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

Igor Dolinka

PREDAVANJA IZ TEORIJE GRUPA

NOVI SAD, 2018.

Sadržaj

1

Definicija i 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. Između ostalog, ovakav zapis 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 $n > 0$,

stepen elementa

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

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 elementa

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 linearne algebre, ali i šire, u teoriji modula i prstena) ponekad se za Abelove

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

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 $na = 0$.

Ovo uvodno poglavlje okončavamo sa tri elementarna, ali značajna svojstva grupa.

Lema 1.1. *U svakoj grupi G važe zakoni kancelacije (skraćivanja), tj. za sve $a, x, y \in G$ imamo:* kancelacija u grupi

$$ax = ay \Rightarrow x = y,$$
$$xa = ya \Rightarrow x = y.$$

Dokaz. Pretpostavimo da je $ax = ay$. Tada je

$$x = a^{-1}(ax) = a^{-1}(ay) = y.$$

Analogno se dokazuje i desno skraćivanje. □

Lema 1.2. *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

Dokaz. Pretpostavimo najpre da $a, b \in M^\times$. Tada je i element $ab \in M$ invertibilan, budući da je $(b^{-1}a^{-1})ab = 1$ i $ab(b^{-1}a^{-1}) = 1$. Sada sledi da je $M^\times$ podmonoid od M u kojem je svaki element invertibilan; dakle, $M^\times$ je grupa. □

Posledica 1.3. *U svakoj grupi G važi $(ab)^{-1} = b^{-1}a^{-1}$ za sve $a, b \in G$.*

Lema 1.4. *Neka je a element konačnog reda grupe G, $o(a) = n$. Tada važi $a^m = 1$ ako i samo ako $n \mid m$.*

Dokaz. Ako $n \mid m$ tada je $m = nk$ za neko $k \in \mathbb{N}$, pa je $a^m = (a^n)^k = 1$. Obratno, pretpostavimo da n ne deli m. Tada je $m = qn + r$ za neko $q \in \mathbb{Z}$ i $0 < r < n$. Sledi da je

$$a^m = (a^n)^q a^r = a^r.$$

Međutim, $r \neq 0$ i $r < n$, pa po definiciji reda elementa (n je najmanji pozitivan ceo broj takav da je $a^n = 1$) zaključujemo da $a^m = a^r \neq 1$. □

Posledica 1.5. *Ako u grupi G za $a \in G$ važi $o(a) = n$, tada za sve $k \in \mathbb{Z}$ važi $o(a^k) = \frac{n}{(n,k)}$.*

Dokaz. Po prethodnoj lemi, važi $1 = (a^k)^m = a^{km}$ ako i samo ako $n \mid km$, Ako označimo $n' = n/(n,k)$ i $k' = k/(n,k)$, tada važi $n \mid km$ ako i samo ako $n' \mid k'm$. Međutim, budući da je $(n', k') = 1$, poslednje tvrđenje je ekvivalentno sa $n' \mid m$, odakle sledi da je red elementa a^k jednak $\frac{n}{(n,k)}$. $\square$

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. S druge strane, u elementarnoj teoriji brojeva radimo sa konačnim prstenima

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

$n \geq 2$, čiji su elementi $0, 1, \dots, n-1$ i gde su operacije $+_n$ i $\cdot_n$ redom sabiranje i množenje *po modulu* n. Naime, važi $a +_n b = c$ ako i samo ako je c (jedinstveno) rešenje kongruencije $c \equiv a + b \pmod{n}$ u skupu $\{0, 1, \dots, n-1\}$; slično, $a \cdot_n b = d$ ako i samo ako d pripada ovom skupu i zadovoljava $d \equiv ab \pmod{n}$. Sada je aditivna grupa $(\mathbb{Z}_n, +_n)$ prstena ostataka po modulu n primer konačne Abelove grupe. Ove grupe, zajedno sa $(\mathbb{Z}, +)$, zovemo *ciklične grupe*. ciklične grupe

Neka je sada R prsten sa jedinicom. Tada je, naravno, njegova multiplikativna struktura $(R, \cdot)$ monoid, pa znamo iz Leme 1.2 da skup $R^\times$ invertibilnih elemenata prstena R čini grupu u odnosu na množenje prstena. Tako je, na primer, $\mathbb{Z}^\times = \{1, -1\}$; 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. Što se tiče prstena ostataka po modulu $n \geq 2$, invertibilnost elementa $a \in \{1, \dots, n-1\}$ ekvivalentna je tvrđenju da linearna kongruencijska jednačina

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

ima rešenja. Kao što je dobro poznato iz teorije brojeva, postojanje rešenja ove jednačine je ekvivalentno sa $(a, n) = 1$, tako da 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.

Razmotrimo još dva primera konačnih grupa sa kojima se često srećemo u teoriji grupa.

Primer 1.6. Nad četvoroelementnim skupom $\{1, a, b, c\}$ definišimo grupu na sledeći način: neka je 1 jedinica, dok za preostala tri elementa važi

Klajnova grupa V_4

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

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.

Primer 1.7. 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 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):

grupa kvaterniona Q_8

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

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

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

Sada se *telo* (nekomutativan 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.

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

1.3 Grupe permutacija i simetrija

Neka je X proizvoljan neprazan skup. Označimo sa $\mathcal{T}_X$ skup svih funkcija $X \to X$, tj. svih *transformacija* skupa X. Kompozicija funkcija je naravno asocijativna operacija, pa $\mathcal{T}_X$ zapravo čini monoid u odnosu na kompoziciju sa jedinicom id_X, *pun monoid transformacija na* X. Vrlo je dobro poznato (i lako se pokazuje) da je 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

notacija za funkcije i njihovu kompoziciju

Napomena. Tokom ovog kursa, u kompoziciji funkcija $f \circ g$ *prvo* primenjujemo funkciju f, a zatim g. Zbog toga je zgodno da se (bar u većini slučajeva) funkcije pišu sa *desne strane* svog argumenta, dakle kao xf umesto $f(x)$, budući da tada imamo $x(f \circ g) = (xf)g$, što je mnemotehnički mnogo pogodnije. Ovo će se odnositi na transformacije skupa X, pa tako i njegove permutacije u grupi $\mathbb{S}_X$.

Izuzetak od ovog pravila će biti *linearne transformacije* vektorskog prostora V (nad poljem F). Naime, ako je V konačne dimenzije i α jedna takva linearna transformacija, tada se – kao što ćemo videti u narednom odeljku – po fiksiranju baze prostora V, α može izraziti kao $\alpha(x) = Ax$ za neku matricu A nad F. Kako bismo množenje matrica sačuvali u uobičajenom obliku sa leva na desno, tako da je $(AB)x = A(Bx)$, pogodno je da se linearne transformacije izuzetno pišu levo od svojih argumenata.

U svakom slučaju, i ovde će važiti konvencija o ispuštanju simbola kompozicije funkcija, tako da ćemo često umesto $f \circ g$ pisati samo fg.

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 1.8. 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

$$d(xf, yf) = d(x, y).$$

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 označavamo sa $E(n)$; ovo je tzv. n-dimenzionalna *Euklidova grupa*.

Primer 1.9. 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 $\Phi f = \Phi$. Ponovo se lako pokazuje da sve simetrije date figure Φ čine grupu, $\mathrm{Sym}(\Phi)$, koja je sadržana u $\mathrm{Iso}(M)$ grupa simetrija figure (tj. u terminologiji koju ćemo uvesti u narednoj glavi, $\mathrm{Sym}(\Phi)$ je *podgrupa* od $\mathrm{Iso}(M)$).

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 $O(n)$. ortogonalna grupa 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 *specijalnu ortogonalnu grupu* $SO(2)$. Koncept specijalne specijalna ortogonalna grupa ortogonalne grupe može se uopštiti na više dimenzije (kao grupa 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.

Primer 1.10. 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. dijedarska grupa Dokazaćemo ne samo da je D_n konačna grupa, već i da je $|D_n| = 2n$ i tačno opisati njene elemente.

Neka su temena posmatranog poligona $A_1, \ldots, A_n$. Dalje, neka ρ označava rotaciju oko P za ugao $\frac{2\pi}{n}$, i neka je σ osna simetrija u odnosu na pravu PA_1.

Jasno, sledeće izometrije su elementi dijedarske grupe:

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

Tvrdimo da su ove izometrije sve različite. Zaista $A_1\rho^k = A_1\sigma\rho^k = A_{k+1}$, što odmah implicira 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 $A_2\sigma = A_n$ i $A_2\rho^k = A_{k+2}$ (gde je po potrebi A_{n+1} druga oznaka za A_1), a $A_n\rho^k = A_k$.

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 $P\tau = P$. 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 $(\triangle PA_1A_2)\tau = \triangle PA_kA_{k+1}$ za neko k, tako da je ili

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

ili

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

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.

Za kasniju primenu, primetimo da važi $\rho^n = \mathrm{id}_{\mathbb{R}^2}$ (tako da je $\rho^{-1} = \rho^{n-1}$), zatim $\sigma^2 = \mathrm{id}_{\mathbb{R}^2}$ (tako da je σ sama sebi inverzna), i, konačno, da važi

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

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 $x = x_1 e_1 + \cdots + x_n e_n$, 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

$$\alpha(\beta(x)) = ABx,$$

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. 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.

Primer 1.11. 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 $O'(n)$ (iz razloga koji će postati jasni već u narednom odeljku). 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

S druge strane, regularna kompleksna matrica je *unitarna* ako je njen inverz jednak njenoj kompleksno konjugovanoj transponovanoj matrici: $A^{-1} = \overline{A}^T$.

grupa unitarnih matrica

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 $SL_n(\mathbb{C})$.

Primer 1.12. Grupe matrica daju, između ostalog, primere elemenata konačnog reda čiji proizvod ne mora biti konačnog reda. Na primer, u $GL_2(\mathbb{Q})$ posmatrajmo matrice

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 2 \\ \frac{1}{2} & 0 \end{pmatrix}.$$

Važi $A^2 = B^2 = E$ (sa E označavamo jediničnu matricu), ali je

$$AB = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & 2 \end{pmatrix}$$

element beskonačnog reda, jer je

$$(AB)^n = \begin{pmatrix} \frac{1}{2^n} & 0 \\ 0 & 2^n \end{pmatrix}.$$

S druge strane, u Abelovim grupama važi da je proizvod elemenata konačnog reda takođe konačnog reda; kao neposrednu polsedicu komutativnosti imamo da je $(ab)^n = a^n b^n$, pri čemu je desna strana jednaka 1 kadgod je n deljivo najmanjim zajedničkim sadržaocem redova $o(a)$ i $o(b)$.

1.5 Izomorfizmi i automorfizmi

izomorfizam grupa

Neka su $(G_1, \cdot)$ i $(G_2, *)$ grupe. Za G_1 i G_2 kažemo da su *izomorfne*, u oznaci $G_1 \cong G_2$, ako postoji bijekcija $\phi : G_1 \to G_2$ takva da za sve $a, b \in G_1$ važi

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

Primetimo da je operacija sa leve strane u grupi G_1, dok je ona sa desne strane u grupi G_2. Izomorfne grupe u algebarskom smislu smatramo (praktično) identičnim – jedina razlika između grupa G_1 i G_2 je zapravo u različitim "imenima" njenih elemenata, ali su svi odnosi, algebarska strukturna svojstva ista, tj. tablica grupe G_2 se dobija prostim preimenovanjem (u skladu sa bijekcijom ϕ) elemenata iz tablice grupe G_1.

Posebno zanimljiv slučaj izomorfizama grupa nastaje kada su G_1 i G_2 (fizički) jedna ista grupa G: izomorfizmi grupe G na samu sebe se nazivaju *automorfizmi* grupe G. Zapravo, radi se o simetrijama same grupe G, njenim permutacijama koje "čuvaju" njenu algebarsku strukturu. Svi automorfizmi grupe G ponovo čine grupu (u odnosu na kompoziciju funkcija), sadržanu u simetričnoj grupi $\mathbb{S}_G$. Grupu automorfizama od G označavamo sa $\mathrm{Aut}(G)$.

Primer 1.13. Grupe $(\mathbb{R}^+, \cdot)$ i $(\mathbb{R}, +)$ su izomorfne: preslikavanje $\phi : \mathbb{R}^+ \to \mathbb{R}$ definisano sa

$$x\phi = \ln x$$

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

Primer 1.14. 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 $\phi : \varepsilon^k \mapsto k$ izomorfizam (zahvaljujući tome što je $e^{2\pi i} = 1$). Ova grupa je dalje izomorfna grupi koju čine rotacije u realnoj ravni $\mathrm{id}_{\mathbb{R}^2}, \rho, \ldots, \rho^{n-1}$, gde je ρ rotacija oko neke tačke O za ugao $\frac{2\pi}{n}$: preslikavanje $k \mapsto \rho^k$ predstavlja jedan izomorfizam. Specijalno, grupa koja se sastoji od $1, i, -1, -i$ pomenuta u Primeru 1.7 izomorfna je cikličnoj grupi $\mathbb{Z}_4$.

Primer 1.15. 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 $SL_2(\mathbb{C})$.

Primer 1.16. 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 restrikcija izomorfizma $\mathrm{Aut}(\mathbb{R}^n)$ i $GL_n(\mathbb{R})$ na izometrije koje fiksiraju koordinatni početak predstavlja izomorfizam ortogonalne grupe $O(n)$ i grupe ortogonalnih matrica $O'(n)$ (što objašnjava ime grupe). Zbog ovog, od sada ćemo i grupu ortogonalnih matrica formata $n \times n$ označavati sa $O(n)$. Iz analognih razloga, imamo $SO(n) \cong SO'(n)$.

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. Lagani dokaz ostavljamo za vežbu.

Lema 1.17. *Neka je $\phi : G_1 \to G_2$ izomorfizam grupa. Tada za sve $a \in G_1$ važi:*

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

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

Posledica 1.18. *(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

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

$i \in \{0, 1\}$, $j \in \{0, 1, 2\}$, 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

Podgrupe

2.1 Definicija podgrupe

U primerima u prethodnoj glavi smo se već susreli sa situacijom gde unutar neke grupe $(G, \cdot)$ određeni neprazan podskup $H \subseteq G$ takođe formira grupu (u odnosu na restrikciju $\cdot|_{H \times H}$ operacije $\cdot$ grupe G). U tom slučaju kažemo da je H *podgrupa* grupe G i pišemo $H \leq G$. Svaka grupa G ima dve *trivijalne podgrupe*: to su sama grupa G i $E = \{1\}$. podgrupe

Propozicija 2.1. *Neka je G grupa i H njen neprazan podskup. Tada H čini podgrupu od G ako i samo ako važe uslovi:*

(1) za sve $a, b \in H$ važi $ab \in H$;

(2) $1 \in H$;

(3) za sve $a \in H$ važi $a^{-1} \in H$.

Dokaz. Očigledno je da uslovi (1)–(3) impliciraju da je H podgrupa od G. Zato pođimo od pretpostavke da je H podgrupa od G. Uslov (1) je automatski zadovoljen. Neka je sada e jedinični element grupe H. Tada je $e \cdot e = e = e \cdot 1$, pa kancelacijom sledi da je $e = 1$, tj. $1 \in H$. Najzad, upravo dokazano poklapanje jedinica grupa G i H i jedinstvenost inverznog elementa u grupi G povlače uslov (3). $\square$

Postoji i nešto kompaktniji način da se zapiše uslov da je H podgrupa od G koji uključuje operacije na podskupovima od G. 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, $(AB)^{-1} = B^{-1}A^{-1}$.

karakterizacije podgrupa

Propozicija 2.2. *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. Po Propoziciji 2.1, uslov (1) 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 tvrđenje sledi po Propoziciji 2.1. □

2.2 Generatorni skupovi

presek familije podgrupa je ponovo podgrupa

Propozicija 2.3. *Neka je $\{H_i : \ i \in I\}$ proizvoljna neprazna familija podgrupa grupe G. Tada je i*

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

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, $ab, a^{-1} \in H$. Pošto su sada ispunjeni svi uslovi Propozicije 2.1, sledi da je $H \leq G$. □

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

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

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

podgrupa generaisana skupom

Kao posledicu Propozicije 2.3 imamo da je za proizvoljne $H_1, H_2 \leq G$, presek $H_1 \cap H_2$ takođe podgrupa od G; štaviše, to je najveća podgrupa sadržana u H_1 i H_2. S druge strane, unija $H_1 \cup H_2$ gotovo nikada nije podgrupa od G (zapravo, lako se pokazuje da je to slučaj ako i samo ako je jedna od podgrupa H_1, H_2 sadržana u drugoj), ali zato konstrukcija generisanja podgrupe datim skupom omogućava da nađemo najmanju podgrupu od G koja sadrži H_1 i H_2: to je $\langle H_1 \cup H_2 \rangle$. Iz navedenih razloga važi naredni rezultat.

Propozicija 2.4. *Neka* $\mathrm{Sub}(G)$ *označava kolekciju svih podgrupa grupe* G. *Tada je parcijalno uređeni skup* $(\mathrm{Sub}(G), \subseteq)$ *mreža.*

podgrupe čine mrežu

Sledeće tvrđenje daje opis elemenata podgrupe generisane nekim podskupom grupe.

Propozicija 2.5. *Neka je* G *grupa i* $A \subseteq G$. *Tada je* $\langle \varnothing \rangle = E$, *dok je u slučaju da je* A *neprazan skup*

opis elemenata podgrupe generisane skupom A

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

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. Tvrđenje sada sledi po Propoziciji 2.1. □

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

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

karakterizacija cikličnih grupa

Teorema 2.6. *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 $\mathbb{Z}$).*

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 $a^k\phi = k$ 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 $a^n\phi = n$ za sve $n \in \mathbb{Z}$ izomorfizam grupa. □

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, zajedno sa Posledicom 1.5, odmah daje sledeći rezultat.

Posledica 2.7. *Neka je $1 \leq k < n$. Tada $\mathbb{Z}_n = \langle k \rangle$ 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 $\mathbb{Z}$.*

podgrupe ciklične grupe

Teorema 2.8. *Svaka podgrupa ciklične grupe je ciklična. Pri tome:*

(i) U $\mathbb{Z}_n$ ostatak 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

$$H = \{r_1, \dots, r_m\}$$

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

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

za neko $0 < r'' < r_1$, odakle sledi da $r'' = r_i - q' r_1 \in H$, kontradikcija. Dakle, $H = \{kr_1 : \ 0 \leq k < n/r_1\}$, što znači da je $m = n/r_1$ i $H \cong \mathbb{Z}_m$. Obratno, za svaki delitelj $d \mid n$, ostatak n/d odredjuje (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, $H = n\mathbb{Z} = \langle n \rangle$. □

2.3 Koseti i indeks podgrupe

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. koseti

Lema 2.9. *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 2.10. *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.

svi koseti su iste kardinalnosti

Propozicija 2.11. *Neka je G grupa, $a, b \in G$ i $H \leq G$. Tada je $|Ha| = |bH| = |H|$.*

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

svaka podgrupa ima jednako mnogo levih i desnih koseta

Propozicija 2.12. *Neka je G grupa i $H \leq G$. Tada je*

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

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

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

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 $(Hg^{-1})\psi = gH$. 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 2.13 (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

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

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 $h_1 g_i = (g_i, h_1)\psi = (g_j, h_2)\psi = h_2 g_j$. 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. $\square$

Posledica 2.14. *Neka je G konačna grupa, $H \leq G$ i $g \in G$. Tada $|H| \mid |G|$ i $o(g) \mid |G|$.*

Posledica 2.15. *(1)* (Ojlerova teorema) *Neka je $n \geq 1$ prirodan broj i $a \in \mathbb{Z}$ takav da je $(a, n) = 1$. Tada je* Ojlerova i mala Fermaova teorema

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

(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 $\varphi(p) = p - 1$. $\square$

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

Posledica 2.16. *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), $G \cong \mathbb{Z}_p$. □

2.4 Neke značajne podgrupe

centar grupe

Primer 2.17. *Centar grupe* G je skup svih onih elemenata G koji komutiraju sa svim elementima grupe G, dakle,

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

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*.

komutator

Primer 2.18. Za $a, b \in G$ definišemo *komutator* elemenata a, b (pri čemu je poredak bitan) sa:

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

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 2.19. 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.

3

Normalne podgrupe

3.1 Definicija normalne podgrupe i osnovne osobine

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 3.1. 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 3.2. 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 3.3. *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, $H \trianglelefteq G$. $\square$

Primer 3.4. 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.

