Alg. strukture (nast. smjerovi) – predavanje 6. travnja 2026.

Na zadnjim predavanjima počeli smo dokazivati teorem karakterizacije direktne sume grupa [AS, Teorem 3.4, str. 33]. Ovdje ćemo dati više detalja negoli piše u [AS].

Teorem. *Neka je G grupa i neka su $G_i \leq G$, $i \in I$, neke njezine podgrupe za koje vrijede sljedeća tri uvjeta:*

(**1**) $G_i \trianglelefteq G$, $\forall i \in I$;
(**2**) $G_j \cap \langle \bigcup_{i \neq j} G_i \rangle = \{e\}$, $\forall j \in I$;
(**3**) $G = \langle \bigcup_I G_i \rangle$.

Tada je

$$G \cong \bigoplus_I G_i.$$

Dokaz. Prvo smo rekli kako BSO možemo uzeti da imamo konačno mnogo podgrupa G_i; tj., imamo neke podgrupe $G_1, \ldots, G_n \leq G$. Zatim smo definirali preslikavanje

$$\phi : G_1 \oplus \cdots \oplus G_n \to G, \quad \phi(g_1, \ldots, g_n) := g_1 \cdots g_n,$$

te smo pokazali da je to homomorfizam grupa. Pritom je kao važna činjenica, koja je korištena u argumentaciji, pokazano kako za bilo koje međusobno različite $i, j \in \{1, \ldots n\}$ te elemente $g_i \in G_i$ i $g_j \in G_j$ imamo

$$g_i g_j = g_j g_i. \qquad (\star)$$

Sada pokazujemo da je ϕ monomorfizam. To je detaljno napravljeno u [AS], pa to tamo pažljivo pročitajte.

Zapravo jedino mjesto u [AS] na kojemu su ispušteni neki detalji je dokaz surjektivnosti homomorfizma ϕ. Navedimo ih ovdje. Prvo, sjetimo se definicije grupe generirane nekim skupom [AS, Def. 1.17]. Neka je G bilo koja grupa i $S \subseteq G$ neki neprazan podskup. Želimo opisati $\langle S \rangle$, podgrupu od G generiranu sa S. Za to definirajmo S^{-1} kao skup svih inverza x^{-1} elemenata $x \in S$; tj. $S^{-1} = \{x^{-1} \mid x \in S\}$. Tvrdimo da je onda ($e$ je, kao uvijek, neutral u G):

$$\langle S \rangle = \{e\} \cup \{x_1 \cdots x_r \mid r \in \mathbb{N},\ x_i \in S \cup S^{-1}\}. \qquad (\triangle)$$

(To je [AS, Zad. 8, str. 14].) Za to pokazati označimo desnu stranu gornje jednakosti s D pa pokažimo da je $\langle S \rangle = D$. Tu treba vidjeti inkluziju $\langle S \rangle \subseteq D$ i zatim obratnu inkluziju $\langle S \rangle \supseteq D$. Za prvu od te dvije inkluzije dovoljno je vidjeti da je $D \leq G$ te da je $S \subseteq D$; što je jasno iz same Def. 1.17 u [AS]. Ali očito za svaki $s \in S$ je $s \in D$; i zato je $S \subseteq D$. Još pokažimo da je D podgrupa od G. U tu svrhu proizvoljan $y \in D$ napišimo kao $y = x_1 \cdots x_r$, gdje su $x_i \in S \cup S^{-1}$. No onda je $y^{-1} = x_r^{-1} x_{r-1}^{-1} \cdots x_1^{-1}$, što je očito također iz D. Znači da je D zatvoren za invertiranje! Nadaalje neka je uz gore dan y još dan i element $v = u_1 \cdots u_t \in D$, gdje su $u_i \in S \cup S^{-1}$. Onda je produkt

$$yv = x_1 \cdots x_r u_1 \cdots u_t$$

također iz D; po samoj definiciji skupa D jer su $x_i, u_j \in S \cup S^{-1}$. Znači da je D zatvoren i za množenje pa je po definiciji podgrupe doista $D \leq G$. Tako imamo inkluziju $\langle S \rangle \subseteq D$. Za obratnu inkluziju treba pokazati da je podgrupa D sadržana u **svakoj** podgrupi $H \leq G$ koja **sadrži** skup S; i onda ćemo, ponovo po Def. 1.17 u [AS], imati da je doista $D \subseteq \langle S \rangle$. Pa neka je $H \leq G$ t.d. je $S \subseteq H$. Ali onda,

