Vaje iz Algebre 2

Hugo Trebše (hugo.trebse@gmail.com)

23. marec 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

1 Podgrupe **3**

2 Kvocientne strukture **4**
2.1 Edinke 4
2.2 Ideali 6

3 Direktne vsoti ter končne Abelove grupe **8**

4 Delovanja grup **9**

5 Polinomi **13**

1 Podgrupe

Trditev 1.1

Vse grupa reda manj kot 6 so Abelove.

Trditev 1.2

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

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

Trditev 1.3

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

Trditev 1.4

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. □

2 Kvocientne strukture

2.1 Edinke

Definicija 2.1

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 2.2

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

Trditev 2.3

- 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 2.4

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

Trditev 2.5

Center grupe G

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

je edinka.

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

Izrek 2.6: Cauchy

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

Izrek 2.7: 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 2.8: 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 2.9

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

Primer 2.10

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

2.2 Ideali

Definicija 2.11

(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 2.12

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 2.13

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 2.14

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 2.15

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 2.16

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 2.17

Množica nilpotentnih elementov kolobarja je ideal.

Trditev 2.18

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

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

3 Direktne vsoti ter končne Abelove grupe

Trditev 3.1

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

Oris dokaza. Komutator je v obeh. □

4 Delovanja grup

Definicija 4.1

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 4.2

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

Izrek 4.3: 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 4.4

Naj G deluje na končni množici X. Naj bo $Z = \{x \in X \mid gx = x \ \forall g \in G\}$ 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 4.5

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 4.6: Dvomljivo Burnsideova lema

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

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

Oris dokaza. □

Izrek 4.7: Razredna formula

Naj bo G končna grupa, ter $C(x) = \{g \in G \mid gx = xg\} \leq G$. 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 4.8

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 sledi velikost centralizatorja, ki je netrivialen. Druga sledi iz prve. □

Definicija 4.9

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

Izrek 4.10: 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 4.11

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 4.12

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 4.13

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 4.14

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

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

□

5 Polinomi

Trditev 5.1

Polinom oblike $X^n + 1$ je nerazcepen nad $\mathbb{Q}$ natanko tedaj, ko je $n = 2^k$ za $k \geq 1$.

Oris dokaza. Očitno je razcepen v primeru, ko ima n lihi faktor. V primeru $n = 2^k$ upoštevamo, da je $X \mapsto X + 1$ avtomorfizem kolobarja polinomov nad $\mathbb{Q}$, zato je $p(X)$ nerazcepen natanko tedaj, ko je nerazcepen $p(X + 1)$. Tako velja

$$(X+1)^{2^k} + 1 = \sum_{i=1}^{2^k} \binom{2^k}{i} X^i + 2.$$

Sedaj lahko uporabimo Eisensteinov kriterij za $p = 2$. □

Nasvet : Nerazcepnost nad $\mathbb{Q}[X]$

- Eisensteinov kriterij (po možnosti skupaj z avtomorfizmom $\mathbb{Q}[X]$).
- Prevod na nerazcepnost nad $\mathbb{Z}_p[X]$.

Trditev 5.2

Naj so $a_0, \ldots, a_n \in \mathbb{Z}$ ter $p \nmid a_n$.

$$a_n X^n + \ldots + a_0 \text{ nerazcepen nad } \mathbb{Q}[X] \implies$$
$$(a_n \bmod p)X^n + \ldots + (a_0 \bmod p) \text{ nerazcepen nad } \mathbb{Z}_p[X]$$

Velja tudi kontrapozicija: če je polinom nerazcepen nad $\mathbb{Z}_p[X]$, potem je nerazcepen tudi nad $\mathbb{Q}[X]$.