ALGEBARSKE STRUKTURE
prva verzija skripte
zima 2010/11

Neven Grbac

Vedrana Mikulić Crnković

Sadržaj

UVOD

I. GRUPE

1. Definicije i osnovni pojmovi

1.1. Binarna operacija. Neka je G neprazan skup. Binarna operacija na skupu G je svako preslikavanje (funkcija) iz Kartezijevog produkta $G \times G$ u G. Uobičajeno je kao oznaku binarne operacije koristiti simbole (npr. $*$, $+$, $\cdot$, $\circ$,...), a ne slova koja se inače koriste kao oznaka za funkcije (npr. f, g,...). Kako bismo naglasili da se radi o nekoj općenitoj operaciji, mi ćemo za početak koristiti oznaku $*$ (kasnije će se radi kratkoće to pretvoriti u $\cdot$). Dakle, binarna operacija $*$ je preslikavanje (funkcija)

$$* : G \times G \to G.$$

Vrijednost binarne operacije $*$ na uređenom paru $(g_1, g_2) \in G \times G$ označavamo

$$g_1 * g_2,$$

umjesto $*(g_1, g_2)$ što bi inače bilo uobičajeno za funkcije. Po definiciji binarne operacije, vrijednost $g_1 * g_2$ je također element iz skupa G. Stoga često, kao sinonim za binarnu operaciju, kažemo da je skup G zatvoren obzirom na operaciju $*$.

1.2. Grupoid. Neka je G neprazan skup. Neka je $*$ operacija na skupu G za koju vrijedi

(G0) $g_1 * g_2 \in G$ za svaki $g_1, g_2 \in G$.

Tada uređeni par $(G, *)$ skupa i operacije zovemo grupoid. Ako je jasno o kojoj se operaciji radi, često kraće kažemo da je G grupoid.

Svojstvo (G0) nije ništa drugo nego uvjet iz definicije binarne operacije. Stoga se to svojstvo naziva zatvorenost. Zapravo, svaki neprazan skup na kojem je definirana binarna operacija tvore grupoid.

1.3. Polugrupa. Neka je G neprazan skup. Neka je $*$ operacija na skupu G za koju vrijedi

(G0) $g_1 * g_2 \in G$ za svaki $g_1, g_2 \in G$,

(G1) $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$ za svaki $g_1, g_2, g_3 \in G$.

Tada uređeni par $(G, *)$ zovemo polugrupa. Kao i kod grupoida često se kaže samo G je polugrupa, kad je jasno o kojoj se operaciji radi.

1.4. Asocijativnost. Svojstvo (G1) zove se asocijativnost operacije $*$. Stoga je polugrupa zapravo grupoid u kojem vrijedi asocijativnost. Svojstvo asocijativnosti (G1) je napisano za tri elementa iz G. Ono pokazuje da ima smisla pisati $g_1 * g_2 * g_3$, jer neovisno o tome gdje stavimo zagrade dobit ćemo isti element iz G.

Matematičkom indukcijom može pokazati da iz (G1) slijedi da za proizvoljan prirodni broj n ima smisla pisati $g_1 * g_2 * \ldots * g_n$. Točnije, taj izraz ne ovisi o tome gdje stavimo zagrade da bi ga izračunali.

1.5. Monoid. Neka je G neprazan skup. Neka je $*$ operacija na skupu G za koju vrijedi

(G0) $g_1 * g_2 \in G$ za svaki $g_1, g_2 \in G$,
(G1) $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$ za svaki $g_1, g_2, g_3 \in G$,
(G2) Postoji $e \in G$ takav da vrijedi $e * g = g * e = g$ za svaki $g \in G$.

Tada uređeni par $(G, *)$ zovemo monoid. Kaže se samo da je G monoid, kad je jasno o kojoj se operaciji radi.

1.6. Neutralni element. Element $e \in G$ za koji vrijedi svojstvo (G2) zove se neutralni element. Dakle, monoid je zapravo polugrupa u kojoj postoji neutralni element. Lako se pokazuje da ako u polugrupi postoji neutralni element, onda je on jedinstven. Zaista, kad bi postojala dva neutralna elementa e_1 i e_2, onda bi po svojstvu (G2) vrijedilo

$$e_1 * g = g * e_1 = g \text{ za svaki } g \in G,$$

$$e_2 * g = g * e_2 = g \text{ za svaki } g \in G.$$

Ali tada bi vrijedilo

$$e_1 = e_1 * e_2 = e_2,$$

v sto pokazuje da su ta dva neutralna elementa zapravo jednaki. Pritom, prva jednakost $e_1 = e_1 * e_2$ vrijedi zato što je e_2 neutralni element, pa se e_1, kao element iz G ne promjeni kad napravimo operaciju $*$ s e_2. Slično, druga jednakost vrijedi zato što je e_1 neutralni element.

Kako smo sad vidjeli da svaki monoid ima jedinstveni neutralni element, često koristimo oznaku e_G umjesto e kad je potrebno naglasiti monoid u kojem je e neutralni element.

1.7. Grupa. Neka je G neprazan skup. Neka je $*$ operacija na skupu G za koju vrijedi

(G0) $g_1 * g_2 \in G$ za svaki $g_1, g_2 \in G$,
(G1) $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$ za svaki $g_1, g_2, g_3 \in G$,
(G2) Postoji $e \in G$ takav da vrijedi $e * g = g * e = g$ za svaki $g \in G$,
(G3) Za svaki $g \in G$ postoji $g^{-1} \in G$ takav da vrijedi $g * g^{-1} = g^{-1} * g = e$.

Tada uređeni par $(G, *)$ zovemo grupa. Kaže se kratko da je G grupa, kad je jasno o kojoj se operaciji radi.

1.8. Inverzni element. Za svaki $g \in G$, element g^{-1}, čije postojanje osigurava svojstvo (G3), zovemo inverzni element od g ili kraće inverz od g. Dakle, grupa je zapravo monoid u kojem svaki element ima svoj inverz. Pokazuje se da je u monoidu inverz svakog elementa jedinstven, ako postoji. Zaista, pretpostavimo da u monoidu postoje dva inverza g_1 i g_2 nekog elementa g. To znači da vrijedi

$$g * g_1 = g_1 * g = e,$$

$$g * g_2 = g_2 * g = e.$$

Tada vrijedi

$$g_1 = g_1 * e = g_1 * (g * g_2) = (g_1 * g) * g_2 = e * g_2 = g_2,$$

pri čemu smo koristili svojstvo neutralnog elementa, asocijativnost, te pretpostavku da su g_1 i g_2 inverzi od g. Time smo pokazali da je $g_1 = g_2$ pa je inverz jedinstven.

Iz jedinstvenosti inverza svakog elementa slijedi i činjenica da je inverz inverza od g jednak g, odnosno

$$(g^{-1})^{-1} = g.$$

Naime, svojstvo (G3) možemo shvatiti i kao definiciju inverza od g^{-1}. To svojstvo kaže da je g inverz od g^{-1}, pa jedinstvenost inverza daje tvrdnju.

Jedinstvenost inverza pokazuje da vrijedi formula

$$(g_1 * g_2)^{-1} = g_2^{-1} * g_1^{-1}$$

za invertiranje produkta, gdje su $g_1, g_2 \in G$. Zaista, desna strana te jednakosti zadovoljava definiciju inverza od $g_1 * g_2$ jer

$$(g_1 * g_2) * (g_2^{-1} * g_1^{-1}) = (g_2^{-1} * g_1^{-1}) * (g_1 * g_2) = e,$$

pa zbog jedinstvenosti inverza mora vrijediti jednakost. Ova formula se poopćava na invertiranje konaňih produkata, što se može lako dokazati bilo direktno bilo matematiňkom indukcijom.

Neutralni element je sam sebi inverz jer $e * e = e$, pa po definiciji inverza $e^{-1} = e$.

1.9. Komutativnost. Svojstvo komutativnosti

$$g_1 * g_2 = g_2 * g_1 \text{ za svake } g_1, g_2 \in G,$$

može biti ispunjeno u svakoj od dosad definiranih algebarskih struktura (grupoid, polugrupa, monoid, grupa). Ukoliko neka od tih struktura ima svojstvo komutativnosti, onda se naziva komutativna. Tako govorimo o komutativnom grupoidu, komutativnoj polugrupi, komutativnom monoidu, komutativnoj grupi. U slučaju grupe, češće se koristi izraz Abelova grupa kao sinonim za komutativnu grupu.

1.10. Potencije. Neka je $(G, *)$ grupa. Za svaki cijeli broj $n \in \mathbb{Z}$, definiramo potenciju g^n elementa $g \in G$ na sljedeći način. Ako je n pozitivan

$$g^n = \underbrace{g * g * \ldots * g}_{n \text{ puta}},$$

gdje n puta označava da se u izrazu na desnoj strani g pojavljuje n puta (dakle izvrši se $n-1$ operacija). Ako je $n = 0$, onda stavimo

$$g^0 = e,$$

gdje je e neutralni element. Ako je n negativan

$$g^n = \underbrace{g^{-1} * g^{-1} * \ldots * g^{-1}}_{|n| \text{ puta}},$$

gdje je g^{-1} inverz od g, a $|n|$ označava apsolutnu vrijednost. Uočimo da ove definicije imaju smisla jer vrijedi asocijativnost, pa zagrade na desnoj strani nije potrebno pisati.

1.11. Svojstva potencija. S ovako definiranim potencijama u grupi računa se donekle na isti način kao i s uobičajenim potencijama realnih brojeva. Razlika je u tome što u grupi ne mora vrijediti komutativnost pa neke formule ne vrijede. Sljedeće formule vrijede u proizvoljnoj grupi:

$$g^n * g^m = g^{n+m} \text{ za svaki } g \in G \text{ i } n, m \in \mathbb{Z},$$

$$(g^n)^m = g^{nm} \text{ za svaki } g \in G \text{ i } n, m \in \mathbb{Z},$$

gdje su zbrajanje i množenje u eksponentima uobičajene operacije na cijelim brojevima.

Međutim, formula $(g_1 * g_2)^n = g_1^n * g_2^n$ ne vrijedi za nekomutativne grupe. Kao vrlo jednostavan zadatak čitaocu ostavljamo da dokaže da je grupa komutativna ako i samo ako vrijedi $(g_1 * g_2)^2 = g_1^2 * g_2^2$.

1.12. Red grupe, red elementa. Neka je $(G, *)$ grupa. Ako je kardinalni broj (broj elemenata) skupa G konačan, onda se taj broj naziva red grupe i grupu zovemo konačna grupa. Ako je kardinalan broj skupa G beskonačan, onda takvu grupu zovemo beskonačna grupa i tada je red grupe beskonačan. Oznaka za red grupe je $|G|$.

Neka je $g \in G$. Ako postoji pozitivan prirodni broj n takav da vrijedi $g^n = e$, onda se najmanji takav n zove red elementa g. Ako takav n ne postoji, onda kažemo da je red elementa g beskonačan.

U istoj grupi može (ali ne mora) biti elemenata različitog reda, i konačnog i beskonačnog. Neutralni element je uvijek jedini element reda 1. U konačnim grupama svi elementi su konaňog reda, jer u njima u nizu potencija g^n, $n \in \mathbb{N}$, zbog konačnog broja elemenata, mora biti ponavljanja. Stoga postoje $m, l \in \mathbb{N}$ takvi da je $m > l$ i vrijedi $g^m = g^l$. Na obje strane ove relacije dodamo operaciju $*$ s g^{-l}, pa po svojstvima potencija slijedi $g^{m-l} = e$, odnosno g je konačnog reda.

1.13. Podgrupe. Neka je $(G, *)$ grupa i neka je H neprazan podskup od G. Tada kažemo da je H podgrupa od G ako je H grupa uz istu operaciju $*$ kao i u grupi G, odnosno $(H, *)$ zadovoljava svojstva (G0)–(G3) iz definicije grupe. Oznaka za podgrupu je $H \leqslant G$ ili preciznije $(H, *) \leqslant (G, *)$.

Uočimo odmah da neka svojstva nije potrebno provjeravati. Na primjer, ako asocijativnost (svojstvo (G1)) vrijedi za sve elemente čitave grupe G, onda će sigurno vrijediti i za sve elemente iz podskupa H. U ovakvoj situaciji kažemo da se svojstvo asocijativnosti u H naslijeđuje iz grupe G. Komutativnost se također uvijek naslijeđuje. Što se tiče postojanja neutralnog elementa (svojstvo (G2)), ako se neutralni element e grupe G nalazi u podskupu H, onda će e imati svojstvo neutralnog elementa i u H. S druge strane, zatvorenost (svojstvo (G0)) i postojanje inverza (svojstvo (G3)) se ne naslijeđuju.

Svaka grupa G je podgrupa same sebe. Također, jednočlani skup $\{e\}$, koji sadrži samo neutralni element, je podgrupa u svakoj grupi. Ove dvije podgrupe se nazivaju trivijalne podgrupe jer su one podgrupe u svakoj grupi. Sve podgrupe neke grupe koje nisu trivijalne nazivaju se netrivijalne podgrupe. Podgrupa koja čini pravi podskup grupe naziva se prava podgrupa. Dakle, prave podgrupe grupe G su sve podgrupe osim nje same.

1.14. Teorem (kriterij za podgrupe). Neka je $(G, *)$ grupa i H neprazan podskup od G. Tada je H podgrupa od G ako i samo ako je $h_1 * h_2^{-1} \in H$ za svake $h_1, h_2 \in H$.

Dokaz. Ako pretpostavimo da je H podgrupa od G, onda za bilo koje $h_1, h_2 \in H$, prema svojstvu (G3), također je $h_2^{-1} \in H$, pa zatim, prema svojstvu (G0), vrijedi da je $h_1 * h_2^{-1} \in H$.

Obratno, pretpostavimo sada da je $h_1 * h_2^{-1} \in H$ za svake $h_1, h_2 \in H$. Najprije pokažimo da je neutralni element e grupe G u podskupu H. Zaista, budući da je H neprazan skup u njemu postoji barem jedan element $h \in H$. Uvrstimo li h i umjesto h_1 i umjesto h_2 u uvjet $h_1 * h_2^{-1} \in H$, dobivamo

$$e = h * h^{-1} \in H.$$

Svojstvo neutralnosti elementa e u H se naslijeđuje iz G, pa vrijedi svojstvo (G2). Napomenimo da iako još nismo dokazali svojstvo (G3), odnosno da je inverz h^{-1} elementa h unutar

podskupa H, gornji zaključak ima smisla jer u grupi G svaki element ima inverz, pa h^{-1} sigurno postoji unutar G.

Sljedeći korak je upravo dokaz svojstva (G3). Sada kad smo već pokazali da je $e \in H$, možemo za proizvoljni $h \in H$ uvrstiti $h_1 = e$ i $h_2 = h$ u uvjet $h_1 * h_2^{-1} \in H$. Time se dobije

$$h^{-1} = e * h^{-1} \in H,$$

pa je zaista inverz od H unutar H i stoga vrijedi (G3).

Budući da se asocijativnost, odnosno svojstvo (G1) naslijeđuje, preostaje dokazati svojstvo (G0) zatvorenosti. Za proizvoljne $h, h' \in H$ uvrstimo $h_1 = h$ i $h_2 = h'^{-1}$ u uvjet $h_1 * h_2^{-1} \in H$. Tada dobivamo

$$h * h' = h * (h'^{-1})^{-1} \in H,$$

što je upravo uvjet zatvorenosti.

Time smo dokazali da je H podgrupa od G provjerivši svojstva (G0)–(G3) iz definicije grupe. □

Ponekad je, umjesto jednog uvjeta $h_1 * h_2^{-1} \in H$ za svake $h_1, h_2 \in H$, jednostavnije odvojeno provjeriti dva uvjeta $h_1 * h_2 \in H$ za svake $h_1, h_2 \in H$ te $h^{-1} \in H$ za svaki $h \in H$. Jasno je da su ta dva uvjeta ekvivalentna uvjetu iz kriterija.

1.15. Ciklička grupa. Neka je $(G, *)$ grupa i neka je $g \in G$ fiksiran. Tada promatramo skup

$$H = \{\ldots, g^{-3}, g^{-2}, g^{-1}, e, g, g^2, g^3, \ldots\} = \{g^n \mid n \in \mathbb{Z}\}.$$

Prema kriteriju za podgrupe, H je podgrupa od G, jer za $g^m, g^l \in H$ vrijedi

$$g^m * (g^l)^{-1} = g^{m-l} \in H,$$

gdje su m i l proizvoljni cijeli brojevi. Takvu podgrupu H zovemo podgrupa generirana elementom g, a g njenim generatorom. Pišemo

$$H = \langle g \rangle.$$

Uočimo da generator podgrupe ne mora biti jedinstveno određen. Primjerice, g i njegov inverz g^{-1} uvijek generiraju istu podgrupu $\langle g \rangle = \langle g^{-1} \rangle$, a nisu uvijek međusobno jednaki (ostavljamo kao mali zadatak dokaz da je $g = g^{-1}$ ako i samo ako je g reda 2 ili $g = e$).

Grupa G se naziva ciklička grupa ako postoji $g \in G$ za koji vrijedi $G = \langle g \rangle$. Drugim riječima, u cikličkoj grupi postoji element koji ju generira. Budući da je podgrupa od G koja je generirana nekim elementom $g \in G$ ciklička, naziva se još i ciklička podgrupa.

