Cela števila

Trd. $\forall m \in \mathbb{Z} . \forall n \in \mathbb{N} . \exists q, r \in \mathbb{Z} . m = qn + r \wedge 0 \le r < n$.
Trd. $\forall m,n \in \mathbb{Z} . \exists \gcd(m,n) . \wedge \exists x,y \in \mathbb{Z} . \gcd(m,n) = mx+ny$.
Trd. $\forall m,n\in\mathbb{Z} . \gcd(m,n)=1 \iff \exists x,y\in\mathbb{Z} . 1=mx+ny$.

1 Uvod v teorijo grup

Lagrange. Naj bo G končna grupa in $H \le G$: $|G| = [G:H]|H|$.

Grupa permutacij
- Zapis s transpozicij: $(i_1 i_2 \dots i_n) = (i_1 i_n)(i_1 i_{n-1})\dots(i_1 i_3)(i_1 i_2)$
- Inverz k-cikla: $(i_1 i_2 \dots i_k)^{-1} = (i_k i_{k-1}\dots i_2 i_1)$
- Konjugiranje: $\pi \in S_n \Rightarrow \pi(i_1 i_2\dots i_k)\pi^{-1} = (\pi(i_1)\pi(i_2)\dots\pi(i_k))$
- TODOA_n, s čim je generirana?

Diedrska grupa D_{2n}
- $z^k r = r^{-k} z = r^{n-k} z$
- $r^k z$ so zrcaljenja, $(r^k z)^2 = 1$

Podgrupe
- $H,K \le G \Rightarrow |HK| = \frac{|H||K|}{|H\cap K|}$.
- Diagonalna podgrupa $\triangle = \{(x,x) \mid x\in G\} \le G\times G$

Ciklične grupe
- Vsaka podgrupa ciklične grupe je ciklična
- Podgrupe v $\mathbb{Z}$ so oblike $n\mathbb{Z}, n\in\mathbb{N}$
- Podgrupe v $\mathbb{Z}_n$ so $\mathbb{Z}_d$, kjer $d\mid n$
- $G=\langle a\rangle, |G|<\infty \Rightarrow G = \langle a^k\rangle \iff \gcd(k,n)=1$
- $k\in Z_n \Rightarrow \operatorname{red} k = \frac{n}{\gcd(n,k)}$
- Konjugiranje ohranja red elementa

Generatorji grup
Naj želimo določiti $\langle A\rangle$. Oglejmo množico $\mathcal{A}$ vseh možnih produktov in inverzov (elementov, ki morajo biti v $\langle A\rangle$) ter pokažemo, da je podgrupa. Nato iz minimalnosti $\langle A\rangle$ sledi enakost.

Splošno
Naj bo $f: X\to X$ preslikava. Velja:
- f ima levi inverz: $g\circ f = \mathrm{id} \iff f$ injektivna. Če f tudi ni surjektivna, potem ima več levih inverzov.
- f ima desni inverz: $f\circ h = \mathrm{id} \iff f$ surjektivna. Če f tudi ni injektivna, potem ima več desnih inverzov.

2 Uvod v teorijo kolobarjev

Brucevo sanje. Naj bo F polje, $\operatorname{char} F = p$. Tedaj $(x+y)^p = x^p+y^p$.
- Kolobar K je Boolov, če $\forall x\in K . x^2 = x$. Boolov kolobar je komutativen in ima karakteristiko 2.
- Kolobar $\mathbb{Z}$ ni algebra nad nobenim poljem.
- Naj bo A končno-razsežna algebra, $a \in A\setminus\{0\}$. Tedaj
  - $(\exists b\in A\setminus\{0\} . ab = 0 \vee ba = 0) \sqcup (\exists a^{-1} . a^{-1}a = aa^{-1} = 1)$.
  - $\exists b \in A . ab = 1 \vee ba = 1 \Rightarrow a^{-1} = b$.
  - Če je A obseg, je vsaka podalgebra podobseg.

Algebra kvaternionov $\mathbb{H}$
- $i^2=j^2=k^2=ijk=-1$
- $Q=\{\pm i,\pm j,\pm k,\pm 1\}$ je kvaternionska grupa.
- $Z(\mathbb{H}) = \mathbb{R}$, $Z(Q)=\{-1,1\}$.
- $\forall h\in\mathbb{H} . \exists\alpha,\beta\in\mathbb{R} . h^2+\alpha h+\beta=0$, kjer $-\alpha = h+\overline{h}$ in $\beta = h\overline{h}$.

