Uvod v teorijo grup

Operacija na množici $S \neq \emptyset$

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

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

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

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

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

Definicija: Polgrupa z enoto je monoid

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

a) $l \in S$ je levi inverz, če velja $lx = x$

b) $d \in S$ je desni inverz, če $x \star d = x$

c) $y \in S$ je inverz, če $x \star y = y \star x = e$

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

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

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

Če je $\star$ komutativna je abelova

Zgledi:

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

2) X neprazna množica

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

operacija: kompozitum $\circ$

asociativnost, enota, inverz

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

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

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

.... simetrična grupa reda n

Ponovitev o permutacijah

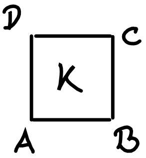
(elementi S_n)

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

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

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

Zgled: Simetrije kvadrata



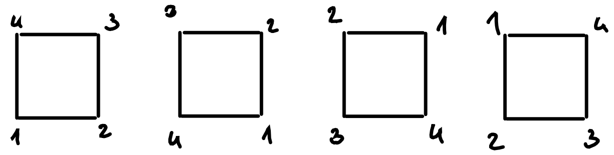
= izometrije $f:\mathbb{R}^2\to\mathbb{R}^2$, da je $f_*(K)=K$

$f|_K: K\to K$ je bijekcija

Preverimo da je množica simetrij grupa za kompozitum

Simetrija slika oglišča v oglišča

↳ permutacija oglišč

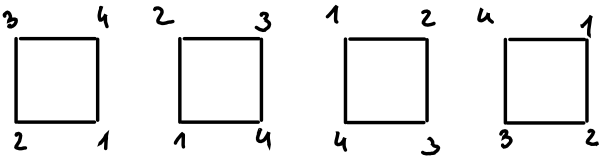


id $\parallel$ r^4

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

r^2

r^3



z - zrcaljenje čez fiksno os simetrije

rz / zr^3

r^2z / zr^2

r^3z / zr

$z^2 = id$

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

$r^3z = zr$

$rzr = 1$

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

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

Trdimo: kvadrat ima največ 8 simetrij

Simetrija je določena s sliko oglišča 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

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

Diederska grupa moči 8

Splošna simetrasija:

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

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

Diederska grupa moči $2n$

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

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

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

S^* je grupa za $\star$

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

Ali je S^* zaprta za operacijo

$x, y \in S^*$

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

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

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

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

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

splošna linearna grupa $n \times n$ matrik

Direktni produkt grup

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

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

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

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

DN: to je grupa

Oznake:

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

Podgrupe

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

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

Trditev: Naslednje trditve so ekvivalentne

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

Dokaz:

$2 \Rightarrow 3$

$1 \in H$

· Izberemo $x \in H$ $y = x$

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

Naj bo $x \in H$ poljuben

$x^{-1} \in H$

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

Izberemo $y \in H$

$y^{-1} \in H$

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

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

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

Primer:

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

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

$H \leq \mathbb{Z}$ brez škode za splošnost H ni trivialna

H gotovo vsebuje vsaj eno neravno število

Naj bo n najmanjše neravno število v H

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

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

Vzemimo poljuben $m \in H$

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

$r = \underset{\in H}{m} - \underset{\in H}{kn} \in H \qquad r < n$

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

Primer

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

je grupa za množenje matrik

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

$SL_n(\mathbb{R})$

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

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

Trditev: Naj bosta $K, K \leq G$

Potem tudi $H \cap K \leq G$

Enako za preseke poljubnih družin podmnožic

Definicija: Naj bosta $HK \subseteq G$

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

produkt grup

Opomba:

HK ni vedno grupa

$G = S_3$

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

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

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

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

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

$HK = KH$

potem je HK podgrupa

Dokaz:

$a, b \in HK$

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

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

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

✓ ∎

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

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

Potem je to tudi podgrupa

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

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

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

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

DN: Naj bo G grupa

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

je podgrupa v G (center grupe G

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

podgrupa v G (centralizator elementa

a v G)

Odsek podgrup in Lagrangeov izrek

Naj bo G grupa in H podgrupa G
Vpeljemo relacijo na G

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

Trditev: relacija je ekvivalenca

Naj bo G končna grupa

G/H je tudi končna

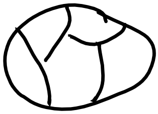
moč množice označimo z $|G:H|$ indeks podgrupe H v grupi G

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

To je Lagrangeev izrek

Dokaz: $|G:H| = r$

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



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

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

$$\varphi : H \longrightarrow a_iH$$
$$h \longmapsto a_ih$$

φ je očitno surjektivna

injektivnost

$$\varphi(h_1) = \varphi(h_2)$$
$$a_ih_1 = a_ih_2 \quad / a_i^{-1}$$
$$h_1 = h_2$$

$\blacksquare$

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

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

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

Dokažemo $(a'+b')-(a+b)\in H$

$$a'+b'-a-b \overset{\text{komutativnost}}{=} (a'-a)-(b-b')\in H$$

G/H je abelova grupa za to operacijo

Generatorji grup, ciklične grupe

Definicija: Naj bo G grupa in X podmnožica v G. Potem označimo z $\langle X \rangle$ najmanjšo podgrupo, v G, ki vsebuje množico X.
Tej podgrupi pravimo <u>podgrupa generirana z množico X</u>

Zakaj je to smiselno?

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

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

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

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

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

Kako izgledajo elementi $\langle X \rangle$?

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

Očitno (DN)

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

Trditev: $\langle X \rangle = S$

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

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

(Vzamemo produkt enega elementa x

$a, b \in S$

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

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

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

Posledica: $a \in G$

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

Pimeri:

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

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

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

(Vsaki dve tuji števili generirata $\mathbb{Z}$

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

Primeri:

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

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

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

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

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

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

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

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

$a^k = a^l \quad / a^{-k}$
$1 = a^{l-k}$ $l-k < n$ kar je v protislovju z predpostavko.

$\Leftarrow$ Recimo da $|\langle a \rangle| = n$
Potem ima a končen red
Po prejšnjem sklepu ima
$\langle a \rangle = \{1, a, \ldots, a^{m-1}\}$
Sledi: $m = n$

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

Posledica: Naj bo G končna grupa

1) $\forall a \in G$. red a deli $|G|$

2) $\forall a \in G$. $a^{|G|} = 1$

3) $|G|$ je praštevilo $\Rightarrow$ G je ciklična

Dokaz:

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

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

2) Naj bo red $a = n$

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

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

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

$a^p = 1$

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

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

Sledi $G = \langle a \rangle$

Uvod v teorijo kolobarjev, obsegov, polj in algeber

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

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

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

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

Če je $\cdot$ komutativna je K komutativen

Zgledi:

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

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

  seštevanje in množenje po točkah

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

Homomorfizm:

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

Homomorfizem kolobarjev:

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

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

$f(1)=1$

zakaj moramo to definirati

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

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

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

$f(1)$ ni enota v tem kolobarju

Homomorfizem algeber $f:A\longrightarrow B$

- f je homomorfizem kolobarjev in
- linearna preslikava

Opomba: če je $f: A \to B$ izomorfizem

potem je f^{-1} izomorfizem

potem $A \cong B$

a je fiksen

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

f je avtomorfizem grup

notranji avtomorfizem

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

K komutativen kolobar

$ev_a : K[X] \to X$ evaluacija

$p \mapsto p(a)$

$N \leq G$ je **Podgrupa edinka**, če

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

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

(Boljše ime bi bila normalna podgrupa)

Oznaka: $N \triangleleft G$

Primeri:

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

Grupe v katerih sta to edini edinki se imenujejo enostavne grupe

če je G abelova je vsaka podgrupa edinka

(obstajajo tudi nekomutativne kjer to velja)

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

Vpeljemo množenje kvaternionov

Kvaternionska grupa. Vsaka grupa je edinka

Trditevi ekvivalentne

1. $N \trianglelefteq G$
2. $\forall a \in G \quad aN \subseteq Na$
3. $\forall a \in G \quad aN = Na$
4. $\forall a \in G \quad aNa^{-1} = N$

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

Trdimo $H \triangleleft G$

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

BŠZS $a \notin H$

imamo dva leva odseka podgrupe H

$1 \cdot H = H$

$aH \neq H$

$G = H \cup aH$ disjunktna unija

$aH = G/H$

Desni odseki:

Lahko je videti, da imamo ~~samo~~ natanko dva desna odseka

H in Ha

$G = H \cup Ha$ disjunktna unija

$Ha = G/H$

Torej $Ha = aH$

Primer

S_n,

$A_n = \{$sode permutacije u $S_n\}$

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

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

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

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

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

Trditev: Naj bo G grupa

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

$$HN = NH \leq G$$

② če sta N, M podgrupi edinki v G

potem je $NM = MN \triangleleft G$

Dokaz:

1) $\forall h \in H$

$hN = Nh \Rightarrow HN = NH$ očitno

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

2) NM je podgrupa

$g \in G$

$gNMg^{-1} \in NM$

$gNg^{-1}gMg^{-1} \in N \cdot M$

Izrek:

Naj bo G grupa $N \triangleleft G$

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

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

dobro definirana operacija

s to operacijo postane množica G/N grupa

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

$\pi(g) = gN$ epimorfizem grup

$\ker \pi = N$

Dokaz:

dobra definiranost

če $aN = a'N$ in $bN = b'N \Rightarrow (ab)N = (a'b')N$

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

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

G/N je grupa

asociativnost pride iz G

enota: $1 \cdot N = N$

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

π je homomorfizem

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

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

Izrek: (1. izrek o izomorfizmu)

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

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

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

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

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

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

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

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

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

Dobro definiranost

$\underbrace{g\ker\rho = g'\ker\rho}$ želimo videti $\rho(g) = \rho(g')$

$\Downarrow$

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

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

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

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

ψ je homomorfizem

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

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

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

ψ je očitno epimorfizem

ψ je monomorfizem

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

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

$\rho(g) = 1$

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

$\ker\psi$ je trivialen torej

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

$\blacksquare$

Opomba: Edinke so jedra

1. homomorfizmov

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

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

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

Pravimo da je ψ induciran s ρ

shematično:

$$\begin{tikzcd} G \arrow[r, "\rho"] \arrow[d, "\pi"] & H \\ G/N \arrow[ur, dotted, "\psi"'] & \end{tikzcd}$$

kanonični epimorfizem

Ta diagram komutira

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

Izrek: (2. izrek o izomorfizmu)

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

Potem je:

1) $N \cap H \lhd H$

2) $N \lhd HN$

3) $HN/N \cong H/_{N \cap H}$

Ideja Dokaza:

1), 2) DN

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

$\varphi(h) := hN$

φ je epimorfizem

$\ker \varphi = H \cap N$

Uporabimo prvi izrek o izomorfizmu

$H/_{\ker \varphi} \cong \operatorname{im} \varphi$

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

Izrek (3. izrek o izomorfizmu)

Naj bo 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 dokaza

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

$\rho(gM) = gN$

ρ je dobro definiran epimorfizem

$\ker \rho = N/M$

Uporabimo 1. izrek o izomorfizm

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

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

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

2) če je $K \triangleleft G$ in φ 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:

zožitev φ na K

1) $\varphi(K) = \mathrm{im}\,\varphi|_K$ je podgrupa v H

2) $\varphi: G \to H$

$\varphi(K) \triangleleft H$

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

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

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

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

$$h x h^{-1} = \varphi(\underbrace{g k g^{-1}}_{\in K}) \in \varphi(K)$$

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

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

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

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

$g \in G$

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

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

Izrek: (Korespondenčni izrek)

Naj bo G grupa in $N \triangleleft G$

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

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

Dokaz a)

DN $H/N \leq G/N$

Obratna smer

Naj bo L poljubna podgrupa v G/N

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

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

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

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

Uporaba:

1. G poljubna grupa, $a \in G$

$\langle a \rangle$

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

Dokaz:

Recimo da reda $= \infty$

$$\begin{aligned} \rho : \mathbb{Z} &\longrightarrow A \\ n &\longmapsto a^n \end{aligned}$$

ρ je homomorfizem
je sur, je inj
$\ker \rho = \{0\}$

Recimo da reda $= n$

$$\begin{aligned} \rho : \mathbb{Z}_n &\longrightarrow \langle a \rangle \\ n &\longmapsto a^n \end{aligned}$$

je epi: $\operatorname{im} \rho = \langle a \rangle$

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

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

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

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

② Podgrupe v $\mathbb{Z}_n$

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

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

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

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

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

③

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

Dokaz:

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

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

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

$(\Rightarrow)$

$a \in G$ $a \neq 1$

$\langle a \rangle$ je netrivialna grupa

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

G je ciklična

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

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

Torej je n praštevilo

4. Izrek: (Cauchyjev izrek za abelove grupe)

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

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

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

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

$$\begin{matrix} \| & \| \\ 1 & 1 \end{matrix}$$

Torej $\text{red}\, aN \mid n$ ∎

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

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

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

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

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

$$\text{red}\, a = p \cdot k$$

$$a^{pk} = 1$$

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

Torej $\exists$ element da $\text{red} = p$

∎

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

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

φ je homomorfizem

$\ker\varphi = \{\pi \in S_n \,;\, \operatorname{sgn}\pi = 1\} = A_n \qquad A_n \triangleleft S_n$

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

⑥ F naj bo polje

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

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

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

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

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

(7.) G_1, G_2 grupi

$G_1 \times G_2$ je tudi grupa

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

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

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

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

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

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

$\tilde{G}_1 \cong G_1$

$(g_1, 1) \longmapsto g_1$

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

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

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

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

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

konjugiranje z elementom a
(Notranji avtomorfizmi)

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

$f_a \circ f_b = f_{ab}$

Z drugimi besedami: imamo homomorfizem

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

$\Phi(a) = f_a$

Φ je surjektiven

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

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

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

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

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

$\iff a \in Z(G)$

center (elementi, ki komutirajo z vsemi)

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

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

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

$\mathrm{Out}\, G = \dfrac{\mathrm{Aut}\, G}{\mathrm{Inn}\, G}$ ... grupa zunanjih avtomorfizmov (niso dejanski avtomorfizmi)

Kvocientni kolobarji in algebre

K naj bo kolobar

Pozabimo na množenje

K za seštevanje je abelova grupa

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

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

na K/I bi radi vpeljali množenje

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

ali to deluje?