1.16. Lema. Red podgrupe $\langle g \rangle$ jednak je redu svog generatora g.

Dokaz. Ako je red generatora g beskonačan, onda među potencijama g^n, $n \in \mathbb{Z}$, nema jednakih. Naime, kad bi vrijedilo $g^m = g^l$, za neke cijele brojeve $m > l$, onda bi $g^{m-l} = e$, što je u kontradikciji s pretpostavkom da je g beskonačnog reda. Stoga je red grupe $\langle g \rangle$ beskonačan (i pritom prebrojiv). Ako je red generatora g jednak prirodnom broju n, onda je

$$\langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\},$$

jer je $g^n = e$, a među potencijama s manjim eksponentom nema jednakih. Zaista, kad bi $g^m = g^l$, za neke cijele brojeve $n > m > l \geq 0$, onda bi bilo $g^{m-l} = e$ i pritom $m - l < n$,

a to je kontradikcija s minimalnošću iz definicije reda elementa. Dakle, red podgrupe $\langle g\rangle$ je jednak n, što je upravo red od g. □

1.17. Lema. Svaka ciklička grupa je komutativna.

Dokaz. Neka je G ciklička grupa generirana elementom g. Dakle,

$$G = \langle g\rangle = \{g^n \mid n \in \mathbb{Z}\}.$$

Tada, za $m, n \in \mathbb{Z}$ vrijedi

$$g^n * g^m = g^{n+m} = g^{m+n} = g^m * g^n,$$

što pokazuje da proizvoljne potencije od g komutiraju, odnosno G je komutativna. Pritom smo koristili komutativnost zbrajanja cijelih brojeva u eksponentu. □

1.18. Presjek grupa. Neka je $(G, *)$ grupa. Neka je H_j, $j \in J$, familija podgrupa od G, gdje je J proizvoljan skup indeksa. Tada je presjek

$$\bigcap_{j\in J} H_j$$

također podgrupa od G. Drugim riječima, presjek podgrupa je opet podgrupa.

Dokaz. Koristimo kriterij za podgrupe. Neka su $h_1, h_2 \in \cap_{j\in J} H_j$. Po definiciji presjeka skupova, to znači da su $h_1, h_2 \in H_j$ za svaki $j \in J$. Budući da je H_j podgrupa za svaki $j \in J$, vrijedi $h_1 h_2^{-1} \in H_j$ za svaki $j \in J$. Stoga $h_1 h_2^{-1} \in \cap_{j\in J} H_j$, pa je prema kriteriju tvrdnja dokazana. □

1.19. Generiranje grupe. Dosad smo se susreli sa cikličkim grupama koje su generirane jednim elementom. Međutim, grupa općenito može biti generirana s nekim skupom svojih elemenata.

Neka je $(G, *)$ grupa i S neprazan podskup od G. Podgrupa od G generirana skupom S se označava $\langle S\rangle$ i definira kao presjek svih podgrupa od G koje sadrže skup S, odnosno

$$\langle S\rangle = \bigcap_{\substack{H\leqslant G\\ S\subseteq H}} H.$$

Dakle, $\langle S\rangle$ je najmanja (u smislu inkluzije) podgrupa od G koja sadrži skup S. Kažemo da je S skup generatora od G.

Za grupu G kažemo da je konačno generirana ako postoji konačan skup S za koji $G = \langle S\rangle$. Ciklička grupa je u stvari grupa za koju postoji jednočlan skup koji ju generira. Naglasimo da ova tvrdnja nije očigledna, jer naša ranija definicija cikličke grupe ne koristi presjek podgrupa koje sadrže jedan element grupe, već daje eksplicitan opis pomoću potencija. Dokaz da su te dvije definicije ekvivalentne je poseban slučaj sljedeće leme.

1.20. Lema. Neka je $(G, *)$ grupa i S neprazan podskup od G. Tada vrijedi

$$\langle S\rangle = \left\{ s_1 * s_2 * \ldots * s_n \,|\, n \in \mathbb{N},\ s_i \in S \text{ ili } s_i^{-1} \in S \text{ za svaki } i = 1, \ldots, n \right\},$$

odnosno $\langle S\rangle$ se sastoji od svih konačnih "produkata" elemenata skupa S i njihovih inverza (ponavljanja su dozvoljena). Posebno, ako je $S = \{g\}$ jednočlan skup, onda vrijedi

$$\langle\{g\}\rangle = \langle g\rangle = \{g^n \,|\, n \in \mathbb{Z}\}.$$

Dokaz. Svaka podgrupa koja sadrži skup S sadrži i inverze elemenata iz S pa onda i sve konačne produkte elemenata iz S i njihovih inverza, što je upravo desna strana tražene jednakosti. Stoga i presjek svih podgrupa koje sadrže S, a to je po definiciji $\langle S\rangle$, sadrži desnu stranu. Sada ako dokažemo da je skup na desnoj strani podgrupa od G, onda smo dokazali tvrdnju jer podgrupa koja sadrži S ne može biti prava podgrupa u $\langle S\rangle$ zbog uvjeta minimalnosti podgrupe generirane sa S.

Za dokaz da je skup na desnoj strani tražene jednakosti grupa koristimo kriterij. Neka su $s_1 * \ldots * s_n$ i $s_1' * \ldots * s_m'$ dva proizvoljna elementa desne strane. Dakle, $s_i \in S$ ili $s_i^{-1} \in S$ za $i = 1, \ldots, n$, te $s_j' \in S$ ili $s_j'^{-1} \in S$ za $j = 1, \ldots, m$. Tada

$$(s_1 * \ldots * s_n) * (s_1' * \ldots * s_m')^{-1} = s_1 * \ldots * s_n * s_m'^{-1} * \ldots * s_1'^{-1},$$

pri čemu $s_i \in S$ ili $s_i^{-1} \in S$ za $i = 1, \ldots, n$, te $s_j'^{-1} \in S$ ili $s_j' = (s_j'^{-1})^{-1} \in S$ za $j = 1, \ldots, m$. Stoga je taj produkt također element skupa na desnoj strani, pa je prema kriteriju desna strana jednakosti podgrupa od G, što je i trebalo dokazati. □

1.21. Direktni produkt grupa. Neka su $(G, *)$ i $(H, \bullet)$ grupe. Promatramo Kartezijev produkt $G \times H$ skupova G i H. Na njemu se definira operacija $\star$ formulom

$$(g_1, h_1) \star (g_2, h_2) = (g_1 * g_2, h_1 \bullet h_2)$$

za sve $g_1, g_2 \in G$ i $h_1, h_2 \in H$. Tada je $(G \times H, \star)$ grupa.

Dokaz. Ovdje ne možemo primijeniti kriterij jer $G \times H$ nije podskup neke grupe. Stoga treba provjeriti svojstva (G0)–(G3) iz definicije grupe. To slijedi iz odgovarajućih svojstava za grupe G i H.

Za zatvorenost znamo da je $g_1 * g_2 \in G$ i $h_1 \bullet h_2 \in H$, pa je uređeni par $(g_1 * g_2, h_1 \bullet h_2) \in G \times H$. Asocijativnost se dobije iz asocijativnosti u grupama G i H, preciznije

$$\begin{aligned}
\big((g_1, h_1) \star (g_2, h_2)\big) \star (g_3, h_3) &= (g_1 * g_2, h_1 \bullet h_2) \star (g_3, h_3) \\
&= \big((g_1 * g_2) * g_3, (h_1 \bullet h_2) \bullet h_3\big) \\
&= \big(g_1 * (g_2 * g_3), h_1 \bullet (h_2 \bullet h_3)\big) \\
&= (g_1, h_1) \star (g_2 * g_3, h_2 \bullet h_3) \\
&= (g_1, h_1) \star \big((g_2, h_2) \star (g_3, h_3)\big),
\end{aligned}$$

za sve $g_1, g_2, g_3 \in G$, $h_1, h_2, h_3 \in H$. Neutralni element u $G \times H$ je $e = (e_G, e_H)$, gdje su e_G i e_H neutralni elementi u grupama G i H, respektivno. Zaista,

$$(e_G, e_H) \star (g, h) = (e_G * g, e_H \bullet h) = (g, h),$$

$$(g, h) \star (e_G, e_H) = (g * e_G, h \bullet e_H) = (g, h),$$

za sve $g \in G$, $h \in H$. Inverz $(g,h)^{-1}$ elementa $(g,h) \in G \times H$ jednak je (g^{-1}, h^{-1}), gdje su g^{-1} i h^{-1} inverzi u grupama G i H, respektivno. Zaista,

$$(g,h) \star (g^{-1}, h^{-1}) = (g * g^{-1}, h \bullet h^{-1}) = (e_G, e_H),$$

$$(g^{-1}, h^{-1}) \star (g,h) = (g^{-1} * g, h^{-1} \bullet h) = (e_G, e_H).$$

□

2. Primjeri grupa

2.1. Aditivne algebarske strukture brojeva. Neka je $\mathbb{N}$, $\mathbb{N}_0$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, redom, skup prirodnih brojeva (to su pozitivni cijeli brojevi), skup prirodnih brojeva i nule, skup cijelih brojeva, skup racionalnih brojeva (razlomaka), skup realnih brojeva, skup kompleksnih brojeva. Na svim tim skupovima definiramo uobičajenu operaciju zbrajanja brojeva koju označavamo s $+$. Odredimo koju od dosad definiranih algebarskih struktura tvore ti skupovi s operacijom zbrajanja.

Najprije uočimo da zbrajanjem bilo koja dva prirodna broja opet dobivamo prirodan broj, zbrajanjem dva prirodna broja ili nule opet dobivamo prirodan broj ili nulu... Isto vrijedi i za zbrajanje cijelih, racionalnih, realnih i kompleksnih brojeva. Dakle, svi ovi skupovi brojeva su zatvoreni za operaciju zbrajanja, odnosno operacija zbrajanja na njima zadovoljava svojstvo zatvorenosti (G0).

Dobro je poznato da za zbrajanje u svim ovim skupovima brojeva vrijedi asocijativnost. Dakle, za sve ove skupove operacija zbrajanja zadovoljava svojstvo (G1).

Jedina mogućnost za neutralni element za operaciju zbrajanja brojeva jest nula, jer je to jedini broj koji ima svojstvo da zbrojen s bilo kojim brojem daje taj broj. Uočimo da skup $\mathbb{N}$ ne sadrži nulu. Stoga, skup $\mathbb{N}$ s operacijom zbrajanja zadovoljava svojstva (G0) i (G1), ali nema neutralni element, pa je $(\mathbb{N}, +)$ polugrupa. Ostali promatrani skupovi brojeva sadrže nulu, pa je za njih svojstvo (G2) ispunjeno za zbrajanje, a neutralni element $e = 0$.

Jedina mogućnost za inverz nekog broja obzirom na operaciju zbrajanja jest njemu suprotan broj, jer oni zbrojeni daju nulu, što je neutralni element. Međutim, skup $\mathbb{N}_0$ ne sadrži negativne brojeve, pa stoga, svi njegovi pozitivni brojevi nemaju inverza. Jedini broj u $\mathbb{N}_0$ koji ima inverz jest 0 i to njegov inverz je on sam. Dakle, $\mathbb{N}_0$ ne zadovoljava svojstvo (G3) za operaciju zbrajanja, ali zadovoljava, kao što smo vidjeli, svojstva (G0), (G1) i (G2), pa je $(\mathbb{N}_0, +)$ monoid. U preostalim skupovima suprotni broj svakog broja je ponovo u promatranom skupu. Primjerice, suprotan broj cijelog broja je opet cijeli broj, suprotan broj razlomka je opet razlomak, i slično za ostale skupove. Dakle, za te skupove operacija zbrajanja zadovoljava svojstvo (G3), pa su $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ grupe.

Sve dobivene algebarske strukture brojeva su komutativne jer znamo da za zbrajanje brojeva vrijedi komutativnost. Tako je $(\mathbb{N}, +)$ komutativna polugrupa, $(\mathbb{N}_0, +)$ komutativni monoid, te $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ komutativne grupe.

Sve ove grupe su beskonačnog reda jer imaju beskonačno mnogo elemenata. Također, svi elementi osim neutralnog, a to je nula, su beskonačnog reda, jer niti jedan broj različit od nule ne može dati nulu zbrajajući ga samog sa sobom.

Grupa $(\mathbb{Z}, +)$ je ciklička, jer primjerice, broj 1 zbrojen sam sa sobom daje sve pozitivne cijele brojeve, a njegov inverz -1 zbrojen sam sa sobom daje sve negativne cijele brojeve, dok je nula neutralni element. Dakle, ciklička podgrupa generirana elementom 1 je cijela

grupa $(\mathbb{Z}, +)$, odnosno

$$\mathbb{Z} \cong \langle 1 \rangle.$$

Osim broja 1, generator grupe $\mathbb{Z}$ je i -1 kao njegov inverz. To su jedini generatori. Ostali cijeli brojevi generiraju cikličke podgrupe koje nisu jednake cijeloj grupi $\mathbb{Z}$. Primjerice, broj 2, kao i njegov inverz -2 generira podgrupu $2\mathbb{Z}$ koja se sastoji od parnih cijelih brojeva, broj 3, kao i -3, generira podgrupu $3\mathbb{Z}$ koja se sastoji od svih cijelih brojeva djeljivih s 3, i tako dalje.

Može se pokazati da su sve podgrupe grupe cijelih brojeva $(\mathbb{Z}, +)$ cikličke i to oblika $m\mathbb{Z}$ za neki $m \in \mathbb{Z}$. Zaista, trivijalna podgrupa $\{0\}$ se dobije kao $0\mathbb{Z}$. Ako je H podgrupa različita od $\{0\}$, onda u njoj postoji barem jedan pozitivni cijeli broj. Odaberimo $m \in H$ kao najmanji takav broj. Kako je $m \in H$, podgrupa $m\mathbb{Z}$ generirana tim m je podgrupa od H. Pokažimo sada i drugu inkluziju, odnosno da je H podgrupa od $m\mathbb{Z}$. Neka je $x \in H$. Zapišimo cijeli broj x u obliku $x = qm + r$, gdje su $q \in \mathbb{Z}$ i $r \in \{0, 1, \ldots, m-1\}$ kvocijent i ostatak pri dijeljenju x sa m. Uočimo da qm nije ništa drugo nego broj m zbrojen sam sa sobom q puta. Kako je $m \in H$, slijedi da je i $qm \in H$. Također je i $x \in H$. Dakle,

$$r = x - qm \in H.$$

Ali $r < m$, a m je minimalni pozitivni element iz H. Stoga mora biti $r = 0$, pa je $x = qm \in m\mathbb{Z}$. Time je dokazano da je podgrupa H upravo jednaka $m\mathbb{Z}$.

Postavlja se pitanje što je s oduzimanjem. Operacija oduzimanja ispunjava puno manje svojstava nego operacija zbrajanja. Zapravo se oduzimanje može promatrati kao dodavanje suprotnog elementa. Primjerice, $2 - 3 = 2 + (-3)$ je zbroj broja 2 i inverza broja 3. Ako se ipak pitamo koju algebarsku strukturu tvore promatrani skupovi brojeva obzirom na oduzimanje, $(\mathbb{N}, -)$ i $(\mathbb{N}_0, -)$ nisu niti grupoidi, jer oduzimanjem većeg prirodnog broja od manjeg dobijemo negativan cijeli broj koji nije u tim skupovima. Preostali skupovi $(\mathbb{Z}, -)$, $(\mathbb{Q}, -)$, $(\mathbb{R}, -)$, $(\mathbb{C}, -)$ jesu grupoidi, ali ništa više od toga, jer za oduzimanje ne vrijedi asocijativnost.

2.2. Multiplikativne algebarske strukture brojeva. Promotrimo sada iste skupove brojeva kao u prethodnom primjeru, ali uz uobičajenu operaciju množenja brojeva, koju označavamo $\cdot$. Pitamo se koje algebarsku strukture dobivamo.

Najprije uočimo da množenjem prirodnih brojeva dobivamo prirodan broj, množenjem prirodnih brojeva ili nule opet dobivamo takav broj. Isto vrijedi i za cijele brojeve, razlomke, realne te kompleksne brojeve. Stoga je za množenje u svim promatranim skupovima brojeva ispunjen uvjet zatvorenosti (G0).

Isto tako, dobro je poznato da za množenje brojeva vrijedi asocijativnost. Stoga svi skupovi brojeva zadovoljavaju svojstvo (G1) za množenje.

Jedini mogući neutralni element za množenje je broj 1. Budući da svi promatrani skupovi sadrže broj 1, svi imaju neutralni element za množenje, pa zadovoljavaju svojstvo (G2).

Inverz za množenje nekog broja je njemu recipročan broj, ali uz uvjet da je sam broj različit od nule. Naime, nula nema inverz za množenje jer vrijedi $0 \cdot x = x \cdot 0 = 0$ za svaki broj x, pa ne može postojati broj x takav da je $0 \cdot x = x \cdot 0 = 1$. Time odmah vidimo da promatrani skupovi koji sadrže nulu ne zadovoljavaju svojstvo (G3). Jedini među tim skupovima koji ne sadrži nulu jest skup prirodnih brojeva $\mathbb{N}$. Ali ni on ne zadovoljava svojstvo (G3) za množenje, jer primjerice inverz prirodnog broja 2 bi trebao biti njemu recipročan broj $1/2$ koji ne pripada skupu $\mathbb{N}$. Dakle, svi promatrani skupovi, $(\mathbb{N}, \cdot)$, $(\mathbb{N}_0, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$,

$(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$, uz operaciju množenja tvore monoid. Svi ti monoidi su komutativni jer znamo da za množenje vrijedi komutativnost.

2.3. Grupa invertibilnih elemenata monoida. Možemo se dalje pitati koliko su multiplikativni monoidi brojeva daleko od toga da budu grupe. Drugim riječima, koji elementi tih monoida imaju inverz za množenje. Općenito se takvi elementi monoida zovu invertibilni. Ako je $(M, *)$ bilo koji monoid, skup njegovih invertibilnih elemenata se označava s $M^\times$. Što je skup $M^\times$ veći, to je M bliže tome da bude grupa jer je više njegovih elemenata invertibilno.

Može se općenito pokazati da je u svakom monoidu $(M, *)$ skup $M^\times$ obzirom na operaciju $*$ grupa. Zaista, ako su $h_1, h_2 \in M^\times$, onda je i $h_1 * h_2 \in M^\times$ jer je $h_2^{-1} * h_1^{-1} \in M$ inverz od $h_1 * h_2$. Stoga vrijedi uvjet zatvorenosti (G0) za $M^\times$. Svojstvo asocijativnosti (G1) se uvijek nasljeđuje. Neutralni element u monoidu je uvijek invertibilan jer je on sam sebi inverz. Stoga je i svojstvo (G2) ispunjeno za $M^\times$. Na kraju, ako je $h \in M^\times$, onda postoji njegov inverz $h^{-1} \in M$. Ali tada je i $h^{-1} \in M^\times$, jer je h njegov inverz. Time smo dokazali da vrijedi i svojstvo (G3). Dakle, zaista je $M^\times$ grupa.