Kolobar Z_n
- Kolobar $\mathbb{Z}$ ima 2 obrnljivih elementa: 1 in -1
- V $\mathbb{Z}_n$ element $k\in\mathbb{Z}_n$ je obrnljiv natanko tedaj, ko $\gcd(k,n)=1$.
- $|\mathbb{Z}_n^*| = \varphi(n)$. Če je p praštevilo, potem $|\mathbb{Z}_p| = p-1$.

Generatorji kolobarjev
Naj želimo določiti $\langle A\rangle$. Postopamo kot pri grupah (vse možne vsote, nasprotni elementi ter produkti). Opazimo tudi, da $\mathcal{A}$ vedno vsebuje 1.

3 Homomorfizmi

- Homomorfizem $\varphi:\mathbb{Z}\to G$, $\varphi(1)=a$ obstaja za vsak $a\in G$. Homomorfizem $\varphi:\mathbb{Z}^n\to G$, $\varphi(1)=a$ natanko tedaj, ko $a^n=1$.
- Naj bo $\varphi: G\to G'$ homomrfizem grup in naj ima element $a\in G$ končen red. Tedaj $\operatorname{red}\varphi(a)\mid\operatorname{red} a$. Če je φ vložitev, potem reda sta enaka.

4 Kvocientne strukture

Izr. Naj bo K komutativen kolobar, $M\triangleleft K$.
Tedaj je M maksimalen $\iff K/_M$ polje.

Kvocientne grupe
- $\langle r\rangle$ je edinka v D_{2n} za $n\ge3$.
- Če je $G/_{Z(G)}$ ciklična, potem je G Abelova.

1. izrek o izomorfizmu
- To, da je podgrupa $N\triangleleft G$ edinka v G lahko dokažemo tako, da najdemo ustrezni homomorfizem φ, za kateri $\ker\varphi = N$.

Kvocientni kolobarji
- Za vsak kolobar K velja, da $\forall a\in K . aK = \{ak\mid k\in K\} = Ka$ je ideal. To je **glavni ideal** v K, generiran z a.
- Enostavnost kolobarja K uporabimo/dokažemo tako, da predpostavimo, da podan ideal ni trivialen, torej mora biti enak K.
- Kolobar $M_n(D)$ je enostaven, če je D obseg.
- Center enostavnega kolobarja je polje. Komutativen kolobar je enostaven natanko tedaj, ko je polje.
- Naj bosta K_1 in K_2 kolobarja. Tedaj vsak ideal direktnega produkta $K_1\times K_2$ je oblike $I_1\times I_2$, kjer je I_1 ideal v K_1 ter I_2 ideal v K_2.

5 Klasifikacija končnih grup

Def. Komutator elementov $a,b\in G$ je $[a,b] := aba^{-1}b^{-1}$.
Def. Naj bo G grupa, potem je $T(G) = \{g\in G \mid \operatorname{red}(g)<\infty\}$ **torzijska podgrupa** G. Če je $T(G)=\{0\}$, pravimo, da je G **brez torzije**.
Izr. Če $\gcd(n,m)=1$, potem $\mathbb{Z}_n\oplus\mathbb{Z}_m\approx\mathbb{Z}_{nm}$.
- G p-grupa, H q-grupa, $p\ne q : G,H$ ciklični $\iff G\oplus H$ ciklična.

Vse grupe do izomorfizma natančno
Naj treba poiskati vse grupe reda n do izomorfizma natančno. Zapišemo $n = p_1^{k_1}\cdot\ldots\cdot p_n^{k_n}$. Nato zapišemo vse grupe moči $p_i^{k_i}$: to so grupe oblike $\mathbb{Z}_{l_1}\oplus\ldots\oplus Z_{l_j}$, kjer $l_1+\ldots+l_j = p_i^{k_i}$ razčlenitev števila $p_i^{k_i}$.