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

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

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

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

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

Opomba:

① Pogoj b) lahko pišemo v obliki: $KI \subseteq I$

Prav tako pogoj c) $IK \subseteq I$

② Če I zadošča pogojema a) in b) pravimo da je I levi ideal

če iz zadošča a) in c) je desni ideal

Včasih idealom rečemo obojestranski ideal

Zgledi:

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

Kolobarjem ki imajo le ta dva ideala pravimo enostavni kolobarji

K kolobar

I je <u>ideal</u> v K, če

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

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

Zgledi:

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

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

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

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

K nekomutativen: Najmanjši Ideal, ki vsebuje a

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

Ideal v $\mathbb{Z}$:

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

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

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

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

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

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

Ideal: I_2, namesto I_1 podprostor v A-ju

Trdimo $I_1 + I_2 \Rightarrow$ podprostor v A

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

$$\alpha a = \alpha(1 \cdot a) = \underbrace{(\alpha \cdot 1)}_{\in A} \cdot \underbrace{a}_{\in I} \in I$$

Namesto podprostor lahko rečemo abelova podgrupa

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

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

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

je kolobar. Pravimo mu kvocientni (faktorski) kolobar.

Dokaz:

+ je dobro definirano (vemo iz grup)

$\cdot$ je dobro definirano

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

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

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

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

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

Lastnosti kolobarja izhajajo iz tega da je K kolobar.

Ničla v K/I: $0+I$

enica v 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. $x \in K$ poljuben

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

Torej $K = I$

Opomba: V prejšnji trditvi je dovolj da je I levi (ali desni) ideal

Trditev: Naj bosta I, J ideala v K

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

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

c) $I + J$ je ideal

Dokaz:

a) DN

b) • IJ je očitno podgrupa za seštevanje

• $\sum x_i y_i \quad x_i \in I \quad y_i \in J$

$$x \in K \qquad x \sum x_i y_i = \sum \underbrace{(x x_i)}_{\in I} \underbrace{y_i}_{\in J} \in I \cdot J$$

Izrek: (1. izrek o izomorfizmu)

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

Dokaz:

$\ker\varphi \triangleleft K$

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

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

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

Podobno xa

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

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

je dobro definiran izomorfizem kolobarjev

$\blacksquare$

Izrek: (2. izrek o izomorfizmu)

Naj bosta I in J ideala v K. Potem je

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

Izrek: (3 izrek o izomorfizmu)

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

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

Izrek: (Korespondenčni izrek)

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

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

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

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

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

Opomba: Komutativnost je nujna:

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

Dokaz:

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

$a+M \neq 0+M$

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

$M \subsetneq M+aK \subseteq K$

Zaradi maksimalnosti je $M+aK = K$

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

$1 - ak \in M$

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

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

($\Leftarrow$)

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

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

$a+M \neq 0+M$

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

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

$$ax - 1 \in M \Rightarrow \underbrace{ax}_{\in I} - 1 \in I$$

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

$\blacksquare$

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

Dokaz uporabi Zornova lemo:

X naj bo delno urejena množica

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

Zgornja meja neke podmnožice Y:

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

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

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

---

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

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

$\mathcal{S} \neq 0$, ker $I \in \mathcal{S}$

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

Vzemimo poljubno verigo $\mathcal{V}$ v $\mathcal{S}$

$U = \bigcup_{J \in \mathcal{V}} J$ Trdimo $U \in \mathcal{S}$

U je ideal v K

- $a, b \in U$. $\exists J_1, J_2 \in \mathcal{V}$. $a \in J_1$, $b \in J_2$

  BŠZS. $J_1 \subseteq J_2$ (ker je $\mathcal{V}$ veriga)

  $a - b \in J_2 \subseteq U$

- $a \in U$, $x \in K$, $\exists J \in \mathcal{V}$. $a \in J$

  $ax, xa \in J \subseteq U$

- $U \neq K$

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

  $\divideontimes$

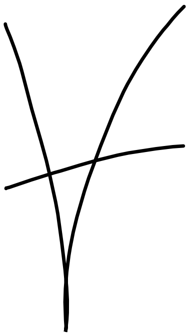
Po zornovi lemi $\mathcal{S}$ vsebuje maksimalen element M

$M \triangleleft K$ $M \neq K$ $I \subseteq M$

M je maksimalen ideal v K

Recimo $\exists N \triangleleft K$. $M \subsetneq N \subsetneq K$. N je pravi ideal v K, ki vsebuje I, torej $N \in \mathcal{S}$ $\divideontimes$

Zapiski od Urške na discordu



Od zadnjič

$|G| = mn$ m, n sta si tuji:

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

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

$G = H + K$

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

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

~~dmx~~ $m(bnx) = b\underbrace{mn}_{|G|}x = 0$

$\Rightarrow bnx \in H$

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

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

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

Ker sta m in n tuji je dovolj premisliti

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

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

Po Cauchyjevem izreku grupa H vsebuje element y reda p

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

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

$cm + dp = 1$

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

$\times$

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

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

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

Edina abelova grupa moči 6

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

Opomba: $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \not\cong \mathbb{Z}_4$, ker ima $\mathbb{Z}_4$ element reda 4 $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ pa ne

Posledica: Naj bo G končna abelova

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

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

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

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

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

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

Dovolj je torej obravnavati končne abelove p-grupe

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

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

Dokaz: $|G| = p^m$

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

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

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

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

$(\Longleftarrow)$ indukcija po moči

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

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

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

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

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

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

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

Oglejmo si

$\varphi: G \longrightarrow G$

$\varphi(x) = px$

φ je homomorfizem grup

$\ker \varphi = N$

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

G/N je p-grupa netrivialne

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

Po indukcijski predpostavki je G/N ciklična

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

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

$x - ka \in N$

$\cancel{k} \in N \quad x = ka+n \quad n \in N$

$G = \langle a \rangle + N$

$\langle a \rangle$ je netrivialna ciklična p-grupa

to ej $\langle a \rangle$ vsebuje element reda p ;

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

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

$\Rightarrow G = \langle a \rangle$ ■

Lema: Naj bo G končna abelova p-grupa. Naj bo C tista ciklična podgrupa v G, ki ima največjo možno moč.
Potem $\exists$ podgrupa $K \leq G$, da je
$G = C \oplus K$

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

Recimo da G ni ciklična. $|G| = p^m$ $m \geq n$
Indukcija po moči $|G|$

Po prejšnji lemi ima G vsaj dve podgrupi moči p
C ima po prejšnji lemi natanko eno podgrupo moči p
Zato $\exists$ podgrupa moči p v G ki ni vsebovana v C. označimo jo z N

Opazimo $C \cap N < N$ $\quad |N| = p$
Torej $C \cap N = \{0\}$

2. izrek o izomorfizmu:

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

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

$\frac{C+N}{N}$ je ciklična podgrupa v G/N
ima največjo moč med cikličnimi podgrupami grupe G/N in ima največjo moč med cikličnimi

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

Po indukcijski predpostavki $\exists K \leq G$
$N \subseteq K$ da je

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

$G = C \oplus K$

iz $*$ sledi
$x \in G$: $x + N \in G/N$

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

$G = C + \underset{\underset{K}{\cap}}{N} + K \Rightarrow$ ~~C+K~~ $G = C + K$

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

$x \in C \cap K$ $\quad x \neq 0$
$x \notin N$ ker $C \cap N = \{0\}$
$x + N \in \frac{C+N}{N} \cap \frac{K}{N} = \{0+N\}$, ker je to direktna vsota
$\Rightarrow x \in N$ $\quad$ ↯

Posledica: $\forall$ končna abelova p-grupa je direktna vsota cikličnih p-grup

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

Kako vidimo ali: dva razcepa abelovih grup na direktni vsoti cikličnih p_i-grup predstavljata isto grupo do izomorfizma natančno

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

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

$G = H_1 \oplus \dots \oplus H_k \qquad |H_i| = p_i^{e_i}$

$\bar{G} = \bar{H}_1 \oplus \dots \oplus \bar{H}_k \qquad |\bar{H}_i| = p_i^{e_i}$

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

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

$\varphi/_{H_1} : H_1 \longrightarrow \bar{H}_1$

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

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

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

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

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

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

predpostavimo

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

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

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

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

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

Po indukciji na r

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

Recimo da velja za vse grupe moči p^s $s<r$

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

ubistvu potenca

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

izpostavljamo lahko ker je abelova

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

$f(pg) = p(fg)$

$f/_{pG}$ je izomorfizem

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

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

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

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

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

pG sta izomorfni in imata manjšo moč kot G

Po indukcijski predpostavki dobimo

$m' = n'$

$k_i - 1 = l_i - 1$

$k_i = l_i$

Torej

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

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

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

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

$\Rightarrow n = m$

Torej je izrek dokazan

Torej vsako ~~abelovo~~ končno abelovo grupo

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

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

Zapis je enoličen do vrstnega reda direktnih sumandov natanko

Vse abelove grupe moči 4032

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

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

5

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

3

Grup je 15

Na podoben način lahko gen.

lahke generirane
končno generirane ciklične
abelove grupe

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

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

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

$(\mathbb{Z}^n = \overbrace{\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}}^{n})$

Ideja dokaza:
G abelova grupa $\quad \leftarrow$ končen red

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

$T(G)$ je podgrupa v G

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

$nh = 0$

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

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

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

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

$G = \langle x_1, \ldots x_n \rangle \Rightarrow G/T(G) = \langle x_1 + T(G), \ldots, x_n + T(G) \rangle$

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

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

$\Downarrow$

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

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

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

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

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

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

Brez dokaza

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

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

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

$$e_i = (0, \dots 0, \overset{i}{\downarrow}{1}, 0, \dots 0) \in \mathbb{Z}^n$$

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

$\alpha_1 e_1 + \dots + \alpha_n e_n$ $\mathbb{Z}^n$ ima bazo zato ima tudi $G/T(G)$ bazo

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

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

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

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

$$H \longrightarrow \mathbb{Z}_n$$
$$f_i \longrightarrow e_i \quad \text{je izomorfizem grup}$$

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

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

$G = H + T(G)$

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

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

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

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

~~Dokazali~~ ~~smo~~

Dokazati moramo še, da je

$T(G)$ končna grupa.