Propozicija 3.5. *Neka je $H \leq G$. Tada su sledeći uslovi ekvivalentni:*

karakterizacije normalnih podgrupa

(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)$\Rightarrow$(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 $Hg = g(g^{-1}Hg) = gH$. $\square$

Posledica 3.6. *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, $G' \trianglelefteq G$. $\square$

3.2 Konjugovanost i klasovna jednačina

Prethodna tvrđenja motivišu uvođenje preslikavanja $\sigma_a : G \to G$ za dato $a \in G$ definisanog sa

unutrašnji automorfizam (konjugacija)

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

Zbog kancelativnosti je σ_a "1-1", a takođe je i "na" (zbog $(aga^{-1})\sigma_a = g$). Dakle, u pitanju je automorfizam grupe G, pošto je $(gh)\sigma_a = a^{-1}gha = (a^{-1}ga)(a^{-1}ha) = (g\sigma_a)(h\sigma_a)$. 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

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

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 $H = g^{-1}Kg = K\sigma_g$ za neko $g \in G$. Prema tome, podgrupa je normalna ako i samo ako se poklapa sa svim svojim konjugovanim podgrupama.

klasa konjugovanosti

Iako ćemo u načelu za relaciju ekvivalencije ρ klasu elementa x označavati sa $x\rho$, specijalno klasu svih elemenata konjugovanih sa x pišemo $\widetilde{x}$.

Lema 3.7. $|\widetilde{x}| = 1$ *ako i samo ako* $x \in Z(G)$.

Dokaz. Važi $|\widetilde{x}| = 1$ ako i samo ako je $x\sigma_g = x$ 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 3.8. $|\widetilde{x}| = (G : C(x))$.

Dokaz. Najpre, jasno je da je $\widetilde{x} = \{x\sigma_g : g \in G\}$. Prema tome, $|\widetilde{x}| = |G/\rho|$ gde je ρ relacija ekvivalencije na G definisana sa $(g, h) \in \rho$ ako i samo ako $x\sigma_g = x\sigma_h$. 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 3.9 (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*

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

Posledica 3.10. *Neka je p prost broj i $|G| = p^n$ za neko $n \geq 1$. Tada je $Z(G)$ netrivijalna grupa.*

p-grupe imaju netrivijalni centar

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

podgrupa je normalna akko je unija celih klasa konjugovanosti

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

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

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

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

Posledica 3.12. *U svakoj grupi G, ako $H \leq Z(G)$ tada je $H \trianglelefteq G$.*

Dokaz. Po Lemi 3.7, svaki element centra $Z(G)$ formira jednoelementnu klasu ekvivalencije relacije $\sim$, pa to isto važi i za H. Sada tvrđenje seldi direktno po prethodnoj teoremi. □

U narednom tvrđenju analiziramo relaciju konjugovanosti u simetričnim grupama.

Propozicija 3.13. *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

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

Zaista, važi

$$\pi = \rho^{-1}\tau\rho = (\rho^{-1}(a_1a_2\dots)\rho)\dots(\rho^{-1}(b_1b_2\dots)\rho),$$

pa je dovoljno analizirati konjugacije pojedinačnih ciklusa, tj. proveriti da je $\rho^{-1}(a_1a_2\dots)\rho = (a_1\rho\ a_2\rho\ \ \dots)$. Neka je $k \in \{1,\dots,n\}$. Ako $k\rho^{-1} \notin \{a_1,a_2,\dots\}$, tada je očito $k(\rho^{-1}(a_1a_2\dots)\rho) = k\rho^{-1}\rho = k$. U suprotnom $k\rho^{-1} = a_i$ za neko i, tj. $k = a_i\rho$. U tom slučaju je

$$k(\rho^{-1}(a_1a_2\dots)\rho) = a_i((a_1a_2\dots)\rho) = a_{i+1}\rho,$$

pri čemu je $a_{i+1} = a_1$ ako je i dužina posmatranog ciklusa. Dakle, $a_i\rho$ se slika u $a_{i+1}\rho$, 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 $1 \le j \le l_i$,

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

Na ovaj način, ρ nije definisano 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 $\pi \sim \tau$. □

normalnost podgrupa nije tranzitivna osobina

Primer 3.14. 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

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

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 3.11 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 “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 $H\phi = H$ (kako je sa svakim automorfizmom ϕ i njegov inverz ϕ^{-1} takođe automorfizam grupe G, može se pokazati da je ovo ekvivalnentno slabijem uslovu $H\phi \subseteq H$). 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 3.15. *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 $K\sigma_g = K$ zbog čega je $\phi = \sigma_g|_K \in \mathrm{Aut}(K)$. Po datim uslovima mora biti $H\phi = H$. Međutim, po definiciji ϕ to znači da je $g^{-1}Hg = H$. Zaključujemo da je $H \trianglelefteq G$. $\square$

3.3 Homomorfizmi i faktor grupe

Neka su $(G, \cdot)$ i $(H, *)$ grupe (ponovo 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

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

Dakle, radi se o istom uslovu kao i u definiciji izomorfizma grupa, samo bez zahteva da ϕ bude bijekcija. Prema tome, izomorfizmi su upravo bijektivni homomorfizmi. 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, kao što smo videli, *automorfizmi* grupe G.

Lako se pokazuje da za svaki homomorfizam mora biti $1_G\phi = 1_H$ kao i $(a^{-1})\phi = (a\phi)^{-1}$ 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

$$\mathrm{Im}\,\phi = G\phi$$

kao i njegovo *jezgro*

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

Slika svakog homomorfizma jeste podgrupa od H (upravo po definiciji homomorfizma), dok se za jezgro može reći i više.

jezgro je uvek normalna podgrupa

Lema 3.16. *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 $a\phi = b\phi = 1_H$, pa je $(ab^{-1})\phi = a\phi * (b\phi)^{-1} = 1_H$, tj. $ab^{-1} \in \operatorname{Ker}\phi$. Normalnost $\operatorname{Ker}\phi$ u G sledi pošto važi

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

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 3.17. *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 $g\nu_N = Ng$ za sve $g \in G$. prirodno preslikavanje

Propozicija 3.18. *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 $(gh)\nu_N = Ngh = (Ng)(Nh) = (g\nu_N)(h\nu_N)$, 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 $g\nu_N = N$ ako i samo ako $Ng = N$ ako i samo ako $g \in N$, pa je $\operatorname{Ker} \nu_N = N$. $\square$

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

Teorema 3.19 (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

$$[(\operatorname{Ker} \phi)a]\psi = a\phi$$

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 $(ab^{-1})\phi = 1_H$ ako i samo ako $a\phi = b\phi$ ako i samo ako $[(\operatorname{Ker} \phi)a]\psi = [(\operatorname{Ker} \phi)b]\psi$. 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 $h = a\phi = [(\operatorname{Ker} \phi)a]\psi$. Konačno, ψ je homomorfizam jer je $[(\operatorname{Ker} \phi)ab]\psi = (ab)\phi = (a\phi)(b\phi) = [(\operatorname{Ker} \phi)a]\psi[(\operatorname{Ker} \phi)b]\psi$ za sve $a, b \in G$. $\square$

Ispostavlja se da postoji veoma tesna veza između strukture podgrupa faktor grupe G/N i podgrupa same grupe G.

Teorema 3.20 (Teorema o korespondenciji)**.** *Neka je G grupa i $N \trianglelefteq G$. Tada je parcijalno uređeni skup (mreža) podgrupa* $\operatorname{Sub}(G/N)$ *faktor grupe G/N izomorfna intervalu $[N, G]$ u parcijalnu uređenom skupu podgrupa* $\operatorname{Sub}(G)$*, tj. mreži svih podgrupa od G koje sadrže N.* teorema o korespondenciji

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

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

odnosno

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

Oba ova preslikavanja su dobro definisana, jer $N \trianglelefteq G$ povlači $N \trianglelefteq H$ za $N \leq H \leq G$; pored toga, $K\psi$ sadrži N i reč je o podgrupi od G, jer $a, b \in K\psi$ 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 $ab^{-1} \in Ng_1g_2^{-1}N = Ng_1g_2^{-1} \subseteq K\psi$ (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 (i zato i izomorfizmi mreža). □

grupa unutrašnjih automorfizama

Budući da za sve $a, b \in G$ važi $\sigma_a\sigma_b = \sigma_{ab}$, $\sigma_a^{-1} = \sigma_{a^{-1}}$ i $\sigma_1 = \mathrm{id}_G$, unutrašnji automorfizmi čine podgrupu od $\mathrm{Aut}(G)$, koju označavamo sa $\mathrm{Inn}(G)$.

Propozicija 3.21. *Za svaku grupu G važi* $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$.

Dokaz. Neka je $\phi \in \mathrm{Aut}(G)$ proizvoljan automorfizam i $a, g \in G$. Tada je

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

pa je $\phi^{-1}\sigma_a\phi = \sigma_{a\phi} \in \mathrm{Inn}(G)$. □

Grupu spoljašnjih automorfizama definišemo kao faktor grupu $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$.

Sada možemo opisati i faktor grupe po njenom centru.

Propozicija 3.22. *Za svaku grupu G važi* $G/Z(G) \cong \mathrm{Inn}(G)$.

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

$$a\phi = \sigma_a.$$

Jasno, $\mathrm{Im}\,\phi = \mathrm{Inn}(G)$. S druge strane, $g \in \mathrm{Ker}\,\phi$ 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, $\mathrm{Ker}\,\phi = Z(G)$, pa rezultat sledi po Teoremi o homomorfizmu. □

3.4 Srž i normalizator

Srž podgrupe $H \leq G$ je

srž podgrupe

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

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

Propozicija 3.23. *Neka je G grupa i $H \leq G$. Tada je $\operatorname{core}(H)$ najveća normalna podgrupa od G sadržana u H.*

karakterizacija srži

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

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

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

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 3.24. *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 3.25 (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 $\operatorname{Aut}(H)$.*

N/C teorema

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

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

Pre svega, ova definicija je korektna jer je zaista $\sigma_g|_H \in \mathrm{Aut}(H)$ zbog $H\sigma_g = g^{-1}Hg = H$ za sve $g \in N(H)$. Odredimo sada jezgro ovog homomorfizma. Imamo da $g \in \mathrm{Ker}\,\phi$ ako i samo ako $g\phi = \mathrm{id}_H$ 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 $\mathrm{Aut}(H)$. □

3.5 Teoreme 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 3.26. *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, $\langle A \cup B \rangle = AB$. □

Posledica 3.27. *Neka je G grupa. Ako je $A \leq G$ i $B \trianglelefteq G$, tada je $AB \leq G$.*

prva teorema o izomorfizmu

Teorema 3.28 (Prva teorema o izomorfizmu)**.** *Neka je G grupa i $A \leq G$, $B \trianglelefteq G$. Tada je $A \cap B \trianglelefteq A$ i važi*

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

Dokaz. Posmatrajmo preslikavanje $\phi : A \to G/B$ koje se dobija kao restrikcija prirodnog preslikavanja ν_B na podgrupu A: $a\phi = Ba$. Sada $g \in Ker\phi$ 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, $\operatorname{Im}\phi = A\phi = \{Ba : a \in A\} = \{Bx : x \in BA = AB\} = AB/B$, pa teorema sledi iz Teoreme o homomorfizmu. $\square$

Primedba 3.29. Primetimo da je (mrežni) izomorfizam ϕ iz dokaza Teoreme o korespondenciji zapravo prirodno preslikavanje ν_N koje deluje na podgrupe od G koja sadrže N. Međutim, sada se lako vidi iz prethodnog dokaza da za *proizvoljnu* podgrupu $K \leq G$ važi $K\nu_N = KN/N$. Ovu opasku ćemo u daljem takođe smatrati delom Teoreme o korespondenciji i podgrupu $KN/N \leq G/N$ pominjati kao "odgovarajuću" podgrupi $K \leq G$ u smislu prirodnog homomorfizma.

proširenje teoreme o korespondenciji

Sada ćemo videti jednu izuzetno značajnu posledicu Prve teoreme o izomorfizmu, *lemu Casenhausa*[3], koja će imati ključnu primenu u sedmoj glavi u izučavanju kompozicionih nizova grupa.

Posledica 3.30 (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*

lema Casenhausa

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

Dokaz. Imajući u vidu Posledicu 3.27 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 $C(D \cap A) = (D \cap A)C$.

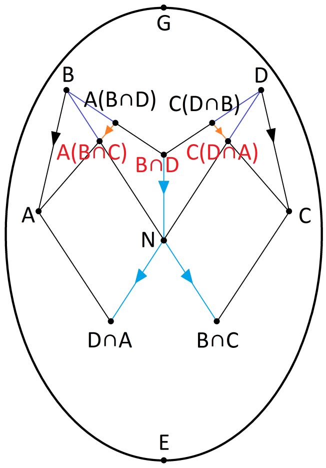
Tvrdimo da je $B \cap C \trianglelefteq B \cap D$; neka je $c \in B \cap C$ i $d \in B \cap D$. Kako $c, d \in B$, odmah sledi da je $d^{-1}cd \in B$. S druge strane, $C \trianglelefteq D$ povlači da $d^{-1}cd \in C$, pa $d^{-1}cd \in B \cap C$. Analogno zaključujemo da je $D \cap A \trianglelefteq D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

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

normalna podgrupa od $B \cap D$.

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.

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



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. □

druga teorema o izomorfizmu

Teorema 3.31 (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*

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

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

$$(Ag)\phi = Bg$$

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 $\operatorname{Ker}\phi = B/A$. Zaista, $Ag \in \operatorname{Ker}\phi$ 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 3.32. *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 3.33. *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'. $\square$

4

Direktni i poludirektni proizvodi grupa

Neka su G_1, G_2 grupe. Posmatrajmo direktan proizvod skupova $G_1 \times G_2 = \{(g, h) : g \in G_1, h \in G_2\}$ 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, *(spoljašnji) direktni 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.

spoljašnji direktan proizvod

Rutinski se pokazuju sledeća tvrđenja.

Lema 4.1. *(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) $Z(G_1 \times G_2) = Z(G_1) \times Z(G_2)$.

projekcije

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

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

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

Propozicija 4.2. *Neka je $G = G_1 \times G_2$.* osobine projekcija

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

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

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

Dokaz. (1) Važi $(c, b)^{-1}(a, 1_{G_2})(c, b) = (c^{-1}ac, 1_{G_2}) \in G\pi_1$ za sve $a, c \in G_1$, $b \in G_2$; izomorfizam $G\pi_1 \cong G_1$ 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. $\square$

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 4.3. *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. $ab = ba$. $\square$

Propozicija 4.4. *Ako je G unutrašnji direktan proizvod svojih (normalnih) podgrupa A, B, tada je $G \cong A \times B$.* unutrašnji direktan proizvod je istovremeno i spoljašnji (i obratno)

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

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

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:

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

što je i trebalo dokazati. □

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

direktnan proizvod konačne familije grupa

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

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

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

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

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) $G = A_1 \ldots A_n$,

(3) $A_i \cap A_1 \ldots A_{i-1}A_{i+1} \ldots A_n = E$ 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 $G \cong A_1 \times \cdots \times A_n$.

Primer 4.5. 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.

Konačno, prelazimo na najopštiji slučaj, kada nam je data proizvoljna familija grupa $\{G_i : i \in I\}$. Tada, naravno, možemo formirati direktan proizvod skupova $\prod_{i\in I} G_i$ (koji se sastoji od svih funkcija $g : I \to \bigcup_{i\in I} G_i$ takvih da je $ig \in G_i$ za sve $i \in I$) i na njemu definisati grupu G sa po-komponentnom primenom operacija, kao i odgovarajuće projekcije $G\pi_i$. Po analogiji sa prethodnim slučajevima, očekivali bismo da će G ispuniti sledeće uslove:

direktan proizvod proizvoljne familije grupa

(1) $G\pi_i \trianglelefteq G$ za sve $i \in I$,

(2) $G = \left\langle \bigcup_{i\in I} G\pi_i \right\rangle$,

(3) $G\pi_i \cap \left\langle \bigcup_{j\in I\setminus\{i\}} G\pi_j \right\rangle = E$ za sve $i \in I$.

Zaista, nije teško proveriti da (1) i (3) zaista važi. Međutim, ukoliko je I beskonačan skup tada (2) *ne* važi: sve projekcije generišu pravu podgrupu od G koja se sastoji od svih funkcija $g : I \to \bigcup_{i\in I} G_i$ takvih da je $ig \neq 1_{G_i}$ za samo *konačno mnogo* vrednosti $i \in I$. Ovu podgrupu ćemo zvati *diskretan direktan proizvod* i *nju* ćemo označavati sa $\prod_{i\in I} G_i$, dok ćemo grupu definisanu na celom direktnom proizvodu domena grupa G_i zvati *kompletan direktan proizvod* i označavati sa $\prod^*_{i\in I} G_i$. Sada diskretan direktan proizvod možemo identifikovati sa unutrašnjim proizvodom (analogno već opisanim tehnikama), dok je tako nešto nemoguće u slučaju kompletnog direktnog proizvoda, budući da je kompletan proizvod beskonačne familije netrivijalnih grupa – neprebrojiva grupa.

diskretan i kompletan proizvod

Primer 4.6. Kolika razlika može da postoji između algebarskih svojstava diskretnog i kompletnog direktnog proizvoda pokazuje sledeći primer. Neka je p_i, $i \in \mathbb{N}$, niz svih prostih brojeva. Definišimo

$$G = \prod_{i\in\mathbb{N}} Z_{p_i} \ \text{ i } \ G^* = \prod_{i\in\mathbb{N}}{}^* Z_{p_i}.$$

U G su svi elementi konačnog reda (naime, $o(g) = \prod_{ig\neq 0} p_i$), dok G^* ima elemente beskonačnog reda: jedan takav je, na primer, niz $ig = 1$ za sve $i \in \mathbb{N}$.

unutrašnji poludirekatn proizvod

Konstrukcija *unutrašnjeg poludirektnog proizvoda* (podgrupa u datoj grupi G) dobija se oslabljenjem uslova koje tražimo od podgrupa A, B. Naime, kažemo da je G unutrašnji poludirketni proizvod svojih podgrupa A, B, u oznaci $G = A \ltimes B$ (pri čemu je redosled navođenja podgrupa bitan!), ako važi:

(1) $B \trianglelefteq G$,

(2) $AB = G$,

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

Dakle, od podgrupe A više ne zahtevamo da bude normalna.

spoljašnji poludirektan proizvod

Poludirektan proizvod ima i svoju "spoljašnju verziju". Za tu konstrukciju su nam potrebne dve grupe G_1, G_2, kao i jedan (unapred fiksiran) homomorfizam $\phi : G_1 \to \mathrm{Aut}(G_2)$. Sada definišemo *spoljašnji poludirektan proizvod* $G_1 \ltimes_\phi G_2$ (u odnosu na ϕ) na skupu parova $G_1 \times G_2$ sa sledećom operacijom:

$$(g_1, g_2)(h_1, h_2) = (g_1 h_1, [g_2(h_1\phi)]h_2)$$

za proizvoljne $g_1, h_1 \in G_1$, $g_2, h_2 \in G_2$ (primetimo da je $h_1\phi$ automrofizam grupe G_2 koji onda deluje na element g_2). Na ovaj način je zaista dobijena grupa, čiji je jedinični element $(1_{G_1}, 1_{G_2})$, dok je inverz para (g_1, g_2) jednak $(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1}(g_1\phi)^{-1})$.