2.4. Multiplikativne grupe brojeva. Primjenimo sad tu činjenicu na monoide brojeva obzirom na množenje. Za monoide $(\mathbb{N}, \cdot)$ i $(\mathbb{N}_0, \cdot)$ jedini invertibilni element je broj 1 koji je neutralni element za množenje. Recipročne vrijednosti svih ostalih prirodnih brojeva su razlomci, a ne prirodni brojevi. Stoga je u ova dva monoida grupa invertibilnih elemenata trivijalna. Za monoid cijelih brojeva $(\mathbb{Z}, \cdot)$, osim neutralnog elementa broja 1, invertibilan je i -1 jer je i on sam sebi inverz. Ostali cijeli brojevi nisu invertibilni jer bi njihovi inverzi trebali biti razlomci koji nisu cijeli brojevi. Dakle

$$\mathbb{Z}^\times = \{1, -1\}$$

je grupa invertibilnih elemenata u monoidu $(\mathbb{Z}, \cdot)$.

U preostalim monoidima, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$, situacija je puno bolja. U njima su svi elementi različiti od nule invertibilni. Zaista, ako je $x \neq 0$ razlomak, onda je njemu recipročan broj $1/x$ također razlomak, ako je realan broj, onda je $1/x$ realan, a ako je kompleksan onda je $1/x$ kompleksan. Dakle, skupovi invertibilnih elemenata su jednaki $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$ i tvore grupe $(\mathbb{Q}^\times, \cdot)$, $(\mathbb{R}^\times, \cdot)$, $(\mathbb{C}^\times, \cdot)$ obzirom na množenje.

2.5. Aditivne grupe ostataka. U ovom primjeru vidjet ćemo da postoje konačne grupe svakog reda. Fiksirajmo jedan prirodan broj $m \geq 2$ i promatramo skup ostataka koji se dobivaju pri dijeljenju cijelih brojeva s m. Taj skup ostataka označavamo sa $\mathbb{Z}_m$. Dakle,

$$\mathbb{Z}_m = \{0, 1, \ldots, m-1\}.$$

Na tom skupu definiramo operaciju $+_m$ zbrajanja modulo m. Ta operacija je za $a, b \in \mathbb{Z}_m$ definirana kao ostatak pri dijeljenju zbroja $a + b$ s m.

Jasno je da je skup $\mathbb{Z}_m$ zatvoren za tu operaciju jer je po samoj definiciji rezultat izvršavanja operacije ostatak pri dijeljenju s m, a to su elementi od $\mathbb{Z}_m$. Stoga je ispunjeno svojstvo (G0).

Asocijativnost operacije $+_m$ na skupu $\mathbb{Z}_m$ se može direktno provjeriti razmatrajući ostatke. Međutim, mi to sad nećemo napraviti jer ćemo u sljedećoj sekciji vidjeti kako asocijativnost, a i sva ostala svojstva grupe, elegantno slijede iz odgovarajućih svojstava zbrajanja

cijelih brojeva. Dakle, za sada uzmimo kao poznato da za $+_m$ na skupu $\mathbb{Z}_m$ vrijedi svojstvo (G1) asocijativnosti.

Kao i kod brojeva, neutralni element za zbrajanje $+_m$ je 0. Naime, 0 je neutralni element za obično zbrajanje cijelih brojeva, a operacija $+_m$ je definirana kao ostatak pri dijeljenju običnog zbroja s m. Stoga, ako 0 ne promijeni broj pri običnom zbrajanju, onda ga ne može promijeniti niti pri $+_m$. Dakle, svojstvo (G2) je ispunjeno za operaciju $+_m$.

Na kraju, provjerimo da svaki ostatak iz $\mathbb{Z}_m$ ima inverz obzirom na operaciju $+_m$. Obzirom da je 0 neutralni element, ona je sama sebi inverz. Za ostatke veće od nula, inverz pri običnom zbrajanju bio bi suprotan broj, ali on nije inverz za $+_m$ jer nije unutar skupa $\mathbb{Z}_m$. Ali umjesto suprotnog broja, možemo se pitati koliko fali ostatku $a \neq 0$ iz skupa $\mathbb{Z}_m$ da postane djeljiv s m. Naime, brojevi djeljivi s m daju ostatak nula pri djeljenju, a to je upravo neutralni element. Ostatku a do m fali točno $m - a$, pa vrijedi

$$a +_m (m - a) = 0$$

jer $a + (m - a) = m$. Pritom je $m - a \in \mathbb{Z}_m$ jer smo pretpostavili $a \neq 0$. Zaključujemo da svi elementi iz $\mathbb{Z}_m$ imaju inverz obzirom na operaciju $+_m$ i on je jednak

$$a^{-1} = \begin{cases} 0, & \text{za } a = 0, \\ m - a, & \text{za } a \neq 0. \end{cases}$$

Dakle, ispunjeno je i svojstvo (G3). Time smo dokazali da je $(\mathbb{Z}_m, +_m)$ grupa. Budući da je operacija $+_m$ definirana preko običnog zbrajanja koje je komutativno, jasno je da je i $+_m$ komutativna, pa je $(\mathbb{Z}_m, +_m)$ komutativna grupa.

Grupa $(\mathbb{Z}_m, +_m)$ je konačna i njen red je upravo jednak m. To pokazuje da za svaki prirodan broj $m \geq 2$ postoji grupa reda m. Grupa reda 1 također postoji. To je trivijalna grupa koja se sastoji samo od neutralnog elementa.

Možemo se dalje pitati koliki je red elemenata grupe $\mathbb{Z}_m$. To je najmanji broj koliko puta moramo neki ostatak zbrojiti sam sa sobom da dobijemo broj djeljiv s m, jer taj broj onda daje ostatak nula pri djeljenju s m, a nula je upravo neutralni element. Za nulu red je 1 jer neutralni element uvijek ima red 1 (i to je jedini takav element). Neka je $a \neq 0$ iz $\mathbb{Z}_m$. Označimo s $d = NZD(a, m)$ najveći zajednički djelitelj od a i m. Neka je $a' = a/d$ i $m' = m/d$. Tada, ako a zbrojimo sam sa sobom m' puta, dobivamo

$$m' \cdot a = \frac{m}{d} \cdot a = m \cdot \frac{a}{d} = m \cdot a',$$

što je djeljivo s m. Pokažimo da je m' najmanji prirodni broj s tim svojstvom. Kad bi za prirodni broj $k < m'$ vrijedilo da je $k \cdot a$ djeljivo s m, onda bi dobili da je

$$k \cdot a = k \cdot a' \cdot d = k \cdot a' \cdot \frac{m}{m'} = \frac{k \cdot a'}{m'} \cdot m$$

djeljivo s m. To bi značilo da je razlomak $\frac{k \cdot a'}{m'}$ zapravo cijeli broj, odnosno m' dijeli $k \cdot a'$. Kako su a' i m' relativno prosti jer su dobiveni dijeljenjem a i m s najvećim zajedničkim djeliteljem, ispalo bi da m' dijeli k. Ali to je nemoguće jer je k prirodan broj i $k < m'$. Dakle, dokazali smo da je red elementa $a \neq 0$ iz $\mathbb{Z}_m$ jednak m', a to je zapravo

$$\frac{m}{NZD(a, m)},$$

gdje je $NZD(a, m)$ najveći zajednički djelitelj od a i m.

Grupa $\mathbb{Z}_m$ je ciklička. Naime, iz upravo dokazane formule za red elementa vidimo da je za ostatke a koji su relativno prosti s m red jednak upravo m. To znači da je red cikličke podgrupe generirane takvim ostatkom a jednak m, a to je red čitave grupe $\mathbb{Z}_m$. Stoga je ta podgrupa jednaka $\mathbb{Z}_m$. Dakle, vrijedi

$$\mathbb{Z}_m = \langle a \rangle$$

za svaki ostatak a relativno prost s m, odnosno takav da je $NZD(a, m) = 1$. Uočimo da takvi ostaci uvijek postoje jer vrijedi $NZD(1, m) = 1$ i $NZD(m - 1, m) = 1$ za svaki prirodan broj $m \geq 2$. Ako je, primjerice, m prost broj, onda su svi ostaci osim nule relativno prosti s m, pa su svi oni generatori čitave grupe $\mathbb{Z}_m$.

Promotrimo za kraj malo detaljnije slučaj $m = 6$, odnosno grupu $(\mathbb{Z}_6, +_6)$. U njoj su redovi elemenata sljedeći: 0 je reda 1, 1 i 5 su reda 6, 2 i 4 su reda 3, te 3 je reda 2. Kako su i sve podgrupe cikličke grupe i same cikličke, iz toga možemo lako napisati sve podgrupe grupe $\mathbb{Z}_6$. Neutralni element 0 generira trivijalnu podgrupu $\{0\}$, a 1 i 5 generiraju čitavu grupu $\mathbb{Z}_6$. Elementi 2 i 4 generiraju istu podgrupu $\{0, 2, 4\}$ koja je, naravno, reda 3. Element 3 generira podgrupu $\{0, 3\}$ reda 2.

2.6. Uvjet "dvije zvjezdice" $(**)$**.** Sad ćemo detaljno proučiti odnos između strukture grupe na nekom nepraznom skupu i relacije ekvivalencije na tom istom skupu. Preciznije, zanima nas može li se, koristeći operaciju grupe, na neki način definirati operacija na novom skupu koji se sastoji od klasa ekvivalencije polaznog skupa obzirom na danu relaciju ekvivalencije.

Odgovor na to važno pitanje daje elegantan dokaz da je $(\mathbb{Z}_m, +_m)$ grupa, posebno pokazuje asocijativnost koju smo u gornjem razmatranju preskočili. Isto tako primjenjuje se i u proučavanju multiplikativnih algebarskih struktura ostataka u nastavku. Međutim, to nisu jedine primjene. Nama će od posebne važnosti biti primjena na određivanje definicije normalne podgrupe i odgovarajuće kvocijentne grupe.

Neka je $*$ binarna operacija definirana na nepraznom skupu G. Drugim riječima, neka je $(G, *)$ grupoid. Neka je $\sim$ relacija ekvivalencije na skupu G. Za $g \in G$, označimo s $[g]$ klasu ekvivalencije tog elementa obzirom na relaciju $\sim$. Neka je $G/_\sim$ skup svih klasa ekvivalencije skupa G obzirom na relaciju $\sim$. Cilj je, na neki način, definirati ili bolje rečeno prenijeti operaciju $*$ na skup $G/_\sim$ klasa ekvivalencije. Jedini razuman pokušaj za to napraviti u ovako općenitoj situaciji jest definirati operaciju pomoću predstavnika klasa. Točnije, za klase $[g_1], [g_2] \in G/_\sim$, pokušaj definiranja operacije $*_\sim$ na $G/_\sim$ bio bi

$$[g_1] *_\sim [g_2] = [g_1 * g_2].$$

Pritom smo operaciju na klasama označili s $*_\sim$ da naglasimo relaciju $\sim$ pomoću koje smo definirali klase. U primjenama kod kojih je jasno o kojoj se relaciji radi ta oznaka se ispušta i naprosto se ponovo koristi ista oznaka $*$ kao i za polaznu operaciju na G.

Ovaj pokušaj definiranja operacije $*_\sim$ na $G/_\sim$ nije uvijek dobar. Naime, desna strana definicije ovisi o tome koje smo predstavnike g_1 i g_2 za klase $[g_1]$ i $[g_2]$ izabrali. Može se desiti da se promjenom tih predstavnika na desnoj strani dobije sasvim druga klasa ekvivalencije. To bi značilo da $[g_1] *_\sim [g_2]$ nije jednoznačno definirana.

Sada ćemo proučiti kakav mora biti odnos operacije $*$ i relacije $\sim$ da bi gornja definicija operacije $*_\sim$ bila dobra. Pitamo se što se dešava kad promijenimo predstavnike klasa. Neka su g_1 i g_1' dva predstavnika iste klase $[g_1]$, a g_2 i g_2' dva predstavnika iste klase $[g_2]$. To znači

da je $g_1 \sim g_1'$ i $g_2 \sim g_2'$. Da bi definicija operacije $[g_1] *_\sim [g_2]$ bila dobra, klasa dobivena na desnoj strani ne smije ovisiti o odabiru predstavnika. Drugim riječima, klasa $[g_1 * g_2]$ i klasa $[g_1' * g_2']$ moraju biti jedna te ista klasa. To znači da mora vrijediti $g_1 * g_2 \sim g_1' * g_2'$. Time smo došli do uvjeta koji osigurava da je definicija operacije $*_\sim$ dobra. Taj uvjet je sljedeći:

(**) ako za $g_1, g_1', g_2, g_2' \in G$ vrijedi $g_1 \sim g_1'$ i $g_2 \sim g_2'$, onda vrijedi i $g_1 * g_2 \sim g_1' * g_2'$.

Zbog važnosti ovog uvjeta dajemo mu posebno ime, a to je uvjet dvije zvjezdice ili kratko uvjet (**) (jedna zvjezdica $*$ je već potrošena kao oznaka operacije).

2.7. Prenos svostava operacije na klase. Pretpostavimo sada da su na istom nepraznom skupu G definirane binarna operacija $*$ i relacija ekvivalencije $\sim$ takve da je uvjet (**) ispunjen. To znači da je operacija $*_\sim$ na skupu $G/_\sim$ klasa ekvivalencije dobro definirana. Dakle, ako je $(G, *)$ grupoid, onda je i $(G/_\sim, *_\sim)$ grupoid. Možemo reći da se svojstvo zatvorenosti (G0) operacije $*$ prenosi s G na $G/_\sim$.

Ispostavlja se da se i sva ostala svojstva operacije $*$ iz definicije grupe te komutativnost prenose s G na $G/_\sim$. Ako za operaciju $*$ na G vrijedi svojstvo asocijativnosti (G1), onda isto vrijedi i za operaciju $*_\sim$ na $G/_\sim$ jer

$$([g_1]*_\sim[g_2])*_\sim[g_3] = [g_1*g_2]*_\sim g_3 = [(g_1*g_2)*g_3] = [g_1*(g_2*g_3)] = [g_1]*_\sim[g_2*g3] = [g_1]*_\sim([g_2]*_\sim[g_3])$$

za sve klase $[g_1], [g_2], [g_3] \in G/_\sim$. Pritom smo koristili asocijativnost operacije $*$ na predstavnicima klasa i formulu za operaciju $*_\sim$.

Svojstvo postojanja neutralnog elementa (G2) se prenosi jer vrijedi

$$[e] *_\sim [g] = [e * g] = [g],$$

$$[g] *_\sim [e] = [g * e] = [g],$$

za sve klase $[g] \in G/_\sim$, gdje je $[e] \in G/_\sim$ klasa čiji predstavnik je neutralni element $e \in G$. Pritom smo koristili svojstvo (G2) za operaciju $*$ i formulu za operaciju $*_\sim$. Može se reći da je neutralni element u $G/_\sim$ klasa neutralnog elementa iz G.

Svojstvo (G3) se prenosi jer se inverz klase $[g] \in G/_\sim$ dobiva po formuli

$$[g]^{-1} = [g^{-1}],$$

gdje je g^{-1} inverz elementa g obzirom na operaciju $*$. Naime, vrijedi

$$[g] *_\sim [g^{-1}] = [g * g^{-1}] = [e],$$

$$[g^{-1}] *_\sim [g] = [g^{-1} * g] = [e],$$

što potvrđuje da je $[g^{-1}]$ inverz od $[g]$. Pritom smo koristili svojstvo (G3) za inverze u G i definiciju operacije $*_\sim$. Može se kratko reći da je inverz klase jednak klasi inverza.

Komutativnost se također prenosi jer vrijedi

$$[g_1] *_\sim [g_2] = [g_1 * g_2] = [g_2 * g_1] = [g_2] *_\sim [g_1]$$

za sve klase $[g_1], [g_2] \in G/_\sim$. Pritom smo koristili komutativnost operacije $*$ na G i definiciju operacije $*_\sim$.

2.8. Aditivne grupe ostataka kao grupe klasa ekvivalencije. Kao ilustraciju korištenja uvjeta (∗∗), primjenimo ga na primjeru grupe $(\mathbb{Z}, +)$ s operacijom zbrajanja i relacije "biti kongruentan modulo m" za prirodni broj $m \geq 2$.

Podsjetimo da je relacija kongruencije $\equiv \mod m$ definirana na skupu cijelih brojeva kao

$$a \equiv b \mod m \quad \text{ako je} \quad a - b \text{ djeljivo s } m.$$

Uočimo da je razlika dva cijela broja djeljiva s m ako i samo ako ta dva broja imaju isti ostatak pri dijeljenju s m. Koristeći ovu karakterizaciju lako se vidi da je relacija kongruencije modulo m zaista relacija ekvivalencije. Naime, relacija je refleksivna jer a i a daju isti ostatak pri djeljenju s m, simetrična jer ako a i b daju isti ostatak pri dijeljenju s m, onda i b i a daju isti ostatak, te tranzitivna jer ako a daje isti ostatak kao b pri dijeljenju s m, a b daje isti ostatak kao c, onda a daje isti ostatak kao i c.

Sada kad znamo da je relacija kongruencije relacija ekvivalencije, jasno je da jednu klasu ekvivalencije tvore svi cijeli brojevi koji daju isti ostatak pri dijeljenju s m. Stoga kao predstavnike klasa možemo izabrati same ostatke. Dobivamo skup klasa ekvivalencije

$$\mathbb{Z}/_{\equiv \mod m} = \{[0], [1], \ldots, [m-1]\}.$$

Za prenos operacije zbrajanja sa $\mathbb{Z}$ na $\mathbb{Z}/_{\equiv \mod m}$, moramo provjeriti da operacija $+$ i relacija $\equiv \mod m$ zadovoljavaju uvjet (∗∗). Zapisan u ovom konkretnom slučaju uvjet (∗∗) glasi

(∗∗) ako za $a, a', b, b' \in \mathbb{Z}$ vrijedi $a \equiv a' \mod m$ i $b \equiv b' \mod m$, onda vrijedi i $a + b \equiv a' + b' \mod m$.

Ali taj uvjet vrijedi jer je to zapravo dobro poznata činjenica da kongruencije možemo zbrajati. To se i odmah lako vidi jer ako su $a - a'$ i $b - b'$ djeljivi s m, onda je i

$$(a + b) - (a' - b') = (a - a') + (b - b')$$

također djeljivo s m.