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

abelska ✓

$$T(G) \cong G/H$$

G/H je kvocient končnogenerirane grupe je končno generirana

$T(G)$ je končnogenerirana grupa v kateri ima $\forall$ element končen red

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

$t \in T(G)$

$t = \alpha_1 t_1 + \ldots + \alpha_k t_k$ (ni baza, amak vseeno lahko tako zapišemo (neenolično) ker je abelska

$0 \leq \alpha_i < m_i$

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

$\Rightarrow T(G)$ končna

KONČNE GRUPE

delovanja grup

Definicija: Naj bo G grupa in X neprazna množica. Grupa G <u>DELUJE</u> na množici X ($G \curvearrowright X$), če $\exists$ preslikava (<u>DELOVANJE</u>)

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

za katero veljata:

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

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

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

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

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

2') $x \cdot 1 = x$

Recimo da imamo levo delovanje $G \curvearrowright X$ $\quad (g,x) \longmapsto g \cdot x$

Potem lahko definiramo desno delovanje

$$X \times G \longrightarrow X$$

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

Zakaj: 1) velja

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

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

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

Opomba: Naj G deluje na X

$\mathrm{Sym}\, X = \{X \rightarrowtail\!\!\!\twoheadrightarrow X\}$

Delovanje porodi homomorfizem grup

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

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

Φ je homomorfizem

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

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

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

Obratno: Če imamo homomorfizem $\Phi : G \longrightarrow \mathrm{Sym}\, X$ potem $G \curvearrowright X$ s predpisom $g \cdot x = \Phi(g)(x)$

Opomba: Zakaj je $\varphi: X \longrightarrow X$, $\varphi(x) = g \cdot x$ bijekcija?

surj:

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

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

$$gx = gy$$

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

Recimo da imamo delovanje G na X

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

$\ker\Phi$ imenujemo jedro delovanja

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

Če je delovanje zvesto:

$$\begin{array}{c} G/\ker\Phi \cong \mathrm{im}\,\Phi \\ \cong \\ G \end{array}$$

G je izomorfna neki podgrupi $\mathrm{Sym}\,X$

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

Primeri delovanj

1) Trivialno delovanje

$$g \cdot x = x \quad \text{za} \ \forall g \in G. \ \forall x \in X$$

2) Grupa G deluje na G z levim množenjem

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

imamo homomorfizem

$$\Phi : G \longrightarrow \operatorname{Sym} G$$
$$\Phi(g)(h) = g \cdot h$$

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

$$\Leftrightarrow g = 1$$

levo regularno delovanje

Cayleyjev izrek:
Množenje z leve je torej zvesto delovanje

$\Rightarrow \forall$ grupa G se vloži v $\operatorname{Sym} G$

V posebnem: G končna. $|G| = n$

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

3) G deluje na G

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

DN: To je delovanje

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

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

G deluje na G/H

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

Dobra definiranost ?

Recimo $xH = yH \Rightarrow gxH = gyH$!

$\downarrow$

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

Oglejmo si $(gx)^{-1} gy = x^{-1} g^{-1} g y = \underbrace{x^{-1} y}_{\in H}$

DN: To je delovanje

5) Recimo da G deluje na X

Y naj bo neprazna množica

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

G deluje na Y^X

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

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

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

To ni res delovanje

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

$$(g(hf))(x) = hf(g^{-1}x) =$$

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

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

$(g, x) \longrightarrow gx \quad (g, y) \longmapsto gy$

Potem $G \curvearrowright Y^X$

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

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

6) V nejbo vektorski prostor

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

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

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

To je delovanje

7) K komutativen kolobar z 1

$K[x_1, \dots, x_n]$

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

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

To je delovanje

Orbite, stabilizatorji, fiksne točke delovanj

Def: Naj grupa G deluje na množici X

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

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

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

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

$$X^g = \{ x \in X;\ gx = x \} = \mathrm{fix}(g)$$

4) fiksne točke delovanja (invariante)

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

Lema: Naj G deluje na X

Recimo da $g \cdot x = y$

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

Dokaz:

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

Trditev: Naj G deluje na X

Potem je $G_x \leq G$

Dokaz:

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

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

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

$\blacksquare$

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

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

Dokaz

Refleksivnost $1x = 1$

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

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

Ekvivalenčni razreda za

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

$$= Gx$$

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

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

X/G je prostor orbit

Delovanju, ki ima eno samo orbito pravimo <u>tranzitivno delovanje</u>

Zgled

1) Naj G deluje na G z levim množenjem

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

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

Tranzitivno delovanje

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

$$\Downarrow$$

$$g = 1$$

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

② G naj deluje na G s konjugiranjem

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

$x \in G$

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

..., centralizator elementa x v G

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

$$= \underbrace{\{gxg^{-1} : g \in G\}}_{} = Cl_G(x)$$

konjugirani razred elementa x v G

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

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

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

Orbita xH

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

tranzitivno delovanje

Fiksne točke (invariante) delovanja

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

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

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

simetrični polinomi

$x_1 + x_2 + x_3$

$x_1 x_2 + x_2 x_3 + x_1 x_3$

Izrek o orbiti in stabilizatorju

Naj grupa G deluje na množici X

orbita — indeks stabilizatorja

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

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

Dokaz:

a) Iščemo bijekcijo med množicama Gx in G/G_x

$\alpha : Gx \longrightarrow G/G_x$

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

Ali je α dobro definirana

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

$gx = hx$

$h^{-1}gx = x$

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

$\Rightarrow hG_x = gG_x$

α očitno surjektivna

α injektivna

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

$h^{-1}gx = x$

$gx = hx$ ✓

∎

b) direktna posledica

Izrek

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

čisti x_i ki jih vsi g_j pustijo pri miru

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

Dokaz: Množica X je disjunktna unija nekih orbit delovanja.

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

vsaka fiksna točka ima enoelementno orbito

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

recimo da jih je r (ker je G končna)

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

orbite z 1 elementom

vse ostale orbite

x_i ji so predstavniki različnih orbit velikosti več kot 1

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

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

Posledica:

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

Potem velja

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

Dokaz:

Po prejšnjem izreku lahko napišemo

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

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

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

je deljiv s p

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

$\blacksquare$

Izrek (Burnsidova lema)

Naj končna grupa G deluje na končno množico

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

Dokaz: Izračunamo moč množice

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

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

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

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

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

orbite

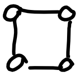
$$= |G|\cdot\sum_{\sigma\in X/G}1 = |G|\cdot|X/G|$$

drugi način

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

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

Primer:

 barvamo oglišča z n barvami

 je isto barvanje

št barvanj glede na to identifikacijo

X.... množica vseh barv □ z n barvami

$|X| = n^4$

r...rotacija za 90°

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

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

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

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

$= |X| = n^4$

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

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

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

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

Razredna formula in Cauchyjev izrek

Posledica: Razredna formula

Naj bo G končna grupa

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

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

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

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

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

$\blacksquare$

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

Dokaz: BŠZS G ni abelova

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

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

$C_G(x_i) \neq G$, ker potem bi x_i bil v centru

Zato $\quad p \,\big|\, |G : C_G(x_i)|$

Torej mora biti $\quad p \,\big|\, |Z(G)|$

$\blacksquare$

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

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

$|G/Z(G)| = p$ torej je ciklična

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

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

Vzemimo $a, b \in G$

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

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

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

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

$= x^j z_2 x^i z_1 = ba$ $\quad$ ker sta potenci istega elementa

torej je G abelova $\blacksquare$

Izrek (Cauchyjev izrek)

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

Dokaz:

Za abelove grupe smo izrek že dokazali.

Indukcija po $|G|$

$|G| = p$: je ciklična torej ✓

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

BŠZS G ni abelova. Uporabimo razredno formulo

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

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

$\Downarrow$ Abelova grupa

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

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

Po razredni formuli

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

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

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

A_4 nima podgrupe moči 6 :(

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

Def: Naj bo G končna grupa, $H \leq G$.
Pravimo da je H p-podgrupa Sylowa v G, če je

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

(Največja podgrupa praštevila pa moči)

Izrek Sylowa:

Naj bo G končna grupa $p \mid |G|$

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

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

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

d) Naj bo n_p število p-podgrup sylowa v grupi G. Potem veljata dve zvezi

i) $n_p \mid |G|$

ii) $n_p \equiv 1 \mod p$

Dokaz:

a) z indukcijo po moči $n = |G|$

$n = p$ očitno

Recimo da trditev za vse grupe moči $< n$

Dokazujemo za grupe moči n

Ločimo dve možnosti:

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

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

Oglejmo si G/Z

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

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

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

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

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

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

$x_i \in G - Z(G)$

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

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

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

(ker x_i ni v centru)

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

b) Dokaz

Pomožen rezultat od zadnjič:

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

Potem $|X| \equiv |X^G| \bmod p$ $\quad (*)$

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

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

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

$H \curvearrowright X$ z levim množenjem

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

Po $(*)$ $|X| \equiv |X^H| \bmod p$

$|X| = |G/S| = \dfrac{|G|}{|S|}$ $\quad$ zaradi maksimalnosti S ja $|X|$ ni deljivo s p

potem $\quad X^H \neq \emptyset$

$\exists xS \in X^H$

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

$x^{-1}axS = S$

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

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

$H \subseteq xSx^{-1}$

$xSx^{-1} \leq G$

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

zato je xSx^{-1} tudi p-podgrupa Sylowa

ki vsebuje H

c) Dokaz

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-podgrupi Sylova v G, torej

imata isto moč. Zato $H = xSx^{-1}$

d) Dokaz

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

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

$n_p = |X|$

G naj deluje na X s konjugiranjem

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

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

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

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

(normalizator S v G)

Izrek o orbiti in stabilizatorju:

moč orbite S = 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

Po $\ast$ $\underbrace{|X|}_{n_p} \equiv |X^S| \mod p$

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

Gotovo velja $S \in X^S$

Naj bo $T \in X^S$

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

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

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

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

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

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

Dobimo $n_p \equiv 1 \mod p$

Opomba:

Iz dokaza sledi

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

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

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

"edina p-podgrupa sylowa je edinka"

Primer:

p, q različni praštevili $p < q$

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

$|G| = p \cdot q$

V G obstaja vsaj ena p-podgrupa Sylowa

P. $|P| = p$

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

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

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

(ker če bi bil p $p \equiv 1 \mod q$ ampak $p < q$

Torej Q je edina q-podgrupa Sylowa

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

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

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

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

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

$PQ = G$

Glede n_p imamo dve možnosti:

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

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

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

2) $n_p = q$

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

Ena 3-podgrupa Sylowa:

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

imamo 3 2-podgrupe Sylowa

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

DN vse grupe moči 77

Končne enostavne grupe

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

Kako zgledajo končne enostavne grupe?

Primer: G končna abelova grupa. Kdaj je enostavna

$\Vert$

Abelova grupa z natanko dvema podgrupama

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

Primer:

$A_n \leqslant S_n \quad |S_n : A_n| = 2 \Rightarrow A_n$ je edinka

$A_3 \cong Z_3$ enostavna

A_4 ni enostavna

$N = \langle (1\,2)(3,4), (1\,3)(2\,4) \rangle \cong \underbrace{\mathbb{Z}_2 \oplus \mathbb{Z}_2}_{\text{Kleinova četverka}}$

DN:

$\forall \pi \in A_n. \quad \pi (1\,2)(3\,4) \pi^{-1} \in N$

$\pi (1\,3)(2\,4) \pi^{-1} \in N$

Izrek:
Če je $n \geq 5$ je A_n enostavna

Dokaz: $N \triangleleft A_n$. $N \neq \{1\}$

Dokazujemo da je $N = A_n$

(1) Recimo da N vsebuje vsaj en tricikel

BŠZS. $(1\,2\,3) \in N$

Vzemimo permutacijo

$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ a & b & c & \dots & * \end{pmatrix}$ naj bo soda permutacija

$\sigma(1\,2\,3)\sigma^{-1} \in N$
$= (a\,b\,c)$

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

A_n je generirana z vsemi 3-cikli

Torej $N = A_n$

(2) N ne vsebuje nobenega 3-cikla

Ločimo še več primerov

2.1 Recimo da N vsebuje π katere razcep na disjunktne cikle vsebuje cikel dolžine ≥ 4

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

Potem je

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

$\pi' = (a_2\,a_3\,a_1\,a_4 \dots)(\dots)\dots(\dots)$

Potem je $\pi'\pi^{-1} \in N$

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

N vsebuje torej 3-cikel $\times$

(2.2) N ne vsebuje nobene permutacije katere razcep na disjunktne cikle bi vseboval cikel dolžine ≥ 4

(2.2.1) Recimo da imamo v N permutacijo oblike

$\pi = (a\,b\,c)(a'\,b'\,c')\dots$

Potem je tudi

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

$\pi' = (a\,b\,a')(c\,c'\,b')\dots$ kot v π

$\pi'\pi \in N$

$\pi'\pi = (a\,a'\,c\,b\,c')$ Torej je cikel dolžine več kot 4 $\times$

(2.2.2) Recimo da je v N permutacija oblike

$\pi = (a\,b\,c)\dots$ s sodo število transpozicij

$\pi^2 \in N$

$\pi^2 = (a\,b\,c)^2 = (a\,c\,b)$ $\times$

(2.2.3) ostane še primer ko so vsi elementi N produkt sodega števila transpozicij