Sledeće dve propozicije pokazuju ekvivalenciju konstrukcija unutrašnjeg i spoljašnjeg poludirektnog proizvoda.

unutrašnji poludirektan proizvod je spoljšnji

Propozicija 4.7. *Neka je grupa G unutrašnji poludirektni proizvod svojih podgrupa A i B, $G = A \ltimes B$. Tada postoji homomorfizam $\phi : A \to \mathrm{Aut}(B)$ tako da je $G \cong A \ltimes_\phi B$.*

Dokaz. Pošto je $B \trianglelefteq G$, važi $g^{-1}Bg = B$ za sve $g \in G$, tj. restrikcija unutrašnjeg automorfizma σ_g na B je permutacija i, zapravo, automorfizam podgrupe B. Stoga definišimo $a\phi = \sigma_a|_B$ za sve $a \in A$. Slično kao i u dokazu Propozicije 4.4, svaki element $g \in G$ ima jedinstvenu faktorizaciju $g = ab$ tako da je $a \in A$, $b \in B$, pa definišimo preslikavanje $\psi : G \to A \times B$ sa

$$g\psi = (a, b).$$

Već imamo da je ψ bijekcija. Dokažimo da je zapravo posredi izomorfizam $G \to A \ltimes_\phi B$. Neka su $g_1, g_2 \in G$ sa faktorizacijama $g_1 = a_1 b_1$ i $g_2 = a_2 b_2$. Tada je

$$(g_1 g_2)\psi = (a_1 b_1 a_2 b_2)\psi = ((a_1 a_2)(a_2^{-1} b_1 a_2 b_2))\psi = (a_1 a_2, (b_1 \sigma_{a_2}) b_2),$$

jer je zbog normalnosti B, $a_2^{-1}b_1a_2 \in B$. Međutim, desna strana je dalje jednaka

$$(a_1a_2, [b_1(a_2\phi)]b_2) = (a_1, b_1)(a_2, b_2) = (g_1\psi)(g_2\psi),$$

što je i trebalo pokazati. □

Propozicija 4.8. *Neka su G_1, G_2 grupe i $\phi : G_1 \to \mathrm{Aut}(G_2)$ homomorfizam. Tada je $G = G_1 \ltimes_\phi G_2$ unutrašnji poludirektni proizvod od $G\pi_1$ i $G\pi_2$.*

spoljašnji poludirektan proizvod je unutrašnji

Dokaz. $G\pi_1$ je očito podgrupa od G, a to je i $G\pi_2$ jer je

$$(1_{G_1}, g_2)(1_{G_1}, h_2) = (1_{G_1}, [g_2(1_{G_1}\phi)]h_2) = (1, g_2h_2).$$

Štaviše, $G\pi_2 \trianglelefteq G$ jer je

$$(g_1, g_2)^{-1}(1_{G_1}, h_2)(g_1, g_2) = (g_1^{-1}, g_2^{-1}(g_1\phi)^{-1})(g_1, [h_2(g_1\phi)]g_2) =$$

$$= (1_{G_1}, [g_2^{-1}(g_1\phi)^{-1}(g_1\phi)][h_2(g_1\phi)]g_2) = (1_{G_1}, g_2^{-1}[h_2(g_1\phi)]g_2).$$

Zbog toga je $(G\pi_1)(G\pi_2) = G$, pošto je

$$(g_1, 1_{G_2})(1_{G_1}, g_2) = (g_1, [1_{G_2}(1_{G_1}\phi)]g_2) = (g_1, g_2).$$

Najzad, očigledno je $G\pi_1 \cap G\pi_2 = E$. Tako je $G = G\pi_1 \ltimes G\pi_2$. □

Primer 4.9. Direktan proizvod $G_1 \times G_2$ je specijalan slučaj spoljašnjeg poludirektnog proizvoda $G_1 \ltimes_\phi G_2$ kada se za $\phi : G_1 \to \mathrm{Aut}(G_2)$ uzme trivijalan homomorfizam koji svakom elementu G_1 dodeljuje identičko preslikavanje na G_2. Zaista, tada je

direktan proizvod kao specijalan slučaj poludirektnog

$$(g_1, g_2)(h_1, h_2) = (g_1h_1, [g_2(h_1\phi)]h_2) = (g_1h_1, g_2h_2)$$

jer je $g_2(h_1\phi) = g_2$.

Primer 4.10. Dijedarske grupe D_n predstavljaju tipičan primer poludirektnih proizvoda. Neka je σ jedna od osa simetrije pravilnog n-tougla i $A = \langle\sigma\rangle$, a ρ rotacija za $2\pi/n$ i $B = \langle\rho\rangle$. Kako je $(D_n : B) = 2$, sledi $B \trianglelefteq D_n$. Po samoj definiciji dijedarskih grupa važi $D_n = AB$, a očito je $A \cap B = E$. Tako je $D_n = A \ltimes B$.

dijedarske grupe su poludirektni proizvodi

Kao spoljašnji poludirektni proizvod, D_n se realizuje kao $\mathbb{Z}_2 \ltimes_\phi \mathbb{Z}_n$ (imajući u vidu da je $A \cong \mathbb{Z}_2$ i $B \cong \mathbb{Z}_n$), gde $\sigma\phi$ mora biti automorfizam ciklične grupe $\mathbb{Z}_n$ reda 2. Dakle, ako je $\rho(\sigma\phi) = \rho^k$, tada mora biti

$$\rho = \rho(\sigma\phi)^2 = \rho^{k^2},$$

pa $n \mid k^2 - 1$, tj. $k^2 \equiv 1(\mathrm{mod}\ n)$. Ova kongruencija ima dva rešenja po modulu n, naime $k = 1$ (što, kao što smo videli u prethodnom primeru, daje direktan proizvod $\mathbb{Z}_2 \times \mathbb{Z}_n$) i $k = -1$. Dakle, $\rho(\sigma\phi) = \rho^{-1}$, što znači da $\sigma\phi$ deluje na B invertovanjem (što je automorfizam od B, jer je B Abelova grupa). Kako je istovremeno $\rho(\sigma\phi) = \sigma^{-1}\rho\sigma = \sigma\rho\sigma$, odmah dobijamo poznatu relaciju dijedarskih grupa $\rho\sigma = \sigma\rho^{-1}$.

5

Grupe permutacija i dejstva

5.1 Simetrične i alternativne grupe

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 5.1 (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 $g\phi = \rho_g$ za sve $g \in G$, gde je permutacija ρ_g na G definisana sa

$$a\rho_g = ag$$

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

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

[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 $(gh)\phi = (g\phi)(h\phi)$, tj. ϕ je homomorfizam. On je injektivan, jer $g\phi = \rho_g = \rho_h = h\phi$ povlači $g = 1\rho_g = 1\rho_h = h$. □

parnost permutacije

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

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

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 5.2. *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. □

Lema 5.3. *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 5.4. *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

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

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

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

Drugim rečima, $\sigma^{-1}\tau\sigma\tau^{-1}$ ima više fiksnih tačaka od τ, pri čemu nije u pitanju identička permutacija jer je $2\sigma^{-1}\tau\sigma\tau^{-1} \in \{1,3\}$. 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 3.14 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 5.5. *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 3.33 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 $\mathbb{S}'_n = \mathbb{A}_n$. □

beskonačne proste grupe

Alternativne grupe nam, zajedno sa sledećim tvrđenjem, sada omogućavaju da konstruišemo primer beskonačne proste grupe.

Propozicija 5.6. *Neka je G grupa i $\{H_\alpha : \alpha \in I\}$ lanac njenih podgrupa (što znači da je I linearno uređen skup i $\alpha, \beta \in I$, $\alpha < \beta$, povlači da je $H_\alpha \subseteq H_\beta$) takav da je $G = \bigcup_{\alpha \in I} H_\alpha$. Ako su sve grupe H_α proste, tada je i G prosta grupa.*

Dokaz. Neka je $E \neq H \trianglelefteq G$. Tada je $H \cap H_\alpha \trianglelefteq H_\alpha$ za sve $\alpha \in I$, pa je $H \cap H_\alpha = E$ ili $H \cap H_\alpha = H_\alpha$, pošto je H_α prosta grupa. Međutim, zbog

$$H = H \cap G = H \cap \bigcup_{\alpha \in I} H_\alpha = \bigcup_{\alpha \in I} (H \cap H_\alpha)$$

mora postojati $\beta \in I$ tako da $H \cap H_\beta \neq E$, tj. $H \cap H_\beta = H_\beta$. No, sada za sve $\gamma > \beta$ ne može biti $H \cap H_\gamma = E$, pa je $H \cap H_\gamma = H_\gamma$; drugim rečima, $H_\gamma \subseteq H$. Otuda je $G \subseteq H$, odnosno $H = G$. □

Primer 5.7. Posmatrajmo simetričnu grupu $\mathbb{S}_\mathbb{N}$. Sada se svaka alternativna grupa $\mathbb{A}_n$ može identifikovati sa podgrupom $\mathbb{A}_n^* \leq \mathbb{S}_\mathbb{N}$ putem potapanja $\pi \mapsto \widehat{\pi}$, gde je

$$i\widehat{\pi} = \begin{cases} i\pi & i \leq n, \\ i & i > n. \end{cases}$$

Sada podgrupu od $\mathbb{S}_\mathbb{N}$ datu sa

$$\mathbb{A}_\mathbb{N} = \bigcup_{n \geq 1} \mathbb{A}_n^*$$

zovemo *beskonačna alternativna grupa*. Kao direktnu posledicu Teoreme 5.4 i prethodnog rezultata dobijamo da je $\mathbb{A}_\mathbb{N}$ prosta grupa. Primetimo da svaki njen konačan podskup pripada (konačnoj) grupi $\mathbb{A}_n^*$ za dovoljno veliko n; zato je svaka konačno generisana podgrupa od $\mathbb{A}_\mathbb{N}$ konačna, tj. $\mathbb{A}_\mathbb{N}$ je *lokalno konačna*. Odatle sledi da $\mathbb{A}_\mathbb{N}$ ne može biti konačno generisana. Međutim, postoje konačno generisane beskonačne proste grupe.

5.2 Dejstvo grupe na skup

(Desno) dejstvo grupe G na neprazan skup X je preslikavanje $\theta : X \times G \to X$ (pri čemu, radi preglednosti, $(x, g)\theta$ ponekad kraće pišemo kao x^g) koje zadovoljava uslove dejstvo grupe na skup

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

i

$$x^1 = x$$

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

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

Propozicija 5.8. *Za svako dejstvo θ grupe G na skup X, preslikavanje $\phi : G \to \mathbb{S}_X$ definisano sa*

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

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

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

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

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

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

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

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

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

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

orbite dejstva

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,

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

tranzitivnost dejstva, odnosno grupe permutacija

Dejstvo θ je *tranzitivno* ako ima tačno jednu orbitu. Analogno, za grupu permutacija $G \leq \mathbb{S}_X$ (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 $x\sigma = y$. Opštije, 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 $x_i\sigma = y_i$ za sve $1 \leq i \leq n$. 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 $x_i \mapsto y_i$, $1 \leq i \leq n-2$ možemo proširiti do permutacije na tačno dva načina, od kojih će jedan biti parna, a drugi neparna permutacija.

Za $x \in X$, skup stabilizator

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

nazivamo *stabilizator* elementa x.

Propozicija 5.9. *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

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

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 5.10. *Ako je G grupa permutacija stepena n koja je k-tostruko tranzitivna, tada* rezultat o redu tranzitivnih grupa

$$k!\binom{n}{k} \mid |G|.$$

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

Dokaz. Neka je

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

Tada G deluje na skup X_k dejstvom θ_k datim sa

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

Po prethodnom tvrđenju,

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

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

jezgro dejstva

Jezgro dejstva θ, $\operatorname{Ker}\theta$, definišemo kao jezgro pridruženog homomorfizma ϕ u smislu Propozicije 5.8: 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 $\mathbb{S}_X$.

dejstvo konjugovanjem

Primer 5.11. 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 5.12. 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.

proste grupe i koset dejstvo

Propozicija 5.13. *Neka je G prosta grupa i H njena prava podgrupa. Tada je G izomorfna grupi permutacija skupa desnih koseta $\{Ha : a \in G\}$.*

Dokaz. Posmatrajmo koset dejstvo θ grupe G u odnosu na H. Pošto je grupa G prosta, to je $\operatorname{core}(H) = E = \operatorname{Ker}\theta$. Zbog toga se G potapa u $\mathbb{S}_X$, gde je $X = \{Ha : a \in G\}$. □

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

Posledica 5.14. *Ako je G prosta grupa i $H \leq G$ takva da je $(G : H) = n$ tada je $|G| \leq n!$ (štaviše, $|G| \mid n!$).*

Posledica 5.15 ($n!$-teorema)**.** *Ako grupa G ima podgrupu H indeksa n, tada ima i pravu normalnu podgrupu indeksa najviše $n!$.*

$n!$-teorema

Primer 5.16. Po Teoremi 5.4, 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.

Ovaj odeljak završavamo rezultatom koji daje broj orbita dejstva konačne grupe na skup.

Propozicija 5.17 (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 5.9 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 sleda 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 $\{(x, g) \in X \times G : x^g = x\}$. □

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

6

Teoreme Silova

6.1 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]. Međutim, istorijski gledano, prvi rezultat u opisanom pravcu je sledeći.

Košijeva lema

Lema 6.1 (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 kardinalosti $|G|^{p-1}$ budući da se lako pokazuje da je preslikavanje $\psi : G^{p-1} \to A$ dato sa

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

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

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

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

Kako $xy = 1$ povlači $yx = 1$ u svakoj grupi, važi da je $A\pi \subseteq A$, 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 $1\theta = \pi$ i stoga $n\theta = \pi^n$ za sve $0 \leq n < p$. 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 5.9 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 6.2. *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 6.3. 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

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

I ovu grupu (slično beskonačnoj alternativnoj grupi) možemo dobiti kao uniju beskonačnog lanca cikličnih podgrupa (reda p^n) od $\mathbb{C}^\times$. Takođe, $\mathbb{Z}_{p^\infty}$ je primer beskonačne grupe u kojoj je svaka prava podgrupa konačna: naime, važi da je $\mathbb{Z}_{p^\infty}$ generisana svakim svojim beskonačnim podskupom, dok je $\langle A\rangle \cong \mathbb{Z}_{p^n}$ za svaki konačan skup A njenih elemenata u kojem je maksimalni red elementa jednak p^n.

Prva teorema Silova predstavlja suštinsko pojačanje Košijeve leme.

prva teorema Silova

Teorema 6.4 (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. Kao baza indukcije mogu nam poslužiti 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, $H = W\nu_K^{-1}$ (gde je $\nu_K : G \to G/K$ prirodni homomorfizam) je podgrupa od G za koju važi $K \trianglelefteq H$ i $H/K = W$, pa je $|H| = p^n$. Time je okončan induktivni dokaz. □

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

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

tome, prethodna teorema tvrdi da p-podgrupe Silova grupe G postoje za svaki prost broj p koji deli red $|G|$. Kasnije ćemo pokazati (u Drugoj teoremi Silova) da su p-podgrupama Silova iscrpljene sve maksimalne p-podgrupe od G, što daje alternativnu definiciju p-podgrupa Silova. No, najpre nam treba pomoćno tvrđenje.

Lema 6.5. *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 $P \leq N(P)$. $\square$

Teorema 6.6 (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

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

Jedina orbita ovog dejstva je $(g^{-1}Pg)^G = \{(ga)^{-1}Pga : \ a \in G\} = A$, pa je θ tranzitivno dejstvo. 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 dejstva θ na podgrupu H. Ako sa $H_{g^{-1}Pg}$ označimo stabilizator elementa $g^{-1}Pg \in A$ u odnosu na θ_0, po Propoziciji 5.9 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

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

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

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

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

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

To, između ostalog, znači da je skup $\{g^{-1}Pg : \ H \leq g^{-1}Pg\}$ neprazan, čime je stavka (i) dokazana: 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 5.9 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 $s_p \equiv 1 (\text{mod } p)$. Zbog toga $s_p \mid k$, pa važi (iii). $\square$

Primer 6.7. Ako je p prost broj koji deli red grupe G, tada važi $s_p = 1$ ako i samo ako postoji jedinstvena p-podgrupa Silova $P \leq G$. Štavše, 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* koje ćemo izučavati u Dodatku E.

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 sledeća dva tvrđenja.

Propozicija 6.8. *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 Odeljku 6.6). 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. $\square$

Sličnim metodama se može pokazati da ne postoje proste grupe reda 40, 56, 70, ... Zapravo, najmanja nekomutativna prosta grupa ima red 60, i jedan primer je $\mathbb{A}_5$. Za kraj ovog odeljka dokazujemo da drugih prostih grupa reda 60 nema.

Propozicija 6.9. $\mathbb{A}_5$ *je (do na izomorfizam) jedina prosta grupa reda 60.* $\mathbb{A}_5$ je jedina prosta grupa reda 60

Dokaz. Neka je G prosta grupa reda 60. Pošto je $60 = 2^2 \cdot 3 \cdot 5$, to G ima p-podgrupe Silova za $p = 2, 3, 5$. Odmah imamo da je $s_p \neq 1$, jer bi u suprotnom odgovarajuća p-podgrupa Silova bila normalna, što je u suprotnosti sa pretpostavkom da je G prosta.

Najpre, iz Druge teoreme Silova je $s_5 \equiv 1 (\mathrm{mod}\ 5)$ i $s_5 \mid 12$, pa mora biti $s_5 = 6$. Kako su sada 5-podgrupe Silova ciklične, one po parovima imaju trivijalan presek, što znači da imamo ukupno 24 elementa reda 5.

Dalje, imamo $s_3 \equiv 1 (\mathrm{mod}\ 3)$ i $s_3 \mid 20$, što znači da je $s_3 \in \{4, 10\}$. Ako bi bilo $s_3 = 4$, tada bi za neku 3-podgrupu Silova P od G važilo $(G : N(P)) = 4$, tj. G bi imala podgrupu indeksa 4. No, tada bi po Posledici 5.14 bilo $|G| \leq 4! = 24$, kontradikcija. Dakle, $s_3 = 10$, pa ponovo zbog cikličnosti 3-podgrupa Silova dobijamo da G ima tačno 20 elemenata reda 3.

Naš cilj je sada da pokažemo da G ima podgrupu H indeksa 5 (tj. reda 12). Objasnićemo najpre zašto to okončava dokaz propozicije. Naime, po Propoziciji 5.13, G je tada izomofna grupi permutacija (5-elementnog) skupa koseta $\{Ha : \ a \in G\}$. Drugim rečima, postoji potapanje $\phi : G \to \mathbb{S}_5$, te je stoga $G\phi$ podgrupa od $\mathbb{S}_5$ (indeksa 2). Primetimo da je element grupe $\mathbb{S}_5$ reda 3 ako i samo ako je u pitanju 3-ciklus, kojih ima $2 \cdot \binom{5}{3} = 20$. Međutim, već smo ustanovili da G sadrži 20 elemenata reda 3, pa isto važi i za $G\phi$. Zbog toga, $G\phi$ sadrži sve 3-cikluse, pa kako oni generišu $\mathbb{A}_5$, sledi da je $\mathbb{A}_5 \leq G\phi$. No, $|\mathbb{A}_5| = 60 = |G| = |G\phi|$, pa tada mora biti $G\phi = \mathbb{A}_5$, tj. $G \cong \mathbb{A}_5$.

Posmatrajmo sada s_2 – broj 2-podgrupa Silova od G. Ovo je neparan broj veći od 1 koji deli 15. $s_2 = 3$ je nemoguće ponovo zbog Posledice 5.14, pa je zato $s_2 \in \{5, 15\}$. Ako je $s_2 = 5$, dokaz je završen, jer je tada po Drugoj teoremi Silova normalizator $N(P)$ bilo koje 2-podgrupe Silova $P \leq G$ podgrupa indeksa 5. Prema tome, preostaje da se razmotri slučaj $s_2 = 15$.

Primetimo najpre da su 2-podgrupe Silova od G reda 4. Ako bi one sve imale po parovima trivijalan presek, tada bi grupa G imala tačno 45 elemenata reda 2 i 4, pa bi ukupno imala bar $1 + 24 + 20 + 45 = 90$ elemenata. Dakle, postoje 2-podgrupe Silova P, Q od G koje imaju netrivijalan presek $D = P \cap Q$ (reda 2). Sada je $D \trianglelefteq P$ i $D \trianglelefteq Q$, tj. $P \leq N(D)$ i $Q \leq N(D)$, odakle je

$$K = \langle P \cup Q \rangle \leq N(D).$$

Drugim rečima $D \trianglelefteq K$. Kako je G prosta grupa, to je $D \ntrianglelefteq G$, pa je zato $K \neq G$. Red $|K| > 4$ je deljiv sa 4, a deli 60 i pri tome je različit od 60; znači, $|K| \in \{12, 20\}$. No, slučaj $|K| = 20$ odmah otpada jer smo već konstatovali da G nema podgrupu indeksa 3; zato je $|K| = 12$, tj. $(G : K) = 5$, što se i tražilo. $\square$

6.2 Konačne Abelove grupe

U ovom odeljku dajemo precizan strukturni opis konačnih Abelovih grupa: pokazaćemo da su one iscrpljene direktnim proizvodima cikličnih grupa.

Naredno tvrđenje zapravo redukuje naš problem na opisivanje konačnih Abelovih p-grupa.

Lema 6.10. *Neka je G konačna grupa koja ima jedinstvenu p-podgrupu Silova ($s_p = 1$) za svaki prost broj p koji deli red $|G|$. Tada je G direktan proizvod svojih podgrupa Silova.*

grupe sa jedinstvenim podgrupama Silova

Dokaz. Neka je $p_1, \dots, p_m$ lista svih prostih faktora od $|G|$ i neka je P_i (jedinstvena i stoga normalna) p_i-podgrupa Silova od G, $1 \le i \le m$. Tvrdimo da je G unutrašnji direktan proizvod podgrupa $P_1, \dots, P_m \trianglelefteq G$, odakle sledi da je $G \cong P_1 \times \dots \times P_m$.