Dakle, uvjet (∗∗) vrijedi pa možemo operaciju zbrajanja prenijeti sa $\mathbb{Z}$ na $\mathbb{Z}/_{\equiv \mod m}$. Prenesena operacija, koju i dalje označavamo s $+$, se dobije kao i u općenitoj situaciji preko predstavnika klasa. To znači da je

$$[a] + [b] = [a + b]$$

za klase ostataka $[a], [b] \in \mathbb{Z}/_{\equiv \mod m}$. Kako je $(\mathbb{Z}, +)$ komutativna grupa, a pri prenosu operacije čuvaju se svojstva iz definicije grupe, zaključujemo da je i $(\mathbb{Z}/_{\equiv \mod m}, +)$ komutativna grupa.

Na kraju uočimo da je dobivena grupa zapravo $(\mathbb{Z}_m, +_m)$. Zaista, ako klasu $[r] \in \mathbb{Z}/_{\equiv \mod m}$ identificiramo s ostatkom $r \in \mathbb{Z}_m$, vidimo da se elementi podudaraju. Operacija zbrajanja definirana na klasama iz $\mathbb{Z}/_{\equiv \mod m}$ podudara se s operacijom $+_m$ jer je klasa $[a + b]$ jednaka klasi $[r]$ gdje je $r \in \mathbb{Z}_m$ ostatak pri dijeljenju zbroja $a + b$ s m. Dakle, ako grupu $(\mathbb{Z}/_{\equiv \mod m}, +)$ shvatimo kao grupu ostataka $(\mathbb{Z}_m, +_m)$ preko ove identifikacije, onda sve upravo dokazano vrijedi za operaciju $+_m$ na skupu $\mathbb{Z}_m$.

Na ovaj način smo dokazali da je $(\mathbb{Z}_m, +_m)$ komutativna grupa koristeći općeniti rezultat o prenosu operacije s grupe na klase ekvivalencije. To ujedno zamjenjuje sve dokaze koje smo ranije napravili za $\mathbb{Z}_m$, te pokazuje asocijativnost operacije $+_m$ koju nismo ranije dokazali.

2.9. Multiplikativne algebarske strukture ostataka. Ovaj primjer proučava multiplikativnu algebarsku strukturu skupa ostataka pri djeljenju s m. Neka je i dalje

$$\mathbb{Z}_m = \{0, 1, \ldots, m-1\},$$

ali sada na njemu promatramo operaciju $\cdot_m$ množenja modulo m. Za $a, b \in \mathbb{Z}_m$ definiramo $a \cdot_m b$ kao ostatak pri dijeljenju produkta $a \cdot b$ s m.

Kao što smo već vidjeli, skup $\mathbb{Z}_m$ možemo promatrati kao skup

$$\mathbb{Z}/_{\equiv \mod m} = \{[0], [1], \ldots, [m-1]\}$$

klasa ekvivalencije za relaciju $\equiv \mod m$ na skupu cijelih brojeva $\mathbb{Z}$. S druge strane, znamo da je $(\mathbb{Z}, \cdot)$ monoid za operaciju množenja. Za prenos operacije množenja sa $\mathbb{Z}$ na $\mathbb{Z}/_{\equiv \mod m}$ treba provjeriti je li uvjet $(**)$ ispunjen za operaciju $\cdot$ i relaciju $\equiv \mod m$. U toj konkretnoj situaciji uvjet $(**)$ glasi

$(**)$ ako za $a, a', b, b' \in \mathbb{Z}$ vrijedi $a \equiv a' \mod m$ i $b \equiv b' \mod m$, onda vrijedi i $a \cdot b \equiv a' \cdot b' \mod m$.

Taj uvjet je ispunjen jer kongruencije smijemo množiti. To se može lako provjeriti jer ako su $a - a'$ i $b - b'$ djeljivi s m, onda je

$$a \cdot b - a' \cdot b' = a \cdot b - a' \cdot b + a' \cdot b - a' \cdot b' = (a - a') \cdot b + a' \cdot (b - b')$$

također djeljivo s m. Prenosom operacije množenja dobivamo operaciju na $\mathbb{Z}/_{\equiv \mod m}$, koju i dalje označavamo $\cdot$, danu formulom

$$[a] \cdot [b] = [a \cdot b]$$

za $[a], [b] \in \mathbb{Z}/_{\equiv \mod m}$. Ta operacija se zapravo podudara s operacijom $\cdot_m$ na skupu $\mathbb{Z}_m$ jer je predstavnik klase $[a \cdot b]$ ostatak pri dijeljenju produkta $a \cdot b$ s m, a to je upravo $a \cdot_m b$.

Stoga sva svojstva operacije množenja na skupu $\mathbb{Z}$ vrijede i za operaciju $+_m$ na skupu $\mathbb{Z}_m$. Kako je $(\mathbb{Z}, \cdot)$ komutativni monoid, zaključujemo da je i $(\mathbb{Z}_m, \cdot_m)$ komutativni monoid. Neutralni element je $1 \in \mathbb{Z}_m$, odnosno klasa $[1]$, jer je to klasa neutralnog elementa iz $(\mathbb{Z}, \cdot)$. Međutim, $(\mathbb{Z}_m, \cdot_m)$ nije grupa jer $0 \in \mathbb{Z}_m$ ne može imati inverz budući da je

$$0 \cdot_m a = a \cdot_m 0 = 0$$

za svaki $a \in \mathbb{Z}_m$.

2.10. Multiplikativne grupe ostataka za $m = p$ prost. Ako želimo promatrati multiplikativne grupe ostataka, moramo sa monoida $(\mathbb{Z}_m, \cdot_m)$ preći na grupu invertibilnih elemenata. Vidjeli smo već da $0 \in \mathbb{Z}_m$ nikad nije invertibilna. Za ostale elemente promatramo odvojeno slučaj kad je m jednak prostom broju p i slučaj kad je m složen broj.

Ako je $m = p$ prost broj, onda su u monoidu $(\mathbb{Z}_p, \cdot_p)$ svi elementi različiti od nule invertibilni. Zaista, ako je $a \neq 0$ iz $\mathbb{Z}_p$, onda su a i p relativno prosti jer je p prost broj. Mali Fermatov teorem iz elementarne teorije brojeva kaže da za prost broj p i cijeli broj a relativno prost s p vrijedi

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

To znači da je za $a \neq 0$ iz $\mathbb{Z}_p$

$$a \cdot a^{p-2} \equiv 1 \mod p.$$

Ako to zapišemo u obliku klasa ekvivalencije za relaciju kongruencije, dobivamo da je

$$[a] \cdot [a^{p-2}] = [a^{p-1}] = 1,$$

što pokazuje da je klasa $[a^{p-2}]$, odnosno ostatak pri dijeljenju a^{p-2} s p, inverz elementa a. Time smo dokazali da je skup invertibilnih elemenata u $(\mathbb{Z}_p, \cdot_p)$ jednak

$$\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\},$$

te da je $(\mathbb{Z}_p, \cdot_p)$ komutativna grupa. Red grupe $\mathbb{Z}_p^\times$ je $p-1$.

2.11. Multiplikativne grupe ostataka za m složen. Ako je m složen, onda nisu svi elementi monoida $(\mathbb{Z}_m, \cdot_m)$ različiti od nule invertibilni. Neka je $a \neq 0$ iz $\mathbb{Z}_m$ takav da su a i m relativno prosti. Eulerov teorem iz elementarne teorije brojeva kaže da ako su cijeli broj a i prirodni broj $m \geq 2$ relativno prosti, onda vrijedi

$$a^{\varphi(m)} \equiv 1 \mod m,$$

gdje je φ Eulerova funkcija. Po definiciji, Eulerova funkcija $\varphi(m)$ je broj prirodnih brojeva ne većih od m koji su relativno prosti s m. Može se pokazati, koristeći formulu uključivanja i isključivanja, da se Eulerova funkcija može izračunati po formuli

$$\varphi(m) = m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_k}\right),$$

gdje je $m = p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}$ rastav broja m na proste faktore. Posebno,

$$\varphi(m_1m_2) = \varphi(m_1)\varphi(m_2)$$

ako su m_1 i m_2 relativno prosti, te

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

za p prost broj. Eulerov teorem pokazuje da je

$$a \cdot a^{\varphi(m)-1} \equiv 1 \mod m.$$

Ako to zapišemo u obliku klasa ekvivalencije, dobivamo

$$[a] \cdot [a^{\varphi(m)-1}] = [a^{\varphi(m)}] = [1].$$

To znači da je $[a^{\varphi(m)-1}]$, odnosno ostatak pri dijeljenju $a^{\varphi(m)-1}$ s m, inverz od a. Dakle, ako su a i m relativno prosti, onda je a invertibilan.

Neka je sada $a \neq 0$ iz $\mathbb{Z}_m$ takav da a i m nisu relativno prosti. Neka je $d = NZD(a,m) > 1$ njihov najveći zajednički djelitelj. Neka je $a' = a/d$ i $m' = m/d$. Kad bi a bio invertibilan, to bi značilo da postoji cijeli broj b takav da je

$$a \cdot b \equiv 1 \mod m,$$

odnosno

$$ab = km + 1,$$

za neki cijeli broj k. Ali tada bi

$$1 = ab - km = da'b - kdm' = d(a'b - km')$$

bio djeljiv s d, što je kontradikcija. Dakle, ako a i m nisu relativno prosti, onda a nije invertibilan.

Time smo pokazali da je skup invertibilnih elemenata monoida $(\mathbb{Z}_m, \cdot_m)$ jednak

$$\mathbb{Z}_m^\times = \{a \in \mathbb{Z}_m \mid a \text{ je relativno prost s } m\},$$

te da je $(\mathbb{Z}_m^\times, \cdot_m)$ komutativna grupa. Red te grupe je jednak broju elemenata u $\mathbb{Z}_m$ koji su relativno prosti s m, a to je $\varphi(m)$ po samoj definiciji Eulerove funkcije.

2.12. Grupe funkcija. U ovom primjeru proučavamo algebarske strukture koje tvore funkcije obzirom na operaciju $\circ$ kompozicije funkcija. Neka je S (neprazan) skup i G skup koji se sastoji od svih funkcija $f : S \to S$. Na skupu G promatramo operaciju $\circ$ kompozicije funkcija. Za funkcije $f_1, f_2 \in G$ kompozicija $f_1 \circ f_2$ je funkcija iz S u S definirana na elementu $x \in S$ formulom

$$(f_1 \circ f_2)(x) = f_1\big(f_2(x)\big).$$

Drugim riječima, kompozicija $f_1 \circ f_2$ se dobije primjenom najprije funkcije f_2, a zatim funkcije f_1 na ono što time dobijemo. Budući da je po definiciji $f_1 \circ f_2 : S \to S$, odmah je jasno da je $f_1 \circ f_2 \in G$. Dakle, skup G je zatvoren za operaciju $\circ$, odnosno vrijedi svojstvo (G0). Spomenimo da za funkcije $f : S \to T$, gdje je T neki drugi skup, ne možemo definirati operaciju kompozicije jer bi domena funkcije koju komponiramo s $f : S \to T$ trebao biti skup T, a ne S.

Svojstvo (G1) asocijativnosti kompozicije vrijedi jer je

$$\begin{aligned}\big((f_1 \circ f_2) \circ f_3\big)(x) &= (f_1 \circ f_2)\big(f_3(x)\big) = f_1\Big(f_2\big(f_3(x)\big)\Big) \\ &= f_1\big((f_2 \circ f_3)(x)\big) = \big(f_1 \circ (f_2 \circ f_3)\big)(x)\end{aligned}$$

za sve $f_1, f_2, f_3 \in G$, gdje je $x \in S$ proizvoljan. Dakle,

$$f_1 \circ (f_2 \circ f_3) = (f_1 \circ f_2) \circ f_3$$

su jednake funkcije za sve $f_1, f_2, f_3 \in G$, a to je upravo uvjet asocijativnosti (G1).

Neka je $id : S \to S$ identiteta na skupu S. To je funkcija koja svaki element od S fiksira, odnosno

$$id(x) = x$$

za svaki $x \in S$. Pokazuje se da je id neutralni element u G za operaciju kompozicije. Naime,

$$(f \circ id)(x) = f\big(id(x)\big) = f(x)$$

$$(id \circ f)(x) = id\big(f(x)\big) = f(x)$$

za svaki $f \in G$, gdje je $x \in S$ proizvoljan. Stoga vrijedi

$$f \circ id = id \circ f = f,$$

kao jednakost funkcija, za sve $f \in G$, što znači da je id neutralni element. Dakle, vrijedi svojstvo (G2) za $(G, \circ)$.

Međutim, svojstvo (G3) nije ispunjeno. Svaka funkcija $f \in G$ koja nije bijekcija, nema inverz. Inverz od f bila bi funkcija $f^{-1} \in G$ za koju vrijedi

$$f \circ f^{-1} = f^{-1} \circ f = id.$$

Ako $f \in G$ nije injekcija, onda $g \circ f$ ne može biti injekcija ni za koju funkciju $g \in G$. Stoga ne može postojati funkcija $f^{-1} \in G$ takva da je $f^{-1} \circ f = id$, jer je identiteta id očito bijekcija. Ako pak $f \in G$ nije surjekcija, onda $f \circ g$ ne može biti surjekcija ni za koju funkciju $g \in G$. Stoga ne može postojati funkcija $f^{-1} \in G$ takva da je $f \circ f^{-1} = id$. Dakle, skup G svih funkcija $f : S \to S$ s operacijom $\circ$ kompozicije funkcija tvori monoid, ali ne tvori grupu.

Monoid $(G, \circ)$ nije komutativan, osim u trivijalnom slučaju kada S ima samo jedan element. Zaista, čim postoje dva elementa $x_1, x_2 \in S$, možemo odabrati funkcije $f_1, f_2 \in G$ takve da je

$$f_1(x_1) = f_1(x_2) = x_1,$$

$$f_2(x_1) = f_2(x_2) = x_2.$$

Za njih vrijedi

$$(f_1 \circ f_2)(x_1) = f_1\big(f_2(x_1)\big) = f_1(x_2) = x_1,$$

$$(f_2 \circ f_1)(x_1) = f_2\big(f_1(x_1)\big) = f_2(x_1) = x_2,$$

pa $f_1 \circ f_2 \neq f_2 \circ f_1$, što pokazuje da komutativnost ne vrijedi.

Kao i u više prethodnih primjera, da dobijemo grupu, promatramo invertibilne elemente monoida $(G, \circ)$. Već smo vidjeli da sve funkcije $f \in G$ koje nisu bijekcije nisu invertibilne. Ako je $f \in G$ bijekcija, onda postoji inverzna funkcija $f^{-1} \in G$, koja se definira na sljedeći način. Neka je $x \in S$. Tada, zbog toga što je $f : S \to S$ bijekcija, postoji i jedinstven je $x' \in S$ takav da je $x = f(x')$. Inverzna funkcija f^{-1} je definirana s

$$f^{-1}(x) = x'.$$

Dakle, što god f napravi s x', inverzna funkcija vrati nazad u x'. Drugim riječima,

$$(f^{-1} \circ f)(x') = f^{-1}\big(f(x')\big) = f^{-1}(x) = x' = id(x'),$$

za svaki $x' \in S$. Stoga je $f^{-1} \circ f = id$. Isto vrijedi i obratno,

$$(f \circ f^{-1})(x) = f\big(f^{-1}(x)\big) = f(x') = x = id(x),$$

za svaki $x \in S$. Stoga je i $f \circ f^{-1} = id$. Zaključujemo da su invertibilni elementi monoida $(G, \circ)$ upravo one funkcije $f \in G$ koje su bijekcije. Dakle,

$$G^\times = \{f : S \to S \,|\, f \text{ je bijekcija}\}$$

je skup invertibilnih elemenata monoida $(G, \circ)$ i stoga $(G^\times, \circ)$ je grupa.

Ova grupa nije komutativna, osim u slučaju kad je S jednočlan ili dvočlan. Lako se provjeri da je u slučaju kad je S jednočlan

$$G = G^\times = \{id\},$$

što je komutativno. U slučaju kad je $S = \{x_1, x_2\}$ dvočlan, postoje dvije bijekcije

$$G^\times = \{id, f\},$$

gdje je $f(x_1) = x_2$, a $f(x_2) = x_1$. Tada je $(G^\times, \circ)$ komutativna jer id kao neutralni element komutira sa svima, a svaki element komutira sam sa sobom.

U slučaju kada S ima barem tri elementa, $x_1, x_2, x_3 \in S$, postoje bijekcije $f_1, f_2 \in G^\times$ za koje je

$$f_1(x_1) = x_2, \quad f_1(x_2) = x_1, \quad f_1(x_3) = x_3,$$

$$f_2(x_1) = x_1, \quad f_2(x_2) = x_3, \quad f_2(x_3) = x_2.$$

Tada je

$$(f_1 \circ f_2)(x_1) = f_1\big(f_2(x_1)\big) = f_1(x_1) = x_2,$$

$$(f_2 \circ f_1)(x_1) = f_2\big(f_1(x_1)\big) = f_2(x_2) = x_3,$$

što pokazuje da $f_1 \circ f_2 \neq f_2 \circ f_1$, odnosno $(G^\times, \circ)$ nije komutativna.

2.13. Grupe izometrija. Neka je sada $S = \Pi$ skup točaka ravnine. Vidjeli smo da skup svih bijekcija $f : \Pi \to \Pi$ obzirom na operaciju $\circ$ kompozicije funkcija tvori grupu. U ovom primjeru tu grupu ćemo označiti s $(G, \circ)$. Dakle,

$$G = \{f : \Pi \to \Pi \,|\, f \text{ je bijekcija}\}.$$

Uočimo da smo ovdje promijenili oznaku jer smo ranije grupu bijekcija označavali $(G^\times, \circ)$.

