Vaje iz Algebre 2

Hugo Trebše (hugo.trebse@gmail.com)

24. september 2025

The good Christian should beware of mathematicians, and all those who make empty prophecies. The danger already exists that the mathematicians have made a covenant with the devil to darken the spirit and to confine man in the bonds of Hell.

---

st. Augustine

Kazalo

Del I

Grupe

1 Grupe

Definicija 1.1

Grupa je par $(G, \cdot)$, kjer je operacija $\cdot$ asociativna, zanjo v G obstaja nevtralni element ter ima vsak element inverz.

Naloga 1.2

Permutaciji imata *enako zgradbo disjunktnih ciklov*, če sta permutaciji produkta disjunktnih ciklov enakih dolžin. Pokaži, da če imata permutaciji σ, σ' enako zgradbo disjunktnih ciklov, potem sta si konjugirani - obstaja $\pi \in S_n$, da je $\sigma' = \pi\sigma\pi^{-1}$.

Oris dokaza. Lahko, po tem ko opazimo, da če je $\sigma = d_1 \dots d_k$ in $\sigma' = d'_1 \dots d'_k$, potem je $\pi^{-1}\sigma\pi = (\pi^{-1}d_1\pi)(\pi^{-1}d_2\pi)\dots(\pi^{-1}d_k\pi)$. Problem je tako reduciran na dokaz, da obstaja π, da je $d'_j = \pi^{-1}d_j\pi$, ne pridemo do problemov, saj so cikli disjunktni. □

2 Podgrupe

V končni grupi red elementa deli red grupe (po Lagrangeevem izreku red $\langle x \rangle$ deli red grupe).

Trditev 2.1

Vse grupa reda manj kot 6 so Abelove.

Trditev 2.2

Za vse pare elementov $a, b \in G$ velja

$$\text{ord}(a) = \text{ord}(bab^{-1}) \quad \text{ter} \quad \text{ord}(ab) = \text{ord}(ba)$$

Trditev 2.3

Za $H, K \leq G$ velja

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$$

Trditev 2.4

Naj bo G končna ter $K, H \leq G$, da velja $K \subseteq H$. Potem velja

$$[G : K] = [G : H][H : K]$$

Trditev 2.5

Grupa, v kateri za vsak element x velja $x^2 = 1$ je Abelova.

Oris dokaza. Vsak element je svoj inverz ter velja $1 = (xy)^2 \iff xy = y^{-1}x^{-1}$. □

Trditev 2.6

Če je a edini element reda 2 v grupi G, potem je $a \in Z(G)$.

Oris dokaza. Za vsak $b \in G$ ima element bab^{-1} red 2, kar pomeni, da je enak a. □

Komentar 2.7

Produkt podgrup ni vedno podgrupa. Podgrupa je natanko tedaj, ko produkt komutira.

Naloga 2.8

Naj bosta H in K končni podgrupi grupe G. Pokaži, da vsak izmed naslednjih pogojev implicira, da je $|H \cap K| = \{1\}$:

- $|H|$ ter $|K|$ sta tuji.
- $|H| = |K| =$ praštevilo ter $H \neq K$.

Oris dokaza. $H \cap K$ je podgrupa H ter K ter velja Lagrangev izrek. □

Naloga 2.9

Naj bo G končna grupa in $H \leq G$. Pokaži, da obstajata $a, b \in G$, da $a, b, ab \notin H$ natanko tedaj, ko je $2 \cdot |H| < |G|$.

Oris dokaza. Očitno po manipulaciji

$$2 < \frac{|G|}{|H|} \iff 2 < [G : H] \iff 3 \leq [G : H].$$

□

Naloga 2.10

Klasificiraj vse podgrupe edinke diederske grupe D_{2n}.

Rešitev. Gotovo so vse grupe oblike $\langle r^d \rangle$ za $d \mid n$ edinke. Za lihe n so to vse edinke, za sode n pa imamo še $\langle r^2, s \rangle$ ter $\langle r^2, rs \rangle$.