Najpre, tvrdimo da je $G = P_1 \dots P_m$. Zaista, neka je $g \in G$ i $o(g) = p_1^{\alpha_1} \dots p_m^{\alpha_m}$. Definišimo (za $1 \le i \le m$) $r_i = o(g)/p_i^{\alpha_i}$ i $g_i = g^{r_i}$; tada je $o(g_i) = p_i^{\alpha_i}$, pa teoreme Silova povlače da je $g_i \in P_i$. Kako je $(r_1, \dots, r_m) = 1$, sledi da postoje $\mu_i \in \mathbb{Z}$ tako da je

$$\mu_1 r_1 + \dots + \mu_m r_m = 1.$$

Zbog toga je

$$g = g_1^{\mu_1} \dots g_m^{\mu_m} \in P_1 \dots P_m.$$

Preostaje da se pokaže da je $P_i \cap Q_i = E$ za svako $1 \le i \le m$, gde je $Q_i = P_1 \dots P_{i-1} P_{i+1} \dots P_m$. Najpre primetimo: ako je $j \ne k$, tada je $[P_j, P_k] = E$. Zaista, svaki komutator $[a, b]$, $a \in P_j$, $b \in P_k$, pripada $P_j \cap P_k = E$, pošto je

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

i $P_j \trianglelefteq G$, $P_k \trianglelefteq G$. Drugim rečima, $[a, b] = 1$, tj. elementi iz različitih podgrupa Silova komutiraju. Prema tome, kako svaki element $a \in Q_i$ može da se predstavi kao

$$a = a_1 \dots a_{i-1} a_{i+1} \dots a_m$$

za neke $a_j \in P_j$, $j \ne i$, sledi da za proizvoljno prirodno ℓ važi

$$a^\ell = (a_1 \dots a_{i-1} a_{i+1} \dots a_m)^\ell = a_1^\ell \dots a_{i-1}^\ell a_{i+1}^\ell \dots a_m^\ell.$$

Zato je red elementa a jednak najmanjem zajedničkom sadržaocu redova elemenata $a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_m$ i stoga $p_i \nmid o(a)$. Tako, odmah sledi željeni zaključak $P_i \cap Q_i = E$. $\square$

Posledica 6.11. *Svaka konačna Abelova grupa je direktan proizvod svojih podgrupa Silova.*

Posledica 6.12. *Ako su $(m,n)=1$, tada je $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$.*

razlaganje Abelovih p-grupa

Lema 6.13. *Neka je p prost broj i A konačna Abelova p-grupa; neka je, dalje, $a \in A$ njen element maksimalnog reda, $o(a) = p^k$. Tada je ciklična grupa $\langle a \rangle \cong \mathbb{Z}_{p^k}$ direktan faktor grupe A, tj. postoji $B \leq A$ tako da je $A = \langle a \rangle \times B$.*

Dokaz. Posmatrajmo sledeću familiju podgrupa od A:

$$\mathcal{F} = \{H \leq A : \langle a \rangle \cap H = E\}.$$

Naravno, ova familija je neprazna (jer je $E \in \mathcal{F}$) i konačna, pa ima maksimalni element B. Tada je $A^* = \langle \{a\} \cup B \rangle$ podgrupa od A koja je (unutrašnji) direktan proizvod od $\langle a \rangle$ i B. Dokazaćemo da je $A^* = A$, čime će i lema biti dokazana.

Pretpostavimo suprotno: postoji $x \in A \setminus A^*$. Posmatrajmo tada niz elemenata:

$$x, x^p, x^{p^2}, \ldots, x^{p^m} = 1$$

(za neko $m \geq 1$, pri čemu mora biti $m \leq k$ po uslovu maksimalnosti reda elementa a). Kako $x \notin A^*$, a, naravno, $1 \in A^*$, zaključujemo da postoji element $y \in A$ (iz navedenog niza) tako da $y \notin A^*$ i $y^p \in A^*$. Sada postoji $\ell \in \mathbb{N}$ tako da je $y^p = a^\ell b$ za neko $b \in B$, pa sledi:

$$1 = y^{p^m} = a^{\ell p^{m-1}} b^{p^{m-1}}.$$

Budući da je $\langle a \rangle \cap B = E$, ovo je moguće samo ako je

$$a^{\ell p^{m-1}} = b^{p^{m-1}} = 1,$$

odakle $p^k \mid \ell p^{m-1}$, tj. $p \mid \ell$. Ako pišemo $\ell = np$, dobijamo da je

$$b = y^p a^{-\ell} = (ya^{-n})^p \in B \leq A^*.$$

Obeležimo sada $z = ya^{-n}$. Ovaj element ne može pripadati A^* (pa tako ni B), jer bi u suprotnom $y = za^n \in A^*$, što je suprotno našoj pretpostavci. Stoga je $B \lneq \langle \{z\} \cup B \rangle = B_1$. Po uslovu maksimalnosti za B u familiji $\mathcal{F}$, $\langle a \rangle \cap B_1 \neq E$, pa $1 \neq a^r \in B_1$ za neko $r \in \mathbb{N}$ i pri tome je $a^r = b' z^s$ za neko $s \in \mathbb{N}$ i $b' \in B$. Kako je $z^p \in B$ i $\langle a \rangle \cap B = E$, možemo pretpostaviti da je pri tome $0 < s < p$. Zbog toga je $(s,p) = 1$, pa postoje $u, v \in \mathbb{Z}$ tako da je $us + vp = 1$. Sada je

$$z = z^{us+vp} = (z^s)^u (z^p)^v = (a^r b'^{-1})^u (z^p)^v \in A^*,$$

kontradikcija. Zaključujemo da mora biti $A^* = A$. □

Posledica 6.14. *Svaka konačna Abelova p-grupa G je direktan proizvod cikličnih p-grupa: postoje $r, k_1, \dots, k_r \geq 1$ tako da je*

$$G \cong \mathbb{Z}_{p^{k_1}} \times \cdots \times \mathbb{Z}_{p^{k_r}}.$$

Preostaje da se uverimo u jedinstvenost direktnog razlaganja opisanog u prethodnoj posledici.

Lema 6.15. *Neka su $k_1 \geq \cdots \geq k_r \geq 1$ i $\ell_1 \geq \cdots \geq \ell_s \geq 1$ dva nerastuća niza takva da je* jedinstvenost razlaganja Abelovih p-grupa

$$\mathbb{Z}_{p^{k_1}} \times \cdots \times \mathbb{Z}_{p^{k_r}} \cong \mathbb{Z}_{p^{\ell_1}} \times \cdots \times \mathbb{Z}_{p^{\ell_s}}.$$

Tada je $r = s$ i za sve $1 \leq i \leq r$ važi $k_i = \ell_i$.

Dokaz. Neka su sa A i B označeni direktni proizvodi redom sa leve, odnosno desne strane. Posmatrajmo skupove $A_1 = \{a \in A : \ a^p = 1\}$ i $B_1 = \{b \in B : b^p = 1\}$. Kako bi bilo $a \in A_1$, mora biti $a = (a_1, \dots, a_r)$ pri čemu je svaki a_i ili jedinični element, ili element reda p u grupi $\mathbb{Z}_{p^{k_i}}$. Dakle, $a_i = tp^{k_i-1}$ za neko $0 \leq t \leq p-1$, pa postoji p izbora za ostatak a_i; zbog toga je $|A_1| = p^r$. Slično, $|B_1| = p^s$, pa iz datog izomorfizma sledi da je $r = s$. Sada tvrđenje dokazujemo indukcijom po r; ono je jasno ako je $r = 1$.

Primetimo da svaka ciklična grupa $\mathbb{Z}_{p^n}$ ima, za $m \leq n$, tačno p^m elemenata x sa osobinom $o(x) \leq p^m$: to su tačno ostaci oblika qp^{n-m} za proizvoljno $0 \leq q \leq p^m - 1$. S druge strane, ako je $n < m$, takvih elemenata u $\mathbb{Z}_{p^n}$ ima p^n (tj. svi imaju osobinu $o(x) \leq p^m$).

Zbog toga, pretpostavimo da je $k_r > \ell_r$ i prebrojmo elemente u A i B reda ne većeg od p^{k_r}. U A je to p^{rk_r}, dok je u B taj broj jednak

$$p^{tk_r + \ell_{t+1} + \cdots + \ell_r},$$

gde je t najveći prirodan broj sa osobinom da je $\ell_t \geq k_r$ (po našoj pretpostavci je $t < r$). Sada je $\ell_{t+1} + \cdots + \ell_r < (r-t)k_r$, pa je

$$tk_r + \ell_{t+1} + \cdots + \ell_r < rk_r,$$

što je kontradikcija sa izomorfizmom $A \cong B$. Iz analognih razloga ne može biti $k_r < \ell_r$, pa je $k_r = \ell_r$. No, sada Abelove grupe A, B imaju (normalne) podgrupe A^*, B^*, respektivno, izomorfne sa $\mathbb{Z}_{p^{k_r}}$, pri čemu je

$$\mathbb{Z}_{p^{k_1}} \times \cdots \times \mathbb{Z}_{p^{k_{r-1}}} \cong A/A^* \cong B/B^* \cong \mathbb{Z}_{p^{\ell_1}} \times \cdots \times \mathbb{Z}_{p^{\ell_{r-1}}}.$$

Po induktivnoj pretpostavci sledi da je $k_i = \ell_i$ za sve $1 \leq i \leq r-1$. $\square$

Posledica 6.16. *Broj Abelovih p-grupa kardinalnosti p^m jednak je $p(m)$ – broju particija prirodnog broja m (tj. broju konačnih nizova $k_1 \geq \cdots \geq k_r \geq 1$ takvih da je $k_1 + \cdots + k_r = m$). Dakle, ako je $n = p_1^{\alpha_1} \dots p_s^{\alpha_s}$ faktorizacija broja n na njegove proste faktore, $\alpha_i \geq 1$ za sve $1 \leq i \leq s$, tada je ukupan broj neizomorfnih Abelovih grupa reda n jednak $\prod_{i=1}^{s} p(\alpha_i)$.*

Prethodna tvrđenja u ovom odeljku kumulativno daju sledeći rezultat.

fundamentalna teorema o konačnim Abelovim grupama

Teorema 6.17 (Fundamentalna teorema o konačnim Abelovim grupama)**.** *Neka je G Abelova grupa konačnog reda n. Tada je*

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

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.

Na kraju, napomenimo da gornja teorema ima svoje uopštenje za proizvoljne konačno generisane Abelove grupe.

Teorema 6.18 (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.

6.3 Grupe reda p^2 i neke grupe reda pq

U narednim odeljcima ove glave 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).

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 6.19. *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 6.20. *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 3.10 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. $\square$

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

Propozicija 6.21. *Neka su $p < q$ prosti brojevi. Ako $p \nmid q-1$ tada je $\mathbb{Z}_{pq}$ (do na izomorfizam) jedina grupa reda pq.* opis grupa reda pq kada $p \nmid q-1$

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 $s_p = 1$. Po Lemi 6.10 je $G \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$. $\square$

Specijalno, jedina grupa reda 15 je ciklična grupa $\mathbb{Z}_{15}$. Kao što ćemo videti u Dodatku D, ukoliko $p \mid q-1$, tada postoji tačno jedna nekomutativna grupa reda pq koja nastaje kao poludirektan proizvod $\mathbb{Z}_p$ i $\mathbb{Z}_q$. U slučaju $p = 2$ taj poludirektan proizvod je baš dijedarska grupa D_p, što ćemo odmah videti u narednom odeljku.

6.4 Grupe reda $2p$

Propozicija 6.22. *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 $G \cong D_p$. $\square$

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

6.5 Grupe reda 8

opis grupa reda 8

Propozicija 6.23. *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).*

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 $ab = (ba)^2 ab = ba(ba^2b) = ba \cdot b^2 = ba$, 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 $k \le 3$. 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. $\square$

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 grupe reda p^3

$$a \mapsto (p+1)a$$

(ovo je automorfizam od $\mathbb{Z}_{p^2}$ reda p jer je $(p+1, p^2) = 1$ i $(p+1)^p \equiv 1 \pmod{p^2}$). 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).

6.6 Grupe reda 12

Propozicija 6.24. *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 ($D_6$, $\mathbb{A}_4$ i poludirektan proizvod $\mathbb{Z}_4 \ltimes_\phi \mathbb{Z}_3$ definisan homomorfizmom $\phi : \mathbb{Z}_4 \to \mathrm{Aut}(\mathbb{Z}_3)$ kojim generator grupe $\mathbb{Z}_4$ deluje invertovanjem na $\mathbb{Z}_3$).* opis grupa reda 12

Dokaz. Primetimo da smo analizu grupa reda 12 već započeli u Propoziciji 6.8: 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 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, poludirektni proizvod iz formulacije ima ova svojstva, pa zaključujemo da je $G \cong \mathbb{Z}_4 \ltimes_\phi \mathbb{Z}_3$ (primetimo da postoji samo jedan nekomutativni poludirektni proizvod grupa $\mathbb{Z}_4$ i $\mathbb{Z}_3$, budući da je $\mathrm{Aut}(\mathbb{Z}_3) \cong \mathbb{Z}_2$).

Neka je sada $H \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. 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 $G \cong D_6$. $\square$

7

Kompozicioni nizovi i rešive grupe

7.1 Kompozicioni nizovi i teorema Žordan-Heldera

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

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

normalni niz i njegovi faktori

se naziva *normalni niz* grupe G (dužine n). Pri tome, notacija $H_{i+1} \triangleleft H_i$ 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.

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 $G = H_0 \triangleright H_1 \triangleright \ldots \triangleright H_{n-1} \triangleright H_n = E$ zovemo *kompozicioni niz* grupe G.

kompozicioni niz

Propozicija 7.1. *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 7.2. Niz

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

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 7.3. 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

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

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

ekvivalencija normalnih nizova

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

Teorema 7.4 (Teorema Žordan-Heldera)**.** *Svaka dva kompoziciona niza grupe G su ekvivalentna.*

teorema Žordan-Heldera

Ovde ćemo dati dva dokaza ove teoreme. Prvi od njih najpre uspostavlja vezu između kompozicionih nizova grupe i njene normalne podgrupe, nakon čega sledi glavni dokaz indukcijom po dužini najkraćeg kompozicionog niza grupe G. Drugi dokaz se oslanja na Šrajerovu[9] teoremu o profinjenju normalnih nizova koju ovde dokazujemo pomoću već dokazane Leme Casenhausa. Za prvi dokaz nam je potrebno sledeće pomoćno tvrđenje.

Lema 7.5. *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.*

lema o kompozicionim nizovima podgrupa

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

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

Dokaz. Fiksirajmo jedan kompozicioni niz grupe G:

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

Uočimo tada sledeći lanac podgrupa od H:

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

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 Teoremi o korespondenciji i 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. □

prvi dokaz teoreme Žordan-Heldera

Prvi dokaz Teoreme 7.4. Teoremu dokazujemo indukcijom po dužini najkraćeg kompozicionog niza grupe G. Ako G ima kompozicioni niz dužine 1, tada je G prosta i $G \rhd E$ 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).

Neka su sada

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

i

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

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. $\square$

drugi (Šrajerov) dokaz teoreme Žordan-Heldera

Drugi dokaz Teoreme 7.4. 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 $1 \leq i < n$ postoji $1 \leq j < m$ tako da je $H_i = K_j$; drugim rečima, prvi niz se dobija od drugog umetanjem dodatnih podgrupa. Sada Žordan-Helderovu teoremu izvodimo kao direktnu posledicu *Šrajerove teoreme o profinjenju* koja 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 $1 \leq i \leq k$ i $0 \leq j \leq l$ definišimo

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

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 3.30) 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 sami biti ekvivalentni. □

Primer 7.6. 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,

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

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.

7.2 Rešive grupe

rešive grupe

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

Primer 7.7. 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 $\mathbb{A}_4$ 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.

$\mathbb{S}_n$ nije rešiva za sve $n \geq 5$

Propozicija 7.8. *Grupa $\mathbb{S}_n$ 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. Zapravo, može se pokazati da je ovo 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. $\square$

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.

Propozicija 7.9. *Grupa G je rešiva ako i samo ako postoji $n \geq 0$ tako da je $G^{(n)} = E$.*

kriterijum rešivosti preko izvodnih podgrupa

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 3.32 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. $\square$

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 7.10. *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 $[g,h]\phi = [g\phi, h\phi]$, sledi da je $(G\phi)' = G'\phi$. 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. $\square$

Važi i tvrđenje (u izvesnom smislu) obratno prethodnom.

Propozicija 7.11. *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.

kompozicioni faktori rešivih grupa

Propozicija 7.12. *Netrivijalna konačna grupa je rešiva ako i samo ako su joj svi kompozicioni faktori ciklične grupe prostog reda.*

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 $G \triangleright H_1 \triangleright H_2 \triangleright \dots \triangleright H_n = E$ njen normalni niz u kome su svi faktori Abelovi. Po Šrajerovoj teoremi o profinjenju, ovaj niz se može profiniti do kompozicionog:

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

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

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. □

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

Lema 7.13. *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 3.10, 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. □

Propozicija 7.14. *Svaka konačna p-grupa je rešiva.*

rešivost konačnih p-grupa

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. □

Neka je G konačna grupa. Za podgrupu $H \leq G$ kažemo da je *Holova*[10] *podgrupa* ako su njen red $|H|$ i indeks $(G : H)$ uzajamno prosti brojevi. Primetimo da su podgrupe Silova zapravo specijalni slučajevi Holovih podgrupa: red p-podgrupe Silova $P \leq G$ jednak je najvišem stepenu kojim p deli $|G|$, iz čega odmah sledi da $p \nmid (G : P)$ i stoga su $|P|$ i $(G : P)$ uzajamno prosti. Ako je sada Π neki skup prostih brojeva, podgrupa $H \leq G$ sa osobinom da su svi prosti faktori njenog reda $|H|$ sadržani u Π, dok njen indeks $(G : H)$ nije deljiv nijednim od elemenata Π, naziva se *Holova* Π*-podgrupa* od G.

Hol [Hall28] je dokazao da za *rešive* grupe važi sledeće uopštenje teorema Silova (koje navodimo bez dokaza).

Teorema 7.15 (F. Hol, 1928)**.** *Neka je G konačna rešiva grupa, a Π proizvoljan skup prostih brojeva.*

Holova teorema

(i) G ima Holovu Π-podgrupu.

(ii) Svaka podgrupa od G sa osobinom da su svi prosti faktori njenog reda sadržani u Π, sadržana je u nekoj Holovoj Π-podgrupi od G.

(iii) Svake dve Holove Π-podgrupe od G su konjugovane.

Pretpostavka rešivosti je ovde esencijalna: na primer, (nerešiva) alternativna grupa $\mathbb{A}_5$ nema podgrupe reda 15 ili 20, iako bi (hipotetički) indeksi tih polugrupa bili 4, odnosno 3, dakle uzajamno prosti sa 15 i 20, respektivno. Tako, $\mathbb{A}_5$

[10] Filip Hol (Philip Hall, 1904–1982), britanski matematičar

nema ni $\{2,5\}$-, ni $\{3,5\}$-podgrupe Hola. Štaviše, postoji prosta grupa reda 168 u kojoj postoje dve Holove $\{2,3\}$-podgrupe (reda 24) koje nisu konjugovane, a postoji i prosta grupa reda 660 u kojoj dve Holove $\{2,3\}$-podgrupe (reda 12) čak nisu ni izomorfne.

Od čuvenih dovoljnih uslova za rešivost konačne grupe, tu je *Bernsajdova pq-teorema* [Bu04].

rešivost grupa reda $p^n q^m$

Teorema 7.16 (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. Kao što znamo, minimalan primer je $\mathbb{A}_5$ reda $60 = 2^2 \cdot 3 \cdot 5$. Znatno kasnije, dokazano je da jedan od tih prostih faktora mora biti 2.

teorema Fajt-Tompsona

Teorema 7.17 (Fajt[11], Tompson[12], 1962/63)**.** *Svaka neabelova konačna prosta grupa je parnog reda. Posledično, svaka grupa neparnog reda je rešiva.*

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.

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

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

A

Slobodne grupe

Neka je $X \neq \varnothing$ *alfabet*; njegove elemente $x \in X$ zovemo *slova*. Datom alfabetu X pridružujemo njegovu bijektivnu kopiju $X^{-1} = \{x^{-1} : x \in X\}$ (napominjemo da ovde oznaka $^{-1}$ za sada ne upućuje ni na kakav inverz u nekoj grupi, radi se samo o notaciji, zgodnom zapisu koji ćemo kasnije dovesti u vezu sa inverzima). Pri tome, operator $^{-1}$ deluje na novi "duplirani" alfabet $X^{\pm 1} = X \cup X^{-1}$ na prirodan način: njegovo dejstvo je očito na slovima iz X, dok za $x^{-1} \in X^{-1}$ definišemo da je $(x^{-1})^{-1} = x$.