Ločimo dve možnosti

(2.2.3.1) Recimo da je $(a,b)(a'\,b') \in N$

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

opazimo:

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

(2.2.3.2) $\forall$ element N je produkt ≥ 4 disjunktnih transpozicij

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

Potem je $\pi' = (a_3\,b_2)(a_2\,b_1)\,\pi\,(a_2\,b_1)(a_3\,b_2)$ $\in N$

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

$\pi'\pi \in N$

$\pi'\pi = (a_1\,a_3\,b_2)\dots$ $\times$

Izkaže se: (klasifikacija končnih enostavnih grup)
če je G končna enostavna grupa, potem sodi v eno od naslednjih kategorij:

1) $\mathbb{Z}_p$, $p \in \mathbb{P}$
2) A_n $n \geq 5$
3) grupe Lijevega tipa
npr: $SL_n(F)$
$$Z(SL_n(F)) = \{\lambda I ; \lambda^n = 1$$
$$PSL_n(F) = SL_n(F) / Z(SL_n(F))$$ ... projektivna
je enostavna
(za skoraj vse n)

4) 26 sporadičnih grup
Največja med njimi je POŠAST
Moonshine theory povezana s to grupo

Zakaj so enostavne grupe $\sum\sum$?

sigma sigma

G končna grupa

Če G ni enostavna, potem $\exists M \underset{\neq}{\triangleleft} G$ ki ni vsebovana v nobeni večji edinki (maksimalna edinka)

G/M je enostavna grupa

Postopek nadaljujemo

$$G \triangleright M \triangleright M_1 \triangleright \ldots \triangleright M_k \triangleright \{1\}$$

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

To je kompozicijska vrsta grupe

M_k poznamo in M_{k-1}/M_k tudi poznamo

teorija razširitev

$\rightarrow$ vse možnosti za M_{k-1}

Rešljive grupe

Grupa G je <u>rešljiva</u>, če obstaja končno zaporedje podgrup
$$\{1\} = G_0 \triangleleft G_1 \triangleleft G_2 \triangleleft \dots \triangleleft G_k$$
Vsaka je edinka večji
za katera velja: G_{i+1}/G_i je abelova

Primeri:

1) Abelove so vse rešljive: $\{1\} \triangleleft G$

2) $A_4 \triangleright \langle (12)(34), (13)(2,4) \rangle \triangleright \{1\}$

kvocient ima moč 3 torej je abelova

$\mathbb{Z}_2 \oplus \mathbb{Z}_2$

kvocient je tudi abelova

3) $S_4 \triangleright A_4 \triangleright \langle (12)(34), (13)(24) \rangle \triangleright \{1\}$

4) G je nekomutativna enostavna grupa

$A_n \geq 5$ niso rešljive

Trditev: Naj bo G rešljiva

1) $H \leq G$ je tudi rešljiva

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

Dokaz:

imamo $\{1\} = G_0 \trianglelefteq \dots \trianglelefteq G_k = G$

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

1) Oglejmo si:

$\{1\} = G_0 \cap H \trianglelefteq \dots \dots \trianglelefteq G_k \cap H$

očitno edinke

$$\frac{G_{i+1} \cap H}{G_i \cap H} = \frac{G_{i+1} \cap H}{(G_{i+1} \cap G_i) \cap H} \cong$$

$$\cong \frac{(G_{i+1} \cap H) G_i}{G_i} \leq \frac{G_{i+1}}{G_i}$$

abelova

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

$\frac{G_{i+1} \cap H}{G_i \cap H}$ podgrupa abelove je abelova

2) $$\frac{\frac{G_{i+1} N}{N}}{\frac{G_i N}{N}} \cong \frac{G_{i+1} N}{G_i N} = \frac{G_{i+1} G_i N}{G_i N} \cong$$

$$\cong \frac{G_{i+1}}{G_{i+1} \cap G_i N} \cong \frac{\left(\frac{G_{i+1}}{G_i}\right)}{\frac{G_{i+1} \cap G_i N}{G_i}}$$

abelova

kvocient abelove je abelova

Trditev:

Naj bo G grupa in $N \triangleleft G$

Če sta N in G/N rešljivi

je tudi G rešljiva

Dokaz: $\{1\} \triangleleft N_0 \triangleleft \dots \triangleleft N_k = N$

N_{i+1}/N_i abelova

$$\{1\} = \frac{M_0}{N} \Rightarrow M_0 = N$$

$$\frac{M_0}{N} \triangleleft \frac{M_1}{N} \triangleleft \dots \triangleleft \frac{M_\ell}{N} = \frac{G}{N}, \quad M_\ell = G$$

$$\text{abelova } \frac{M_{i+1}/N}{M_i/N} \cong \frac{M_{i+1}}{M_i} \text{ je abelova}$$

Vrsta za G

$$\{1\} \triangleleft N_0 \triangleleft \dots \triangleleft N_k = M_0 \triangleleft M_1 \triangleleft \dots \triangleleft M_\ell = G$$

$\blacksquare$

Opomba: Izkaže se da so vse grupe lihe moči rešljive

(Feit-Thompsonov izrek)

DN. G je končna p-grupa potem je rešljiva

Nasvet $Z(G) \neq \{1\}$. Indukcija po $|G|$

Kolabarji polinomov

(nad polji)

$\mathbb{F}$ bo vedno polje

Pravimo da je $p(x)$ stopnje n ko

$p(x) = a_n x^n + \dots + a_0 \quad a_n \neq 0$

Stopnja ničelnega polinoma je $-\infty$

Opazimo:

$st(p(x) \cdot g(x)) = st(p(x)) + st(g(x))$

(ker produkt dveh neničelnih ni neničeln)

ker je $\mathbb{F}$ polje

Opomba: $\mathbb{Z}_4[x]$

$p(x) = 2x^2 + 1$

$g(x) = 2x^3 + 1$

$st(p(x) \cdot g(x)) = 3 \neq st(p(x)) + st(g(x))$

Posledica:

Kolobar $F[x]$ je brez deliteljev niča

Obrnljivi elementi $F[x]$ so natanko neničelni konstantni polinomi

Dokaz: sledi iz formule za $st(p(x) \cdot g(x))$

Izrek: Osnovni izrek o deljenju polinomov

Za poljubna polinoma $f(x)$ in $g(x)$ iz $\mathbb{F}[x]$, $g(x) \neq 0$, obstajata enolično določena polinoma $k(x)$ in $r(x)$ da je

$$f(x) = k(x) \cdot g(x) + r(x)$$

$$st(r(x)) < st(g(x))$$

Dokaz: $f(x) = a_m x^m + \ldots + a_0 \quad ; a_m \neq 0$

(BŠZS $f(x) \neq 0$)

$g(x) = b_n x^n + \ldots + b_0 \quad ; b_n \neq 0$

Indukcija po m

(BŠZS $m \geq n$ (če $m < n$, potem $k(x) = 0$ in $r(x) = f(x)$))

Baza indukcije: $m = 0$

$$a_0 = (a_0 b_0)^{-1} \cdot b_0 + 0 \quad \text{(ker smo v } \mathbb{F})$$

Recimo da velja za vse polinome stopnje $< m$

$$a_m \cdot b_n^{-1} x^{m-n} \cdot g(x) = a_m x^m + \ldots$$

$f(x) - a_m b_n^{-1} x^{m-n} \cdot g(x)$ polinom stopnje $< m$

$$f(x) - a_m b_n^{-1} x^{m-n} \cdot g(x) = k_1(x) \cdot g(x) + r(x)$$

$$f(x) = (\underbrace{k_1(x) + a_m b_n^{-1} x^{m-n}}_{k(x)}) g(x) + r(x)$$

enoličnost:

$$f(x) = k_1(x) g(x) + r_1(x) = k_2(x) g(x) + r_2(x)$$

$$st(r_1(x)) < st(g(x))$$

$$st(r_2(x)) < st(g(x))$$

$$(k_1(x) - k_2(x)) \cdot g(x) = r_2(x) - r_1(x)$$

Primerjamo stopnji:

$$st(r_2(x) - r_1(x)) < st\, g(x)$$

$st((k_1(x) - k_2(x)) \cdot g(x)) \geq st(g(x))$ če $k_1 - k_2 \neq 0$

Torej $\Rightarrow k_1 = k_2 \Rightarrow r_2 = r_1$

Posledica: $\forall$ ideal v kolobarju $\mathbb{F}[x]$ je glavni (generiran z enim elementom)

($I = (a)$ $\quad I = \{ka \,;\, k \in K\}$ ker je K komutativen)

Dokaz:

$I \triangleleft F[x]$ poljuben ideal

$I = \{0\} \Rightarrow I = (0)$

$I = \mathbb{F}[x] \Rightarrow I = (1)$

$I \notin \{\{0\}, \mathbb{F}[x]\}$

V I lahko najdemo neničeln polinom $p(x)$ najnižje možne stopnje

Trdimo $I = (p(x))$

Vzemimo poljuben $f(x) \in I$

$$\underbrace{f(x)}_{\in I} = \underbrace{k(x) \cdot p(x)}_{\in I} + r(x) \Longrightarrow r(x) \in I$$

$$st(r(x)) < st(p(x))$$

$$\Rightarrow r(x) = 0 \Rightarrow$$

$$f(x) = k(x) \cdot p(x)$$

Če $p(x) \in \mathbb{F}[x]$ $\quad a \in \mathbb{F}$ $\quad p(x) = \sum^{n} a_j x^j$

$$p(a) = \sum^{n} a_j a^j \in \mathbb{F}$$

a je ničla polinoma $p(x)$, če je $p(a) = 0$

Opomba: $p(x)$..... abstraktna vsota potenc x^j

Polinom lahko gledamo kot $p: \mathbb{F} \to \mathbb{F}$
$a \mapsto p(a)$

(polinomske funkcija)

Polinomov ne moremo identificirati s polinomskimi funkcijami:

$\mathbb{Z}_2[x]$

$p(x) = 0 \quad g(x) = x^{2025} + x$

različna polinoma

$p: \mathbb{Z}_2 \to \mathbb{Z}_2$
$0 \mapsto 0$
$1 \mapsto 0$

$g: \mathbb{Z}_2 \to \mathbb{Z}_2$
$0 \mapsto 0$
$1 \mapsto 0$

Trditev: $p(x) \in \mathbb{F}[x]$ $a \in \mathbb{F}$

a je ničla polinoma p $\Leftrightarrow$ polinom $(x-a)$ deli $p(x)$

Dokaz: $p(x) = k(x) \cdot (x-a) + r(x)$ ← konstanta

a ničla $p(x)$

$p(a) = k(a) \cdot 0 + r = 0$

$\Longleftrightarrow r = 0$

$\blacksquare$

Posledica:

$p(x) \in \mathbb{F}[x]$ neničeln

potem je v $\mathbb{F}$ kvečjemu $st(p(x))$ ničel polinoma

Dokaz: indukcija po stopnji

nerazcepni polinomi

Def: Naj bo $p(x) \in \mathbb{F}[X]$ stopnje ≥ 1

Pravimo da je $p(x)$ nerazcepen nad $\mathbb{F}$, če

iz enakosti $p(x) = g(x)h(x)$, $g(x), h(x) \in \mathbb{F}[X]$

sledi da je eden od $g(x)$ in $h(x)$ konstanten

Primer:

$\mathbb{C}[X]$ nerazcepni polinomi so natanko

linearni polinomi

$\mathbb{R}[X]$ linearni polinomi in kvadratni polinomi

brez ničel

Trditev:

Naj bo $p(x) \in \mathbb{F}[x]$ stopnje ≥ 1

a) Če $st(p(x)) = 1 \Rightarrow p(x)$ je nerazcepen

b) Če je $st\, p(x) \geq 2$ in je $p(x)$ nerazcepen, potem $p(x)$ nima ničle v $\mathbb{F}$

c) Če je $st(p(x)) = 2 \vee st(p(x)) = 3 \Rightarrow$

$p(x)$ je nerazcepen nad $\mathbb{F} \Leftrightarrow$

$p(x)$ nima ničle v $\mathbb{F}$

Od tudelje gledamo $\mathbb{Q}[X]$

$p(X) \in \mathbb{Q}[X]$

Če $p(X)$ pomnožimo s skupnim menovalcem koeficientov dobimo polinom v $\mathbb{Z}[X]$

Def: $p(X) = a_n X^n + \dots + a_0 \in \mathbb{Z}[X]$ je <u>primitiven polinom</u> če so $a_0, a_1, \dots, a_n$ tuja cela števila

