Sigma$?

\cap sigma sigma

G končne grupe

Če G ni enostavna, potem $\exists M \triangleleft G$ ki n:

rsebarana v nekaj vecji edinki (maksimalne edinki)

G/M je enostavna grupa

Poštepel nedeljujemo

$G \triangleleft M_1 \triangleleft \dots \triangleleft M_k \triangleleft \Sigma^1$

$G/M \quad M/M_1 \quad \dots \quad \frac{M_{k-1}}{M_k} \quad M_k$ vse enostavne

To je kompozicijska vrsta grupe

M_k poznamo in $\frac{M_{k-1}}{M_k}$ tudi poznamo



vse možnosti za M_{k-1}

Resljive grupe

Grupa G je resljiva, če obstaja

konečna zaporedje podgrup

$$\{1\} = G_0 \triangleleft G_1 \triangleleft G_2 \triangleleft \dots \triangleleft G_k$$

Vsebujo edinko večji
in kakšna velja: $\frac{G_{i+1}}{G_i}$ je abelova

Primer:

- 1) Abelove so vse resljive: $\{1\} \triangleleft G$
- 2) $A_n \triangleright \langle (12)(34), (13)(24) \rangle \triangleright \{1\}$
 \downarrow
kvocient
imamo 3
torej je abelova
- 3) $S_n \triangleright A_n \triangleright \langle (12)(34), (13)(24) \rangle \trianglelefteq \{1\}$
- 4) G je nekomentativna enostavna grupa
 $A_n \geq 5$ niso resljive

Trditev: Nej bo G resljive.

1) $H \leq G$ je tudi resljiva

2) $N \trianglelefteq G \Rightarrow G/N$ je resljiva

Dokaz:

imemo $\{1\} = G_0 \triangleleft \dots \triangleleft G_n = G$

$\frac{G_{i+1}}{G_i}$ so abelove

1) Gglejmo s:

$\{1\} = G_0 \cap H \triangleleft \dots \triangleleft G_n \cap H$
Faktorjevne celine

$$\frac{G_{i+1} \cap H}{G_i \cap H} = \frac{G_{i+1} \cap H}{(G_{i+1} \cap G_i) \cap H} \cong \\ \cong \frac{(G_i \cap H) G_i}{C_i} \leq \frac{G_{i+1}}{G_i}$$

$$\frac{H}{N \cap H} \cong \frac{HN}{N}$$
 abelova

$\frac{G_{i+1} \cap H}{G_i \cap H}$ podgrupe abelove je abelova

2) $\frac{G_{i+1} N}{N}$

$$\frac{\frac{G_{i+1} N}{N}}{\frac{G_i N}{N}} \cong \frac{G_{i+1} N}{G_i N} = \frac{G_{i+1} G_i N}{G_i N} \cong$$

$$\cong \frac{G_{i+1}}{G_{i+1} \cap G_i N} \cong \frac{\frac{G_{i+1}}{G_i}}{\frac{G_{i+1} \cap G_i N}{G_i}} \leftarrow \text{abelova}$$

kocient abelove je abelova

Trditev:

Naj bo G grupa in $N \triangleleft G$

če sta $N :> G/N$ rešljivi;

je tudi G rešljivo

Dokaz: $\{1\} = N_0 \triangleleft \dots \triangleleft N_k = N$

N_{i+1}/N_i abelovo

$$\{1\} = \frac{N_0}{N} \Rightarrow N_0 = N$$

$$\frac{N_0}{N} \triangleleft \frac{N_1}{N} \triangleleft \dots \triangleleft \frac{N_k}{N} = \frac{G}{N}$$

$$\text{abelovo } \frac{N_{i+1}}{N_i} \cong \frac{M_{i+1}}{M_i} \text{ je abelovo}$$

Versta za G

$$\{1\} \triangleleft N_0 \triangleleft \dots \triangleleft N_k = M_0 \triangleleft M_1 \triangleleft \dots \triangleleft M_\ell = G$$

■

Opomba: Izkaže se da so vse grupe l'he moči rešljive

(Feit-Thompsonov izrek)

DN. G jo končne p-grupe potem je rešljiva

Nasvet $Z(G) \neq \{1\}$. (Hukkejeva po/G)

Kolaborji: polinomov (nad poljih)

\mathbb{F} bo vedno polje

Pravimo da je polinom stopnje n ko

$$p(x) = a_n x^n + \dots + a_0 \quad a_n \neq 0$$

Stopnja n;čelnega polinoma je $-\infty$

Opazimo:

$$\text{st}(p(x) \cdot g(x)) = \text{st}(p(x)) + \text{st}(g(x))$$

(ker produkt dveh neničelnih n_1, n_2 neničeln)

Ker je \mathbb{F} polje

Opomba: $\mathbb{Z}_n[x]$

$$p(x) = 2x^2 + 1$$

$$g(x) = 2x^3 + 1$$

$$\text{st}(p(x) \cdot g(x)) = 3 \neq \text{st}(p(x)) + \text{st}(g(x))$$

Posledica:

Kdaber $F[x]$ je brez deliteljev nica

Obrnjeni elementi $F[x]$ so najmanje nenični konstantni polinom:

Dokaz: sledi iz formule za st($p(x), q(x)$)

Izrek: Osnovni izrek o deljenju polinoma
Za poljubne polinome $f(x)$ in $g(x)$ iz
 $\mathbb{F}[x]$, $g(x) \neq 0$, obstajata enodno
določena polinome $k(x)$ in $r(x)$ da je

$$f(x) = k(x) \cdot g(x) + r(x)$$

$$\text{st}(r(x)) < \text{st}(g(x))$$

Dokaz: $f(x) = a_m x^m + \dots + a_0 ; a_m \neq 0$
(BESZS $f(x) \neq 0$)

$$g(x) = b_n x^n + \dots + b_0 ; b_n \neq 0$$

Indukcija po m

(BESZS $m \geq n$ (če $m < n$, potem $k(x) = 0$
in $r(x) = f(x)$))

Baza indukcije: $m = 0$

$$a_0 = (a_0 b_0)^{-1} \cdot b_0 + 0 \quad (\text{ker } a_0 \vee \mathbb{F})$$

Recimo da velja za vse polinome stopnje $< m$

$$a_m \cdot b_n^{-1} x^{m-n} \cdot g(x) = a_m x^m + \dots$$

$f(x) - a_m b_n^{-1} x^{m-n} \cdot g(x)$ polinom stopnje $< m$

$$f(x) - a_m b_n^{-1} x^{m-n} \cdot g(x) = k_1(x) \cdot g(x) + r(x)$$

$$f(x) = \underbrace{(k_1(x) + a_m b_n^{-1} x^{m-n})}_{k(x)} g(x) + r(x)$$

Analognost:

$$f(x) = k_1(x) g(x) + r_1(x) = k_2(x) g(x) + r_2(x)$$

$$\begin{aligned} \text{st}(r_1(x)) &< \text{st}(g(x)) \\ \text{st}(r_2(x)) &< \text{st}(g(x)) \end{aligned}$$

$$(k_1(x) - k_2(x)) \cdot g(x) = r_2(x) - r_1(x)$$

Primerjamo stopnji:

$$\text{st}(r_2(x) - r_1(x)) < \text{st}(g(x))$$

$$\text{st}((k_1(x) - k_2(x)) \cdot g(x)) \geq \text{st}(g(x)) \text{ Če}$$

$$k_1 - k_2 \neq 0$$

$$\text{torej} \Rightarrow k_1 = k_2 \Rightarrow r_2 = r_1$$

Posledica: V ideal v kolobarju $\mathbb{F}[x]$ je
glavní (generiran zemim elementom)

($I = \{0\}$ $I = \{ka; k \in \mathbb{K}\}$ ker je \mathbb{K} komutativen)

Dohaz:

$I \triangleleft \mathbb{F}[x]$ 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 $\underline{I = (p(x))}$

Vzemimo poljuben $f(x) \in I$

$$\underbrace{f(x)}_{\in I} = \underbrace{k(x) \cdot p(x)}_{\in I} + r(x) \Rightarrow r(x) \in I$$
$$\text{st}(r(x)) < \text{st}(p(x))$$

$$\Rightarrow r(x) = 0 \Rightarrow$$

$$f(x) = k(x) \cdot p(x)$$

$\exists c \quad p(x) \in F[x] \quad a \in F \quad p(x) = \sum_{j=0}^n a_j x^j$

$$p(a) = \sum a_j a^j \in F$$

a je nista polinoma $p(x)$, $\exists c \in F$ je $p(c) = 0$

Opozba: $p(x)$ abstraktna vrednost x^j

Polinom lahko gledamo kot $p: F \rightarrow F$
 $a \mapsto p(a)$

(polinomske funkcije)

Polinomov ne merimo identificirati s polinomskimi funkcijami:

$$\mathbb{Z}_2[x]$$

$$p(x) = 0 \quad g(x) = x^{2025} + x$$

radionicne polinome

$$P: \mathbb{Z}_2 \rightarrow \mathbb{Z}_2$$

$$0 \mapsto 0$$

$$1 \mapsto 0$$

$$g: \mathbb{Z}_2 \rightarrow \mathbb{Z}_2$$

$$0 \mapsto 0$$

$$1 \mapsto 0$$

Teoretički: $p(x) \in \mathbb{F}[x] \quad a \in \mathbb{F}$

a je nula polinoma $p \Leftrightarrow$ polinom
 $(x-a)$ deli $p(x)$

Dokaz: $p(x) = k(x) \cdot (x-a) + r(x)$

a nula $p(x)$

$$p(a) = k(a) \cdot 0 + r = 0 \\ \Leftrightarrow r = 0$$

□

Posledica:

$p(x) \in \mathbb{F}[x]$ neničeln

Potem je v \mathbb{F} krajnjemu st($p(x)$) nikel polinom

Dokaz: indukcija po stopnji;

nerazcepni polinomi

Def: Naj bo $p(x) \in \mathbb{F}[x]$ stopnje ≥ 1

Pravimo da je $p(x)$ nerazcepna nad \mathbb{F} , če
iz enakosti $p(x) = g(x)h(x)$, $g(x), h(x) \in \mathbb{F}[x]$

Stoti da je eden od $g(x)$ in $h(x)$ konstanten

Primer:

$\mathbb{C}[x]$ nerazcepni polinomi so natančno

linearni polinomi;

$\mathbb{R}[x]$ linearni polinomi in kvadratni polinomi
brez nicoel

Trditv:

Naj bo $p(x) \in F[x]$ stopnje ≥ 1

a) Če $\text{st}(p(x)) = 1 \Rightarrow p(x)$ je nerazcepna

↳ Če je $\text{st}(p(x)) \geq 2$ in je $p(x)$ nerazcepna,
potem $p(x)$ nima nicle v F

c) Če je $\text{st}(p(x)) = 2 \vee \text{st}(p(x)) = 3 \Rightarrow$
 $p(x)$ je nerazcepna nad $F \Leftrightarrow$
 $p(x)$ nima nicle v F

Od tada je ogleđeno $\mathbb{Q}[x]$

$p(x) \in \mathbb{Q}[x]$

Če $p(x)$ pomočimo s skupnim menovalcem koeficijenata dobimo polinom $v \in \mathbb{Z}[x]$

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 teža cela števila

Trditev: (Gaussova lema)

Proizvod dveh primitivnih polinomov je
svet primitiven polinom

Dokaz:

Naj bosta $p(x), g(x) \in \mathbb{Z}[x]$ primitivne

Rečimo da $p(x) \cdot g(x)$ n. primitiven
zato obstaja nelo pravščilo p, k deli
vse koeficiente polinoma $p(x) \cdot g(x)$

$$p(x) \cdot g(x) \in p \cdot \mathbb{Z}[x] \triangleleft \mathbb{Z}[x]$$

$$\text{kaj je } \mathbb{Z}[x]/p\mathbb{Z}[x] \cong \mathbb{Z}_p[x]$$

$$\gamma: \mathbb{Z}[x] \longrightarrow \mathbb{Z}_p[x]$$

$\sum a_j x^j \longmapsto \sum (a_j + p\mathbb{Z}) x^j$ je homomorfizem
je surjektiven

$$\ker \gamma = p\mathbb{Z}[x]$$

$$\text{Torej } \mathbb{Z}[x]/p\mathbb{Z}[x] \cong \mathbb{Z}_p[x]$$

$p(x)$ je primitiven $\Rightarrow p(x) \notin \ker \gamma$
 $g(x)$ je primitiven $\Rightarrow g(x) \notin \ker \gamma$

$p(x) + p\mathbb{Z}[x]$ je nevrven 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 nica terj

ime $\mathbb{Z}_p[x]$ delitelje nica

Ker je $\mathbb{Z}_p[x]$ r-eje nima deliteljev nica *

Izrek: Nej bo $f(x) \in \mathbb{Z}[x]$. Recimo da $f(x)$ ne moremo zapisati kot produkt dveh nekonstantnih polinomov v $\mathbb{Z}[x]$. Potem jo $f(x)$ nerazcepim v $\mathbb{Q}[x]$.