U ravnini Π definirana je funkcija d udaljenosti među točkama. To je funkcija $d : \Pi \times \Pi \to \mathbb{R}$ koja paru točaka (P, Q) ravnine Π pridružuje njihovu udaljenost, odnosno duljinu dužine koja ih spaja. Svojstva funkcije udaljenosti su sljedeća:

- $d(P, Q) \geq 0$ za sve $P, Q \in \Pi$,
- $d(P, Q) = 0$ ako i samo ako $P = Q$,
- $d(P, Q) = d(Q, P)$ za sve $P, Q \in \Pi$,
- $d(P, Q) \leq d(P, R) + d(R, Q)$ za sve $P, Q, R \in \Pi$ (nejednakost trokuta).

Prva tri svojstva su očita jer je duljina dužine između dvaju različitih točaka pozitivna i ne ovisi o poretku krajnjih točaka dužine. Duljina nula se dobije ako i samo ako se dvije točke podudaraju. Četvrto svojstvo je dobro poznata nejednakost trokuta koja kaže da je zbroj duljina bilo koje dvije stranice trokuta veći od duljine treće stranice. Jednakost se dobiva jedino u slučaju da su tri točke P, Q, R kolinearne (leže na istom pravcu) i pritom je R između P i Q.

Izometrija ravnine se definira kao funkcija $f : \Pi \to \Pi$ koja čuva udaljenosti među točkama, odnosno

$$d\big(f(P), f(Q)\big) = d(P, Q) \quad \text{za sve } P, Q \in \Pi.$$

Dokažimo da je svaka izometrija ravnine bijekcija. Injektivnost slijedi iz drugog svojstva funkcije udaljenosti. Naime, ako za izometriju f vrijedi $f(P) = f(Q)$ za neke $P, Q \in \Pi$, onda je $d(f(P), f(Q)) = 0$. Kako je f izometrija, slijedi da je i $d(P, Q) = 0$, pa stoga $P = Q$, što pokazuje injektivnost. Za dokaz surjektivnosti najprije fiksirajmo tri točke $A, B, C \in \Pi$ koje nisu kolinearne (ne leže na istom pravcu). Neka su $A' = f(A)$, $B' = f(B)$ i $C' = f(C)$ slike tih točaka pri izometriji f. Kako f čuva udaljenosti, trokut ABC je sukladan trokutu $A'B'C'$ obzirom da su im duljine stranica jednake. Sada uočimo da je svaka točka ravnine jedinstveno određena svojim udaljenostima od tri fiksirane točke koje nisu kolinearne. Zaista, neka je P točka u ravnini. Njene udaljenosti od A, B i C određuju tri kružnice sa središtima u A, B i C, redom, u čijem presjeku se točka P nalazi. Ali tri kružnice čija središta nisu kolinarna sijeku se u najviše jednoj točki. To se vidi jer se dvije kružnice sijeku u najviše dvije točke koje su osno simetrične obzirom na pravac koji spaja njihova središta. Kad bi obje te toķe ležale na trećoj kružnici, onda bi njeno središte moralo ležati na tom pravcu, a to je kontradikcija jer tri središta nisu kolinearna. Dakle, točka P je jedinstveno određena kao presjek tri kružnice oko točaka A, B i C s polumjerima jednakim udaljenostima točke P od tih točaka. Sada je jasno da je f surjekcija jer ako je P' proizvoljna točka ravnine, ona je jedinstveno određena svojim udaljenostima od točaka A', B' i C'. Kako su trokuti ABC i $A'B'C'$ sukladni, te iste udaljenosti ali gledane od točaka A, B i C određuju jedinstvenu točku P u ravnini. Budući da f čuva udaljenosti, mora biti $f(P) = P'$. Time smo dokazali surjektivnost, pa je svaka izometrija bijekcija.

Dakle, prema upravo dokazanom, skup

$$H = \{f : \Pi \to \Pi \,|\, f \text{ je izometrija}\}$$

je podskup grupe $(G, \circ)$ bijekcija ravnine. Također, H je neprazan jer je identiteta id ravnine Π očito izometrija. Dokažimo, koristeći kriterij za podgrupe, da je H podgrupa od G. Neka su $f_1, f_2 \in H$ proizvoljne izometrije. Tada vrijedi

$$d\big((f_1 \circ f_2)(P), (f_1 \circ f_2)(Q)\big) = d\Big(f_1\big(f_2(P)\big), f_1\big(f_2(Q)\big)\Big) = d\big(f_2(P), f_2(Q)\big) = d(P, Q)$$

za sve $P, Q \in \Pi$, pa je kompozicija također izometrija, odnosno $f_1 \circ f_2 \in H$. Neka je sada $f \in H$ izometrija. Neka su $P', Q' \in \Pi$ proizvoljne dvije točke ravnine. Kako je f bijekcija, postoje i jedinstvene su točke $P, Q \in \Pi$ takve da je $f(P) = P'$ i $f(Q) = Q'$. Tada, za inverznu funkciju f^{-1} vrijedi $f^{-1}(P') = P$ i $f^{-1}(Q') = Q$. Stoga, koristeći da je f izometrija, dobivamo

$$d(f^{-1}(P'), f^{-1}(Q')) = d(P, Q) = d(f(P), f(Q)) = d(P', Q').$$

Kako su P' i Q' bile proizvoljne, time smo pokazali da je inverzna funkcija f^{-1} također izometrija, odnosno $f^{-1} \in H$. Dakle, prema kriteriju zaključujemo da je H podgrupa grupe bijekcija $(G, \circ)$. Grupu $(H, \circ)$ zovemo grupa izometrija.

Grupa izometrija ravnine ima brojne podgrupe. To su primjerice podgrupa koja se sastoji od svih translacija, podgrupa svih rotacija oko jedne fiksirane točke P. Dokaze provodimo koristeći kriterij.

Za podgrupu svih translacija uočimo da je kompozicija dvaju translacija ponovo translacija i to za vektor koji se dobije kao zbroj vektora polaznih translacija. Inverz translacije je translacija za suprotni vektor. Dakle, translacije zaista čine podgrupu. Ta grupa je komutativna jer je zbrajanje vektora komutativno.

Slično, za rotacije oko točke P, kompozicija dviju rotacija je opet rotacija oko točke P i to za kut koji je jednak zbroj kuteva polaznih rotacija. Inverz rotacije je rotacija oko točke P za isti kut u suprotnom smjeru. Stoga rotacije oko fiksirane točke tvore podgrupu. I ta podgrupa je komutativna jer je zbrajanje kuteva komutativno.

2.14. Grupa izometrija peterokuta. U prošlom primjeru našli smo dvije podgrupe grupe $(H, \circ)$ svih izometrija ravnine. To su bile podgrupa svih rotacija oko iste točke i podgrupa svih translacija. Obje su beskonačnog reda.

U ovom primjeru promatramo podgrupu konačnog reda grupe $(H, \circ)$ svih izometrija ravnine. Takve podgrupe možemo dobiti primjerice ako promatramo skup svih izometrija za koje se neki pogodni geometrijski lik ne promjeni. Mi ćemo detaljno proučiti slučaj pravilnog peterokuta.

Označimo vrhove pravilnog peterokuta brojevima 1, 2, 3, 4, 5, u smjeru suprotnom od kazaljke na satu (taj smjer se obiňo zove pozitivan). Odredimo izometrije koje taj peterokut ostavljaju na mjestu. Najprije to je svakako identiteta id. Zatim, to je i pet osnih simetrija σ_1, σ_2, σ_3, σ_4, σ_5, gdje je os simetrije σ_i pravac koji prolazi vrhom i i okomit je na nasuprotnu stranicu peterokuta. I na kraju to su četiri rotacije ρ_1, ρ_2, ρ_3, ρ_4, oko središta peterokuta, gdje je ρ_i rotacija u pozitivnom smjeru za kut

$$i \cdot \frac{360^\circ}{5} = i \cdot 72^\circ.$$

Dakle, skup H' svih izometrija koje ostavljaju zadani peterokut na mjestu je

$$H' = \{id, \rho_1, \rho_2, \rho_3, \rho_4, \sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_5\},$$

pa ima 10 elemenata.

$\circ$	id	ρ_1	ρ_2	ρ_3	ρ_4	σ_1	σ_2	σ_3	σ_4	σ_5
id	id	ρ_1	ρ_2	ρ_3	ρ_4	σ_1	σ_2	σ_3	σ_4	σ_5
ρ_1	ρ_1	ρ_2	ρ_3	ρ_4	id	σ_4	σ_5	σ_1	σ_2	σ_3
ρ_2	ρ_2	ρ_3	ρ_4	id	ρ_1	σ_2	σ_3	σ_4	σ_5	σ_1
ρ_3	ρ_3	ρ_4	id	ρ_1	ρ_2	σ_5	σ_1	σ_2	σ_3	σ_4
ρ_4	ρ_4	id	ρ_1	ρ_2	ρ_3	σ_3	σ_4	σ_5	σ_1	σ_2
σ_1	σ_1	σ_3	σ_5	σ_2	σ_4	id	ρ_3	ρ_1	ρ_4	ρ_2
σ_2	σ_2	σ_4	σ_1	σ_3	σ_5	ρ_2	id	ρ_3	ρ_1	ρ_4
σ_3	σ_3	σ_5	σ_2	σ_4	σ_1	ρ_4	ρ_2	id	ρ_3	ρ_1
σ_4	σ_4	σ_1	σ_3	σ_5	σ_2	ρ_1	ρ_4	ρ_2	id	ρ_3
σ_5	σ_5	σ_2	σ_4	σ_1	σ_3	ρ_3	ρ_1	ρ_4	ρ_2	id

TABLICA 1. Cayleyjeva tablica grupe izometrija peterokuta

Dokažimo, koristeći kriterij, da je H' podgrupa grupe $(H, \circ)$ svih izometrija. Za to nije potrebno poznavati točno od kojih se izometrija sastoji skup H'. Ovaj isti dokaz vrijedi i za izometrije koje ostavljaju na mjestu bilo koji geometrijski lik. Neka su $f_1, f_2 \in H'$ dvije izometrije. One ostavljaju zadani peterokut na mjestu, pa i njihova kompozicija $f_1 \circ f_2$ ostavlja peterokut na mjestu jer pri kompoziciji naprosto primjenjujemo izometrije jednu za drugom. Neka je sad $f \in H'$ izometrija. Ona ostavlja zadani peterokut na mjestu. Tada i njoj inverzna izometrija f^{-1} ostavlja peterokut na mjestu jer inverzna funkcija vraća u početno stanje sve što polazna funkcija napravi. Dakle, $(H', \circ)$ je zaista podgrupa od $(H, \circ)$ koju zovemo podgrupa izometrija peterokuta.

Grupa $(H', \circ)$ je reda 10 jer H' ima 10 elemenata. Sljedeći cilj je proučiti detaljnije njenu strukturu. Kako grupa ima konačno elemenata, može se napraviti "tablica množenja" grupe, iz koje se mogu isčitati takvi podaci. Takva tablica naziva se Cayleyeva tablica grupe. Za grupu $(H', \circ)$ Cayleyeva tablica je dana u tablici 1.

U Cayleyjevoj tablici na presjeku i–tog retka i j–tog stupca je kompozicija i–te i j–te izometrije u poretku kakav je dan u retku lijevo od oznake operacije i stupcu ispod oznake operacije. Primjerice, kompozicija $\sigma_2 \circ \rho_3$ se nalazi u presjeku retka označenog sa σ_2 i stupca označenog s ρ_3. Dakle, $\sigma_2 \circ \rho_3 = \sigma_3$. Obratno, na križanju retka označenog s ρ_3 i stupca označenog s σ_2 dobivamo $\rho_3 \circ \sigma_2 = \sigma_1$.

Sam račun kompozicija koji smo napravili da dobijemo Cayleyevu tablicu može se provesti na dva načina. Jedan način je geometrijski, poznavajući činjenice o osnim simetrijama i rotacijama, kao što je činjenica da je kompozicija dvije osne simetrije čije se osi sijeku rotacija za dvostruki kut među osima. Drugi način, koji ćemo detaljnije objasniti, je više algebarski i koristimo ga u narednim primjerima. Bazira se na tome da se izometrije peterokuta promatraju kao preslikavanja njegovih vrhova budući da oni u potpunosti određuju peterokut i samu izometriju. Primjerice, osna simetrija σ_2 na vrhovima djeluje na sljedeći način:

$$1 \mapsto 3, \quad 2 \mapsto 2, \quad 3 \mapsto 1, \quad 4 \mapsto 5, \quad 5 \mapsto 4.$$

Običaj je da se to zapisuje vertikalno u obliku

$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix},$$

gdje prvi stupac predstavlja $1 \mapsto 3$, drugi $2 \mapsto 2$, i tako dalje. Ovakav zapis rotacije ρ_3 je

$$\rho_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix},$$

jer se $1 \mapsto 4$, $2 \mapsto 5$, $3 \mapsto 1$, $4 \mapsto 2$, $5 \mapsto 3$. Kao primjer, izračunajmo kompoziciju $\sigma_2 \circ \rho_3$ u ovom zapisu izometrija. Dakle računamo,

$$\sigma_2 \circ \rho_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix}.$$

Rezultat dobivamo tako da redom promatramo kuda kompozicija šalje brojeve 1, 2, 3, 4, 5, i to upisujemo u drugi redak zapisa kompozicije. Kao uvijek kod kompozicije funkcija, prvo djeluje desna izometrija. Stoga iz zapisa za ρ_3 čitamo u prvom stupcu da ρ_3 šalje broj 1 u broj 4. Zatim djeluje σ_2 koja dobiveni broj 4 šalje u 5 kao što vidimo iz četvrtog stupca u zapisu za σ_2. Dakle, kompozicija $\sigma_2 \circ \rho_3$ šalje 1 u 5 i to zapisujemo u prvom stupcu rezultata. Zatim nastavljamo na isti način s brojem 2. U drugom stupcu zapisa za ρ_3 vidimo da ρ_3 šalje 2 u 5, a zatim iz petog stupca zapisa za σ_2 vidimo da σ_2 šalje dobiveni broj 5 u 4. Dakle, kompozicija $\sigma_2 \circ \rho_3$ šalje 2 u 4 što zapisujemo u drugi stupac zapisa te kompozicije. Nastavljamo s preostalim brojevima na isti način i dobivamo

$$\sigma_2 \circ \rho_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix},$$

a to je zapis osne simetrije σ_3 jer je 3 fiksan, a 1 i 5, kao i 2 i 4, se zamijene. Na ovaj način možemo izračunati sve kompozicije i popuniti Cayleyevu tablicu.

Ovaj zapis izometrija peterokuta je pogodan i za računanje inverza. Kako inverz izometrije vraća vrhove u početni položaj, određujemo ga čitajući zapis izometrije odozdo prema gore. Primjerice, za

$$\rho_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \end{pmatrix},$$

čitajući odozdo prema gore vidimo da je inverz jednak

$$\rho_3^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{pmatrix}.$$

To je zapis rotacije ρ_2, pa je $\rho_3^{-1} = \rho_2$.

Pogledajmo na ovom primjeru što se sve o grupi može isčitati iz Cayleyjeve tablice. Zatvorenost operacije se odmah vidi po tome što su u tablici samo elementi grupe. Asocijativnost nije lako direktno vidjeti iz tablice. Neutralni element je u onom retku koji se podudara s poretkom elemenata grupe u zaglavlju tablice. Inverz nekog elementa nađemo tako da u retku označenom tim elementom pronađemo neutralni element. Tada je inverz onaj element kojim je označen taj stupac. Operacija je komutativna ako i samo ako je Cayleyjeva tablica simetrična obzirom na glavnu (padajuću) dijegonalu.

2.15. Grupe permutacija (simetrična grupa). Neka je n prirodan broj. Permutacija skupa od n elemenata je svaka uređena n–torka tih elemenata s time da se elementi ne smiju više puta pojaviti u n–torci. Drugim riječima, permutacija je jedan poredak elemenata n–članog skupa.

Obično se za skup od n elemenata uzima skup $X_n = \{1, 2, \ldots, n\}$. Njegova permutacija σ je naprosto jedan poredak brojeva od 1 do n. Označimo taj poredak

$$\sigma = (a_1, a_2, \ldots, a_n),$$

gdje su $a_1, a_2, \ldots, a_n \in X_n$ različiti. Uočimo da permutaciju σ možemo shvatiti kao preslikavanje

$$\sigma : X_n \to X_n$$

koje preslikava broj 1 u a_1, broj 2 u a_2, i tako dalje. Dakle,

$$\sigma(k) = a_k \text{ za } k \in X_n.$$

Tako definirano preslikavanje σ je očito injekcija jer su svi a_k različiti po definiciji permutacije. Kako je skup X_n konačan, svaka injekcija iz X_n u X_n je i surjekcija. Stoga je σ bijekcija. Dakle, permutacija od n elemenata može se promatrati kao bijekcija iz skupa X_n na samog sebe. Skup svih permutacija od n elemenata, shvaćenih kao bijekcije, označimo sa S_n.

Promatranje permutacija kao bijekcija omogućava definiranje operacije na skupu S_n permutacija od n elemenata kao kompozicije funkcija. Za permutacije $\sigma_1, \sigma_2 \in S_n$ njihovu kompoziciju označavamo $\sigma_1 \circ \sigma_2$. Ranije smo već vidjeli da skup bijekcija bilo kojeg skupa tvori grupu obzirom na operaciju kompozicije. Posebno, to znači da je $(S_n, \circ)$ grupa. Grupa $(S_n, \circ)$ naziva se simetrična grupa. Također smo već vidjeli da je grupa S_n nekomutativna za $n \geq 3$, a komutativna za $n = 1$ i $n = 2$. Red grupe S_n je jednak broju permutacija skupa od n elemenata, a to je, prema teoremu o uzastopnom prebrojavanju iz kombinatorike, jednako $n!$.

Uobičajeno je permutacije zapisivati u obliku tablice kao i izometrije peterokuta u prethodnom primjeru. Ako je

$$\sigma = (a_1, a_2, \ldots, a_n),$$

gdje su $a_1, \ldots, a_n \in X_n$ različiti, onda se σ zapisuje u obliku

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ a_1 & a_2 & a_3 & \ldots & a_{n-1} & a_n \end{pmatrix}.$$

Kompozicija permutacija i inverz permutacije u ovom zapisu računaju se na isti način kao u primjeru grupe izometrija peterokuta. Zapravo, grupa izometrija peterokuta je podgrupa grupe $(S_5, \circ)$.