posebno jer je H zatvorena za invertiranje, imamo da je $S \subseteq H$. A sada, ako su dani bilo koji elementi $x_1, \ldots, x_r \in S \cup S^{-1}$, koristeći činjenicu da je H zatvorena i za množenje, slijedi da je produkt $x_1 \cdots x_r$ iz H. No to pokazujee da je doista $D \subseteq H$, kako smo i tvrdili.

Konačno pokazujemo da je doista ϕ epimorfizam. Naime ako stavimo $S := G_1 \cup \cdots \cup G_n$, onda po uvjetu (**3**) i jednakosti ($\triangle$) imamo da je grupa $G = \langle S \rangle$ jednaka skupu svih produkata $x_1 \cdots x_r$, gdje su $x_i \in S$. (Važno je primijetiti da je sada $S = S^{-1}$, jer su sve G_i podgrupe od G pa su posebno zatvorene za invertiranje; tako da ako je $x \in G_i \subseteq S$, onda je i njegov inverz $x^{-1} \in G_i \subseteq S$.) Sada, neka je $y \in G$ proizvoljan element i napišimo ga kao produkt $y = x_1 \cdots x_r$, za neke $x_i \in S$. Koristeći činjenicu ($\star$) vidimo da taj zapis za y možemo preurediti tako da na početak zapisa stavimo sve faktore x_j koji su iz podgrupe G_1; na način da neki element iz podgrupe G_i može "izpreskakati sve elemente iz svih preostalih podgrupa G_j gdje $j \neq i$", onako kako je to bilo objašnjeno na zadnjim predavanjima. (Moguće da nema nikoji takav x_j, pa onda "zaboravimo na" G_1 i idemo gledati postoje li neki faktori koji su iz G_2.) Pritom treba naglasiti kako sam poredak svih faktora koji jesu iz G_1, i koje smo "nagurali na početak zapisa", **ne smijemo mijenjati**; jer općenito dva elementa iz G_1 ne komutiraju pri množenju. Recimo da od tih r faktora imamo neke $u_1^{(1)}, \ldots, u_{m_1}^{(1)}$ koji su svi iz G_1. Onda definiramo produkt $z_1 := u_1^{(1)} \cdots u_{m_1}^{(1)}$, svih tih elemenata, i primijetimo da je $z_1 \in G_1$. (Ako ne bi bio nikoji x_i iz G_1 stavimo $z_1 := e$.) Tako smo moguće "potrošili" neke x_i-ove pa sada one faktore koji su preostali označimo npr. kao $c_1, \ldots, c_p \in S$, gdje je $p \leq r$. Tako je zapravo $y = z_1 c_1 \cdots c_p$. A onda u produktu $c_1 \cdots c_p$ opet stvar preuredimo tako da sve faktore koji su iz G_2 stavimo na početak i produkt svih njih oznaačimo s $z_2 \in G_2$. Postupk nastavljamo! Tako nakon konačno mnogo koraka dolazimo do zapisa $y = z_1 z_2 \cdots z_n$, pri čemu su $z_i \in G_1$. (Kako smo rekli, moguće da su neki z_i-ovi jednaki neutralu e.) A sada iz tako dobivenih $z_1, \ldots, z_n$ napravimo n-torku

$$(z_1, \ldots, z_n) \in G_1 \oplus \cdots \oplus G_n$$

te primijetimo da je upravo $\phi(z_1, \ldots, z_n) = y$. Zaključak: doista je ϕ epi. Tako je teorem detaljno dokazan! □

Napomena. Instruktivno je pročitati Primjere 3.5 i 3.6 u [AS] koji zorno pokazuju kako se primjenjuje dokazani teorem kada želimo pokazati da je neka grupa izomorfna direktnoj sumi (konačno mnogo) svojih normalnih podgrupi; koje zadovoljavaju i uvjete (**2**) i (**3**) iz teorema.

