UNIVERZITET U NOVOM SADU
PRIRODNO-MATEMATIČKI FAKULTET
DEPARTMAN ZA MATEMATIKU I INFORMATIKU

Igor Dolinka

PREDAVANJA IZ ALGEBRE 2

Novi Sad, decembar 2022.

Sadržaj

1

Primeri grupa

1.1 Definicija grupe

Neka je G neprazan skup i neka je $\cdot : G \times G \to G$ binarna operacija na njemu. Tada algebarsku strukturu $(G, \cdot)$ zovemo *grupoid*. Grupoidi mogu imati određena dodatna svojstva koja su od interesa za posebno proučavanje, na primer:

(i) Grupoid $(G, \cdot)$ je *asocijativan* ukoliko za sve $a, b, c, \in G$ važi

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

Asocijativni grupoidi se još zovu i *polugrupe*.

(ii) Grupoid $(G, \cdot)$ *ima jedinicu* ako postoji element $1 \in G$ (koji je, kao što se lako vidi, nužno jedinstven) tako da

$$1 \cdot a = a \cdot 1 = a$$

važi za sve $a \in G$. Polugrupe sa jedinicom se nazivaju *monoidi*.

(iii) Neka je $(G, \cdot)$ grupoid sa jedinicom 1. Za element $a \in G$ kažemo da je *invertibilan* ako postoji $b \in G$ tako da je

$$b \cdot a = a \cdot b = 1.$$

Za element b kažemo da je *inverz* elementa a. Veoma se lako pokazuje da je inverz elementa a, ako postoji, jedinstven, pa ima smisla da se taj inverz označi sa a^{-1} (budući da je on jednoznačno određen elementom a).

definicija grupe

Grupa je monoid u kojem je svaki element invertibilan; zbog toga je sa logičkog stanovišta najprirodnije definisati grupe kao algebarske strukture

$$(G, \cdot, {}^{-1}, 1)$$

(tipa $(2, 1, 0)$) koje zadovoljavaju identitete $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, $1 \cdot x = x \cdot 1 = x$ i $x^{-1} \cdot x = x \cdot x^{-1} = 1$. Međutim, u ovom tekstu mi nećemo praviti distinkciju između algebarske strukture i njenog nosača (skupa na kojem je definisana), te ćemo tako govoriti prosto "grupa G" podrazumevajući da su u svakoj takvoj situaciji operacije jasne iz konteksta; ovakav pristup je prilično uobičajen u klasičnoj algebri. Takođe, kada koristimo multiplikativnu notaciju – tj. simbol $\cdot$ za operaciju grupe – uobičajeno je da se on izostavlja i zamenjuje konkatenacijom (dopisivanjem) faktora, pa da se tako umesto $a \cdot b$ piše ab. (To naravno ne znači da se za operaciju u grupi ne koriste i drugi simboli, poput $+, *, \star, \circ, \dots$)

stepen elementa

Ovakav zapis u multiplikativnoj notaciji (koja je ipak najčešća) omogućava da se uvedu *stepeni* a^n elementa a grupe G, $n \in \mathbb{Z}$. Po definiciji će uvek biti $a^0 = 1$, dok je za $n > 0$,

$$a^n = \underbrace{aa \dots a}_{n}.$$

red elementa

Za negativne eksponente definišemo $a^{-n} = (a^{-1})^n$. Za datu grupu G i $a \in G$ može se dogoditi da je neki stepen elementa a jednak jedinici, $a^n = 1$. Ukoliko postoji, najmanji pozitivan ceo broj n sa ovom osobinom zovemo *red elementa* a u G i označavamo sa $o(a)$ (ili eventualno $o_G(a)$ ukoliko grupa G nije jasna iz konteksta). U suprotnom, ako takvo n ne postoji, kažemo da je element a *beskonačnog reda* i pišemo $o(a) = \infty$.

red grupe

Red grupe G je kardinal $|G|$. Prema tome, razlikujemo *konačne* i *beskonačne* grupe.

Komutativne grupe, tj. grupe G koje zadovoljavaju

$$ab = ba$$

Abelove grupe

za sve $a, b \in G$ zovemo *Abelove*[1] *grupe*. Sledeći tradiciju u teoriji grupa (ali i standardnu notaciju u nekim drugim fundamentalnim oblastima algebre, poput

[1] u čast velikog norveškog matematičara Nilsa Henrika Abela (1802-1829)

linearne algebre, ali i šire, u teoriji modula i prstena) ponekad se za Abelove grupe koristi aditivna notacija, tj. njihove operacije se najčešće označavaju simbolom $+$. U tom slučaju, inverz elementa a pišemo $-a$, "jedinica" grupe se zapravo označava sa 0, a stepeni elementa postaju njegovi umnošci (sa celim koeficijentima):

$$na = \underbrace{a + a + \cdots + a}_{n}.$$

Red elementa je sada najmanji pozitivan ceo broj n tako da je $na = 0$.

Sada ćemo rezimirati nekoliko elementarnih osobina grupa koje gotovo neposredno slede iz prethodnih definicija:

- U svakoj grupi G važi $(ab)^{-1} = b^{-1}a^{-1}$ za sve $a, b \in G$. pravilo "cipele-čarape"
- U svakoj grupi G važe zakoni kancelacije (skraćivanja), tj. za sve $a, x, y \in G$ imamo: kancelativnost

$$\begin{aligned} ax = ay \quad &\Rightarrow \quad x = y, \\ xa = ya \quad &\Rightarrow \quad x = y. \end{aligned}$$

- Neka je M monoid sa jedinicom 1. Tada skup $M^\times$ svih invertibilnih elemenata monoida M čini grupu (u odnosu na operaciju monoida). grupa invertibilnih elemenata monoida
- Neka je a element konačnog reda grupe G, $o(a) = n$. Tada važi $a^m = 1$ ako i samo ako $n \mid m$. Stoga, za sve $k \in \mathbb{Z}$ važi

$$o(a^k) = \frac{n}{(n, k)}.$$

1.2 Prvi primeri grupa

Najočigledniji primeri grupa nastaju od struktura (prstena i polja) koje formiraju skupovi brojeva. Najpre, ako je R proizvoljan prsten, tada je po definiciji $(R, +)$ Abelova grupa. Zbog toga su $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ primeri (beskonačnih) Abelovih grupa. grupe brojeva u odnosu na $+$

S druge strane, ako je R prsten sa jedinicom, tada je njegova multiplikativna struktura $(R, \cdot)$ monoid, pa skup $R^\times$ invertibilnih elemenata prstena R čini grupu u odnosu na množenje prstena. Tako je, na primer, $\mathbb{Z}^\times = \{1, -1\}$ 2-elementna grupa (ovde je 1 jedinica grupe invertibilnih elemenata, a -1 je element reda 2). U svakom polju je, međutim, svaki nenula element invertibilan, pa su tako $\mathbb{Q}^\times = (\mathbb{Q} \setminus \{0\}, \cdot)$, $\mathbb{R}^\times = (\mathbb{R} \setminus \{0\}, \cdot)$, $\mathbb{C}^\times = (\mathbb{C} \setminus \{0\}, \cdot)$ novi primeri beskonačnih Abelovih grupa. grupe brojeva u odnosu na $\cdot$

Primer 1.1. U elementarnoj teoriji brojeva, osnovna algebarska struktura sa kojom radimo je *prsten ostataka po modulu* n $(n \geq 2)$:

$$(\mathbb{Z}_n, +_n, \cdot_n),$$

čiji su elementi $\overline{0}, \overline{1}, \ldots, \overline{n-1}$, klase relacije ekvivalencije $\equiv \pmod{n}$ "kongruentno po modulu n", tzv. *klase ostataka* (npr. ako je $n = 26$, tada je $\overline{6} = \{\ldots, -46, -20, 6, 32, 58, \ldots\}$), dok su operacije $+_n$ i $\cdot_n$ redom sabiranje i množenje po modulu n. Aditivna grupa $(\mathbb{Z}_n, +_n)$ prstena ostataka po modulu n je primer konačne Abelove grupe. Ove grupe, zajedno sa $(\mathbb{Z}, +)$, zovemo *ciklične grupe*.

ciklične grupe

Primer 1.2. Nastavljajući se na prethodni primer, lako se pokazuje da je za $a \in \{1, \ldots, n-1\}$ klasa $\overline{a}$ invertibilna u $\mathbb{Z}_n$ ako i samo ako je $(a, n) = 1$; naime, invertibilnost $\overline{a}$ ekvivalentna je postojanju rešenja kongruencijske jednačine

$$ax \equiv 1 \pmod{n}.$$

grupa invertibilnih ostataka po modulu n

Tako je $|\mathbb{Z}_n^\times| = \varphi(n)$, gde je φ Ojlerova funkcija (koja prebraja pozitivne cele brojeve manje od n i uzajamno proste sa n). Upravo iz ovog razloga, prsten $\mathbb{Z}_n$ je polje ako i samo ako je n prost broj – upravo tada i samo tada je svaki nenula ostatak invertibilan.

Klajnova grupa V_4

Primer 1.3. Nad četvoroelementnim skupom $\{1, a, b, c\}$ definišimo grupu na sledeći način: neka je 1 jedinica, dok za preostala tri elementa važi

$$a^2 = b^2 = c^2 = 1,$$
$$ab = ba = c, \quad bc = cb = a, \quad ca = ac = b.$$

Lako se proverava da se na ovaj način dobija jedna Abelova grupa (u kojoj je svaki element inverzan samom sebi) koju zovemo *Klajnova*[2] *četvorna grupa* V_4.

grupa kvaterniona Q_8

Primer 1.4. Evo jednog primera konačne nekomutativne grupe kojeg je otkrio irski matematičar ser Vilijem Rouen Hamilton (1805–1865) šetajući se Dablinom 16. oktobra 1843. Hamilton je, naime, tragao za uopštenjem kompleksnih brojeva "u više dimenzija". Primetimo da je polje kompleksnih brojeva $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$ u izvesnom smislu zasnovano na grupi koju čine $1, -1, i, -i$ (u kojoj su elementi $i, -i$ reda 4 pošto je $i^2 = (-i)^2 = -1$, dok je -1 reda 2, $(-1)^2 = 1$). Hamilton je neko vreme bezuspešno pokušavao da

[2] po nemačkom matematičaru Feliksu Klajnu (Felix Klein, 1849–1925)

nađe 3-dimenzionalno uopštenje kompleksne ravni i kompleksnih brojeva, pa se zatim okrenuo pokušajima da to učini u četiri dimenzije. Tokom šetnje je iznenada došao do otkrića, pa je perorezom uklesao na ogradu mosta Brum na Kraljevskom kanalu sledeću formulu (koja se i danas može videti):

$$i^2 = j^2 = k^2 = ijk = -1.$$

Reč je o koncizno zapisanim definicionim relacijama *grupe kvaterniona* Q_8 čiji su elementi simboli $1, -1, i, -i, j, -j, k, -k$, pri čemu je

$$\begin{gathered} i^2 = j^2 = k^2 = -1, \quad (-1)^2 = 1 \\ ij = k, \quad jk = i, \quad ki = j, \quad ji = -k, \quad kj = -i, \quad ik = -j, \\ (-1)x = x(-1) = -x \ \text{(za sve } x, \text{ pri čemu je } -(-x) = x) \end{gathered}$$

Sada se *telo* (ne nužno komutativan prsten sa jedinicom u kojem je svaki nenula element invertibilan) *kvaterniona* dobija od skupa svih elemenata oblika

$$a + bi + cj + dk,$$

$a, b, c, d \in \mathbb{R}$, pri čemu se, pored množenja koeficijenata u polju realnih brojeva, primenjuju međusobna množenja elemenata $1, i, j, k$ iz grupe Q_8.

Za radoznalce

Ono što je Hamilton zapravo pokušavao da pronađe bila je asocijativna invertibilna algebra konačne dimenzije nad poljem realnih brojeva $\mathbb{R}$, a koja bi bila različita od jedine dve takve do tada poznate strukture: samog $\mathbb{R}$, i $\mathbb{C}$. Naime, *asocijativna algebra* je algebarska struktura A koja je vektorski prostor nad nekim poljem F, ali koja pri tome ima definisanu i operaciju množenja elemenata koja je asocijativna (tako da je A istovremeno i prsten) i bilinearna u odnosu na struktru vektorskog prostora. Potreba da se nađe takva struktura proizašla je iz želje da se razvije matematički aparat koji bi modelirao određene pojave u fizici elektromagnetizma. Posle neuspešnih pokušaja da se nađe takva algebra dimenzije 3, Hamilton je pokušao da konstruiše primer dimenzije 4, i tako je "rođena" algebra kvaterniona, čiju bazu čine $1, i, j, k$.

Dosta kasnije, F. G. Frobenius je 1877. dokazao svoju čuvenu teoremu: $\mathbb{R}, \mathbb{C}$ i algebra kvaterniona $\mathbb{H}$ su *jedine* konačno-dimenzionalne asocijativne invertibilne algebre nad poljem realnih brojeva (koje su redom dimenzije 1,2,4, prve dve komutativne, treća nekomutativna). Nije ni čudo što se Hamilton toliko mučio da pronađe primer, kada su kvaternioni zapravo jedini netrivijalan primer koji je matematički moguć! Ovaj rezultat ima dalje značajne posledice u topologiji i funkcionalnoj analizi, u klasifikaciji normiranih algebri i topoloških prstena. Frobeniusova teorema

1.3 Grupe permutacija i simetrija

Primer 1.5. Neka je X proizvoljan neprazan skup. Označimo sa $\mathcal{T}_X$ skup svih funkcija $X \to X$, tj. svih *transformacija* skupa X. Kompozicija funkcija (data sa $(f \circ g)(x) = g(f(x))$ za sve $x \in X$) je naravno asocijativna operacija, pa $\mathcal{T}_X$ zapravo čini monoid u odnosu na kompoziciju sa jedinicom id_X, *pun monoid transformacija na* X. Naravno, transformacija $f : X \to X$ invertibilna (tj. postoji transformacija g tako da je $f \circ g = g \circ f = \mathrm{id}_X$) ako i samo ako je f bijekcija, odnosno *permutacija* skupa X. Grupu invertibilnih elemenata $\mathcal{T}_X^\times$ označavamo sa $\mathbb{S}_X$ i zovemo *simetrična grupa* na skupu X. Ukoliko je skup X konačan, $|X| = n$, umesto $\mathbb{S}_X$ koristimo notaciju $\mathbb{S}_n$ za simetričnu grupu *stepena* n. Permutacije n-elementnog skupa ćemo ređe pisati u Košijevoj notaciji (kao $2 \times n$ matricu čiji se prvi red sastoji od originala, a drugi od odgovarajućih slika), a češće kao proizvode disjunktnih ciklusa (npr. $(12)(345)$).

simetrična grupa

U praksi se često dešava da skup X ima neku dodatnu matematičku strukturu, te da bismo želeli da posmatramo ne baš sve permutacije skupa X, već da se ograničimo samo na one koje na izvestan način korespondiraju sa tom strukturom. Evo jednog tipičnog primera.

Primer 1.6. Neka je $M = (X, d)$ metrički prostor. Permutacija f skupa X je *izometrija* prostora M ako čuva rastojanje u M, tj. za sve $x, y \in X$ važi

$$d(f(x), f(y)) = d(x, y).$$

Lako se pokazuje da je kompozicija dve izometrije ponovo izometrija, kao i da je za svaku izometriju f prostora M, f^{-1} takođe izometrija. Zbog toga sve izometrije prostora M čine grupu koju označavamo sa $\mathrm{Iso}(M)$. U slučaju da je $M = \mathbb{R}^n$, $n \geq 1$, sa uobičajenim euklidskim rastojanjem

grupa izometrija

$$d(x, y) = \sqrt{(x_1 - y_1)^2 + \cdots + (x_n - y_n)^2}$$

za sve $x = (x_1, \ldots, x_n)^T$, $y = (y_1, \ldots, y_n)^T$, tada odgovarajuću grupu izometrija ozančavamo sa $E(n)$; ovo je tzv. n-dimenzionalna *Euklidova grupa*.

Primer 1.7. Nastavljajući se na prethodni primer, neka je $\Phi \subseteq X$ *figura* u M (proizvoljan skup tačaka metričkog prostora). Za izometriju $f \in \mathrm{Iso}(M)$ kažemo da je *simetrija* figure Φ ako je $f(\Phi) = \Phi$. Ponovo se lako pokazuje da sve simetrije date figure Φ čine grupu, $\mathrm{Sym}(\Phi)$, koja je sadržana (kao podgrupa) u $\mathrm{Iso}(M)$.

grupa simetrija figure

Za radoznalce

Na primer, ako je M euklidski prostor dimenzije n (tako da je $\mathrm{Iso}(M) = E(n)$), tada grupu simetrija figure koja se sastoji od jedne jedine tačke (recimo, koordinatnog početka P) nazivamo *ortogonalna grupa* dimenzije n i označavamo je sa $O(n)$. Nije teško pokazati da se $O(n)$ zapravo poklapa sa grupom simetrija proizvoljne sfere (u slučaju $n = 2$, kruga) sa centrom u P. U slučaju $n = 2$, grupa $O(2)$ se sastoji od svih rotacija oko tačke P i osnih simetrija u odnosu na prave koje sadrže P. Od ovih transformacija u ravni, primetimo da rotacije čuvaju orijentaciju, dok je osne simetrije obrću, tako da rotacije same čine *grupu rotacija* ili tzv. *specijalnu ortogonalnu grupu* $SO(2)$. Koncept specijalne ortogonalne grupe može se uopštiti na više dimenzija (kroz grupu simetrija koordinatnog početka koje čuvaju orijentaciju), pa tako dobijamo grupe $SO(n)$. Na primer, još je Ojler pokazao da se grupa $SO(3)$ sastoji od svih prostornih rotacija oko prava koje sadrže koordinatni početak, dok je već struktura grupe $SO(4)$ znatno složenija. Ove grupe imaju fundamentalni značaj u teorijskoj fizici, a naročito u fizici elementarnih čestica.

ortogonalna grupa

specijalna ortogonalna grupa

Primer 1.8. Neka je Π_n pravilan n-tougao u ravni (bez ograničenja opštosti, neka je njegov centar baš u koordinatnom početku P). Grupu njegovih simetrija $\mathrm{Sym}(\Pi_n)$ (koja je sadržana u $O(2)$) zovemo *dijedarska grupa* stepena n i označavamo je kraće sa D_n. Grupa D_n je konačna; zapravo, važi $|D_n| = 2n$. Naime, ako je ρ rotacija oko koordinatnog početka za ugao $\frac{2\pi}{n}$, a σ osna simetrija u odnosu na pravu koja sarži koordinatni početak i jedno teme poligona, tada su svi elementi grupe D_n sledeći:

dijedarska grupa

$$\mathrm{id}_{\mathbb{R}^2}, \rho, \rho^2, \dots, \rho^{n-1}, \sigma, \sigma\rho, \sigma\rho^2, \dots, \sigma\rho^{n-1}.$$

Primetimo da važi $\rho^n = \mathrm{id}_{\mathbb{R}^2}$ (tako da je $\rho^{-1} = \rho^{n-1}$), zatim $\sigma^2 = \mathrm{id}_{\mathbb{R}^2}$ (σ je sama sebi inverzna), i, konačno, lako se pokazuje da je

$$\rho\sigma = \sigma\rho^{-1} = \sigma\rho^{n-1}.$$

Ove relacije između simetrija ρ i σ (koje generišu D_n) u izvesnom smislu (koji se precizno može definisati tek u tzv. *kombinatornoj teoriji grupa* [LSch77, MKS66]) u potpunosti "određuju" dijedarsku grupu D_n.

Za radoznalce

Evo skice dokaza koji pokazuje korektnost liste izometrija u ravni koje čine dijedarsku grupu. Neka su temena posmatranog poligona $A_1, \dots, A_n$i neka je σ, na primer, osna simetrija u odnosu na pravu PA_1. Najpre tvrdimo da su sve izometrije navedene u gornjem primeru različite. Zaista $\rho^k(A_1) = \rho^k(\sigma(A_1)) = A_{k+1}$, što odmah povlači da za $j \neq k$ važi $\rho^j \neq \rho^k$, $\rho^j \neq \sigma\rho^k$ i $\sigma\rho^j \neq \sigma\rho^k$; tako, preostaje da pokažemo da je $\rho^k \neq \sigma\rho^k$. Međutim, ovo je očigledno pošto je $\sigma(A_2) = A_n$ i $\rho^k(A_2) = A_{k+2}$ (gde je po potrebi A_{n+1} druga oznaka za A_1), a $\rho^k(A_n) = A_k$.

Dokažimo sada da Π_n nema drugih simetrija. Neka je, dakle, $\tau \in D_n$. Najpre, očigledno je da svaka simetrija od Π_n fiksira P, zbog čega je $\tau(P) = P$. Takođe, slika svakog temena mora biti teme poligona i, štaviše, slika svake strane poligona (tj. para susednih temena) je strana poligona. Iskoristimo poznati stav iz euklidske geometrije da je svaka izometrija u ravni jednoznačno određena slikama bilo koje tri nekolinearne tačke, pa zato posmatrajmo sliku $\triangle PA_1A_2$. Po prethodnim primedbama, mora biti $\tau(\triangle PA_1A_2) = \triangle PA_kA_{k+1}$ za neko k, tako da je ili

$$\tau(A_1) = A_k, \quad \tau(A_2) = A_{k+1},$$

ili

$$\tau(A_1) = A_{k+1}, \quad \tau(A_2) = A_k.$$

Međutim, primetimo da i ρ^{k-1} zadovoljava prvi od ova dva uslova, pa u tom slučaju mora biti $\tau = \rho^{k-1}$. S druge strane, i izometrija $\sigma\rho^k$ zadovoljava potonji uslov, kada mora biti $\tau = \sigma\rho^k$. To znači da smo pronašli sve simetrije od Π_n, tj. sve elemente grupe D_n.

1.4 Grupe matrica

Neka je α linearna transformacija tj. endomorfizam vektorskog prostora V konačne dimenzije n nad poljem F. Pretpostavimo da smo fiksirali jednu bazu $e_1, \ldots, e_n$ prostora V. Posmatrajmo slike ovih baznih elemenata u odnosu na α; tada postoje koeficijenti $a_{ij} \in F$, $1 \leq i, j \leq n$, tako da važi

$$\alpha(e_j) = \sum_{i=1}^{n} a_{ij} e_i.$$

Tada, ako uzmemo proizvoljan vektor $x = x_1e_1 + \cdots + x_ne_n$, dobijamo

$$\alpha(x) = \sum_{j=1}^{n} x_j \alpha(e_j) = \sum_{j=1}^{n} x_j \sum_{i=1}^{n} a_{ij} e_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{n} a_{ij} x_j \right) e_i,$$

što znači da ako svaki element x gornjeg oblika identifikujemo sa vektor-kolonom $(x_1, \ldots, x_n)^T$, tada α poprima oblik

$$\alpha(x) = Ax,$$

gde je $A = (a_{ij})$. Pri tome, ako endomorfizmu β odgovara matrica B, tada je

$$(\alpha \circ \beta)(x) = \beta(\alpha(x)) = BAx,$$

odakle sledi da je $\mathrm{End}(V)$, monoid endomorfizama od V, izomorfan sa *punim matričnim monoidom* $\mathcal{M}_n(F)$ svih matrica formata $n \times n$ nad poljem F (putem izomorfizma $\alpha \mapsto A^T$, gde je matrica A na malopre opisan način dobijena iz α, jer se tada $\alpha \circ \beta$ slika u $(BA)^T = A^T B^T$). U tom izomorfizmu, grupa invertibilnih elemenata $\mathrm{End}(V)^\times = \mathrm{Aut}(V)$ (tj. *grupa automorfizama* od V) odgovara kolekciji svih matrica nad F čija je determinanta invertibilni element u F (u slučaju polja, bilo koji nenula element). Dakle, radi se o grupi svih regularnih (invertibilnih) $n \times n$ matrica, koju zovemo *opšta linearna grupa* i označavamo sa $GL_n(F)$.

opšta linearna, specijalna linearna i afina grupa

Ako se ograničimo samo na matrice čija je determinanta jednaka 1, dobijamo podgrupu od $GL_n(F)$ koju zovemo *specijalna linearna grupa*, u oznaci $SL_n(F)$. S druge strane, opšte linearne grupe možemo smestiti u "širi kontekst" *afinih grupa* $AGL_n(F)$ koje se sastoje od svih transformacija na F^n oblika

$$x \mapsto Ax + b,$$

gde je $A \in GL_n(F)$ i $b \in F^n$. Specijalno, sve izometrijske transformacije euklidske ravni, odnosno prostora (koordinatizovane u odnosu na npr. standardnu bazu) sadržane su u $AGL_2(\mathbb{R})$, odnosno $AGL_3(\mathbb{R})$, respektivno.

Za radoznalce

Regularna realna matrica A je *ortogonalna* ako je njen inverz jednak njenoj transponovanoj matrici, $A^{-1} = A^T$. Sve ortogonalne matrice čine grupu (sadržanu u $GL_n(\mathbb{R})$) koju označavamo sa $O'(n)$ Opet ako se ograničimo samo na ortogonalne matrice čija je determinanta jednaka 1, dobijamo grupu (sadržanu u $SL_n(\mathbb{R})$) koju označavamo sa $SO'(n)$.

grupa ortogonalnih matrica

Neka je α linearna transformacija euklidskog prostora $\mathbb{R}^n$. Tada α, naravno, fiksira koordinatni početak, jer je $\alpha(0) = 0$. Može se pokazati da α definiše izometriju u odnosu na euklidsku metriku ako i samo ako je pridružena matrica $A \in GL_n(\mathbb{R})$ (matrica A takva da je $\alpha(x) = Ax$) ortogonalna. Zbog toga se pomenuti izomorfizam $\mathrm{Aut}(\mathbb{R}^n) \to GL_n(\mathbb{R})$ restrikuje na izomorfizam ortogonalne grupe $O(n)$ i grupe ortogonalnih matrica $O'(n)$ (što objašnjava ime grupe). Iz analognih razloga, imamo izomorfizam $SO(n)$ i $SO'(n)$.