2.16. Zapis permutacije pomoću disjunktnih ciklusa. Za određivanje reda permutacije koristimo zapis permutacije pomoću disjunktnih ciklusa. Ciklus u S_n je permutacija $\sigma \in S_n$ za koju postoje međusobno različiti $k_1, k_2, \ldots, k_d \in X_n$, gdje je $d \geq 2$, takvi da vrijedi

$$\sigma(k_1) = k_2, \quad \sigma(k_2) = k_3, \quad \ldots \quad \sigma(k_{d-1}) = k_d, \quad \sigma(k_d) = k_1,$$

te

$$\sigma(l) = l \quad \text{za sve} \quad l \in X_n \setminus \{k_1, \ldots, k_d\}.$$

Drugim riječima, ciklus σ preslikava

$$k_1 \mapsto k_2 \mapsto \ldots \mapsto k_d \mapsto k_1,$$

a sve ostale točke su fiksne. Duljina ciklusa je broj elemenata koji su uključeni u ciklus. Za ciklus σ duljina je d. Red ciklusa kao elementa grupe S_n jednak je njegovoj duljini. Zaista, uzastopnom primjenom ciklusa σ na element k_i, za $i = 1, \ldots, d$, dobivamo redom

$k_{i+1}, k_{i+2}, \ldots$ pa je potrebno najmanje d puta primjeniti σ da se dobije ponovo k_i. Kako su elementi $l \in X \setminus \{k_1, \ldots, k_d\}$ fiksni, time smo dokazali da je duljina d jednaka redu ciklusa σ.

Ciklus σ se zapisuje u obliku

$$\sigma = (k_1, k_2, \ldots, k_d) \in S_n.$$

U ovom zapisu ciklusa važno je naglasiti da je ciklus iz S_n, jer se to ne može vidjeti iz samog zapisa. Primjerice, ciklus $\sigma = (1, 2, 5)$ može biti iz S_5, ali i bilo koje veće simetrične grupe S_n, $n \geq 5$. Također, ovakav zapis nije jedinstven, jer prebacivanjem jednog po jednog elementa ciklusa s početka na kraj zapisa, ili obratno, s kraja na početak, ciklus se ne mijenja. Tako se ciklus σ može zapisati kao

$$\sigma = (k_i, k_{i+1}, \ldots, k_d, k_1, k_2, \ldots, k_{i-1})$$

za svaki $i = 1, 2, \ldots, d$. Zaista, u ovom zapisu koji počinje s k_i ciklus σ preslikava

$$k_i \mapsto k_{i+1} \mapsto \ldots \mapsto k_d \mapsto k_1 \mapsto k_2 \mapsto \ldots \mapsto k_{i-1} \mapsto k_i,$$

a to je isto preslikavanje kao i u zapisu koji počinje s k_1.

Za dva ciklusa

$$\sigma_1 = (k_1, k_2, \ldots, k_d) \in S_n, \quad \sigma_2 = (k'_1, k'_2, \ldots, k'_{d'}) \in S_n$$

kažemo da su disjunktni ako su skupovi

$$\{k_1, k_2, \ldots, k_d\} \quad \text{i} \quad \{k'_1, k'_2, \ldots, k'_{d'}\}$$

disjunktni. Dakle, disjunktni ciklusi ne uključuju niti jedan zajednički element. Disjunktni ciklusi komutiraju jer

$$\begin{aligned}
\sigma_1 \circ \sigma_2(k_i) = \sigma_1(k_i) = k_{i+1} &\qquad \text{za } i = 1, \ldots, d, \text{ gdje } k_{d+1} = k_1,\\
\sigma_1 \circ \sigma_2(k'_j) = \sigma_1(k'_{j+1}) = k'_{j+1} &\qquad \text{za } j = 1, \ldots, d', \text{ gdje } k'_{d'+1} = k'_1,\\
\sigma_1 \circ \sigma_2(l) = \sigma_1(l) = l &\qquad \text{za } l \in X_n \setminus \{k_1, \ldots, k_d, k'_1, \ldots, k'_{d'}\},
\end{aligned}$$

$$\begin{aligned}
\sigma_2 \circ \sigma_1(k_i) = \sigma_2(k_{i+1}) = k_{i+1} &\qquad \text{za } i = 1, \ldots, d, \text{ gdje } k_{d+1} = k_1,\\
\sigma_2 \circ \sigma_1(k'_j) = \sigma_2(k'_j) = k'_{j+1} &\qquad \text{za } j = 1, \ldots, d', \text{ gdje } k'_{d'+1} = k'_1,\\
\sigma_2 \circ \sigma_1(l) = \sigma_2(l) = l &\qquad \text{za } l \in X_n \setminus \{k_1, \ldots, k_d, k'_1, \ldots, k'_{d'}\},
\end{aligned}$$

pa se $\sigma_1 \circ \sigma_2$ i $\sigma_2 \circ \sigma_1$ podudaraju. To se zapravo može i odmah zaključiti jer su svi elementi koje ne fiksira jedan od disjunktnih ciklusa fiksne za drugi ciklus.

Pokažimo sada da se svaka permutacija σ može zapisati kao kompozicija disjunktnih ciklusa i to na jedinstven način do na poredak ciklusa. Neka je $\sigma \in S_n$ proizvoljna permutacija. Na skupu X_n definiramo relaciju $\sim$ na sljedeći način. Za dva elementa $k_1, k_2 \in X_n$ kažemo da je k_1 u relaciji $\sim$ s k_2, i pišemo $k_1 \sim k_2$, ako postoji cijeli broj $m \in \mathbb{Z}$ takav da je

$$k_2 = \sigma^m(k_1).$$

Podsjetimo da je σ^m potencija u grupi S_n, odnosno potencija obzirom na operaciju kompozicije permutacija. Dokažimo da je $\sim$ relacija ekvivalencije. Refleksivnost vrijedi jer je, za svaki $k \in S_n$,

$$k = id(k) = \sigma^0(k)$$

pa je $k \sim k$. Simetričnost vrijedi jer ako je $k_1 \sim k_2$, onda postoji $m \in \mathbb{Z}$ takav da je $k_2 = \sigma^m(k_1)$, pa komponiranje te jednakosti sa σ^{-m} daje $k_1 = \sigma^{-m}(k_2)$, odnosno $k_2 \sim k_1$. Tranzitivnost vrijedi jer ako je $k_1 \sim k_2$ i $k_2 \sim k_3$, onda postoje cijeli brojevi $m, m' \in \mathbb{Z}$ takvi da je $k_2 = \sigma^m(k_1)$ i $k_3 = \sigma^{m'}(k_2)$. Tada vrijedi

$$\sigma^{m'+m}(k_1) = (\sigma^{m'} \circ \sigma^m)(k_1) = \sigma^{m'}\big(\sigma^m(k_1)\big) = \sigma^{m'}(k_2) = k_3,$$

pa je stoga $k_1 \sim k_3$.

Kao svaka relacija ekvivalencije, relacija $\sim$ definira particiju skupa X_n u klase ekvivalencije. Klasu čiji predstavnik je $k \in X_n$ označavamo s $[k]$. Prema definiciji relacije $\sim$ vrijedi

$$\begin{aligned} [k] &= \{l \in X_n \,|\, k \sim l\} \\ &= \{l \in X_n \,|\, \text{postoji } m \in \mathbb{Z} \text{ takav da je } l = \sigma^m(k)\} \\ &= \{\sigma^m(k) \,|\, m \in \mathbb{Z}\}. \end{aligned}$$

Dakle, klasa ekvivalencije $[k]$ sastoji se od svih različitih elemenata niza

$$\ldots, \sigma^{-2}(k), \sigma^{-1}(k), k, \sigma(k), \sigma^2(k), \ldots,$$

u kojem mora biti ponavljanja jer je $[k]$ konačna kao klasa ekvivalencije u konačnom skupu X_n. Neka su stoga $m, m' \in \mathbb{Z}$ takvi da je $m > m'$ i $\sigma^m(k) = \sigma^{m'}(k)$. Tada komponiranjem sa $\sigma^{-m'}$ dobivamo da je

$$\sigma^{m-m'}(k) = k$$

i pritom $m - m' > 0$. Odaberimo najmanji prirodni broj m_0 u skupu svih prirodnih brojeva za koje vrijedi taj uvjet. Takav m_0 sigurno postoji jer uvjet vrijedi za prirodni broj $m - m'$, a u skupu prirodnih brojeva svaki neprazan podskup sadrži minimalan element. Dakle, za m_0 vrijedi

$$\sigma^{m_0}(k) = k$$

i m_0 je najmanji prirodni broj za koji to vrijedi. Tada su brojevi

$$k, \sigma(k), \ldots, \sigma^{m_0-1}(k)$$

svi različiti jer kad bi postojali $l, l' \in \{0, 1, \ldots, m_0 - 1\}$ takvi da je $l > l'$ i $\sigma^l(k) = \sigma^{l'}(k)$, onda bi vrijedilo $\sigma^{l-l'}(k) = k$. Pritom je $0 < l - l' \leq m_0 - 1$ pa bi $l - l'$ bio prirodan broj manji od m_0 koji zadovoljava uvjet $\sigma^{l-l'}(k) = k$. S druge strane, svaki $m \in \mathbb{Z}$ možemo zapisati u obliku

$$m = q \cdot m_0 + r,$$

gdje je $q \in \mathbb{Z}$ kvocijent dijeljenja m s m_0, a $r \in \{0, 1, \ldots, m_0 - 1\}$ ostatak. Tada, zbog $\sigma^{m_0}(k) = k$, vrijedi

$$\sigma^m(k) = \sigma^{qm_0+r}(k) = \big(\sigma^r \circ \underbrace{\sigma^{m_0} \circ \ldots \circ \sigma^{m_0}}_{q \text{ puta}}\big)(k) = \sigma^r(k).$$

Dakle, svaka potencija $\sigma^m(k)$ jednaka je nekom od $\sigma^r(k)$ za $r \in \{0, 1, \ldots, m_0 - 1\}$. Time smo dokazali da je

$$[k] = \{k, \sigma(k), \ldots, \sigma^{m_0-1}(k)\}$$

upravo klasa ekvivalencije s predstavnikom k. Uočimo da je točka $k \in X_n$ fiksna točka permutacije σ ako i samo ako je klasa ekvivalencije $[k]$ jednočlana. Naime, točka k je fiksna

ako i samo ako je $\sigma(k) = k$, a to onda znači i da je $\sigma^m(k) = k$ za sve $m \in \mathbb{Z}$, odnosno $[k] = \{k\}$.

Sada za svaku klasu ekvivalencije koja nije jednočlana definiramo po jedan ciklus iz S_n. Neka je

$$[k] = \{k, \sigma(k), \ldots, \sigma^{m_0-1}(k)\}$$

jedna takva klasa ekvivalencije, gdje je $m_0 \geq 2$. Tada definiramo ciklus

$$\sigma_{[k]} = \big(k, \sigma(k), \ldots, \sigma^{m_0-1}(k)\big) \in S_n.$$

Ova definicija ne ovisi o izboru predstavnika klase $[k]$. Zaista, neka je $\sigma^l(k)$, za neki $l \in \{0, \ldots, m_0 - 1\}$, predstavnik klase $[k]$, odnosno $[\sigma^l(k)] = [k]$. Tada gornja konstrukcija za predstavnika $\sigma^l(k)$ daje ciklus

$$\sigma_{[\sigma^l(k)]} = \big(\sigma^l(k), \ldots, \sigma^{m_0-1}(k), k, \sigma(k) \ldots, \sigma^{l-1}(k)\big) \in S_n.$$

Međutim, ciklusi $\sigma_{[\sigma^l(k)]}$ i $\sigma_{[k]}$ su jednaki, jer se dobiveni zapis ciklusa $\sigma_{[\sigma^l(k)]}$ dobije od zapisa ciklusa $\sigma_{[k]}$ prebacivanjem prvih $l - 1$ članova s početka na kraj zapisa. Vidjeli smo ranije da takvo prebacivanje u zapisu ne mijenja ciklus.

Uočimo da su ciklusi dobiveni od klasa ekvivalencije na ovaj način disjunktni jer u njima sudjeluju točno elementi jedne klase, a one su disjunktne. Stoga, kako smo već vidjeli, one komutiraju, pa možemo definirati permutaciju

$$\prod_{[k]} \sigma_{[k]},$$

gdje je produkt oznaka za operaciju kompozicije i ide po svim klasama ekvivalencije $[k]$ koje nisu jednočlane. Pritom poredak nije bitan jer svi ciklusi u produktu međusobno komutiraju. Ako su sve klase ekvivalencije $[k]$ jednočlane, onda dobivamo produkt po praznom skupu koji definiramo da je jednak identiteti. Dokažimo da je

$$\sigma = \prod_{[k]} \sigma_{[k]}.$$

Ako je $l \in X_n$ fiksna točka permutacije σ, onda je njena klasa $[l]$ jednočlana pa se ne javlja na desnoj strani. Također, l je fiksna točka svih ciklusa u produktu na desnoj strani, jer se l ne javlja u niti jednoj klasi ekvivalencije $[k]$ koja ima više od jednog elementa. Dakle, za takav l dobivamo

$$\sigma(l) = \prod_{[k]} \sigma_{[k]}(l) = l.$$

Neka je sada $l \in X_n$ takav da l nije fiksna točka permutacije σ. Tada klasa $[l]$ ima barem dva elementa pa se javlja u produktu na desnoj strani. Za odgovarajući ciklus

$$\sigma_{[l]}(l) = \sigma(l).$$

Za sve ostale cikluse $\sigma_{[k]}$ vrijedi

$$\sigma_{[k]}(l) = l$$

jer l nije u klasi $[k]$ pa se ne javlja u ciklusu $\sigma_{[k]}$, što znači da je fiksna točka tog ciklusa. Stoga računamo

$$\left(\prod_{[k]}\sigma_{[k]}\right)(l)=\left(\sigma_{[l]}\circ\prod_{[k]\neq[l]}\sigma_{[k]}\right)(l)=\sigma_{[l]}\left(\prod_{[k]\neq[l]}\sigma_{[k]}(l)\right)=\sigma_{[l]}(l)=\sigma(l).$$

Time smo dokazali da se permutacije σ i $\prod_{[k]}\sigma_{[k]}$ podudaraju u svim elementima $l\in X_n$ pa su stoga jednake. Dakle, dobili smo zapis permutacije σ kao kompozicije disjunktnih ciklusa.

Preostaje dokazati da je taj zapis jedinstven. Pretpostavimo da postoji još jedan zapis permutacije σ kao kompozicije disjunktnih ciklusa. To znači da postoje disjunktni ciklusi $\sigma_1,\ldots,\sigma_r\in S_n$ takvi da je

$$\sigma=\prod_{i=1}^{r}\sigma_i.$$

Ako je $l\in X_n$ fiksna točka od σ, onda se l ne pojavljuje u niti jednom od ciklusa σ_i jer inače, zbog njihove disjunktnosti, l ne bi bila fiksna točka produkta σ_i. Ako $l\in X_n$ nije fiksna točka za σ, onda se mora javiti u jednom od ciklusa σ_j. Ali tada vrijedi

$$\sigma(l)=\left(\prod_{i=1}^{r}\sigma_i\right)(l)=\left(\sigma_j\circ\prod_{\substack{i=1\\ i\neq j}}^{r}\sigma_i\right)(l)=\sigma_j\circ\left(\prod_{\substack{i=1\\ i\neq j}}^{r}\sigma_i(l)\right)=\sigma_j(l),$$

pa vidimo da se $\sigma(l)$ javlja u istom ciklusu σ_j kao i l i to neposredno nakon elementa l. Indukcijom se na isti način vidi da se i sve potencije $\sigma^m(l)$, za $m\in\mathbb{Z}$, javljaju redom u ciklusu σ_j. Pokažimo da su to svi elementi ciklusa σ_j. Zaista, ako je $l'\in X_n$ u ciklusu σ_j, onda primjenom tog ciklusa određeni broj puta na l dobivamo l', odnosno postoji cijeli broj $m\geq 0$ takav da je $\sigma_j^m(l)=l'$. Zbog disjunktnosti ciklusa l' je fiksna točka svih ostalih ciklusa σ_i za $i\neq j$. Također, budući da disjunktni ciklusi komutiraju, vrijedi

$$(\sigma_1\circ\ldots\circ\sigma_r)^m=\sigma_1^m\circ\ldots\circ\sigma_r^m.$$

Stoga je

$$\sigma^m(l)=\left(\prod_{i=1}^{r}\sigma_i\right)^m(l)=\left(\prod_{i=1}^{r}\sigma_i^m\right)=\left(\sigma_j^m\circ\prod_{\substack{i=1\\ i\neq j}}^{r}\sigma_i^m\right)(l)=\sigma_j^m\circ\left(\prod_{\substack{i=1\\ i\neq j}}^{r}\sigma_i^m(l)\right)=\sigma_j^m(l)=l',$$

pa je zaista $l'=\sigma^m(l)$. Time smo dokazali da ako je $l\in\sigma_j$, onda mora biti $\sigma_j=\sigma_{[l]}$ pa se ovaj rastav $\prod_{i=1}^{r}\sigma_i$ mora podudarati s prethodno dobivenim rastavom $\prod_{[k]}\sigma_{[k]}$.

Rastav permutacije $\sigma\in S_n$ u kompoziciju disjunktnih ciklusa

$$\sigma=\prod_{[k]}\sigma_{[k]}$$

omogućava jednostavno računanje njenog reda u grupi S_n. Zbog disjunktnosti ciklusa u rastavu oni komutiraju, pa vrijedi

$$\sigma^m=\prod_{[k]}\sigma_{[k]}^m$$

za svaki $m \in \mathbb{Z}$. Stoga je $\sigma^m = id$ ako i samo ako je $\sigma_{[k]}^m = id$ za sve klase $[k]$. Od ranije znamo da je red ciklusa jednak njegovoj duljini, pa je $\sigma_{[k]}^m = id$ ako i samo ako je m višekratnik duljine ciklusa $[k]$. Stoga je red permutacije σ, odnosno najmanji prirodni broj m za koji je $\sigma_{[k]}^m = id$ za sve klase $[k]$, jednak najmanjem zajedničkom višekratniku duljina svih ciklusa u rastavu.