!!! Materiju iz podtočke 3.2 u [AS] gotovo u potpunosti izostavljamo; tj., bilo bi pohvalno pročitati očemu se u njoj radi, no ona nije u programu predmeta Alg. strukture za nastavničke smjerove. Jedino ćemo malo kasnije spomenuti kao primjer važne serije konačnih nekomutativnih grupa tzv. diedralne grupe D_n, koje su definirane i opisane u **Primjeru 3.12** pa njega pročitajte (bez da trebate razumijeti što to znači da je "grupa D_n do na izomorfizam jednaka semidirektnom produktu cikličkih grupa $\mathbb{Z}/n\mathbb{Z}$ i $\mathbb{Z}/2\mathbb{Z}$).

Za predavanja mi nastavljamo s odjeljkom 4 u [AS]; stranica 43. Tu se podsjetimo definicija cikličke grupe i konačno generirane grupe, koje smo dali na nekom od prijašnjih predavanja. Prvo dokazujemo [AS, Teorem 4.1].

Teorem. (Strukturni teorem za cikličke grupe)
Neka je G ciklička grupa . Tada vrijedi sljedeće:

(i) *Svaka podgrupa $H \leq G$ je također ciklička.*
(ii) *Ili je $G \cong \mathbb{Z}$ ili je $G \cong \mathbb{Z}/n\mathbb{Z}$, za neki $n \in \mathbb{N}$.*
(iii) *Svaka homomorfna slika od G je ciklička; tojest, ako je $f : G \to H$ homomorfizam, onda je* $\operatorname{im} f$ *ciklička grupa.*

Dokaz. Dio (i) teorema detaljno je dokazan u [AS, str. 43,44], pa to pročitajte tamo. U samom argument koristi se dobro poznat teorem o dijeljenju s ostatkom u $\mathbb{Z}$. Navedimo ga ipak ovdje, poradi potpunosti izlaganja.

Teorem. *Neka su $n \in \mathbb{Z}$ i $m \in \mathbb{N}$. Tada* postoje*, i* jedinstveni su*, cijeli brojevi q i $0 \leq r < m$ takvi da je*

$$n = qm + r.$$

(Broj q je *kvocijent* a r je *ostatak* pri dijeljenju.)

I dio (ii) teorema je u [AS] detaljno argumentiran pa i to pročitajte tamo.

(iii) Neka je g generator grupe G; i onda je

$$G = \{g^k \mid k \in \mathbb{Z}\} = \{\ldots, (g^{-1})^2, g^{-1}, e, g, g^2, g^3, \ldots\}.$$

I onda je očito slika

$$\operatorname{im} f = f(G) = \{f(g^k) \mid k \in \mathbb{Z}\} = (\text{jer je } f \text{ homo.}) = \{(f(g))^k \mid k \in \mathbb{Z}\};$$

tj., $\operatorname{im} f$ je ciklička grupa s generatorom $f(g)$. □

Napomena. Primijetimo kako po tvrdnji (ii) gornjeg teoremu uvijek kada imamo neku cikličku grupu zapravo možemo uzeti da je ta grupa ili $\mathbb{Z}$ (ukoliko je ona beskonačna grupa) ili je ona $\mathbb{Z}/n\mathbb{Z}$ za neki $n \in \mathbb{N}_0$ (ukoliko je to konačna grupa). Tako se gotovo uvijek može jednostavnije rješavati razne zadatke s cikličkim grupama ili posebno provoditi neke račune.

Kao jednu direktnu posljedicu prethodnog teorema imamo ovaj korolar.

Korolar. *Ako je G ciklička grupa i H neka njezina (ciklička) podgrupa, onda je i kvocijentna grupa G/H također ciklička. Dakle,* **sve podgrupe i sve kvocijentne grupe cikličke grupe su također cikličke.**

Cikličke grupe su najjednostavnije grupe koje se pojavljuju u matematici, tj. u Teoriji grupa. Sljedeće po složenosti njihove strukture su konačno generirane komutativne grupe. O takvim grupama mi navodimo tek jedan važan rezultat u formi teorema, i to bez njegova dokaza. (Za napisati sve potrebne detalje trebalo bi prvo proučiti strukturu tzv. slobodnih komutativnih grupa a zatim bi se preko nekih pomoćih rezultata dobilo spomenuti teorem; što bi svakako uzelo nekoliko sati predavanja.)