S druge strane, regularna kompleksna matrica je *unitarna* ako je njen inverz jednak njenoj kompleksno konjugovanoj transponovanoj matrici: $A^{-1} = \overline{A}^T$. Ponovo nije teško pokazati da sve unitarne matrice čine grupu koju označavamo sa $U(n)$, dok grupu koja se sastoji od svih unitarnih matrica sa determinantom 1 označavamo sa $SU(n)$. Ove grupe su redom sadržane u $GL_n(\mathbb{C})$ i $SL_n(\mathbb{C})$.

grupa unitarnih matrica

2

Osnovni koncepti teorije grupa

2.1 Podgrupe

Ako je $(G, \cdot)$ grupa, podskup $H \subseteq G$ koji takođe čini grupu (u odnosu na restrikciju $\cdot|_{H\times H}$ operacije $\cdot$ polazne grupe G) zovemo *podgrupa* grupe G, i pišemo $H \leq G$. Svaka grupa G ima dve *trivijalne podgrupe*: to su sama grupa G i $E = \{1\}$. Gotovo se neposredno vidi da za $H \subseteq G$ važi $H \leq G$ ako i samo ako je skup H zatvoren na operacije grupe G, tj. ako za sve $a, b \in H$ važi $ab \in H$, $a^{-1} \in H$, kao i $1 \in H$.

podgrupa

Operacije date grupe lako se proširuju na njene podskupove. Naime, ako je $A, B \subseteq G$, definišemo

$$AB = \{ab : \ a \in A, \ b \in B\},$$

kao i

$$A^{-1} = \{a^{-1} : \ a \in A\}.$$

Lako se pokazuje da je množenje podskupova asocijativno, tj. važi $(AB)C = A(BC)$ za sve $A, B, C \subseteq G$, kao i formula za inverz proizvoda, $(AB)^{-1} = B^{-1}A^{-1}$. U ovoj notaciji, imamo nekoliko “konciznih” karakterizacija podgrupa.

karakterizacije podgrupa

Propozicija 2.1. *Neka je G grupa i H njen neprazan podskup. Tada je uslov $H \leq G$ ekvivalentan sa svakim od sledećih uslova:*

(1) $HH = H$ *i* $H^{-1} = H$.

(2) $HH = H$ *i* $HH^{-1} = H$.

(3) $HH^{-1} = H$.

(4) $HH^{-1} \subseteq H$.

Dokaz. Uslov (1) jasno važi za svaku podgrupu. Implikacije (2)⇒ (3)⇒(4) su trivijalne, a i implikacija (1)⇒(2) sledi neposredno. Prema tome, preostaje da pokažemo da uslov (4) implicira da je H podgrupa od G.

Zaista, pretpostavka (4) daje da $ab^{-1} \in H$ za sve $a, b \in H$. Specijalno, tada je $1 = aa^{-1} \in H$, a takođe i $b^{-1} \in H$ za sve $b \in H$. Zbog toga, pretpostavka $a, b \in H$ povlači

$$ab = a(b^{-1})^{-1} \in H,$$

pa zaključujemo da je H zatvoreno na operacije grupe G. □

2.2 Podgrupe i generatorni skupovi

Propozicija 2.2. *Neka je* $\{H_i : i \in I\}$ *proizvoljna neprazna familija podgrupa grupe* G. *Tada je i* presek familije podgrupa je ponovo podgrupa

$$H = \bigcap_{i \in I} H_i$$

takođe podgrupa od G.

Dokaz. Kako za sve $i \in I$ važi $1 \in H_i$, sledi da $1 \in H$. Pretpostavimo sada da $a, b \in H$. Tada $a, b \in H_i$ za sve $i \in I$, pa $ab, a^{-1} \in H_i$ za sve $i \in I$. Zbog toga, $ab, a^{-1} \in H$, pa sledi da je $H \le G$. □

Zahvaljujući ovoj osobini, možemo lako uvideti da za svaki podskup $A \subseteq G$ postoji najmanja podgrupa od G (u smislu skupovne inkluzije) koja sadrži A; naime, to je

$$\bigcap_{A \subseteq H \le G} H.$$

Za ovu podgrupu kažemo da je *generisana skupom* A, i označavamo je sa $\langle A \rangle$. podgrupa generisana skupom

Sledeće tvrđenje daje opis elemenata podgrupe generisane nekim podskupom grupe.

opis elemenata podgrupe generisane skupom A

Propozicija 2.3. *Neka je G grupa i $A \subseteq G$. Tada je $\langle \varnothing \rangle = E$, dok je u slučaju da je A neprazan skup*

$$\langle A \rangle = \{a_1^{\varepsilon_1} \dots a_n^{\varepsilon_n} : \ n \geq 1 \ a_i \in A, \ \varepsilon_i \in \{1, -1\} \text{ za sve } 1 \leq i \leq n\}.$$

Dokaz. Najpre, neposredno se uočava da svaka podgrupa od G koja sadrži sve elemente iz A mora da sadrži i sve elemente navedene na desnoj strani gornje jednakosti.

S druge strane, skup sa desne strane određuje podgrupu od G. Zaista, proizvod dva konačna proizvoda elemenata skupa A i njihovih inverza je ponovo proizvod istog tipa. Dalje, posmatrani skup sadrži $1 = aa^{-1}$ (za prozivoljno $a \in A$). Najzad, inverz proizvoljnog elementa posmatranog skupa

$$(a_1^{\varepsilon_1} \dots a_n^{\varepsilon_n})^{-1} = a_n^{-\varepsilon_n} \dots a_1^{-\varepsilon_1}$$

je ponovo u tom skupu. □

Kada je A konačan skup, $A = \{a_1, \dots, a_n\}$, uobičajeno je da se u zapisu podgrupe genrisane sa A skupovne zagrade izostave i da se piše $\langle a_1, \dots, a_n \rangle$.

Ukoliko je $\langle A \rangle = G$ kažemo da je A *generatorni skup* grupe G. Grupa je *konačno generisana* ako ima konačan generatorni skup.

2.3 Koseti i indeks podgrupe

koseti

Neka je $H \leq G$ i $g \in G$. Skup oblika $H\{g\}$ (koji kraće pišemo Hg) zovemo *desni koset* podgrupe H. Analogno definišemo i *levi koset* gH podgrupe H u G.

Lema 2.4. *Neka je $H \leq G$ i $a, b \in G$. Tada važi:*

(i) $Ha = Hb$ *ako i samo ako* $ab^{-1} \in H$;

(ii) $aH = bH$ *ako i samo ako* $a^{-1}b \in H$.

Dokaz. Dokazujemo samo tačku (i), pošto je druga tačka analogna. Ako je $Ha = Hb$ tada je $Hab^{-1} = Hbb^{-1} = H$, tj. za sve $h \in H$ važi da $hab^{-1} \in H$. Specijalno, za $h = 1$ dobijamo željeni rezultat $ab^{-1} \in H$.

Obratno, za sve $h \in H$ važi $Hh = H$; zaista, $Hh \subseteq HH = H$, dok obratna inkluzija sledi iz jednakosti $g = g(h^{-1}h) = (gh^{-1})h \in Hh$ za proizvoljno $g \in H$. Prema tome, ako je $ab^{-1} \in H$, tada je $Hab^{-1} = H$, pa je $Hb = Hab^{-1}b = Ha$. □

Propozicija 2.5. *Desni (levi) koseti podgrupe H grupe G čine particiju skupa G.*

Dokaz. Svaki element $g \in G$ je ujedno i element koseta Hg, jer $1 \in H$; zbog toga je unija svih desnih koseta jednaka G. Dokažimo još da su različiti desni koseti disjunktni. Zaista, pretpostavimo da $Ha \cap Hb \neq \varnothing$. Tada postoji $c \in Ha \cap Hb$, pa je

$$c = h_1 a = h_2 b$$

za neke $h_1, h_2 \in H$. Sledi da je $ab^{-1} = h_1^{-1} h_2 \in H$, pa je po prethodnoj lemi $Ha = Hb$. Tvrđenje za leve kosete sledi analogno. □

Jasno, sama podgrupa H jeste istovremeno desni i levi koset: $H = H1 = 1H$. Primetimo da je ona jedini desni ili levi koset koji je podgrupa od G.

Propozicija 2.6. *Neka je G grupa, $a, b \in G$ i $H \leq G$. Tada je $|Ha| = |bH| = |H|$.*

svi koseti su iste kardinalnosti

Dokaz. Preslikavanje $\psi : H \to Ha$ definisano sa $\psi(h) = ha$ je "1-1" zbog kancelativnosti, a takođe je i "na", pa je ψ bijekcija. Analogno se dokazuje i $|bH| = |H|$. □

Propozicija 2.7. *Neka je G grupa i $H \leq G$. Tada je*

svaka podgrupa ima jednako mnogo levih i desnih koseta

$$|\{Hg : g \in G\}| = |\{gH : g \in G\}|.$$

Dokaz. Definišimo preslikavanje $\psi : \{Hg : g \in G\} \to \{gH : g \in G\}$ tako da je

$$\psi(Hg) = g^{-1}H$$

za proizvoljno $g \in G$. Pre svega, radi se o dobro definisanoj funkciji, jer $Ha = Hb$ imlicira $a^{-1}H = (Ha)^{-1} = (Hb)^{-1} = b^{-1}H$. Budući da važi i obratno, ψ je injektivno, a takođe je i "na" jer je $\psi(Hg^{-1}) = gH$. Prema tome, ψ je bijekcija. □

Upravo prethodna propozicija motiviše definiciju *indeksa* $(G : H)$ podgrupe H u G kao kardinala $|\{Hg : g \in G\}|$.

indeks podgrupe

Teorema 2.8 (Lagranž)**.** *Za svaku grupu G i njenu podgrupu H važi*

Lagranžova teorema

$$|G| = (G : H)|H|.$$

Dokaz. Fiksirajmo skup $T = \{g_i : i \in I\}$ koji sadrži tačno po jedan element iz svakog desnog koseta podgrupe H (ovakve skupove zovemo *desne transverzale* grupe G u odnosu na H). Očito, $|T| = (G : H)$. Definišimo preslikavanje $\psi : T \times H \to G$ sa

$$\psi(g_i, h) = hg_i.$$

Kako za proizvoljno $a \in G$ imamo da važi $a \in Hg_i$ za neko (zapravo, tačno jedno) $i \in I$, to je ψ "na". Pretpostavimo, dalje, da je $h_1 g_i = \psi(g_i, h_1) = \psi(g_j, h_2) = h_2 g_j$. Tada koseti Hg_i i Hg_j nisu disjunktni, pa mora biti $Hg_i = Hg_j$. Međutim, po izboru skupa T sledi da je $i = j$, tj. $g_i = g_j$. Zbog toga je $h_1 = h_2$, pa je ψ "1-1", odnosno bijekcija. □

Posledica 2.9. *Neka je G konačna grupa, $H \leq G$ i $g \in G$. Tada $|H| \mid |G|$ i $o(g) \mid |G|$.*

Ojlerova i mala Fermaova teorema

Posledica 2.10. *(1)* (Ojlerova teorema) *Neka je $n \geq 1$ prirodan broj i $a \in \mathbb{Z}$ takav da je $(a, n) = 1$. Tada je*

$$a^{\varphi(n)} \equiv 1 (\mathrm{mod}\ n).$$

(2) (Mala Fermaova teorema) *Ako je p prost broj i $a \in \mathbb{Z}$ takav da $p \nmid a$ tada je*

$$a^{p-1} \equiv 1 (\mathrm{mod}\ p).$$

Dokaz. (1) Posmatrajmo grupu $\mathbb{Z}_n^\times$ invertibilnih ostataka po modulu n u odnosu na operaciju množenja. Već smo zaključili da je ostatak r element ove grupe ako i samo ako $(r, n) = 1$, zbog čega je $|\mathbb{Z}_n^\times| = \varphi(n)$. Dakle, po datim uslovima, ostatak $\overline{a}$ broja a po modulu n pripada $\mathbb{Z}_n^\times$. Po prethodnoj posledici, $o(\overline{a}) \mid \varphi(n)$, tj. $\varphi(n) = o(\overline{a})k$ za neko celo k. Sada u $\mathbb{Z}_n^\times$ važi

$$\overline{a}^{\varphi(n)} = \overline{a}^{o(\overline{a})k} = (\overline{a}^{o(\overline{a})})^k = 1.$$

Drugim rečima, $a^{\varphi(n)} \equiv 1 (\mathrm{mod}\ n)$.

(2) Ovo je specijalan slučaj prethodne tačke, pošto za proste brojeve p važi $\varphi(p) = p - 1$. □

2.4 Homomorfizmi, izomorfizmi

Neka su $(G, \cdot)$ i $(H, *)$ grupe (zbog lakšeg praćenja sledećih definicija koristimo različite oznake za operacije ovih grupa). Za preslikavanje $\phi : G \to H$ kažemo da je *homomorfizam* ako za sve $a, b \in G$ važi

homomorfizam grupa

$$\phi(ab) = \phi(a) * \phi(b).$$

Ukoliko je pri tome preslikavanje ϕ bijekcija, kažemo da je ϕ *izomorfizam* grupa G i H, a ove grupe su tada *izomorfne*, što pišemo $G \cong H$. Izomorfne grupe sa algebarskog stanovišta smatramo identičnim: jedina razlika između izomorfnih grupa G i H je zapravo u različitim imenima njenih elemenata i operacija, ali su svi odnosi, algebarska strukturna svojstva ista, tj. tablica grupe H se dobija prostim preimenovanjem (u skladu sa bijekcijom ϕ) elemenata iz tablice grupe G.

izomorfizam grupa

Lako se pokazuje da za svaki homomorfizam mora biti $\phi(1_G) = 1_H$ kao i $\phi(a^{-1}) = (\phi(a))^{-1}$ za sve $a \in G$, pri čemu je inverz sa leve strane uzet u grupi G, a sa desne u grupi H.

Za proizvoljan homomorfizam $\phi : G \to H$ definišemo njegovu *sliku*

slika i jezgro homomorfizma

$$\operatorname{Im} \phi = \phi(G)$$

kao i njegovo *jezgro*

$$\operatorname{Ker} \phi = \{a \in G : \ \phi(a) = 1_H\}.$$

Po samoj definiciji, slika svakog homomorfizma jeste podgrupa od H.

Injektivni homomorfizam se još naziva i *potapanje*: reč je zapravo o izomorfizmu G i neke podgrupe od H. U slučaju kada je $(G, \cdot) = (H, *)$ govorimo o *endomorfizmima* grupe G – homomorfimima G u samu sebe. Bijektivni endomorfizmi su *automorfizmi* grupe G: u pitanju su zapravo "simetrije" same grupe G kao matematičkog objekta (koje čuvaju njenu algebarsku strukturu, i te simetrije takođe čine grupu $\operatorname{Aut}(G) \leq \mathbb{S}_G$ – *grupu automorfizama* od G.

grupa automorfizama

Primer 2.11. Grupe $(\mathbb{R}^+, \cdot)$ i $(\mathbb{R}, +)$ su izomorfne: preslikavanje $\phi : \mathbb{R}^+ \to \mathbb{R}$ definisano sa

$$\phi(x) = \ln x$$

je bijekcija i dobro je poznato pravilo za logaritme $\ln(xy) = \ln x + \ln y$.

Primer 2.12. Neka je $n \geq 1$ prirodan broj i

$$\varepsilon = e^{\frac{2\pi i}{n}} = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}.$$

Tada skup kompleksnih brojeva $\{\varepsilon^k :\ 0 \leq k \leq n-1\}$ u odnosu na množenje čini grupu koja je izomorfna cikličnoj grupi $\mathbb{Z}_n$: lako se pokazuje da je

$$\phi : \varepsilon^k \mapsto \overline{k}$$

izomorfizam (zahvaljujući tome što je $e^{2\pi i} = 1$). Specijalno, grupa koja se sastoji od $1, i, -1, -i$ pomenuta u Primeru 1.4 izomorfna je cikličnoj grupi $\mathbb{Z}_4$.

Primer 2.13. Posmatrajmo kompleksne matrice

$$I = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Ako E označava jediničnu matricu, lako se proverava da važi

$$I^2 = J^2 = K^2 = -E$$

kao i

$$IJ = K,\ JK = I,\ KI = J,\ JI = -K,\ KJ = -I,\ IK = -J.$$

Zbog toga, matrice $E, -E, I, -I, J, -J, K, -K$ čine grupu, a $1 \mapsto E$, $i \mapsto I$, $j \mapsto J$ i $k \mapsto K$ definiše izomorfizam sa grupom kvaterniona Q_8. Primetimo da sve ove matrice imaju determinantu jednaku 1, tako da smo našli izomorfnu "fotokopiju" grupe kvaterniona unutar specijalne linearne grupe $SL_2(\mathbb{C})$.

Kao što ćemo videti iz narednog tvrđenja, multiskup redova elemenata grupe je invarijanta u odnosu na izomorfizme. Stoga analiza tog multiskupa može biti korisno sredstvo u pokazivanju da dve grupe nisu izomorfne, naročito u slučaju konačnih grupa.

Lema 2.14. *Neka je $\phi : G \to H$ izomorfizam grupa. Tada za sve $a \in G$ važi:*

(i) Ako je a konačnog reda onda je $o(a) = o(\phi(a))$.

(ii) Ako je a beskonačnog reda, onda je to i $\phi(a)$.

Posledica 2.15. *(i)* $V_4 \ncong \mathbb{Z}_4$.

(ii) $D_3 \cong \mathbb{S}_3 \ncong \mathbb{Z}_6$.

(iii) $D_4 \ncong Q_8$.

Dokaz. (i) U grupi V_4 svi nejedinični elementi su reda 2, dok u $\mathbb{Z}_4$ postoji element reda 4 (naime, ostatak 1 po modulu 4).

(ii) Direktno se proverava da je preslikavanje $\phi : D_3 \to \mathbb{S}_3$ dato sa

$$\phi(\sigma^i \rho^j) = (23)^i (123)^j,$$

$i \in \{0, 1\}$, $j \in \{0, 1, 2\}$, izomorfizam. Drugi deo tvrđenja sledi iz činjenice da $\mathbb{Z}_6$ ima element reda 6, što nije slučaj sa $\mathbb{S}_3$.

(iii) Direktnom proverom utvrđujemo da D_4 ima 1 element reda 1, 5 elemenata reda 2 i 2 elementa reda 4, dok Q_8 sadrži po jedan element reda 1 i 2, i 6 elemenata reda 4. $\square$

2.5 Ciklične grupe

Teorema 2.16. *Grupa G ima jednoelementni generatorni skup ako i samo ako je ciklična (tj. izomorfna sa $\mathbb{Z}_n$ za neko $n \geq 1$, ili sa $\mathbb{Z}$).* karakterizacija cikličnih grupa

Dokaz. Najpre, primetimo da sve ciklične grupe imaju jednoelementni generatorni skup: u svim slučajevima to je ostatak 1 (po modulu n), odnosno ceo broj 1.

Zato pođimo od pretpostavke da je $G = \langle a \rangle$ grupa sa jednoelementnim generatornim skupom. Razmatramo dva slučaja. Ako je a konačnog reda, $o(a) = n$, tada se G sastoji iz elemenata

$$1, a, \ldots, a^{n-1}$$

koji su svi različiti (jednakost bilo koja dva različita elementa iz ovog niza bi bila u kontradikciji sa redom elementa a). Zato je preslikavanje $\phi : G \to \mathbb{Z}_n$ definisano sa $\phi(a^k) = k$ za sve $0 \leq k < n$ izomorfizam. U suprotnom, a je beskonačnog reda, pa se po prethodnoj propoziciji G sastoji od elemenata a^n, $n \in \mathbb{Z}$, koji ponovo moraju biti svi različiti. Sada je preslikavanje $\phi : G \to \mathbb{Z}$ definisano sa $\phi(a^n) = n$ za sve $n \in \mathbb{Z}$ izomorfizam grupa. $\square$

Zbog ove teoreme, od sada ćemo sve grupe sa jednoelementnim generatorom zvati *cikličnim grupama*.

Generalno, možemo primetiti da se u proizvoljnoj grupi G i za bilo koje $a \in G$ red elementa $o(a)$ poklapa sa redom $|\langle a \rangle|$ podgrupe od G generisane sa a. Ova primedba odmah daje sledeća dva rezultata.

Posledica 2.17. *Neka je $1 \leq k < n$. Tada $\mathbb{Z}_n = \langle \overline{k} \rangle$ ako i samo ako je $(k, n) = 1$; prema tome, ciklična grupa $\mathbb{Z}_n$ ima tačno $\varphi(n)$ jednoelementnih generatora. S druge strane, 1 i -1 su jedini jednoelementni generatori grupe celih brojeva $\mathbb{Z}$.*

$\mathbb{Z}_p$ je jedina grupa reda p

Posledica 2.18. *Svaka grupa prostog reda je ciklična. Tako, za svaki prost broj p, grupa $\mathbb{Z}_p$ je do na izomorfizam jedina grupa reda p.*

Dokaz. Neka je $|G| = p$ i $a \in G$, $a \neq 1$. Tada $o(a) \mid p$, pa pošto je $o(a) \neq 1$ sledi da je $o(a) = p$. Zbog toga je $G = \langle a \rangle$, tj. G je ciklična grupa (koja je generisana svakim svojim nejediničnim elementom), $G \cong \mathbb{Z}_p$. □

podgrupe ciklične grupe

Teorema 2.19. *Svaka podgrupa ciklične grupe je ciklična. Pri tome:*

(i) U $\mathbb{Z}_n$ klasa $\overline{k}$ generiše podgrupu izomorfnu sa $\mathbb{Z}_d$, gde je $d = n/(k, n)$. Podgrupe od $\mathbb{Z}_n$ su u bijektivnoj korespondenciji sa pozitivnim deliteljima broja n.

(ii) Sve podgrupe od $\mathbb{Z}$ su oblika $n\mathbb{Z} = \langle n \rangle$, gde je n pozitivan ceo broj.

Dokaz. Razmotrimo najpre konačnu cikličnu grupu $\mathbb{Z}_n$. Neka je

$$H = \{\overline{0}, \overline{r_1}, \dots, \overline{r_{m-1}}\}$$

neka njena podgrupa i $0 < r_1 < \cdots < r_{m-1} < n$. Najpre tvrdimo da $r_1 \mid n$. Zaista, u suprotnom važi $n = qr_1 + r'$ za neko $0 < r' < r_1$; no, tada $\overline{qr_1} \in H$, a za $r' = n - qr_1 \in H$ klasa $\overline{r'}$ je inverz elementa $\overline{qr_1}$ (jer je $\overline{qr_1} +_n \overline{r'} = 0$), što je kontradikcija sa minimalnošću r_1. Dalje, tvrdimo da je $H = \langle \overline{r_1} \rangle$. Jasno, mora biti $\langle \overline{r_1} \rangle \subseteq H$, pa H mora da sadrži sve klase oblika $\overline{kr_1}$, $1 \leq k < n/r_1$. Ako bi H sadržao neku klasu $\overline{r_i}$ koji nije ovog oblika tada bismo imali

$$r_i = q'r_1 + r''$$

za neko $0 < r'' < r_1$, odakle sledi da za $r'' = r_i - q'r_1$ važi $\overline{r''} \in H$, kontradikcija. Dakle, $H = \{\overline{kr_1} : 0 \leq k < n/r_1\}$, što znači da je $m = n/r_1$ i $H \cong \mathbb{Z}_m$. Obratno, za svaki delitelj $d \mid n$, klasa $\overline{n/d}$ određuje (jedinstvenu) podgrupu od $\mathbb{Z}_n$ izomorfnu sa $\mathbb{Z}_d$.

Neka je sada H (netrivijalna) podgrupa od $\mathbb{Z}$. Slično kao u slučaju konačnih cikličnih grupa, neka je n najmanji pozitivan broj koji pripada H. Tada jasno $n\mathbb{Z} \leq H$. S druge strane, ako bi postojao $k \in H \setminus n\mathbb{Z}$ tada bismo imali

$$k = qn + r$$

za neko $0 < r < n$, pa bi zaključak $r = k - qn \in H$ vodio u kontradikciju. Prema tome, $H = n\mathbb{Z} = \langle n \rangle$. □

2.6 Neke značajne podgrupe

Primer 2.20. *Centar grupe* G je skup svih onih elemenata G koji komutiraju sa svim elementima grupe G, dakle, centar grupe

$$Z(G) = \{g \in G : \ gx = xg \text{ za sve } x \in G\}.$$

Nije teško uočiti da je $Z(G)$ uvek podgrupa od G. Zaista, $1 \in Z(G)$. Dalje, ako $a, b \in Z(G)$ i $x \in G$ je proizvoljno, tada $abx = axb = xab$, pa $ab \in Z(G)$. Takođe, $a^{-1}x = a^{-1}(xa)a^{-1} = a^{-1}(ax)a^{-1} = xa^{-1}$, tj. $a^{-1} \in Z(G)$.

U izvesnom smislu, centar grupe meri koliko je grupa G "daleko" od toga da bude Abelova; očigledno važi da je G Abelova ako i samo ako je $G = Z(G)$. Drugi ekstrem nastaje kada je $Z(G) = E$; tada kažemo da je grupa G *bez centra*.

Primer 2.21. Za $a, b \in G$ definišemo *komutator* elemenata a, b (pri čemu je poredak bitan) sa: komutator

$$[a, b] = a^{-1}b^{-1}ab.$$

Naziv potiče od toga što $[a, b]$ u izvesnom smislu izražava "razliku" elemenata ab i ba (slično kao u prstenima), budući da očito važi $ab = ba[a, b]$.

Podgrupa grupe G generisana svim njenim komutatorima zove se *komutatorska* ili *izvodna grupa* od G: izvodna podgrupa

$$G' = \langle [a, b] : \ a, b \in G\rangle$$

Budući da je inverz svakog komutatora ponovo komutator,

$$[a, b]^{-1} = (a^{-1}b^{-1}ab)^{-1} = b^{-1}a^{-1}ba = [b, a],$$

sledi da se izvodna podgrupa G' sastoji od svih konačnih proizvoda komutatora u G. U odnosu na izvodu podgrupu, Abelove grupe su sada karakterisane uslovom $G' = E$.