Na kraju ovog poglavlja pokažimo kako se za konkretnu permutaciju računa njen rastav u disjunktne cikluse. Neka je

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 2 & 8 & 1 & 7 & 9 & 5 & 4 & 6 \end{pmatrix} \in S_9.$$

Započnimo određivanje ciklusa brojem 1. Permutacija σ šalje broj 1 u 3. Zatim pogledamo u treći stupac gdje vidimo da σ šalje 3 u 8. Zatim 8 šalje u 4, i na kraju 4 natrag u 1. Dakle, prvi ciklus u rastavu je

$$(1, 3, 8, 4) \in S_9.$$

Sljedeći neiskorišteni broj je broj 2. Ali iz drugog stupca vidimo da je 2 fiksna točka permutacije σ. Stoga se broj 2 ne javlja u rastavu. Sljedeći neiskorišten je broj 5. Njega σ šalje u 7, a zatim 7 nazad u 5. Dakle, ciklus u rastavu je

$$(5, 7) \in S_9.$$

Sljedeći neiskorišten je 6, kojeg σ šalje u 9, pa 9 vraća u 6. Dakle, ciklus u rastavu je

$$(6, 9) \in S_9.$$

Tu stajemo jer više nema neiskorištenih brojeva. Dakle,

$$\sigma = (1, 3, 8, 4) \circ (5, 7) \circ (6, 9) \in S_9.$$

Red permutacije σ kao elementa grupa S_9 jednak je najmanjem zajedničkom višekratniku duljina ciklusa u rastavu, a to su njihove duljine 4, 2 i 2. Stoga je red jednak 4.

2.17. Teorem. Svaka konačna grupa $(G, *)$ može se realizirati kao podgrupa simetrične grupe $(S_n, \circ)$ za neki prirodni broj n. Točnije, elementi grupe G mogu se poistovjetiti s permutacijama iz S_n na takav način da se operacija u grupi G podudara s operacijom kompozicije na tim permutacijama.

Prije dokaza napomenimo da ovaj teorem pokazuje izuzetnu važnost simetričnih grupa. Primjer za njegovu tvrdnju već smo susreli kad smo grupu izometrija peterokuta zapisali preko permutacija iz S_5. Općenito dokaz ove tvrdnje bazira se na Cayleyevoj tablici i daje realizaciju grupe reda m u simetričnoj grupi S_m. Međutim, ta realizacija nije jedinstvena, kao što pokazuje i primjer grupe izometrija peterokuta koja je realizirana kao podgrupa od S_5 u ranijem primjeru, a kroz dokaz ovog teorema realizira se i kao podgrupa grupe S_{10} jer je njen red jednak 10.

Dokaz. Neka je $(G, *)$ konačna grupa reda n. Numerirajmo njene elemente kao

$$G = \{g_1, g_2, \ldots, g_n\}$$

i pri tome neka je $g_1 = e$ neutralni element. Formirajmo Cayleyevu tablicu grupe G u čijem su prvom retku i stupcu elementi grupe složeni redom $g_1, g_2, \ldots, g_n$.

U svakom retku Cayleyeve tablice javlja se svaki element grupe točno jedanput. Naime, u retku označenom elementom g_i nalaze se produkti

$$g_i * g_1, g_i * g_2, \ldots, g_i * g_n.$$

Oni su svi različiti jer ako u grupi vrijedi

$$g_i * g_k = g_i * g_l,$$

onda primjenom operacije $*$ s lijeva elementom g_i^{-1} dobivamo $g_k = g_l$. Budući da ih ima n u retku su svi elementi grupe.

Dakle, svaki redak Cayleyjeve tablice predstavlja jednu permutaciju skupa $\{g_1, g_2, \ldots, g_n\}$. Označimo sa σ_i, gdje $i = 1, \ldots, n$, permutaciju u retku označenom s g_i. Svi retci, odnosno permutacije σ_i, su međusobno različite, jer na prvom mjestu stoji produkt

$$g_i * g_1 = g_i * e = g_i,$$

pa se tu već razlikuju. Na ovaj način možemo poistovjetiti element $g_i \in G$ s permutacijom $\sigma_i \in S_n$.

Neka je

$$H = \{\sigma_1, \sigma_2, \ldots, \sigma_n\} \subset S_n$$

tako dobiveni podskup od S_n. Pokažimo da se grupa G realizira kao podgrupa H od $(S_n, \circ)$. Točnije, pokažimo da za proizvoljne elemente $g_i, g_j \in G$ koje smo poistovjetili s permutacijama $\sigma_i, \sigma_j \in H$ vrijedi da je $g_i * g_j \in G$ poistovjećen s kompozicijom $\sigma_i \circ \sigma_j$. Time automatski dobivamo i činjenicu da je H podgrupa od S_n.

Najprije zapišimo permutacije σ_i i σ_j, koje odgovaraju recima Cayleyjeve tablice označenim s g_i i g_j, u obliku tablica

$$\sigma_i = \begin{pmatrix} g_1 & g_2 & \ldots & g_n \\ g_i * g_1 & g_i * g_2 & \ldots & g_i * g_n \end{pmatrix},$$

$$\sigma_j = \begin{pmatrix} g_1 & g_2 & \ldots & g_n \\ g_j * g_1 & g_j * g_2 & \ldots & g_j * g_n \end{pmatrix}.$$

Također, $g_i * g_j$ se poistovjećuje s permutacijom σ koju određuje redak kojeg označava element $g_i * g_j$, a to je

$$\sigma = \begin{pmatrix} g_1 & g_2 & \ldots & g_n \\ g_i * g_j * g_1 & g_i * g_j * g_2 & \ldots & g_i * g_j * g_n \end{pmatrix}.$$

Računamo, za proizvoljan $g_k \in G$,

$$(\sigma_i \circ \sigma_j)(g_k) = \sigma_i\big(\sigma_j(g_k)\big) = \sigma_i(g_j * g_k) = g_i * (g_j * g_k) = g_i * g_j * g_k = \sigma(g_k),$$

što pokazuje da je zaista $\sigma_i \circ \sigma_j = \sigma$. □

2.18. Neke grupe malog reda. U ovom primjeru određujemo sve moguće strukture grupa reda 2, 3 i 4. Drugim riječima, cilj je pronaći sve moguće Cayleyeve tablice do na poredak elemenata grupe. Time zapravo pokazujemo da, neovisno o konkretnoj realizaciji, svaka grupa tih redova ima jednu od Cayleyjevih tablica dobivenih u ovom primjeru.

Napomenimo najprije da je svaka grupa reda 1 naprosto trivijalna grupa koja se sastoji samo od neutralnog elementa. Njegova priroda ovisi o konkretnoj realizaciji, pa tako neutralni element može biti, primjerice, broj nula uz operaciju zbrajanja, broj 1 uz množenje, funkcija identitete uz operaciju kompozicije.

Za grupu $(G, *)$ reda 2, označimo elemente s

$$G = \{g_1, g_2\},$$

gdje je $g_1 = e$ neutralni element. Stoga je Cayleyeva tablica oblika

$*$	g_1	g_2
g_1	g_1	g_2
g_2	g_2	

gdje na prazno mjesto mora doći g_1 jer se u retku (i stupcu) Cayleyjeve tablice mora javiti svaki element grupe točno jednom. Tu činjenicu smo dokazali u prethodnom teoremu. Iz simetričnosti tablice obzirom na dijagonalu vidimo da vrijedi komutativnost. Dakle, sve grupe reda 2 imaju jednaku strukturu, odnosno jednaku Cayleyjevu tablicu, samo im realizacija može biti različita. Tako je, primjerice, struktura grupe $(\mathbb{Z}_2, +_2)$ reda 2, jednaka kao struktura grupe $(\{id, \sigma\}, \circ)$, gdje je σ bilo koja osna simetrija ravnine. Pritom ostatak 0 i id odgovaraju elementu g_1, a 1 i σ elementu g_2.

Neka je sada $(G, *)$ grupa reda 3. Označimo elemente te grupe s

$$G = \{g_1, g_2, g_3\},$$

gdje je $g_1 = e$ neutralni element. Tada treba vidjeti kako se sve može popuniti prazna mjesta Cayleyjeve tablice

$*$	g_1	g_2	g_3
g_1	g_1	g_2	g_3
g_2	g_2		
g_3	g_3		

pri čemu se u svakom retku i svakom stupcu javljaju svi elementi grupe točno jednom. To se može na samo jedan način. Najprije na križanju retka elementa g_2 i stupca elementa g_3 ne smije biti niti g_2 niti g_3, pa je tu sigurno g_1. Isto vrijedi i za redak elementa g_3 i stupac elementa g_2. Na kraju popunimo dijagonalu s elementima koji još fale u pojedinom retku. Dobije se

$*$	g_1	g_2	g_3
g_1	g_1	g_2	g_3
g_2	g_2	g_3	g_1
g_3	g_3	g_1	g_2

kao jedina moguća Cayleyjeva tablica grupe reda 3. Simetričnost tablice obzirom na dijagonalu pokazuje komutativnost. Kao i u slučaju grupa reda 2, time smo pokazali da sve grupe reda 3 imaju istu strukturu, jedino se njihova realizacija može razlikovati. Tako primjerice grupa $(\mathbb{Z}_3, +_3)$ se dobije ako za g_1 uvrstimo ostatak 0, za g_2 ostatak 1, te za g_3 ostatak 2.

Za grupu reda 4 označimo elemente

$$G = \{g_1, g_2, g_3, g_4\},$$

gdje je $g_1 = e$ neutralni element. Sada treba popuniti Cayleyjevu tablicu

$*$	g_1	g_2	g_3	g_4
g_1	g_1	g_2	g_3	g_4
g_2	g_2			
g_3	g_3			
g_4	g_4			

s time da se svaki element grupe javlja točno jednom u svakom retku i svakom stupcu. Za to ima više mogućnosti, ali među njima su samo dvije suštinski različite, odnosno sve ostale se mogu dobiti preimenovanjem elemenata iz te dvije. Te dvije tablice su

$*$	g_1	g_2	g_3	g_4
g_1	g_1	g_2	g_3	g_4
g_2	g_2	g_3	g_4	g_1
g_3	g_3	g_4	g_1	g_2
g_4	g_4	g_1	g_2	g_3

i

$*$	g_1	g_2	g_3	g_4
g_1	g_1	g_2	g_3	g_4
g_2	g_2	g_1	g_4	g_3
g_3	g_3	g_4	g_1	g_2
g_4	g_4	g_3	g_2	g_1

što prepuštamo čitaocu da provjeri. Uočimo da su ove dvije tablice suštinski različite jer su u prvoj elementi g_2 i g_4 reda 4, a samo g_3 reda 2, dok su u drugoj svi elementi osim neutralnog elementa g_1 reda 2.

Obje tablice su zaista Cayleyjeve tablice grupa. Prva tablica je Cayleyjeva tablica za primjerice grupu $(\mathbb{Z}_4, +_4)$ pri čemu ostatci 0, 1, 2, 3 odgovaraju, redom, elementima g_1, g_2, g_3 i g_4. Primjer grupe koja daje drugu Cayleyjevu tablicu je direktni produkt grupe $(\mathbb{Z}_2, +_2)$ same sa sobom. Dakle,

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1)\},$$

uz operaciju definiranu s

$$(k_1, l_1) +_2 (k_2, l_2) = (k_1 +_2 k_2, l_1 +_2 l_2),$$

za sve $(k_1, l_1), (k_2, l_2) \in \mathbb{Z}_2 \times \mathbb{Z}_2$. Pritom, $(0,0)$, $(0,1)$, $(1,0)$, $(1,1)$ odogovaraju, redom, elementima g_1, g_2, g_3 i g_4.

2.19. Grupa kružnice i grupe korijena iz jedinice. Ove grupe su podgrupe multiplikativne grupe kompleksnih brojeva $(\mathbb{C}^\times, \cdot)$ koju smo susreli u jednom od ranijih primjera.

Neka je

$$S^1 = \{z \in \mathbb{C} \,:\, |z| = 1\},$$

gdje je $|\,|$ oznaka za apsolutnu vrijednost kompleksnog broja. Ako je $z = a + b\sqrt{-1}$, onda je $|z| = \sqrt{a^2 + b^2}$ zapravo udaljenost kompleksnog broja z od ishodišta u kompleksnoj ravnini. Dakle, S^1 je jedinična kružnica u kompleksnoj ravnini.

Dokažimo da je S^1 podgrupa od $\mathbb{C}^\times$. Koristimo kriterij i svojstva apsolutnih vrijednosti. Naime, ako su $z_1, z_2 \in S^1$, odnosno $|z_1| = |z_2| = 1$, onda je

$$|z_1 \cdot z_2^{-1}| = |z_1| \cdot |z_2^{-1}| = |z_1| \cdot |z_2|^{-1} = 1,$$

pa je i $z_1 \cdot z_2^{-1} \in S^1$. Podgrupa $(S^1, \cdot)$ se obično naziva grupa kružnice.

Poznato je da kompleksan broj z možemo pisati u polarnom obliku

$$z = r \cdot e^{i\varphi} = r\,(\cos\varphi + i \sin\varphi)\,,$$

gdje je $i = \sqrt{-1}$ te e baza prirodnog logaritma. Pritom je $r = |z|$, a φ kut koji orjentirana dužina od ishodišta do točke z u kompleksnoj ravnini zatvara s pozitivnim dijelom realne osi. Tada je

$$S^1 = \left\{e^{i\varphi} \,:\, \varphi \in [0, 2\pi\rangle\right\}$$

jer na S^1 vrijedi $r = 1$, a funkcije sinus i kosinus su periodične s osnovnim periodom 2π pa je dovoljno promatrati kuteve $\varphi \in [0, 2\pi\rangle$. Dakle, jediničnu kružnicu S^1 možemo kao skup

identificirati s intervalom $[0, 2\pi\rangle$ pri čemu se kompleksan broj $z = e^{i\varphi} \in S^1$ identificira s kutem $\varphi \in [0, 2\pi\rangle$.

Množenje kompleksnih brojeva u polarnom obliku dano je formulom

$$z_1 \cdot z_2 = r_1 e^{i\varphi_1} \cdot r_2 e^{i\varphi_2} = r_1 r_2 \cdot e^{i(\varphi_1+\varphi_2)}.$$

Podsjetimo da vrijedi

$$e^{2k\pi i} = \cos(2k\pi) + i\sin(2k\pi) = 1$$

za sve $k \in \mathbb{Z}$. Stoga je zbroj $\varphi_1 + \varphi_2$ dovoljno promatrati do na dodavanje brojeva $2k\pi$ za $k \in \mathbb{Z}$. Drugim riječima, ako $\varphi_1 + \varphi_2$ zapišemo u obliku

$$\varphi_1 + \varphi_2 = 2k\pi + \psi,$$

pri čemu je $k \in \mathbb{Z}$, a $\psi \in [0, 2\pi\rangle$, onda su k i ψ jedinstveno određeni. To znači da za $\varphi_1, \varphi_2 \in [0, 2\pi\rangle$ možemo definirati operaciju $+_{2\pi}$ zbrajanja modulo 2π kao

$$\varphi_1 +_{2\pi} \varphi_2 = \psi.$$

Budući da je $\psi \in [0, 2\pi\rangle$, time je definirana binarna operacija na $[0, 2\pi\rangle$. U grupi S^1 vrijedi

$$e^{i\varphi_1} \cdot e^{\varphi_2} = e^{i(\varphi_1 +_{2\pi} \varphi_2)}$$

pa zapravo kompleksni brojevi iz S^1 koji odgovaraju kutevima φ_1 i φ_2 iz $[0, 2\pi\rangle$ pomnoženi daju kompleksan broj iz S^1 koji odgovara kutu $\varphi_1 +_{2\pi} \varphi_2$. To znači da se operacija $\cdot$ množenja na S^1 podudara s operacijom $+_{2\pi}$ na $[0, 2\pi\rangle$ kroz identifikaciju kompleksnog broja iz S^1 s odgovarajućim kutem iz $[0, 2\pi\rangle$. Posebno, $([0, 2\pi\rangle, +_{2\pi})$ je grupa. Može se reći da su $(S^1, \cdot)$ i $([0, 2\pi\rangle, +_{2\pi})$ dvije realizacije strukturno jedne te iste grupe.

U grupi kružnice ima još interesantnih podgrupa. Neka je n prirodan broj. Neka je

$$\mu_n = \{z \in \mathbb{C} : z^n = 1\}$$

skup svih n–tih korijena iz jedinice. Jasno je da je μ_n podskup od S^1 jer iz uvjeta $z^n = 1$ slijedi $|z|^n = 1$, a onda, budući da je $|z| \geq 0$, dobivamo $|z| = 1$.

Dokažimo koristeći kriterij da je μ_n podgrupa grupe kružnice $(S^1, \cdot)$. Neka su $z_1, z_2 \in \mu_n$, odnosno $z_1^n = z_2^n = 1$. Tada vrijedi

$$(z_1 \cdot z_2^{-1})^n = z_1^n \cdot (z_2^{-1})^n = z_1^n \cdot (z_2^n)^{-1} = 1$$

pa je i $z_1 \cdot z_2^{-1} \in \mu_n$. Dakle, μ_n je podgrupa grupe $(S^1, \cdot)$ koja se obično naziva grupa n–tih korijena iz jedinice.

Uočimo da je red grupe μ_n jednak n. To se vidi iz činjenice da uvjet $z^n = 1$ zapravo kaže da se μ_n sastoji od svih nultočaka polinoma $z^n - 1$. Taj polinom je n–tog stupnja i može se provjeriti da su sve nultočke različite. Dakle, ima ih točno n različitih.