Denimo, da podgrupa edinka ni podgrupa grupe prve oblike - sledi, da vsebuje nek element reda 2 (element oblike $r^i d$ ima gotovo red 2). Naj bo n lih. Ker so vsi elementi reda 2 konjugirani tako sledi, da podgrupa vsebuje vsaj n elementov reda 2, ker pa vsebuje še identiteto ima podgrupa tako $n+1$ elementov, zato je enaka celotni grupi. Naj bo n sod. Vsak element reda 2 je bodisi v odseku zD_{2n}, bodisi v odseku $(rz)D_{2n}$. Če prava podgrupa edinka vsebuje nek element reda 2 tako vsebuje vsaj $\frac{2n}{4}$ elementov reda 2. Zaključimo z opazovanjem kvocienta, ki ima red kvečjemu 4. □

3 Kvocientne strukture

3.1 Homomorfizmi

Trditev 3.1

Red slike elementa deli red elementa. Če je homomorfizem injektiven sta reda enaka.

3.2 Edinke

Definicija 3.2

Podgrupa N grupe G je *podgrupa edinka*, če za vsak $a \in G$ velja

$$aNa^{-1} \subseteq N.$$

Definicija edinke omogoča, da v množico odsekov grupe po edinki vpeljemo množenje predstavnikov, ki je dobro definirana operacija, ki naredi iz množice odsekov grupo, imenovana *kvocientna grupa*.

Trditev 3.3

Če sta $H, K \leq G$ je $HK = \{hk | h \in H, k \in K\}$ podgrupa G natanko tedaj, ko je $HK = KH$. Pogoj je gotovo izpolnjen, če je ena izmed H, K edinka.

Trditev 3.4

- Podgrupa indeksa 2 je edinka.
- Naj bo $a \in G$ reda 2. $\{1, a\}$ je edinka natanko tedaj, ko je $a \in Z(G)$.

Trditev 3.5

Naj bo N končna podgrupa grupe G. Če je N edina podgrupa reda $|N|$ je N edinka.

Oris dokaza. Ker je edina je enaka vsem konjugiranim podgrupam. □

Trditev 3.6

Center grupe G

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

je edinka.

$$G/Z(G) \quad \text{ciklična} \quad \Longrightarrow \ G \quad \text{Abelova.}$$

Oris dokaza. Vsak element G je oblike $t^k \cdot z$, kjer je $z \in Z(G)$ ter t, ki je generator $G/Z(G)$, saj odseki G po $Z(G)$ tvorijo particijo. □

Izrek 3.7: Cauchy

Naj bo $p \in \mathbb{P}$, da velja $p \mid |G|$. Potem ima G element reda p.

Izrek 3.8: O izomorfizmu

- Naj bo $\varphi : G \to H$ homomorfizem. Potem je
$$G/\ker(\varphi) \cong \mathrm{im}(\varphi)$$
- Naj bo $N \lhd G$ ter $H \leq G$. Potem je
$$H/(H \cap N) \cong HN/N$$
- Naj bo $M, N \lhd G$ ter $N \subseteq M$. Potem je
$$G/M \cong (G/N)/(M/N)$$

Izrek 3.9: Korespondenčni izrek

Naj bo $N \lhd G$

- Vsaka podgrupa grupe G/N je oblike H/N za $H \leq G$.
- Vsaka podgrupa edinka G/N je oblike M/N za $M \lhd G$ ter $N \subseteq M$.