Primer 2.22. Neka je G grupa i $X \subseteq G$. Definišemo *centralizator* skupa X u G kao skup svih elemenata G koji komutiraju sa svim elementima iz X: centralizator

$$C(X) = \{g \in G : \ gx = xg \text{ za sve } x \in X\}.$$

Ukoliko je potrebno naglasiti u kojoj grupi posmatramo centralizator, pišemo ga i kao $C_G(X)$; ako je $X = \{x\}$ tada centralizator označavamo prosto sa $C(x)$. Slično kao i u slučaju centra se lako pokazuje da je $C(X) \leq G$; zapravo, centar grupe je specijalan slučaj centralizatora, naime $Z(G) = C(G)$ je centralizator cele grupe G.

2.7 Normalne podgrupe

normalna podgrupa

Za podgrupu H grupe G kažemo da je *normalna*, u oznaci $H \trianglelefteq G$, ako za sve $g \in G$ važi

$$gH = Hg,$$

tj. ako se svaki levi koset od H poklapa sa odgovarajućim desnim kosetom.

prosta grupa

Grupa G je *prosta* ako ne sadrži netrivijalne normalne podgrupe (različite od E i G, koje su uvek normalne).

Primer 2.23. Svaka podgrupa Abelove grupe je normalna. Obrat ovog tvrđenja ne važi: na primer, u grupi kvaterniona Q_8 svaka podgrupa je normalna, ali Q_8 nije Abelova.

S druge strane, postoje podgrupe koje nisu normalne. Na primer, posmatrajmo najmanju neabelovu grupu $\mathbb{S}_3 \cong D_3$ i njenu (cikličnu) podgrupu $H = \langle(12)\rangle$. Tada je $(13)H = \{(13),(132)\} \neq \{(13),(123)\} = H(13)$, pa H nije normalna u $\mathbb{S}_3$.

Primer 2.24. Centar grupe $Z(G)$ je uvek normalna podgrupa od G, budući da po samoj definiciji centra važi $ga = ag$ za sve $g \in G$, $a \in Z(G)$, pa je $gZ(G) = Z(G)g$.

Lema 2.25. *Ako je $H \leq G$ i $(G : H) = 2$ tada je $H \trianglelefteq G$.*

Dokaz. Koseti podgrupe H su $gH = H = Hg$ ako je $g \in H$, a u suprotnom, ako je $g \notin H$, tada imamo $gH = G \setminus H = Hg$. Prema tome, $H \trianglelefteq G$. □

Primer 2.26. U dijedarskoj grupi D_n, rotacije $\mathrm{id}_{\mathbb{R}^2}, \rho, \ldots, \rho^{n-1}$ čine (cikličnu) podgrupu R takvu da je $(D_n : R) = 2$. Zbog toga je $\mathbb{Z}_n \cong R \trianglelefteq D_n$

Evo jednog tvrđenja koje proveru normalnosti podgrupe čini nešto operativnijom.

karakterizacije normalnih podgrupa

Propozicija 2.27. *Neka je $H \leq G$. Tada su sledeći uslovi ekvivalentni:*

(1) $H \trianglelefteq G$.

(2) $g^{-1}Hg = H$ *za sve* $g \in G$.

(3) $g^{-1}Hg \subseteq H$ *za sve* $g \in G$.

Dokaz. Ako je $H \trianglelefteq G$ tada je $gH = Hg$ pa je $H = g^{-1}gH = g^{-1}Hg$. Implikacija (2)⇒(3) je trivijalna. Konačno, pretpostavimo da je $g^{-1}Hg \subseteq H$ za sve $g \in G$. Tada za neki fiksirani element $g \in G$, osim $g^{-1}Hg \subseteq H$, važi i $gHg^{-1} = (g^{-1})^{-1}Hg^{-1} \subseteq H$. Otuda važi $H = g^{-1}(gHg^{-1})g \subseteq g^{-1}Hg$, pa je $H = g^{-1}Hg$, tj. važi uslov (2). Iz njega se lako zaključuje da je $Hg = g(g^{-1}Hg) = gH$. □

Posledica 2.28. *Za svaku grupu G je $G' \trianglelefteq G$.*

Dokaz. Neka su $a, b, g \in G$ proizvoljni. Tada je

$$g^{-1}[a,b]g = (g^{-1}a^{-1}g)(g^{-1}b^{-1}g)(g^{-1}ag)(g^{-1}bg) = [g^{-1}ag, g^{-1}bg],$$

pa je $g^{-1}G'g \subseteq G'$. Po prethodnoj propoziciji, $G' \trianglelefteq G$. □

2.8 Direktni proizvodi

Neka su G_1, G_2 grupe. Posmatrajmo direktan proizvod skupova $G_1 \times G_2 = \{(a,b) : a \in G_1, b \in G_2\}$ i na njemu definišimo operaciju sa

$$(a,b)(a',b') = (aa', bb')$$

za sve $a, a' \in G_1$, $b, b' \in G_2$, pri čemu se na prvoj koordinati primenjuje operacija grupe G_1, a na drugoj operacija grupe G_2. Na ovaj način je definisana nova grupa, *direktan proizvod* $G_1 \times G_2$, čija je jedinica $(1_{G_1}, 1_{G_2})$, dok je inverz dat sa $(a,b)^{-1} = (a^{-1}, b^{-1})$, pri čemu se opet na prvoj koordinati uzima inverz u grupi G_1, a na drugoj u grupi G_2. direktan proizvod

Rutinski se pokazuju sledeća tvrđenja.

Lema 2.29. *(1)* $|G_1 \times G_2| = |G_1| \cdot |G_2|$.

(2) $o_{G_1 \times G_2}(g,h) = [o_{G_1}(g), o_{G_2}(h)]$.

(3) $Z(G_1 \times G_2) = Z(G_1) \times Z(G_2)$.

Definišemo *projekcije* direktnog proizvoda $G = G_1 \times G_2$ sa projekcije

$$\pi_1(G) = \{(a, 1_{G_2}) : a \in G_1\} \text{ i } \pi_2(G) = \{(1_{G_1}, b) : b \in G_2\}.$$

Zapravo, ovo su slike endomorfizama π_1, π_2 proizvoda $G_1 \times G_2$ definisanih sa $\pi_1(a,b) = (a, 1_{G_2})$ i $\pi_2(a,b) = (1_{G_1}, b)$ za sve $a \in G_1, b \in G_2$.

osobine projekcija

Propozicija 2.30. *Neka je $G = G_1 \times G_2$.*

(1) $\pi_i(G) \trianglelefteq G$ i $\pi_i(G) \cong G_i$ za $i = 1, 2$,

(2) $\pi_1(G)\pi_2(G) = G$,

(3) $\pi_1(G) \cap \pi_2(G) = E$.

Dokaz. (1) Važi $(c, b)^{-1}(a, 1_{G_2})(c, b) = (c^{-1}ac, 1_{G_2}) \in \pi_1(G)$ za sve $a, c \in G_1$, $b \in G_2$; izomorfizam $\pi_1(G) \cong G_1$ je dat sa $\phi : (a, 1_{G_2}) \mapsto a$, $a \in G_1$. Isto postupamo i za drugu projekciju.

(2) sledi iz $(a, b) = (a, 1_{G_2})(1_{G_1}, b)$, a (3) je očigledno. □

Inspirisan prethodnom propozicijom, prirodno se postavlja sledeći problem: ako je data grupa G, kada se ona može "razložiti" u direktan proizvod svojih podgrupa, tj. kada je $G \cong A \times B$ za neke $A, B \leq G$? Iz prethodnoj se vidi da tada A, B moraju biti normalne podgrupe od G koje zajedno generišu G, a presek im je trivijalan. Zbog toga kažemo da je G *unutrašnji direktan proizvod* svojih podgrupa A, B ako važi:

unutrašnji direktan proizvod

(1) $A, B \trianglelefteq G$,

(2) $AB = G$,

(3) $A \cap B = E$.

Lema 2.31. *Neka je G grupa. Ako su $A, B \trianglelefteq G$ takve da $A \cap B = E$, tada važi $ab = ba$ za sve $a \in A$, $b \in B$.*

Dokaz. Zbog uslova normalnosti je

$$[a, b] = a^{-1}b^{-1}ab = a^{-1}(b^{-1}ab) = (a^{-1}b^{-1}a)b \in A \cap B.$$

No, tada mora biti $[a, b] = 1$, tj. $ab = ba$. □

unutrašnji direktan proizvod je istovremeno i spoljašnji (i obratno)

Propozicija 2.32. *Ako je G unutrašnji direktan proizvod svojih (normalnih) podgrupa A, B, tada je $G \cong A \times B$.*

Dokaz. Definišimo preslikavanje $\phi : G \to A \times B$ sa

$$\phi(g) = (a, b) \Longleftrightarrow g = ab.$$

Ova definicija je logički dobra jer ako imamo neku drugu faktorizaciju tako da je $ab = a_1b_1$, $a_1 \in A$, $b_1 \in B$, tada je

$$a^{-1}a_1 = bb_1^{-1} \in A \cap B,$$

pa je $a^{-1}a_1 = bb_1^{-1} = 1$, tj. $a = a_1$ i $b = b_1$. S druge strane, zbog $G = AB$ svaki element G ima faktorizaciju opisanog tipa, što odmah takođe implicira da je ϕ "na". Trivijalno, ϕ je injekcija, pa preostaje da pokažemo da je homomorfizam. Stoga uočimo $g, g_1 \in G$ tako da je $g = ab$ i $g_1 = a_1b_1$ za $a, a_1 \in A$, $b, b_1 \in B$. Koristeći prethodnu lemu, dobijamo:

$$\phi(gg_1) = \phi(aba_1b_1) = \phi(aa_1bb_1) = (aa_1, bb_1) = (a, b)(a_1, b_1) = \phi(g)\phi(g_1),$$

što je i trebalo dokazati. □

Obratno, spoljašnji direktan proizvod $G_1 \times G_2$ je istovremeno unutrašnji direktni proizvod svojih podgrupa $\pi_1(G) \cong G_1$ i $\pi_2(G) \cong G_2$.

Pojmove spoljašnjeg i unutrašnjeg direktnog proizvoda, kao i odgovarajuća tvrđenja, možemo uopštiti i na proizvoljne konačne familije grupa. Spoljašnji direktni proizvod $G = G_1 \times \dots \times G_n$ datih grupa $G_1, \dots, G_n$ definisan je primenama operacija odgovarajućih grupa po komponentama. Projekcije definišemo kao $(1 \le i \le n)$ direktnan proizvod konačne familije grupa

$$\pi_i(G) = \{(1_{G_1}, \dots, g_i, \dots, 1_{G_n}) : \; g_i \in G_i\}.$$

Slično kao i malopre, važi $\pi_i(G) \cong G_i$, $\pi_i(G) \trianglelefteq G$ i $G = \pi_1(G) \dots \pi_n(G)$. No, važi i više od $\pi_1(G) \cap \dots \cap \pi_n(G) = E$: imamo da je

$$\pi_i(G) \cap \pi_1(G) \dots \pi_{i-1}(G)\pi_{i+1}(G) \dots \pi_n(G) = E$$

za sve $1 \le i \le n$. Zato za grupu G kažemo da je unutrašnji direktan proizvod svojih podgrupa A_i, $1 \le i \le n$, ako važe sledeći uslovi:

(1) $A_i \trianglelefteq G$ za sve $1 \le i \le n$,

(2) $G = A_1 \dots A_n$,

(3) $A_i \cap A_1 \dots A_{i-1}A_{i+1} \dots A_n = E$ za sve $1 \le i \le n$.

Na analogan način kao i ranije se pokazuje da pretpostavka da je G unutrašnji proizvod svojih podgrupa A_i, $1 \le i \le n$, implicira da je $G \cong A_1 \times \dots \times A_n$.

Primer 2.33. Posmatrajmo grupe reda 8 – već smo upoznali tri takve: jednu Abelovu, $\mathbb{Z}_8$, i dve nekomutativne, D_4 i Q_8. Sada možemo konstruisati još dve Abelove grupe reda 8, naime $\mathbb{Z}_2 \times \mathbb{Z}_4$ i $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Prva ima element reda 4 (ali ne i reda 8), dok su u drugoj grupi svi elementi reda 2; zbog toga su ovi proizvodi, zajedno sa $\mathbb{Z}_8$, tri različite Abelove grupe. Kasnije ćemo videti da su ovim grupama iscrpljene (do na izomorfizam) sve grupe reda 8.

3

Konjugovanost

Opis normalnih podgrupa dat u Propoziciji 2.27 motiviše uvođenje preslikavanja $\sigma_a : G \to G$ (za dato $a \in G$) definisanog sa unutrašnji automorfizam (konjugacija)

$$\sigma_a(g) = a^{-1}ga.$$

Zbog kancelativnosti je σ_a "1-1", a takođe je i "na" (zbog $\sigma_a(aga^{-1}) = g$). Pošto je

$$\sigma_a(gh) = a^{-1}gha = (a^{-1}ga)(a^{-1}ha) = \sigma_a(g)\sigma_a(h)$$

za sve $g, h \in G$, u pitanju je automorfizam grupe G. Ovaj automorfizam σ_a se naziva *konjugacija* ili *unutrašnji automorfizam* grupe G (koji odgovara elementu a).

Putem unutrašnjih automorfizama definišemo *relaciju konjugovanosti* u grupi G sa

$$x \sim y \iff x = g^{-1}yg = \sigma_g(y) \text{ za neko } g \in G$$

za sve $x, y \in G$. Veoma se lako proverava da je $\sim$ relacija ekvivalencije na G. Osim konjugovanosti dva pojedinačna elementa, za dve podgrupe $H, K \leq G$ kažemo da su *konjugovane* ako je $H = g^{-1}Kg = \sigma_g(K)$ za neko $g \in G$ (pri tome, relacija konjugovanosti je takođe relacija ekvivalencije na skupu $\mathrm{Sub}(G)$ svih podgrupa od G). Prema tome, podgrupa je normalna ako i samo ako se poklapa sa svim svojim konjugovanim podgrupama.

Označimo sa $\widetilde{x}$ klasu svih elemenata posmatrane grupe G konjugovanih sa x. Najpre želimo da saznamo kada je ova klasa jednoelementna. klasa konjugovanosti

Lema 3.1. $|\widetilde{x}| = 1$ *ako i samo ako* $x \in Z(G)$.

Dokaz. Važi $|\widetilde{x}| = 1$ ako i samo ako je $\sigma_g(x) = x$ za sve $g \in G$, tj. ako i samo ako je $xg = gx$ za sve $g \in G$. Poslednji uslov je pak ekvivalentan sa $x \in Z(G)$. □

Možemo postaviti pitanje o kardinalnosti proizvoljne klase konjugovanosti. Odgovor nam daje sledeće tvrđenje.

kardinalnost klase konjugovanosti

Propozicija 3.2. $|\widetilde{x}| = (G : C(x))$.

Dokaz. Najpre, jasno je da je $\widetilde{x} = \{\sigma_g(x) : \ g \in G\}$. Prema tome, $|\widetilde{x}| = |G/\rho|$ gde je ρ relacija ekvivalencije na G definisana sa $(g, h) \in \rho$ ako i samo ako $\sigma_g(x) = \sigma_h(x)$. Međutim, poslednji uslov ekvivalentan je sa $g^{-1}xg = h^{-1}xh$, odnosno

$$xgh^{-1} = gh^{-1}x,$$

tj. $gh^{-1} \in C(x)$. Prema tome, klase ekvivalencije relacije ρ su upravo desni koseti centralizatora $C(x)$, odakle sledi tvrđenje. □

Sledeća jednakost (koja sledi iz prethodna dva tvrđenja i činjenice da je $\sim$ relacija ekvivalencije), poznata pod imenom *klasovna jednačina*, povezuje red grupe, red njenog centra i indekse netrivijalnih centralizatora.

klasovna jednačina

Posledica 3.3 (Klasovna jednačina)**.** *Neka je* $\{x_i :\in i \in I\}$ *transverzala nejednoelementnih klasa konjugovanosti grupe* G*, tj. skup koji sadrži tačno po jednog predstavnika klasa ekvivalencije relacije* $\sim$ *koje leže van centra* $Z(G)$*. Tada važi*

$$|G| = |Z(G)| + \sum_{i \in I} (G : C(x_i)).$$

p-grupe imaju netrivijalni centar

Posledica 3.4. *Neka je* p *prost broj i* $|G| = p^n$ *za neko* $n \geq 1$*. Tada je* $Z(G)$ *netrivijalna grupa.*

Dokaz. Ako $x \notin Z(G)$ tada $C(x) \neq G$, pa je $(G : C(x)) > 1$. U tom slučaju, mora biti $p \mid (G : C(x))$. Kako $p \mid |G|$, po klasovnoj jednačini sledi da $p \mid |Z(G)|$, zbog čega ne može biti $Z(G) = E$. □

Klase konjugovanosti sada daju jasan kriterijum normalnosti podgrupe.

Teorema 3.5. *Neka je $H \leq G$. Tada je $H \trianglelefteq G$ ako i samo ako postoji $X \subseteq G$ tako da je*

$$H = \bigcup_{x \in X} \widetilde{x},$$

tj. ako i samo ako je H unija nekih klasa konjugovanosti u grupi G.

podgrupa je normalna akko je unija celih klasa konjugovanosti

Dokaz. ($\Rightarrow$) Stavimo $X = H$. Zaista, ako je $h \in H$ tada po uslovu normalnosti za proizvoljno $g \in G$ važi $\sigma_g(h) \in H$, pa je $\widetilde{h} \subseteq H$. Otuda sledi inkluzija $\supseteq$, dok je obratna inkluzija očita.

($\Leftarrow$) Jasno, za svako $g \in G$ važi $\sigma_g(\widetilde{x}) = g^{-1}\widetilde{x}g \subseteq \widetilde{x}$. Zbog toga je $H\sigma_g \subseteq H$, pa je $H \trianglelefteq G$. $\square$

Posledica 3.6. *U svakoj grupi G, ako $H \leq Z(G)$ tada je $H \trianglelefteq G$.*

Dokaz. Po Lemi 3.1, svaki element centra $Z(G)$ formira jednoelementnu klasu ekvivalencije relacije $\sim$, pa to isto važi i za H. Sada tvrđenje sledi direktno po prethodnoj teoremi. $\square$

Relacija konjugovanosti u simetričnim grupama ima veoma jasan, koncizan opis.

Propozicija 3.7. *Za $\pi, \tau \in \mathbb{S}_n$ važi $\pi \sim \tau$ ako i samo ako π i τ u dekompoziciji na disjunktne cikluse imaju istu strukturu ciklusa, tj. imaju isti broj različitih disjunktnih ciklusa i među ciklusima se može uspostaviti bijekcija tako da su odgovarajući ciklusi iste dužine.*

konjugovanost u simetričnim grupama

Dokaz. Neka je $\pi = \rho^{-1}\tau\rho$ za neku permutaciju $\rho \in \mathbb{S}_n$. Razložimo τ na proizvod disjunktnih ciklusa:

$$\tau = (a_1 a_2 \dots) \dots (b_1 b_2 \dots).$$

Tvrdimo da je tada

$$\pi = (\rho(a_1)\ \rho(a_2)\ \dots) \dots (\rho(b_1)\ \rho(b_2)\ \dots).$$

Zaista, važi

$$\pi = \rho^{-1}\tau\rho = (\rho^{-1}(a_1 a_2 \dots)\rho) \dots (\rho^{-1}(b_1 b_2 \dots)\rho),$$

pa je dovoljno analizirati konjugacije pojedinačnih ciklusa, tj. proveriti da je $\rho^{-1}(a_1 a_2 \dots)\rho = (\rho(a_1)\ \rho(a_2)\ \dots)$. Neka je $k \in \{1, \dots, n\}$. Ako $\rho^{-1}(k) \notin$

$\{a_1, a_2, \dots\}$, tada je očito $(\rho^{-1}(a_1 a_2 \dots)\rho)(k) = (\rho^{-1}\rho)(k) = k$. U suprotnom $\rho^{-1}(k) = a_i$ za neko i, tj. $k = \rho(a_i)$. U tom slučaju je

$$(\rho^{-1}(a_1 a_2 \dots)\rho)(k) = ((a_1 a_2 \dots)\rho)(a_i) = \rho(a_{i+1}),$$

pri čemu je $a_{i+1} = a_1$ ako je i dužina posmatranog ciklusa. Dakle, $\rho(a_i)$ se slika u $\rho(a_{i+1})$, pa tvrđenje sledi. Stoga π i τ imaju istu strukturu ciklusa.

Obratno, pretpostavimo da π i τ imaju istu cikličku strukturu, $\pi = \xi_1 \dots \xi_m$ i $\tau = \eta_1 \dots \eta_m$, gde su $\xi_1, \dots, \xi_m$, odnosno $\eta_1, \dots, \eta_m$ dve familije disjunktnih ciklusa. Neka pri tome ξ_i i η_i imaju istu dužinu za sve $1 \le i \le m$: $\xi_i = (a_1^{(i)} \dots a_{l_i}^{(i)})$ i $\eta_i = (b_1^{(i)} \dots b_{l_i}^{(i)})$. Definišimo parcijalno injektivno preslikavanje ρ na $\{1 \dots, n\}$ tako da je za sve $1 \le i \le m$ i $1 \le j \le l_i$,

$$\rho\left(a_j^{(i)}\right) = b_j^{(i)}.$$

Na ovaj način, preslikavanje ρ je ostalo nedefinisano na skupu $\{1, \dots, n\} \setminus \{a_j^{(i)} : 1 \le i \le m,\ 1 \le j \le l_i\}$ od $n - l$ elemenata, gde je $l = l_1 + \dots + l_m$. Međutim, van slike ρ je ostalo takođe tačno $n - l$ elemenata, naime $\{1, \dots, n\} \setminus \{b_j^{(i)} : 1 \le i \le m,\ 1 \le j \le l_i\}$, pa se zbog toga ρ može dopuniti (i to na $(n-l)!$ različitih načina) do permutacije skupa $\{1, \dots, n\}$. No, zbog argumenata identičnih onima u prethodnom pasusu, sada je $\rho^{-1}\pi\rho = \tau$, pa je $\pi \sim \tau$. □

Primer 3.8. Konstrukciju iz drugog dela prethodnog dokaza ilustrovaćemo na konkretnom primeru. Neka je $n = 9$; posmatrajmo

$$\pi = (12)(34)(567) \quad \text{i} \quad \tau = (14)(26)(973).$$

Po prethodnoj propoziciji, ove dve permutacije jesu konjugovane u $\mathbb{S}_9$ pošto imaju istu cikličku strukturu (dve transpozicije i jedan tercet, uz po dve fiksne tačke). Ukoliko želimo do pronađemo (bar jednu) permutaciju ρ koja realizuje konjugovanost $\rho^{-1}\pi\rho = \tau$, moramo imati

$$\rho = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 4 & 2 & 6 & 9 & 7 & 3 & ? & ? \end{pmatrix}.$$

Vidimo da ρ još nismo definisali u tačkama 8 i 9, a da su s druge strane preostale "neiskorišćene" slike 5 i 8. Njih možemo popuniti umesto upitnika (na bilo koja od dva moguća načina), i tako dobijamo permutaciju koja odgovarajućim konjugovanjem prevodi π u τ.

Primer 3.9. Prethodna propozicija nam omogućava da pokažemo da svojstvo normalnosti podgrupe u grupi *nije* tranzitivno, tj. da se iz $H \trianglelefteq K \trianglelefteq G$ ne može u opštem slučaju zaključiti da je $H \trianglelefteq G$. Zaista, uzmimo $G = \mathbb{S}_4$ i definišimo

normalnost podgrupa nije tranzitivna osobina

$$K = \{\mathrm{id}_n, (12)(34), (13)(24), (14)(23)\}, \quad H = \{\mathrm{id}_n, (12)(34)\}.$$

Pri tome je K izomorfna Klajnovoj grupi V_4, dok je H njena ciklična podgrupa reda 2. Kako je $(K : H) = 2$, odmah imamo $H \trianglelefteq K$. Takođe, po Teoremi 3.5 imamo $K \trianglelefteq G$, pošto K čine trivijalna permutacija i svi mogući proizvodi dva disjunktna ciklusa dužine 2. Međutim, upravo iz istog razloga $H \ntrianglelefteq G$.

Za radoznalce

Za "tranzitivni prenos" normalnosti potreban je jači pojam, naime pojam karakteristične podgrupe. Za $H \leq G$ kažemo da je *karakteristična podgrupa* grupe G ako za sve $\phi \in \mathrm{Aut}(G)$ važi $\phi(H) = H$ (kako je sa svakim automorfizmom ϕ i njegov inverz ϕ^{-1} takođe automorfizam grupe G, može se pokazati da je ovo ekvivalnentno slabijem uslovu $\phi(H) \subseteq H$). Naravno, svaka karakteristična podgrupa jeste normalna, dok obratno, u opštem slučaju, ne važi. Sada nije teško pokazati da pretpostavke da je H karakteristična u K i K karakteristična u G impliciraju da je H karakteristična (i stoga normalna) u G. Međutim, važi i jače tvrđenje.

karakteristična podgrupa

Propozicija 3.10. *Ako je $K \trianglelefteq G$ i H karakteristična podgrupa grupe K, tada je $H \trianglelefteq G$.*

Dokaz. Neka je $g \in G$ proizvoljno; posmatrajmo unutrašnji automorfizam σ_g. Imamo $\sigma_g(K) = K$ zbog čega je $\phi = \sigma_g|_K \in \mathrm{Aut}(K)$. Po datim uslovima mora biti $\phi(H) = H$. Međutim, po definiciji ϕ to znači da je $g^{-1}Hg = H$. Zaključujemo da je $H \trianglelefteq G$. □

4

Teoreme o homomorfizmu i korespondenciji

4.1 Jezgro i faktor grupa

Podsetimo se, za homomorfizam grupa $\phi : G \to H$ *jezgro* tog homomorfizma čine svi elementi od G koji se slikaju u jedinicu grupe H:

$$\operatorname{Ker}\phi = \{a \in G : \ \phi(a) = 1_H\}.$$

jezgro je uvek normalna podgrupa

Lema 4.1. *Za proizvoljan homomorfizam $\phi : G \to H$ važi $\operatorname{Ker}\phi \trianglelefteq G$.*

Dokaz. Uverimo se najpre da je $\operatorname{Ker}\phi \leq G$. Zaista, za proizvoljne $a, b \in \operatorname{Ker}\phi$ važi $\phi(a) = \phi(b) = 1_H$, pa je $\phi(ab^{-1}) = \phi(a) * (\phi(b))^{-1} = 1_H$, tj. $ab^{-1} \in \operatorname{Ker}\phi$. Normalnost $\operatorname{Ker}\phi$ u G sledi pošto važi

$$\phi(g^{-1}ag) = (\phi(g))^{-1} * \phi(a) * \phi(g) = (\phi(g))^{-1} * \phi(g) = 1_H$$

za proizvoljno $g \in G$ i $a \in \operatorname{Ker}\phi$. □

Postavlja se prirodno pitanje: jesu li jezgrima homomorfizama (iz grupe G u neku grupu) iscrpljene sve normalne podgrupe grupe G ? Odgovor je *potvrdan* i u tom smislu su koncepti normalne podgrupe i homomorfizma definisanog na datoj grupi ekvivalentni: jezgro svakog homomorfizma je normalna podgrupa, i za svaku normalnu podgrupu N od G postoji homomorfizam grupe G u neku grupu čije je jezgro baš N. Kako bismo ovo pokazali, potrebno je da uvedemo fundamentalan pojam *faktor grupe* G/N, "količnika" grupe G u odnosu na N.

faktor grupa

Neka je, dakle, $N \trianglelefteq G$. Grupa G/N biće definisana na skupu koseta $\{Ng : g \in G\}$ podgrupe N tako što za $a, b \in G$ definišemo

$$Na \cdot Nb = Nab$$

(primetimo da je Nab upravo i rezultat množenja koseta Na i Nb kao podskupova grupe G, pošto je zbog normalnosti N, $NaNb = NNab = Nab$).