Trditev: (Gaussova lema)
Produkt dveh primitivnih polinomov je spet primitiven polinom

Dokaz:
Naj bost $p(x), g(x) \in \mathbb{Z}[x]$ primitivna
Recimo da $p(x) \cdot g(x)$ ni primitiven
zato obstaja neko praštevilo p, ki deli vse koeficiente polinoma $p(x) \cdot g(x)$

$p(x) \cdot g(x) \in p \cdot \mathbb{Z}[x] \triangleleft \mathbb{Z}[x]$

kaj je $\mathbb{Z}[x] / p\mathbb{Z}[x] \cong \mathbb{Z}_p[x]$

$$\varphi : \mathbb{Z}[x] \longrightarrow \mathbb{Z}_p[x]$$
$$\sum a_j x^j \longmapsto \sum (a_j + p\mathbb{Z}) x^j$$

je homomorfizem

je surjektiven

$\ker \varphi = p\mathbb{Z}[x]$

Torej $\mathbb{Z}[x] / p\mathbb{Z}[x] \cong \mathbb{Z}_p[x]$

$p(x)$ je primitiven $\Rightarrow p(x) \notin \ker \varphi$
$g(x)$ je primitiven $\Rightarrow g(x) \notin \ker \varphi$

$p(x) + p\mathbb{Z}[x]$ je neničeln element
$(p(x) + p\mathbb{Z}[x])(g(x) + p\mathbb{Z}[x]) =$
$p(x) \cdot g(x) + p\mathbb{Z}[x] = 0$

Torej $\mathbb{Z}[x] / p\mathbb{Z}[x]$ delitelje niča torej ima $\mathbb{Z}_p[x]$ delitelje niča

Ker je $\mathbb{Z}_p[x]$ p-če nima deliteljev niča $\times$

Izrek: Naj bo $f(x) \in \mathbb{Z}[x]$. Recimo da $f(x)$ ne moremo zapisati kot produkt dveh nekonstantnih polinomov v $\mathbb{Z}[x]$. Potem je $f(x)$ nerazcepen v $\mathbb{Q}[x]$

Dokaz:
Recimo da $f(x) = g(x) \cdot h(x)$ $g(x), h(x) \in \mathbb{Q}[x]$

Dokažemo: en od teh je konstanten

Znebimo se ulomkov:

k = skupni imenovalec koeficientov $g(x)$

l = skupni —||— od $h(x)$

$$k \cdot l \; f(x) = \underbrace{(k g(x))}_{\text{celi koeficienti}} \cdot \underbrace{(l \cdot h(f(x))}_{\in \mathbb{Z}[x]}$$

Dokaz (nezesay)

$f(x) \in \mathbb{Z}[x]$

recimo $f(x) = g(x) \cdot h(x)$ ← skupni imenovalec l

↑ skupni imenovalec k

$$klf(x) = kg(x) \cdot l \cdot h(x)$$

d ... največji skupni delitelj koeficientov $f(x)$

d_1 ... –||– za $kg(x)$

d_2 ... –||– za $lh(x)$

$$kl\, d f_0(x) = d_1 d_2 g_0(x) \cdot h_0(x)$$

primitivni

Po gaussovi lemi so $g_0(x) \cdot h_0(x)$ primitivni.

Največji skupni koef $kl\, d f_0(x) = kld$

–||– $d_1 d_2 g_0(x) h_0(x) = d_1 d_2$

Torej $d_1 d_2 = kld$

$f_0(x) = g_0(x) h_0(x)$

$f(x) = d f_0(x) = d g_0(x) h_0(x)$

Po predpostavki mora biti eden od polinomskih faktorjev konst

Izrek: (Eisenov kriterij)

Naj bo $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$

Naj bo p praštevilo, za katero velja:

i) $p \nmid a_n$

ii) $p \mid a_{n-1}, \dots, a_0$

iii) $p^2 \nmid a_0$

Potem je $f(x)$ nerazcepen nad $\mathbb{Q}[x]$

Dokaz:

Recimo da ton: res.

Po prejšnji trditvi obstajata nekonstantna polinoma $g(x), h(x) \in \mathbb{Z}[x]$ da je

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

$g(x) = b_r x^r + \dots + b_0$

$h(x) = c_s x^s + \dots + c_0$

Primerjamo koeficiente

$b_0 \cdot c_0 = a_0$

ker $p \mid a_0$ in $p^2 \nmid a_0 \Rightarrow p$ deli natanko enega od b_0, c_0. BSZS. $p \mid b_0$ $p \nmid c_0$

$a_n = b_r c_s$

ker $p \nmid a_n$ $p \nmid b_r, c_s$

Naj bo k najmanjši tak, da $p \mid b_0, \dots, b_{k-1}$ in p ne deli b_k $k \leq r$

$a_k = \underbrace{b_k \cdot c_0}_{\text{ni deljiv s } p} + \underbrace{b_{k-1} c_1 + \dots + b_0 c_k}_{\text{deljiv s } p}$

$k < n \Rightarrow p \mid a_k$

$\times$

$\blacksquare$

Primer:

p naj bo praštevilo

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \dots + x + 1 \in \mathbb{Z}[x]$$

Ta polinom ni razcepen nad $\mathbb{Q}$.

Eisensteinov kriterij ni uporaben. Ali pač?

Trik:

$$\Phi_p(x+1) = (x+1)^{p-1} + (x+1)^{p-2} + \dots + 1$$

Dovolj je pokazati da je $\Phi_p(x+1)$ nerazcepen

$$(x-1)\Phi_p(x) = x^p - 1 \qquad \text{premaknemo}$$

$$x\Phi_p(x+1) = (x+1)^p - 1$$

$$\Phi_p(x+1) = x^{p-1} + \binom{p}{1}x^{p-2} + \binom{p}{2}x^{p-3} + \dots + \binom{p}{p-2}x + \binom{p}{p-1}$$

$\binom{p}{1} \dots \binom{p}{p-1}$ so deljivi s p

1 ni deljiv s p

Po Eisensteinu je $\Phi_p(x+1)$ nerazcepen nad $\mathbb{Q}$, torej isto velja za $\Phi_p(x)$

Iz zveze $(x-1)\Phi_p(x) = x^p - 1$ vidimo

$$\Phi_p(x) = \prod_{k=1}^{p-1}(x - \omega_k)$$

$$\omega_k = \cos\frac{2k\pi}{p} + i\sin\frac{2k\pi}{p} = e^{i\frac{2k\pi}{p}}$$

$\hookrightarrow$ primitivni p-ti koreni enote

Za splošen n:

$$\Phi_n(x) = \prod (x - \omega_k)$$

$$\omega_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} = e^{i\frac{2k\pi}{n}}$$

kjer sta k in n tuja

Izkaže se $\Phi_n(x)$ so tudi celoštevilski polinomi in so tudi nerazcepni nad $\mathbb{Q}$

$\Phi_n(x)$.... ciklotomični polinom

Razširitve polj

Definicija. Naj bosta K in F polji. $F \leq K$.
Potem pravimo da je polje K razširitev polja F. Oznaka K/F

Zgledi:

$\mathbb{R}/\mathbb{Q}$ $\mathbb{R}$ je razširitev polja $\mathbb{Q}$

$\mathbb{C}/\mathbb{R}$, $\mathbb{C}/\mathbb{Q}$

$\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2};\ a,b \in \mathbb{Q}\}$ je polje

$\mathbb{Q}(\sqrt{2})/\mathbb{Q}$

Motivacija $\mathbb{R}/\mathbb{Q}$

Lepa iracionalna števila: $\sqrt{2}$

$\sqrt{2}$ je ničla polinoma $x^2 - 2 \in \mathbb{Q}[x]$

Grda iracionalna števila: π

π ni ničla nobenega neničelnega polinoma v $\mathbb{Q}[x]$

Def: Naj bo K/F razširitev poj. a∈K.

Pravimo:

a) a je algebraičen polinom $p(x) \in F[x]$ da je $p(a) = 0$

b) a je transcendenten nad F, če ni algebraičen nad F

Primer:

$\sqrt{2}$ je algebraičen nad $\mathbb{Q}$ in π je transcendenten nad $\mathbb{Q}$

Definicija: Naj bo K/F razširitev polj

$a \in K$ naj bo algebraičen nad F

Polinomu $p(x) \in F[X]$, ki ima vodilni koeficient 1 velja da je $p(a) = 0$ in je najmanjše stopnje med tistimi neničelnimi polinomi ki uničijo a pravimo minimalni polinom elementa a nad F

DN: minimalni polinom je enolično določen

Trditev:

Naj bo K/F razširitev polj, $a \in K$ naj bo algebraičen nad F. Naj bo $p(a)=0$. $p(x) \in F[x]$

Naslednje trditve so ekvivalentne:

i) $p(x)$ je minimalni polinom za a

ii) $p(x)$ je nerazcepen nad F

iii) $p(x)$ deli vsak polinom $f(x) \in F[x]$, za katerega je $f(a)=0$

Dokaz:

i) $\Rightarrow$ ii) Če je $p(x)$ razcepen:

$$p(x) = g(x) \cdot h(x) \qquad g(x), h(x) \in F[x]$$
nekonstantna

$$p(a) = g(a) \cdot h(a) = 0 \Rightarrow$$
$$h(a)=0 \lor g(a)=0$$

Če na primer $g(a)=0$ je $g(x)$ polinom, ki ima nižje stopnjo kot $p(x)$ in uniči a

$\times$

ii) $\Rightarrow$ iii)

$$I = \{ f(x) \in F[x] : f(a) = 0 \}$$

I ideal v $F[x]$. I je zato glavni ideal (ker je generiran z enim elementom)

$\exists p_1(x): I = (p_1(x)) = \{ k(x)\, p_1(x) : k(x) \in F[x] \}$

$p(x) \in I \Rightarrow p(x) = k(x) \cdot p_1(x) \qquad p_1(a) = 0$

Zaradi nerazcepnosti je $k(x)$ konstanten zato $I = (p(x))$

Sledi da je $\forall f(x) \in I$ večkratnik $p(x)$

iii) $\Rightarrow$ i)

Če $p(x)$ ni minimalen polinom $\exists g(x) \in F[x]$ neničelen, $st(g(x)) < st(p(x))$ in $g(a)=0$

Po predpostavki: $p(x) \mid g(x)$ $\times$ (stopnje

Def: K/F $a \in K$ naj bo alg nad F

$p(x)$ naj bo minimalen polinom a-ja nad F

če $st(p(x)) = n$ pravimo da je

<u>a algebraičen stopnje n</u>

Zgled:

① K/F alg. elementov stopnje 1 = ničle lin. polinoma

$x - a$ $a \in F$

To so natanko elementi F

② $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$

$\sqrt{2}$ je ničla $X^2 - 2 \in \mathbb{Q}[x]$

To je minimalni polinom

$\sqrt{2}$ je algebraičen stopnje 2 nad $\mathbb{Q}$

③ $\mathbb{C}/\mathbb{R}$

i je ničla polinoma X^2+1

i je algebraičen stopnje 2 nad $\mathbb{R}$

Splošneje: $\forall z \in \mathbb{C}$ je algebraičen nad $\mathbb{R}$

stopnje 1 ali 2

z je ničla $X^2 - (z+\bar{z})X + z\bar{z} \in \mathbb{R}[x]$

$= (X-z)(X-\bar{z})$

④ $\mathbb{R}/\mathbb{Q}$ $\sqrt{2}+\sqrt{3}$ algebraičen nad $\mathbb{R}$?