Standardna protiprimera v teoriji grup sta:

Primer 3.10

$$K \leq H \times G \not\Rightarrow K = H_1 \times G_1 \quad \text{za} \quad H_1 \leq H, K_1 \leq K$$

Oris dokaza. $H = G = \mathbb{Z}$ ter $K = \langle 1, 1 \rangle$. Če bi bil $K = H_1 \times G_1$ bi H_1 ter G_1 vsak vsebovala celoten $\mathbb{Z}$, kar seveda ni res. □

Primer 3.11

$$N \lhd G \quad \text{Abelova ter} \quad G/N \quad \text{Abelova} \quad \not\Rightarrow \quad G \quad \text{Abelova.}$$

Naloga 3.12

Pokaži, da je podgrupa edinka generirana z množico X enaka podgrupi generirani z množico $\{gxg^{-1} | g \in G, x \in X\}$. Kot posledico pokaži, da je vsak element iz G enak produktu elementov konjugiranem nekem fiksnem elementu $x \neq 1$.

Definicija 3.13

- Grupa G je *enostavna*, če nima pravih netrivialnih edink.
- $M \lhd G$ je *maksimalna edinka*, če $M \neq G$ ter ne obstaja $N \lhd G$, da velja $M \subset N \subset G$.

Naloga 3.14

M je maksimalna edinka natanko tedaj, ko je G/M enostavna.

4 Direktne vsoti ter končne Abelove grupe

Trditev 4.1

Če sta $M, N \lhd G$ ter je $M \cap N = \{1\}$, potem elementi M in N komutirajo.

Oris dokaza. Komutator je v obeh. □

Trditev 4.2

$$Z_m \times Z_n \cong Z_{mn} \iff \gcd(m,n) = 1.$$

Trditev 4.3

Če je $|G| = mn$ Abelova grupa, kjer sta m ter n tuji, potem za podgrupi

$$H = \{x \in G | mx = 0\} \quad \text{ter} \quad K = \{x \in G | nx = 0\}$$

velja $G = H \oplus K$ ter $|H| = m; |K| = n$.

Oris dokaza. Po Bezoutovi lemi je $G = H + K$, obenem sta H in K disjunktni, zato velja $G = H + K$. Ustrezen red H in K preberemo po uporabi Cauchyjevega izreka. □

Z rekurzivno uporabo zgornje leme lahko ugotovimo, da je vsaka Abelova grupa reda $n = p_1^{k_1} \dots p_m^{k_m}$ direktna vsota grup, ki imajo zaporedoma red $p_i^{k_i}$

Trditev 4.4

Netrivialna p-grupa je ciklična natanko tedaj, ko ima eno samo podgrupo reda p.

Oris dokaza. Za p-ciklične grupe je ta grupa seveda natanko $p^{k-1}Z_{p^k}$. V nasprotnem primeru je edina podgrupa reda p jedro endomorfizma $\varphi(x) = px$. Z uporabo prvega izreka o izomorfizmu ter uporabo indukcijske predpostavke na kvocientu ugotovimo, da je začetna grupa ciklična. □

Izrek 4.5

Naj bo p praštevilo ter $k_1 \geq \dots \geq k_u$ naravna števila, prav tako $\ell_1 \geq \dots \geq \ell_v$, ter naj velja

$$\mathbb{Z}_{p^{k_1}} \oplus \mathbb{Z}_{p^{k_2}} \oplus \dots \oplus \mathbb{Z}_{p^{k_u}} = \mathbb{Z}_{p^{\ell_1}} \oplus \dots \oplus \mathbb{Z}_{p^{\ell_v}}.$$

Potem $v = u$ ter $k_i = \ell_i$ za vse $i \in \{1, \dots, v\}$.

Izrek 4.6

Vsaka Abelova grupa je direktna vsota cikličnih p-podgrup. Če je

$$G = C_1 \oplus C_2 \oplus \ldots \oplus C_k \quad \text{ter} \quad G = D_1 \oplus D_2 \oplus \ldots \oplus D_l,$$

kjer so $\{C_i\}$ ter $\{D_i\}$ ciklične grupa reda potenc praštevil je $k = l$ ter lahko s permutiranjem faktorjem dosežemo enakost razcepa.

Trditev 4.7

Denimo, da je grupa G notranji produkt svojih podgrup edink, ki so vse Abelove. Pokaži, da je G Abelova.