Dokaz:

Recimo da $f(x) = g(x) \cdot h(x)$ $g(x), h(x) \in \mathbb{Q}[x]$

Dokazujemo: enačba teh je konstanten

Zmobilimo se ulomku:

$k = \text{skupn: menavalec koeficientov } g(x)$

$l = \text{skupn: -ti - od } h(x)$

$$k \cdot l \mid f(x) = \underbrace{(k \cdot g(x))}_{\text{ceri koeficienti}} \cdot \underbrace{(l \cdot h(x))}_{\in \mathbb{Z}[x]}$$

ceri koeficienti $\in \mathbb{Z}[x]$

Dokaz (accesay)
 $f(x) \in \mathbb{Z}[x]$

recimo $f(x) = g(x) \cdot h(x)$

\uparrow

skupn: imenovalec l
skupn: imenovalec k

$$klf(x) = kg(x) \cdot l \cdot h(x)$$

d... največja skupn: delitev koeficijentov $f(x)$

$$d_1 \dots -||- za kg(x)$$

$$d_2 \dots -||- za lh(x)$$

$$kl df_0(x) = d_1 d_2 g_0(x) \cdot h_0(x)$$

primitivni:

Po geometriji tem sa $g_0(x) \cdot h_0(x)$ primitivni.

Največji skupn: koef $kl df_0(x) = kl d$

$$-||- \qquad \qquad d_1 d_2 g_0(x) h_0(x) = d_1 d_2$$

Torej $d_1 d_2 = kl d$

$$f_0(x) = g_0(x) h_0(x)$$

$$f(x) = df_0(x) = dg_0(x)h_0(x)$$

Po predpostavki mora Liki 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 prstevilo, za katere velja:

i) $p \nmid a_n$

ii) $p \mid a_{n-1}, \dots, a_0$

iii) $p^2 \nmid a_0$

Potem je $f(x)$ nerazcegen nad $\mathbb{Q}(x)$

Dokaz:

Rocimo da ton: res.

Pa prejšnji izrek: obstajata nekonstantni polinomi $g(x), h(x) \in \mathbb{Z}[x]$ da je

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

$$g(x) = b_r x^r + \dots + b_0$$

$$h(x) = c_s x^s + \dots + c_0$$

Primerjavo koeficiente

$$b_0 \cdot c_0 = a_0$$

Ker $p \nmid a_0$ in $p^2 \nmid a_0 \Rightarrow p$ deli natančno enega od b_0, c_0 . Besed. $p \mid b_0 \wedge p \nmid c_0$

$$a_n = b_r c_s$$

Ker $p \nmid a_n \wedge p \nmid b_r, c_s$

Naj bo k najmanjši tak, da $p \mid b_0, \dots, b_{k-1}$ in p ne deli b_k $k \leq r$

$$a_k = \underbrace{b_k \cdot c_0 + b_{k-1} c_1 + \dots + b_0 c_k}_{\text{najmanjši deljiv sp}} \quad \underbrace{p \mid a_k \text{ deljiv sp}}$$



Primer:

p naj bo prastevilo

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \dots + x + 1 \in \mathbb{Z}[x]$$

Ta polinom n: razcegen nad \mathbb{Q} .

Eisensteinov kriterij n: uporaben. Aljpac?

Trdi:

$$\Phi_p(x+1) = (x+1)^{p-1} + (x+1)^{p-2} + \dots + 1$$

Davalj je pokazati da je $\Phi_p(x+1)$ nerazcegen

$$(x-1)\Phi_p(x) = x^{p-1} \quad \text{premakemo}$$

$$x\Phi_p(x+1) = (x+1)^{p-1}$$

$$\Phi_p(x+1) = x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \dots + \binom{p}{p-2}x + \binom{p}{p-1}$$

$$\binom{p}{1}, \dots, \binom{p}{p-1} \text{ so deljivi s } p$$

$$1 \text{ n: deljiv s } p$$

po Eisensteinku je $\Phi_p(x+1)$ nerazcegen nad \mathbb{Q} ,
torej isto velja za $\Phi_p(x)$

Iz zorce $(x-1)\Phi_p(x) = x^{p-1}$ vidimo

$$\Phi_p(x) = \prod_{k=1}^{p-1} (x - \omega_k)$$

$$\omega_k = \cos \frac{2k\pi}{p} + i \sin \frac{2k\pi}{p} = e^{i \frac{2k\pi}{p}}$$

\hookrightarrow primitive koren enote

Zu splaßen n :

$$\Phi_n(x) = \pi(x - \omega_k)$$
$$\omega_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n} = e^{i \frac{2k\pi}{n}}$$

gibt ω_k in n Werte

Ist $\Phi_n(x)$ so tridiagonal ist
polynom in x so tridiagonal ist

$\Phi_n(x)$... cyclotomisch polynom

Razširitev polj

Definicija. Nej bosta K in F polji: $F \subseteq K$.

Potem pravimo da je polje K razširitev polja F , označka K/F

Zapledi:

$$R/Q \quad R \text{ je razširitev polja } Q$$

$$C/P, C/Q$$

$$Q(\sqrt{2}) = \{a+b\sqrt{2}; a, b \in Q\} \quad \text{je polje}$$

$$Q(\sqrt{2})/Q$$

Motivacija \mathbb{R}/\mathbb{Q}

Loga iracionalne števile: $\sqrt{2}$

$\sqrt{2}$ je ničla polinoma $x^2 - 2 \in \mathbb{Q}[x]$

Građa iracionalna števila: π

π n: ničla nekog \checkmark polinoma $\nu \mathbb{Q}[x]$

Def: Njihova k/f razširitev je v. aek.

Pravimo:

a) a je algebraičen polinom $p(x) \in F[x]$
da je $p(a) = 0$

b) a je transcendenten nad F , ce
n: algebraičen nad F

Primer:

$\sqrt{2}$ je algebraičen nad \mathbb{Q} in π je
transcendenten nad \mathbb{Q}

Definicija: Naj α K/F razširitev polj

$a \in K$ naj bo algebraičen nad F

Polinomu $p(x) \in F[x]$, kjer ima vodilni

koeficient 1 velja da je $p(a) = 0$ in je
nejmanjše stopnje med tistimi, revidčnim:
polinom, ki ustreza a pravimo **minimálni**
polinom elementa a nad F

DN: minimálni polinom je enolično določen

Teoretički:

Naj bo k/F razširitev polj, a ek nuj bo algebraičen nad F . Nuj bo $p(a) = 0$. ~~potem je~~

Naslednje teoretične so ekvivalentne:

i) $p(x)$ je minimalni polinom za a

ii) $p(x)$ je nerazcepna 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 $p(x)$ razcepna:

$$p(x) = g(x) \cdot h(x) \quad g(x), h(x) \in F[x] \\ \text{nekonstantne}$$

$$p(a) = g(a) \cdot h(a) = 0 \Rightarrow$$

$$h(a) = 0 \vee g(a) = 0$$

če ne prim. $g(a) = 0$ je $g(x)$ polinom,

ki ima nujjo stopnjo kot $p(x)$ in unike a

*

ii) \Rightarrow iii)

$$I = \{f(x) \in F[x] : f(a) = 0\}$$

I ideal v $F[x]$. I je zato glavn:

ideal (ker je generiran z enim elementom)

$$\exists p_1(x) : I = (p_1(x)) = \{k(x) \cdot p_1(x) : k(x) \in F[x]\}$$

$$p(x) \in I \Rightarrow p(x) = k(x) \cdot p_1(x) \quad p_1(a) = 0$$

Zaradi nerazcepnosti je $k(x)$ konstanten
zato $I = (p(x))$

Sledi da je $\forall f(x) \in I$ vodenotnik $p(x)$

iii) \Rightarrow i)

če $p(x)$ ni minimalni polinom $\exists q(x) \in F[x]$
neniečen, $st(q(x)) < st(p(x))$ in $q(a) = 0$

Po predpostavki: $p(x) | q(x)$ *
(stopnje)

Def: K/F aek n, t. bo alg nad F

$p(x)$ naj bo minimalen polinom a-jedn. \bar{a} ce st $(p(\bar{a})) = n$ pravino da je
a algebraicen stopnje n

Zgled:

① K/F alg. elementov stopnje 1 - nicle lin. polinoma
 $x-a \quad a \in F$
to so natanko elementi F

② $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$

$\sqrt{2}$ je nicle $x^2 - 2 \in \mathbb{Q}[x]$

to je minimalni polinom

$\sqrt{2}$ je algebraicen stopnje 2 nad \mathbb{Q}

③ \mathbb{C}/\mathbb{R}

i je nicle polinoma $x^2 + 1$

i je algebraicen stopnje 2 nad \mathbb{R}

Sleduje: $\forall z \in \mathbb{C}$ je algebraicen nad \mathbb{R}

stopnje 1 ali 2

$$\begin{aligned} z \text{ je nicle } & x^2 - (z+\bar{z})x + z\bar{z} \in \mathbb{R}[x] \\ &= (x-z)(x-\bar{z}) \end{aligned}$$

④ \mathbb{R}/\mathbb{Q} $\sqrt{2} + \sqrt{3}$ algebraicen nad \mathbb{R} ?

$$a = \sqrt{2} + \sqrt{3}$$

$$a^2 = 5 + 2\sqrt{6} \quad / \cdot 10$$

$$a^4 = 49 + 20\sqrt{6} +$$

$$a^4 - 10a^2 + 1 = 0$$

$\sqrt{2} + \sqrt{3}$ je nicle polinoma $x^4 - 10x^2 + 1 \in \mathbb{Q}[x]$

DN: to je minimalni polinom $\sqrt{2} + \sqrt{3}$ nad \mathbb{Q}

Končne razširitev polj

K/F naj bo razširitev polj

V K imamo sestevanje

Če elemente iz F imenujemo skalarji;
in elemente K -ja vektorji; imamo
dopolnjeno množenje s skalarjem:

$$F \times K \rightarrow K$$

$$(\alpha, k) \mapsto \alpha k$$

K lahko gledamo kot vektorski prostor nad F

Def: razširitev polj K/F je končna, če
je K končnorazsežen vektorski
prostор nad F

Oznaka:

$$\dim_F K = [K : F] \dots \text{stopnja razširitev}$$

Zadáno:

• \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}

$$\forall r \in \mathbb{R} \quad r = \underbrace{g_1 r_1 + \dots + g_n r_n}_{\text{samo stejno nekoncne mnozeste}}$$

samo stejno nekoncne mnozeste

Trditev:

$F \subseteq L \subseteq K$ naj bodo Pdj.