Posmatrajmo sada skup svih reči $(X^{\pm 1})^*$ nad alfabetom $X^{\pm 1}$: radi se o skupu svih konačnih nizova $(x_1^{\varepsilon_1}, \ldots, x_n^{\varepsilon_n})$ (gde je $\varepsilon_i \in \{1, -1\}$ za sve $1 \leq i \leq n$) koji uključuje i *praznu reč* $()$. Ipak, mi ćemo se ovde držati tradicionalnije notacije prema kojoj reči pišemo bez zagrada i zareza: $x_1^{\varepsilon_1} \ldots x_n^{\varepsilon_n}$, dok ćemo praznu reč (iz razloga koji će uskoro postati jasniji) označavati sa 1.

Za reč $w \in (X^{\pm 1})^*$ kažemo da je *redukovana* ako ne sadrži podreč oblika aa^{-1} za neko $a \in X^{\pm 1}$: nijedno slovo u w nije susedno sa svojim "inverznim" slovom. redukovane reči

U vezi sa tim, na skupu svih reči $(X^{\pm 1})^*$ uvodimo relaciju $\sim$ na sledeći način. *Elementarnom transformacijom* na reči w zovemo brisanje neke podreči oblika aa^{-1}, $a \in X^{\pm 1}$ (ako takva podreč postoji), ili umetanje podreči tog oblika na bilo kom mestu u reči w. Sada za dve reči $w_1, w_2 \in (X^{\pm 1})^*$ pišemo $w_1 \sim w_2$ ako postoji niz elementarnih transformacija koje reč w_1 prevode u w_2 (uključujući i slučaj kada je $w_1 = w_2$, kada je taj niz dužine 0). Lako se vidi da je $\sim$ relacija ekvivalencije na $(X^{\pm 1})^*$. elementarna transformacija

Pored toga, lako se uočava da za svaku reč w postoji bar jedna redukovana reč w' tako da je $w \sim w'$. Naime, ukoliko w nije već redukovana, ona sadrži podreč oblika aa^{-1}, $a \in X^{\pm 1}$, pa se opredelimo za bilo koju od takvih podreči i obrišimo je; sa dobijenom reči ponavljamo postupak, koji mora biti konačan zato što se u svakom koraku dobija kraća reč od prethodne. Krajnji rezultat ovog postupka, naravno, mora biti redukovana reč ekvivalentna početnoj. No, primetimo da u tom postupku postoji veliki stepen priozvoljnosti (u izboru “inverznih” susednih parova slova koje ćemo brisati) – zbog toga bi, teoretski, moglo da postoji više različitih redukovanih reči koje se dobijaju kao rezultat takvog postupka. Da to ipak nije slučaj (te da je zbog toga izbor parova slova koje se brišu u pojedinim koracima postupka nebitan sa stanovišta krajnjeg rezultata) pokazuje naredno tvrđenje.

jedinsvenost redukcije reči

Lema A.1. *Za svaku reč $w \in (X^{\pm 1})^*$ postoji jedinstvena redukovana reč w_0 tako da je $w \sim w_0$.*

Dokaz. Egzistencija je već malopre obrazložena, pa preostaje da se pokaže jedinstvenost. Za to je dovoljno da se dokaže sledeće tvrđenje: ako su $u, v \in (X^{\pm 1})^*$ redukovane reči takve da je $u \sim v$, tada je $u = v$.

Pretpostavimo suprotno. Kako je $u \sim v$, postoji niz reči

$$u = w_1, w_2, \dots, w_{m-1}, w_m = v$$

u kojem se svaka od reči dobija iz prethodne primenom neke elementarne transformacije. Od svih ovakvih nizova, uočimo onaj kod koga je zbir

$$N = \sum_{i=1}^{m} |w_i|$$

minimalan (gde $|w|$ označava dužinu reči w). Po pretpostavci, $u \neq v$, pa je $m \geq 2$, a kako su reči u, v redukovane, mora biti $|w_1| < |w_2|$ i $|w_{m-1}| > |w_m|$ (jer w_2 možemo dobiti samo umetanjem nekog inverznog para u u, a v samo brisanjem nekog inverznog para u w_{m-1}). Sledi da mora da postoji indeks i za koji važi $|w_{i-1}| < |w_i| > |w_{i+1}|$. Tada se obe reči w_{i-1}, w_{i+1} dobijaju iz w_i brisanjem nekog inverznog para susednih slova; recimo, neka se w_{i-1} dobija iz w_i brisanjem određenog pojavljivanja podreči aa^{-1} ($a \in X^{\pm 1}$), a w_{i+1} iz w_i brisanjem određenog pojavljivanja podreči bb^{-1} ($b \in X^{\pm 1}$). Ako se ova dva pojavljivanja poklapaju, tada je $w_{i-1} = w_{i+1}$, što je u suprotnosti sa minimalnošću N (jer je tada $u = w_1, w_2, \dots, w_{i-1}, w_{i+2}, \dots, w_{m-1}, w_m = v$ takođe niz elementarnih transformacija koji prevodi u u v). Slično, ako se ova dva pojavljivanja ne poklapaju, ali se preklapaju, tada je $b = a^{-1}$, pa w_i sadrži jednu od podreči $aa^{-1}a$, odnosno $a^{-1}aa^{-1}$, i pri tome se i w_{i-1} i w_{i+1} dobijaju iz w_i zamenom uočene podreči sa a, odnosno a^{-1}, respektivno. Opet zaključujemo $w_{i-1} = w_{i+1}$, što je ponovo nemoguće zbog minimalnosti N. Prema tome, preostaje slučaj kada su posmatrana pojavljivanja podreči aa^{-1} i bb^{-1} disjunktna. Međutim, tada uočimo reč w' koja se dobija iz w_i brisanjem *obe* ove podreči. Sada je

$$u = w_1, w_2, \ldots, w_{i-1}, w', w_{i+1}, \ldots w_{m-1}, w_m = v$$

takođe niz elementarnih transformacija koje prevode u u v, ali je ukupan zbir dužina reči koje učestvuju u ovom nizu jednak $N' = N-4$. Ovo je kontradikcija sa izborom N, što povlači da mora biti $u = v$. □

Zbog prethodne leme, za svaku reč $w \in (X^{\pm 1})^*$ možemo definisati *redukciju* $\mathrm{red}(w)$ reči w kao jedinsvenu redukovanu reč sa osobinom da je $w \sim \mathrm{red}(w)$. Redukcija date reči se efektivno dobija primenom postupka opisanog pre prethodne leme, pri čemu sada znamo da izbor inverznih parova slova koje brišemo i redosled koraka nije bitan.

Pojam redukcije reči nam sada omogućava da na skupu $R(X)$ svih redukovanih reči nad $X^{\pm 1}$ definišemo strukturu grupe. Naime, za $u, v \in R(X)$ definišemo njihov proizvod sa

$$u \cdot v = \mathrm{red}(uv),$$

gde uv sa desne strane predstavlja konkatenaciju (dopisivanje) reči u i v. Lako se pokazuje da je ovom operacijom zaista definisana grupa, koju označavamo sa F_X i zovemo *grupa redukovanih reči nad* X (pri tome slova iz X zapravo identifikujemo sa odgovarajućim rečima dužine 1). Nije teško videti da je prazna reč 1 jedinica ove grupe, a da je inverz elementa $w = x_1^{\varepsilon_1} \ldots x_n^{\varepsilon_n}$ jednak

grupa redukovanih reči

$$w^{-1} = x_n^{-\varepsilon_n} \ldots x_1^{-\varepsilon_1}.$$

Specijalno, sada je x^{-1} zaista inverz (jednoslovne reči) x, jer je očito

$$\mathrm{red}(xx^{-1}) = \mathrm{red}(x^{-1}x) = 1.$$

Ključna osobina grupa redukovanih reči nad datim alfabetom jeste da su one zapravo (do na izomorfizam jedinstvene) slobodne grupe. Naime, za grupu F kažemo da je *slobodna grupa sa bazom* $X \subseteq F$ ako za svaku grupu G i svako

slobodne grupe

preslikavanje $\phi : X \to G$ postoji jedinstveno proširenje ϕ do homomorfizma $\overline{\phi} : F \to G$ (tako da je $\overline{\phi}|_X = \phi$).

Najpre ćemo videti da za datu kardinalnost baze, postoji do na izomorfizam najviše jedna slobodna grupa, a zatim da su grupe F_X upravo slobodne grupe sa bazom X.

jedinsvenost slobodne grupe sa datom bazom

Propozicija A.2. *Neka su F_1 i F_2 slobodne grupe redom sa bazama X_1 i X_2. Ako je $|X_1| = |X_2|$ tada je $F_1 \cong F_2$.*

Dokaz. Neka je $\phi_1 : X_1 \to X_2$ proizvoljna bijekcija i $\phi_2 = f_1^{-1}$ (zapravo, možemo formalno pretpostaviti da su kodomeni za ϕ_1, odnosno ϕ_2 već F_2, odnosno F_1, respektivno). Tada se ove dve funkcije mogu proširiti do homomorfizama $\overline{\phi_1} : F_1 \to F_2$ i $\overline{\phi_2} : F_2 \to F_1$. Sada su $\overline{\phi_1}\,\overline{\phi_2}$ odnosno $\overline{\phi_2}\,\overline{\phi_1}$ redom endomorfizmi grupa F_1 i F_2 koji proširuju identička preslikavanja na X_1, odnosno X_2, respektivno. Međutim, i identički endomorfizmi id_{F_1} i id_{F_2} imaju ista svojstva, pa je po uslovu jedinstvenosti $\overline{\phi_1}\,\overline{\phi_2} = \mathrm{id}_{F_1}$ i $\overline{\phi_2}\,\overline{\phi_1} = \mathrm{id}_{F_2}$. Otuda je $\overline{\phi_1}$ izomorfizam (i $\overline{\phi_2} = \overline{\phi_1}^{-1}$). □

grupa redukovnih reči je slobodna

Propozicija A.3. *Grupa F_X redukovanih reči nad X je slobodna grupa sa bazom X.*

Dokaz. Neka je G proizvoljna grupa i $\phi : X \to G$ proizvoljno preslikavanje skupa (jednoslovnih reči) X u G. Definišimo $\overline{\phi} : F_X \to G$ sa

$$(x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n})\overline{\phi} = (x_1\phi)^{\varepsilon_1} \dots (x_n\phi)^{\varepsilon_n}.$$

Primetimo da se ovo preslikvanje može na analogan način konzistentno dalje proširiti do $\phi^* : (X^{\pm 1})^* \to G$, budući da očito $w_1 \sim w_2$ povlači $w_1\phi^* = w_2\phi^*$. Zato je

$$(u \cdot v)\overline{\phi} = (\mathrm{red}(uv))\overline{\phi} = (uv)\phi^* = (u\phi^*)(v\phi^*) = (u\overline{\phi})(v\overline{\phi}),$$

za sve $u, v \in F_X$, pa je $\overline{\phi}$ homomorfizam. Iz same njegove definicije (tj. iz činjenice da X generiše F_X) je jasno da ne može biti drugih homomorfizama $F_X \to G$ koji proširuju X. □

Kardinalnost $|X|$ baze X slobodne grupe F se naziva *rang* od F. Primetimo da je slobodna grupa ranga 0 trivijalna, dok je slobodna grupa ranga 1 izomorfna sa $\mathbb{Z}$.

Centralni značaj slobodnih grupa (naročito za oblast *kombinatorne teorije grupa* [LSch77, MKS66]) leži u sledećem tvrđenju.

Teorema A.4. *Neka je G grupa generisana svojim podskupom A, $|A| = \kappa$. Tada je G homomorfna slika (i stoga izomorfna faktor grupi) slobodne grupe ranga κ.* svaka grupa je faktor slobodne grupe

Dokaz. Neka je X proizvoljan skup kardinalnosti κ i $\phi : X \to A$ bijekcija. Tada postoji jedinstveni homomorfizam $\overline{\phi} : F_X \to G$ koji proširuje ϕ. Kako slika $X\overline{\phi} = A$ generatornog skupa X od F_X generiše G, sledi da je $\operatorname{Im}\overline{\phi} = G$. Po Teoremi o homomofizmu sledi da je $F_X/N \cong G$, gde je $N = \operatorname{Ker}\overline{\phi}$. □

Ukoliko je normalna podgrupa N iz prethodnog dokaza generisana *kao normalna podgrupa* skupom reči R (što znači da je N najmanja normalna podgrupa od F_X koja sadrži R) tada kažemo da je grupa $G \cong F_X/N$ *prezentirana* parom (X, R) (u odnosu na $\phi : X \to A$, bijekcijom koja identifikuje slova alfabeta X sa stvarnim generatorima grupe G). Teorija prezentacija grupa predstavlja jednu od najznačajnijih tema kombinatorne teorije grupa, sa ogromnim primenama u topologiji i geometriji. prezentacija grupe

Na primer, $(\{a\}, \{a^n\})$ predstavlja prezentaciju ciklične grupe $\mathbb{Z}_n$. Takođe, na osnovu informacija sadržanih u Primeru 1.10 nije teško pokazati da

$$(\{a, b\}, \{a^n, b^2, abab\})$$

predstavlja prezentaciju dijedarske grupe D_n (u odnosu na ϕ koje slovo a slika na rotaciju ρ, a slovo b na osnu simetriju σ).

B

Primitivne grupe permutacija

primitivne grupe permutacija

Neka je $G \leq \mathbb{S}_X$ grupa permutacija na skupu X. Pravi podskup $A \subsetneq X$ je *blok* grupe G ako ima bar dva elementa i ako za sve $\pi \in G$ važi $A\pi = A$ ili $A\pi \cap A = \varnothing$. Za G kažemo da je *primitivna* ako je tranzitivna i nema blok.

primitivnost i particije

Propozicija B.1. *Neka je G tranzitivna grupa permutacija na X. Tada G nije primitivna ako i samo ako postoji netrivijalna (uniformna) particija ρ skupa X (relacija ekvivalencije čije sve klase imaju istu kardinalnost) tako da je svaka permutacija iz G ujedno i permutacija skupa X/ρ (tako da je $(x\rho)\pi = (x\pi)\rho$ za sve $x \in X$).*

Dokaz. ($\Rightarrow$) Neka je A blok grupe G. Dokažimo da je tada $\{A\pi : \pi \in G\}$ čini traženu particiju. Zaista, po uslovu tranzitivnosti, $\bigcup_{\pi \in G} A\pi = X$. Gornja familija skupova čini particiju, jer $x \in A\pi \cap A\sigma$ povlači da $x\sigma^{-1} \in A \cap A\pi\sigma^{-1}$. Pošto je A blok, mora biti $A\pi\sigma^{-1} = A$, tj. $A\pi = A\sigma$. Iz definicije bloka sledi da je ova particija netrivijalna, a takođe je i uniformna, jer je $|A\pi| = |A\sigma|$ za sve $\pi, \sigma \in G$.

($\Leftarrow$) Trivijalno, pošto je svaka klasa particije ρ blok grupe G. $\square$

Posledica B.2. *Ako je A blok grupe $G \leq \mathbb{S}_X$, tada je $|X| = k|A|$ za neko $k \geq 2$. Stoga je svaka tranzitivna grupa permutacija prostog stepena primitivna.*

primitivnost i stabilizatori

Propozicija B.3. *Neka je G tranzitivna grupa permutacija na X. G je primitivna ako i samo ako su svi njeni stabilizatori maksimalne podgrupe od G.*

Dokaz. ($\Rightarrow$) Pretpostavimo da G_x nije maksimalna podgrupa od G za neko $x \in X$; drugim rečima, postoji pogrupa H takva da $G_x \lneq H \lneq G$. Definišimo

$$A = \{y \in X : x\pi = y \text{ za neko } \pi \in H\}.$$

Najpre, očito $x \in A$, ali A mora sadržati bar još jednu tačku iz X, naime $x\pi$ za proizvoljno $\pi \in H \backslash G_x$. Dakle, $|A| \geq 2$. S druge strane, ako bi bilo $A = X$ tada bi za proizvoljno $\sigma \in G \setminus H$ postojala permutacija $\pi \in H$ tako da je $x\pi = x\sigma$. No, u tom slučaju bi bilo $x\sigma\pi^{-1} = x$, tj. $\sigma\pi^{-1} \in H$, što je u kontradikciji sa $\sigma \notin H$. Sada se lako proverava da je A blok grupe G, pa ona nije primtivna.

($\Leftarrow$) Pretpostavimo da grupa G nije primitivna, i neka je $x \in X$. Budući da iz dokaza prethodne propozicije sledi da svaki element od X pripada nekom bloku od G, neka je A blok od G koji sadrži x. Definišimo

$$H = \{\pi \in G : x\pi \in A\}.$$

Jasno, H je podgrupa od G koja sadrži stabilizator G_x. Pri tome su obe inkluzije $G_x \subseteq H \subseteq G$ stroge zbog tranzitivnosti G: postoji permutacija $\sigma \in G$ tako da je $x\sigma = y \in A$ i $y \neq x$ (koja onda pripada H, ali ne i G_x), a takođe postoji i permutacija $\tau \in G$ tako da je $x\tau = z \notin A$ (koja ne pripada H). $\square$

Lema B.4. *Svaka dvostruko tranzitivna grupa (permutacija na X) je primitivna.*

dvostruko tranzitivne grupe su primitivne

Dokaz. Pretpostavimo da je grupa G dvostruko tranzitivna na X, ali da ima blok $A \subsetneq X$. Tada postoji $\pi \in G$ i dva različita elementa $a, b \in A$ tako da je $a\pi = a$ i $b\pi = c \notin A$. Sada je $A\pi \neq A$, ali i $A \cap A\pi \neq \varnothing$. Kontradikcija. $\square$

Lema B.5. *Neka je G primitivna grupa permutacija na X i $E \neq H \trianglelefteq G$. Tada je i H tranzitivna grupa na X.*

tranzitivnost normalnih podgrupa primitivnih grupa

Dokaz. Pretpostavimo suprotno, da grupa H nije tranzitivna. Tada postoji više od jedne orbite x^H, $x \in X$, i pošto je $H \neq E$, bar jedna od tih orbita ima bar dva elementa. Neka je $A = x^H$ jedna takva orbita. Dokazaćemo da je tada A blok grupe G.

Neka je $\pi \in G$ proizvoljno. Kako je $H \trianglelefteq G$, sledi da je za proizvoljno $\sigma \in H$,

$$A\pi\sigma = (A\pi\sigma\pi^{-1})\pi = A\pi,$$

budući da je $\pi\sigma\pi^{-1} \in H$ i svaki element iz H fiksira svaku orbitu dejstva H na X. Sada sledi da je $A\pi$ takođe jedna od orbita dejstva H na X (pošto je σ

fiksira). Zbog tranzitivnosti G je $\bigcup_{\pi \in G} A\pi = X$, a kako je reč o orbitama, to je $\{A\pi : \pi \in G\}$ particija skupa X (čiju svaku klasu fiksira svaki element iz H). Sada je A blok od G, kontradikcija. $\square$

Glavna primena primitivnih grupa leži u tome što nam one, pod određenim dodatnim uslovima, daju "mehanizam" da dokažemo da je neka grupa permutacija prosta. Ovaj mehanizam je poznat pod nazivom *Ivasavina*[13] *lema*.

Ivasavina lema

Teorema B.6 (Ivasava, 1941)**.** *Neka je G grupa permutacija skupa X koja zadovoljava sledeća tri uslova:*

(1) $G' = G$.

(2) G je primitivna.

(3) Postoji $x \in X$ čiji stabilizator ima normalnu Abelovu podgrupu $A \trianglelefteq G_x$ takvu da sve njene konjugovane podgrupe $\pi^{-1}A\pi$, $\pi \in G$ generišu G:

$$G = \left\langle \bigcup_{\pi \in G} \pi^{-1} A \pi \right\rangle .$$

Tada je grupa G prosta.

Dokaz. Pretpostavimo da je $E \neq H \trianglelefteq G$. Po uslovu (2) i prethodnoj lemi, H je tranzitivna na X. Tvrdimo da je $G = HG_x$. Zaista, neka je $\pi \in G$ i $y = x\pi$. Zbog tranzitivnosti H, postoji $\sigma \in H$ tako da je $y = x\sigma$; sada je $\pi\sigma^{-1} \in G_x$, odakle sledi da je $\pi \in G_x\sigma \subseteq G_xH = HG_x$. Dalje, pokazujemo da je $HA \trianglelefteq HG_x = G$. Sa tim ciljem neka je $\pi = \sigma\tau \in G$, gde je $\sigma \in G_x$ i $\tau \in H$. Važi:

$$(\sigma\tau)^{-1}HA\sigma\tau = [(\sigma\tau)^{-1}H\sigma\tau][(\sigma\tau)^{-1}A\sigma\tau] = H(\tau^{-1}A\tau),$$

jer je $H \trianglelefteq G$ i $A \trianglelefteq G_x$. Sada je zbog normalnosti H, $\tau^{-1}A\tau \subseteq HAH = HHA = HA$, pa dobijamo da je $(\sigma\tau)^{-1}HA\sigma\tau \subseteq HA$, što je dovoljno da konstatujemo da je $HA \trianglelefteq HG_x = G$.