Propozicija 4.2. *Neka je G grupa i $N \trianglelefteq G$. Tada je G/N dobro definisana grupa.*

Dokaz. Dobru definisanost pokazujemo pretpostavljajući da je $Na = Nc$ i $Nb = Nd$ za neko $a, b, c, d \in G$. Tada je $ac^{-1}, bd^{-1} \in N$. Međutim, tada je

$$ab(cd)^{-1} = abd^{-1}c^{-1} = (ac^{-1})[c(bd^{-1})c^{-1}] \in N$$

zbog normalnosti podgrupe N, odakle sledi $Nab = Ncd$. Asocijativnost se automatski prenosi iz G. Jedinica je $N = N1$, a inverzni element koseta Na je Na^{-1}. □

Primetimo da je $|G/N| = (G : N)$.

Sada definišemo *prirodno preslikavanje* $\nu_N : G \to G/N$ sa $\nu_N(g) = Ng$ za sve $g \in G$. prirodno preslikavanje

Propozicija 4.3. *Neka je G grupa i $N \trianglelefteq G$. Tada je prirodno preslikavanje ν_N homomorfizam grupa takav da je $\operatorname{Ker} \nu_N = N$.* svaka normalna podgrupa je jezgro

Dokaz. Za $g, h \in G$ važi $\nu_N(gh) = Ngh = (Ng)(Nh) = \nu_N(g)\nu_N(h)$, zbog čega je ν_N homomorfizam (lako se vidi da je on sirjektivan, $\operatorname{Im} \nu_N = G/N$). Važi $g \in \operatorname{Ker} \nu_N$ ako i samo ako $\nu_N(g) = N$ ako i samo ako $Ng = N$ ako i samo ako $g \in N$, pa je $\operatorname{Ker} \nu_N = N$. □

4.2 Teorema o homomorfizmu

Jedna od centralnih teorema koja se vezuje za pojam homomorfizma grupa i koja ima veoma široku primenu jeste *teorema o homomorfizmu*.

Teorema 4.4 (Teorema o homomorfizmu)**.** *Neka je $\phi : G \to H$ homomorfizam grupa. Tada je* teorema o homomorfizmu

$$G/\operatorname{Ker} \phi \cong \operatorname{Im} \phi.$$

Dokaz. Definišimo preslikavanje $\psi : G/\operatorname{Ker}\phi \to \operatorname{Im}\phi$ sa

$$\psi\left((\operatorname{Ker}\phi)a\right) = \phi(a)$$

za sve $a \in G$. Sada za proizvoljne $a, b \in G$ važi $(\operatorname{Ker}\phi)a = (\operatorname{Ker}\phi)b$ ako i samo ako $ab^{-1} \in \operatorname{Ker}\phi$ ako i samo ako $\phi(ab^{-1}) = 1_H$ ako i samo ako $\phi(a) = \phi(b)$ ako i samo ako $\psi((\operatorname{Ker}\phi)a) = \psi((\operatorname{Ker}\phi)b)$. Zbog toga je ψ dobro definisano i injektivno. Očigledno je da je ψ "na", jer za sve $h \in \operatorname{Im}\phi$ postoji $a \in G$ tako da je $h = \phi(a) = \psi((\operatorname{Ker}\phi)a)$. Konačno, ψ je homomorfizam jer je

$$\psi((\operatorname{Ker}\phi)ab) = \phi(ab) = \phi(a)\phi(b) = \psi((\operatorname{Ker}\phi)a)\psi((\operatorname{Ker}\phi)b)$$

za sve $a, b \in G$. □

Kao prvi primer primene Teoreme o homomorfizmu, opisujemo faktor grupe po njenom centru. Naime, primetimo da za sve $a, b \in G$ važi $\sigma_a \circ \sigma_b = \sigma_{ab}$, $\sigma_a^{-1} = \sigma_{a^{-1}}$ i $\sigma_1 = \mathrm{id}_G$. Zbog toga, unutrašnji automorfizmi čine podgrupu od $\operatorname{Aut}(G)$, koju označavamo sa $\operatorname{Inn}(G)$.

grupa unutrašnjih automorfizama

Propozicija 4.5. *Za svaku grupu G važi $G/Z(G) \cong \operatorname{Inn}(G)$.*

Dokaz. Posmatrajmo homomorfizam $\phi : G \to \operatorname{Aut}(G)$ definisan sa

$$\phi(a) = \sigma_a.$$

Jasno, $\operatorname{Im}\phi = \operatorname{Inn}(G)$. S druge strane, $g \in \operatorname{Ker}\phi$ ako i samo ako $\sigma_g = \mathrm{id}_G$ ako i samo ako $g^{-1}ag = a$ za sve $a \in G$ ako i samo ako $ga = ag$ za sve $a \in G$ ako i samo ako $g \in Z(G)$. Dakle, $\operatorname{Ker}\phi = Z(G)$, pa rezultat sledi po Teoremi o homomorfizmu. □

Uzgred budi rečeno, $\operatorname{Inn}(G)$ je uvek normalna podgrupa od $\operatorname{Aut}(G)$, pošto za proizvoljan automorfizam $\phi \in \operatorname{Aut}(G)$ i $a, g \in G$ imamo

$$(\phi^{-1} \circ \sigma_a \circ \phi)(g) = \phi(a^{-1}\phi^{-1}(g)a) = (\phi(a))^{-1}g\phi(a) = \sigma_{\phi(a)}(g),$$

pa je $\phi^{-1} \circ \sigma_a \circ \phi = \sigma_{\phi(a)} \in \operatorname{Inn}(G)$. Tako, možemo definisati faktor $\operatorname{Out}(G) = \operatorname{Aut}(G)/\operatorname{Inn}(G)$ koji zovemo *grupa spoljašnjih automorfizma* od G.

4.3 Srž, normalizator, N/C teorema

Srž podgrupe $H \leq G$ je srž podgrupe

$$\mathrm{core}(H) = \bigcap_{g \in G} g^{-1}Hg.$$

Budući da je presek proizvoljne familije podgrupa od G ponovo podgrupa od G, odmah imamo da je $\mathrm{core}(H) \leq G$.

Propozicija 4.6. *Neka je G grupa i $H \leq G$. Tada je* $\mathrm{core}(H)$ *najveća normalna podgrupa od G sadržana u H.* karakterizacija srži

Dokaz. Očito, $\mathrm{core}(H) \subseteq H$. Pored toga, $\mathrm{core}(H) \trianglelefteq G$, jer je za proizvoljno $a \in G$,

$$a^{-1}[\mathrm{core}(H)]a = a^{-1}\left(\bigcap_{g \in G} g^{-1}Hg\right)a = \bigcap_{g \in G}(ga)^{-1}H(ga) = \mathrm{core}(H).$$

Konačno, ako je N normalna podgrupa od G sadržana u H, tada je $N = g^{-1}Ng \subseteq g^{-1}Hg$ za sve $g \in G$, pa je $N \subseteq \mathrm{core}(H)$. □

Normalizator skupa $X \subseteq G$ je sledeći skup elemenata grupe G: normalizator

$$N(X) = \{g \in G : \ gX = Xg\}.$$

Slično kao kod centralizatora, pišemo $N_G(X)$ ako je potrebno naglasiti unutar koje grupe se posmatra normalizator. Lako se pokazuje da je za sve $X \subseteq G$ normalizator $N(X)$ podgrupa od G.

Propozicija 4.7. *Neka je G grupa i $H \leq G$. Tada je $N(H)$ najveća podgrupa od G u kojoj je H normalna.* karakterizacija normalizatora

Dokaz. Po samoj definiciji normalizatora, $H \trianglelefteq N(H)$. Neka je sada $H \trianglelefteq K \leq G$. Tada za sve $g \in K$ važi $gH = Hg$, pa sledi $g \in N(H)$ i $K \subseteq N(H)$. □

Za kraj ovog kratkog odeljka, navodimo još jedan rezultat koji je koristan u raznim primenama.

Propozicija 4.8 (N/C teorema)**.** *Neka je G grupa i $H \leq G$. Tada je $C(H) \trianglelefteq N(H)$ i pri tome se faktor $N(H)/C(H)$ može potopiti u* $\mathrm{Aut}(H)$. N/C teorema

Dokaz. Posmatrajmo homomorfizam $\phi : N(H) \to \mathrm{Aut}(H)$ definisan sa

$$\phi(g) = \sigma_g|_H.$$

Pre svega, ova definicija je korektna jer je zaista $\sigma_g|_H \in \mathrm{Aut}(H)$ zbog $\sigma_g(H) = g^{-1}Hg = H$ za sve $g \in N(H)$. Odredimo sada jezgro ovog homomorfizma. Imamo da $g \in \mathrm{Ker}\,\phi$ ako i samo ako $\phi(g) = \mathrm{id}_H$ ako i samo ako za sve $h \in H$ važi $g^{-1}hg = h$, tj. $gh = hg$. Ovaj poslednji uslov važi ako i samo ako $g \in C(H) \cap N(H) = C(H)$, što znači da je $\mathrm{Ker}\,\phi = C(H)$. Otuda je $C(H) \trianglelefteq N(H)$ i, po Teoremi o homomorfizmu, važi da je $N(H)/C(H)$ izomorfno sa $\mathrm{Im}\,\phi$, što je podgrupa od $\mathrm{Aut}(H)$. Drugim rečima, postoji potapanje $N(H)/C(H)$ u $\mathrm{Aut}(H)$. □

4.4 Teorema o korespondenciji

Teorema o korespondenciji izražava tesnu vezu između podgrupa faktor grupe G/N i podgrupa same grupe G.

teorema o korespondenciji

Teorema 4.9 (Teorema o korespondenciji)**.** *Neka je G grupa i $N \trianglelefteq G$. Tada je $K \leq G/N$ ako i samo ako važi $K = H/N$ za neku podgrupu $H \leq G$ koja sadrži N.*

Pri tome, $H \mapsto H/N$ predstavlja izomorfizam intervala $[N, G]$ u parcijalno uređenom skupu $(\mathrm{Sub}(G), \subseteq)$ svih podgrupa od G i parcijalno uređenog skupa $(\mathrm{Sub}(G/N), \subseteq)$ svih podgrupa faktor grupe G/N.

Dokaz. Neka su preslikavanja $\phi : [N, G] \to \mathrm{Sub}(G/N)$ i $\psi : \mathrm{Sub}(G/N) \to [N, G]$ definisana sa

$$\phi(H) = H/N,$$

odnosno

$$\psi(K) = \bigcup_{Ng \in K} Ng.$$

Oba ova preslikavanja su dobro definisana, jer $N \trianglelefteq G$ povlači $N \trianglelefteq H$ za $N \leq H \leq G$; pored toga, $\psi(K)$ sadrži N i reč je o podgrupi od G, jer $a, b \in \psi(K)$ implicira $a \in Ng_1$, $b \in Ng_2$ za neke $g_1, g_2 \in G$ takve da $Ng_1, Ng_2 \in K$, pa $ab^{-1} \in Ng_1g_2^{-1}N = Ng_1g_2^{-1} \subseteq \psi(K)$ (zbog $Ng_1g_2^{-1} \in K$).

Dalje, ova preslikavanja su očigledno injektivna i monotona. Konačno, preostaje da se primeti da je $\phi\psi$ identičko preslikavanje na $[N, G]$, a da je $\psi\phi$ identičko preslikavanje na $\mathrm{Sub}(G/N)$, zbog čega su oba preslikavanja bijekcije i, zapravo, izomorfizmi parcijalno uređenih skupova. □

5

Teoreme o izomorfizmu

5.1 Prva teorema o izomorfizmu

Neka su A, B dve podgrupe grupe G. U opštem slučaju proizvod AB nije podgrupa i stoga je uži od $\langle A \cup B \rangle$. Pod određenim uslovima to ipak jeste slučaj.

Lema 5.1. *Neka je G grupa i $A, B \leq G$. Tada je $\langle A \cup B \rangle = AB \leq G$ ako i samo ako je $AB = BA$.*

Dokaz. ($\Rightarrow$) Primetimo da za proizvoljne $a \in A$, $b \in B$ imamo $a = a1 \in AB$ i $b = 1b \in AB$. Kako je AB, po pretpostavci, podgrupa, $ba \in AB$; zbog toga je $BA \subseteq AB$. S druge strane, pošto su A, B podgrupe, važi $A^{-1} = A$ i $B^{-1} = B$, pa je $AB = A^{-1}B^{-1} = (BA)^{-1} \subseteq (AB)^{-1} = B^{-1}A^{-1} = BA$. Tako zaključujemo da je $AB = BA$.

($\Leftarrow$) Jasno, $AB \subseteq \langle A \cup B \rangle$. Neka su $x, y \in AB$ proizvoljni. Tada je $xy^{-1} \in AB(AB)^{-1} = ABB^{-1}A^{-1} = ABA = AB$, pa je $AB \leq G$, zbog čega je $\langle A \cup B \rangle \subseteq AB$. Prema tome, $\langle A \cup B \rangle = AB$. $\square$

Posledica 5.2. *Neka je G grupa. Ako je $A \leq G$ i $B \trianglelefteq G$, tada je $AB \leq G$.*

Teorema 5.3 (Prva teorema o izomorfizmu)**.** *Neka je G grupa i $A \leq G$, $B \trianglelefteq G$. Tada je $A \cap B \trianglelefteq A$ i važi* prva teorema o izomorfizmu

$$AB/B \cong A/A \cap B.$$

Dokaz. Posmatrajmo preslikavanje $\phi : A \to G/B$ koje se dobija kao restrikcija prirodnog preslikavanja ν_B na podgrupu A: $\phi(a) = Ba$. Sada $g \in \operatorname{Ker}\phi$ ako i samo ako $g \in A$ i $Bg = B$, što je dalje ekvivalentno sa $g \in A \cap B$. Prema tome, $A \cap B$ je jezgro homomorfizma ϕ i zato je $A \cap B \trianglelefteq A$. S druge strane, $\operatorname{Im}\phi = \phi(A) = \{Ba : a \in A\} = \{Bba : a \in A, b \in B\} = \{Bx : x \in BA = AB\} = AB/B$, pa teorema sledi iz Teoreme o homomorfizmu. $\square$

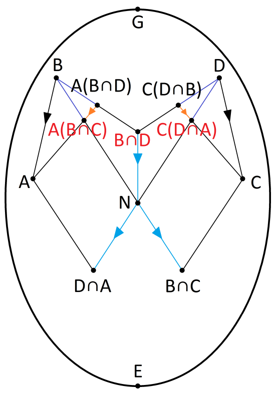
Za radoznalce

Sada ćemo videti jednu izuzetno značajnu (ali složeniju) posledicu Prve teoreme o izomorfizmu, *lemu Casenhausa*[3]. Ona ima ključnu ulogu u alternativnom dokazu Teoreme Žordan-Heldera (Glava 11) preko Šrajerove teoreme o profinjenju.

lema Casenhausa

Posledica 5.4 (Lema Casenhausa)**.** *Neka su A, B, C, D podgrupe grupe G takve da je $A \trianglelefteq B$ i $C \trianglelefteq D$. Tada je $A(B \cap C) \trianglelefteq A(B \cap D)$ i $C(D \cap A) \trianglelefteq C(D \cap B)$ i važi*

$$A(B \cap D)/A(B \cap C) \cong C(D \cap B)/C(D \cap A).$$



Dokaz. Imajući u vidu Posledicu 5.2 i činjenicu da je $A \trianglelefteq B$ i $B \cap C \leq B$, sledi da je $A(B \cap C)$ podgrupa od B (generisana sa $A \cup (B \cap C)$). Analogno, $C(D \cap A)$ je podgrupa od D. Takođe, po istoj posledici imamo $A(B \cap C) = (B \cap C)A$ i $C(D \cap A) = (D \cap A)C$.

Tvrdimo da je $B \cap C \trianglelefteq B \cap D$; neka je $c \in B \cap C$ i $d \in B \cap D$. Kako $c, d \in B$, odmah sledi da je $d^{-1}cd \in B$. S druge strane, $C \trianglelefteq D$ povlači da $d^{-1}cd \in C$, pa $d^{-1}cd \in B \cap C$. Analogno zaključujemo da je $D \cap A \trianglelefteq D \cap B = B \cap D$. Zbog toga je

$$N = (B \cap C)(D \cap A) = (D \cap A)(B \cap C)$$

normalna podgrupa od $B \cap D$.

[3] Hans Casenhaus (Hans Julius Zassenhaus, 1912–1991), nemački matematičar

Sada je dovoljno pokazati da je $A(B \cap C) \trianglelefteq A(B \cap D)$, odnosno da je $A(B \cap D)/A(B \cap C)$ izomorfno sa $B \cap D/N$. Ukoliko to pokažemo, analogno će slediti $C(D \cap B)/C(D \cap A) \cong B \cap D/N$ i tvrđenje će biti dokazano.

Najpre, neka je $g \in A(B \cap D)$. Tada je $g = ab$ gde je $a \in A$ i $b \in B \cap D$, pa je, imajući u vidu $A \trianglelefteq B$ i $B \cap C \trianglelefteq B \cap D$,

$$gA(B \cap C) = abA(B \cap C) = aAb(B \cap C) =$$

$$= A(B \cap C)b = (B \cap C)Aab = A(B \cap C)g.$$

Zbog toga sledi da je $A(B \cap C) \trianglelefteq A(B \cap D)$.

Primenimo sada Prvu teoremu o izomorfizmu sa $A(B \cap D)$ kao osnovnom grupom, a u odnosu na njenu podgrupu $H = B \cap D$ i normalnu podgrupu $K = A(B \cap C)$. Sada je

$$HK = (B \cap D)A(B \cap C) = A(B \cap D)(B \cap C) = A(B \cap D),$$

kao i

$$H \cap K = B \cap D \cap A(B \cap C) = N,$$

pri čemu je u poslednjoj jednakosti inkluzija $\supseteq$ očita, dok suprotna inkluzija sledi jer $x \in B \cap D \cap A(B \cap C)$ implicira $x = ab$ za neke $a \in A$ i $b \in B \cap C$, a $x \in D$ povlači da je $a = xb^{-1} \in DC^{-1} = D$. Uvrštavajući sada ove podgrupe u $HK/K \cong H/H \cap K$ dobijamo upravo željeni izomorfizam, a time i okončavamo dokaz. $\square$

5.2 Druga teorema o izomorfizmu

Teorema 5.5 (Druga teorema o izomorfizmu)**.** *Neka je G grupa i $A \leq B \trianglelefteq G$, $A \trianglelefteq G$. Tada je $B/A \trianglelefteq G/A$ i važi* druga teorema o izomorfizmu

$$(G/A)/(B/A) \cong G/B.$$

Dokaz. Posmatrajmo preslikavanje $\phi : G/A \to G/B$ definisano sa

$$\phi(Ag) = Bg$$

za sve $g \in G$. Ovo je dobro definisani (sirjektivni) homomorfizam, jer $Ag = Ah$ povlači $gh^{-1} \in A \subseteq B$, pa tako i $Bg = Bh$. Zbog toga, teorema će biti dokazana (na osnovu Teoreme o homomorfizmu) čim dokažemo da je $\mathrm{Ker}\,\phi = B/A$. Zaista, $Ag \in \mathrm{Ker}\,\phi$ ako i samo ako $Bg = B$, što je ekvivalentno sa $g \in B$, odnosno sa $Ag \in B/A$. $\square$

Kao ilustraciju ove teoreme, pokazujemo da je faktor G/G' jedinstvena maksimalna Abelova homomorfna slika grupe G. Najpre nam treba pripremno tvrđenje koje karakteriše Abelove faktore. maksimalna Abelova homomorfna slika

Lema 5.6. *Neka je H podgrupa grupe G. Tada je $H \trianglelefteq G$ i faktor G/H je Abelova grupa ako i samo ako je $G' \leq H$.*

Dokaz. ($\Rightarrow$) Po datim uslovima, važi $abH = Hab = HaHb = HbHa = Hba = baH$ za sve $a, b \in G$. Zato je $[a, b] = (ba)^{-1}ab \in H$, tj. $G' \leq H$.

($\Leftarrow$) Pretpostavimo da H sadrži sve komutatore grupe G. Tada za sve $g \in G$, $h \in H$ važi $[h, g] = h^{-1}g^{-1}hg \in H$, odnosno $g^{-1}hg \in H$, pa je podgrupa H normalna u G. S druge strane, za proizvoljne $a, b \in G$ imamo $[a, b] = (ba)^{-1}ab \in H$, pa je $Hba = baH = abH = Hab$, pa je faktor G/H Abelova grupa. $\square$

Posledica 5.7. *Neka je G proizvoljna grupa i A Abelova grupa. Sledeća dva tvrđenja su ekvivalentna:*

(1) Postoji sirjektivni homomorfizam $\phi : G \to A$;

(2) Postoji sirjektivni homomorfizam Abelovih grupa $\psi : G/G' \to A$.

Dokaz. (2)$\Rightarrow$(1) je trivijalno, pošto se ϕ može dobiti kao kompozicija prirodnog homomorfizma $\nu_{G'}$ i ψ.

(1)$\Rightarrow$(2) Po Teoremi o homomorfizmu je $G/\operatorname{Ker}\phi \cong A$. No, tada je po prethodnoj lemi $G' \leq \operatorname{Ker}\phi$. Kako su i $\operatorname{Ker}\phi$ i G' normalne podgrupe od G, po Drugoj teoremi o izomorfizmu sledi da je $(G/G')/(\operatorname{Ker}\phi/G') \cong A$, pa je tako A homomorfna slika od G/G'. $\square$

6

Grupe permutacija

6.1 Kejlijeva teorema

Podsetimo se (iz uvodne glave) da smo sa $\mathbb{S}_X$ označili grupu svih permutacija skupa X (bijekcija $X \to X$) u odnosu na kompoziciju preslikavanja, te da smo tu grupu nazvali *simetrična grupa* na X. Svaku podgrupu $G \leq \mathbb{S}_X$ zovemo *grupa permutacija*; ako je pri tome $|X| = n$, tada je grupa permutacija G *stepena* n. Jedan od najosnovnijih rezultata teorije grupa, *Kejlijeva*[4] *teorema*, pokazuje da su – do na izomorfizam – grupama permutacija iscrpljene *sve* grupe.

Teorema 6.1 (Kejli)**.** *Svaka grupa je izomorfna nekoj grupi permutacija.* Kejlijeva teorema

Dokaz. Neka je G grupa. Dokazujemo da se ona može potopiti u simetričnu grupu $\mathbb{S}_G$ na svom sopstvenom nosaču. Definišimo $\phi : G \to \mathbb{S}_G$ sa $\phi(g) = \rho_g$ za sve $g \in G$, gde je permutacija ρ_g na G definisana sa

$$\rho_g(a) = ag$$

za sve $a \in G$. (ρ_g je permutacija zbog kancelativnosti u G i $\rho_g(ag^{-1}) = a$ za sve $a \in G$.) Sada imamo:

$$[\phi(gh)](a) = \rho_{gh}(a) = a(gh) = (ag)h = \rho_h(\rho_g(a)) = [\phi(g) \circ \phi(h)](a)$$

[4]Artur Kejli (Arthur Cayley 1821–1895), britanski matematičar, jedan od osnivača teorije grupa u savremenom smislu te reči

za sve $a \in G$, pa je $\phi(gh) = \phi(g) \circ \phi(h)$, tj. ϕ je homomorfizam. On je injektivan, jer $\phi(g) = \rho_g = \rho_h = \phi(h)$ povlači $g = \rho_g(1) = \rho_h(1) = h$. $\square$

6.2 Parnost permutacije, alternativne grupe

parnost permutacije

Za $n \geq 2$ i $\pi \in \mathbb{S}_n$ definišemo *parnost* permutacije π sa

$$p(\pi) = \prod_{1 \leq i < j \leq n} \frac{\pi(j) - \pi(i)}{j - i}.$$

Lako se pokazuje da je uvek $p(\pi) \in \{1, -1\}$. $p(\pi)$ zapravo meri parnost broja *inverzija* u π – parova (i, j), $i < j$, takvih da je $\pi(i) > \pi(j)$. Zbog toga za π sa osobinom $p(\pi) = 1$ kažemo da je *parna* permutacija, a u suprotnom je *neparna*. Takođe se lako uočava da je proizvod dve parne permutacije ponovo parna permutacija (zapravo, p je homomorfizam sa $\mathbb{S}_n$ na grupu $\mathbb{Z}^\times \cong \mathbb{Z}_2$ i parne permutacije čine jezgro tog homomorfizma), pa tako parne permutacije čine (normalnu) podgrupu od $\mathbb{S}_n$ indeksa 2. Tu podgrupu označavamo sa $\mathbb{A}_n$ i zovemo *alternativna grupa* (stepena n).

alternativne grupe $\mathbb{A}_n$

Tipičan primer parne permutacije je 3-ciklus (abc), $a < b < c$, budući da on ima dve inverzije: (b, c) (koji se slika u (c, a)) i (a, c) (koji se slika u (b, a)). Međutim, 3-ciklusi imaju posebnu ulogu u alternativnim grupama $\mathbb{A}_n$: oni je generišu. Zapravo, vredi i nešto jače tvrđenje.

generatori $\mathbb{A}_n$

Lema 6.2. *Ciklusi $\pi_k = (12k)$, $3 \leq k \leq n$, generišu $\mathbb{A}_n$.*

Dokaz. Najpre, lako se vidi da je grupa $\mathbb{A}_n$ generisana svim dvostrukim proizvodima transpozicija $(ab)(cd)$ (ovo se može pokazati, na primer, indukcijom po broju inverzija u posmatranoj parnoj permutaciji π). Zbog toga ćemo najpre pokazati da se svaki 3-ciklus može dobiti kao proizvod ciklusa oblika π_k, a zatim i da je svaki dvostruki proizvod transpozicija proizvod 3-ciklusa.