6 Delovanje grup

Naj G deluje na X.
Def. Orbita elementa $x\in X$ je $G\cdot x := \{g\cdot x\mid g\in G\}$.
Def. Stabilizator elementa x je $G_x := \{g\in G\mid g\cdot x = x\}$.
Def. Množica fiksnih točk $g\in G$ je $X^g := \{x\in X\mid g\cdot x = x\}$.
Def. Fiksne točke delovanja je množica $X^G := \bigcap_{g\in G} X^g$.
Def. Konjugiranostni razred $x\in G$ je $\operatorname{Raz}(x) := \{axa^{-1}\mid a\in G\}$.
Konjugiranostni razred je orbita pri delovanju G na G s konjugiranjem.
- Konjugiranostni razred x je $\{x\}\iff x\in Z(G)$.

O orbite in stabilizatorju. Potem za $\forall x\in X$ velja $|G\cdot x| = [G:G_x]$ in če G končna $|G| = |G\cdot x|\cdot|G_x|$.

7 Izreki Sylowa

Def. Naj bo $H\le G$, množici $N(H) := \{a\in G\mid aHa^{-1} = H\}$ pravimo **normalizator** H.
Def. $H\le G$ je **p-podgrupa Sylowa**, če je $|H| = p^k \wedge p^{k+1}\nmid |G|$.
Z n_p ozn. #p-podgrup Sylowa grupe G.
Sylow. Naj praštevilo p deli red končne grupe G:
- $p^k\mid|G| \implies G$ vsebuje vsaj eno p-podgrupo reda p^k.
- $\forall p$-podgrupa G je vsebovani v kaki p-podgrupi Sylowa.
- $\forall p$-podgrupi Sylowa sta konjugirani.
- #p-podgrup Sylowa grupe G deli $|G|$.
- #p-podgrup Sylowa grupe G je $pm+1$ za nek $m\ge0$.

Trd. $n_p = 1 \iff p$-podgrupa Sylowa je edinka.
Def. Grupa G je **enostavna**, če sta njeni edini edinki $\{1\}$ in G.
- To, da grupa ni enostavna lahko dokažemo tako, da najdemo edino p-podgrupo Sylowa.
- Opazujemo tudi moč preseka in produkta dveh podgrup.

8 Kolobar polinomov

Naj bo F polje.

Nerazcepnost
Trd. Naj bo $p(x)\in F[x]$, $\deg(p)>0$:
- $\deg(p)=1\implies p(x)$ nerazcepen.
- $\deg(p)\ge2$ in $p(x)$ nerazcepen $\implies$ nima ničle v F.
- $\deg(p)\in\{2,3\} \implies (p(x)$ nerazcepen $\iff$ nima ničle v $F)$.

Izr. Naj bo $f(x)\in\mathbb{Z}[x]$ tak, da ga ne moremo zapisati kot produkt dveh nekonstantnih polinomov v $\mathbb{Z}[x]$, potem je $f(x)$ nerazcepen tudi nad $\mathbb{Q}[x]$.
Eisenstein. Naj bo $f(x) = a_nx^n+\cdots+a_1x+a_0$ in $\exists p\in\mathbb{P}$, da $p\mid a_i$ za $i<n$, $p\nmid a_n$ in $p\nmid a_0^2$. Potem je $f(x)$ nerazcepen nad $\mathbb{Q}[x]$. **Trd.** $f(x) = x^n+1$ nerazcepen nad $\mathbb{Q}\iff n=2^k, k\ge1$.
Trd. Če je polinom $a_nx^n+\ldots+a_1x+a_0$ razcepen nad $\mathbb{Q}$, kjer so $a_0,\ldots,a_n\in\mathbb{Z}$, potem je $a_nx^n+\ldots+a_1x+a_0$ razcepen nad $\mathbb{Z}_p$, kjer $p\in\mathbb{P}$, $p \not| a_n$, koeficienti pa po modulu p.
Trd. a,b,c liha $\implies ax^4+bx+c$ nerazcepen nad $\mathbb{Q}$.
Trd. Naj bodo $a_1,\ldots,a_n\in\mathbb{Z}$ različna števila, potem sta polinoma $(x-a_1)\cdots(x-a_n)-1$ in $(x-a_1)^2\cdots(x-a_n)^2+1$ nerazcepna nad $\mathbb{Q}$.
Trd. x^p-x+1 je nerazcepen in separabilen nad $\mathbb{Z}_p$.
- Lahko pogledamo $f(x+1)$.
- Nad $\mathbb{Z}_2$ je x^2+x+1 edini nerazcepni polinom stopnje 2. Ostali polinomi pa so x^2, x^2+1, x^2+x.
- Uporabimo Brucevo sanje.