Oris dokaza. Za vsaki dve edinki $M, N \lhd G$ velja $M \cap N = \{1\}$, zato njuni elementi komutirajo. Tako element vsake izmed edink komutira z elementi ostalih edink. Ker element poljubne edinke komutira tudi z drugimi elementi te edinke sledi, da vsi elementi komutirajo, saj lahko poljuben element grupe G zapišemo kot produkt elementov edink. □

5 Delovanja grup

Definicija 5.1

Delovanje grupe G na množici X je preslikava $\cdot : G \times X \to X$, za katero velja

$$1_g \cdot x = x \quad \text{ter} \quad g_1 \cdot (g_2 \cdot x) = (g_1 g_2) \cdot x$$

Pojem je ekvivalenten homomorfizmu iz G v grupo $\mathrm{Sym}(X)$. Kanonična primera delovanja grupe na sebi sta *levo množenje* $g \cdot h = gh$ ter *konjugiranje* $g \cdot h = ghg^{-1}$.

Definicija 5.2

$$\mathrm{Orb}_x = G \cdot x = \{y \in X | \exists g \in G.\, y = gx\} \subseteq X$$
$$\mathrm{Stab}_x = G_x = \{g \in G | gx = x\} \leq G$$
$$\mathrm{Stab}_{gx} = g \cdot \mathrm{Stab}_x \cdot g^{-1}$$

Izrek 5.3: O orbiti in stabilizatorju

Za vse $x \in X$ je $|G \cdot x| = [G : G_x]$. Če je $|G| < \infty$ je

$$|G| = |\mathrm{Orb}_x| \cdot |\mathrm{Stab}_x|\,.$$

Oris dokaza. Definiramo preslikavo $a \cdot x \mapsto a\mathrm{Stab}_x$. Preverimo, da je dobro definirana ter injektivna, očitno je tudi surjektivna. Sledi, da je bijektivna. Zaključek sledi po Lagrangevem izreku. □

Izrek 5.4

Naj G deluje na končni množici X. Naj bo $Z = \{x \in X | gx = x \ \forall g \in G\}$ ter naj so $\{x_i\}_{i=1}^t$ predstavniki ekvivalenčnih razredov, ki so orbite velikosti vsaj 2. Potem je

$$|X| = |Z| + \sum_{i=1}^{t} |\mathrm{Orb}_{x_i}| = |Z| + \sum_{i=1}^{t} [G : G_{x_i}]$$

Oris dokaza. Ekvivalenčni razredi tvorijo particijo množice. □

Trditev 5.5

Naj končna p-grupa deluje na končni množici X. Potem $p \mid |X| - |Z|$

Oris dokaza. Če je $Z = X$ smo končali. Drugače so G_{x_j} prave podgrupe končne p-grupe, zato je njihov indeks netrivialen ter zato deljiv s p. □

Lema 5.6: Lema, ki ni Burnsideova

Končna grupa G deluje na končni množici X. Za vsak $g \in G$ definiramo $\mathrm{Fix}(g) = \{x \in X | gx = x\}$. Potem je

$$\#\text{ orbit} = \frac{1}{|G|} \sum_{g \in G} |\mathrm{Fix}(g)|$$

Oris dokaza. □

Izrek 5.7: Razredna formula

Naj bo G končna grupa, ter $C(x) = \{g \in G | gx = xg\} \leq G$. Tedaj velja

$$|G| = |Z| + \sum_{i=1}^{t} [G : C(x_j)],$$

kjer so $\{x_i\}_{i=1}^{t}$ predstavniki netrivialnih orbit.

Oris dokaza. G deluje na sami sebi z konjugiranjem. Sledi po zgornji trditvi. □

Trditev 5.8

Kot posledice prejšnje trditve dobimo:

- Končna netrivialna p-grupa ima netrivialen center.
- $|G| = p^2 \implies G$ Abelova.
- Če je G končna grupa in $p \mid |G|$, potem G vsebuje element reda p.