Naj bosta L/F in K/L konan; razširiti; Potem je K/F konan
in velja $[K:F] = [K:L] \cdot [L:F]$

Dokaz: Baza L -ja kot vekt. prost. nad
 $F: \{a_1, \dots, a_m\}$

Baza K -ja kot vekt. prost. nad $L: \{b_1, \dots, b_n\}$

$B = \{a_i b_j; i \in \{1, \dots, m\}, j \in \{1, \dots, n\}\} \cup$
baza K nad F

K lahko razvijemo po b_1, \dots, b_n nad L

$$k = \lambda_1 b_1 + \lambda_2 b_2 + \dots + \lambda_n b_n \quad \lambda_i \in L$$

$\lambda_i \in L \Rightarrow$ lahko razvijemo po a nad F

$$\lambda_i = p_{i1} a_1 + \dots + p_{im} a_m \quad p_{ij} \in F$$

$$k = p_{11} a_1 b_1 + p_{12} a_2 b_1 + \dots + \dots + p_{nm} a_m b_n$$

linearne neodvisnosti:

$$\sum \sum p_{ij} a_j b_i = 0 \quad p_{ij} \in F$$

$$\underbrace{\left(\sum p_{ij} a_j \right)}_{\in L} b_i = 0$$

$$\Rightarrow \sum p_{ij} a_j = 0 \Rightarrow p_{ij} = 0 \quad \forall i, j$$

Def: Razširitev K nad F je algebraična, če je Vsekakor algebraičen nad K
(je razširitev neke polinomske enačbe)
in transcendenčna če ni algebraična

Trditve: Vsaka končna razširitev K/F je algebraična

Dokaz: Recimo da je $a \in K$ n. algebraičen nad F
 $1, a, a^2, \dots$ so linearno neodvisni nad F
* ker je $\dim K/F$ končna

■

Oznaka: K/F $a \in K$

$F[a] = \text{njemanjsi podkolobar } v K, \text{ ko vsebuje}$

$F \text{ in } a = \text{podkolobar } v K \text{ generiran}$

$\hookrightarrow F \text{ in } a$

$$F[a] = \{ p(a) ; p(x) \in F[x] \}$$

$F(a) = \text{podpolje } v K \text{ generirano z } F \text{ in } a$

$$F(a) = \{ x y^{-1} ; x \in F[a], y \in F[a] - \{0\} \}$$

Poddno lahko definiramo

$$F[a_1, \dots, a_n], F(a_1, \dots, a_n)$$

$$F[a_1, \dots, a_n] = F[a_1, \dots, \underline{a_{n-1}}][a_n]$$

Def: Rassiriter k/F je primitive,
če $\exists \alpha \in k$. da je $k = F(\alpha)$

Zgled: $\mathbb{Q}[\sqrt{2}] = \{\alpha + \beta\sqrt{2}; \alpha, \beta \in \mathbb{R}\}$
 $\mathbb{Q}(\sqrt{2})[\alpha + \beta\sqrt{2}; \alpha, \beta \in \mathbb{Q}] = \mathbb{Q}[\sqrt{2}]$
leto je, ker je $\sqrt{2}$ algebričen

Izrek: Nej bo K/F razširitev polj
in nej bo $a \in K$ algebričen nad F
stopnje n . Potem je $F(a) = F[\underline{a}]$
in velja $[F(a) : F] = n$

Dokaz:

Nej bo $p(x) \in F[x]$ minimalni polinom
 a -ja $\deg(p(x)) = n$

Dovolj je pokazati da je vsak nenihčen
element $v \in F[\underline{a}]$ obrnjiv

$$f(a) \neq 0 \quad f(x) \in F[x]$$

Zaradi minimalnosti $p(x)$ sledi da
sta $f(x)$ in $p(x)$ tudi polinoma

Zato obstajata polinoma $r(x)$ in $s(x)$
 $\in F[x]$ da

$$f(x)r(x) + p(x)s(x) = 1$$

(iz razširjenega euklidovega algoritma)

Izračunamo $v a$:

$$f(a) \cdot r(a) = 1$$

$r(a)$ je inverz $f(a)$ -ja

Sed drug del:

$$F(a) = \{ f(a) : f \in F[x] \}$$

$$p(a) = a$$

$$p(x) = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$$

a^n je linearne kombinacije $1, a, a^2, \dots, a^{n-1}$
 $m \geq n \Rightarrow a^m$ 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 algebrnični 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) $\mathbb{Q}(\sqrt[n]{p}) \quad p \in \mathbb{P}$

Polinom je racionalni; koeficienti ki umnoži $\sqrt[n]{p}$: $x^n - p$

Po Eisensteinovem kriteriju je ta polinom irreverzibilen nad \mathbb{Q} , zato je minimálni polinom $\sqrt[n]{p}$ nad \mathbb{Q} .
Zato je sto p nje te razširitev = n

2) K/F aek

eval: $F[x] \rightarrow F[a]$

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

je surjektivna \Rightarrow je epimorfizem kolobarjev

kerival = ?

- Če je a transcendenten nad $F \Rightarrow \text{keraval} = \{0\}$
a n: n-de način na n-ih nega polinoma

če je a transcendenten: $F[x] \cong F[a]$

- Če je a algebrničen nad $F \Rightarrow$
Naj bo $p(x) \in F[x]$ naj bo njegov minimálni polinom: $p(a) = 0$

če je $f(x) \in \text{keraval} \Leftrightarrow f(a) = 0 \Leftrightarrow$

$$p(x) | f(x)$$

keraval = vektoristički $p(x) = (p(x))$

$$\text{To je alg } \Rightarrow \frac{F[\lambda]}{(p(x))} \cong F[a] = F(\lambda)$$

Izrek: Maj 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 pa posledica končne razširitev F

Po izrekru (enem voz) je $F(a, b)/F$ algebraična
razširitev, torej $\frac{F(a, b)}{F} \subseteq L$

Med drugim $a \cdot b \in L$, $a^{-1} \in L$

$$\hat{c} \in a \neq 0$$



Obrat ne velja (obstaje algebraične
rešitev ki niso končne)

Primer: algebraična rešitev α je, ki niso
končne.

\mathbb{C}/\mathbb{Q}

$$L = \left\{ \alpha \in A ; \exists p \in \mathbb{Q}[X], p(\alpha) = 0 \right\}$$

L je podpolje v \mathbb{C}

L/\mathbb{Q} je algebraična razširitev

$$\underline{[L : \mathbb{Q}]} = \infty$$

Raziamo da bi bila končna $[L : \mathbb{Q}] = m$

$$\sqrt[n]{2} \in L$$

$$\mathbb{Q}(\sqrt[n]{2}) \subseteq L \quad \forall n$$

$$\left[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q} \right] \Big| \left[L : \mathbb{Q} \right] = m$$

$\frac{n}{m}$

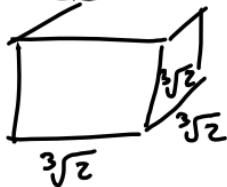
m mora biti deljiv z vsakim naravnim
stevilom

Konstrukcije z ravnilom in šestilom



z ravnilom in šestilom naredi

kocke z 2x večjim volumenom



Podvojite kocke

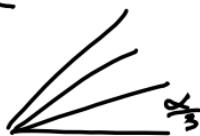
kvadratura kroga:

$$\textcircled{1} \rightarrow \frac{P}{\sqrt{\pi}}$$

A1: lahko naredim kvadrat

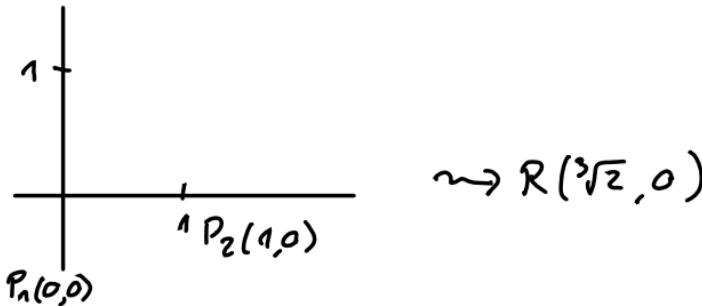
2: isto plazimo

trisekcija kot

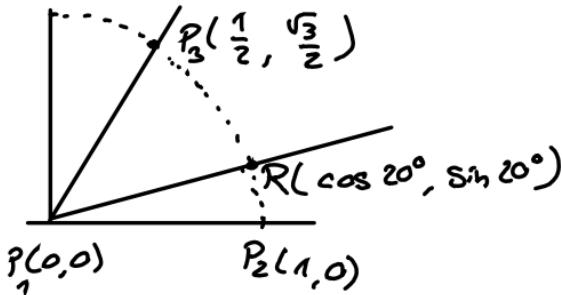


Formulacija problema

Motivacija



Trisekcija 60°

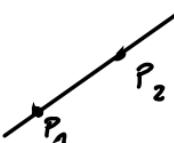


$P_1, P_2, \dots, P_n \in \mathbb{R}^2$

Konstrukcije:

- 2 reuniom:

'cez sve tocke potcogneno premico'



- 3 sečilom:



nove tocke: presecica

Postopek

$$q = \{P_1, \dots, P_n\}$$

konstruiramo novo točku A ne smješ od
teh trih mjestih

$$P \leftarrow P \cup \{A\}$$

Ponovno postopek

izrek: P naj bo množica točk v $\mathbb{R} \times \mathbb{R}$

Recimo da je F podpolje v \mathbb{R}

da $P \subseteq F \times F$

Recimo da je A(a,b) konstruktibilna s pomočjo točk iz P

Potem sta ta dva elementa a, b algebraična nad F, s to pomejno razširitev, ki sta potenci števila 2

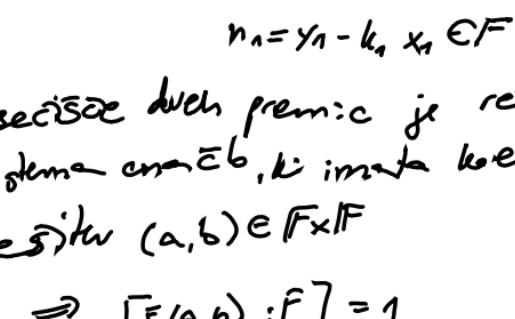
Dokaz: Nej bo najprej A(a,b) prva točka v tej konstrukciji:

Trdimo: $[F(a,b) : F] \in \{1, 2\}$

(če je dvojikas polinom se stopnja mn = 2ⁿ)
npr. $[F(c,d) : F(a,b)] \in \{1, 2\} \Rightarrow c \in \{1, 2, 4\}$

A(a,b) smo dobili na enega dveh načinov

1) presecisce dveh premic



1. premica: $x = a_1$ ali $y = k_1 x + n_1$

2. premica: $x = a_2$ ali $y = k_2 x + n_2$

$$a_1, a_2 \in F \quad k_1 = \frac{y_2 - y_1}{x_2 - x_1} \in F$$

$$n_1 = y_1 - k_1 x_1 \in F$$

Presecisce dveh premic je resitev linearnega sistema enačb, ki imata koef. v F

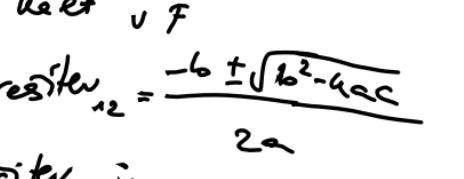
Resitev $(a, b) \in F \times F$

$$\Rightarrow [F(a,b) : F] = 1$$

2) presecisce premice in kvadratne

premica: $x = a_1$ ali $y = k_1 x + n_1$ in $k_1, n_1 \in F$

kroznica:



$$(x - x_1)^2 + (y - y_1)^2 = (x_3 - x_1)^2 + (y_3 - y_1)^2$$

$$x^2 + y^2 + \alpha x + \beta y + \gamma = 0 \quad \alpha, \beta, \gamma \in F$$

če je premica $x = a_1$ dobimo

enecas rey

s koef. iz F

če je premica $y = k_1 x + n_1$

dobimo kvadrant enecas za x

s koef. v F

$$\text{resitev } x_2 = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Resitev je v F, ki mu dedimo

ta korenček ($\sqrt{b^2 - 4ac}$)

$$\Rightarrow zato [F(a,b) : F] = 2 \text{ ali } 1$$

3) 2 kroznici

-isto kot 2) ker

= presecisce kroznice in kvadratne

Ponavljamo postopek

$$P \subseteq F \times F$$

A(a,b) konstruiramo $[F(a,b) : F] \in \{1, 2\}$

$$P \leftarrow P \cup \{A\}, F \leftarrow F(a,b)$$

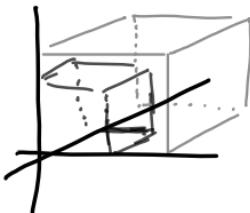
$$B(c,d) [F(a,b)(c,d) : F(a,b)] \in \{1, 2\}$$

$$[F(a,b)(c,d) : F] =$$

$$[F(a,b)(c,d) : F(a,b)] \cdot [F(a,b) : F] \in \{1, 2, 4\}$$

Posledica:

Kocke ne moremo podvajati z ravnilom in sečilom



$$P(0,0), P(1,0) \rightsquigarrow P_3(\sqrt[3]{2}, 0)$$

$$P_1, P_2 \in \mathbb{Q} \times \mathbb{Q}$$

$$[\mathbb{Q}(\sqrt[3]{2}); \mathbb{Q}] = 3 \neq 2^n$$

Posledica: kvadratura kroga n: mogoča je ravnilom in sečilom



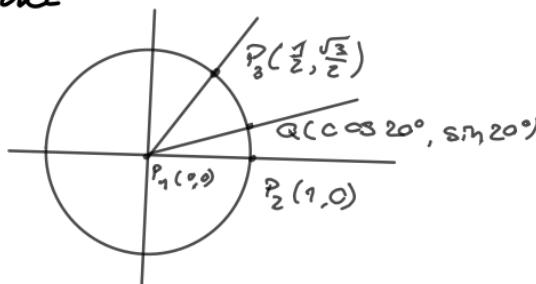
$$P(0,0), P(1,0) \rightsquigarrow P_3(\sqrt{\pi}, 0)$$

$$[\mathbb{Q}(\sqrt{\pi}); \mathbb{Q}] = \infty$$

π je transcendentna.