Zaista, neposrednim računom permutacija se dobija da važi

$$(1ab) = (1a2)(12b) = (12a)^2(12b), \quad (2ab) = (12a)(1b2) = (12a)(12b)^2,$$

$$(abc) = (12a)(12b)^2(12c)(12a)^2$$

za sve međusobno različite $a, b, c \geq 3$. S druge strane, za različite $a, b, c, d \geq 1$ imamo

$$(ab)(ac) = (abc)$$

i

$$(ab)(cd) = (ab)(bc)(bc)(cd) = (bac)(cbd),$$

pa lema sledi. $\square$

Lema 6.3. *Neka je $H \trianglelefteq \mathbb{A}_n$, $n \geq 3$. Ako H sadrži 3-ciklus, tada je $H = \mathbb{A}_n$.*

Dokaz. Pretpostavimo da $(abc) \in H$. Neka je π proizvoljna parna permutacija koja a slika u 1, b slika u 2, a c u 3; tada je $(123) = \pi^{-1}(abc)\pi \in H$, kao i $(213) = (123)^2 \in H$. No, tada se i svi konjugovani elementi ciklusa (213) nalaze u H. Odaberimo $\sigma = (12)(3k)$ za $k \geq 4$ i primetimo da je σ parna permutacija; tada je $\sigma^{-1}(213)\sigma = (12k) \in H$. Međutim, po prethodnoj lemi, ovi ciklusi zajedno sa (123) generišu $\mathbb{A}_n$, pa je $H = \mathbb{A}_n$. $\square$

Sledeći rezultat ilustruje veliki značaj alternativnih grupa u teoriji grupa.

Teorema 6.4. *Za sve $n \geq 5$, grupa $\mathbb{A}_n$ je prosta.* $\mathbb{A}_n$ su proste grupe za sve $n \geq 5$

Dokaz. Pretpostavimo da je H netrivijalna normalna podgrupa od $\mathbb{A}_n$. Neka je pri tome $\tau \in H$ netrivijalna permutacija sa maksimalnim brojem fiksnih tačaka od svih permutacija koje pripadaju H. Dokazaćemo da je τ 3-ciklus, dočim teorema onda sledi direktno iz prethodne leme.

Pretpostavimo suprotno. Tada se u ciklusnoj reprezentaciji τ (tj. u razlaganju na disjunktne cikluse) javljaju bar četiri simbola. Bez umanjenja opštosti, možemo pretpostaviti (uz preimenovanje elemenata osnovnog skupa, po potrebi) da su fiksne tačke permutacije τ baš $k+1, \dots, n$, te da su disjunktni ciklusi τ definisani na uzastopnim elementima koji zajedno čine skup $\{1, \dots, k\}$. Pri tome je $k \geq 4$.

Posmatramo dva slučaja: prvi je kada τ sadrži bar jedan ciklus dužine bar 3, a drugi kada je τ proizvod transpozicija. U oba slučaja ćemo koristiti ciklus $\sigma = (345) \in \mathbb{A}_n$.

U prvom slučaju možemo pisati, bez umanjenja opštosti,

$$\tau = (12 \dots m)\tau'$$

za neko $m \geq 3$, pri čemu je ili $m \geq 4$, ili $m = 3$ i $\tau' \neq \mathrm{id}_n$ (tako da 4 nije fiksna tačka od τ'). Sada je zapravo $k \geq 5$, budući da je slučaj $k = 4$ nemoguć: (1234) nije parna permutacija. Posmatrajmo sada permutaciju $\sigma^{-1}\tau\sigma\tau^{-1} \in H$. Za sve $1 \leq i \leq n-k$ važi

$$\sigma^{-1}\tau\sigma\tau^{-1}(k+i) = k+i,$$

jer je $k+i$ fiksna tačka kako od τ tako i od σ. Međutim, pošto je $\tau(1)=2$ i $1,2$ su fiksne tačke od σ, sledi

$$\sigma^{-1}\tau\sigma\tau^{-1}(1)=1.$$

Drugim rečima, $\sigma^{-1}\tau\sigma\tau^{-1}$ ima više fiksnih tačaka od τ, pri čemu nije u pitanju identička permutacija jer je $\sigma^{-1}\tau\sigma\tau^{-1}(2)\in\{1,3\}$. Kontradikcija.

Preostaje da se razmotri drugi slučaj kada je

$$\tau=(12)(34)\tau'$$

za neki proizvod transpozicija τ'. Ako je on trivijalan (tj. $k=4$), tada je $\sigma^{-1}\tau\sigma\tau^{-1}=(345)\in H$, pa imamo kontradikciju. Ako je pak

$$\tau=(12)(34)(56)\tau'',$$

tada je $\sigma^{-1}\tau\sigma\tau^{-1}=(35)(46)$, a to je ponovo permutacija sa više fiksnih tačaka (naime, $n-4$) nego τ, što je nemoguće.

Prema tome, τ mora biti 3-ciklus, pa je teorema dokazana. □

Zapravo $\mathbb{A}_n$ je uvek prosta grupa osim u slučaju $n=4$: $\mathbb{A}_1$ i $\mathbb{A}_2$ su trivijalne grupe i $\mathbb{A}_3\cong\mathbb{Z}_3$. Međutim, $\mathbb{A}_4$ ima normalnu podgrupu $K\cong V_4$ koju smo videli u Primeru 3.9 koju čine identička permutacija i dvostruki proizvodi ciklusa $(12)(34),(13)(24),(14)(23)$ (ta podgrupa je zapravo normalna u celoj simetričnoj grupi $\mathbb{S}_3$). Grupa $\mathbb{A}_4$ je reda 12, a $\mathbb{A}_4/K\cong\mathbb{Z}_3$: koseti su K, $K(123)$ i $K(132)$.

Posledica 6.5. *Za sve $n\geq 5$ važi $\mathbb{S}'_n=\mathbb{A}'_n=\mathbb{A}_n$.*

Dokaz. Najpre, pošto je $\mathbb{A}_n$ prosta po prethodnoj teoremi, izvodna grupa $\mathbb{A}'_n$ može biti samo E ili $\mathbb{A}_n$; međutim, prvi slučaj otpada pošto $\mathbb{A}_n$ nije Abelova. Zato je $\mathbb{A}'_n=\mathbb{A}_n$, odakle odmah sledi da $\mathbb{A}_n\leq\mathbb{S}'_n$. Međutim, po Posledici 5.7 znamo da je $\mathbb{S}_n/\mathbb{S}'_n$ maksimalna Abelova homomorfna slika grupe $\mathbb{S}_n$. Budući da $\mathbb{S}_n$ ima homomorfizam na $\mathbb{Z}_2$ (naime, parnost p), sledi da je $(\mathbb{S}_n:\mathbb{S}'_n)\geq 2$, pa mora biti $\mathbb{S}'_n=\mathbb{A}_n$. □

7

Dejstvo grupe na skup

7.1 Dve definicije dejstva

(Desno) dejstvo grupe G na neprazan skup X je preslikavanje

dejstvo grupe na skup

$$\theta : X \times G \to X$$

(pri čemu, radi preglednosti, $\theta(x, g)$ ponekad kraće pišemo kao x^g) koje zadovoljava uslove

$$(x^g)^h = x^{gh}$$

i

$$x^1 = x$$

za sve $x \in X$, $g, h \in G$. Pojam dejstva grupe G na X ekvivalentan je konceptu homomorfizma $G \to \mathbb{S}_X$ (tzv. *permutacijske reprezentacije* grupe G na X) u sledećem smislu.

Propozicija 7.1. *Za svako dejstvo θ grupe G na skup X, preslikavanje $\phi : G \to \mathbb{S}_X$ definisano sa*

dejstvo grupe G na skup X ekvivalentno je homomorfizmu $G \to \mathbb{S}_X$

$$[\phi(g)](x) = x^g$$

je homomorfizam grupa. Obratno, za svaki homomorfizam $\phi : G \to \mathbb{S}_X$, preslikavanje $\theta : X \times G \to X$ dato sa $\theta(x, g) = [\phi(g)](x)$ je dejstvo G na X.

Dokaz. Najpre, uočimo da je za sve $g \in G$, funkcija $x \mapsto x^g$ (tj. $\phi(g)$) zaista permutacija skupa X: ovo zaključujemo na osnovu $(x^g)^{g^{-1}} = (x^{g^{-1}})^g = x^1 = x$, zbog čega je $\phi(g) \circ \phi(g^{-1}) = \phi(g^{-1}) \circ \phi(g)$ identičko preslikavanje na X. Sada za proizvoljno $x \in X$ važi

$$[\phi(g) \circ \phi(h)](x) = (x^g)^h = x^{gh} = [\phi(gh)](x),$$

pa je $\phi(gh) = \phi(g) \circ \phi(h)$, tj. ϕ je homomorfizam.

Obratno, ako je dat homomorfizam $\phi : G \to \mathbb{S}_X$, tada je

$$\theta(\theta(x,g),h) = [\phi(g) \circ \phi(h)](x) = [\phi(gh)](x) = \theta(x,gh)$$

za sve $x \in X$ i $g, h \in G$, kao i $\theta(x,1) = [\phi(1)](x) = x$, pa je θ dejstvo. $\square$

7.2 Orbite, tranzitivnost, stabilizator, jezgro

Neka je G grupa i θ njeno dejstvo na skup X. Na skupu X definišemo relaciju $\sim$ na sledeći način:

$$x \sim y \iff y = x^g \text{ za neko } g \in G.$$

Lako se pokazuje da je $\sim$ relacija ekvivalencije na X. Klasu ekvivalencije elementa $x \in X$ zovemo *orbita* od x i označavamo sa x^G. Dakle,

orbite dejstva

$$x^G = \{x^g : \; g \in G\}.$$

tranzitivnost dejstva, odnosno grupe permutacija

Dejstvo θ je *tranzitivno* ako ima tačno jednu orbitu, tj. ako za sve $x, y \in X$ postoji $g \in G$ tako da je $x^g = y$. Analogno, za grupu permutacija $G \le \mathbb{S}_X$ (koja na prirodan način deluje na skup X putem trivijalnog potapanja $\mathrm{id}_G : G \to \mathbb{S}_X$) kažemo da je tranzitivna ako za sve $x, y \in X$ postoji $\sigma \in G$ tako da je $\sigma(x) = y$.

Opštije, grupa permutacija G je *n-tostruko tranzitivna* ako za sve n-torke $(x_1, \ldots, x_n), (y_1, \ldots, y_n)$ različitih elemenata iz X postoji $\sigma \in G$ tako da je $\sigma(x_i) = y_i$ za sve $1 \le i \le n$. Na primer, $\mathbb{S}_n$ je n-tostruko tranzitivna grupa na $\{1, \ldots, n\}$ (što je samo drugi način da se kaže da $\mathbb{S}_n$ sadrži sve permutacije na n-elementom skupu), dok je $\mathbb{A}_n$ $(n-2)$-tostruko tranzitivna na istom skupu: ako imamo međusobno različite $x_1, \ldots, x_{n-2}$ kao i međusobno različite $y_1, \ldots, y_{n-2}$ tada parcijalnu injekciju $x_i \mapsto y_i$, $1 \le i \le n-2$ možemo proširiti do permutacije na tačno dva načina, od kojih će jedan biti parna, a drugi neparna permutacija.

stabilizator

Za $x \in X$, skup

$$G_x = \{g \in G : \; x^g = x\}$$

nazivamo *stabilizator* elementa x.

Propozicija 7.2. *Neka je G grupa i θ njeno dejstvo na skup X. Tada je za sve $x \in X$, $G_x \leq G$, i važi* kardinalnost orbite

$$|x^G| = (G : G_x).$$

Dokaz. Kako je $x^1 = x$, to je $1 \in G_x$. Dalje, neka je $g, h \in G_x$. Tada je $x^{gh} = (x^g)^h = x^h = x$, pa $gh \in G_x$. Takođe, $x \mapsto x^{g^{-1}}$ je inverzno preslikavanje permutacije $x \mapsto x^g$, pa $x^g = x$ povlači $x^{g^{-1}} = x$, tj. $g^{-1} \in G_x$. Zbog toga je $G_x \leq G$.

Definišimo sada preslikavanje $\psi : x^G \to \{G_x g : \ g \in G\}$ sa

$$\psi(x^g) = G_x g.$$

Ovo preslikavanje je dobro definisano, jer $x^g = x^h$ implicira $x^{gh^{-1}} = x$, tj. $gh^{-1} \in G_x$, $G_x g = G_x h$. Budući da važi i obratan lanac implikacija, sledi da je ψ injekcija, a očito je da je ψ "na". □

Posledica 7.3. *Ako je G grupa permutacija stepena n (dakle, $G \leq \mathbb{S}_n$) koja je k-tostruko tranzitivna, tada* rezultat o redu tranzitivnih grupa

$$k!\binom{n}{k} \,\Big|\, |G|.$$

Specijalno, red svake tranzitivne grupe permutacija stepena n je deljiv sa n.

Dokaz. Neka je

$$X_k = \{(x_1, \dots, x_k) : \ i \neq j \Rightarrow x_i \neq x_j\} \subseteq X^k.$$

Tada G deluje na skup X_k dejstvom θ_k datim sa

$$\theta_k((x_1, \dots, x_k), \pi) = (\pi(x_1), \dots, \pi(x_k)).$$

Po prethodnom tvrđenju,

$$|G| = |(x_1, \dots, x_k)^G| \cdot |G_{(x_1,\dots,x_k)}|.$$

Međutim, zbog uslova k-tostruke tranzitivnosti imamo da je $(x_1, \dots, x_k)^G = X_k$, pa dobijamo traženi rezultat iz $|X_k| = n(n-1)\dots(n-k+1) = k!\binom{n}{k}$. □

Jezgro dejstva θ, $\operatorname{Ker}\theta$, definišemo kao jezgro pridruženog homomorfizma ϕ u smislu Propozicije 7.1: u pitanju su svi elementi $g \in G$ takvi da je $x \mapsto x^g$ identičko preslikavanje (tj. presek svih stabilizatora). Po Teoremi o homomorfizmu, $G/\operatorname{Ker}\theta$ se potapa u $\mathbb{S}_X$ (tj. izmorfno je podgrupi od $\mathbb{S}_X$). jezgro dejstva

7.3 Dejstvo konjugovanjem i koset dejstvo

dejstvo konjugovanjem

Primer 7.4. Neka je G grupa i θ njeno dejstvo na sopstveni domen definisano sa $x^g = g^{-1}xg$ – ovo je *dejstvo konjugovanjem* (lako se proverava da su uslovi za dejstvo zaista zadovoljeni). Tada se jezgro ovog dejstva poklapa sa centrom $Z(G)$, jer je $x^g = x$ za sve $x \in G$ ako i samo ako $xg = gx$ za sve $x \in G$ ako i samo ako $g \in Z(G)$.

Orbite ovog desjtva su

$$x^G = \{g^{-1}xg : \ g \in G\} = \widetilde{x},$$

dakle, klase konjugovanosti. Stabilizator elementa x je

$$G_x = \{g \in G : \ g^{-1}xg = x\} = \{g \in G : \ gx = xg\},$$

tj. poklapa se sa centralizatorom $C(x)$.

koset dejstvo

Primer 7.5. Još jedan prirodan primer dejstva grupe je *koset dejstvo*, gde grupa G deluje na skup $\{Ha : \ a \in G\}$ desnih koseta neke podgrupe $H \leq G$. Pri tome je

$$(Ha)^g = Hag.$$

Odredimo jezgro ovog dejstva. Imamo da $g \in \operatorname{Ker}\theta$ ako i samo ako je $Hag = Ha$ za sve $a \in G$, a što je ekvivalentno sa $aga^{-1} \in H$ tj. $g \in a^{-1}Ha$ za sve $a \in G$. Prema tome, $\operatorname{Ker}\theta = \operatorname{core}(H)$ – jezgro koset dejstva je srž podgrupe H.

Pored toga, svako koset dejstvo je tranzitivno, budući da je orbita koseta $H = H1$ jednaka $H^G = \{Hg : \ g \in G\}$, skupu svih desnih koseta od H.

$n!$-teorema

Posledica 7.6 ($n!$-teorema)**.** *Ako grupa G ima podgrupu H indeksa n, tada ima i pravu normalnu podgrupu indeksa najviše $n!$.*

Dokaz. Ako je $(G : H) = n$, tada H ima tačno n desnih koseta u G, pa za koset dejstvo grupe G u odnosu na H važi da se $G/\operatorname{Ker}\theta$ potapa u $\mathbb{S}_n$. Prema tome, $|G/\operatorname{Ker}\theta| \leq n!$, pa je tako $\operatorname{Ker}\theta = \operatorname{core}(H)$ normalna podgrupa od G indeksa $\leq n!$. Ona je prava, jer je sadržana u H. □

Ovaj rezultat povlači da proste grupe ne mogu imati "velike" prave podgrupe, i to u sledećem smislu.

Posledica 7.7. *Ako je G prosta grupa i $H \leq G$ takva da je $(G : H) = n$ tada je $|G| \leq n!$ (štaviše, $|G| \mid n!$).*

Primer 7.8. Po Teoremi 6.4, grupa $\mathbb{A}_n$ je prosta za $n \geq 5$. Dakle, ako je $H \leq \mathbb{A}_n$ prava podgrupa, tada je $(\mathbb{A}_n : H) \geq n$, jer bi u suprotnom bilo $|\mathbb{A}_n| = \frac{1}{2}n! \leq (n-1)!$ – kontradikcija.

Zapravo, u prostoj grupi G za svaku pravu podgrupu H važi $\mathrm{core}(H) = E$, zbog čega je jezgro koset dejstva trivijalno i stoga se G može predstaviti kao grupa permutacija na skupu desnih koseta od H.

7.4 Bernsajdova lema

Ovu glavu završavamo rezultatom koji daje broj orbita dejstva konačne grupe na skup.

Propozicija 7.9 (Bernsajdova[5] lema)**.** *Neka je G konačna grupa koja deluje na skup X (putem θ), i označimo* $\mathrm{Fix}(g) = \{x \in X : x^g = x\}$ *za proizvoljno $g \in G$, skup svih fiksnih tačaka dejstva elementa g na X. Tada je broj orbita dejstva θ jednak*

Bernsajdova lema o broju orbita dejstva konačne grupe

$$|\{x^G : x \in X\}| = \frac{1}{|G|}\sum_{x\in X}|G_x| = \frac{1}{|G|}\sum_{g\in G}|\mathrm{Fix}(g)|.$$

Dokaz. Po Propoziciji 7.2 imamo da je za proizvoljno $x \in X$ kardinalnost njegove orbite $|x^G| = (G : G_x) = |G|/|G_x|$. Prema tome, $|G_x| = |G|/|x^G|$, pa je

$$\sum_{y\in x^G}|G_x| = |x^G|\frac{|G|}{|x^G|} = |G|.$$

Otuda sledi da je

$$\sum_{x\in X}|G_x| = |G|\cdot|\{x^G : x \in X\}|,$$

pa neposredno sledi prva jednakost. Druga jednakost je direktna posledica od

$$\sum_{x\in X}|G_x| = \sum_{g\in G}|\mathrm{Fix}(g)|,$$

što odmah uviđamo da važi budući da obe sume izražavaju kardinalnost skupa $\{(x,g) \in X \times G : x^g = x\}$. $\square$

[5] Vilijam Bernsajd (William Burnside, 1852–1927), britanski matematičar

8

Teoreme Silova

Po Lagranžovoj teoremi, ako je H podgrupa grupe G reda n, tada red $|H|$ deli n. U opštem slučaju, ne važi obrat ovog tvrđenja ("ako $k \mid n = |G|$ tada G ima podgrupu reda k"); najjednostavniji kontraprimer je grupa $\mathbb{A}_4$ koja je reda 12, ali nema podgrupu reda 6. Ipak, pitanje kada konačna grupa ima podgrupu određenog reda (kao i želja za stvaranjem "kataloga" svih konačnih grupa, do na izomorfizam) u ogromnoj meri je motivisalo razvoj teorije končnih grupa. Uz određena ograničenja u odnosu na k i n svaka grupa reda n ipak ima podgrupu reda k – na ovaj način su nastale tzv. *teoreme Silova*[6].

8.1 Košijeva lema

Istorijski gledano, prvi rezultat u upravo opisanom pravcu je sledeći. On se odnosi na slučaj kada je k prost broj.

Košijeva lema

Lema 8.1 (Košijeva lema)**.** *Neka je G konačna grupa i p prost broj takav da $p \mid |G|$. Tada G ima element reda p.*

Dokaz. Definišimo sledeći podskup od G^p:

$$A = \{(g_1, \dots, g_p) : \; g_1 \dots g_p = 1\}.$$

[6]Ludvig Silov (Peter Ludwig Mejdell Sylow, 1832–1918), norveški matematičar; poznat između ostalog i po tome što je zajedno sa Sofusom Lijem (Marius Sophus Lie, 1842–1899) sredio i objavio sabranu matematičku zaostavštinu N. H. Abela.

Ovaj podskup je kardinalnosti $|G|^{p-1}$ budući da se lako pokazuje da je preslikavanje $\psi : G^{p-1} \to A$ dato sa

$$\psi(g_1, \dots, g_{p-1}) = (g_1, \dots, g_{p-1}, (g_1 \cdots g_{p-1})^{-1})$$

bijekcija. Zaključujemo da je $|A|$ deljivo sa p.

Definišimo sada preslikavanje $\pi : G^p \to G^p$ sa

$$\pi(g_1, g_2, \dots, g_p) = (g_2, \dots, g_p, g_1).$$

Kako $xy = 1$ povlači $yx = 1$ u svakoj grupi, važi da je $\pi(A) \subseteq A$, pa umesto preslikavanja π možemo posmatrati njegovu restrikciju na A (što ćemo i činiti u ostatku dokaza). Lako se sada vidi da je π permutacija od A, a očito je da važi $\pi^p = \mathrm{id}_A$.

Konačno, definišimo sada dejstvo ciklične grupe $\mathbb{Z}_p$ na skup A određeno homomorfizmom (koje je zapravo potapanje) $\theta : \mathbb{Z}_p \to \mathbb{S}_A$ koji generator $\mathbb{Z}_p$ slika u π; dakle $\theta(\overline{1}) = \pi$ i stoga $\theta(\overline{m}) = \pi^m$ za sve $0 \leq m < p$. Stabilizator svake p-torke iz A je podgrupa od $\mathbb{Z}_p$, tako da je on ili 1-elementna podgrupa ili celo $\mathbb{Z}_p$. Iz Propozicije 7.2 sledi da svaka orbita posmatranog dejstva ima ili 1 ili p elemenata.

Pretpostavimo da imamo tačno k orbita, od kojih su j jednoelementne. Kako orbite čine particiju skupa A, zaključujemo da važi

$$|A| = j + p(k - j).$$

Sledi da $p \mid j$. Međutim, pri tome mora biti $j \geq 1$, jer postoji bar jedna p-torka iz A sa jednoelementom orbitom: to je, na primer, $(1, 1, \dots, 1)$. Otuda je $j \geq p \geq 2$, pa postoji bar još jedna p-torka sa jednoelementnom orbitom. U toj p-torci su sve ciklične permutacije jednake, pa ona mora biti oblika $(g, g, \dots, g)$. Kako ona pripada A, sledi da je $g^p = 1$, tj. $o(g) = p$. □

Za prost broj p, grupa G je *p-grupa* ako za svako $g \in G$ ($g \neq 1$) postoji $n \geq 1$ tako da je $o(g) = p^n$. Košijeva lema nam omogućava da opišemo redove konačnih p-grupa. p-grupe

Lema 8.2. *Neka je p prost broj. Konačna grupa je p-grupa ako i samo ako je $|G| = p^n$ za neko $n \geq 1$.*

Dokaz. ($\Rightarrow$) Neka je q prost broj, $q \neq p$. Ako bi $q \mid |G|$, tada bi po Košijevoj lemi G imala element reda q, što je suprotno definiciji p-grupe. Dakle, p je jedini prost faktor broja $|G|$, pa je $|G| = p^n$ za neko n. Obrat ($\Leftarrow$) sledi direktno iz Lagranžove teoreme. □

Priferove grupe: primer beskonačnih p-grupa

Primer 8.3. Za sve proste brojeve p postoje i beskonačne p-grupe. Najpoznatiji primer su *Priferove*[7] ili *kvaziciklične grupe* $\mathbb{Z}_{p^\infty}$, podgrupe multiplikativne grupe $\mathbb{C}^\times$ kompleksnih brojeva određene sa

$$\{z \in \mathbb{C} : \ z^{p^n} = 1 \text{ za neko } n \geq 1\}.$$

Grupe $\mathbb{Z}_{p^\infty}$ imaju sledeće zanimljivo svojstvo: one su beskonačne, ali je svaka njihova prava podgrupa konačna (i zapravo ciklična). Naime, za $A \subseteq \mathbb{Z}_{p^\infty}$ važi da je $\langle A \rangle = \mathbb{Z}_{p^\infty}$ ako i samo ako je skup A beskonačan; u suprotnom, ako je A konačan, tada je $\langle A \rangle \cong \mathbb{Z}_{p^m}$, gde je $p^m = \max_{z \in A} o(z)$.