Međutim, pošto je $A \leq HA$, sledi da HA mora da sadrži i sve konjugovane podgrupe $\pi^{-1}A\pi$ od A, $\pi \in G$, a sa time, po uslovu (3), i celo G, pa je $HA = G$. Po Prvoj teoremi o izomorfizmu dobijamo:

$$G/H = HA/H \cong A/A \cap H.$$

[13] Kenkiči Ivasava (1917–1998), japanski matematičar

Prema tome, faktor grupa G/H je izomorfna faktoru Abelove grupe A, zbog čega je i sama Abelova. No, sada po Lemi 3.32 sledi da je $G' \leq H$, pa je zbog uslova (1) $H = G$. Zaključujemo da grupa G mora biti prosta. $\square$

C

Projektivne linearne grupe

projektivna geometrija

Neka je Π skup sa bar tri elementa i $\Lambda \subseteq \mathcal{P}(\Pi)$ neka familija podskupova od Π. Par $\Gamma = (\Pi, \Lambda)$ je *projektivna geometrija* – pri čemu elemente skupa Π zovemo *tačke*, a elemente od Λ *prave* – ako važe sledeći uslovi:

(1) Svaki par različitih tačaka pripada tačno jednoj pravoj.

(2) Svaka prava sadrži bar tri tačke.

(3) Za $X \subseteq \Pi$ neka $C(X)$ označava najmanji podskup od Π koji sadrži X i koji sadrži sve tačke svih pravih sa kojima ima bar dve zajedničke tačke. Ako je $X \subseteq \Pi$ i ako su $p, q \in \Pi \setminus X$, $p \neq q$, tačke sa osobinom da je $p \in C(X \cup \{q\})$, tada postoji tačka $r \in C(X)$ tako da je $p \in C(\{q, r\})$.

dimenzija geometrije

Najmanji kardinal κ takav da postoji skup $X \subseteq \Pi$ od $\kappa + 1$ tačaka za koji je $C(X) = \Pi$ je *dimenzija* geometrije Γ.

U narednom primeru razmatramo kanonički način da se od vektorskih prostora konstruše projektivna geometrija konačne dimenzije.

projektivna geometrija vektorskog prostora

Primer C.1. Neka je $V \cong F^n$ vektorski prostor dimenzije n nad poljem F. Definišimo skup tačaka Π kao skup 1-dimenzionalnih potprostora od V, dok su prave (Λ) 2-dimenzionalni potprostori od V, pri čemu "tačka" pripada "pravoj" ako i samo ako važi inkluzija odgovarajućih potprostora od V.

Tvrdimo da je $\Gamma_{n-1}(F) = (\Pi, \Lambda)$ projektivna geometrija dimenzije $n - 1$. Zaista, ako su $U = \langle x \rangle$ i $U' = \langle y \rangle$ dva različita jednodimenzionalna potprostora od V, tada su vektori x, y linearno nezavisni, pa je $W = \langle x, y \rangle$ potprostor dimenzije 2 (dakle, "prava") koji sadrži U i U'. Dalje, neka je W dvodimenzionalni potprostor od V i neka vektori $x, y \in V$ čine njegovu bazu. Tada su potprostori $\langle x \rangle$, $\langle y \rangle$ i $\langle x + y \rangle$ različiti (na primer, $x + y \in \langle x \rangle$ bi značilo da je $x + y = \alpha x$ za neko $\alpha \in F$, pa bi bilo $(1 - \alpha)x + y = 0$, kontradikcija) i svi leže u W. Najzad, primetimo da je u ovom kontekstu $C(X)$ upravo familija svih 1-dimenzionalnih potprostora koji leže u potprostoru od V generisanom 1-dimenzionalnim potprostorima ("tačkama") iz X. Prema tome, $p \in C(X \cup \{q\})$ znači da postoje (po parovima linearno nezavisni) vektori $u, v, x_1, \dots, x_k \in V$ tako da $p = \langle u \rangle$, $q = \langle v \rangle$ i $\langle x_i \rangle \in X$ za sve $1 \le i \le k$, kao i

$$u = \alpha_1 x_1 + \cdots + \alpha_k x_k + \beta v.$$

Stoga, ako definišemo $r = \langle \alpha_1 x_1 + \cdots + \alpha_k x_k \rangle$, imamo da $u \in \langle \alpha_1 x_1 + \cdots + \alpha_k x_k, v \rangle$, tj. $p \in C(\{q, r\})$, kao što je i traženo.

Za par preslikavanja $\phi = (\phi^{(1)}, \phi^{(2)})$ kažemo da je *automorfizam* projektivne geometrije $\Gamma = (\Pi, \Lambda)$ ako je $\phi^{(1)}$ permutacija od Π i $\phi^{(2)}$ permutacija od Λ tako da za sve $p \in \Pi$, $\ell \in \Lambda$ važi $p \in \ell$ ako i samo ako $\phi^{(1)}(p) \in \phi^{(2)}(\ell)$ (podsetimo se da po ranijoj konvenciji u ovom tekstu automorfizmi vektorskih prostora deluju sleva na svoj argument).

automorfizam projektivne geometrije

Podsetimo se da smo u Odeljku 1.4 pokazali da je grupa $\mathrm{Aut}(V)$ automorfizama n-dimenzionalnog vektorskog prostora V nad poljem F izomorfna opštoj linearnoj grupi $GL_n(F)$ regularnih kvadratnih matrica formata n nad F. Kao direktnu posledicu činjenice da se svaki linearno nezavsni skup vektora može dopuniti do baze prostora, sledi da je za sve $k \le n$ grupa $GL_n(F)$ tranzitivna na skupu svih nizova dužine k linearno nezavisnih vektora. Specijalno, $GL_n(F)$ je tranzitivna na $V \setminus \{0\}$, ali u opštem slučaju ne i dvostruko tranzitivna na tom skupu (pošto je nemoguće dva proporcionalna vektora preslikati na par linearno nezavisnih vektora; jedini izuzetak čini dvoelementno polje F_2 gde su svaka dva nenula vektora linearno nezavisna, pa je grupa $GL_n(F_2)$ dvostruko tranzitivna na $V \setminus \{0\}$). Drugim rečima, za svako $1 \le k \le n$, $GL_n(F)$ je tranzitivna na skupu svih potprostora od V dimenzije k.

U ovom smislu, sada svakom automorfizmu ϕ prostora V (pa tako i pridruženoj matrici $A_\phi \in GL_n(F)$ u odnosu na neku fiksiranu bazu od V) na prirodan način odgovara automorfizam $\overline{\phi}$ projektivne geometrije $\Gamma_{n-1}(F)$ kao rezultat (tranzitivnih) dejstava ϕ na potprostore od V dimenzije 1, odnosno 2. Neka je sada $Z_n(F)$ skup svih matrica $A \in GL_n(F)$ sa osobinom da automorfizam $\phi_A : x \mapsto Ax$ prostora V indukuje identičko preslikavanje na geometriji $\Gamma_{n-1}(F)$ (tj. ϕ_A fiksira sve potprostore od V dimenzije ≤ 2). Lako se vidi da je $\overline{\phi_{AB}}^{(i)}(t) =$

$\overline{\phi_A}^{(i)}\overline{\phi_B}^{(i)}(t)$ za bilo koju tačku ($i = 1$) ili pravu ($i = 2$) t geometrije $\Gamma_{n-1}(F)$ i $A, B \in GL_n(F)$, pa je $A \mapsto \overline{\phi_A}$ (sirjektivni) homomorfizam grupa $GL_n(F) \to \mathrm{Aut}(\Gamma_{n-1}(F))$ čije je jezgro baš $Z_n(F) \trianglelefteq GL_n(F)$. Sada faktor grupu

$$PGL_n(F) = GL_n(F)/Z_n(F)$$

projektivna linearna grupa

zovemo *projektivna (linearna) grupa* (stepena n nad poljem F).

U daljem za matricu A i polje F sa FA označavamo kolekciju matrica $\{\alpha A : \alpha \in F\}$.

Propozicija C.2. *$Z_n(F) = FE = Z(GL_n(F))$, tako da je $PGL_n(F) = GL_n(F)/FE$.*

Dokaz. Kako bismo dokazali da je $Z_n(F) = FE$ potrebno je i dovoljno dokazati da je $\overline{\phi_A}$ identičko preslikavanje na $\Gamma_{n-1}(F)$ ako i samo ako je A skalarna matrica, tj. $A = \alpha E$ za neko $\alpha \in F$. Jasno je da sve skalarne matrice indukuju trivijalni automorfizam geometrije $\Gamma_{n-1}(F)$; zato pretpostavimo, obratno, da je A proizvoljna matrica takva da je $\overline{\phi_A}$ trivijalni automorfizam od $\Gamma_{n-1}(F)$. Neka je $e_1, \dots, e_n$ baza prostora V takva da je pridružena matrica od $\phi_A \in \mathrm{Aut}(V)$ baš A. Zbog toga za sve $1 \le i \le n$ važi

$$Ae_i = \alpha_i e_i$$

za neko $\alpha_i \in F$. Zbog toga je $a_{ij} = 0$ za sve $j \neq i$, tj. A je dijagonalna matrica. Takođe, za sve $1 \le i \neq j \le n$ postoji $\beta_{ij} \in F$ tako da je

$$A(e_i + e_j) = \beta_{ij}(e_i + e_j),$$

pa iz $A(e_i + e_j) = Ae_i + Ae_j = \alpha_i e_i + \alpha_j e_j$ odmah sledi da je $\alpha_i = \beta_{ij} = \alpha_j$. Drugim rečima, svi dijagonalni elementi matrice A su međusobno jednaki, pa je A skalarna matrica, $A \in FE$.

Pokažimo da skalarne matrice nad F čine centar linearne grupe $GL_n(F)$. Očigledno, skalarna matrica αE komutira sa svakom matricom. Obratno, pretpostavimo da A komutira sa svim matricama iz $GL_n(F)$. Tada, specijalno, A komutira i sa svakom matricom E_{ij}, $i \neq j$, koja ima jedinice na glavnoj dijagonali kao i na polju (i, j), a nule na svim ostalim poljima: $AE_{ij} = E_{ij}A$. Međutim, lako se uočava da je AE_{ij} matrica koja se dobija od A dodavanjem i-te kolone j-toj koloni, dok se $E_{ij}A$ dobija od A dodavanjem j-te vrste i-toj vrsti. Ove dve matrice mogu biti jednake za sve $i \neq j$ ako i samo ako su svi vandijagonalni elementi od A jednaki 0, a dijagonalni elementi međusobno jednaki. Sledi da je A skalarna matrica. $\square$

Podsetimo se da smo sa $SL_n(F)$ označili normalnu podgrupu od $GL_n(F)$ koja se sastoji od svih matrica čija je determinanta $= 1$, tzv. specijalnu linearnu grupu. Po Teoremi o korespondenciji, njoj odgovara (normalna) podgrupa $SL_n(F)Z_n(F)/Z_n(F)$ projektivne grupe $PGL_n(F)$, koja je pak, po Prvoj teoremi o izomorfizmu, izomorfna sa

$$PSL_n(F) = SL_n(F)/SZ_n(F),$$

gde je $SZ_n(F) = Z_n(F) \cap SL_n(F) = \{\alpha E : \alpha^n = 1\}$. Ovu grupu zovemo *specijalna projektivna grupa* (stepena n nad poljem F). specijalna projektivna grupa

Sledeća propozicija se dokazuje analogno kao i prethodna.

Propozicija C.3. $SZ_n(F) = Z(SL_n(F))$.

Značaj specijalnih projektivnih grupa u teoriji grupa permutacija ogleda se u sledećem rezultatu.

Teorema C.4. *Za svako polje F i $n \geq 2$, grupe $PGL_n(F)$ i $PSL_n(F)$ su dvostruko tranzitivne.* dvostruka tranzitivnost projektivnih grupa

Dokaz. Posmatrajmo dve različite tačke geometrije $\Gamma_{n-1}(F)$: $p = \langle x_1 \rangle$ i $q = \langle x_2 \rangle$; tada su vektori x_1, x_2 linearno nezavisni. Zbog toga, za svake dve različite tačke $p' = \langle y_1 \rangle$ i $q' = \langle y_2 \rangle$ u $\Gamma_{n-1}(F)$ postoji matrica $A \in GL_n(F)$ takva da je $Ax_i = y_i$ za $i = 1, 2$. Tako je $\overline{\phi_A}^{(1)}(p) = p'$ i $\overline{\phi_A}^{(1)}(q) = q'$, odakle odmah sledi 2-tranzitivnost grupe $PGL_n(F)$.

Za grupe $PSL_n(F)$ posmatrajmo matricu $B = A/\det(A) \in SL_n(F)$. Sada je $Bx_i = y_i/d$ gde je $d = \det(A)$. Međutim, važi $\langle y_i/d \rangle = \langle y_i \rangle$, pa imamo $\overline{\phi_B}^{(1)}(p) = p'$ i $\overline{\phi_B}^{(1)}(q) = q'$; zbog toga su i grupe $PSL_n(F)$ 2-tranzitivne. $\square$

Posledica C.5. *Za sve $n \geq 2$ i proizvoljno polje F, $PGL_n(F)$ i $PSL_n(F)$ su primitivne grupe.*

Kao kulminaciju našeg razmatranja projektivnih linearnih grupa, ilustrujemo Ivasavinu lemu iz prethodnog dodatka njenom najznačajnijom primenom: dokazom da su specijalne projektivne grupe $PSL_n(F)$ (sa dva sporadična izuzetka) proste. Ovo je čuvena Teorema Žordan-Mur-Diksona.

teorema
Žordan-Mur-Diksona

Teorema C.6 (Žordan, Mur, Dikson[14]). *Neka je F proizvoljno polje. Ako je $n \geq 2$, a pri tome nije $n = 2$ i $|F| \leq 3$, tada je $PSL_n(F)$ prosta grupa.*

Prva dva dela dokaza ovog rezultata izdvajamo kao zasebna pomoćna tvrđenja.

Lema C.7. *Neka je H_{ij} matrica nad poljem F čiji su svi elementi 0 osim pozicije (i, j) na kojoj se nalazi 1. Za $1 \leq i \neq j \leq n$ i $\alpha \in F$ definišimo matrice*

$$Z_{ij}(\alpha) = E + \alpha H_{ij}.$$

Tada ove matrice generišu $SL_n(F)$.

Dokaz. Podsetimo se (iz linearne algebre) *elementarnih transformacija* matrica:

- transformacije tipa I: zamena i-te i j-te vrste, odnosno i-te i j-te kolone;
- transformacije tipa II: dodavanje i-toj vrsti j-te vrste pomnožene nenula skalarom $\alpha \in F$ i analogna operacija na kolonama, pri čemu je $i \neq j$;
- transformacije tipa III: množenje i-te vrste (kolone) nenula skalarom $\alpha \in F$.

Primetimo da se trasformacije tipa II realizuju upravo množenjem matricama $Z_{ij}(\alpha)$ sleva (za operaciju na vrstama), odnosno $Z_{ji}(\alpha)$ zdesna (za operaciju na kolonama). Na sličan način, množenje matricama

$$\begin{aligned} P_{ij} &= E + H_{ij} + H_{ji} - H_{ii} - H_{jj} \\ &= (E + H_{ij})(E - H_{ji})(E + H_{ij})(E - 2H_{ii}) = \\ &= Z_{ij}(1)Z_{ji}(-1)Z_{ij}(1)(E - 2H_{ii}) \end{aligned}$$

realizuje elementarne transformacije tipa I.

Sada koristimo jedan od osnovnih rezultata linearne algebre: svaka matrica se putem transformacija tipa I i II može svesti na dijagonalnu matricu. Preciznije, postoje matrice P i Q koje su obe proizvodi matrica oblika $Z_{ij}(\alpha)$ i P_{ij} tako da je

$$PAQ = D,$$

[14]Kamij Žordan (Marie Ennemond Camille Jordan, 1838–1922), francuski matematičar; Ilajakim Mur (Eliakim Hastings Moore, 1862–1932) i Leonard Dikson (Leonard Eugene Dickson, 1874–1954), američki matematičari. Žordan je najpre dokazao ovo tvrđenje samo za konačna polja F prostog reda; kasnije je Mur rešio opšti slučaj za $n = 2$, a Dikson za $n \geq 3$.

gde je D dijagonalna matrica sa dijagonalnim elementima redom $d_1, \dots, d_n \in F$, pri čemu je $d_1 \dots d_n = (-1)^n \det(A)$. Zapravo, matrice P, Q su proizvodi matrica oblika $Z_{ij}(\alpha)$ i $E - 2H_{ii}$. Sada primetimo da važi sledeća jednakost:

$$Z_{ij}(\alpha)(E - 2H_{ii}) = (E - 2H_{ii})Z_{ij}(-\alpha)$$

za sve $i \neq j$ i $\alpha \in F$. Ove jednakosti omogućavaju da se u proizvodu koji formira P svi faktori oblika $E - 2H_{ii}$ izdvoje sa leve strane, a da se u proizvodu koji izražava Q isto to učini sa desne strane. Primetimo da su $E - 2H_{ii}$ zapravo dijagonalne matrice koje na svim dijagonalnim poljima imaju 1 osim na i-tom, gde stoji -1. Zato je $(E - 2H_{ii})^2 = E$, tj. sve matrice $E - 2H_{ii}$ su same sebi inverzne. Dakle, množenjem relacije $PAQ = D$ odgovarajućim matricama ovog oblika sleva i zdesna dobijamo

$$P_1AQ_1 = D_1,$$

gde su P_1, Q_1 proizvodi matrica oblika $Z_{ij}(\alpha)$. Zbog toga važi $\det(P_1) = \det(Q_1) = 1$, pa ako za A odaberemo proizvoljnu matricu iz $SL_n(F)$, imamo da je i $\det(D_1) = \det(A) = 1$. Neka su $d'_1, \dots, d'_n$ dijagonalni elementi od D_1.

Sada definišimo preslikavanje $\psi_{ij}^{\alpha,\beta} : GL_n(F) \to GL_n(F)$, $i \neq j$, $\alpha, \beta \in F \setminus \{0\}$, sa:

$$X\psi_{ij}^{\alpha,\beta} = [Z_{ij}(\alpha^{-1} - 1)Z_{ji}(1)Z_{ij}(-1)]X[Z_{ij}(\beta)Z_{ji}(-\beta^{-1})].$$

Nije teško proveriti da je za svaku dijagonalnu matricu X koja na i-tom dijagonalnom polju ima α a na j-tom polju β, matrica $X\psi_{ij}^{\alpha,\beta}$ takođe dijagonalna matrica koja na svim poljima ima iste elemente kao i X osim i-tog dijagonalnog polja na kojem ima 1 i j-tog polja na kojem stoji $\alpha\beta$. Zbog toga je

$$D_1\psi_{12}^{d'_1,d'_2} \dots \psi_{n-1,n}^{d'_1 \dots d'_{n-1},d'_n} = E.$$

Zaključujemo da postoje matrice P_2, Q_2 koje se mogu predstaviti kao proizvodi matrica oblika $Z_{ij}(\alpha)$ tako da je

$$P_2AQ_2 = E,$$

odakle sledi $A = P_2^{-1}Q_2^{-1}$. Prema tome, A je generisana matricama $Z_{ij}(\alpha)$, pa one generišu grupu $SL_n(F)$. □

Lema C.8. *Ako je $n \geq 3$, ili $n = 2$ i $|F| > 3$, tada je $PSL_n(F)' = PSL_n(F)$.*

Dokaz. Ovde je dovoljno dokazati da je $SL_n(F)' = SL_n(F)$ (pod datim uslovima za n i F), budući da za svake dve grupe G, H za koje postoji sirjektivni homomorfizam $\phi : G \to H$, $G' = G$ povlači $H' = H$.

Razmotrimo najpre slučaj $n \geq 3$. Ako odaberemo indeks $k \notin \{i, j\}$, tada važi

$$Z_{ij}(\alpha) = Z_{ik}(\alpha)Z_{kj}(1)Z_{ik}(-\alpha)Z_{kj}(-1)$$

za proizvoljno $\alpha \in F$. Otuda je $Z_{ij}(\alpha) = [Z_{ik}(-\alpha), Z_{kj}(-1)]$ budući da je $Z_{pq}(\alpha)^{-1} = Z_{pq}(-\alpha)$ za proizvoljne $p \neq q$ i $\alpha \in F$. Kako matrice $Z_{ij}(\alpha)$ generišu $SL_n(F)$, sledi da je svaki element ove grupe proizvod komutatora, tj. $SL_n(F)' = SL_n(F)$.