Pozledice: kote 60° se ne more razdeliti na tri enake dele = ravn. insct.

Dokz



$$\{P_1, P_2, P_3\} \subseteq \mathbb{Q}(\sqrt{3}) \times \mathbb{Q}(\sqrt{3})$$

če se Q da konstruirati potem
 $[\mathbb{Q}(\sqrt{3}), \cos 20^\circ] : \mathbb{Q}(\sqrt{3})] = 2^k$

$$\cos 3\varphi = 4\cos^3\varphi - 3\cos\varphi \quad \varphi = 20^\circ$$

$$\frac{1}{2} = 4a^3 - 3a \quad \cos 20^\circ = a$$

$$8a^3 - 6a - 1 = 0$$

$$a \text{ je nicle polinom } p(x) = 8x^3 - 6x - 1$$

Treimo de je pol. nerazcegen nad $\mathbb{Q}(\sqrt{3})$

Recimo de je razcegen nad $\mathbb{Q}(\sqrt{3})$.

Ker je stopnje 3 mora imeti neko nicle v $\mathbb{Q}(\sqrt{3})$
 $\alpha + \beta\sqrt{3}$ je nicle tege polinoma $\alpha, \beta \in \mathbb{Q}$

$$\text{Tr: h: } (2x)^3 - 3 \cdot 2x - 1 = 0$$

BZS: $\alpha + \beta\sqrt{3}$ je nicle polinome $y^3 - 3y - 1 = 0$

$$(\alpha + \beta\sqrt{3})^3 - 3(\alpha + \beta\sqrt{3}) - 1 = 0$$

$$\alpha^3 + 3\alpha^2\beta\sqrt{3} + 3\alpha\beta^2 + 3\beta^3\sqrt{3} - 3\alpha - 3\beta\sqrt{3} - 1 = 0$$

$$\alpha^3 + 3\alpha\beta^2 - 3\alpha - 1 + \sqrt{3}(3\alpha\beta^2 + 3\beta^3 - 3\beta) = 0$$

$$\text{Dob. mo } \alpha^3 + 3\alpha\beta^2 - 3\alpha - 1 = 0 \quad \text{in}$$

$$\beta(3\alpha^2 + 3\beta^2 - 3) = 0$$

$$1) \beta = 0 \Rightarrow \alpha^3 - 3\alpha - 1 = 0 \text{ nime racional!}$$

$$2) \alpha^2 + \beta^2 = 1 \Rightarrow \text{vstavimo v prvo enacbo} \quad \text{nichel}$$

in dobimo enacebo 3 stopnje brez racional. res.

Sluč: pol. je res razcegen nad $\mathbb{Q}(\sqrt{3})$

$$\text{Torej je } [\mathbb{Q}(\sqrt{3}, \cos 20^\circ) : \mathbb{Q}(\sqrt{3})] = 3$$

Razpadne polje polinomov

Motivacija: $x^2 - 2 \in \mathbb{Q}[x]$ nima nihel v \mathbb{Q}
če gledamo $x^2 - 2 \in \mathbb{R}[x]$ ga lahko
razpolimo na linearne faktorje

Složno: $f(x) \in F[x]$, naj obstaja neka razširitev
 K/F , da ima $f(x)$ neko nihel $a \in K$
lahko gledamo kot polinom v $K[x]$:
$$f(x) = (x - a) \cdot f_1(x) \quad ; \quad f_1(x) \in K[x]$$

Ocitno: K/F , $f(x) \in F[x]$, st $f(x) = n \Rightarrow$
K vsebuje korejance n nihel $f(x)$

Treba: Napiši bo $f(x) \in F[x]$ nekonst. polinom.

Potem obstaja k/F , ki vsebuje vsaj eno nico polinoma $f(x)$.

Dokaz:

Napiši bo $p(x)$ nerazcegan $\in F[x]$ 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 $p(x)$ nerazcegan, je največji skupni delitelj $g(x)$ in $p(x)$ enak 1

$$a(x), b(x) \in F[x]$$

$$g(x) \cdot a(x) + p(x) \cdot b(x) = 1$$

$$(g(x) + (p(x))) (a(x) + (p(x))) = g(x) \cdot a(x) + (p(x)) \\ = 1 + (p(x))$$

$g(x) + (p(x))$ je obrnljiv

k vsebuje F, ker

$$F \rightarrow F[x]/(p(x))$$

$$\alpha \mapsto \alpha + (p(x)) \quad \text{je monomorfizem}$$

$f(x) \in F[x]$ lahko zredimo kot polinom v $K[x]$

$$f(x) = \sum a_k x^k \rightsquigarrow \sum (a_k + (p(x))) \cdot x^k$$

Kater: element k je nica tega polinoma

$$x + (p(x)) \in K$$

$$f(x + (p(x))) = \sum (a_k + (p(x))) (x^k + (p(x))) =$$

$$= \sum a_k x^k + (p(x)) = f(x) + (p(x)) = (p(x))$$

Postledica: $f(x) \in F[x] \Rightarrow \exists$ polje $K \geq F$, da

$$f(x) = c(x-a_1)(x-a_2) \dots (x-a_n)$$

$$a_i \in K \subset F$$

Def: $f(x) \in F[x]$ razpade nad poljem K , če
ga lahko v $K[x]$ lahko razstavimo
ne-linearne faktorje

Def: za $f(x) \in F[x]$ je polje K razpadno
polje, če $f(x)$ razpade nad K in ne
razpade nad nobenim manjšim poljem
v K

Opomba: Razpadno polje polinoma vedno
obstaja

Po postledici $\exists K$ ki vsakega več nih a_1, \dots, a_n
polinoma $f(x) \in F[x]$

Razpadno polje je polje $F(a_1, \dots, a_n)$

Koliko je razpadnih polj

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

$\mathbb{Q}(\sqrt{2})$ je razpadno polje

$$\frac{\mathbb{Q}[x]}{(x^2 - 2)} \cong \mathbb{Q}(\sqrt{2})$$

Vsa razpadna polja so med sabo izomorfna

Opoomba: Razpadno polje podimoma $\in F[x]$ je končne razširitev polja F

Oznaka: Nej boste F, F' polji;
 $\varphi: F \rightarrow F'$ homomorfizem

$$\text{f(x)} \in F[x]: f(x) = \sum_{k=0}^n a_k x^k \quad a_k \in F$$

$$F_p[x] = \sum_{k=0}^n \varphi(a_k) x^k \in F'[x]$$

Lema: polinom $F[x]$ ne razcepil polinom

$a \in K$ nej bo nicle $p(x)$

$f: F \rightarrow F'$ nej bo izomorfizem polj

Polinom $p_p(x) \in F[x]$ nej ima neko nicle $a' \in K'$

Potem obstaja nekakšen izomorfizem

$\tilde{\Phi}: F(a) \rightarrow F'(a')$ da

$$\tilde{\Phi}_F = f \quad \text{in} \quad \tilde{\Phi}(a) = a'$$

Ostali so linearne kombinacije teh dveh

Dokaz: $p(x)$ je minimalni polinom a -ja

Ker je f izomorfizem je $p_p(x)$ minimalni polinom a'

$$\begin{array}{ccc} F[x]/(p(x)) & \xrightarrow{\tilde{\epsilon}} & F(a) & \epsilon: F[x] \rightarrow F(a) \\ \downarrow \pi & \cong & \downarrow \tilde{\Phi} & \text{evalvacija homomorfizem} \\ F[x]/p(x) & \xrightarrow{\tilde{\epsilon}} & F'(a') & \end{array}$$

Določimo $\Pi: F[x]/(p(x)) \rightarrow F'[x]/(p'(x))$

$$p(x) + (p(x)) \mapsto p'(x) + (p'(x))$$

DN: Π je izomorfizem polj

$$\tilde{\Phi} = \tilde{\epsilon} \circ \Pi \circ \tilde{\epsilon}^{-1}$$

Endovzrost:

$$\tilde{\Phi}(\sum \lambda_n a^n) = \sum \tilde{\Phi}(\lambda_n) \tilde{\Phi}(a^n) = \sum f(\lambda_n) a'^n$$

Recimo da imamo tudi izomorfizem $\tilde{\Phi}$

$$\tilde{\Phi}(\sum \lambda_n a^n) = \sum \tilde{\Phi}(\lambda_n) \tilde{\Phi}(a^n) = \sum f(\lambda_n) a'^n$$

Izrek: F, F' nej bošta polji:

$\varphi: F \xrightarrow{\cong} F'$ posoj bo nekonstanten polinom
 $v F(x)$ k nej bo razpredno polje $f(x)$
 k' nej bo razpredno polje polinoma
 $f_p(x) \in F'(x)$. Potem obstaja izomorfizem
 $\tilde{\Phi}: k \rightarrow k'$

Pošljedica: Če je $f(x) \in F[x]$ nekonstanten polinom sta poljubni razpredni polji:
polinoma $f(x)$ izognati:

Dokazi: Uporabimo izrek za $F' = F$ $\varphi = \text{id}_F$

Dokaz:

Indukcija po $n = [k:F]$

$$n=1: K=F \xrightarrow{f:x} K'=F'$$

$n>1$: $f(x)$ ne razpredne linijalne je nad F

Naj bo $p(x) \in F[x]$ nerazognen polinom ki deli $f(x)$; $\text{st}(p(x)) > 1$

K vsebuje neko nico a polinoma $r(x)$, ker je razceg polja $r(x)$

Poddana k' vsebuje nico a' polinoma

$$p_{r'}(x) \in F'(x)$$

Po temi obstaja razstanka en izomorfizem

$$\tilde{\Phi}: F(a) \rightarrow F'(a')$$

$$\tilde{\Phi}/_F = \varphi$$

$$\tilde{\Phi}(a) = a'$$

K je razpredno polje $f(x)$ tudi nad $F(a)$
poddana je x' razceg polje nad $f_p(x)$ nad $F'(a')$

$$[K:F(a)] = [k:F] : [F(a):F] = \frac{n}{\text{st}(p(x))} < n$$

\nwarrow
 a minimum
polinoma $p(x)$

Po ind. pred. obstaja izomorfizem

$$\tilde{\Phi}^*: k \rightarrow k'$$

$$\tilde{\Phi}^*/_{F(a)} = \tilde{\Phi}$$

$$\tilde{\Phi}^*/_F = \Phi/F = \varphi$$

Normalne razširjive polj

Def: Naj bo K/F razširitev polj;

Pravimo da je ta razširitev normalna, če
za vsek nerezogen podpolinum $p(x) \in F[x]$
velja ena od možnosti:

- 1) $p(x)$ ima vse nicle v K
- 2) $p(x)$ nima nobene nicle v K

Izrek: Naj bo K/F končna razširitev.