Oris dokaza. Prva in tretja točka sledita po indukciji na G ter razredni formuli. Če $p \nmid |Z(G)|$ potem nujno ne deli indeksa nekega centralizatorja, zato deli velikost centralizatorja, ki je netrivialen. Druga sledi iz prve. □

Definicija 5.9

Podgrupa $H \leq G$ je p-podgrupa Sylowa, če je $|H| = p^\ell$ ter $p^{\ell+1} \nmid |G|$.

Izrek 5.10: Sylow

- $p^\ell \mid |G| \implies G$ ima podgrupo reda p^ℓ (p-podgrupa Sylowa tako vedno obstaja).
- p-podgrupa G je vedno vsebovana v neki podgrupi Sylowa.
- Vsaki podgrupi Sylowa sta si konjugirani.
- $\#p$-podgrup Sylowa grupe G deli $|G|$.
- $\#p$-podgrup Sylowa je kongruentno $1 \pmod{p}$.

Oris dokaza. Prva točka: izvajamo indukcijo na $|G|$. Ločimo primera glede na to ali $p \mid Z(G)$. Če ne, potem isti argument z razredno formulo, ki pokaže, da ima končna netrivialna p-grupa netrivialen center. Če $p \mid Z(G)$ najdemo element c reda p v $Z(G)$. $\langle c \rangle$ je edinka v $Z(G)$. Tvorimo $Z(G)/\langle c \rangle$ in v njej najdemo podgrupo reda $p^{\ell-1}$, kar lahko storimo po indukcijski predpostavki. Korespondenčni izrek pove, da je ta podgrupa oblike $H/\langle c \rangle$, sledi, da ima H red p^ℓ. □

Definiramo $n_p = \#p$-podgrup Sylowa grupe G. To število je zanimivo, saj nam s svojimi lastnostmi omogoča dokazati, da grupa ni enostavna - ima netrivialno edinko. Za n_p velja

$$S \text{ je } p\text{-podgrupa Sylowa } G. \;\; S \lhd G \iff n_p = 1$$

Trditev 5.11

Grupa reda pq, kjer sta $p, q \in \mathbb{P}$ različni ni enostavna.

Oris dokaza. Naj bo $p < q$. Tako je $n_q = qm + 1$ ter $n_q \mid p$. Sledi, da je $n_p = 1$. □

Trditev 5.12

Grupa G reda pq, kjer $p < q$ ter $p \nmid q - 1$ je ciklična.

Oris dokaza. Velja $n_q = 1$, zato ima G edinko reda q. Ker $n_p \mid q$ je $n_p \in \{1, q\}$. Če bi veljalo $mp + 1 = n_p = q$ bi kršili deljivostni pogoj, zato je $n_p = 1$. Po Largrangevem izreku imata edinki redov p ter q trivialen presek, zato komutirata. Ker sta grupi redov p ter q ciklični lahko hitro izpeljemo, da ima produkt njunih generatorjev red pq. □

Trditev 5.13

Grupa reda p^2q, kjer $p \nmid q - 1$ ter $p < q$ je Abelova.

Oris dokaza. $n_p \mid q \implies n_p \in \{1, q\}$. Druga možnost bi kršila pogoj deljivosti, zato je $n_p = 1$. $n_q \mid p^2 \implies n_q \in \{1, p, p^2\}$. Obenem je $n_q = mq + 1$. Ker je $q > p$ možnost p odpade. Tako ostane le še $mq + 1 = n_q = p^2 \implies q \mid p^2 - 1$. $\implies q \mid p - 1$ ali $q \mid p + 1$, oboje odpade zaradi velikosti. Tako je $n_q = 1$.