8.2 Prva teorema Silova

Prva teorema Silova predstavlja suštinsko pojačanje Košijeve leme.

prva teorema Silova

Teorema 8.4 (Prva teorema Silova)**.** *Neka je G konačna grupa, $|G| = p^n k$, gde je p prost broj i $n, k \geq 1$ takvi da $p \nmid k$ (dakle, izdvojili smo najviši stepen kojim p deli $|G|$). Tada G ima podgrupu reda p^n.*

Dokaz. Dokaz izvodimo indukcijom po redu grupe G. Bazu indukcije predstavljaju slučajevi $n = 1$, odnosno $k = 1$. Slučaj $k = 1$ je trivijalan, dok u slučaju $n = 1$ tvrđenje sledi iz Košijeve leme. Zato pretpostavimo da tvrđenje teoreme važi za sve grupe reda $p^{n'} k'$ gde je ili $1 \leq n' < n$, ili $1 \leq k' < k$ (pri čemu $p \nmid k'$).

Ako G ima pravu podgrupu H takvu da $p \nmid (G : H)$, tada iz $|H|(G : H) = |G| = p^n k$ sledi da je $|H| = p^n k'$. Kako $p \nmid k'$, po induktivnoj pretpostavci sledi da H ima podgrupu reda p^n koja je, naravno, podgrupa i u G.

U suprotnom, za sve prave podgrupe H od G važi $p \mid (G : H)$. Tada klasovna jednačina povlači da je red centra $Z(G)$ deljiv sa p, pa po Košijevoj lemi postoji $a \in Z(G)$ tako da je $o(a) = p$. Ako je $K = \langle a \rangle$, tada je $K \leq Z(G)$ i stoga $K \trianglelefteq G$. Pored toga, važi $|G/K| = p^{n-1} k$, pa po induktivnoj pretpostavci G/K ima podgrupu W reda p^{n-1}. Po Teoremi o korespondenciji, W mora biti oblika H/K za neku podgrupu H takvu da je $K \trianglelefteq H \leq G$ (naime, za $H = \nu_K^{-1}(W)$, gde je $\nu_K : G \to G/K$ prirodni homomorfizam). No, sada je

$$|H| = |H/K| \cdot |K| = |W| \cdot |K| = p^{n-1} \cdot p = p^n.$$

Time je okončan induktivni dokaz. □

[7] Hajnc Prifer (Ernst Paul Heinz Prüfer 1896–1934), nemački matematičar

Ako je G konačna grupa takva da je $|G| = p^n k$, gde je $n, k \geq 1$ i $p \nmid k$, tada svaku podgrupu od G reda p^n zovemo *p-podgrupa Silova* od G. Prema tome, prethodna teorema tvrdi da p-podgrupe Silova grupe G postoje za svaki prost broj p koji deli red $|G|$.

8.3 Druga teorema Silova

Druga teorema Silova tvrdi da su p-podgrupama Silova iscrpljene sve maksimalne (u smislu poretka indukovanog skupovnom inkluzijom) p-podgrupe od G, dalje, da su p-podgrupe Silova konjugovane, a daje i korisne kvantitativne informacije o njima. No, najpre nam treba pomoćno tvrđenje.

Lema 8.5. *Neka je P p-podgrupa Silova konačne grupe G, a H neka njena p-podgrupa. Tada je $H \leq N(P)$ ako i samo ako je $H \leq P$.*

Dokaz. ($\Rightarrow$) Pretpostavimo da je $H \leq N(P)$. Tada je $hP = Ph$ za sve $h \in H$, pa je $HP = PH$ podgrupa od G. Štaviše, $P \trianglelefteq HP$ (jer je $HP \leq N(P)$). Po Prvoj teoremi o izomorfizmu (u odnosu na grupu HP) je $H \cap P \trianglelefteq H$ i $HP/P \cong H/H \cap P$, pa je

$$|HP| = \frac{|H| \cdot |P|}{|H \cap P|}.$$

Kako je $H \cap P \leq H$, $H \cap P$ je p-podgrupa od G. Iz gornje jednakosti sada sledi da je i HP p-podgrupa od G. No, s druge strane imamo $P \leq HP$, pri čemu je P p-podgrupa Silova od G, pa mora biti $HP = P$. Otuda je $|H| = |H \cap P|$, pa kako se radi o konačnim grupama, dobijamo da je $H = H \cap P$, tj. $H \leq P$.

($\Leftarrow$) Trivijalno, budući da je $P \leq N(P)$. □

Teorema 8.6 (Druga teorema Silova)**.** *Neka je p prost broj i G konačna grupa, $|G| = p^n k$ za neke $n, k \geq 1$ takve da $p \nmid k$.* druga teorema Silova

(i) Svaka p-podgrupa od G sadržana je u nekoj p-podgrupi Silova od G.

(ii) Svake dve p-podgrupe Silova od G su konjugovane.

(iii) Broj svih p-podgrupa Silova od G je $s_p = (G : N(P))$, gde je P proizvoljna p-podgrupa Silova. Pri tome je $s_p \equiv 1 (\mathrm{mod}\ p)$ i $s_p \mid k$.

Dokaz. Ako je P p-podgrupa Silova od G, tada za prozivoljno $g \in G$ imamo $g^{-1}Pg \leq G$ i $|g^{-1}Pg| = |P|$, pa je i $g^{-1}Pg$ takođe p-podgrupa Silova od

G. Zbog toga, G deluje konjugovanjem na skup $A = \{g^{-1}Pg : \ g \in G\}$; preciznije, dejstvo je dato sa

$$\theta(g^{-1}Pg, a) = a^{-1}(g^{-1}Pg)a = (ga)^{-1}Pga.$$

Ovo dejstvo je tranzitivno, jer očito važi $\theta(g^{-1}Pg, a) = h^{-1}Ph$ za $a = g^{-1}h$. Stabilizator elementa $g^{-1}Pg$ je

$$\{a \in G : \ (ga)^{-1}Pga = g^{-1}Pg\} = N(g^{-1}Pg).$$

Neka je sada H proizvoljna p-podgrupa od G, i neka je θ_0 restrikcija upravo definisanog dejstva θ na podgrupu H. (Dakle, umesto dejstva $\theta : A \times G \to A$ posmatramo $\theta_0 : A \times H \to A$.) Ako sa $H_{g^{-1}Pg}$ označimo stabilizator elementa $g^{-1}Pg \in A$ u odnosu na θ_0, po Propoziciji 7.2 imamo

$$|(g^{-1}Pg)^H| = (H : H_{g^{-1}Pg}),$$

što znači da su sve orbite dejstva θ_0 ili jednoelementne, ili kardinalnosti koja je deljiva sa p. Pri tome je orbita $|(g^{-1}Pg)^H|$ jednoelementna ako i samo ako je $(ga)^{-1}Pga = g^{-1}Pg$ za sve $a \in H$, što je pak ekvivalentno sa $H \leq N(g^{-1}Pg)$. Po prethodnoj lemi, poslednja inkluzija važi ako i samo ako je $H \leq g^{-1}Pg$.

Kako orbite od θ_0 čine particiju skupa A, sledi da je

$$|A| \equiv |\{g^{-1}Pg : \ H \leq g^{-1}Pg\}| (\mathrm{mod}\ p).$$

Pri tome, primetimo da gornja kongruencija važi za *proizvoljnu* p-podgrupu H od G (pa tako imamo slobodu da je po želji variramo). Tako, ako odaberemo $H = P$, odmah sledi da je

$$|A| \equiv 1 (\mathrm{mod}\ p),$$

jer $P \leq g^{-1}Pg$ povlači $P = g^{-1}Pg$, pa je $\{g^{-1}Pg : \ P \leq g^{-1}Pg\} = \{P\}$. Zbog toga, za bilo koju p-podgrupu $H \leq G$ važi

$$|\{g^{-1}Pg : \ H \leq g^{-1}Pg\}| \equiv 1 (\mathrm{mod}\ p).$$

To, između ostalog, znači da je skup $\{g^{-1}Pg : \ H \leq g^{-1}Pg\}$ neprazan, čime je stavka (i) dokazana: za bilo koju p-podgrupu H postoji (bar jedna) p-podgrupa Silova $g^{-1}Pg \leq G$ koja sadrži H.

Ako su sada P, Q proizvoljne p-podgrupe Silova od G, po prethodno dokazanom postoji $g \in G$ tako da je $Q \leq g^{-1}Pg$. Međutim, kako je $|Q| = |P| = |g^{-1}Pg|$, ovo je moguće samo ako je $Q = g^{-1}Pg$. Dakle, važi (ii): svake dve p-podgrupe Silova grupe G su konjugovane.

Najzad, primetimo da je s_p zapravo kardinalnost jedinsvene orbite $P^G = A$ tranzitivnog dejstva θ grupe G na A, $s_p = |A|$. Po Propoziciji 7.2 imamo $s_p = (G : G_P) = (G : N(P))$, pošto smo već dokazali da je stabilizator od P baš $N(P)$. Odavde sledi da $s_p \mid p^n k = |G|$, a već smo pokazali da je $s_p \equiv 1 (\mathrm{mod}\ p)$. Zbog toga $s_p \mid k$, pa važi (iii). $\square$

Odmah beležimo sledeću značajnu primedbu.

Primer 8.7. Ako je p prost broj koji deli red grupe G, tada važi $s_p = 1$ znači da postoji jedinstvena p-podgrupa Silova $P \leq G$, i tada po prethodnoj teoremi (stavka (ii)) mora biti $P \trianglelefteq G$. Zbog toga u svakoj Abelovoj grupi G imamo $s_p = 1$ za sve proste brojeve p koji dele $|G|$. Međutim, postoje i druge grupe u kojima važi ovaj uslov; zapravo, u klasi konačnih grupa ovaj uslov karakteriše tzv. *nilpotentne grupe*.

Za radoznalce

Nilpotentne grupe predstavljaju uopštenje Abelovih, i nalaze se "između" Abelovih i *rešivih* grupa koje ćemo izučavati u Glavi 12. Uslov nilpotentnosti za konačne grupe (jedinstvenost, i stoga normalnost, svake podgrupe Silova) ima čitav niz ekvivalenata, a ovde pominjemo samo dva: konačna grupa je nilpotetna ako i samo ako je izomorfna direktnom proizvodu svih svojih podgrupa Silova, odnosno ako i samo ako svaka dva njena elementa uzajamno prostih redova komutiraju. Grupa kvaterniona Q_8 je primer nilpotentne grupe koja nije Abelova.

Konstatacija iz prethodnog primera ($s_p = 1 \Rightarrow$ jedinstvena p-podgrupa Silova je normalna u G) daje jednu od mnogih primena teorema Silova: budući da one pružaju mogućnost za nalaženje netrivijalnih normalnih podgrupa posmatrane konačne grupe, one se mogu iskoristiti za dokazivanje da grupe određenog reda ne mogu biti proste. Ovakav način primene teorema Silova ilustrujemo kroz sledeće tvrđenje.

Propozicija 8.8. *Neka su p, q dva različita prosta broja i G grupa reda p^2q. Tada G nije prosta.*

grupe reda p^2q nisu proste

Dokaz. Koristeći Drugu teoremu Silova dobijamo da je $s_p \in \{1, q\}$ i $s_q \in \{1, p, p^2\}$. Ako je $s_p = 1$ ili $s_q = 1$, dokaz je završen, jer smo našli netrivijalnu normalnu podgrupu od G. Zato pretpostavimo da je $s_p = q$ i $s_q \in \{p, p^2\}$. Tada je $q \equiv 1 (\mathrm{mod}\ p)$, pa je $q > p$, što odmah onemogućava slučaj $s_q = p$ (jer bi tada bilo $p \equiv 1 (\mathrm{mod}\ q)$ i stoga $p > q$). Prema tome, važi $s_q = p^2 \equiv 1 (\mathrm{mod}\ q)$; drugim rečima, $q \mid p^2 - 1 = (p-1)(p+1)$. Ponovo, ne može biti $q \mid p - 1$, pa $q \mid p + 1$, zbog čega je $q \leq p + 1$. Kako je $p < q$, sledi da je $q = p + 1$, tj. $p = 2$, $q = 3$.

Znači, preostaje razmatranje grupa reda 12 (kompletna klasifikacija ovih grupa biće izvršena nešto kasnije, u Glavi 10). Zapravo, zanima nas da li je moguće da je pri tome $s_2 = 3$ i $s_3 = 4$. Neka su Q_1, Q_2, Q_3, Q_4 3-podgrupe Silova grupe G reda 12. One su ciklične grupe reda 3, pa za $i \neq j$ važi $Q_i \cap Q_j = E$, zbog čega je $|Q_1 \cup Q_2 \cup Q_3 \cup Q_4| = 9$. (Drugim rečima, G ima 8 elemenata reda 3.) S druge strane, ako je P bilo koja 2-podgrupa Silova od G, tada je $|P| = 4$ i svi njeni nejedinični elementi su reda 2 ili 4. To mogu biti samo preostala 3 elementa grupe G, pa sledi da je 2-podgrupa Silova od G jedinstvena, što je u suprotnosti sa $s_2 = 3$. Kontradikcija. $\square$

9

Konačne Abelove grupe

U ovoj glavi, cilj je da se dokaže *Fundamentalna teorema o konačnim Abelovim grupama*.

Teorema 9.1. *Neka je G Abelova grupa konačnog reda n. Tada je G izomorfna direktnom proizvodu cikličnih grupa, gde je red svake od tih cikličnih grupa stepen prostog broja; drugim rečima, važi* fundamentalna teorema o konačnim Abelovim grupama

$$G \cong \mathbb{Z}_{p_1^{m_1}} \times \cdots \times \mathbb{Z}_{p_t^{m_t}}$$

za (ne nužno različite) proste brojeve $p_1, \dots, p_t$ i $m_1, \dots, m_t \geq 1$ takve da je $n = p_1^{m_1} \dots p_t^{m_t}$. Pri tome je gornje direktno razlaganje do na permutaciju faktora jednoznačno određeno grupom G.

Dokaz ove značajne teoreme sprovodimo u nekoliko faza, tačnije u četiri "etape". Najpre pokazujemo da se, pod određenim "blagim" uslovima, dati generatorni skup konačno generisane Abelove grupe može zameniti drugim generatornim skupom u kojem figuriše unapred zadati element.

Lema 9.2. *Neka je $G = \langle x_1, \dots, x_d \rangle$ Abelova grupa i*

$$y = x_1^{k_1} \dots x_d^{k_d}$$

njen element takav da je $(k_1, \dots, k_d) = 1$. Tada postoje $y_2, \dots, y_d \in G$ tako da je

$$G = \langle y, y_2, \dots, y_d \rangle.$$

Dokaz. Dokaz izvodimo indukcijom po d. Najpre, ako je $d = 1$, tada je po datom uslovu $k_1 \in \{1, -1\}$, pa odmah imamo da je $\langle y \rangle = \langle x_1 \rangle = G$.

Neka je sada $d = 2$. Tada, budući da pretpostavljamo da je $(k_1, k_2) = 1$, postoje $\alpha, \beta \in \mathbb{Z}$ tako da je

$$\alpha k_1 + \beta k_2 = 1.$$

Stoga, ako definišemo $y_2 = x_1^{\beta} x_2^{-\alpha}$, imamo (ne zaboravljajući komutativnost u grupi G):

$$\begin{aligned} x_1 = x_1^{\alpha k_1 + \beta k_2} &= x_1^{\alpha k_1} x_1^{\beta k_2} x_2^{\alpha k_2} x_2^{-\alpha k_2} \\ &= x_1^{\alpha k_1} x_2^{\alpha k_2} x_1^{\beta k_2} x_2^{-\alpha k_2} \\ &= (x_1^{k_1} x_2^{k_2})^{\alpha} (x_1^{\beta} x_2^{-\alpha})^{k_2} \\ &= y^{\alpha} y_2^{k_2} \in \langle y, y_2 \rangle. \end{aligned}$$

Slično,

$$\begin{aligned} x_2 = x_2^{\alpha k_1 + \beta k_2} &= x_1^{\beta k_1} x_2^{\beta k_2} x_1^{-\beta k_1} x_2^{\alpha k_1} \\ &= (x_1^{k_1} x_2^{k_2})^{\beta} (x_1^{\beta} x_2^{-\alpha})^{-k_1} \\ &= y^{\beta} y_2^{-k_1} \in \langle y, y_2 \rangle. \end{aligned}$$

Tako je $G = \langle x_1, x_2 \rangle \subseteq \langle y, y_2 \rangle \subseteq G$, pa je $G = \langle y, y_2 \rangle$.

Konačno, neka je $d \geq 3$ i pretpostavimo da tvrđenje leme važi za sve Abelove grupe sa $< d$ generatora. Neka je $t = (k_1, \ldots, k_{d-1})$ i $m_i = k_i / t$ za sve $1 \leq i \leq d - 1$. Definišimo

$$z = x_1^{m_1} \ldots x_{d-1}^{m_{d-1}}.$$

Po konstrukciji, $(m_1, \ldots, m_{d-1}) = 1$, pa možemo primeniti induktivnu pretpostavku koja garantuje postojanje elemenata $y_2, \ldots, y_{d-1} \in G$ za koje je

$$\langle x_1, \ldots, x_{d-1} \rangle = \langle z, y_2, \ldots, y_{d-1} \rangle.$$

Primetimo da je

$$y = x_1^{k_1} \ldots x_{d-1}^{k_{d-1}} x_d^{k_d} = (x_1^{t m_1} \ldots x_{d-1}^{t m_{d-1}}) x_d^{k_d} = z^t x_d^{k_d},$$

kao i da važi $(t, k_d) = (k_1, \ldots, k_{d-1}, k_d) = 1$. Stoga nam slučaj $d = 2$ obezbeđuje element $y_d \in G$ takav da je

$$\langle z, x_d \rangle = \langle y, y_d \rangle.$$

Tako je

$$\begin{aligned} G &= \langle x_1, \ldots, x_{d-1}, x_d \rangle = \langle x_1, \ldots, x_{d-1} \rangle \langle x_d \rangle = \langle z, y_2, \ldots, y_{d-1} \rangle \langle x_d \rangle = \\ &= \langle z, y_2, \ldots, y_{d-1}, x_d \rangle = \langle z, x_d \rangle \langle y_2, \ldots, y_{d-1} \rangle = \\ &= \langle y, y_d \rangle \langle y_2, \ldots, y_{d-1} \rangle = \langle y, y_2, \ldots, y_d \rangle, \end{aligned}$$

čime je induktivni dokaz okončan. □

Propozicija 9.3. *Svaka konačno generisana Abelova grupa je izomorfna direktnom proizvodu cikličnih grupa.*

Dokaz. Neka je $G = \langle x_1, \ldots, x_d \rangle$; dokaz izvodimo indukcijom po d. Naravno, ako je $d = 1$ tada je grupa G ciklična i propozicija sledi neposredno.

Zato, pretpostavimo da je $d \geq 2$ i da tvrđenje važi za sve Abelove grupe generisane sa $< d$ elemenata. Pri tome, pretpostavimo da je d najmanje moguće, odnosno da smo uočili po kardinalnosti minimalan generatorni skup za G. Štaviše, bez ograničenja opštosti, možemo pretpostaviti da smo za tu fiksiranu vrednost d među svim generatornim skupovima za G od d elemenata uočili onaj kod koga je red $o(x_1)$ najmanji.

Posmatrajmo podgrupe $H = \langle x_1 \rangle$ i $K = \langle x_2, \ldots, x_d \rangle$ od G. Tvrdimo da je G unutrašnji direktan proizvod od H i K. Zaista, $H, K \trianglelefteq G$, budući da je G Abelova grupa. Pored toga, $HK = \langle x_1 \rangle \langle x_2, \ldots, x_d \rangle = \langle x_1, \ldots, x_d \rangle = G$. Prema tome, preostaje da se pokaže da je $H \cap K = E$.

Pretpostavimo suprotno, tj. da $H \cap K$ sadrži element

$$g = x_1^{m_1} = x_2^{m_2} \ldots x_d^{m_d}$$

različit od jedinice grupe G, pri čemu je $1 \leq m_1 < o(x_1)$. Definišimo $t = (m_1, m_2, \ldots, m_d)$, zatim $k_i = m_i/t$ za $1 \leq i \leq d$ i, najzad,

$$y = x_1^{-k_1} x_2^{k_2} \ldots x_d^{k_d}.$$

Po konstrukciji, $(-k_1, k_2, \ldots, k_d) = 1$, pa po prethodnoj lemi postoje elementi $y_2, \ldots, y_d \in G$ tako da je $G = \langle y, y_2, \ldots, y_d \rangle$. Ako bi bilo $y = 1$ imali bismo da je $G = \langle y_2, \ldots, y_d \rangle$, što je u suprotnosti sa pretpostavljenom minimalnošću d. No, sada je

$$y^t = x_1^{-m_1} x_2^{m_2} \ldots x_d^{m_d} = 1,$$

pa mora biti $o(y) \leq t \leq m_1 < o(x_1)$, a što je pak kontradikcija sa izborom generatornog skupa $\{x_1, \ldots, x_d\}$ načinjenog na početku dokaza. Stoga, mora biti $H \cap K = E$.

Dakle, $G \cong H \times K$, gde je H ciklična grupa, a K je Abelova grupa generisana sa $d-1$ elemenata. Po induktivnoj pretpostavci, K je izomorfno direktnom proizvodu cikličnih grupa, pa zato ista konstatacija sada važi i za G. $\square$

Primetimo da do sada uopšte nismo koristili uslov *konačnosti* posmatrane Abelove grupe. Sada ćemo se podsetiti dobro poznatog tvrđenja o konačnim cikličnim grupama.

Lema 9.4. *Ako je* $(m, n) = 1$ *tada važi*

$$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n.$$

Prema tome, ako je $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ *razlaganje prirodnog broja* n *na proste faktore (gde su* $p_1, \dots, p_r$ *različiti prosti brojevi) tada je*

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_r^{\alpha_r}}.$$

Zajedno sa prethodnom propozicijom, ova lema neposredno daje prvi deo Fundamentalne teoreme, tj. pokazuje egzistenciju opisanog razlaganja Abelove grupe G. Kako bismo kompletirali dokaz, preostaje da se pokaže (suštinska) jedinstvenost tog razlaganja.

Propozicija 9.5. *Razlaganje konačne Abelove grupe* G *u direktan proizvod cikličnih grupa čiji je red stepen nekog prostog broja je jedinstven do na poredak faktora u direktnom proizvodu.*

Dokaz. Fiksirajmo neki prost broj p koji deli red grupe G. Pretpostavimo da je – u nekom razlaganju G na proizvod cikličnih grupa – $\mathbb{Z}_{p^t}$ najveći ciklični faktor čiji je red stepen od p. Za $1 \leq i \leq t$, neka α_i označava broj faktora u tom razlaganju koji su izomorfni sa $\mathbb{Z}_{p^i}$. Tvrdimo da su brojevi $\alpha_1, \dots, \alpha_t$ potpuno određeni grupom G. Radi preglednijeg zapisa, pretpostavimo da je $G \cong G_1 \times \cdots \times G_k$ posmatrano razlaganje G u direktan proizvod cikličnih grupa.

Najpre želimo da prebrojimo elemente u G čiji red deli posmatrani prost broj p (dakle, koji su reda 1 ili p), tj. k-torke

$$\mathbf{x} = (x_1, \dots, x_k) \in G_1 \times \cdots \times G_k$$

koje zadovoljavaju uslov $\mathbf{x}^p = 1$. Jasno, ovo će se desiti ako i samo ako važi $x_i^p = 1$ u svakoj pojedinačnoj cikličnoj grupi G_i, $1 \leq i \leq k$. Ako red $|G_i|$ *nije* stepen prostog broja p, tada je, jasno, jedini izbor $x_i = 1$ (ovde 1 označava jedinični element grupa G_i). U suprotnom, $G_i \cong \mathbb{Z}_{p^m}$ za neko $m \geq 1$, pa tada x_i možemo izabrati na p načina, jer su u grupi $\mathbb{Z}_{p^m}$ klase ostataka reda 1 ili p sledeće: $\overline{0}, \overline{p^{m-1}}, \overline{2p^{m-1}}, \ldots, \overline{(p-1)p^{m-1}}$. Dakle, broj načina na koji možemo izabrati element $\mathbf{x} \in G$ je

$$p^{\alpha_1} \ldots p^{\alpha_t} = p^{\alpha_1 + \cdots + \alpha_t}.$$

Sada prelazimo na prebrajanje elemenata $\mathbf{x}$ grupe G čiji red deli p^2 (dakle, čiji je red 1, ili p, ili p^2). Slično kao i malopre, za one "koordinate" i za koje $|G_i|$ nije stepen od p jedini izbor je $x_i = 1$. Ako je pak $G_i \cong \mathbb{Z}_p$ tada svih p elemenata grupe G_i dolaze u obzir kao moguće vrednosti za x_i (budući da tražimo da bude $x_i^{p^2} = 1$). Najzad, ako je $G_i \cong \mathbb{Z}_{p^m}$ za neko $m \geq 2$, tada G_i ima tačno p^2 elemenata x_i koji zadovoljavaju traženi uslov (tj. u $\mathbb{Z}_{p^m}$ imamo p^2 klasa ostataka čiji red deli p^2, to su: $\overline{0}, \overline{p^{m-2}}, \overline{2p^{m-2}}, \ldots, \overline{(p^2-1)p^{m-1}}$). Tako, broj načina na koji možemo izabrati element $\mathbf{x}$ za koji će važiti $\mathbf{x}^{p^2} = 1$ je

$$p^{\alpha_1} (p^2)^{\alpha_2} \ldots (p^2)^{\alpha_t} = p^{\alpha_1 + 2\alpha_2 + \cdots + 2\alpha_t}.$$

Analognim zaključivanjem, za $1 \leq j \leq t$ dobijamo da je broj elemenata grupe G čiji red deli p^j jednak

$$p^{\alpha_1} (p^2)^{\alpha_2} \ldots (p^j)^{\alpha_j} \ldots (p^j)^{\alpha_t} = p^{\alpha_1 + 2\alpha_2 + \cdots + j\alpha_j + \cdots + j\alpha_t}.$$

Prema tome, sledeći niz brojeva je jedinstveno određen grupom G:

$$\begin{gathered}
\alpha_1 + \alpha_2 + \alpha_3 + \cdots + \alpha_t \\
\alpha_1 + 2\alpha_2 + 2\alpha_3 + \cdots + 2\alpha_t \\
\alpha_1 + 2\alpha_2 + 3\alpha_3 + \cdots + 3\alpha_t \\
\vdots \\
\alpha_1 + 2\alpha_2 + 3\alpha_3 + \cdots + t\alpha_t
\end{gathered}$$

Oduzimanjem svakog od ovih zbirova od sledećeg u nizu, zaključujemo da je sledeći niz brojeva jedinstveno određen grupom G:

$$\begin{aligned}
\alpha_1 + \alpha_2 + \alpha_3 + \cdots + \alpha_t \\
\alpha_2 + \alpha_3 + \cdots + \alpha_t \\
\alpha_3 + \cdots + \alpha_t \\
\vdots \\
\alpha_t
\end{aligned}$$

odakle pak odmah sledi da su pojedinačni brojevi $\alpha_t, \alpha_{t-1}, \ldots, \alpha_1$ jedinstveno određeni grupom G.