Preostaje da razmotrimo slučaj $n = 2$. Po uslovima leme je $|F| \geq 4$, pa postoji skalar $\delta \in F \setminus \{-1, 0, 1\}$. Neka je

$$D = \begin{pmatrix} \delta^{-1} & 0 \\ 0 & \delta \end{pmatrix}.$$

Tada direktnim računom proveravamo da važi

$$Z_{12}(\alpha) = D^{-1}Z_{12}(\mu)DZ_{12}(\mu)^{-1} = [D, Z_{12}(\mu)^{-1}] = [D, Z_{12}(-\mu)],$$

gde je $\mu = \alpha/(\delta^2 - 1)$. Slično dobijamo da je i $Z_{21}(\alpha)$ u izvodnoj grupi od $SL_n(F)$, pa isto kao i malopre zaključujemo da je $SL_n(F)' = SL_n(F)$. $\square$

Dokaz Teoreme C.6. Po prethodnoj lemi, posmatrane grupe $PSL_n(F)$ zadovoljavaju uslov (1) Ivasavine leme, a po Posledici C.5 i uslov (2). Prema tome, dovoljno je dokazati da je zadovoljen i uslov (3), tj. da pronađemo normalnu Abelovu podgrupu A stabilizatora (u $PSL_n(F)$) neke tačke projektivne geometrije $\Gamma_{n-1}(F)$ čije sve konjugovane podgrupe generišu $PSL_n(F)$.

Neka je $e_1, \ldots, e_n$ bilo koja baza n-dimenzionalnog vektorskog prostora V nad F. Tada je $p = \langle e_1 \rangle$ tačka u $\Gamma_{n-1}(F)$; posmatraćemo stabilizator G_p u $PSL_n(F)$. U pitanju je kolekcija svih koseta $SZ_n(F)A$ gde je $A \in SL_n(F)$ matrica takva da je Ae_1 nenula vektor iz $\langle e_1 \rangle$, tj. $Ae_1 = \alpha e_1$ za neko $\alpha \in F \setminus \{0\}$. Jasno, ovo je ekvivalnentno uslovu da matrica A mora imati α u gornjem levom uglu, a sve ostale elemente prve kolone jednake 0 – dakle, ona je oblika

$$A = \begin{pmatrix} \alpha & \beta_1 & \ldots & \beta_{n-1} \\ 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{pmatrix}.$$

gde su $\beta_1, \ldots, \beta_{n-1} \in F$ i matrica A' je formata $n-1$ tako da je $\det(A') = 1/\alpha$. Po teoremi o korespondenciji, sve ovakve matrice čine podgrupu H od $SL_n(F)$ (koja očito sadrži $SZ_n(F)$), pri čemu je $G_p \cong H/SZ_n(F)$. Posmatrajmo sada homomorfizam grupa $\phi : H \to GL_{n-1}(F)$ koji svakoj matrici A gornjeg oblika dodeljuje matricu formata $n-1$ iz njenog donjeg desnog ugla, $\phi : A \mapsto A'$. Jezgro ovog homomorfizma – kojeg ćemo označiti sa K – čine sve matrice oblika

$$\begin{pmatrix} 1 & \beta_1 & \ldots & \beta_{n-1} \\ 0 & & & \\ \vdots & & E_{n-1} & \\ 0 & & & \end{pmatrix},$$

gde E_{n-1} označava jediničnu matricu formata $n-1$. Sada imamo da je $K \trianglelefteq H$, pa, po Teoremi o korespondenciji i Drugoj teoremi o izomorfizmu, za njoj odgovarajuću podgrupu u $PSL_n(F)$ važi $SZ_n(F)K/SZ_n(K) \trianglelefteq H/SZ_n(F)$. Primetimo da važi

$$\begin{pmatrix} 1 & \beta_1 & \ldots & \beta_{n-1} \\ 0 & & & \\ \vdots & & E_{n-1} & \\ 0 & & & \end{pmatrix} \begin{pmatrix} 1 & \gamma_1 & \ldots & \gamma_{n-1} \\ 0 & & & \\ \vdots & & E_{n-1} & \\ 0 & & & \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & \beta_1 + \gamma_1 & \ldots & \beta_{n-1} + \gamma_{n-1} \\ 0 & & & \\ \vdots & & E_{n-1} & \\ 0 & & & \end{pmatrix},$$

pa je zato grupa K izomorfna F^{n-1}, aditivnoj grupi svih $(n-1)$-dimenzionalnih vektora nad F – izomorfizam je

$$\begin{pmatrix} 1 & \beta_1 & \ldots & \beta_{n-1} \\ 0 & & & \\ \vdots & & E_{n-1} & \\ 0 & & & \end{pmatrix} \mapsto \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_{n-1} \end{pmatrix}.$$

Sledi da je K Abelova grupa, odakle je $SZ_n(F)K/SZ_n(K)$ normalna Abelova podgrupa stabilizatora G_p. Prema tome, preostaje da se pokaže da sve njene (u $PSL_n(F)$) konjugovane podgrupe generišu $PSL_n(F)$; za to je dovoljno da pokažemo da sve konjugovane podgrupe od K generišu $SL_n(F)$.

Podsetimo se sada jednakosti iz prethodne leme:

$$Z_{ij}(\alpha) = Z_{ik}(\alpha)Z_{kj}(1)Z_{ik}(-\alpha)Z_{kj}(-1).$$

Sve matrice oblika $Z_{1j}(\alpha)$, $j \geq 2$, $\alpha \in F$, su po definiciji sadržane u K. Stoga, ako je $i, j \geq 2$, tada izborom $k = 1$ gornja relacija postaje

$$Z_{ij}(\alpha) = [Z_{i1}(\alpha)Z_{1j}(1)Z_{i1}(-\alpha)]Z_{1j}(-1),$$

pri čemu treba primetiti da je matrica u uglastoj zagradi konjugovana sa matricom $Z_{1j}(1) \in K$. Zbog toga preostaje da se razmotri slučaj $j = 1$, tj. matrice $Z_{i1}(\alpha)$ za $i \geq 2$. Uočimo sada matricu

$$B_i = E - H_{11} - H_{ii} - H_{i1} + H_{1i}.$$

Veoma se lako vidi da je $\det(B_i) = 1$, tj. $B_i \in SL_n(F)$, kao i da važi relacija

$$Z_{i1}(\alpha) = B_i^{-1} Z_{1i}(-\alpha) B_i.$$

Tako, i sve matrice $Z_{i1}(\alpha)$ pripadaju podgrupama koje su konjugovane sa K. Sada možemo zaključiti da unija svih konjugovanih podgrupa od K generiše $SL_n(F)$. Time je okončan dokaz da grupe $PSL_n(F)$ imaju osobinu (3) iz Ivasavine leme, pa ona sada implicira traženi rezultat. $\square$

Dve specijalne projektivne grupe izuzete iz prethodne teoreme zaista nisu proste. Naime, ako F_2 označava dvoelementno polje, tada je $PSL_2(F_2) \cong SL_2(F_2) \cong \mathbb{S}_3$, dok je $PSL_2(F_3) \cong \mathbb{A}_4$ (gde F_3 označava troelementno polje).

D

Grupe reda pq

Kako bismo opisali sve grupe reda pq za proste brojeve $p < q$, najpre moramo opisati grupu automorfizama ciklične grupe prostog reda. Podsetimo se (iz teorije brojeva) da je ostatak r, $0 < r < n$, *primitivni koren* po modulu $n \geq 2$ ako i samo ako

$$r, r^2, \ldots, r^{\varphi(n)}$$

(gde je φ Ojlerova funkcija) čini redukovan sistem ostataka po modulu n (što znači da za svaki ostatak $0 < s < n$ takav da je $(s, n) = 1$ postoji $1 \leq k \leq \varphi(n)$ tako da je $r^k \equiv s(\mathrm{mod}\ \ n)$). Specijalno, za prost modul p imamo da je $\varphi(p) = p - 1$, pa gornji uslov izražava da je $0, r, r^2, \ldots, r^{p-1}$ potpun sistem ostataka po modulu p (svaki ostatak je zastupljen tačno jednom u ovom nizu). Jedan od osnovnih rezultata teorije brojeva tvrdi da svaki prost modul p ima primitivni koren, što se u algebarskoj terminologiji može izraziti uslovom da je $\mathbb{Z}_p^\times$ ciklična grupa, a da je primitivni koren njen generator. Drugim rečima, $\mathbb{Z}_p^\times \cong \mathbb{Z}_{p-1}$ (odakle odmah sledi da modul p ima tačno $\varphi(p-1)$ primitivnih korena).

Lema D.1. *Neka je p prost broj. Tada je* $\mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$.

Dokaz. Svaki automorfizam $\phi \in \mathrm{Aut}(\mathbb{Z}_p)$ jednoznačno je određen slikom proizvoljnog generatora od $\mathbb{Z}_p$: na primer, ako je $1\phi = r < p$ tada mora biti $a\phi \equiv ra(\mathrm{mod}\ \ p)$ za sve $0 \leq a < p$ (pri tome, jasno, ne može biti $r = 0$, jer to rezultuje trivijalnim endomorfizmom, a ne automorfizmom). S druge strane, svako opisano preslikavanje $\mathbb{Z}_p \to \mathbb{Z}_p$ jeste automorfizam: ono je očigledno endomorfizam, koji je pri tome još i bijekcija jer $p \mid r(a-a')$ za neko $0 \leq a, a' < p$ implicira $a - a' = 0$, tj. $a = a'$. Prema tome, ako sa ϕ_r označimo automorfizam određen uslovom $1\phi_r = r$, tada su sa $\phi_1 = \mathrm{id}_{\mathbb{Z}_p}, \phi_2, \ldots, \phi_{p-1}$ iscrpljeni svi automorfizmi grupe $\mathbb{Z}_p$.

Pošto sada znamo da je grupa $\mathrm{Aut}(\mathbb{Z}_p)$ reda $p-1$, preostaje da pokažemo da je ciklična. Primetimo da za proizvoljno $k \geq 1$ i ostatak a po modulu p važi

$$a\phi_r^k \equiv r^k a (\mathrm{mod}\ p) \equiv r_k a (\mathrm{mod}\ p) \equiv a\phi_{r_k},$$

gde je r_k ostatak r^k pri deljenju sa p, pa je $a\phi_r^k = a\phi_{r_k}$ tj. $\phi_r^k = \phi_{r_k}$. Ako sada za r uzmemo bilo koji primitivni koren po modulu p, dobijamo da je

$$\phi_{r_1} = \phi_r, \phi_{r_2} = \phi_r^2, \ldots, \phi_{r_{p-1}} = \phi_1 = \phi_r^{p-1}$$

neka permutacija prethodne liste svih automorfizama od $\mathbb{Z}_p$. Zato je $\mathrm{Aut}(\mathbb{Z}_p) = \langle \phi_r \rangle$ ciklična grupa. □

opis grupa reda pq

Teorema D.2. *Neka su $p < q$ prosti brojevi. Postoji tačno jedna Abelova grupa reda pq, $\mathbb{Z}_{pq} \cong \mathbb{Z}_p \times \mathbb{Z}_q$. Ako $p \nmid q-1$, ovo je ujedno i jedina grupa reda pq; u suprotnom (ako $p \mid q-1$) postoji tačno jedna nekomutativna grupa reda pq, poludirektan proizvod $\mathbb{Z}_p \ltimes_\psi \mathbb{Z}_q$ određen homomorfizmom $\psi : \mathbb{Z}_p \to \mathrm{Aut}(\mathbb{Z}_q)$ koji generatoru grupe $\mathbb{Z}_p$ dodeljuje automorfizam $\phi_r^{(q-1)/p}$, gde je r proizvoljan primitivni koren po modulu q.*

Dokaz. Na početku, primetimo da su (p-,q-)podgrupe Silova P, Q svake grupe G reda pq ciklične, tj. izomorfne sa $\mathbb{Z}_p$, odnosno $\mathbb{Z}_q$, respektivno. Pri tome po teoremama Silova imamo $s_q \equiv 1(\mathrm{mod}\ q)$ i $s_q \mid p$, odakle zbog $p < q$ odmah sledi $s_q = 1$. Prema tome, $Q \trianglelefteq G$ je jedinstvena q-podgrupa Silova od G.

S druge strane, imamo $s_p \equiv 1(\mathrm{mod}\ p)$ i $s_p \mid q$. Ako je $s_p = 1$, tada je i $P \trianglelefteq G$ i odmah dobijamo da je $G \cong P \times Q$, tj. da je u pitanju Abelova grupa $\mathbb{Z}_{pq} \cong \mathbb{Z}_p \times \mathbb{Z}_q$. U suprotnom $s_p = q$, što je sada očito moguće samo ako je $q-1$ deljivo sa p; ako $p \nmid q-1$ neabelove grupa reda pq ne postoje.

Prema tome, preostaje da razmotrimo slučaj $p \mid q-1$ i $s_p = q$ (kada podgrupa P nije normalna u G, jer ima q konjugovanih podgrupa). Primetimo da je $P \cap Q = E$, kao i da je zbog normalnosti Q, $PQ = QP$, pa je PQ podgrupa od G reda pq, zbog čega je $G = PQ$. Prema tome, G je unutrašnji poludirektni proizvod $G = P \ltimes Q$.

Kako su P, Q ciklične grupe, fiksirajmo neke njihove generatore, $P = \langle a \rangle$, $Q = \langle b \rangle$, i posmatrajmo element $a^{-1}ba$. Pošto je $Q \trianglelefteq G$, ovaj element mora pripadati Q, tj. mora biti

$$a^{-1}ba = b^k$$

za neko $k < q$. Pri tome je $k > 1$, jer bismo za $k = 1$ dobili $ab = ba$ i $G = P \times Q$. Kako u P važi $a^p = 1$, to u Q mora biti $b = a^{-p}ba^p = b^{k^p}$, pa sledi da je $k^p \equiv 1 (\mathrm{mod}\ q)$. To znači da postoji primitivni koren r po modulu q tako da je $k = r^{(q-1)/p}$. S druge strane, primetimo da gornja relacija ($a^{-1}ba = b^k$) jednoznačno određuje grupu G: ona obezbeđuje da se svi njeni elementi mogu (jedinstveno) izraziti u obliku a^ib^j za neko $0 \le i < p$ i $0 \le j < q$, kao i da je množenje tih elemenata dato sa

$$(a^ib^j)(a^ub^v) = a^{i+u}(a^{-u}b^ja^u)b^v = a^{i+u}b^{jk^u+v}.$$

Neposredno se proverava da je ovim zaista zadata grupa od pq elemenata.

Dokažimo da dobijena grupa, do na izomorfizam, ne zavisi od izbora primitivnog korena r. Neka je G_k grupa koja se dobija na osnovu relacije $a^{-1}ba = b^k$ za $k = r^{(q-1)/p}$, a G_ℓ grupa koja je dobijena iz $a^{-1}ba = b^\ell$ gde je $\ell = s^{(q-1)/p}$ za neki drugi primitivni koren s po modulu q. Međutim, tada je $r \equiv s^t (\mathrm{mod}\ q)$ za neko t tako da je $(t, q-1) = 1$ (pa tako, specijalno, $p \nmid t$), odakle je $k \equiv \ell^t (\mathrm{mod}\ q)$. Posmatrajmo sada preslikavanje $\xi : G_k \to G_\ell$ dato sa $(a^ib^j)\xi = a^{ti}b^j$ za sve $0 \le i < p$, $0 \le j < q$. Imamo da je

$$(a^ib^j)\xi(a^ub^v)\xi = (a^{ti}b^j)(a^{tu}b^v) = a^{t(i+u)}b^{j\ell^{tu}+v} =$$

$$= a^{t(i+u)}b^{jk^u+v} = [(a^ib^j)(a^ub^v)]\xi,$$

tj. ξ je homomorfizam grupa. On je bijekcija, jer $(a^ib^j)\xi = (a^{i'}b^{j'})\xi$ povlači (pored $b^j = b^{j'}$) $a^{ti} = a^{ti'}$, odnosno $p \mid t(i - i')$, pa zbog $p \nmid t$ sledi $p \mid i - i'$ i $a^i = a^{i'}$. Dakle, $G_k \cong G_\ell$.

Zaključujemo da u slučaju $p \mid q-1$ postoji tačno jedna nekomutativna grupa reda pq koja je poludirektan proizvod svoje p-podgrupe i q-podgrupe Silova; koristeći Propoziciju 4.7 dobijamo da se on realizuje kao spoljašnji poludirektan proizvod baš kao što je i navedeno u formulaciji (generator ciklične grupe $\mathbb{Z}_p$ deluje na $\mathbb{Z}_q$ automorfizmom $x \mapsto x^k$). $\square$

Primetimo da u slučaju $p = 2$ nekomutativni poludirektan proizvod $\mathbb{Z}_p \ltimes \mathbb{Z}_q$ uvek postoji: to je upravo dijedarska grupa D_q.

E

Nilpotentne grupe

Uopštavajući pojam izvodne podgrupe, za dve podgrupe $A, B \leq G$ definišemo njihov *komutant* $[A, B]$ kao podgrupu od G generisanu svim komutatorima oblika $[a, b]$, $a \in A$, $b \in B$. Za niz podgrupa

komutant

$$G = H_0 \geq H_1 \geq \cdots \geq H_n = E$$

centralni niz

kažemo da je *centralni niz* grupe G ako za sve $0 \leq i \leq n-1$ važi da je

$$[H_i, G] \leq H_{i+1}.$$

nilpotentna grupa

Grupa G koja ima centralni niz je *nilpotentna*. Odmah ćemo uočiti da je svaki centralni niz grupe normalan, ali da zapravo važi i više od toga.

svaki centralni niz se sastoji od normalnih podgrupa

Lema E.1. *Ako je*

$$G = H_0 \geq H_1 \geq \cdots \geq H_n = E$$

centralni niz grupe G, tada je $H_i \trianglelefteq G$ za sve $0 \leq i \leq n$.

Dokaz. Ako je $[H_i, G] \leq H_{i+1}$ tada je i $[H_i, G] \leq H_i$. Stoga, za sve $g \in G$, $h \in H_i$ važi $h^{-1}g^{-1}hg \in H_i$, tj. $g^{-1}hg \in H_i$. No, sada je očito $H_i \trianglelefteq G$. $\square$

Naredna lema će objasniti poreklo termina "centralni niz".

Lema E.2. *Neka je G grupa i $H \leq K \leq G$, pri čemu je $H \trianglelefteq G$. Tada važi $[K, G] \leq H$ ako i samo ako je $K/H \leq Z(G/H)$.*

Dokaz. K/H je sadržano u centru od G/H ako i samo ako za sve $k \in K$ i $g \in G$ važi $kgH = Hkg = (Hk)(Hg) = (Hg)(Hk) = Hgk = gkH$. Međutim, poslednji uslov je ekvivalentan sa $[k, g] = (gk)^{-1}kg \in H$, tj. $[K, G] \leq H$. □

Znači, u centralnom nizu grupe G (ako on postoji) svaki faktor H_i/H_{i+1} je Abelova grupa, jer je sadržan u centru količnika G/H_{i+1}. (Štaviše, svaki količnik H_i/H_j, $i \leq j$ – koji postoji jer je $H_j \trianglelefteq G$ – je Abelov, jer je sadržan u $Z(G/H_j)$.) Zato odmah imamo sledeće.

Posledica E.3. *Svaka nilpotentna grupa je rešiva.*

S druge strane, svaka Abelova grupa G je nilpotentna, jer je niz $G \geq E$ trivijalno centralan. Tako, klasa Abelovih grupa je sadržana u klasi nilpotentnih grupa, i pri tome je inkluzija stroga, jer je neabelova grupa Q_8 nilpotentna: lako se proverava da je niz

$$Q_8 \rhd Q_8' = \{1, -1\} \rhd \{1\}$$

centralan. S druge strane, klasa nilpotentnih grupa je sadržana u klasi rešivih grupa, i ta inkluzija je takođe stroga, jer rešiva grupa $\mathbb{S}_3$ nije nilpotentna: imamo da je $\mathbb{S}_3' = \mathbb{A}_3$, pa bi naredni član njenog (hipotetičkog) centralnog niza morao biti $\mathbb{A}_3$, no kako je $[\mathbb{A}_3, \mathbb{S}_3] = \mathbb{A}_3$ sledi da $\mathbb{S}_3$ nema centralni niz.