G ima tako edinko M reda p^2 ter edinko N reda q. Njun produkt je ponovno podgrupa. Ker sta edinki sami podgrupi njunega produkta velja $|MN| = p^2q \implies MN = G$. Obenem je $M \cap N = \{1\}$, tako je G notranja direktna vsota Abelovih grup, zato Abelova. □

Trditev 5.14

Naj sta $H, K \leq G$, kjer je G končna grupa. Tedaj je

$$|HK| = \frac{|H|\,|K|}{|H \cap K|}.$$

Dokaz. Čeprav nam je formula že znana jo ponovno overimo z delovanji grup. Naj grupa $H \times K$ deluje na G z delovanjem $(h,k) \cdot g = hgk^{-1}$. Množica HK je tako orbita 1_G. Velja

$$|HK| = \frac{|H \times K|}{\mathrm{Stab}_x} = \frac{|H| \cdot |K|}{\{(h,k) \in H \times K | hk^{-1} = 1\}} = \frac{|H| \cdot |K|}{|H \cap K|}.$$

□

Naloga 5.15

Pokaži, da grupa reda 48 ni enostavna.

Oris dokaza. $n_2 \in \{1,3\}$ ter $n_3 = 1 \pmod 3$ ter $n_3 \mid 16 \implies n_3 \in \{1,4,16\}$. 2-podgrupa Sylowa ima red 16. Denimo, da obstajajo tri 2-podgrupe Sylowa, H, K, L. $|H \cap K| \mid 16$ ter

$$|HK| = \frac{|H|\,|K|}{|H \cap K|} = \frac{16^2}{|H \cap K|} \leq 48 \implies \frac{16}{3} \leq |H \cap K| \implies |H \cap K| = 8,$$

kjer zadnji sklep sledi, ker grupi H in K ne sovpadata. Opazimo, da je $H \cap K \leq H$ ter $H \cap K \leq K$, ker sta obe indeksa dva sta edinki. Tako je

$$|N_G(H \cap K)| \geq |H| + |K| - |H \cap K| = 24.$$

Če je $|N_G(H \cap K)| = 24$ imamo podgrupo indeksa 2, ki je edinka, zato G ni enostavna. Če je $|N_G(H \cap K)| = 48$ pa je $H \cap K$ edinka. □

Trditev 5.16

Naj bo G končna grupa in $H < G$. Če

$$|G| \nmid [G : H]!,$$

potem G ni enostavna.

Rešitev. Fakulteta nas spomni na obstoj grupe $\mathrm{Sym}(G : H)$. G deluje na množici odsekov G po H z levim množenjem. Tako obstaja homomorfizem iz G v $\mathrm{Sym}(G : H)$, jedro katerega je edinka. Pokažimo, da je nemogoče da je jedro trivialno ali polno. Če je $|\ker(\varphi)| = \{1\}$ je $|G| = |\mathrm{im}(\varphi)|$, slednja pa je podgrupa $\mathrm{Sym}(G : H)$, kar krši pogoj ne-deljivosti. Če je $\ker(\varphi) = G$ je $\varphi_g(xH) = xH = gxH$ za vse $g \in G$. V specifičnem primeru je $\varphi_g(1H) = gH = 1H$ za vse $g \in G$. Tako sledi, da je $g \in H$ za vse $g \in G$, kar je v prostislovju z $H < G$. □

Naloga 5.17

Naj bo $|G| = 2^k \cdot 3$ za $k \geq 2$. Pokaži, da G ni enostavna

Rešitev. 2-podgrupa Sylowa je reda 2^k ter indeksa 3. Ker za $k \geq 2$ ne velja $2^k \mid 3! = 6$ sledi, da G ni enostavna. □

Naloga 5.18

Naj bo $|G| = 2m$, kjer je m liho. Pokaži, da G ni enostavna.