Kako ovaj argument važi za bilo koji prost delitelj reda grupe G, tvrđenje sledi. $\square$

Za radoznalce

Fundamentalna teoreme koju smo razmatrali u ovoj glavi ima svoje uopštenje za proizvoljne konačno generisane Abelove grupe.

Teorema 9.6 (Fundamentalna teorema o konačno generisanim Abelovim grupama)**.** *Neka je A konačno generisana Abelova grupa. Tada postoji konačna podgrupa $G \leq A$ i ceo broj $k \geq 0$ tako da je*

$$A \cong G \times \mathbb{Z}^k.$$

Prema tome, i dalje važi da su konačno generisane Abelove grupe iscrpljene direktnim proizvodima konačno mnogo cikličnih grupa; jedina razlika u odnosu na konačan slučaj je u tome što neke od tih cikličnih grupa mogu biti beskonačne.

10

Grupe malog reda

U ovoj glavi naš cilj će biti da na osnovu prethodnih teorijskih rezultata "izgradimo" katalog grupa malog reda – do 15 elemenata. Pri tome ćemo zapravo dobiti dva opštija tvrđenja koja klasifikuju grupe reda p^2 (gde je p prost broj) i reda $2p$ (gde je p neparan prost broj); takođe ćemo zabeležiti bitnu primedbu u vezi sa grupama reda pq (gde su p, q različiti prosti brojevi).

10.1 Grupe reda p^2 i pq

Primetimo da za svaki prost broj p postoji samo jedna grupa reda p: to je ciklična grupa $\mathbb{Z}_p$. Time smo automatski opisali sve grupe reda 2,3,5,7,11,13, 17,19,... Prema tome, prvi zadatak nam je da razmotrimo grupe reda 4, pa zato odmah prelazimo na analizu grupa reda p^2 za proste brojeve p.

Lema 10.1. *Ako je $G/Z(G)$ ciklična grupa, tada je G Abelova.*

Dokaz. Neka je $g \in G$ takav da je $G/Z(G) = \langle Z(G)g \rangle$. Tada svaki element grupe G pripada kosetu oblika $Z(G)g^n$ za neko $n \in \mathbb{Z}$, pa je $G = \langle \{g\} \cup Z(G) \rangle$. Sada smo našli generatorni skup od G čija svaka dva elementa komutiraju, pa G mora biti Abelova grupa. $\square$

Propozicija 10.2. *Neka je p prost broj. Svaka grupa G reda p^2 je Abelova, pa je $G \cong \mathbb{Z}_{p^2}$ ili $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$.* opis grupa reda p^2

Dokaz. Po Posledici 3.4 klasovne jednačine, G ima netrivijalan centar; preciznije, p deli $|Z(G)|$. Ako je $|Z(G)| = p^2$, grupa G je Abelova, pa po Fundamentalnoj teoremi o konačnim Abelovim grupama dobijamo dve grupe iz formulacije propozicije. U suprotnom, $|Z(G)| = p$. Ali, tada je $|G/Z(G)| = p$, pa $G/Z(G)$ mora biti ciklična grupa. No, tada je po prethodnoj lemi G Abelova, što je u kontradikciji sa $|Z(G)| = p$ (tj. $Z(G) \lneq G$). Prema tome, postoje samo dve navedene grupe reda p^2, i obe su Abelove. □

Time smo opisali sve grupe reda 4,9,25,...

opis grupa reda pq kada $p \nmid q-1$

Propozicija 10.3. *Neka su $p < q$ prosti brojevi. Ako $p \nmid q-1$ tada je $\mathbb{Z}_{pq}$ (do na izomorfizam) jedina grupa reda pq.*

Dokaz. Neka je G grupa reda pq. Kako $s_q \mid p$ i $s_q \equiv 1 (\mathrm{mod}\ q)$, odmah sledi da je $s_q = 1$. Međutim, važi i $s_p \mid q$ i $s_p \equiv 1 (\mathrm{mod}\ p)$. Po datom uslovu otpada mogućnost da je $s_p = q$, pa sledi da je $s_p = 1$. Dakle, G ima jedinstvenu (i stoga normalnu) p-podgrupu Silova $P \cong \mathbb{Z}_p$, kao i jedinstvenu q-podgrupu Silova $Q \cong \mathbb{Z}_q$. Sada je očito $PQ = G$ i $P \cap Q = E$, pa je G unutrašnji direktan proizvod od P i Q. Sledi da je $G \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$. □

Tako je, na primer, jedina grupa reda 15 je ciklična grupa $\mathbb{Z}_{15}$.

Za radoznalce

grupe reda pq kada $p \mid q-1$

"Opšte kulture" radi, pomenimo da u slučaju kada $p \mid q-1$ postoje tačno dve grupe reda pq: Abelova grupa $\mathbb{Z}_{pq}$, kao i jedna nekomutativna grupa (sa normalnom q-podgrupom Silova i q različitih p-podgrupa Silova). U slučaju kada je $p = 2$, u pitanju je upravo dijedarska grupa D_q (vidi naredni odeljak). Ova grupa nastaje konstrukcijom tzv. *poludirektnog proizvoda*: u njoj se pojavljuju, kao i kod direktnih proizvoda, dve podgrupe A, B grupe G takve da je $AB = G$ i $A \cap B = E$, međutim, sada samo od podgrupe B zahtevamo da bude normalna. Tada pišemo $G = A \ltimes B$.

Postoji i "spoljašnji" pandan konstrukcije poludirektnog proizvoda, koji polazi od dve grupe G_1 i G_2, i čija definicija zahteva jedan homomorfizam

$$\phi : G_1 \to \mathrm{Aut}(G_2).$$

Tako dobijenu grupu označavamo sa $G_1 \ltimes_\phi G_2$. Pomenuta nekomutativna grupa reda pq se dobija kao poludirektan proizvod $\mathbb{Z}_p \ltimes_\psi \mathbb{Z}_q$ i njegova konskrucija (i jedinstvenost) se zasniva na činjenici da je za prost broj q, grupa automorfizama $\mathrm{Aut}(\mathbb{Z}_q)$ izomorfna cikličnoj grupi $\mathbb{Z}_{q-1}$, kao i fundamentalnom rezultatu iz teorije brojeva koji tvrdi da u odnosu na svaki prost modul postoji tzv. *primitivni koren* (odnosno, da je grupa invertibilnih elemenata $\mathbb{Z}_p^\times$ monoida $(\mathbb{Z}_p, \cdot_p)$ ciklična kadgod je p prost broj, pri čemu primitivnim korenom zovemo svaki generator potonje ciklične grupe).

10.2 Grupe reda $2p$

Propozicija 10.4. *Neka je p neparan prost broj i G grupa reda $2p$. Tada je $G \cong \mathbb{Z}_{2p}$ ili $G \cong D_p$.* opis grupa reda $2p$

Dokaz. Ako G ima element reda $2p$, tada je očito $G \cong \mathbb{Z}_{2p}$.

U suprotnom, svi nejedinični elementi grupe G su reda p ili 2. Kao i u prethodnoj propoziciji, $s_p = 1$, pa G ima jedinstvenu p-podgrupu Silova $P \cong \mathbb{Z}_p$. Ona je generisana bilo kojim svojim nejediničnim elementom (reda p); neka je a jedan od njih, $P = \langle a \rangle$. Sada je $(G : P) = 2$, pa $P \trianglelefteq G$ ima tačno dva koseta: P i $Pb = \{b, ab, \ldots, a^{p-1}b\}$ za bilo koje $b \notin P$ (odakle sledi da je $o(b) = 2$). Zbog normalnosti P važi da je $b^{-1}ab = a^k$ za neko $1 \leq k < p$, pa imamo

$$a = b^{-2}ab^2 = a^{k^2},$$

što znači da $p \mid k^2 - 1 = (k-1)(k+1)$. Slučaj $k = 1$ povlači komutativnost grupe G (i stoga $G \cong \mathbb{Z}_2 \times \mathbb{Z}_p \cong \mathbb{Z}_{2p}$), pa preostaje slučaj $k = p-1$. Tada važi $ab = ba^{p-1}$ ili, ekvivalentno, $ba = a^{-1}b$. Primetimo da informacije koje smo do sada prikupili o grupi G u potpunosti određuju množenje u G: ova grupa je generisana sa a, b i važi $a^p = b^2 = 1$, što uz prethodnu relaciju daje, za sve $0 \leq i, i' < p$, $j, j' \in \{0, 1\}$,

$$(a^i b^j)(a^{i'} b^{j'}) = a^i (b^j a^{i'}) b^{j'} = \begin{cases} a^{i+i'} b^{j'} & j = 0, \\ a^{i-i'} b^{j'+1} & j = 1. \end{cases}$$

Stoga postoji najviše jedna nekomutativna grupa reda $2p$. Međutim, dijedarska grupa D_p jeste jedna takva grupa, pa mora biti $G \cong D_p$. □

Time smo opisali sve grupe reda 6,10,14,22,26,…

10.3 Grupe reda 8

Propozicija 10.5. *Postoji do na izomorfizam ukupno pet grupa reda 8: tri Abelove ($\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$) i dve nekomutativne ($D_4$ i Q_8).* opis grupa reda 8

Dokaz. Prvi deo tvrđenja sledi iz Fundamentalne teoreme o konačnim Abelovim grupama. Zato pretpostavimo da je G nekomutativna grupa reda 8.

Najpre, G nema element reda 8 (jer bi u suprotnom bilo $G \cong \mathbb{Z}_8$). S druge strane, ako bi svi nejedinični elementi bili reda 2, tada bismo za sve $a, b \in$

G imali $ab = (ba)^2ab = ba(ba^2b) = ba \cdot b^2 = ba$, pa bi G ponovo bila komutativna. Prema tome, G ima element a reda 4. Tada zbog $(G : \langle a \rangle) = 2$ imamo $\langle a \rangle \trianglelefteq G$ i $G/\langle a \rangle \cong \mathbb{Z}_2$, pa za proizvoljno $b \notin \langle a \rangle$ imamo $b^2 \in \langle a \rangle$ (pri tome je $G = \langle a, b \rangle = \{1, a, a^2, a^3, b, ab, a^2b, a^3b\}$). Dakle, $b^2 \in \{1, a, a^2, a^3\}$, pri čemu slučajevi $b^2 \in \{a, a^3\}$ otpadaju (jer bi tada bilo $o(b) = 8$). Znači, $b^2 = 1$ ili $b^2 = a^2$.

Sada posmatrajmo element $b^{-1}ab$. Zbog $\langle a \rangle \trianglelefteq G$ imamo da je $b^{-1}ab = a^k$ za neko $k \leq 3$. Pošto je $o(b^{-1}ab) = o(a)$, sledi da je $k \in \{1, 3\}$. Slučaj $k = 1$ implicira komutativnost G, pa mora biti $b^{-1}ab = a^3 = a^{-1}$.

Na kraju primetimo da relacije $a^4 = 1$, $b^{-1}ab = a^{-1}$ (koja je ekvivalentna sa $aba = b$) i bilo koja od dve mogućnosti $b^2 = 1$, $b^2 = a^2$, jedinstveno određuju operaciju grupe G: naime, za $i, i' \in \{0, 1, 2, 3\}$, $j, j' \in \{0, 1\}$ važi

$$(a^i b^j)(a^{i'} b^{j'}) = a^{i-i'}(a^{i'} b^j a^{i'}) b^{j'} = \begin{cases} a^{i+i'} b^{j'} & j = 0, \\ a^{i-i'} b^{j'+1} & j = 1. \end{cases}$$

Zbog toga, postoje najviše dve nekomutativne grupe reda 8. No, mi već znamo za dve takve: to su D_4 i Q_8, pa su to i jedine neabelove grupe reda 8. □

Za radoznalce

grupe reda p^3

Napomenimo da ovo tvrđenje ima svoje "produženje" na grupe reda p^3, gde je p neparan prost broj. Takvih grupa ima takođe pet: tri Abelove ($\mathbb{Z}_{p^3}$, $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$, $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$) i dve nekomutativne. Jedna takva nekomutativna grupa se dobija kao poludirektan proizvod $\mathbb{Z}_p \ltimes_\phi \mathbb{Z}_{p^2}$ definisan homomorfizmom $\phi : \mathbb{Z}_p \to \mathrm{Aut}(\mathbb{Z}_{p^2})$ kojim generator grupe $\mathbb{Z}_p$ deluje na $\mathbb{Z}_{p^2}$ automorfizmom

$$\overline{a} \mapsto \overline{(p+1)a}$$

(ovo je automorfizam od $\mathbb{Z}_{p^2}$ reda p jer je $(p+1, p^2) = 1$ i $(p+1)^p \equiv 1 (\mathrm{mod}\ p^2)$). Druga nekomutativna grupa reda p^3 je $UT(3, p)$, grupa svih gornjih trougaonih matrica formata 3×3 nad p-elementnim poljem sa sva tri dijagonalna elementa jednaka 1. U ovoj grupi su svi nejedinični elementi reda p (dočim prethodni poludirektni proizvod ima elemente reda p^2).

10.4 Grupe reda 12

opis grupa reda 12

Propozicija 10.6. *Postoji do na izomorfizam ukupno pet grupa reda 12: dve Abelove ($\mathbb{Z}_{12} \cong \mathbb{Z}_4 \times \mathbb{Z}_3$ i $\mathbb{Z}_2 \times \mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$) i tri nekomutativne (od kojih su dve dijedarska grupa D_6 i alternativna grupa $\mathbb{A}_4$).*

Dokaz. Primetimo da smo analizu grupa reda 12 već započeli u Propoziciji 8.8: naime, grupa G reda 12 ima 2- i 3-podgrupe Silova, i pri tome nije moguće da je istovremeno $s_2 = 3$ i $s_3 = 4$. S druge strane, $s_2 = s_3 = 1$ daje Abelov slučaj, koji sledi po Fundamentalnoj teoremi. Prema tome, preostaju mogućnosti $s_2 = 1$, $s_3 = 4$, odnosno $s_2 = 3$, $s_3 = 1$. U svakom slučaju, 3-podgrupe Silova od G su ciklične grupe reda 3.

Razmotrimo najpre prvu mogućnost: $s_2 = 1$, $s_3 = 4$. Neka je P jedinstvena (i normalna) 2-podgrupa Silova od G. Pošto je $|P| = 4$, imamo dva podslučaja: $P \cong \mathbb{Z}_4$ i $P \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Ako je $P = \langle a \rangle \cong \mathbb{Z}_4$ i $Q = \langle b \rangle$ jedna 3-podgrupa Silova od G, tada je $b^{-1}ab = a^k$ za neko $k \leq 3$, pa sledi

$$a = b^{-3}ab^3 = a^{k^3},$$

zbog čega $4 \mid k^3 - 1$. Jedina mogućnost je $k = 1$, pa je $ab = ba$, što znači da je grupa G Abelova; no, to je u suprotnosti sa $s_3 = 4$, pa je ovaj slučaj nemoguć.

Drugi podslučaj je $P \cong \mathbb{Z}_2 \times \mathbb{Z}_2$; neka su a, b, c elementi grupe G reda 2. Ako je sada $Q = \langle d \rangle$ jedna od 3-podgrupa Silova, tada konjugacija sa d (zbog $d^{-1}Pd = P$) mora biti automorfizam od P reda 3, pa on ciklično permutuje elemente a, b, c. Bez umanjenja opštosti, neka je $d^{-1}ad = b$, $d^{-1}bd = c$ i $d^{-1}cd = a$. Drugim rečima, važi $da = cd$, $db = ad$ i $dc = bd$. Sada se svaki element grupe G može izraziti u obliku xd^i za $x \in \{1, a, b, c\}$, $i \in \{0, 1, 2\}$, i pri tome je svaki proizvod $(xd^i)(yd^j)$ ($x, y \in \{1, a, b, c\}$, $0 \leq i, j \leq 2$) jedinstveno određen. Zato postoji najviše jedna grupa koja zadovoljava $s_2 = 1$ i $s_3 = 4$. Međutim, lako se neposredno proverava da je alternativna grupa $\mathbb{A}_4$ grupa reda 12 koja ima jedinstvenu 2-podgrupu Silova $\{\mathrm{id}_{\{1,2,3,4\}}, (12)(34), (13)(24), (14)(23)\}$ i četiri 3-podgrupe Silova (generisane 3-ciklusima), pa je u ovom slučaju $G \cong \mathbb{A}_4$.

Preostaje da se razmotri slučaj $s_2 = 3$, $s_3 = 1$. Sada G ima jedinstvenu (i normalnu) 3-podgrupu Silova $Q = \langle a \rangle \cong \mathbb{Z}_3$. Neka je H jedna 2-podgrupa Silova od G. Svaki element od G se može izraziti kao $a^i h$ za neko $0 \leq i \leq 2$ i $h \in H$.

Ako je $H = \langle b \rangle \cong \mathbb{Z}_4$, tada a, b ne mogu da komutiraju (jer je u suprotnom G Abelova), pa mora biti $b^{-1}ab = a^2 = a^{-1}$. Otuda je

$$(a^i b^j)(a^k b^\ell) = a^i (b^j a^k b^{-j}) b^{j+\ell} = \begin{cases} a^{i+k} b^{j+\ell} & j \in \{0, 2\}, \\ a^{i-k} b^{j+\ell} & j \in \{1, 3\}, \end{cases}$$

pa je množenje u grupi G jedinstveno određeno. To pokazuje da postoji najviše jedna grupa reda 12 u kojoj je $s_2 = 3$, $s_3 = 1$ i 2-podgrupe Silova su ciklične.

Međutim, nije teško direktno proveriti da je gornjim pravilom na skupu $\{a^i b^j : 0 \le i \le 2,\ 0 \le j \le 3\}$ zaista definisana grupa: množenje je asocijativno i svaki element ima inverz (naime, $(a^i b^j)^{-1}$ je jednako $a^{3-i}b^{4-j}$ ako je j parno, a $a^i b^{4-j}$ ako je j neparno).

Konačno, pretpostavimo da je $H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Zbog nekomutativnosti G mora postojati $x \in H$ tako da je $x^{-1}ax = a^{-1}$, tj. $axa = x$. Ako su y, z preostala dva elementa H reda 2, tada je $z = xy$, pa $y^{-1}ay = a^{-1}$ implicira $z^{-1}az = a$, dok $y^{-1}ay = a$ povlači $z^{-1}az = a^{-1}$. Prema tome, bez umanjenja opštosti možemo pretpostaviti da važi prvi slučaj, tako da je $aya = y$ i $az = za$. Koristeći ove jednakosti, zaključujemo da je svaki proizvod oblika $(a^i h)(a^j h')$ jednoznačno određen, pa opet zaključujemo da može da postoji najviše jedna grupa sa opisanim svojstvima. Kako dijedarska grupa D_6 ima ova svojstva (jedinsvena 3-podgrupa Silova je generisana rotacijom za $2\pi/3$, a tri 2-podgrupe Silova su generisane parovima osnih simetrija sa ortogonalnim osama), sledi da je $G \cong D_6$. $\square$

Za radoznalce

Nije teško pokazati da je grupa u pretposlednjem slučaju u prethodnom dokazu zapravo poludirektni proizvod cikličnih grupa $\mathbb{Z}_4$ i $\mathbb{Z}_3$. Budući da smo ranije napomenuli da je $\mathrm{Aut}(\mathbb{Z}_3)$ dvoelementna (ciklična) grupa, jedini automorfizmi u $\mathbb{Z}_3$ su identičko preslikavanje i invertovanje (koje permutuje klase ostataka $\overline{1}$ i $\overline{2}$). Sada homomorfizam iz $\mathbb{Z}_4$ koji $\overline{0}$ i $\overline{2}$ šalje u identički automorfizam, a $\overline{1}$ i $\overline{3}$ u invertovanje (što je jedini netrivijalni homomorfizam $\mathbb{Z}_4 \to \mathbb{Z}_2$) definiše posmatrani poludirketni proizvod.

11

Kompozicioni nizovi, teorema Žordan-Heldera

Neka je G proizvoljna grupa. Niz podgrupa od G koji zadovoljava

$$G = H_0 \rhd H_1 \rhd \ldots \rhd H_{n-1} \rhd H_n = E$$

se naziva *normalni niz* grupe G (dužine n). Pri tome, notacija $H_{i+1} \lhd H_i$ označava da je $H_{i+1} \trianglelefteq H_i$ i $H_{i+1} \neq H_i$. Primetimo da se pri tome od podgrupa H_k (osim, naravno, H_1) ne traži da budu normalne u G, već samo u prethodnom članu niza, H_{k-1}. Grupe H_i/H_{i+1}, $0 \leq i \leq n-1$, se nazivaju *faktori* posmatranog normalnog niza.

normalni niz i njegovi faktori

Ako je za sve $0 \leq i \leq n-1$, H_{i+1} maksimalna normalna podgrupa od H_i, drugim rečima, ako su svi faktori proste grupe, tada normalni niz $G = H_0 \rhd H_1 \rhd \ldots \rhd H_{n-1} \rhd H_n = E$ zovemo *kompozicioni niz* grupe G.

kompozicioni niz

Propozicija 11.1. *Svaka konačna grupa G ima kompozicioni niz.*

Dokaz. Tvrđenje neposredno sledi indukcijom po redu grupe G. Ono trivijalno važi ako je $|G| = 1$. U suprotnom, G ima maksimalnu normalnu podgrupu H_1. Kako je $|H_1| < |G|$, po induktivnoj pretpostavci H_1 ima kompozicioni niz. Nadovezivanjem G na taj niz dobijamo kompozicioni niz za G. $\square$

Primer 11.2. Niz

$$\mathbb{A}_4 \rhd \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\} \rhd \{\mathrm{id}, (12)(34)\} \rhd \{\mathrm{id}\}$$

je kompozicioni niz alternativne grupe $\mathbb{A}_4$, pošto su njegovi faktori redom izomorfni sa $\mathbb{Z}_3$, $\mathbb{Z}_2$, i ponovo $\mathbb{Z}_2$ (što su sve očito proste grupe).

Primer 11.3. Grupa celih brojeva $\mathbb{Z}$ nema kompozicioni niz, jer su svi lanci njenih podgrupa u kojem je svaka podgrupa maksimalna u prethodnoj oblika

$$\mathbb{Z} \rhd p_1\mathbb{Z} \rhd p_1p_2\mathbb{Z} \rhd p_1p_2p_3\mathbb{Z} \rhd \dots,$$

gde je $p_1, p_2, p_3, \dots$ proizvoljan beskonačan niz (ne nužno različitih) prostih brojeva.

Za normalne nizove

$$G = H_0 \rhd H_1 \rhd \dots \rhd H_{n-1} \rhd H_n = E$$

i

$$G = K_0 \rhd K_1 \rhd \dots \rhd K_{m-1} \rhd K_m = E$$

ekvivalencija normalnih nizova

kažemo da su *ekvivalentni* ako je $n = m$ i pri tome postoji permutacija π skupa $\{0, 1, \dots, n-1\}$ tako da je $H_i/H_{i+1} \cong K_{\pi(i)}/K_{\pi(i)+1}$ za sve $0 \le i \le n-1$. Drugim rečima, multiskupovi faktora posmatranih normalnih nizova se poklapaju, do na izomorfizam grupa.

Glavni rezultat u vezi sa kompozicionim nizovima grupa (u slučaju kada oni uopšte postoje) je čuvena *teorema Žordan-Heldera*[8].

teorema Žordan-Heldera

Teorema 11.4 (Teorema Žordan-Heldera)**.** *Svaka dva kompoziciona niza grupe G su ekvivalentna.*

Za dokaz ove teoreme nam je potrebno sledeće pomoćno tvrđenje koje uspostavlja vezu između kompozicionih nizova grupe i njenih normalnih podgrupa.

lema o kompozicionim nizovima podgrupa

Lema 11.5. *Neka je $H \trianglelefteq G$, gde je G grupa koja ima kompozicioni niz. Tada i H ima kompozicioni niz, i njegovi faktori su (kao multiskup) sadržani među faktorima nekog kompozicionog niza grupe G.*

Dokaz. Fiksirajmo jedan kompozicioni niz grupe G:

$$G = K_0 \rhd K_1 \rhd \dots \rhd K_{n-1} \rhd K_n = E.$$

Uočimo tada sledeći lanac podgrupa od H:

$$H = H \cap K_0 \rhd H \cap K_1 \rhd \dots \rhd H \cap K_{n-1} \rhd H \cap K_n = E.$$

[8] Oto Helder (Otto Ludwig Hölder, 1859–1937), nemački matematičar

Ovo je u suštini normalni niz grupe H, s tim da su u gornjem lancu moguća neka ponavljanja uzastopnih podgrupa, tako da njihovom eleminacijom dobijamo normalni niz za H. Dokazaćemo da je tako dobijen normalni niz zapravo kompozicioni niz grupe H.