$a = \sqrt{2}+\sqrt{3}$

$a^2 = 5 + 2\sqrt{6}$ $/ \cdot 10$

$a^4 = 49 + 20\sqrt{6} +$

$a^4 - 10a^2 + 1 = 0$

$\sqrt{2}+\sqrt{3}$ je ničla polinoma $X^4 - 10X^2 - 1 \in \mathbb{Q}[X]$

DN: To je minimalni polinom $\sqrt{2}+\sqrt{3}$ nad $\mathbb{Q}$

Končne razširitve polj

K/F naj bo razširitev polj

V K imamo seštevanje

Če elemente iz $\mathbb{F}$ imenujemo skalarji in elemente K-ja vektorji imamo definirano množenje s skalarjem:

$$F \times K \longrightarrow K$$
$$(\alpha, k) \longmapsto \alpha k$$

K lahko gledamo kot vektorski prostor nad $\mathbb{F}$

Def: <u>razširitev polj</u> K/F je <u>končna</u>, če je K končnorazsežen vektorski prostor nad $\mathbb{F}$

Označ.:
$\dim_F K = [K:F]$ .... stopnja razširitve

Zgled:

- $\mathbb{C}/\mathbb{R}$:

  Baza $\mathbb{C}$ nad $\mathbb{R}$: $\{1, i\}$

  $[\mathbb{C}:\mathbb{R}] = 2$

- $[\mathbb{R}:\mathbb{Q}] = \infty$

  Recimo $[\mathbb{R}:\mathbb{Q}] < \infty$

  $\{r_1, \dots, r_n\}$ baza $\mathbb{R}$ nad $\mathbb{Q}$

  $\forall r \in \mathbb{R} \quad r = \underbrace{q_1 r_1 + \dots + q_n r_n}_{\text{samo števno neskončno možnosti}}$

Trditev:

$F \subseteq L \subseteq K$ naj bodo polja

Naj bosta L/F in K/L končni razširitvi, potem je K/F končna

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 vek. pr. nad L: $\{b_1 \dots b_n\}$

$B = \{a_i b_j \; ; i \in \{1 \dots m\}, j \in \{1 \dots n\}\}$ je 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

$\lambda_i = \varphi_{i1} a_1 + \dots + \varphi_{im} a_m \quad \varphi_{ij} \in F$

$k = \varphi_{11} a_1 b_1 + \varphi_{12} a_2 b_1 + \dots + \dots \varphi_{nm} a_m b_n$

linearna neodvisnost:

$\sum \sum \varphi_{ij} a_j b_i = 0 \quad \varphi_{ij} \in F$

$\sum (\underbrace{\sum \varphi_{ij} a_j}_{\in L}) b_i = 0$

$\Rightarrow \sum \varphi_{ij} a_j = 0 \Rightarrow \varphi_{ij} = 0$ za $\forall ij$

Def: Razširitev K nad F je algebraična, če je $\forall a \in K$. algebraičen nad K (je rešitev neke polinomske enačbe) in transcendentna če ni algebraična

Trditev: Vsaka končna razširitev K/F je algebraična

Dokaz: Recimo da $a \in K$ ni algebraična nad F
$1, a, a^2, \ldots$ so linearno neodvisni nad F
$\times$ ker je dim K/F končna

$\blacksquare$

Oznaka: K/F $a \in K$

$F[a]$ = najmanjši podkolobar v K, ki vsebuje F in a = podkolobar v K generiran z F in a

$$F[a] = \{p(a);\ p(x) \in F[x]\}$$

$F(a)$ = podpolje v K generirano z F in a

$$F(a) = \{xy^{-1};\ x \in F[a],\ y \in F[a] - \{0\}\}$$

Podobno lahko definiramo

$$F[a_1 \ldots a_n],\ F(a_1 \ldots a_n)$$

$$F[a_1 \ldots a_n] = F[a_1 \ldots a_{n-1}][a_n]$$

Def: Razširitev K/F je primitivna,
če $\exists a \in K$. da je $K = F(a)$

Zgled: $\mathbb{Q}[\sqrt{2}] = \{\alpha + \beta\sqrt{2} ; \alpha, \beta \in \mathbb{R}\}$

$\mathbb{Q}(\sqrt{2}) [\alpha + \beta\sqrt{2} ; \alpha, \beta \in \mathbb{R}\} = \mathbb{Q}[\sqrt{2}]$

Isto je, ker je $\sqrt{2}$ algebraičen

Izrek: Naj bo K/F razširitev polj in naj bo $a \in K$ algebraičen nad F stopnje n. Potem je $F(a) = F[a]$ in velja $[F(a) : F] = n$

Dokaz:

Naj bo $p(x) \in F[X]$ minimalni polinom a-ja $st(p(x)) = n$

Dovolj je pokazati da je vsak neničeln element v $F[a]$ obrnljiv

$f(a) \neq 0 \quad f(x) \in F[X]$

Zaradi minimalnosti $p(x)$ sledi da sta $f(x)$ in $p(x)$ tuja polinoma

Zato obstajata polinoma $r(x)$ in $s(x)$ v $F[x]$ da

$$f(x) r(x) + p(x) \cdot s(x) = 1$$

(iz razširjenega euklidovega algoritma)

Izračunamo v a:

$$f(a) \cdot r(a) = 1$$

$r(a)$ je inverz $f(a)$-ja

še drugi del:

$$F(a) = \{ f(a) : f \in F[X] \}$$

$p(a) = 0$

$p(x) = x^n + \alpha_{n-1} x^{n-1} + \dots \alpha_1 x + \alpha_0$

a^n je linearna kombinacija $1, a, a^2, \dots a^{n-1}$

$m \geq n \Rightarrow a^m$ tudi lin. kombinacija $1, a \dots a^{n-1}$

$1, a, a^2 \dots a^{n-1}$ je ogrodje $F(a)$ nad F

Zaradi minimalnosti $p(x)$ so

$1, a, \dots, a^{n-1}$ lin. neodvisni

Torej $\dim_F F(a) = n$ $\blacksquare$

Posledica:

Če K/F in $a_1, \dots, a_n \in K$ naj bodo algebraični nad F. Potem velja

$F(a_1 \dots a_n) = F[a_1 \dots a_n]$ in velja

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

Zgledi:

1) $\mathbb{Q}(\sqrt[n]{p})$ $p \in \mathbb{P}$

Polinom z racionalnimi koeficienti ki uniči $\sqrt[n]{p}$: $X^n - p$

Po eisensteinovem kriteriju je ta polinom nerazcepen nad $\mathbb{Q}$, zato je minimalni polinom $\sqrt[n]{p}$ nad $\mathbb{Q}$

Zato je stopnja te razširitve $= n$

2) K/F $a \in K$

$$\mathrm{eval}: F[X] \to F[a]$$
$$f(x) \mapsto f(a)$$

je surjektivna $\Rightarrow$ je epimorfizem kolobarjev

$\ker \mathrm{eval} = ?$

- Če je a transcendenten nad $F \Rightarrow \ker \mathrm{eval} = \{0\}$
  a ni ničla nobenega neničelnega polinoma

Če je a transendenten: $F[X] \simeq F[a]$

- Če je a algebraičen nad $F \Rightarrow$
  Naj bo $p(x) \in F[x]$ naj bo njegov minimalni polinom: $p(a) = 0$
  Če je $f(x) \in \ker \mathrm{eval} \Leftrightarrow f(a) = 0 \Leftrightarrow$
  $p(x) \mid f(x)$
  $\ker \mathrm{eval} =$ večkratniki $p(x) = (p(x))$
  to ej alg $\Rightarrow \frac{F[X]}{(p(x))} \cong F[a] = F(a)$

Izrek: Naj bo K/F razširitev

$L = \{a \in K ;\ a \text{ je algebraičen nad } F\}$

Potem je L podpolje v K

Dokaz: $a, b \in L$; a, b sta algebraična nad F

$F(a,b)$ je po posledici končna razširitev F

Po izreku (enem prej) je $F(a,b)/F$ algebraična razširitev, torej $F(a,b)/F \subseteq L$

Med drugim $a \cdot b \in L$, $a - b \in L$ in $a^{-1} \in L$ če $a \neq 0$

$\blacksquare$

Obrat ne velja (obstaje algebraične razširitev ki ni končna)

Primer: algebraične razširitev $\mathbb{Q}$-je, ki ni končna.

$\mathbb{C}/\mathbb{Q}$

$L = \{ a \in A ; \exists p(x) \in \mathbb{Q}[X] . p(a) = 0 \}$

L je podpolje v $\mathbb{C}$

$L/\mathbb{Q}$ je algebraična razširitev

$[L : \mathbb{Q}] = \infty$

Recimo da bi bila končna $[L:\mathbb{Q}] = m$

$\sqrt[n]{2} \in L$

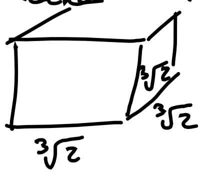
$\mathbb{Q}(\sqrt[n]{2}) \subseteq L$ za $\forall n$

$\underbrace{[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}]}_{= n} \mid [L : \mathbb{Q}] = m$

m mora biti deljiv z vsakim naravnim številom

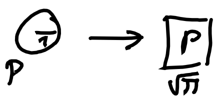
Konstrukcije z ravnilom in šestilom

Z ravnilom in šestilom nariši kocko z 2x večjim volumnom



Podvojitev kocke

kvadratura kroga:

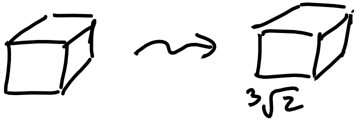


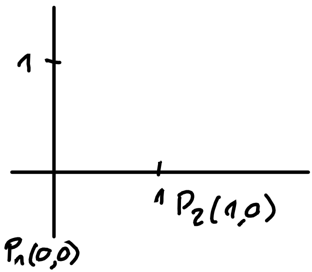
Ali lahko narišem kvadrat z isto ploščino

Trisekcija kota

Formulacija problema

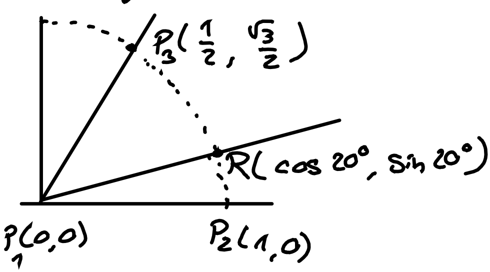
Motivacija





$\rightsquigarrow R(\sqrt[3]{2}, 0)$

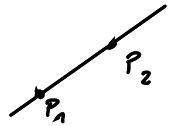
Trisekcija 60°



$P_1, P_2, \ldots, P_n \in \mathbb{R}^2$

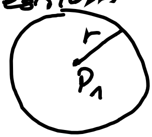
Konstrukcije:

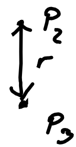
- z ravnilom:



  · čez dve točki potegnemo premico

- s šestilom:





nove točke: presečišča

Postopek

$\mathcal{P} = \{P_1, \ldots, P_n\}$

konstruiramo novo točko A na enega od teh treh načinov

$\mathcal{P} \leftarrow \mathcal{P} \cup \{A\}$

Ponovimo postopek

Izrek: $\mathcal{P}$ naj bo množica točk v $\mathbb{R}\times\mathbb{R}$

Recimo da je $\mathbb{F}$ podpolje v $\mathbb{R}$

da $\mathcal{P}\subseteq \mathbb{F}\times\mathbb{F}$

Recimo da je $A(a,b)$ konstruktibilna s pomočjo točk iz $\mathcal{P}$

Potem sta ta dva elementa a, b algebraična nad $\mathbb{F}$, s stopnjama razširitve, ki sta potenci števila 2

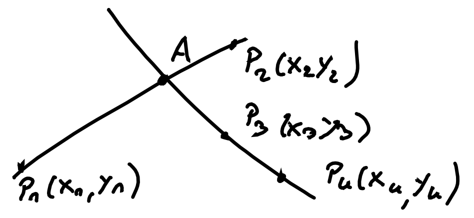
Dokaz: Naj bo najprej $A(a,b)$ prva točka v tej konstrukciji:

Trdimo: $[F(a,b):F]\in\{1,2\}$

(To je dovolj, ker potem se stopnje množijo naprej $([F_{(a,b)}(c,d):F(a,b)]\in\{1,2\}\Rightarrow [F(a,b)(c,d):F] \in\{1,2,4\}$ itd.)