K/F je normalna razširitev \Leftrightarrow

$\Leftrightarrow K$ je razpredno polje nekega podistema iz $F[x]$

Dokaz:

$\Rightarrow K/F$ naj bo normalna, $K = F(a_1, \dots, a_n)$

Naj bo $p_i(x)$ minimalni podistem za:

Po definiciji normalnosti K vsebuje vse nicle polinoma $p_i(x)$

$$f(x) := p_1(x)p_2(x) \dots p_n(x)$$

Naj bo L razpredno polje $f(x)$

$$K = L$$

$$a_1, \dots, a_n \text{ so nicle } f(x) \Rightarrow$$

$$a_1, \dots, a_n \in L \Rightarrow F(a_1, \dots, a_n) \subseteq L \Rightarrow K \subseteq L$$

$$L \subseteq K$$

ker K vsebuje vse nicle $f(x)$, L pa je najmanjši tak, ki vsebuje vse nicle $f(x)$

$$\text{po definiciji: } L \subseteq K$$

$\Leftarrow K$ naj bo razpredno polje $f(x) \in F[x]$

Izberemo poljuben nerazcepren polinom $p(x) \in F[x]$.

Naj bo a nica polinoma $p(x)$, ki $\nmid p(x)$

v K . Naj bo b poljubna druga nica polinoma $p(x)$

$$b \in K$$

$p(x)$ je minimalni podistem za a in b

Identično prešlikava $F \rightarrow F$ lahko

razširimo do izomorfizma $\bar{\Phi}: F(a) \xrightarrow{\cong} F(b)$

$$\bar{\Phi}|_F = \text{id} \quad \bar{\Phi}$$

$$\bar{\Phi}(a) = b$$

K razp. polje $f(x)$

$p(x)$ nerazcepren $\Leftrightarrow a \in K$ nica

b poljubna nica $p(x)$

Razpredno polje polinoma $f(x)$ nad

$$F(a) : F(a; a_1, \dots, a_n) = K$$

$$\overbrace{K}^n$$

$$\text{n nad } F(b) : F(b, a_1, \dots, a_n) = K'$$

Po izreku obstaja

$$\bar{\Phi}^*: K \rightarrow K'$$

$$\bar{\Phi}^*|_{F(a)} = \bar{\Phi}$$

$$\bar{\Phi}^*(a) = b$$

$$a \in K = F(a_1, \dots, a_n)$$

$$a = \text{"polinam" v } a_1, \dots, a_n$$

$$b = \bar{\Phi}^*(a) \Rightarrow b \text{ je polinam v } \underbrace{a_1, \dots, a_n}_{\text{ker } \bar{\Phi}}$$

$$\text{torej } b \in F(a_1, \dots, a_n) = K$$

Zgled:

① $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ je normalna, ker jo

\mathbb{Q} razpadno polje $x^2 - 2 \in \mathbb{Q}[x]$

② $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ n: normalna, ker

$\sqrt[3]{2}$ je rdeča $x^3 - 2 \in \mathbb{Q}[x]$ nerazcepna

Toda $\mathbb{Q}(\sqrt[3]{2})$ ne vsebuje vseh rdečih
 $x^3 - 2$

③ p prasterivilo, $\epsilon = e^{\frac{2\pi i}{p}}$ (primitivni p-ti
keren enote)

$\mathbb{Q}(\epsilon)/\mathbb{Q}$ je normalna, ker

$\mathbb{Q}(\epsilon)$ razpadno polje $x^p - 1$

↳ rdeča tega polinoma

s o $\epsilon, \epsilon^2, \dots, \epsilon^{p-1}, 1$

vse rdeči zivip v $\mathbb{Q}(\epsilon)$

Algebraično zaprtje polja

Def: A polje. pravimo da je A algebraično zaprtje če ima & nekonst. polinom $p \in A[x]$ vsej eno nico

$$\text{Ekvivalentno: } f(x) = c(x-a_1)\dots(x-a_n); c, a_i \in A$$

Lema: $F \subseteq L \subseteq K$ naj bodo polja, L/F algebraične. Nej bo $a \in K$ algebraičen nad L. Potem je a algebraičen nad F

Dokaz:

Po definiciji: $\exists p(x) \in L[x], p(a)=0$
 $p(x) = \sum a_n x^n \quad a_n \in L$

$\tilde{F} = F(a_1 \dots a_n), p(x) \in \tilde{F}[x] \Rightarrow$
a algebraičen nad \tilde{F}

$[\tilde{F}(a) : F]$ dava, je dekorati le je to $< \infty$
 $[\tilde{F}(a) : F] = \underbrace{[F^a(a) : F]}_{< \infty} \cdot [\tilde{F} : F]$
ker je a alg. nad \tilde{F}

L/F algebraične, $a_n \in L \Rightarrow a_n$ algebr nad F
 $\Rightarrow [F(a_1 \dots a_n) : F] < \infty \Rightarrow [\tilde{F} : F] < \infty \Rightarrow$
 $[\tilde{F}(a) : F] < \infty$ ■

Def: Nej bo F polje. Algebraično zaprtje
polje 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 vsake
polje vsebovano v nekem algebraičnem
zaprtem polju.

Da se pokazati da algebraično zaprtje polja
vedno obstaja in je do izomorfizma endično
določeno

Primer

\mathbb{R} :

\mathbb{C} je alg zaprto

$\mathbb{R} \subseteq \mathbb{C}$ \mathbb{C}/\mathbb{R} je razširitev stopnje 2
 $\Rightarrow \overline{\mathbb{R}} = \mathbb{C}$

\mathbb{Q} ; \mathbb{C}/\mathbb{Q} n: algebraična $\overline{\mathbb{Q}} \neq \mathbb{C}$

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: Dokazati smo že, da je K polje, ki vsebuje F . K/F je algebraična razširitev pod poljem K . $\underbrace{F \subseteq K \subseteq A}_{\text{alg.}}$

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) nico $a \in A$ a je algebraičen nad K , K/F je alg. razširitev.

Potem je a algebraičen nad F .

Po definiciji $a \in K$



Zafred:

$$\overline{\mathbb{Q}} = \{a \in \mathbb{C} : a \text{ je nica nekega nenihrega polinoma iz } \mathbb{Q}[X]\} = \{\text{algebraične številke}\}$$

Končna polja

Naj bo K končno polje

Potem je karakteristika tega polja

$$\text{char } K = p \quad p \in \mathbb{P}.$$

Zato je \mathbb{Z}_p podpolje v K . K/\mathbb{Z}_p

Trditve: $|K| = p^n$ za nek $n \in \mathbb{N}$

Dokaz: K/\mathbb{Z}_p je končne razširitev.

K ima kot vek. prostor nad \mathbb{Z}_p , končno bazo a_1, \dots, a_n

Vsek element K se de enolično

zapisati kot $\underbrace{\alpha_1 a_1 + \alpha_2 a_2 + \dots + \alpha_n a_n}_{p \quad p \quad \dots \quad p} \quad \alpha_k \in \mathbb{Z}_p$ možnosti.

Izjema torej natanko p^n možnosti za elemente K

Lema: Nej bo K polje modi p^n .

Potem je K razpadno polje polinoma

$$x^{p^n} - x \in \mathbb{Z}_p[x]$$

Dokaz: (K^*, \cdot) je grupa modi p^{n-1}

Po lagrangovem izreku

$$\forall a \in K^* \quad a^{p^{n-1}} = 1 \quad / \cdot a$$

$$\forall a \in K \quad a^{p^n} = a$$

Vsi elementi K je nicle polinoma $x^{p^n} - x$

Ker je $\text{st}(x^{p^n} - x) = p^n$ ima ta polynom $\leq p^n$ nicle v polju kar razširiti:

Ker K vsebuje vse nicle, ter noben podpolje ne vsebuje vseh niclev, je K razpadno polje $x^{p^n} - x$



Lemai:

Naj bo L razpedno podje $X^{p^n} - X$ 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

$K = L \iff K$ je podje

Frobeniusov endomorfizem:

$$\varphi: L \rightarrow L$$

$$x \mapsto x^p$$

$$K = \{a \in L; a^{p^n} = a\} = \{a \in L; \varphi^n(a) = a\}$$

$$x, y \in K : \varphi^n(x-y) = \varphi^n(x) - \varphi^n(y) = x-y \Rightarrow x-y \in K$$

Podobno $x \cdot y, x^{-1}$ če $x \neq 0$

Torej je K podje $\Rightarrow K = L$

Za dokaz da je $|L| = p^n$ je dovolj da imam eno enostavno ničlo polinom $f(x)$

Ena ničla: $a=0$

$$f(x) = \underbrace{(x^{p^{n-1}} - 1)}_{\text{O ničla tege polinoma}} \cdot x$$

O ničla tege polinoma

$\Rightarrow 0$ je enostavna ničla

Recimo da $a \neq 0$ ničla:

Iz prejšnjega dokaza $a^{p^{n-1}} = 1$

$$f(x) = (x^{p^{n-1}} - a^{p^{n-1}})x =$$

$$(x-a)x \underbrace{(x^{p^{n-2}} + ax^{p^{n-3}} + \dots + a^{p^{n-3}}x + a^{p^{n-2}})}_{g(x)}$$

$$g(a) = a^{p^{n-2}} \cdot (p^n - 1) \neq 0$$

Torej je a enostavna ničla

Pošledice: Za vsako prostovilo p in
vsoko $n \in \mathbb{N}$ obstaja natančno ena
(do izomorfizma natančno) polje modri p^n

Oznake: \mathbb{F}_{p^n} , $GF(p^n)$

Opomba: Wedderburnova izrek:
Vsak končen obseg je polje

Trditev: Multiplikativna grupa končnega
polja je vedno ciklična

Dokaz: Nej bo $G = (\mathbb{F}_{p^n}^*, \cdot)$

G je končna abelova grupa modri p^{n-1}
v nej bo najmanjši skupni večkratnik
redov elementov grupe G .

Iz klasifikacije končnih abelovih grup
sledi (DN), da grupa G vsebuje
element reda v

Po Lagrangevem izreku $v | (p^n - 1)$ $v \leq p^n - 1$

Davalj je videti deje $p^n - 1 \leq v$

$x^v - 1$ ima kvečjema v nikel
ker je v skupni večkratnik redov elem.
grupe G , za $\forall g \in G, g^v = 1$

$$\Rightarrow p^n - 1 \leq v \Rightarrow v = p^n - 1$$

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 nicle v poljubnem razširitvu polja F enostavne.

Def: Naj bo K/F algebraična razširitev. Pravimo da je ta razširitev separabilna če je za $\text{char } K$ minimalni polinom a-ja nad F separabilen.

teoretički: Naj bo F polje s karakteristiko 0.

Naj bo $p(x)$ poljuben nerezcepren polinom. Potem je poljubna nica $p(x)$ v poljubni razširiti K/F enostavna.

Posledica: Če je $\text{char } F = 0$ je vsaka algebraična razširitev F separabilna.

Primer razsiritev, ki ni separabilna

$K = \mathbb{F}_p(X) = \{\text{racionalne funkcije } \frac{f(x)}{g(x)} : f(x), g(x) \in \mathbb{F}_p[X]\}$

$F = \mathbb{F}_p(X^p)$

če si ogledamo $a = X \in K$ je njegov minimalni polinom $P(y) = y^p - X^p = (y - X)^p$

To polinom nima enostavne nikelje

Definicija K/F algebraične razsiritev. To je enostavna razsiritev, če $\exists a \in K. K = F(a)$

izrek: (o primitivnem elementu)

Vseke končne separabilne rezidrite je enostavna.

Dokaz: K/F končna separabilna.

1. F je neskončno polje

Dovolj je dokazati $a, b \in K, \exists \lambda \in F, f(a, b) =$

$p(x) \in F[x]$ nej bo minimalni polinom a -ja

$g(x) \in F[x]$ nej bo minimalni polinom b -ja

nidepot: $a_1 = a, a_2, \dots, a_m \}$ enostavne

nice: $b_1 = b, b_2, \dots, b_n \}$ nice

L nej bo razpadno polje $p(x)g(x)$

L ter je vsebajo vse nice $a_1, \dots, a_m, b_1, \dots, b_n$

Trik: Vzamemo $\lambda \in F - \left\{ \frac{a_i - a_j}{b_i - b_j} : i \in [m], j \in [n] \right\}$
Artinov trik

(To deluje, ker je polje F neskončno)

Definiramo $f(x) = p(a + \lambda b - \lambda x) \in F(a, \lambda b)[x]$

$$f(b) = p(a) = 0$$

$f(x)$ ima vsaj eno skupno nico s $g(x)$.