Za neko fiksirano i, označimo kraće $L = H \cap K_i$. Kako je $L \trianglelefteq K_i$ (a takođe i $K_{i+1} \trianglelefteq K_i$) sledi da je $LK_{i+1} \trianglelefteq K_i$; s druge strane, K_{i+1} je normalna u svakoj podgrupi od K_i koja je sadrži, pa je zato $K_{i+1} \trianglelefteq LK_{i+1}$. Po Prvoj teoremi o izomorfizmu je

$$LK_{i+1}/K_{i+1} \cong L/L \cap K_{i+1}.$$

No, sada je $L \cap K_{i+1} = H \cap K_i \cap K_{i+1} = H \cap K_{i+1}$, pa je

$$L/L \cap K_{i+1} = (H \cap K_i)/(H \cap K_{i+1}).$$

S druge strane, po Drugoj teoremi o izomorfizmu je $LK_{i+1}/K_{i+1} \trianglelefteq K_i/K_{i+1}$. Međutim, ovaj poslednji faktor je prosta grupa, pa zato gornji izomorfizam pruža dve mogućnosti: ili je $(H \cap K_i)/(H \cap K_{i+1})$ trivijalna grupa (tj. $H \cap K_i = H \cap K_{i+1}$), ili je pak

$$(H \cap K_i)/(H \cap K_{i+1}) \cong K_i/K_{i+1}.$$

Prema tome, uklanjanjem ponavljanja iz ranije uočenog lanca podgrupa od H dobija se normalni niz te grupe u kojem je svaki faktor prost; dakle, radi se o kompozicionom nizu. Takođe, odmah sledi da su svi faktori tog kompozicionog niza sadržani (do na izmomorfizam) u multiskupu kompozicionih faktora polazne grupe G. □

Dokaz Teoreme 11.4. Dokaz izvodimo indukcijom po dužini najkraćeg kompozicionog niza grupe G. Ako G ima kompozicioni niz dužine 1, tada je G prosta i $G \triangleright E$ je jedini kompozicioni niz. Pretpostavimo da je tvrđenje tačno za sve grupe koje imaju kompozicioni niz dužine ne veće od $n-1$ (pri čemu su tada svi kompozicioni nizovi takve grupe iste dužine). Dokaz teoreme Žordan-Heldera

Neka su sada

$$G = H_0 \triangleright H_1 \triangleright \ldots \triangleright H_{n-1} \triangleright H_n = E$$

i

$$G = K_0 \triangleright K_1 \triangleright \ldots \triangleright K_{m-1} \triangleright K_m = E.$$

dva kompoziciona niza neke grupe G. Pokazaćemo da su oni ekvivalentni.

Razmatramo dva slučaja. Prvi nastupa kada je $H_1 = K_1$, kada se indukitvni dokaz okončava gotovo neposredno. Naime, možemo primeniti induktivnu pretpostavku na grupu H_1 koja ima kompozicione nizove

$$H_1 \rhd \ldots \rhd H_{n-1} \rhd H_n = E$$

i

$$H_1 = K_1 \rhd \ldots \rhd K_{m-1} \rhd K_m = E$$

dužina $n-1$ i $m-1$, respektivno. Induktivna pretpostavka implicira da je $n-1 = m-1$ (zbog čega je $n = m$), te da su gornja dva niza ekvivalentna. No, tada su i početna dva kompoziciona niza grupe G ekvivalentna: multiskupovi njihovih kompozicionih faktora se dobijaju dodavanjem faktora $G/H_1 = G/K_1$.

Zato pretpostavimo da je $H_1 \neq K_1$. Budući da je G/H_1 prosta grupa, jedine normalne podgrupe od G koje sadrže H_1 su H_1 i samo G; isto važi i za K_1. Međutim, $H_1K_1 \trianglelefteq G$ i pri tome $H_1 \leq H_1K_1$ i $K_1 \leq H_1K_1$, pa bi $H_1K_1 \neq G$ impliciralo da je $H_1 = H_1K_1 = K_1$; zato mora biti $H_1K_1 = G$. Po Prvoj teoremi o izomorfizmu je

$$G/H_1 = H_1K_1/H_1 \cong K_1/H_1 \cap K_1,$$

a takođe i

$$G/K_1 = H_1K_1/K_1 \cong H_1/H_1 \cap K_1.$$

Označimo $L = H_1 \cap K_1$. Kako je $L \trianglelefteq G$, po prethodnoj lemi L ima kompozicioni niz:

$$L = L_0 \rhd L_1 \rhd \ldots \rhd L_{k-1} \rhd L_k = E.$$

Dodajmo ovom nizu H_1 sleva; time dobijamo jedan kompozicioni niz za H_1 budući da smo upravo ustanovili da je $H_1/L \cong G/K_1$, što je prosta grupa. Kako H_1 već ima kompozicioni niz dužine $n-1$ (dakle, kraći od n), mora biti $k+1 = n-1$, tj. $k = n-2$, a nizovi $H_1 \rhd L \rhd L_1 \rhd \ldots \rhd L_k = E$ i $H_1 \rhd H_2 \rhd \ldots \rhd H_n = E$ su ekvivalentni. Kako je $K_1/L \cong G/H_1$ takođe prosta grupa, isti ovaj postupak možemo ponoviti i sa dodavanjem K_1 sleva na gornji kompozicioni niz – time se dobija da je $k = m-2$, odakle sledi da je $m = n$. Dakle, i K_1 ima kompozicioni niz dužine manje od n (naime, $K_1 \rhd K_2 \rhd \ldots \rhd K_n = E$), pa na osnovu induktivne pretpostavke zaključujemo da su i nizovi $K_1 \rhd L \rhd L_1 \rhd \ldots \rhd L_k = E$ i $K_1 \rhd K_2 \rhd \ldots \rhd K_n = E$ ekvivalentni. Dakle, kompozicione faktore niza $G = H_0 \rhd H_1 \rhd \ldots \rhd H_{n-1} \rhd H_n = E$ dobijamo tako što faktorima niza $H_1 \rhd L \rhd L_1 \rhd \ldots \rhd$

$L_k = E$ dodamo faktor $G/H_1 \cong K_1/L$, a faktore niza $G = K_0 \rhd K_1 \rhd \ldots \rhd K_{m-1} \rhd K_m = E$ tako što faktorima niza $K_1 \rhd L \rhd L_1 \rhd \ldots \rhd L_k = E$ dodamo faktor $G/K_1 \cong H_1/L$. Sledi da su posmatrana dva kompoziciona niza grupe G ekvivalentna. $\square$

Primer 11.6. Pomalo "lakonski", Teorema Žordan-Heldera bi se mogla formulisati ovako: svaka grupa koja ima bar jedan kompozicioni niz jednoznačno određuje svoje kompozicione faktore. Obratno, međutim, ne važi. Na primer,

$$\mathbb{S}_3 \rhd \{\mathrm{id}, (123), (132)\} (= \mathbb{A}_3) \rhd \{\mathrm{id}\}$$

je kompozicioni niz (neabelove) grupe $\mathbb{S}_3$ i njeni kompozicioni faktori su izomorfni sa $\mathbb{Z}_2$ i $\mathbb{Z}_3$. Međutim, iste grupe su kompozicioni faktori i ciklične (dakle, Abelove) grupe $\mathbb{Z}_6$. Prema tome, na osnovu kompozicionih faktora se čak ne može ni reći da li je posmatrana grupa Abelova ili ne.

Za radoznalce

Ovde prikazujemo alternativni dokaz Teoreme Žordan-Heldera koji koristi Šrajerovu[9] teoremu o profinjenju, a koja se pak oslanja na Lemu Casenhausa. Ovaj dokaz jeste koncizniji, ali istovremeno i tehnički složeniji.

Šrajerov dokaz teoreme Žordan-Heldera

Za normalni niz

$$G = K_0 \rhd K_1 \rhd \ldots \rhd K_{m-1} \rhd K_m = E$$

kažemo da je *profinjenje* niza

$$G = H_0 \rhd H_1 \rhd \ldots \rhd H_{n-1} \rhd H_n = E$$

ako za sve $1 \le i < n$ postoji $1 \le j < m$ tako da je $H_i = K_j$; drugim rečima, prvi niz se dobija od drugog umetanjem dodatnih podgrupa. *Šrajerova teorema o profinjenju* tvrdi da svaka dva normalna niza proizvoljne grupe G imaju ekvivalentna profinjenja.

Dakle, neka su

$$G = M_0 \rhd M_1 \rhd \ldots \rhd M_{k-1} \rhd M_k = E$$

i

$$G = N_0 \rhd N_1 \rhd \ldots \rhd N_{l-1} \rhd N_l = E$$

dva normalna niza grupe G. Za $1 \le i \le k$ i $0 \le j \le l$ definišimo

$$M_{ij} = M_i(M_{i-1} \cap N_j),$$

[9]Oto Šrajer (Otto Schreier, 1901–1929), austrijski matematičar, jedan od osnivača kombinatorne teorije grupa (uz fon Dika i Nilsena)

dok za $0 \leq i \leq k$ i $1 \leq j \leq l$ definišemo

$$N_{ij} = N_j(N_{j-1} \cap M_i).$$

Pri tome je $M_{i0} = M_i(M_{i-1} \cap G) = M_i M_{i-1} = M_{i-1}$ i $M_{il} = M_i(M_{i-1} \cap E) = M_i$, dok je očito $M_{ij} \geq M_{i,j+1}$ za sve $0 \leq j < l$. Dakle, umetanjem podgrupa M_{ij} između M_{i-1} i M_i u prvi niz (za sve $1 \leq i \leq k$) dobijamo nerastući niz podgrupa od G dužine kl. Dualno, umetanjem podgrupa N_{ij} između N_{j-1} i N_j u drugi niz (za sve $1 \leq j \leq l$) takođe dobijamo nerastući niz podgrupa od G dužine kl.

Želimo da pokažemo da su ovako dobijeni nizovi normalni – sa eventualnim ponavljanjima – kao i da su oni ekvivalentni. Lema Cahenhausa (Posledica 5.4) povlači da je

$$M_{ij} = M_i(M_{i-1} \cap N_j) \trianglelefteq M_i(M_{i-1} \cap N_{j-1}) = M_{i,j-1}$$

i

$$N_{ij} = N_j(N_{j-1} \cap M_i) \trianglelefteq N_j(N_{j-1} \cap M_{i-1}) = N_{i-1,j};$$

pored toga, važi i

$$M_{i,j-1}/M_{ij} = M_i(M_{i-1} \cap N_{j-1})/M_i(M_{i-1} \cap N_j) \cong$$

$$\cong N_j(N_{j-1} \cap M_{i-1})/N_j(N_{j-1} \cap M_i) = N_{i-1,j}/N_{ij}.$$

Prema tome, $M_{i,j-1} = M_{ij}$ ako i samo ako je $N_{i-1,j} = N_{ij}$. To znači da kada u dva posmatrana niza podgrupa od G dužine kl obrišemo sva ponavljanja podgrupa dobijamo dva niza iste dužine koji su pri tome još i ekvivalentna. Time je Šrajerova teorema dokazana.

Budući da su normalni nizovi koji nemaju profinjenja tačno kompozicioni nizovi, svako profinjenje kompozicionog niza neke grupe je jednako početnom nizu. Šrajerova teorema tvrdi da svaka dva normalna niza grupe imaju ekvivalentna profinjenja, pa odmah sledi da svaka dva kompoziciona niza moraju biti međusobno ekvivalentna.

12

Rešive grupe

Za grupu G kažemo da je *rešiva* ako ima normalni niz čiji su svi faktori Abelove grupe. rešive grupe

Primer 12.1. Očito, sve Abelove grupe A su rešive ($A \rhd E$ je trivijalan normalni niz sa Abelovim faktorom). S druge strane, postoje i neabelove rešive grupe: u prethodnom primeru smo videli da $\mathbb{S}_3(\cong D_3)$ ima kompozicioni niz sa faktorima $\mathbb{Z}_2$ i $\mathbb{Z}_3$. (Zapravo, rešiva je svaka dijedarska grupa D_n jer rotacije čine normalnu podgrupu indeksa 2 – kojoj odgovara faktor $\mathbb{Z}_2$ – a koja je pri tome izomorfna sa $\mathbb{Z}_n$.) Takođe, ako se na kompozicioni niz grupe $\mathbb{A}_4$ (iz Primera 11.2) doda $\mathbb{S}_4$, dobija se normalni (zapravo, kompozicioni) niz grupe $\mathbb{S}_4$ sa svim Abelovim faktorima, pa su zato i grupe $\mathbb{S}_4$ i $\mathbb{A}_4$ rešive. S druge strane, za $n \geq 5$, $\mathbb{A}_n$ je neabelova prosta grupa, pa zato nije rešiva (jer je $\mathbb{A}_n \rhd E$ jedini njen normalni niz).

Zapravo, poslednja primedba iz prethodnog primera se može uopštiti i na simetrične grupe.

Propozicija 12.2. *Grupa $\mathbb{S}_n$ nije rešiva za sve $n \geq 5$.* $\mathbb{S}_n$ nije rešiva za sve $n \geq 5$

Dokaz. Kako je $n \geq 5$, niz $\mathbb{S}_n \rhd \mathbb{A}_n \rhd E$ je kompozicioni za $\mathbb{S}_n$ jer su mu faktori proste grupe $\mathbb{Z}_2$ i $\mathbb{A}_n$. Otuda $\mathbb{S}_n$ nije rešiva jer ima neabelov kompozicioni faktor. $\square$

Za radoznalce

Može se pokazati da je kompozicioni niz iz prethodne propozicije zapravo jedinstven kompozicioni niz grupe $\mathbb{S}_n$. Zaista, svaki drugi kompozicioni niz bi morao biti oblika $\mathbb{S}_n \rhd H \rhd E$ gde je ili $(\mathbb{S}_n : H) = 2$, ili je pak H normalna ciklična podgrupa reda 2. Prva mogućnost otpada, jer bi tada bilo $\mathbb{S}_n = \mathbb{A}_n H$ i $\mathbb{Z}_2 \cong \mathbb{A}_n H/H \cong \mathbb{A}_n/\mathbb{A}_n \cap H$, pa bi $\mathbb{A}_n \cap H$ bila podgrupa indeksa 2 (i stoga normalna) u $\mathbb{A}_n$, a što je nemoguće jer jer $\mathbb{A}_n$ prosta. S druge strane, ako bi bilo $H = \{\mathrm{id}, \sigma\}$, tada bi normalnost H povlačila $\pi^{-1}\sigma\pi = \sigma$ za sve $\pi \in \mathbb{S}_n$ i stoga $\sigma \in Z(\mathbb{S}_n)$. Međutim, lako se pokazuje da je grupa $\mathbb{S}_n$ bez centra, pa ni ovaj drugi slučaj nije moguć.

n-ta izvodna podgrupa

Za $n \geq 0$ definišemo n-tu *izvodnu podgrupu* grupe G tako što je $G^{(0)} = G$ i

$$G^{(n+1)} = (G^{(n)})'$$

za sve $n \geq 0$. Kako je $H' \trianglelefteq H$ i H/H' Abelova grupa za svaku grupu H (štaviše, znamo da je u pitanju maksimalni Abelov faktor od H), u lancu podgrupa

$$G \rhd G' \rhd G'' \rhd \ldots \rhd G^{(n)}$$

su svi faktori Abelovi. Uslov da se taj lanac "spušta" do trivijalne podgrupe u konačno mnogo koraka jeste možda najpoznatiji kriterijum rešivosti.

kriterijum rešivosti preko izvodnih podgrupa

Propozicija 12.3. *Grupa G je rešiva ako i samo ako postoji $n \geq 0$ tako da je $G^{(n)} = E$.*

Dokaz. ($\Rightarrow$) Neka je G rešiva grupa i neka je

$$G = H_0 \rhd H_1 \rhd \ldots \rhd H_n = E$$

jedan njen normalni niz sa Abelovim faktorima. Po Lemi 5.6 važi da je $H_i' \leq H_{i+1}$ za sve $0 \leq i < n$, pa induktivno dobijamo da $G^{(i)} \leq H_i$. Specijalno, $G^{(n)} \leq H_n = E$, pa je $G^{(n)} = E$.

($\Leftarrow$) Uočimo najmanji prirodan broj n za koji je $G^{(n)} = E$. Tada imamo normalni niz

$$G = G^{(0)} \rhd G^{(1)} \rhd \ldots \rhd G^{(n)} = E,$$

jer bi $G^{(k)} = G^{(k+1)}$ impliciralo $G^{(m)} = G^{(k)}$ za sve $m \geq k$, pa ne bi moglo biti $G^{(n)} = E$. Faktori ovog niza $G^{(k)}/G^{(k+1)} = G^{(k)}/(G^{(k)})'$ su Abelove grupe, pa je G rešiva grupa. □

Ako je G rešiva grupa, najmanje n za koje važi $G^{(n)} = E$ zovemo *dužina rešivosti* grupe G. Iz prethodnog dokaza sledi da je posredi dužina najkraćeg normalnog niza za G sa Abelovim faktorima – jedan takav niz je baš niz izvodnih podgrupa.

Propozicija 12.4. *Neka je G rešiva grupa.*

podgrupe i faktori rešivih grupa

(i) Ako je $H \leq G$ tada je H rešiva grupa.

(ii) Ako je $H \trianglelefteq G$ tada je G/H rešiva grupa.

Dokaz. Pretpostavimo da je n dužina rešivosti grupe G; dakle, $G^{(n)} = E$.

(i) Iz pretpostavke sledi da je $H' \leq G'$, zatim $H'' \leq G''$ i, induktivno, $H^{(k)} \leq G^{(k)}$ za svako k. Prema tome, $H^{(n)} = E$, tj. H je rešiva grupa i pri tome dužina rešivosti H nije veća od n.

(ii) Kako za bilo koji homomorfizam ϕ definisan na grupi G važi $\phi([g,h]) = [\phi(g), \phi(h)]$, sledi da je $(\phi(G))' = \phi(G')$. Specijalno, $(G/H)'$ se sastoji od koseta Hg takvih da je $g \in G'$. Induktivno, otuda sledi da je $(G/H)^{(k)} = \{Hg : g \in G^{(k)}\}$, pa je $(G/H)^{(n)}$ trivijalna grupa $\{H\}$. Dakle, G/H je rešiva grupa i ponovo njena dužina rešivosti nije veća od n. □

Važi i tvrđenje (u izvesnom smislu) obratno prethodnom.

Propozicija 12.5. *Neka je G grupa i $H \trianglelefteq G$. Ako su H i G/H rešive grupe, onda je to i G.*

Dokaz. Neka je s dužina rešivosti grupe G/H, a t dužina rešivosti za H. Tada je $(G/H)^{(s)} = \{H\}$, što znači da je $G^{(s)} \leq H$. No tada je $G^{(s+t)} \leq H^{(t)} = E$, pa je G rešiva grupa (čija dužina rešivosti nije veća od $s+t$). □

Ako se sada usresredimo na konačne grupe, tada osobina rešivosti ima sledeći elegantan opis.

Propozicija 12.6. *Netrivijalna konačna grupa je rešiva ako i samo ako su joj svi kompozicioni faktori ciklične grupe prostog reda.*

kompozicioni faktori rešivih grupa

Dokaz. ($\Leftarrow$) Trivijalno, jer su sve ciklične grupe Abelove, pa posmatrani kompozicioni niz predstavlja normalni niz koji obezbeđuje rešivost.

($\Rightarrow$) Neka je G netrivijalna konačna rešiva grupa: pretpostavimo da je $G \rhd H_1 \rhd H_2 \rhd \dots \rhd H_n = E$ njen normalni niz u kome su svi faktori Abelovi. Po Šrajerovoj teoremi o profinjenju, ovaj niz se može profiniti do kompozicionog:

$$G \rhd K_{1,1} \rhd K_{1,2} \rhd \dots K_{1,m_1} = H_1 \rhd K_{2,1} \rhd \dots \rhd K_{2,m_2} = H_2 \rhd \dots$$

$$\dots \rhd K_{n,m_n} = H_n = E.$$

Pri tome je podgrupa H_i normalna u svim podgrupama $K_{i,1}, \dots, K_{i,m_i}$ za sve $1 \leq i \leq n$. Po Drugoj teoremi o izomorfizmu je

$$K_{i,j}/K_{i,j+1} \cong (K_{i,j}/H_i)/(K_{i,j+1}/H_i),$$

pa je prosta grupa $K_{i,j}/K_{i,j+1}$ homomorfna slika Abelove grupe $K_{i,j}/H_i \leq H_{i-1}/H_i$ i stoga je i sama Abelova. Sledi da je $K_{i,j}/K_{i,j+1}$ ciklična grupa prostog reda, a analogan zaključak sledi i za $G/K_{1,1}$, kao i $H_i/K_{i+1,1}$. Prema tome, svi kompozicioni faktori od G su zaista ciklične grupe prostog reda. $\square$

Naš naredni cilj je da pokažemo da je svaka konačna p-grupa rešiva.

Lema 12.7. *Svaka grupa reda p^n ($n \geq 1$) ima normalnu podgrupu reda p^{n-1}.*

Dokaz. Dokaz leme izvodimo indukcijom po n. Ako je $n = 1$, tvrđenje je trivijalno; zato pretpostavimo da je $n \geq 2$ i da tvrđenje leme važi za sve p-grupe reda $\leq p^{n-1}$. Prema Posledici 3.4, red $|Z(G)|$ centra posmatrane grupe G deljiv je sa p. Po Košijevoj lemi, postoji $z \in Z(G)$ tako da je $o(z) = p$. Tada je $H = \langle z \rangle \leq Z(G)$, pa mora biti $H \trianglelefteq G$. Sada je $|G/H| = p^{n-1}$, pa po induktivnoj pretpostavci G/H ima normalnu podgrupu kardinalnosti p^{n-2}. Po Teoremi o korespondenciji, ta normalna podgrupa je oblika K/H, gde je K neka normalna podgrupa od G koja sadrži H. Sada je $|K| = p^{n-2}|H| = p^{n-1}$, pa je induktivni dokaz okončan. $\square$

rešivost konačnih p-grupa

Propozicija 12.8. *Svaka konačna p-grupa je rešiva.*

Dokaz. Neka je G konačna p-grupa, $|G| = p^n$. Dokaz sledi indukcijom po n. Za $n = 1$ imamo da je $G \cong \mathbb{Z}_p$, što je evidentno rešiva grupa. Ako je $n \geq 2$, po prethodnoj lemi G ima normalnu podgrupu H reda p^{n-1}. Po indukitvnoj pretpostavci, H je rešiva grupa, pa ima normalni niz sa Abelovim faktorima. Kako je $G/H \cong \mathbb{Z}_p$, nadovezivanjem G na početak tog niza dobijamo normalni niz za G u kome su svi faktori Abelovi, pa sledi da je G takođe rešiva. $\square$

Za radoznalce

Danas je poznat čitav niz dovoljnih uslova za rešivost konačne grupe. Jedan od klasičnih rezultata u tome smislu je *Bernsajdova pq-teorema* [Bu04].

rešivost grupa reda $p^n q^m$

Teorema 12.9 (Bernsajd, 1904)**.** *Svaka konačna grupa reda $p^n q^m$, gde su $p \neq q$ prosti brojevi i $n, m \geq 0$, je rešiva.*

Zbog toga, red svake neabelove konačne proste grupe mora biti deljiv sa bar tri različita prosta faktora. Minimalan primer je $\mathbb{A}_5$ reda $60 = 2^2 \cdot 3 \cdot 5$ (i to je jedina prosta grupa reda 60). Znatno kasnije, dokazano je da jedan od tih prostih faktora mora biti 2.

Teorema 12.10 (Fajt[10], Tompson[11], 1962/63)**.** *Svaka neabelova konačna prosta grupa je parnog reda. Posledično, svaka grupa neparnog reda je rešiva.* teorema Fajt-Tompsona

U vreme kada je ovaj rezultat publikovan, njegov dokaz (koji zauzima 255 strana čitavog jednog broja časopisa *Pacific Journal of Mathematics* [FT63]) bio je možda i najsloženiji dokaz jedne teoreme u matematici uopšte.

[10] Valter Fajt (Walter Feit, 1930–2004), američki matematičar austrijskog porekla

[11] Džon Tompson (John Griggs Thompson, 1932–), američki matematičar, dobitnik Fildsove medalje 1970. i Abelove nagrade 2008. godine

Literatura

[BM90] Nataša Božović, Žarko Mijajlović: *Uvod u teoriju grupa*, Naučna knjiga, Beograd, 1990.

[Bu04] W. Burnside: On groups of order $p^\alpha q^\beta$, *Proc. London Math. Soc. (2)* **1** (1904), 388–392.

[Cam05] Peter J. Cameron: *Permutation Groups*, Cambridge University Press, 2005.

[CDM98] Siniša Crvenković, Igor Dolinka, Rozália Sz. Madarász: *Odabrane teme opšte algebre – grupe, prsteni, polja, mreže*, Edicija "Univerzitetski udžbenik", Vol. 47, Prirodno-matematički fakultet, Univerzitet u Novom Sadu, 1998.

[DF99] David S. Dummit, Richard M. Foote: *Algebra*, John Wiley & Sons, New York, 1999.

[FT63] Walter Feit, John G. Thompson: Solvability of groups of odd order, *Pacific J. Math.* **13** (1963), 775–1029.

[Gr97] Milan Z. Grulović: *Osnovi teorije grupa*, Institut za matematiku, Univerzitet u Novom Sadu, 1997.

[Hall28] P. Hall: A note on soluble groups, *J. London Math. Soc. (1)* **3** (1928), 98–105.

[Hu73] Thomas W. Hungerford: *Algebra*, Holt, Rinehard & Winston, New York , 1973.

[KM77] M. I. Kargapolov, Ju. I. Merzljakov: *Osnovi teorije grupa* [na ruskom], Nauka, Moskva, 1977.

[Kiss07] Kiss Emil: *Bevezetés az algebrába*, Typotex, Budapest, 2007.

[Ku67] A. G. Kuroš: *Teorija grupa* [na ruskom], Nauka, Moskva, 1967.

[LSch77] Roger C. Lyndon, Paul E. Schupp: *Combinatorial Group Theory*, Springer-Verlag, Berlin, Heidelberg, New York, 1977.

[MKS66] W. Magnus, A. Karrass, D. Solitar: *Combinatorial Group Theory*, Wiley, New York, 1966.

[Per80] Veselin Perić: *Algebra I-II*, Svjetlost, Sarajevo, 1980.

[Rob82] Derek J. S. Robinson: *A Course in the Theory of Groups*, Springer-Verlag, New York, 1982.

[Ros94] John S. Rose: *A Course on Group Theory*, Dover Publications, New York, 1994.

[Rot94] Joseph J. Rotman: *An Introduction to the Theory of Groups*, Springer-Verlag, New York, 1994.

[Sc87] W. R. Scott: *Group Theory*, Dover Publications, New York, 1987.

[SP98] Zoran Stojaković, Đura Paunić: *Zadaci iz algebre – grupe, prsteni, polja*, Edicija "Univerzitetski udžbenik", Vol. 60, Prirodno-matematički fakultet, Univerzitet u Novom Sadu, 1998.