$A(a,b)$ smo dobili na enega od teh načinov

1) presečišče dveh premic



1. premica: $x=a_1$ ali: $y=k_1x+n_1$

2. premica: $x=a_2$ ali: $y=k_2x+n_2$

$a_2\, a_1\in F$ $\quad k_1=\dfrac{y_2-y_1}{x_2-x_1}\in F$

$n_1=y_1-k_1x_1\in F$

Presečišče dveh premic je rešitev linearnega sistema enačb, ki imata koef. v $\mathbb{F}$

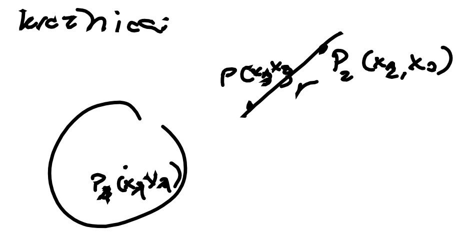
Rešitev $(a,b)\in\mathbb{F}\times\mathbb{F}$

$\Rightarrow [F(a,b):F]=1$

2) Presečišče premice in krožnice

premica: $x=a_1$ ali $y=k_1x+n_1$ $\quad a_1,k_1,n_1\in F$

krožnica:



$$(x-\underbrace{x_1}_{\in F})^2+(y-\underbrace{y_1}_{\in F})^2=\underbrace{(x_3-x_2)^2+(y_3-y_2)^2}_{\in F}$$

$x^2+y^2+\alpha x+\beta y+\gamma=0 \qquad \alpha,\beta,\gamma\in F$

Če je premica $x=a_1$ dobimo enačbo za y s koef. iz F

Če je premica $y=k_1x+n_1$ dobimo kvadratno enačbo za x s koef v F

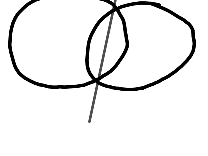
$$\text{rešitev}_{1,2}=\frac{-b\pm\sqrt{b^2-4ac}}{2a}$$

Rešitev je v $\mathbb{F}$, ki mu dodamo ta koren $\left(\sqrt{b^2-4ac}\right)$

$\Rightarrow$ zato $[F(a,b):F]=2$ ali 1 če koren že v F

3) 2 krožnici

isto kot 2) ker



= presečišče krožnice in premice

Ponavljamo postopek

$\mathcal{P}\subseteq\mathbb{F}\times\mathbb{F}$

$A(a,b)$ konstruiramo $[F(a,b):F]\in\{1,2\}$

$\mathcal{P}\leftarrow\mathcal{P}\cup\{A\}$, $F\leftarrow F(a,b)$

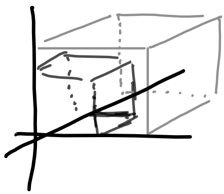
$B(c,d)$ $[F(a,b)(c,d):F(a,b)]\in\{1,2\}$

$[F(a,b)(c,d):F]=$

$[F(a,b)(c,d):F(a,b)]\cdot[F(a,b):F]\in\{1,2,4\}$

Posledica:

Kocke ne moremo podvojiti z ravnilom in sestilom

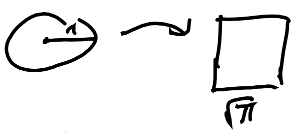


$P(0,0)$, $P(1,0)$ $\rightarrow$ $P_3(\sqrt[3]{2}, 0)$

$P_1, P_2 \in \mathbb{Q} \times \mathbb{Q}$

$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3 \neq 2^n$

Posledica: kvadratura kroga ni mogoča z ravnilom in sestilom



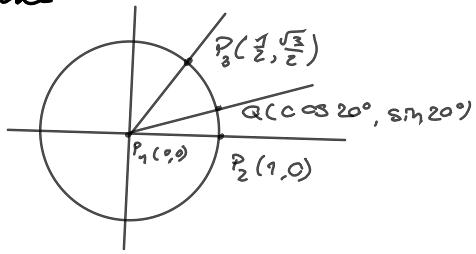
$P(0,0)$, $P(1,0)$ $\rightarrow$ $P_3(\sqrt{\pi}, 0)$

$[\mathbb{Q}(\sqrt{\pi}) : \mathbb{Q}] = \infty$

π je transcendenten

Posledica: kota $60°$ se ne more razdeliti na tri enake dele z ravn. in šest.

Dokz



$\{P_1, P_2, P_3\} \subseteq \mathbb{Q}(\sqrt{3}) \times \mathbb{Q}(\sqrt{3})$

Če se Q da konstruirati potem

$[\mathbb{Q}(\sqrt{3}, \cos 20°) : \mathbb{Q}(\sqrt{3})] = 2^k$

$\cos 3\varphi = 4\cos^3\varphi - 3\cos\varphi$ $\qquad \varphi = 20°$

$\cos 20° = a$

$\frac{1}{2} = 4a^3 - 3a$

$8a^3 - 6a - 1 = 0$

a je ničla polinoma $p(x) = 8x^3 - 6x - 1$

Trdimo da je $p(x)$ nerazcepen nad $\mathbb{Q}(\sqrt{3})$

Recimo da je razcepen nad $\mathbb{Q}(\sqrt{3})$.

Ker je stopnje 3 mora imeti neko ničlo v $\mathbb{Q}(\sqrt{3})$

$\alpha + \beta\sqrt{3}$ je ničla tega polinoma $\alpha, \beta \in \mathbb{Q}$

Trik: $(2x)^3 - 3 \cdot 2x - 1 = 0$

BSZS: $\alpha + \beta\sqrt{3}$ je ničla polinoma $y^3 - 3y - 1 = 0$

$(\alpha + \beta\sqrt{3}) - 3(\alpha + \beta\sqrt{3}) - 1 = 0$

$\alpha^3 + 3\alpha^2\beta\sqrt{3} + 9\alpha\beta^2 + 3\beta^3\sqrt{3} - 3\alpha - 3\beta\sqrt{3} - 1 = 0$

$\alpha^3 + 9\alpha\beta^2 - 3\alpha - 1 + \sqrt{3}(3\alpha^2\beta + 3\beta^3 - 3\beta) = 0$

Dobimo $\alpha^3 + 9\alpha\beta^2 - 3\alpha - 1 = 0$ in

$\beta(3\alpha^2 + 3\beta^2 - 3) = 0$

1) $\beta = 0 \Rightarrow \alpha^3 - 3\alpha - 1 = 0$ nima racional. ničel

2) $\alpha^2 + \beta^2 = 1 \Rightarrow$ vstavimo v prvo enačbo in dobimo enačbo 3 stopnje brez rac. reš.

Sklep: $p(x)$ je res nerazcepen nad $\mathbb{Q}(\sqrt{3})$

Torej je $[\mathbb{Q}(\sqrt{3}, \cos 20°) : \mathbb{Q}(\sqrt{3})] = 3$

Razpadna polja polinomov

Motivacija: $x^2-2 \in \mathbb{Q}[x]$ nima ničel v $\mathbb{Q}$

Če gledamo $x^2-2 \in \mathbb{R}[x]$ ga lahko razcepimo na linearne faktorje

Splošno: $f(x) \in F[x]$, naj obstaja neka razširitev K/F, da ima $f(x)$ neko ničlo $a \in K$

$f(x)$ lahko gledamo kot polinom v $K[x]$:

$$f(x) = (x-a) \cdot f_1(x) \quad ; f_1(x) \in K[x]$$

Očitno: K/F, $f(x) \in F[x]$, $\operatorname{st} f(x) = n \Longrightarrow$

K vsebuje kvečjemu n ničel $f(x)$

Trditev: Naj bo $f(x) \in F[X]$ nekonst. polinom. Potem obstaja K/F, ki vsebuje vsaj eno ničlo polinoma $f(x)$

Dokaz:

Naj bo $p(x)$ nerazcepen $\in F[X]$ polinom, ki deli $f(x)$; stopnja $p(x) > 1$ BSZS

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

<u>K je polje</u>

$g(x) + (p(x)) \in F[X]/(p(x))$ neničeln element

$g(x) \notin (p(x))$. Ker je $p(x)$ nerazcepen, je največji skupni delitelj $g(x)$ in $p(x)$ enak 1

$a(x), b(x) \in F[X]$

$$g(x) \cdot a(x) + p(x) \cdot b(x) = 1$$

$$(g(x) + (p(x)))\,(a(x) + (p(x))) = g(x)a(x) + (p(x))$$
$$= 1 + (p(x))$$

$g(x) + (p(x))$ je obrnljiv

K vsebuje F, ker

$$F \longrightarrow F[X]/(p(x))$$
$$\alpha \longmapsto \alpha + (p(x)) \quad \text{je monomorfizem}$$

$f(x) \in F[X]$ lahko gledamo kot polinom v $K[X]$

$$f(x) = \sum a_k X^k \rightsquigarrow \sum (a_k + (p(x))) \cdot X^k$$

Kateri element K je ničla tega polinoma

$$X + (p(x)) \in K$$

$$f(X + (p(x))) = \sum (a_k + (p(x)))\,(X^k + (p(x))) =$$
$$= \sum a_k X^k + (p(x)) = f(x) + (p(x)) = (p(x))$$

∎

Posledica: $f(x) \in F[x] \Rightarrow \exists$ polje $K \geq F$, da

$$f(x) = c(x-a_1)(x-a_2) \cdot \ldots \cdot (x-a_n)$$

$a_i \in K \quad c \in F$

Def: $f(x) \in F[x]$ razpade nad poljem K, če ga lahko v $K[x]$ lahko razstavimo na 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 posledici $\exists K$ ki vsebuje vse ničle $a_1 \ldots a_n$ polinoma $f(x) \in F[x]$

Razpadno polje je potem $F(a_1 \ldots a_n)$

Koliko je razpadnih polj

$x^2-2 \in \mathbb{Q}[X]$

$\mathbb{Q}(\sqrt{2})$ je razpadno polje

$$\mathbb{Q}[X]/(x^2-2) \cong \mathbb{Q}(\sqrt{2})$$

Vsa razpadna polja so med sabo izomorfna

Opomba: Razpadno polje polinoma $\in F[X]$ je končna razširitev polja F

Oznaka: Naj bosta F, F' polji

$\varphi: F \to F'$ homomorfizem

$f(x) \in F[X]: f(x) = \sum_{k=1}^{n} a_k x^k \quad a_k \in F$

$$F_\varphi[X] = \sum_{k=1}^{n} \varphi(a_k) X^k \in F'[X]$$

Lema: $p(x) \in F[x]$ nerazcepen polinom

$a \in K$ naj bo ničla $p(x)$

$\varphi: F \longrightarrow F'$ naj bo izomorfizem polj

Polinom $p_\varphi(x) \in F'[x]$ naj ima neko ničlo $a' \in K'$

Potem obstaja natanko en izomorfizem $\Phi: F(a) \longrightarrow F'(a')$ da

$\Phi|_F = \varphi$ in $\Phi(a) = a'$

Ostali so linearna kombinacija teh dveh

Dokaz: $p(x)$ je minimalni polinom a-ja

Ker je φ izomorfizem je $p_\varphi(x)$ minimalni polinom a'

$$\begin{tikzcd} F[x]/(p(x)) \arrow[r, "\overline{\varepsilon}", "\cong"'] \arrow[d, "\pi"] & F(a) \arrow[d, dashed, "\Phi"] \\ F'[x]/(p_\varphi(x)) \arrow[r, "\tilde{\varepsilon}", "\cong"'] & F'(a') \end{tikzcd}$$

$\varepsilon: F[x] \to F(a)$ evalvacijski homomorfizem

Definirajmo $\pi: F[x]/(p(x)) \longrightarrow F'[x]/(p_\varphi(x))$

$$f(x) + (p(x)) \longmapsto f_\varphi(x) + (p_\varphi(x))$$

DN: π je izomorfizem polj

$$\Phi = \tilde{\varepsilon} \circ \pi \circ \overline{\varepsilon}^{-1}$$

Enoličnost:

$$\Phi\left(\sum \lambda_k a^k\right) = \sum \Phi(\lambda_k)\Phi(a^k) = \sum \varphi(\lambda_k) a'^k$$

Recimo da imamo še en tak izomorfizem $\tilde{\Phi}$

$$\tilde{\Phi}\left(\sum \lambda_k a^k\right) = \sum \tilde{\Phi}(\lambda_k)\tilde{\Phi}(a^k) = \sum \varphi(\lambda_k) a'^k$$

Izrek: F, F' naj bosta polji:

$\varphi: F \xrightarrow{\cong} F'$ $f(x)$ naj bo nekonstanten polinom v $F(x)$, K naj bo razpadno polje $f(x)$, K' naj bo razpadno polje polinoma $f_\varphi(x) \in F'(x)$. Potem obstaja izomorfizem $\bar{\Phi}: K \to K'$

Posledica: Če je $f(x) \in F[x]$ nekonstanten polinom sta poljubni razpadni polji polinoma $f(x)$ izomorfni:

Dokaz: Uporabimo izrek za $F' = F$ $\varphi = id_F$

Dokaz:

Indukcija po $n = [K:F]$

$n = 1$: $K = F \overset{\varphi\ izo}{\Rightarrow} K' = F'$

$n > 1$: $f(x)$ ne razpade na lin. faktorje nad F

Naj bo $p(x) \in F[x]$ nerazcepen polinom ki deli $f(x)$; $st(p(x)) > 1$

K vsebuje neko ničlo a polinoma $p(x)$, ker je razcep. polje $f(x)$

Podobno K' vsebuje ničlo a' polinoma $p_\varphi(x) \in F'[x]$

Po lemi obstaja natanko en izomorfizem

$\bar{\Phi}: F(a) \to F'(a')$

$\bar{\Phi}/_F = \varphi$

$\bar{\Phi}(a) = a'$

K je razpadno polje $f(x)$ tudi nad $F(a)$, podobno je K' razcepno polje nad $f_\varphi(x)$ nad $F'(a')$

$$[K:F(a)] = [K:F] : [F(a):F] = \frac{n}{\underbrace{st(p(x))}_{\geq 2}} < n$$

a maminimalni polinom $p(x)$

Po ind. pred. obstaja izomorfizem

$\bar{\Phi}^*: K \to K'$

$\bar{\Phi}^*/_{F(a)} = \bar{\Phi}$

$\bar{\Phi}^*/_F = \bar{\Phi}/_F = \varphi$

Normalne razširitve polj

Def: Naj bo K/F razširitev polj
Pravimo da je ta razširitev normalna, če za vsak nerazcepen polinom $p(x) \in F[X]$ velja ena od možnosti:

1) $p(x)$ ima vse ničle v K
2) $p(x)$ nima nobene ničle v K

Izrek: Naj bo K/F končna razširitev.