Ali ima še kakšno skupno nico?

b_2 ; ali je nica $f(x)$

$$f(b_2) = p(a + \lambda b - \lambda b_2) \text{ ali je lahko}$$

$$a + \lambda b - \lambda b_2 = a; \text{ a nek:}$$

$$\lambda = \frac{a - a}{b - b_2} \quad \text{tak \lambda ne obstaja}$$

iTD.

b je tudi eden skupna nica $f(x)$ in $g(x)$

\Rightarrow nevečji skupni delitelj; $f(x)$ in $g(x)$ je $(x - b)$

$\Rightarrow \exists c(x), d(x) \in F(a + \lambda b)[x]. (x - b) = \underbrace{c(x)f(x)}_{\in F(a + \lambda b)[x]} + \underbrace{d(x)g(x)}_{\in F(a + \lambda b)[x]}$

$\Rightarrow x - b \in F(a + \lambda b)[x] \Rightarrow$ koeficiente tega polinoma

stv v $F(a + \lambda b)[x] \Leftrightarrow 1, b \in F(a, \lambda b)$

$$a = \underbrace{a + \lambda b - \lambda b}_{\in F(a + \lambda b)}$$

samo zadnji dokaz: dejstvo nati:

$F(a, b) \subseteq F(a - \lambda b)$ dokazano

obratna izključitev očiščen

2. F končno polje $F = \mathbb{F}_{p^n}$

K je tudi končno polje $K = \mathbb{F}_{p^m}$

$$K = F(c_1, \dots, c_r)$$

$$BZ: c_i \neq 0 \quad \overset{C}{\alpha_i} \in K^*$$

K^* je za množanje określona grupa

generator $\in \alpha \in C$

$$c_i = C^n$$

$$K = F(c_1, \dots, c_r) = F(C)$$

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 razložiti kot racionalno funkcijo $\sqrt{2} + \sqrt{3}$

$$\sqrt{2} + \sqrt{3} + \frac{1}{\sqrt{2} + \sqrt{3}} = \sqrt{2} + \sqrt{3} + \frac{\sqrt{3} - \sqrt{2}}{1} = 2\sqrt{3}$$

$$\sqrt{3} = \frac{1}{2} (\sqrt{2} + \sqrt{3} + (\sqrt{2} + \sqrt{3})^{-1})$$

$$\sqrt{2} = \sqrt{2} + \sqrt{3} - \sqrt{3}$$

Def: Polje F je perfektno, če je vsake končne razširitev F separabilna

Primer: polja s $\text{char } F = 0$ so perfektna

Toditev: Končna polje so primitivne

Dokaz:

F naj bo končno polje, K/F naj bo končna razširitev

Recimo da $\exists f(x) \in F[x]$ ki nima enostavnih nihel, ne razcepien

a naj bo večkratna nihel

$$f'(a) = 0$$

Zaradi minimalnosti $f(x)$ je $f'(x) \equiv 0$

$f(x)$ je torej oblike $f(x) = \sum a_k x^{pk}$

$a_k \in F = F_p =$ razpredelovno 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 $-x$



Def: Normalnim separabilnim razširivam
pravimo Galoisjeva razširitev

Pomemni:

- 1) F karakteristike 0, k razgradnepočit polinoma $f(x) \in F[x]$
 $\Rightarrow K/F$ Galoisjeva razširitev
- 2) \mathbb{Z}_p . Vseke končne razširitev K/\mathbb{Z}_p je Galoisjeva

$\ker \mathbb{Z}_p$ pravilno $\Rightarrow K/\mathbb{Z}_p$ separabilna
 $\Rightarrow K$ je razgradnepočit $X^p - X \in \mathbb{Z}_p[X]$
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 $\Rightarrow K/L$ normalne
- 3) K/F separabilna $\Rightarrow K/L$ separabilna

Dokaz:

- 1) Enostavno
- 2) $f(x) \in L[X]$ ima eno nico aek
(nerezogen)
Dokazujemo: Vsičke nicoe $f(x) \in K$

Naj bo $p(x) \in F[X]$ minimalni polinom a nad F
 $p(x)$ ima eno nico v K , K/F je normalna
 $\Rightarrow p(x)$ ima vse nicoe v K

Trdimo: $f(x) \mid p(x)$

d(x) največji skupni delitelj: $f(x), p(x) \in L[X]$
 $d(x) = f(x)$.

$f(x), p(x)$ imata skupno nico a $\Rightarrow d(x) = 0$
 $\Rightarrow d(x)$ ni konstanten, deli $f(x)$, ki je nerezogen
 $\Rightarrow d(x) = f(x) \Rightarrow f(x) \mid p(x) \Rightarrow$
 \Rightarrow nicoe $f(x)$ so tudi nicoe $p(x)$, torej $\in K$

3) aek, $p(x) \in L[X]$ minimalni polinom a je nad L

Naj bo $g(x) \in F[X]$ minimalni polinom
a je nad F

K/F separabilna $\Rightarrow g(x)$ ima sene enostevne
nicoe.

Isti dokaz kot v 2) poleži $p(x) \mid g(x)$
zato $p(x)$ nima vedenih nicoel

Opoziba: $F \subseteq L \subseteq K$

- 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)

$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[3]{2}, \epsilon_1)$

normalna \nearrow
je normalna \searrow

$x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4})$ razpadno polje $x^3 - 2$ nad \mathbb{Q}

$-\epsilon_1 + \epsilon_2 = -\sqrt[3]{2}$

\uparrow
 $\text{ni re}\nearrow\text{re}$

Galoisova grupa razširitive

Def: K/F nej bo razširitev. Nej bo $\alpha: K \rightarrow K$ automorfizem.

Pravimo da je α F -automorfizem, če je $\alpha|_F = \text{id}_F$

Množici vseh automorfizmov polja K pravimo Galoisova grupa razširitve K/F

Opomba:

Automorfizm: polja K : $\text{Aut}(K)$

To je grupa za kompozicijo

Galoisova grupa razširitive bomo označili:

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

$\text{Gal}(K/F)$ je podgrupa v $\text{Aut}(K)$

$\alpha, \beta \in \text{Gal}(K/F)$:

$$x \in F. (\alpha(\beta^{-1})(x)) = \alpha(\beta^{-1}(x)) = \overset{\substack{\text{"id" na } F \\ \text{"}}}{\alpha(x)} = x$$

Trdítav: Mož bo $p(x) \in \mathbb{K}[x]$ in akk
nicle teža polinoma

Za polinom $\delta \in \text{Aut}(\mathbb{K}/F)$ je tudi

$\delta(a)$ nicle polinoma $p(x)$

Dokaz:

$$p(x) = \sum_{k=0}^n a_k x^k \quad a_k \in F$$

$$p(a) = 0$$

$$p(\delta(a)) = \sum a_k (\delta(a))^k = \sum a_k (\delta(a^k)) =$$

$$= \sum \underbrace{\delta(a_k) \cdot \delta(a^k)}_{\substack{a_k \in F \\ \delta_F = id}} = \sum \delta(a_k a^k) =$$

$$\delta_F = id$$

$$= \delta \left(\sum a_k a^k \right) = \delta(0) = 0$$

$$p(a) = 0$$



Komentar: V praksi bomo gledeči primere
ko je K/F končna separabilna.

Zadek. $K = F(a)$ (izrek - primitivevem elementu)

$\delta \in \text{Gal}(K/F)$ je nekakšna delovanja s stikom a-ja

$$x \in K: x = \sum a_n \cdot a^n \quad \delta(x) = \sum a_n \delta(a^n)$$
$$a_n \in F$$

Če je pod $\text{EF}(x)$ minimalni polinom a-ja nad F ,
je $\delta(a)$ tudi nista, ki leži v K

To pomeni: $\text{Gal}(K/F)$ je končna grupe in
 $|\text{Gal}(K/F)| \leq \text{st. nista}$ pod $v K$

V resnici velja enačaj:

$b \in K$ naj bo poljubna nista polinoma pod

Trdimo: $\exists \delta \in \text{Gal}(K/F), \delta: a \mapsto b$
a in b imata stevilo: minimalni polinom

Po neki trditvi: \exists izomorfizem $F(a) \rightarrow F(b)$

$$\tilde{\delta}|_F = \text{id} \quad " \quad "$$

za v nista imamo en izomorfizem

Sklep: $|\text{Gal}(K/F)| = \text{st. nista}$ pod $v K$

Postedica:

Če je K/F končna Galoisova razširitev,
potem $|\text{Gal}(K/F)| = [K : F]$

Dokaz:

Ob označah na prejšnji strani: ima
poljske nicle nad K zaradi normalnosti
 $|\text{Gal}(K/F)| = \text{st pol} = [K : F]$

Opomba K/F končna separabilna $K = FG$
polje $F[\bar{x}]$ minimalni polinom
 a_0, \dots, a_n nicle polja ki so v K
 $\delta \in \text{Gal}(K/F)$ zaradi bijektivnosti
 δ permutira nicle (slike nicle v nicle)
 δ določa permutacijo S_n

DN: name injektiven homomorfizem grup
 $\text{Gal}(K/F) \longrightarrow S_n$

Primer:

• Gal (\mathbb{C}/\mathbb{R})

$$\mathbb{C} = \mathbb{R}(i)$$

$\delta \in \text{Gal}(\mathbb{C}/\mathbb{R})$ je določen s katerim je

$$\begin{aligned} p(x) &= x^2 + 1 \quad \text{minimální polynom}: j \\ &= (x-i)(x+i) \end{aligned}$$

$\delta(i)$ je ena od níčel k: $i \mapsto \pm i$ v \mathbb{C}

$\delta \in \{id; i \mapsto -i\}$

$$\delta(a+bi) = a+b\delta(i) = a-bi \quad \text{konjugiranje}$$

DN: 3rd premišljek za $\text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$

• $\text{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$: normalna razširitev

$\delta \in \text{Gal}(\dots)$:

minimální polynom $p(x) = x^2 - 2$

níčle: $\sqrt{2}, 2$ komplementi:

Edina možnost $\delta(\sqrt{2}) = \sqrt{2} \Rightarrow id$ je edina tak avtomorfizem $\Rightarrow \text{Gal}(\dots) = \{id\}$

• $\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = ?$

Vsek d v $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ je oblike

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$$

$$(x^2 - 2)(x^2 - 3) \quad \text{určí } \sqrt{2} \text{ in } \sqrt{3}$$

degledu $\sqrt{2} = x^2 - 2$ ga urči:

δ gleda $\sqrt{2}$ v eno od teh níčel

$$\sqrt{2} \mapsto \pm \sqrt{2}$$

enak premišlek za $\sqrt{3}$

$$\sqrt{3} \mapsto \pm \sqrt{3}$$

Imamo 4 automorfizme

$$|\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})| = 4 \quad x \in \mathbb{Z}_2 \text{ ali } \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

$$\delta_1: \sqrt{2} \mapsto \sqrt{2}, \sqrt{3} \mapsto \sqrt{3} =: id$$

$$\delta_2: \sqrt{2} \mapsto -\sqrt{2}, \sqrt{3} \mapsto \sqrt{3} \quad \text{red 2}$$

$$\delta_3: \sqrt{2} \mapsto \sqrt{2}; \sqrt{3} \mapsto -\sqrt{3} \quad \text{red 2}$$

$$\delta_4: \sqrt{2} \mapsto -\sqrt{2}; \sqrt{3} \mapsto -\sqrt{3} \quad \text{red 2}$$

Def: Nej bo $f(x) \in F[x]$. Galoizova grupe polinoma $f(x)$ nad F je

$\text{Gal}_F f(x) = \text{Gal}(K/F)$ kjer je K razpadno polje polinoma $f(x)$ nad F

Opozber:

$K = F(a_1, \dots, a_m)$ a_1, \dots, a_m nicle $f(x)$

$\delta \in \text{Gal}_F f(x)$ spet permutira a_1, \dots, a_m

$$\text{Gal}_F f(x) \rightarrow S_m$$

Primer:

$f(x) \in \mathbb{Q}[x]$ polinom stopnje 2

$\text{Gal}_{\mathbb{Q}} f(x) = ?$

a_1, a_2 nicle

$K = \mathbb{Q}(a_1, a_2)$

$$f(x) = x^2 + px + q$$

$$a_1 + a_2 = -p \quad po \text{ Vieta's formulah}$$

$$\Rightarrow \mathbb{Q}(a_1, a_2) = \mathbb{Q}(a_1)$$

$\delta \in \text{Gal}_{\mathbb{Q}} F$ je deljenec z $\delta(a_1)$

$$1) a_1 \in \mathbb{Q} \Rightarrow \delta(a_1) = a_1 \Rightarrow \delta = id \Rightarrow \text{Gal}_{\mathbb{Q}} = \{id\}$$

2) $a_1 \notin \mathbb{Q} \Rightarrow f(x)$ je minimalni polinom a_1 z močnostjo:

$$\begin{array}{l} a_1 \mapsto a_1 \\ a_1 \mapsto a_2 \end{array} \quad x \in \mathbb{Z}_2$$

$$f(x) = x^2 + px + q \in \mathbb{Q}[x]$$

a_1, a_2, a_3 nijo bodo nicle

$$K = \mathbb{Q}(a_1, a_2, a_3)$$

$$\text{Vieta: } (x-a_1)(x-a_2)(x-a_3)$$

$$a_1 + a_2 + a_3 = -p$$

$$a_3 = -p - a_1 - a_2$$

$$K = \mathbb{Q}(a_1, a_2)$$

lastne prime:

$$1) a_1, a_2 \in \mathbb{Q} \Rightarrow \delta = id \Rightarrow \text{Gal}_F f(x) = \{id\}$$

$$2) a_1 \in \mathbb{Q}, a_2 \notin \mathbb{Q} \quad a_1 \mapsto a_1 \quad \text{minim. pol.} \quad a_2 \mapsto a_3 \quad \text{Gal}_{\mathbb{Q}} f(x) = \{id, (2, 3)\}$$

$$3) a_1, a_2 \notin \mathbb{Q}, a_3 \in \mathbb{Q} \quad a_1 \mapsto a_2 \quad a_2 \mapsto a_1 \quad \text{Gal} = \{id, (1, 2)\}$$

$$a_3 \mapsto a_3$$

$$a_1 \mapsto a_2 \quad a_2 \mapsto a_1 \quad \text{Gal} = \{id, (1, 2)\}$$

$$a_3 \mapsto a_3$$

$$a_1 \mapsto a_2 \quad a_2 \mapsto a_3 \quad a_3 \mapsto a_1 \quad \text{Gal} = \{id, (1, 2, 3)\}$$

$$a_1 \mapsto a_3 \quad a_3 \mapsto a_1 \quad \text{Gal} = \{id, (1, 3)\}$$

$$a_2 \mapsto a_1 \quad a_1 \mapsto a_2 \quad \text{Gal} = \{id, (2, 1)\}$$

$$a_3 \mapsto a_2 \quad a_2 \mapsto a_3 \quad \text{Gal} = \{id, (3, 2)\}$$

Dobimo vse permutacije niclev niclev

$$\text{Gal} \cong S_3$$

Primer

$$\text{Gal}_\alpha((x^2-2)(x^2-3)) = \text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

\uparrow

$$K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

$$\text{Gal}_\alpha(x^5-1)$$

$$\varepsilon = \cos \frac{2\pi}{5} + i \sin \frac{2\pi}{5}$$

$$\text{mild}: 1, \varepsilon, \varepsilon^2, \varepsilon^3, \varepsilon^4$$

Rozpadne podje:

$$K = \mathbb{Q}(\varepsilon)$$

$$\text{minimalni polinom } \varepsilon: (x-1) \underbrace{(x^4 + x^3 + x^2 + x + 1)}$$

$$\delta \in \text{Gal}_\alpha(x^5-1)$$

$$\begin{matrix} \text{minimalni polinom} \\ \text{mild: } \varepsilon, \varepsilon^2, \varepsilon^3, \varepsilon^4 \end{matrix}$$

$$\varepsilon \mapsto \varepsilon \quad \varepsilon \mapsto \varepsilon^2 \quad \varepsilon \mapsto \varepsilon^3 \quad \varepsilon \mapsto \varepsilon^4$$

$$\text{id} \quad \delta_1 \neq \text{id}$$

$$\text{Gal}_\alpha(x^5-1) \cong \mathbb{Z}_4$$

Lemma: Nej bo K/F konzra, aek

$$H \subseteq \text{Gal}(K/F)$$

$$\text{Nej bo } \{\sigma(a); \sigma \in H\} = \{a = a_1, \dots, a_m\}$$

Potem $p(x) = (x-a_1)(x-a_2) \dots (x-a_n)$
minimalni polinom aje nad K^H

Dokaz:

$$p(x) \in K^H[x]$$

$$p(x) = \sum a_k x^k$$

$\varphi \in H$ polinom

$$\begin{aligned} p_\varphi(x) &= \sum p(\alpha_k) x^k = (x - p(\alpha_1)) \dots (x - p(\alpha_m)) \\ &= (x - \underbrace{p(\sigma_1(a))}_{\in H \text{ "a" }}) \dots (x - \underbrace{p(\sigma_m(a))}_{\in H \text{ "a" }}) \end{aligned}$$

Pazadi injektivnosti permutira a_1, \dots, a_m

$p_\varphi(x)$ je do premešanja nebenzo polinom

$$p_\varphi(x) = p(x)$$

m: minimalnost

$$g(x) \in K^H[x], g(x) = 0 \Rightarrow (x-a) \mid g(x) \text{ v } K[x]$$

$\forall \sigma \in H : \sigma(a)$ jeholi niza $g(x) \Rightarrow$

$$(x-a_1) \mid g(x), \dots, (x-a_m) \mid g(x)$$

\nwarrow tuji so si med seba

$$\Rightarrow p(x) \mid g(x)$$

Lema: Naj bo K/F končna, separabilna (resiriva),
 $H \leq \text{Gal}(K/F)$

a) $|H| = [K : K^H]$

b) $K^F = |H| \cdot [K^H : F]$

Dokaz:

Po izreku o primitivnem elementu

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

$$K = K^H(a) = F(a)$$

$$K = F(a) \subseteq K^H(a) \subseteq K$$

$[K : K^H] = \text{stopnja minimalnega polinoma}$

a-ja nad K^H

$$= |\{\sigma(a); \sigma \in H\}|$$

po prejšnjih temi

Davalje je videti da ceimamo σ_1 in $\sigma_2 \in H$

$$\sigma_1 \neq \sigma_2 \Rightarrow \sigma_1(a) \neq \sigma_2(a)$$

$$\sigma_1, \sigma_2: K \rightarrow K$$

$$\sigma_1|_{K^H} = \text{id} = \sigma_2|_{K^H}$$

kr $K = K^H(a)$, če bo veljalo

$$\sigma_1(a) = \sigma_2(a) \text{ bi sledilo } \sigma_1 = \sigma_2$$



Izrek:

Naj bo K/F končna separabilna niz.

NTSE

$$1) |\text{Gal}(K/F)| = [K:F]$$

$$2) K^{\text{Gal}(K/F)} = F$$

3) K/F je normalna

Dokazi:

$$1) \Rightarrow 2) \text{ Po prejšnjem lem.}$$

$$[K : K^{\text{Gal}(K/F)}] = |\text{Gal}(K/F)| = [K:F]$$

$$\text{Po drugi strani: } [K:F] = [\underbrace{K : \text{Gal}(K/F)}_{\text{II}}] [\underbrace{K^{\text{Gal}(K/F)} : F}_{\text{I}}]$$

$$\Rightarrow K^{\text{Gal}(K/F)} = F$$

II
I

$$2) \Rightarrow 3)$$

Naj bo $f(x) \in F[x]$ nerazce polinom, ki ima eno nizo v K

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

Uporabimo 1. lemo;

$f(x)$ je minimalni polinom z nizo $K^{\text{Gal}(K/F)}$

$$f(x) = (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_m)$$

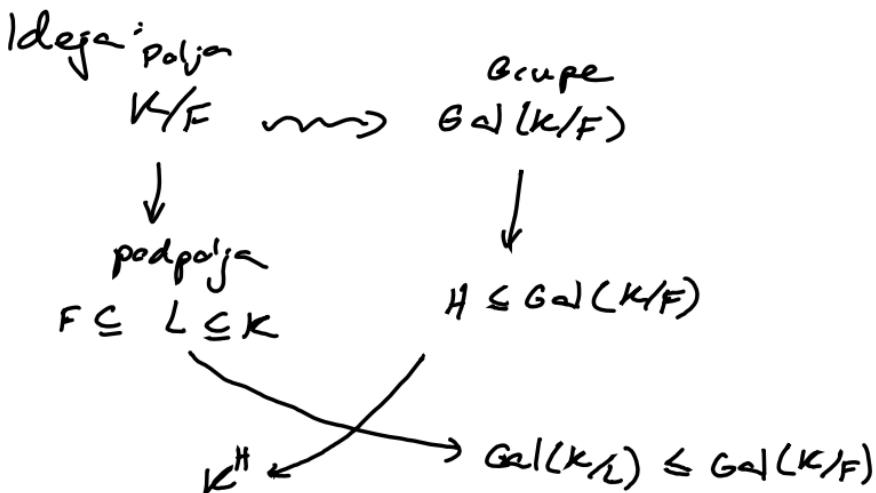
Ostale nizi $f(x)$ so $\sigma(\alpha)$; $\sigma \in \text{Gal}(K/F)$

$$\sigma(\alpha) \in K$$

\Rightarrow Ostale nizi s = v K

3) $\Rightarrow 1)$ Če dokazemo

Fundamentalni izrek Galoisove teorije



Izrek: Maj bo K/F končna Galoisova razširitev

Oznakimo $\bar{F} = \{\text{vmesna polja med } F \text{ in } K\}$

$$\mathcal{G} = \{\text{podgrupe } \text{Gal}(K/F)\}$$

Dopolnilne projekcije

$$\alpha: \mathcal{G} \longrightarrow \bar{F} \quad \beta: \bar{F} \longrightarrow \mathcal{G}$$

$$H \longmapsto K^H \quad L \longmapsto \text{Gal}(K/L)$$

a) α in β sta vzejmo izvesni preslikavi
Obstaja torej bijektivna korespondenca
med vmesnimi polji razširitve K/F in
podgrupami Galoisove grupe (K/F)

b) $|\text{Gal}(K/L)| = [K:L] \quad \forall F \subseteq L \subseteq K$

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

c) L, L' nej boste mešni podji, potem
 $L \subseteq L' \iff \text{Gal}(K/L') \subseteq \text{Gal}(K/L)$

d) L/F je normalna razš. $\iff \text{Gal}(K/L) \trianglelefteq \text{Gal}(K/F)$

V tem primeru je $\frac{\text{Gal}(K/F)}{\text{Gal}(K/L)} \cong \text{Gal}(L/F)$

Opozor: $F \subseteq L \subseteq K$; končnost (normalnost
separabilnost) se iz K/F vedno podedejuje
na K/L

ne L/F se podedejuje končnost in
separabilnost, izrek pa ne kaže da
normalnost

Dokaz:

K/L je Galoisova razširitev

$$\alpha \circ \beta: L \xrightarrow{\beta} \text{Gal}(K/L) \xrightarrow{\alpha} K^{\text{Gal}(K,L)} = L$$

$$\beta \circ \alpha: H \rightarrow K^H \rightarrow \text{Gal}(K/K^H) = H$$

$$\text{Gal}(K/K^H) = [K : K^H] = |H|$$

Po definiciji: $\forall H \subseteq \text{Gal}(K/K^H)$

$$\Rightarrow H = \text{Gal}(K/K^H) \quad (\text{podgrupa je izjema močjo})$$

b)