Rešitev. Želeli bi epimorfizem $f : G \to \mathbb{Z}_2$, ker bi to impliciralo obstoj edinke reda 2. Levo množenje poda homomorfizem $\varphi : G \to \mathrm{Sym}(G)$. Po Cauchyjevem izreku ima G element a reda 2. Opazimo, da je permutacija σ_a pravzaprav le produkt transpozicij, saj nima fiksnih točk (sledi iz $\mathrm{ord}(a) = 2$). Teh transpozicij je m, tako je $\mathrm{sgn}(\sigma_a) = (-1)^m = -1$. Želen homomorfizem f je tako $f : G \to \mathrm{Sym}(G) \to \mathbb{Z}_2$, kjer druga puščica predstavlja homomorfizem sign. □

Naloga 5.19

Koliko p-podgrup Sylowa ima S_p?

Rešitev. Elementi reda p v S_p so natanko p-cikli oblike $(1, a_1, \ldots, a_{p-1})$, kjer so $\{a_i\}_{i=1}^{p-1}$ permutacija $\{2, \ldots, p-1\}$, katerih je natanko $(p-1)!$. Vsaka p-podgrupa (Sylowa) S_p ima $p-1$ elementov reda p, zato skupaj obstaja $\frac{(p-1)!}{p-1} = (p-2)!$ p-podgrup (Sylowa) v S_p. □

5.1 Kompozicijska vrsta

Definicija 5.20

$M \lhd G$ je *maksimalna edinka*, če $M \neq G$ ter ne obstaja $N \lhd G$, da velja $M \subset N \subset G$.

Končna netrivialna edinka ima gotovo maksimalno edinko, namreč edinko z maksimalnim redom.

Tvorimo verigo maksimalnih edink, oblike

$$\{1\} \lhd M_s \lhd \ldots \lhd M_1 \lhd G,$$

kjer so vse grupe oblike M_{j+1}/M_j enostavne, kot posledica korespondenčnega izreka.

Izrek 5.21: Jordan-Hölder

Če ima grupa G dve kompozicijski vrsti $\{M_i\}_{i=1}^{s}$ ter $\{N_i\}_{i=1}^{t}$ je $t = s$ ter obstaja $\sigma \in S_t$, da je

$$M_i/M_{i+1} \cong N_{\sigma(i)}/N_{\sigma(i)+1}$$

Trditev 5.22

A_n je enostavna za $n \geq 5$.

Oris dokaza. Če A_n vsebuje tricikel, potem vsebuje vse elemente. Preostane obravnava nekaj primerov. □

Definicija 5.23

Grupa G je *rešljiva*, če obstaja zaporedje edink

$$\{1\} \lhd M_1 \lhd \ldots \lhd G,$$

kjer je M_{i+1}/M_i Abelova grupa.

Trditev 5.24

Naj bo G rešljiva.

- Če je $H \leq G$ je H rešljiva.
- Če je $N \lhd G$ je G/N rešljiva.

Dokaz. Naj bo

$$\{1\} \lhd M_1 \cap H \lhd \ldots \lhd M_k \cap H = H.$$

$$\frac{M_{i+1} \cap H}{M_i \cap H} = \frac{M_{i+1} \cap H}{M_{i+1} \cap M_i \cap H} \cong \frac{(M_{i+1} \cap H)M_i}{M_i} \leq \frac{M_{i+1}}{M_i},$$

kjer je zadnja grupa Abelova, izomorfizem pa sledi iz drugega izreka o izomorfizmu.

Naj bo

$$\{1\} \lhd M_1N/N \lhd M_2N/N \lhd \ldots \lhd G/N.$$

Zaključek sedaj sledi iz tretjega izreka o izomorfizmu ter dejstvu, da je kvocient podgrupa Abelove grupe z Abelovo, zato tudi sama Abelova. □

Trditev 5.25

Naj bo $N \lhd G$. Če sta N ter G/N rešljivi, je tudi G rešljiva.

Trditev 5.26

Grupa reda p^k je rešljiva.

Rešitev. Grupa reda p je gotovo rešljiva, saj je Abelova, kar pomeni, da kompozicijska vrsta $\{1\} \lhd Z_p$ izpolni pogoj.