K/F je normalna razširitev $\Leftrightarrow$

$\Leftrightarrow$ K je razpadno polje nekega polinoma iz $F[x]$

Dokaz:

$\Rightarrow$ K/F naj bo normalna. $K = F(a_1, \dots, a_n)$

Naj bo $p_i(x)$ minimalni polinom od a_i.

Po definiciji normalnosti K vsebuje vse ničle polinoma $p_i(x)$

$$f(x) := p_1(x) p_2(x) \dots p_n(x)$$

Naj bo L razpadno polje $f(x)$

$K = L$

$a_1 \dots a_n$ so ničle $f(x)$ $\Rightarrow$

$a_1, \dots, a_n \in L \Rightarrow F(a_1, \dots, a_n) \subseteq L \Rightarrow K \subseteq L$

$L \subseteq K$

ker K vsebuje vse ničle $f(x)$, L pa je najmanjši tak, ki vsebuje vse ničle $f(x)$ po definiciji: $L \subseteq K$

$\Leftarrow$ K naj bo razpadno polje $f(x) \in F[x]$

Izberemo poljuben nerazcepen polinom $p(x) \in F[x]$.

Naj bo a ničla polinoma $p(x)$, ki leži v K. Naj bo b poljubna druga ničla polinoma $p(x)$

$b \in K$

$p(x)$ je minimalni polinom za a in b

Identično preslikavo $F \to F$ lahko razširimo do izomorfizma $\Phi : F(a) \xrightarrow{\cong} F(b)$

$\Phi|_F = id$ Φ

$\Phi(a) = b$

K razp. polje $f(x)$

$p(x)$ nerazcepen z $a \in K$ ničlo

b poljubna ničla $p(x)$

Razpadno polje polinoma $f(x)$ nad

$F(a)$: $F(\underset{\underset{K}{\cap}}{a}, a_1, \dots, a_n) = K$

nad $F(b)$: $F(b, a_1 \dots a_n) = K'$

Po izreku obstaja

$\Phi^* : K \to K'$

$\Phi^*|_{F(a)} = \Phi$

$\Phi^*(a) = b$

$a \in K = F(a_1, \dots, a_n)$

a = „polinom" v $a_1, \dots, a_n$

$b = \Phi^*(a) \Rightarrow b$ je polinom v $\underbrace{a_1 \dots a_n}_{\text{ker } id}$

Torej $b \in F(a_1 \dots a_n) = K$

Zgled:

1. $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ je normalna, ker je
   $\mathbb{Q}$ razpadno polje $x^2-2 \in \mathbb{Q}[X]$

2. $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ ni normalna, ker
   $\sqrt[3]{2}$ je ničla $x^3-2 \in \mathbb{Q}[X]$ nerazcepen
   Toda $\mathbb{Q}(\sqrt[3]{2})$ ne vsebuje vseh ničel x^3-2

3. p praštevilo, $\varepsilon = e^{\frac{2\pi i}{p}}$ (primitivni p-ti koren enote)
   $\mathbb{Q}(\varepsilon)/\mathbb{Q}$ je normalna, ker
   $\mathbb{Q}(\varepsilon)$ razpadno polje x^p-1
   $\hookrightarrow$ ničle tega polinoma so $\varepsilon, \varepsilon^2, \dots, \varepsilon^{p-1}, 1$

   vse ničle živijo v $\mathbb{Q}(\varepsilon)$

Algebraično zaprtje polja

Def: A polje. Pravimo da je A algebraično zaprto če ima $\forall$ nekonst. polinom $f \in A[x]$ vsaj eno ničlo.

Ekvivalentno: $f(x) = c(x-a_1)\dots(x-a_k)$; $c, a_i \in A$

Lema: $F \subseteq L \subseteq K$ naj bodo polja, L/F algebraične. Naj bo $a \in K$ algebraičen nad L. Potem je a algebraičen nad F

Dokaz:

Po definiciji $\exists p(x) \in L[X]$, $p(a) = 0$

$p(x) = \sum a_k X^k \quad a_k \in L$

$\tilde{F} = F(a_1 \dots a_n)$, $p(x) \in \tilde{F}[X] \Rightarrow$ a algebraičen nad $\tilde{F}$

$[\tilde{F}(a) : F]$ dovolj je dokazati da je to $< \infty$

$[\tilde{F}(a) : F] = \underbrace{[\tilde{F}(a) : \tilde{F}]}_{< \infty} \cdot [\tilde{F} : F]$

ker je a alg. nad $\tilde{F}$

L/F algebraične, $a_k \in L \Rightarrow a_k$ algebr. nad F

$\Rightarrow [F(a_1, \dots a_n) : F] < \infty \Rightarrow [\tilde{F} : F] < \infty \Rightarrow$

$[\tilde{F}(a) : F] < \infty$ ∎

Def: Naj bo F polje. Algebraično zaprtje polja F je takšno algebraično zaprto polje $\overline{F}$, ki vsebuje F in je $\overline{F}/F$ algebraično

(DN: $\overline{F}$ je najmanjše algebraično zaprto polje, ki vsebuje F)

Opomba: Da se pokazati da je vsako polje vsebovano v nekem algebraičnem zaprtem polju.
Da se pokazati da algebraično zaprtje polja vedno obstaja in je do izomorfizma enolično določeno

Primer

$\mathbb{R}$:

$\mathbb{C}$ je alg zaprto

$\mathbb{R} \subseteq \mathbb{C}$ $\quad \mathbb{C}/\mathbb{R}$ je razširitev stopnje 2

$\Rightarrow \overline{\mathbb{R}} = \mathbb{C}$

$\mathbb{Q}$; $\quad \mathbb{C}/\mathbb{Q}$ ni algebraična $\quad \overline{\mathbb{Q}} \neq \mathbb{C}$

Izrek: Naj bo F vsebovano v nekem algebraičnem zaprtem polju A

$K := \{a \in A .\ a \text{ algebraičen nad } F\}$

Potem je $K = \overline{F}$

Dokaz: Dokazali smo že, da je K polje, ki vsebuje F. K/F je algebraična razširitev po def K. $\underbrace{F \subseteq K}_{\text{alg.}} \subseteq A$

Dokazati moramo še,

da je K algebraično zaprto polje.

Naj bo $f(x) \in K[x]$ nek nekonst. polinom

Ker je A alg zaprto ima $f(x)$ ničlo $a \in A$

a je algebraičen nad K, K/F je alg. razširitev.

Po lemi je a algebraičen nad F.

Po definiciji $a \in K$

$\blacksquare$

Zgled:

$\overline{\mathbb{Q}} = \{a \in \mathbb{C} : a$ je ničla nekega neničelnega polinoma iz $\mathbb{Q}[x]\} = \{$algebraična števila$\}$

Končna polja

Naj bo K končno polje
Potem je karakteristika tega polja
$\operatorname{char} K = p \quad p \in \mathbb{P}$.
Zato je $\mathbb{Z}_p$ podpolje v K. $\quad K/\mathbb{Z}_p$

Trditev: $|K| = p^n$ za nek $n \in \mathbb{N}$

Dokaz: $K/\mathbb{Z}_p$ je končna razširitev.
K ima kot vek. prostor nad $\mathbb{Z}_p$ končno
bazo $a_1, \ldots, a_n$
Vsak element K se da enolično
zapisati kot $\underbrace{\alpha_1}_{p} a_1 + \underbrace{\alpha_2}_{p} a_2 + \ldots + \underbrace{\alpha_n}_{p} a_n \quad \alpha_k \in \mathbb{Z}_p$
p možnosti

Imamo torej natanko p^n možnosti za elemente K

$\blacksquare$

Lema: Naj bo K polje moči p^n.
Potem je K razpadno polje polinoma

$$X^{p^n} - X \in \mathbb{Z}_p[X]$$

Dokaz: $(K^*, \cdot)$ je grupa moči $p^n - 1$
Po lagrangevem izreku

$$\forall a \in K^*: \; a^{p^n - 1} = 1 \quad / \cdot a$$

$$\forall a \in K \quad a^{p^n} = a$$

$\forall$ element K je ničla polinoma $X^{p^n} - X$

Ker je $st(X^{p^n} - X) = p^n$ ima ta polinom $\leq p^n$ ničel v poljubni razširitvi

Ker K vsebuje vse ničle, ter nobeno podpolje ne vsebuje vseh ničel, je K razpadno polje $X^{p^n} - X$

$\blacksquare$

Lema:

Naj bo L razpadno polje $X^{p^n}-X$ nad $\mathbb{Z}_p$. Potem je $|L|=p^n$

Dokaz:

Naj bo K množica vseh ničel polinoma $f(x)=X^{p^n}-x$ v L

$$\underline{K=L} \Leftarrow \underline{K \text{ je polje}}$$

zaradi minimalnosti L-ja

Frobeniusev endomorfizem:

$$\varphi: L \to L$$
$$x \mapsto x^p$$

$$K=\{a\in L ; a^{p^n}=a\}=\{a\in L ; \varphi^n(a)=a\}$$

$$x,y\in K : \varphi^n(x-y)=\varphi^n(x)-\varphi^n(y)=x-y \Rightarrow x-y\in K$$

Podobno $x\cdot y$, x^{-1} če $x\neq 0$

Torej je K polje $\Rightarrow$ $K=L$

Za dokaz da je $|L|=p^n$ je dovolj da ima naš polinom $f(x)$ samo enostavne ničle

Ena ničla: $a=0$

$$f(x)=(\underbrace{x^{p^{n}-1}-1}_{})x$$

0 ni ničla tega polinoma

$\Rightarrow$ 0 je enostavna ničla

Recimo da $a\neq 0$ ničla:

Iz prejšnjega dokaza $a^{p^n-1}=1$

$$f(x)=(x^{p^n-1}-a^{p^n-1})x=$$

$$(x-a)x\underbrace{(x^{p^n-2}+ax^{p^n-3}+\dots+a^{p^n-3}x+a^{p^n-2})}_{g(x)}$$

$$g(a)=a^{p^n-2}\cdot(p^n-1)\neq 0$$

Torej je a enostavna ničla

Posledica: Za vsako praštevilo p in vsako $n \in \mathbb{N}$ obstaja natanko eno (do izomorfizma natančno) polje moči p^n

Oznake: $\mathbb{F}_{p^n}$, $GF(p^n)$

Opomba: Wedderburnov izrek: Vsak končen obseg je polje

Trditev: Multiplikativna grupa končnega polja je vedno ciklična

Dokaz: Naj bo $G = (\mathbb{F}_{p^n}^*, \cdot)$

G je končna abelova grupa moči $p^n - 1$
v naj 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 $v \mid (p^n - 1)$ $\quad v \leq p^n - 1$
Dovolj je videti da je $p^n - 1 \leq v$

$x^v - 1$ ima kvečjemu v ničel
Ker je v skupni večkratnik redov elem. grupe G, za $\forall g \in G$. $g^v = 1$

$\Rightarrow \quad p^n - 1 \leq v \quad \Rightarrow v = p^n - 1$

Torej ima nek element a red $v = p^n - 1$

$\Rightarrow G = \langle a \rangle$

Separabilne razširitve

Def: Naj bo $p(X) \in F[X]$ nekonstanten polinom. Pravimo da je $p(X)$ separabilen če so njegove ničle v poljubni razširitvi polja F enostavne

Def: Naj bo K/F algebraična razširitev. Pravimo da je ta razširitev <u>separabilna</u> če je za $\forall a \in K$ minimalni polinom a-ja nad F separabilen

Izrek: Naj bo F polje s karakteristiko 0. Naj bo $p(x)$ poljuben nerazcepen polinom. Potem je poljubna ničla $p(x)$ v poljubni razširitvi K/F enostavna

Posledica: če je $\operatorname{char} F = 0$ je vsaka algebraična razširitev F separabilna