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

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

$$c) \quad = [L : F]$$

$$(\Rightarrow) \sigma \in \text{Gal}(K/L) \Rightarrow \sigma|_L = id \Rightarrow \sigma|_L = id \Rightarrow \sigma \in \text{Gal}(K/L)$$

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

$L = K^{\text{Gal}(K/L)}$ ker ste K/L in K/L Galoisov;

$$x \in L = K^{\text{Gal}(K/L)} \Rightarrow \forall \sigma \in \text{Gal}(K/L), \sigma(x) = x$$

$$\Rightarrow \forall \sigma \in \text{Gal}(K/F), \sigma(x) = x \Rightarrow$$

$$x \in K^{\text{Gal}(K/L)} = L$$

a) Naj prej si ogledimo

$$\text{Gal}(K/L) \triangleleft \text{Gal}(K/F) \Leftrightarrow$$

$$\forall \sigma \in \text{Gal}(K/F), \forall g \in \text{Gal}(K/L), \sigma^{-1}g\sigma \in \text{Gal}(K/L)$$

$$\Leftrightarrow \forall x \in L, \sigma^{-1}g\sigma(x) = x \quad \forall \sigma, g$$

$$\Leftrightarrow g(\sigma(x)) = \sigma(x)$$

$$\Leftrightarrow \forall x \in L, \sigma(x) \in K^{\text{Gal}(K/L)} = L$$

\Leftrightarrow

$$\forall \sigma \in \text{Gal}(K/F), \sigma(L) \subseteq L$$

$$\Leftrightarrow \forall \sigma \in \text{Gal}(K/F), \sigma(L) = L$$

Dokazimo ekvivalenco:

L/F je normalne

$$\Leftrightarrow \text{Naj bo } \text{Gal}(K/L) \triangleleft \text{Gal}(K/F)$$

$$\forall \sigma \in \text{Gal}(K/F), \sigma|_L = id$$

$$\Leftrightarrow \sigma \in \text{Gal}(K/L)$$

$$\text{ker } \Phi = \text{Gal}(K/F)$$

$$\text{nato: } \frac{\text{Gal}(K/F)}{\text{Gal}(K/L)} \cong \text{im } \Phi \leq \text{Gal}(K/F)$$

Med drugim:

$$\text{Gal}(K/F) : \text{Gal}(K/L) \leq \text{Gal}(L/F)$$

$$\Leftrightarrow [L : L^{\text{Gal}(L/F)}] \leq [L : F] = \frac{[K : F]}{[K : L]}$$

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

$$\Rightarrow vse neenakosti tu so enacji:$$

$|\text{Gal}(L/F)| = [L : F]$ za konkrete razpoložitve, to pomeni: L/F je normalna

severje neenakosti, tudi implicira da je

Φ surjektiven

$$(\Leftarrow) L/F je normalna, torej je L razpoložna po kakega polinoma$$

$$L = F(a_1, \dots, a_n) \quad a_1, \dots, a_n \text{ nicle pos}$$

Izberimo poljuben $\sigma \in \text{Gal}(K/F)$

σ je delocen s slikami: a_1, \dots, a_n

$\sigma(a_i)$ je tudi nicle od pos

$$\Rightarrow \sigma(L) \subseteq L \quad (\text{ker } \Phi \text{ samo preuredi nicle})$$

$$\Rightarrow \text{Gal}(K/L) \triangleleft \text{Gal}(K/F)$$

Primer

$$\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$$

$$\sqrt{2} \mapsto \pm\sqrt{2}$$

$$\sqrt{3} \mapsto \pm\sqrt{3}$$

elementi $\mathbb{Q}(\sqrt{2}, \sqrt{3})$:

$$\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} ; a, b, c, d \in \mathbb{Q}\}$$

$$\text{id}: \begin{array}{l} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{array}$$

$$\sigma: \begin{array}{l} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto \sqrt{3} \end{array}$$

$$\tau: \begin{array}{l} \sqrt{2} \mapsto \sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{array}$$

$$\sigma \circ \tau: \begin{array}{l} \sqrt{2} \mapsto -\sqrt{2} \\ \sqrt{3} \mapsto -\sqrt{3} \end{array}$$

$$\text{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}) = \{\text{id}, \sigma, \tau, \sigma \circ \tau\}$$

Podgrupe:

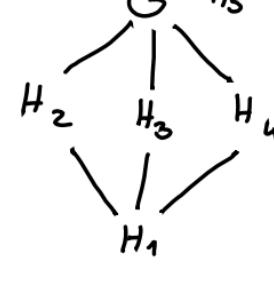
$$H_1 = \{\text{id}\}$$

$$H_2 = \{\text{id}, \sigma\}$$

$$H_3 = \{\text{id}, \tau\}$$

$$H_4 = \{\text{id}, \sigma \circ \tau\}$$

$$H_5 = G$$



Fikirna podgrupa: po fundamentalnem izreku so to nekakšne vsevmesne podgrupe med \mathbb{Q} in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$

$$K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

$$K^{H_1} = K^{\{\text{id}\}} = K$$

$$K^{H_2} = K^{\{\text{id}, \sigma\}}$$

$$\begin{aligned} \sigma(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) &= \\ &= a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6} = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \end{aligned}$$

$$b = 0 = d$$

$$K^{H_2} = \{a + c\sqrt{3} ; a, c \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{3})$$

$$K^{H_3} = \mathbb{Q}(\sqrt{2})$$

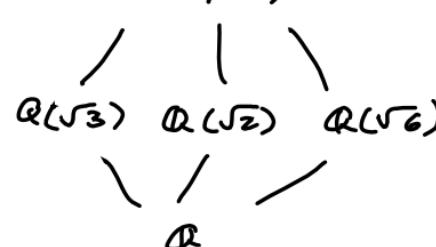
$$K^{H_4} = \mathbb{Q}(\sqrt{6})$$

$$\sigma(\tau(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6})) =$$

$$a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6} = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$$

$$\Rightarrow K^{H_4} = \{a + d\sqrt{6} ; a, d \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{6})$$

$$K^{H_5} = \mathbb{Q}$$



(NE) Rešljivost polinomskih enačb
z radikeli

Def: $f(x) \in F[x]$ je rešljiv z radikeli:
 $\Leftrightarrow \exists a_1, \dots, a_k \in K$ (k je rezidr. na F), za
katere velja.

1) $f(x)$ razpade nad $F(a_1, \dots, a_k)$

2) $\exists n_1 \in \mathbb{N}, a_1^{n_1} \in F$

$\exists n_2 \dots n_r \in \mathbb{N}, a_i^{n_i} \in F(a_1, \dots, a_{i-1})$

Kaj to pomeni?

1) nicle $f(x)$ so v $F(a_1, \dots, a_k)$

\Downarrow
nicle so rac. funkcije a-i-jev

2) $a_1 = \sqrt[n_1]{\alpha} \quad \alpha \in F$

$a_2 = \sqrt[n_2]{\beta} \quad \beta \in F(a_1)$

$= \sqrt[n_2]{\sqrt[n_1]{\beta}}$ rationalna F v $\sqrt[3]{\alpha}$

Primer

$$ax^2 + bx + c \quad a, b, c \in F$$

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

$f(x)$ razпаде на $F(a_1) \quad a_1^2 = b^2 - 4ac$

$$a_1^2 \in F$$

Polinom: stepnje 2 s oršljivim radikeli
polobno za 3 stepnje

Lem a:

Naj bo $F \subseteq \mathbb{C}$, $\alpha \in F$ nelič.

Potem je $\text{Gal}_F(x^n - \alpha)$ rešljiva grupe

Opomba: Lastnosti rešljivih grup

- 1) Podgrupe rešljive grupe je rešljive
- 2) Kvocient rešljive je rešljive
- 3) $\forall \alpha \in G \wedge G/\langle \alpha \rangle$ rešljivi $\Rightarrow G$ rešljivo

Dokaz:

$K = \text{razpadno polje } x^n - \alpha \text{ nad } F$

Naj bo a neka nicle $x^n - \alpha$

Vse nicle: $a, aw, aw^2, \dots, aw^{n-1} \quad w = e^{\frac{2\pi i}{n}}$

$K = F(a, w) \Rightarrow F(a, w)/F$ je normalna razširitev. Zaradi karakteristike 0 je Galoisova

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

$F(w)/F$ Galoisova

$$\underbrace{F}_{\text{normalne}} \subseteq F(w) \subseteq F(a, w)$$

Po fundamentalnem izreku:

$$\text{Gal}(F(a, w)/F(w)) \triangleleft \text{Gal}(F(a, w)/F)$$

Velja še: $\frac{\text{Gal}(F(a, w)/F)}{\text{Gal}(F(a, w)/F(w))} \cong \text{Gal}(F(w)/F)$
za to dokazujemo da je rešljiva

Dokaz: bomo določili $\text{Gal}(F(w)/F)$ in

$\text{Gal}(F(a, w)/F(w))$ abelovi

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

σ, τ sta določeni s sliko w

$$\sigma(w) = w^j \quad \tau(w) = w^i$$

$$\sigma \tau(w) = w^{j+i} = w^{i+j} = \tau \sigma(w)$$

$$\Rightarrow \sigma \tau = \tau \sigma$$

Podobno za $\text{Gal}(F(a, w)/F(w))$

Po 3) iz opombe sledi rezultat

Izrek: $F \subseteq \mathbb{C}$, $f(x) \in F[x]$

nej bo $F[x]$ rešljiv z radikali nad F

\Rightarrow Galojeva grupa $\text{Gal}(F)$ nad F je vedno rešljiva

Opomba: $p(x) \in \mathbb{Q}[x]$ nerazcegen nad \mathbb{Q} st. 5

če ima $p(x)$ natanko 3 reštne nicle

\Rightarrow Galojeva grupa $\text{Gal}(F)$ nad $\mathbb{Q} \cong S_3$

S_3 ni rešljiva $\Rightarrow p(x)$ ni rešljiv z radikali nad $\mathbb{Q} \Rightarrow$ ni formula :

(ampak nad \mathbb{R} se da)

Primer: $p(x) = x^5 - 3x^4 + 3$

Dokaz: $\exists a_1, \dots, a_m$ fks razpade nad $F(a_1, \dots, a_m)$

$a_i^{n_i} \in F$

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

$K_p :=$ razpadna polje $f(x)$ nad F

Dokazjemo $\underline{\text{Gal}}(K_p/F)$ rešljiva

$K_\alpha :=$ razpadna polje $x^{n_1} - \alpha$ nad F $\alpha = a_i^{n_i}$

$K :=$ razpadna polje fks nad K_α

$a_1 \in K_\alpha$

$F \subseteq K_\alpha \subseteq K$

$F \subseteq K_p \subseteq K$

K je tudi razpadna polje $f(x)(x^{n_1} - \alpha)$ nad F

$\Rightarrow K/F$ je galojsava razširitev

Vemo $\underline{\text{Gal}}(K_\alpha/F)$ in $\underline{\text{Gal}}(K_p/F)$ sta tudi Galojsav.

Po Amd. izrek je

$\text{Gal}(K/F) \triangleleft \text{Gal}(K_p/F)$

in $\frac{\text{Gal}(K/F)}{\text{Gal}(K/K_p)} \cong \underbrace{\text{Gal}(K_p/F)}$
dokazjemo da je ta rešljiva

Dovolj je dokazati da je $\text{Gal}(K/F)$ rešljiva
indukcija po m

$m=1$: fks 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 $K = K_\alpha$

$\text{Gal}(K/F) = \text{Gal}(K_\alpha/F)$ je po tem: rešljiva

$m > 1$:
 $a_n \in K(\alpha)$

$f(x)$ razpade nad $K_\alpha(a_2, \dots, a_n)$

po ind. predpostavki je $\text{Gal}(K/K_\alpha)$ rešljive

K_α/F je normalna

zato je $\text{Gal}(K/K_\alpha) \triangleleft \text{Gal}(K/F)$

$\frac{\text{Gal}(K/F)}{\text{Gal}(K/K_\alpha)} \cong \underbrace{\text{Gal}(K_\alpha/F)}$ $\Rightarrow \text{Gal}(K/F)$

rešljiva rešljiva rešljiva