Denimo, da so vse grupe reda p^ℓ rešljive za $\ell < k$. Center p-grupe p^k je netrivialna edinka v grupi reda p^k, zato je edinka reda p^m, kvocient pa je grupa reda p^{k-m}. Po indukcijski predpostavki sta obe grupi rešljivi, zato je tudi grupa reda p^k rešljiva. □

Del II

Kolobarji

5.2 Ideali

Definicija 5.27

(Dvostranski) ideal kolobarja K je aditivna podgrupa K I, za katero za vsak $a \in K$ velja

$$aI \subseteq I \quad \text{ter} \quad Ia \subseteq I.$$

Definicija ideala omogoča, da v množico odsekov kolobarja po idealu vpeljemo seštevanje in množenje predstavnikov, ki sta dobro definirani operaciji, ki iz množice odsekov naredita kolobar, imenovan *kvocientni kolobar*.

Trditev 5.28

Če obravnavamo le enostranske ideale velja, da sta naslednji množici zaporedoma desni ter levi ideal matričnega kolobarja nad kolobarjem K

$$\begin{bmatrix} x & y \\ 0 & 0 \end{bmatrix} \quad \text{ter} \quad \begin{bmatrix} x & 0 \\ y & 0 \end{bmatrix}.$$

Trditev 5.29

Vsota, produkt ter presek idealov I in J je ideal, za katere velja

$$IJ \subseteq I \cap J \subseteq I, J \subseteq I + J.$$

Trditev 5.30

Naj sta I ter J ideala komutativnega kolobarja K, za katera velja $I + J = K$. Pokaži, da velja

$$IJ = I \cup J$$

Oris dokaza. Pogoj je ekvivalenten obstoju elementov i ter j, za katera velja $i + j = 1$. Pokažemo le inkluzijo $I \cup J$ v IJ. Velja $a \in I \cap J \implies a \cdot 1 = ai + aj \in I \cap J, \quad ai \in IJ \quad \text{ter} \quad aj \in IJ.$ □

Trditev 5.31

Naj bo D obseg. Potem je $M_n(D)$ enostaven kolobar.

Oris dokaza. Velja $E_{ij} \circ E_{kl} = \delta_{j=k} E_{il}$. Za neničelen element ideala lahko dobimo matrično enoto, z enko na mestu njegovega neničelnega elementa. Potem lahko z množenjem te matrične enote dobimo vse ostale matrične enote, kar nam da I, sledi, da je ideal enak $M_n(K)$. □

Trditev 5.32

Naj bo $I \lhd K_1 \times K_2$. Pokaži, da je $I = I_1 \times I_2$, za $I_i \lhd K_i$ za $i \in \{1, 2\}$.

Oris dokaza. Projeciramo I na obe komponenti ter dobimo kandidata za ideala I_1 ter I_2. Očitno njun produkt vsebuje I. Naj bo

$$(x, y) \in I_1 \times I_2 \implies \exists x' \in I_1 \wedge y' \in I_2 . (x, y') \in I \wedge (x', y) \in I.$$

Tako velja, da je

$$(1, y)(x, y') = (x, yy') \in I \quad \text{ter} \quad (x', y)(1, y') = (x', yy') \in I.$$

Sledi, da je

$$(x, yy') - (x', yy') = (x - x', 0) \in I \implies (x - x', 0) + (x', y) = (x, y) \in I,$$

kar smo želeli pokazati. □

Trditev 5.33

Množica nilpotentnih elementov kolobarja je ideal.

Trditev 5.34

Naj so $\{n_i\}$ paroma tuja števila, za katera velja $N = \prod_i n_i$. Preslikava $\varphi : \mathbb{Z}/nZ \to \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z}$ je izomorfizem kolobarjev, definiran z

$$\varphi(x \bmod N) = (x \bmod n_1, \ldots x \bmod n_k)$$