Razširitve polj
Naj bo K/F razširitev polj.
Def. $a\in K$ **algebraičen** nad F, če $\exists p(x)\in F[x] . p(a)=0$. Če je $p(x)$ moničen in minimalne stopnje, pravimo da je $m_a(x) := p(x)$ **minimalni polinom** za a nad F in a stopnje algebraičnosti $\deg(m_a(x))$ nad F. Sicer je a **transcendentalen** nad F.
Izr. Naj bo $a\in K$ algebraičen nad F in $p(x)\ne0\in F[x] . p(a)=0$ moničen. NTSE:
1. $p(x)$ minimalen polinom za a.
2. $p(x)$ nerazcepen.
3. $\forall q(x)\in F[x] . q(a)=0\implies p(x)|q(x)$.

Def. Razširitev K/F je **končna**, če je K končno razsežen vektorski prostor nad F in pišemo $[K:F] := \dim_F(K)$.
Izr. Naj bosta razširitvi L/K in K/F končni razširitvi.
Tedaj velja $[L:F] = [L:K]\cdot[K:F]$.
Trd. Vsaka končna razširitev je algebraična.

Def. Razširitev K/F je **primitivna**, če $\exists a \in K \,.\, K = F(a)$. Elementu a pravimo **primitivni element** K.

Izr. Naj bo K/F razširitev in $a \in K$ algebraičen nad F stopnje n. Potem je $F(a) = F[a] = \{\alpha_0 + \alpha_1 a + \cdots + \alpha_{n-1} a^{n-1} \mid \alpha_i \in F\}$ končna razširitev F in $[F(a) : F] = n$. Torej, $a_0, \ldots, a_{n-1}$ je baza prostora.

Trd. Naj bosta a, b alg. nad F in $\gcd([F(a) : F], [F(b) : F]) = 1$. Tedaj $[F(a, b) : F] = [F(a) : F] \cdot [F(b) : F]$.

Trd. Naj bo $[E : F] = p \in \mathbb{P}$, potem je $\forall a \in E \backslash F$ algebraičen stopnje p nad F.

Trd. $F(a^k, a^l) = F(a^d)$ za $d = \gcd(k, l)$.

Trd. Naj bosta $a_1, \ldots, a_n$ algebraični nad F.
Tedaj $[F(a_1, \ldots, a_n) : F] \leq [F(a_1) : F] \cdot \ldots \cdot [F(a_n) : F]$.

Trd. Ničle $f(x)$ so v poljubni razširitvi F enostavne $\iff$ $f(x)$ in $f'(x)$ tuja.

Trd. Naj bo E/F razširitev in $\text{char}(F) = 0$, $a \in E$ je k-kratna ničla $f(x) \in F[x] \iff f(a) = f'(a) = \cdots = f^{(k)}(a) = 0$ in $f^{(k+1)}(a) \neq 0$.

- Stopnja primitivni razširitvi $[F(a) : F]$ je enaka stopnje minimalnega polinoma a nad F.
- Naj bo $E \subseteq F$, $a \in F$. Tedaj $E(a) = E \iff [E(a) : E] = 1$.
- Stopnjo razširitve določimo bodisi s pomočjo minimalnega polinoma bodisi s pomočjo verigi razširitev.
- Lahko dokažemo, da je $F(a, b) = F(a + b)$.

Razpadna polja

Def. Naj bo K/F razširitev in $f(x) \in F[x]$. Pravimo da $f(x)$ **razpade** nad K, če je enak produktu linearnih polinomov v $K[x]$. Če $\nexists$ pravo podpolje K, v katerem $f(x)$ razpade, pravimo da je K **razpadno polje** $f(x)$ nad F.

- Razpadno polje dobimo tako, da vzemimo vsa ničla polinoma in tvorimo $F(x_1, \ldots, x_n)$. Ponavadi je treba dokazati enakost z drugim poljem. To naredimo z levo in desno vsebovanostjo.