Spomenuti je teorem u [AS] dan kao **Teorem 4.2**. On govori da se svaka konačno generirana komutativna grupa može do na izomorfizam opisati kao konačna direkta suma cikličkih grupa. Fraza "do na izomorfizam" znači da je svaka takva grupa izomorfna nekoj od grupa s niže dolje danim opisom; i zato de facto kad imamo posla s kon. generiranim komutativnim grupama uvijek možemo zamišljati da su

to grupe koje imaju jedan od tih opisanih oblika. A radi se o tome da ako je G neka kon. generirana komutativna grupa, onda je ona oblika

$$G \cong \left(\mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_t\mathbb{Z}\right) \oplus \mathbb{Z}^k;$$

gdje je $k \in \mathbb{N}_0$ a m_i-ovi su prirodni brojevi $m_1 > 1$ takvi da m_1 dijeli m_2, m_2 dijeli m_3,..., m_{t-1} dijeli m_t. I tu je jasno

$$\mathbb{Z}^k = \mathbb{Z} \oplus \cdots \oplus \mathbb{Z},$$

direktna suma od k primjeraka beskonačne cikličke grupe $\mathbb{Z}$.

Pritom se broj k zove **rang** grupe G a brojevi m_i su tzv. **invarijante** grupe G. Rang i invarijante $m_1, \ldots, m_t$ u potpunosti određuju strukturu grupe G.

Sjetimo se da smo bili definirali pojam tzv. **torzijske podgrupe** neke komutativne grupe G kao

$$\mathrm{tor}(G) := \{x \in G \mid \mathrm{ord}(x) < \infty\};$$

tj. $\mathrm{tor}(G)$ je skup svih elemenata iz G čiji je red konačan. Pokazali smo da je $\mathrm{tor}(G) \leq G$, podgrupa. Sada je jasno da je za grupu oblika

$$\left(\mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_t\mathbb{Z}\right) \oplus \mathbb{Z}^k$$

njezin torzijski dio jednak "prvom sumandu", tj.

$$\mathrm{tor}(G) = \mathbb{Z}/m_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/m_t\mathbb{Z};$$

to je konačna grupa i to reda $|\mathrm{tor}(G)| = m_1 m_2 \cdots m_t$. A "drugi sumand" je $\mathbb{Z}^k$; to je tzv. **slobodni dio** grupa G. Na taj način bi se **Teorem 4.2** mogao jednostavnije (ali i manje precizno) napisati kao

$$G \cong \mathrm{tor}(G) \oplus \mathbb{Z}^k.$$

U [AS] naveden je i **Teorem 4.2′**. U njemu je dan jedan malo drugačiji opis kako do na izomorfizam izgledaju sve kon. generirane komutativne grupe. To je opis preko tzv. Sylowljevih p-podgrupa. Ponekad je za neke argumente i račune pogodnije raditi s tim opisom grupa koje promatramo. Inače, jedan se opis u drugi lako provodi preko jednog jdnostavnog pomoćnog retzultata, Leme 4.4, na str. 44 u [AS]. Primijetite kako zapravo "prebacujemo jedan oblik u drugi" samo za spomenuti torzijski dio grupe G.

Predavanja o grupama završavaju s podtočkom **4.2 Nekomutativne grupe**. Cilj je u kratkim crtama de facto dati pregled nekih grupa koje smo prije definirali i/ili promatrali ili su pak one poznate iz linearne algebre (kao npr. ortogonalne grupe i unitarne grupe). Onošto treba znati je materija, zapravo tek definicije grupa, dana od početka spomenute podtočke pa uključno do primjera (4) na str. 46 u [AS]. Jasno, poželjno je barem informativno pročitati napisano u [AS] do kraja str. 51; ali to nije nešto što će se recimo pitati bilo na pismenim ili usmenim ispitima...

Onio što slijedi je drugi dio predmeta *Alg. strukture*, a to su osnove tzv. Teorije prstena...