Slično kao i u slučaju rešivih grupa (gde je najkraći normalni niz sa Abelovim faktorima bio niz izvodnih podgrupa), i za nilpotentne grupe možemo konstruisati "kanoničke" centralne nizove koji su minimalne dužine. Zapravo, imamo, za svaku nilpotentnu grupu, dva takva kanonička centralna niza. *Donji centralni niz* dobijamo kada definišemo sledeći niz podgrupa od G: $K_0(G) = G$ i, za sve $i \geq 0$, donji centralni niz

$$K_{i+1}(G) = [K_i(G), G].$$

Propozicija E.4. *Grupa G je nilpotentna ako i samo ako je $K_n(G) = E$ za neko $n \in \mathbb{N}$. Pri tome je, u slučaju nilpotentnosti, donji centralni niz najkraći centralni niz grupe G, i za svaki drugi centralni niz* nilpotentnost i donji centralni niz

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

važi $K_i(G) \leq H_i$.

Dokaz. Dokažimo indukcijom po i samo poslednje tvrđenje, pošto sve ostalo sledi iz njega. Zaista, $K_0(G) = G = H_0$. Pretpostavimo sada da je $K_i(G) \leq H_i$ za neko i. Tada je $K_{i+1}(G) = [K_i(G), G] \leq [H_i, G] \leq H_{i+1}$. □

gornji centralni niz

Gornji centralni niz podgrupa $Z_i(G) \leq G$, $i \geq 0$, dobijamo tako što definišemo $Z_0(G) = E$ i, za sve $i \geq 0$,

$$Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G)).$$

Ova definicija logički ima smisla budući da po Teoremi o korespondenciji centar grupe $G/Z_i(G)$ jeste njena podgrupa koja je oblika $H/Z_i(G)$ za (jedinstveno određenu) podgrupu H od G koja sadrži $Z_i(G)$; kako je u pitanju normalna podgrupa od $G/Z_i(G)$, sledi da je $H \trianglelefteq G$ i upravo to H obeležavamo sa $Z_{i+1}(G)$.

nilpotentnost i gornji centralni niz

Propozicija E.5. *Grupa G je nilpotentna ako i samo ako je $Z_n(G) = G$ za neko $n \in \mathbb{N}$. Pri tome je, u slučaju nilpotentnosti, gornji centralni niz najkraći centralni niz grupe G, i za svaki drugi centralni niz*

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

važi $H_i \leq Z_{n-i}(G)$, gde je n najmanji prirodan broj za koji je $Z_n(G) = G$.

Dokaz. Najpre, gornji centralni niz je zaista centralan zbog Leme E.2, budući da $Z_{i+1}(G)/Z_i(G) = Z(G/Z_i(G))$ implicira da je $[Z_{i+1}(G), G] \leq Z_i(G)$. Zato $Z_n(G) = G$ za neko n povlači nilpotentnost grupe G.

Obratno, neka je G nilpotentna grupa sa centralnim nizom kao u formulaciji propozicije. Indukcijom po i dokazujemo da je $H_{n-i} \leq Z_i(G)$. Zaista, $H_n = E = Z_0(G)$. Pretpostavimo sada da je za neko i, H_{n-i} sadržano u $Z_i(G)$. Kako su (po Lemi E.1) H_{n-i} i $Z_i(G)$ normalne podgrupe od G, po Drugoj teoremi o izomorfizmu imamo sirjektivni homomorfizam $\phi : G/H_{n-i} \to G/Z_i(G)$. (U pitanju je, u suštini, prirodni homomorfizam u odnosu na $Z_i(G)/H_{n-i} \trianglelefteq G/H_{n-i}$ koji za svaku podgrupu K takvu da $H_{n-i} \leq K \leq G$, podgrupu $K/H_{n-i} \leq G/H_{n-i}$ slika u $(K/H_{n-i})\phi = KZ_i(G)/Z_i(G)$.) Budući da je $[H_{n-i-1}, G] \leq H_{n-i}$, po Lemi E.2, H_{n-i-1}/H_{n-i} je sadržano u centru grupe G/H_{n-i}. Međutim, lako se pokazuje da za svaki sirjektivni homomorfizam grupa $\psi : G_1 \to G_2$ važi $Z(G_1)\psi \leq Z(G_2)$, pa je zbog toga

$$H_{n-i-1}Z_i(G)/Z_i(G) = (H_{n-i-1}/H_{n-i})\phi \leq Z(G/H_{n-i})\phi \leq$$

$$\leq Z(G/Z_i(G)) = Z_{i+1}(G)/Z_i(G).$$

Zaključujemo da je $H_{n-i-1} \leq H_{n-i-1}Z_i(G) \leq Z_{i+1}(G)$, što okončava induktivni dokaz. Sada sledi da je $G = H_0 \leq Z_n(G)$, pa mora biti $Z_n(G) = G$. $\square$

Kao posledicu prethodne dve propozicije imamo da su za svaku nilpotentnu grupu G dužine njihovih donjih i gornjih centralnih nizova jednake. Tu dužinu zovemo *indeks nilpotentnosti* grupe G. Primetimo da su grupe indeksa nilpotentnosti 1 tačno Abelove grupe.

indeks nilpotentnosti

Propozicija E.6. *Svaka konačna p-grupa je nilpotentna. Pri tome, ako je $|G| = p^n$, tada je indeks nilpotentnosti G ne veći od $n-1$.*

konačne p-grupe su nilpotentne

Dokaz. Slučaj $n = 1$ je trivijalan, jer je tada grupa G Abelova. Zato pretpostavimo da je $n \geq 2$.

Prema Posledici 3.10, centar $Z_1(G) = Z(G)$ ima bar p elemenata. Takođe, ako je $Z_i(G) \neq G$, tada je $Z_{i+1}(G) \neq Z_i(G)$, jer je $Z_{i+1}(G)/Z_i(G)$ centar netrivijalne p-grupe $G/Z_i(G)$. Otuda induktivno sledi da je $|Z_i(G)| \geq p^i$ za sve $1 \leq i \leq n-2$. Prema tome, grupa $G/Z_{n-2}(G)$ je p-grupa sa ne više od p^2 elemenata, pa je stoga Abelova i zato jednaka svom centru. Odatle je $Z_{n-1}(G) = G$. □

Tako, Propozicija 7.14 (tvrđenje da su sve konačne p-grupe rešive) je direktna posledica prethodnog rezultata i Posledice E.3. Nešto kasnije ćemo videti da se još neka značajna svojstva konačnih p-grupa očituju kao posledice njihove nilpotentnosti.

Propozicija E.7. *Neka je G nilpotentna grupa.*

nilpotentne grupe i konstrukcije

(i) Ako je $H \leq G$, tada je H nilpotentna.

(ii) Ako je $H \trianglelefteq G$, tada je G/H nilpotentna.

(iii) Ako su G_1 i G_2 nilpotentne grupe, tada je i $G_1 \times G_2$ nilpotentna.

Dokaz. (i) Po konstrukciji donjeg centralnog niza je $K_i(H) \leq K_i(G)$ za sve i. Specijalno, mora biti $K_n(H) = E$, gde je n indeks nilpotencije od G.

(ii) Ako je $\phi : G \to L$ sirjektivni homomorfizam grupa, tada za sve podgrupe $A, B \leq G$ važi $[A, B]\phi = [A\phi, B\phi]$, pa je $K_i(L) = [K_i(G)]\phi$. Zbog toga $K_n(G) = E$ implicira $K_n(L) = E$. Rezultat sledi primenjujući ove primedbe na prirodni homomorfizam $G \to G/H$.

(iii) Pošto se lako pokazuje da je $K_i(G_1 \times G_2) = K_i(G_1) \times K_i(G_2)$, sledi da je indeks nilpotencije grupe $G_1 \times G_2$ jednak većem od indeksa nilpotencije grupa G_1, G_2. □

Međutim, za razliku od rešivih grupa, nije tačno da nilpotentnost $H \trianglelefteq G$ i G/H povlači nilpotentnost G: kontraprimer je grupa $\mathbb{S}_3$ koja nije nilpotentna, ali to jesu kako $\mathbb{Z}_3 \cong \mathbb{A}_3 \trianglelefteq \mathbb{S}_3$, tako i $\mathbb{S}_3/\mathbb{A}_3 \cong \mathbb{Z}_2$.

Prelazimo sada na karakterizaciju konačnih nilpotentnih grupa.

karakterizacija konačnih nilpotentnih grupa

Teorema E.8. *Neka je G konačna grupa. Sledeći uslovi su ekvivalentni:*

(1) G je nilpotentna.

(2) G je (unutrašnji) direktan proizvod svih svojih podgrupa Silova.

(3) Svaka podgrupa Silova od G je normalna (i stoga jedinstvena za dato p).

(4) Za svaku podgrupu $H \lneqq G$ važi $H \lneqq N(H)$.

(5) Svaka maksimalna podgrupa od G je normalna.

Dokaz. (1)⇒(4) Neka je H prava podgrupa od G, i neka je

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

neki centralni niz grupe G. Pri tome, H ne sadrži H_0, ali sadrži H_n, pa postoji indeks i tako da $H_i \not\leq H$ i $H_{i+1} \leq H$. Tvrdimo da je $H_i \leq N(H)$, odakle sledi tvrđenje (4).

Zaista, neka je $a \in H_i$. Kako je $[H_i, H] \leq [H_i, G] \leq H_{i+1} \leq H$, to za proizvoljno $h \in H$ važi $[a, h^{-1}] \in H$, pa tako i

$$a^{-1}ha = [a, h^{-1}]h \in H.$$

Drugim rečima, $a^{-1}Ha \subseteq H$, pa je $a \in N(H)$.

(4)⇒(5) Neka je M maksimalna podgrupa od G. Po uslovu (4), $M \lneqq N(M)$, pa mora biti $N(M) = G$, odnosno $M \trianglelefteq G$.

(5)⇒(3) Neka je p prost broj i P jedna p-podgrupa Silova od G. Tvrdimo da je svaka podgrupa H od G koja sadrži normalizator $N(P)$ jednaka svom sopstvenom normalizatoru, $H = N(H)$. Zaista, pretpostavimo da je $a \in N(H)$; tada je $a^{-1}Ha = H$. Kako H sadrži P (pošto zadrži $N(P)$), P je i p-podgrupa Silova od H, a to važi i za $a^{-1}Pa \leq a^{-1}Ha = H$. Po teoremama Silova, P i $a^{-1}Pa$ su konjugovane u H, tj. postoji $h \in H$ tako da je $h^{-1}Ph = a^{-1}Pa$. Stoga je $ah^{-1}P = Pah^{-1}$, pa je $ah^{-1} \in N(P) \leq H$; otuda sledi da je $a \in H$.

Ako bi sada bilo $N(P) \lneqq G$, tada bi postojala maksimalna podgrupa M od G koja sadrži $N(P)$, pa bismo imali $N(M) = M$. Međutim, po uslovu (5) je $M \trianglelefteq G$, pa je $N(M) = G$, kontradikcija. Zato mora biti $N(P) = G$, tj. $P \trianglelefteq G$.

(3)⇒(2) Ovo je sadržaj Leme 6.10.

(2)⇒(1) Ovo je direktna posledica Propozicije E.6 i tačke (iii) Propozicije E.7. □

Na osnovu ove teoreme uviđamo da možemo dokazati tvrđenje koje je mnogo jače od Leme 7.13.

Posledica E.9. *Svaka maksimalna podgrupa konačne p-grupe G, $|G| = p^n$, je normalna i indeksa p (i, posledično, kardinalnosti p^{n-1}).*

Takođe, iz prethodnog dokaza možemo izvući sledeći opis konačnih nilpotentih grupa koji objašanjava zašto su one "skoro Abelove".

Posledica E.10. *Konačna grupa G je nilpotentna ako i samo ako svaki par njenih elemenata uzajamno prostih redova komutira.*

Naše razmatranje nilpotentnih grupa završavamo ispitivanjem osnovnih osobina tzv. *Fratinijeve*[15] *podgrupe* $\Phi(G)$ date grupe G. Ukoliko G ima bar jednu maksimalnu podgrupu, $\Phi(G)$ se definiše kao presek svih maksimalnih podgrupa od G; u suprotnom, po konvenciji je $\Phi(G) = G$.

Fratinijeva podgrupa

Propozicija E.11. *Za proizvoljnu grupu G, $\Phi(G)$ je karakteristična podgrupa od G.*

Dokaz. Tvrđenje sledi iz činjenice da svaki automorfizam ϕ grupe G indukuje permutaciju na skupu svih maksimalnih podgrupa od G. Zaista, ako su M_1, M_2 dve različite maksimalne podgrupe od G, tada su $M_1\phi \neq M_2\phi$ takođe maksimalne podgrupe od G. Štaviše, ako je M makismalna podgrupa od G, tada je $M\phi^{-1}$ takođe maksimalna podgrupa od G za koju važi $(M\phi^{-1})\phi = M$. Otuda je podgrupa $\Phi(G)$ invarijantna za sve automorfizme grupe G (pri čemu je slučaj $\Phi(G) = G$ trivijalan). □

Lema E.12. *Za svaku grupu G, $\Phi(G)$ se poklapa sa skupom svih elemenata grupe G koji se mogu eliminisati iz svakog generatornog skupa grupe G, tj.*

opis elemenata Fratinijeve podgrupe

$$\Phi(G) = \{g \in G : \ G = \langle A \cup \{g\} \rangle \ \Rightarrow \ G = \langle A \rangle \text{ za sve } A \subseteq G\}.$$

[15] Đovani Fratini (Giovanni Frattini, 1852–1925), italijanski matematičar

Dokaz. Pretpostavimo najpre da je $g \in \Phi(G)$; najpre posmatrajmo slučaj kada G ima maksimalne podgrupe i kada se g nalazi u svim maksimalnim podgrupama od G, pri čemu je $G = \langle A \cup \{g\} \rangle$. Posmatrajmo familiju podgrupa

$$\mathcal{F} = \{H \leq G : \ A \subseteq H, g \notin H\}.$$

Po aksiomi izbora (tj. po Cornovoj lemi), ako je $\mathcal{F} \neq \varnothing$, tada $\mathcal{F}$ ima maksimalni element M. Očito, $M \neq G$. Pri tome je M maksimalna podgrupa od G, jer $M \lneq K$ povlači da je $A \subseteq K$ i $g \in K$, odakle je $K = G$. No, tada je $g \in M$, kontradikcija. Znači, familija $\mathcal{F}$ mora biti prazna: $A \subseteq H$ povlači $g \in H$, tj. $g \in \langle A \rangle$. Sledi da je $G = \langle A \rangle$.

U slučaju da G nema maksimalne podgrupe, polazimo od pretpostavke da je $g \in G = \langle A \cup \{g\} \rangle$ proizvoljan element i formiramo familiju $\mathcal{F}$ kao i malopre. Zaključujemo da je $\mathcal{F} = \varnothing$, jer u suprotnom $\mathcal{F}$ ima maksimalni element koji bi bio maksimalna podgrupa u G, pa je zato $g \in \langle A \rangle = G$.

Obratno, pretpostavimo da se g može izbaciti iz svakog generatornog skupa grupe G (za koju možemo pretpostaviti da ima maksimalne podgrupe – u suprotnom je tvrđenje trivijalno). Neka je H jedna maksimalna podgrupa od G. Ako bi bilo $g \notin H$, tada bismo imali $\langle H \cup \{g\} \rangle = G$. No, naša pretpostavka bi povlačila da je $H = \langle H \rangle = G$, kontradikcija. Prema tome, mora biti $g \in H$. □

Fratinijev argument

Lema E.13 (Fratinijev argument)**.** *Ako je G konačna grupa, $H \trianglelefteq G$, i P jedna p-podgrupa Silova od H, tada je $G = HN_G(P)$.*

Dokaz. Neka je $g \in G$ proizvoljno. Tada je $g^{-1}Pg \leq g^{-1}Hg = H$, pa je $g^{-1}Pg$ takođe p-podgrupa Silova od H. Po teoremama Silova, P i $g^{-1}Pg$ su konjugovane u H, pa postoji $h \in H$ tako da je $h^{-1}g^{-1}Pgh = P$. Stoga je $gh \in N_G(P)$, pa je $g \in N(P)h^{-1} \subseteq N(P)H = HN(P)$. □

Lema E.14. *Neka je G grupa. Ako je Fratinijeva podgrupa $\Phi(G)$ konačno generisana i $H \leq G$ takva da je $G = \Phi(G)H$, tada je $H = G$.*

Dokaz. Pretpostavimo da je $\Phi(G) = \langle g_1, \ldots, g_n \rangle$. Tada je

$$G = \langle H \cup \{g_1, \ldots, g_n\} \rangle,$$

pa uzastopnom primenom Leme E.12 sledi da je $G = \langle H \rangle = H$. □

Značaj Fratinijeve podgrupe u izučavanju nilpotentnih grupa ogleda se pre svega u sledećem rezultatu.

Propozicija E.15. *Za svaku konačnu grupu G, $\Phi(G)$ je nilpotentna grupa.*

Fratinijeva podgrupa je nilpotentna

Dokaz. Neka je P jedna p-podgrupa Silova od $\Phi(G)$. Kako je $\Phi(G) \trianglelefteq G$, po Fratinijevom argumentu je $G = \Phi(G)N_G(P)$. Međutim, po prethodnoj lemi je tada $G = N_G(P)$. Zato je $P \trianglelefteq G$, a samim tim i $P \trianglelefteq \Phi(G)$. Tvrđenje sada sledi po Teoremi E.8. □

Za sam kraj, kao primenu Fratinijevog argumenta, dajemo još dve karakterizacije konačnih nilpotentnih grupa koje koriste Fratinijevu podgrupu.

Teorema E.16. *Konačna grupa G je nilpotentna ako i samo ako je $G' \leq \Phi(G)$.*

konačne nilpotentne grupe i Fratinijeva podgrupa

Dokaz. ($\Rightarrow$) Neka je G nilpotentna grupa. Tada je po Teoremi E.8 svaka maksimalna podgrupa M od G normalna, i pri tome, po Teoremi o korespondenciji, G/M nema pravih podgrupa, te je zato G/M ciklična (dakle, Abelova), zbog čega je po Lemi 3.32 $G' \leq M$. Dakle, G' je sadržano u svakoj maksimalnoj podgrupi od G, zbog čega je $G' \leq \Phi(G)$.

($\Leftarrow$) Neka je P neka p-podgrupa Silova od G. Definišimo $H = P\Phi(G)$. Ovo je podgrupa od G, jer je $\Phi(G) \trianglelefteq G$. Za proizvoljne $g \in G$ i $h \in H$ sada važi

$$h^{-1}(g^{-1}hg) = [h, g] \in G' \leq \Phi(G) \leq H,$$

pa sledi da je $g^{-1}hg \in H$. tj. $H \trianglelefteq G$. Primetimo da je P ujedno i p-podgrupa Silova u H, pa je po Fratinijevom argumentu

$$G = HN(P) = N(P)H = N(P)P\Phi(G) = N(P)\Phi(G).$$

No, po Lemi E.14 sada sledi da je $G = N(P)$, tj. $P \trianglelefteq G$. Dakle, grupa G je nilpotentna po Teoremi E.8. □

Teorema E.17. *Konačna grupa G je nilpotentna ako i samo ako je $G/\Phi(G)$ nilpotentna grupa.*

Dokaz. ($\Rightarrow$) Po Propoziciji E.7(ii), svaki količnik nilpotentne grupe je nilpotentan, pa tako i $G/\Phi(G)$.

($\Leftarrow$) Neka je P neka p-podgrupa Silova od G. Tada, po Teoremi o korespondenciji, $P\Phi(G)/\Phi(G)$ mora biti p-podgrupa Silova od $G/\Phi(G)$ (ona je zbog $P\Phi(G)/\Phi(G) \cong P/(P \cap \Phi(G))$ svakako p-podgrupa, a postojanje veće p-podgrupe u $G/\Phi(G)$ u kojoj bi $P\Phi(G)/\Phi(G)$ bila indeksa p^k bi impliciralo postojanje p-podgrupe od G kardinalnosti $p^k|P|$, što je nemoguće). Zbog toga je $P\Phi(G)/\Phi(G) \trianglelefteq G/\Phi(G)$, budući da je $G/\Phi(G)$ nilpotentna grupa, odakle dobijamo da je $P\Phi(G) \trianglelefteq G$. Jasno, P je p-podgrupa Silova od $P\Phi(G)$, pa po argumentu Fratinija sledi

$$G = (P\Phi(G))N(P) = N(P)P\Phi(G) = N(P)\Phi(G).$$

Identično kao i u prethodnoj teoremi, ovo implicira $G = N(P)$, odnosno $P \trianglelefteq G$, pa zaključujemo da je G nilpotentna grupa. $\square$

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.