Elementi grupe μ_n su n–ti korijeni iz jedinice, pa se u polarnom obliku mogu zapisati kao

$$\mu_n = \{e^{\frac{2k\pi i}{n}} : k = 0, 1, \ldots, n-1\} = \{1, e^{\frac{2\pi i}{n}}, e^{\frac{4\pi i}{n}}, \ldots, e^{\frac{2(n-1)\pi i}{n}}\}.$$

Množenje u polarnom obliku je dano formulom

$$e^{\frac{2k_1\pi i}{n}} \cdot e^{\frac{2k_2\pi i}{n}} = e^{\frac{2k_1\pi i}{n} + \frac{2k_2\pi i}{n}} = e^{\frac{2(k_1+k_2)\pi i}{n}}.$$

Budući da je $e^{2k\pi i} = 1$ za sve cijele brojeve $k \in \mathbb{Z}$, ako $k_1 + k_2$ zapišemo kao

$$k_1 + k_2 = q \cdot n + r,$$

gdje je $q \in \mathbb{Z}$ kvocijent, a $r \in \{0, 1, \ldots, n-1\}$ ostatak pri dijeljenju broja $k_1 + k_2$ s n, onda dalje dobivamo

$$e^{\frac{2(k_1+k_2)\pi i}{n}} = e^{\frac{2(q\cdot n+r)\pi i}{n}} = e^{2q\pi i} \cdot e^{\frac{2r\pi i}{n}} = e^{\frac{2r\pi i}{n}} = e^{\frac{2(k_1+_n k_2)\pi i}{n}}.$$

Pritom smo iskoristili činjenicu da je $k_1 +_n k_2 = r$ po samoj definiciji operacije $+_n$ zbrajanja modulo n. Dakle, za sve $k_1, k_2 \in \{0, 1, \ldots, n-1\} = \mathbb{Z}_n$, množenje u grupi μ_n dano je formulom

$$e^{\frac{2k_1\pi i}{n}} \cdot e^{\frac{2k_2\pi i}{n}} = e^{\frac{2(k_1+_n k_2)\pi i}{n}}.$$

Drugim riječima, ako μ_n kao skup identificiramo sa skupom $\mathbb{Z}_n$ i pritom $e^{\frac{2k\pi i}{n}} \in \mu_n$ odgovara elementu $k \in \mathbb{Z}_n$, onda množenjem elemenata iz μ_n koji odgovaraju ostacima $k_1, k_2 \in \mathbb{Z}_n$ dobivamo element iz μ_n koji odgovara ostatku $k_1 +_n k_2 \in \mathbb{Z}_n$. Stoga je grupa n–tih korijena iz jedinice $(\mu_n, \cdot)$ zapravo samo druga realizacija aditivne grupe ostataka $(\mathbb{Z}_n, +_n)$.

Na kraju, pitamo se što se dobije kad se n–ti korijeni iz jedinice za sve prirodne brojeve n promotre zajedno. Pokazuje se da na taj način ponovo dobivamo grupu, još jednu podgrupu od $(S^1, \cdot)$. Neka je

$$\mu = \bigcup_{n=1}^{\infty} \mu_n$$

skup svih korijena iz jedinice. Taj skup μ je podskup jedinične kružnice S^1 jer su svi μ_n podskupovi od S^1. Stoga se može primijeniti kriterij za podgrupe kako bi se dokazalo da je $(\mu, \cdot)$ grupa. Neka su $z_1, z_2 \in \mu$. Tada postoje prirodni brojevi n_1 i n_2 takvi da vrijedi

$$z_1^{n_1} = z_2^{n_2} = 1.$$

Takvi n_1 i n_2 nisu jedinstveni. Tada za $z_1 \cdot z_2^{-1}$ vrijedi

$$\left(z_1 \cdot z_2^{-1}\right)^{n_1 \cdot n_2} = z_1^{n_1 \cdot n_2} \cdot z_2^{-n_1 \cdot n_2} = (z_1^{n_1})^{n_2} \cdot (z_2^{n_2})^{-n_1} = 1,$$

pa je $z_1 \cdot z_2^{-1} \in \mu$. Uočimo da smo, umjesto s $n_1 \cdot n_2$, dokaz mogli provesti koristeći najmanji zajednički višekratnik od n_1 i n_2, ali tada bi zapis bio malo složeniji. Dakle, dokazali smo da je $(\mu, \cdot)$ grupa koju obično nazivamo grupa (svih) korijena iz jedinice.

2.20. Aditivna grupe matrica. Najprije promotrimo aditivne grupe matrica. Neka je $M_{m,n}(F)$ skup svih matrica tipa $m \times n$, što znači s m redaka i n stupaca, s elementima iz F, gdje je F jedan od skupova brojeva $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$. Dakle,

$$M_{m,n}(F) = \left\{ A = \begin{pmatrix} a_{1,1} & a_{1,2} & \ldots & a_{1,n} \\ a_{2,1} & a_{2,2} & \ldots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m,1} & a_{m,2} & \ldots & a_{m,n} \end{pmatrix} : a_{i,j} \in F \text{ za sve } i = 1, \ldots, m, j = 1, \ldots, n \right\}.$$

Matricu $A \in M_{m,n}(F)$ čiji je element na presjeku i–tog retka i j–tog stupca jednak $a_{i,j}$ kraće pišemo

$$A = (a_{i,j}),$$

gdje $i = 1, \ldots, m$, $j = 1, \ldots, n$. Također, za matricu $A \in M_{m,n}(F)$ koristimo oznaku $A_{i,j}$ za element na presjeku i–tog retka i j–tog stupca.

Na skupu matrica $M_{m,n}(F)$ definiramo operaciju + zbrajanja na sljedeći način. Neka su $A, B \in M_{m,n}(F)$. Tada je $A + B$ matrica u $M_{m,n}(F)$ koja na presjeku i–tog retka i j–tog stupca ima element

$$(A + B)_{i,j} = A_{i,j} + B_{i,j},$$

za sve $i = 1, \ldots, m$, $j = 1, \ldots, n$, gdje je zbrajanje na desnoj strani uobičajeno zbrajanje brojeva. Drugim riječima, matrice istog tipa zbrajamo element po element.

Uočimo da matrice iz $M_{m,n}(F)$ možemo promatrati kao uređene $m \cdot n$–torke brojeva iz F jer zapravo jedina, i to nevažna, razlika je u tome pišemo li elemente u nizu ili u pravokutnoj tablici. Zbog definicije zbrajanja element po element to zapravo znači da je $(M_{m,n}(F), +)$ direktni produkt aditivne grupe brojeva $(F, +)$ same sa sobom $m \cdot n$ puta. Kako smo već vidjeli da je direktni produkt grupa ponovo grupa, dobivamo da je $(M_{m,n}(F), +)$ grupa. Ta grupa je komutativna jer je i $(F, +)$ komutativna. U nastavku ćemo se baviti više multiplikativnim grupama matrica, jer ovaj opis preko direktnog produkta pokazuje da se svojstva aditivne grupe $(M_{m,n}(F), +)$ svode na svojstva grupa $(F, +)$.

2.21. Opća i specijalna linearna grupa. Za multiplikativne grupe potrebno je definirati množenje matrica. Poznato je da je to moguće jedino ako su matrice ulančane, to jest ako je broj stupaca prve matrice u produktu jednak broju redaka druge. Međutim, ako pritom matrice nisu kvadratne, odnosno imaju redaka koliko i stupaca, onda se množenjem ne ostaje u matricama istog tipa. Stoga, da bi se dobila multiplikativna algebarska na skupu matrica potrebno je promatrati kvadratne matrice.

Neka je $M_{n,n}(F)$ skup kvadratnih matrica tipa $n \times n$, odnosno s n redaka i n stupaca, gdje je sada F neki od skupova brojeva $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$. Neka su $A, B \in M_{n,n}(F)$. Tada je produkt $A \cdot B$ matrica iz $M_{n,n}(F)$ koja na presjeku i–tog retka i j–tog stupca ima element

$$(A \cdot B)_{i,j} = \sum_{k=1}^{n} A_{i,k} \cdot B_{k,j},$$

za sve $i, j = 1, \ldots, n$, gdje je zbrajanje i množenje na desnoj strani uobičajeno zbrajanje i množenje brojeva. Ova naizgled komplicirana definicija množenja posljedica je interpretacije matrice kao zapisa linearnog operatora u nekoj bazi, pri čemu množenje dvije matrice predstavlja kompoziciju odgovarajućih linearnih operatora. Međutim, mi ovdje nećemo objasniti tu vezu linearnih operatora i matrica.

Odredimo sada koju algebarsku strukturu tvori skup $M_{n,n}(F)$ kvadratnih matrica uz operaciju množenja matrica. Prema samoj definiciji množenja vidimo da je za $A, B \in M_{n,n}(F)$ i produkt $A \cdot B \in M_{n,n}(F)$ jer elementi produkta ostaju u skupu brojeva F. To znači da vrijedi svojstvo (G0) zatvorenosti za množenje u $M_{n,n}(F)$.

Svojstvo (G1) asocijativnosti množenja matrica također vrijedi. To se može dokazati direktno iz definicije množenja, ali elegantnije je sjetiti se interpretacije množenja kao kompozicije linearnih operatora i iskoristiti ranije dokazanu činjenicu da je kompozicija funkcija uvijek asocijativna.

Neutralni element za množenje matrica u $M_{n,n}(F)$ je jedinična matrica koju označavamo s I_n. To je matrica koja na glavnoj (silaznoj) dijagonali ima samo jedinice, a svi ostali

elementi su nule, odnosno

$$I_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & 1 \end{pmatrix}.$$

Koristeći Kroneckerov delta simbol

$$\delta_{i,j} = \begin{cases} 1, & \text{ako } i = j, \\ 0, & \text{ako } i \neq j, \end{cases}$$

za $i, j = 1, \dots, n$, jedinična matrica se može zapisati u obliku $I_n = (\delta_{i,j})$. Za proizvoljnu matricu $A = (a_{i,j}) \in M_{n,n}(F)$ računamo

$$(A \cdot I_n)_{i,j} = \sum_{k=1}^{n} A_{i,k} \cdot (I_n)_{k,j} = \sum_{k=1}^{n} a_{i,k} \cdot \delta_{k,j} = a_{i,j} \cdot 1 + \sum_{\substack{k=1 \\ k \neq j}}^{n} a_{i,k} \cdot 0 = a_{i,j} = A_{i,j},$$

$$(I_n \cdot A)_{i,j} = \sum_{k=1}^{n} (I_n)_{i,k} \cdot A_{k,j} = \sum_{k=1}^{n} \delta_{i,k} \cdot a_{k,j} = 1 \cdot a_{i,j} + \sum_{\substack{k=1 \\ k \neq i}}^{n} 0 \cdot a_{k,j} = a_{i,j} = A_{i,j},$$

što vrijedi za sve $i, j = 1, \dots, n$, pa je

$$A \cdot I_n = I_n \cdot A = A.$$

Time smo dokazali da je I_n neutralni element pa vrijedi svojstvo (G2).

Poznato je iz linearne algebre da je matrica invertibilna ako i samo je njena determinanta različita od nule, a to je ako i samo ako su reci, pa onda i stupci, linearno nezavisni. Takve matrice nazivaju se regularne. Ove činjenice postaju jasnije ako matricu iz $M_{n,n}(F)$ interpretiramo kao zapis linearnog operatora na n–dimenzionalnom vektorskom prostoru. Matrica je invertibilna ako i samo ako je odgovarajući linearni operator invertibilan. Ali već smo vidjeli da je funkcija na nekom skupu invertibilna ako i samo ako je bijekcija. Stoga je matrica invertibilna ako i samo ako je odgovarajući linearni operator bijekcija. Bijektivnost linearnog operatora ekvivalentna je gornjim uvjetima za invertibilinost (regularnost) matrice preko determinante i linearne nezavisnosti redaka. Sada je jasno da osim regularnih postoje i singularne matrice, a to su one čija je determinanta jednaka nuli, jer postoje linearni operatori koji nisu bijekcije. Stoga svojstvo (G3) postojanja inverza ne vrijedi za množenje na skupu matrica $M_{n,n}(F)$.

Dakle, skup $M_{n,n}(F)$ s operacijom množenja matrica čini monoid, ali ne čini grupu. Osim u posebnom slučaju $n = 1$ kada $M_{1,1}(F) = F$, taj monoid nije komutativan. Nije teško pronaći primjer matrica koje ne komutiraju. Primjerice, u $M_{2,2}(F)$ vrijedi

$$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 \\ 0 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix},$$

što pokazuje da komutativnost ne vrijedi. Ovaj primjer se jednostavno proširi na matrice iz $M_{n,n}(F)$ dodavajući jedinice na dijagonalu. Naime,

$$\begin{pmatrix} 2 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 1 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix} \cdot \begin{pmatrix} 2 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix},$$

pokazuje nekomutativnost množenja na $M_{n,n}(F)$.

Kao što smo vidjeli, invertibilni elementi svakog monoida tvore grupu. U monoidu $M_{n,n}(F)$ invertibilni elementi su regularne matrice. Skup svih takvih matrica označavamo s

$$GL_n(F) = \{A \in M_{n,n}(F) \,:\, A \text{ je regularna}\}.$$

Stoga je $(GL_n(F), \cdot)$ grupa koju nazivamo opća linearna grupa. Ta grupa je nekomutativna, osim u slučaju $n = 1$ kada je $GL_1(F) = F^\times$. To pokazuje, primjerice, isti primjer kao za $M_{n,n}(F)$ jer su u njemu matrice regularne.

Opća linearna grupa ima brojne važne podgrupe, od kojih ćemo mi neke spomenuti. Najprije, neka je

$$SL_n(F) = \{A \in GL_n(F) \,:\, \det A = 1\}.$$

Tada je $SL_n(F)$ podgrupa opće linearne grupe $(GL_n(F), \cdot)$ i nazivamo ju specijalna linearna grupa. To se dokazuje koristeći kriterij za podgrupe te Binet–Cauchyjev teorem koji daje multiplikativnost determinante. Zaista, ako su $A_1, A_2 \in SL_n(F)$, odnosno $\det A_1 = \det A_2 = 1$, onda

$$\det(A_1 \cdot A_2^{-1}) = \det A_1 \cdot \det(A_2^{-1}) = \det A_1 \cdot (\det A_2)^{-1} = \frac{\det A_1}{\det A_2} = 1,$$

pa je i $A_1 \cdot A_2^{-1} \in SL_n(F)$.

2.22. Klasične grupe. Podgrupe opće linearne grupe $GL_n(F)$, gdje je F neki od skupova brojeva $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$, možemo definirati nekim uvjetom koji matrice moraju zadovoljavati. Posebno su važni uvjeti oblika

$${}^tA \cdot J \cdot A = J, \qquad \text{te} \qquad {}^*A \cdot J \cdot A = J,$$

gdje je $J \in M_{n,n}(F)$ neka zadana matrica, ${}^tA$ označava matricu transponiranu matrici A, a ${}^*A$ konjugiranu matricu transponiranu matrici A. Transponirana matrica ${}^tA$ je matrica koja se dobije kad se reci matrice A zapišu u stupce, a konjugirana transponirana matrica ${}^*A$ kad se svi elementi transponirane matrice konjugiraju kao kompleksni brojevi. Podsjetimo da je za kompleksan broj $z = a + bi \in \mathbb{C}$, gdje je $i = \sqrt{-1}$, te $a, b \in \mathbb{R}$, kompleksno konjugiranje definirano sa

$$\overline{z} = a - bi.$$

Uočimo da za realne i racionalne brojeve vrijedi $\overline{z} = z$, pa za matrice iz $M_{n,n}(\mathbb{Q})$ i $M_{n,n}(\mathbb{R})$ vrijedi ${}^*A = {}^tA$.

Neka je skup

$$H = \{A \in GL_n(F) \,:\, {}^tA \cdot J \cdot A = J\}$$

definiran prvim od gornjih uvjeta. Tada je H podgrupa od $GL_n(F)$, što se pokazuje prema kriteriju za podgrupe. Zaista, neka su $A_1, A_2 \in H$, odnosno

$${}^tA_1 \cdot J \cdot A_1 = J,$$

$${}^tA_2 \cdot J \cdot A_2 = J.$$

Tada za $A_1 \cdot A_2^{-1}$ vrijedi

$${}^t(A_1 \cdot A_2^{-1}) \cdot J \cdot (A_1 \cdot A_2^{-1}) = {}^tA_2^{-1} \cdot ({}^tA_1 \cdot J \cdot A_1) \cdot A_2^{-1} = {}^tA_2^{-1} \cdot J \cdot A_2^{-1} = J,$$

pa je i $A_1 \cdot A_2^{-1} \in H$. Na isti način se vidi da je skup

$$H' = \{A \in GL_n(F) \,:\, {}^*A \cdot J \cdot A = J\},$$

definiran drugim od gornjih uvjeta, također podgrupa grupe $GL_n(F)$. U prethodnom se dokazu jedino transponiranje mora zamijeniti s konjugiranim transponiranjem. Uočimo da se za $F = \mathbb{Q}$ i $F = \mathbb{R}$ transponiranje podudara s konjugiranim transponiranjem, pa je $H' = H$. Stoga nam H' daje nešto novo u odnosu na H jedino u slučaju kompleksnih brojeva $F = \mathbb{C}$.

Navedimo sada neke važnije podgrupe koje se dobiju iz uvjeta koji smo koristili u definiciji podgrupa H i H' za neke posebne matrice J. Njima je zajedničko da se javljaju u klasičnoj geometriji kao grupe simetrija vektorskog prostora konačne dimenzije s nekom nedegeneriranom bilinearnom formom čija matrica je upravo J. Odatle i zajednički naziv klasične grupe. Neka je

$$J_n = \begin{pmatrix} 0 & \dots & 0 & 1 \\ \vdots & .^{\cdot^{\cdot}} & 1 & 0 \\ 0 & .^{\cdot^{\cdot}} & .^{\cdot^{\cdot}} & \vdots \\ 1 & 0 & \dots & 0 \end{pmatrix} \in M_{n,n}(F)$$

matrica koja na sporednoj (rastućoj) dijagonali ima jedinice, a sve ostalo su nule.

Simplektička grupa $Sp_{2n}(F)$ je podgrupa opće linearne grupe $GL_{2n}(F)$ definirana kao

$$Sp_{2n}(F) = \left\{ A \in GL_{2n}(F) \,:\, {}^tA \cdot \begin{pmatrix} 0 & J_n \\ -J_n & 0 \end{pmatrix} \cdot A = \begin{pmatrix} 0 & J_n \\ -J_n & 0 \end{pmatrix} \right\}.$$

Ovdje je matrica $J \in M_{2n,2n}(F)$ iz opće definicije grupe H jednaka

$$J = \begin{pmatrix} 0 & J_n \\ -J_n & 0 \end{pmatrix}.$$

Spomenimo da je determinanta svih matrica u simplektičkoj grupi jednaka jedan. Stoga je $Sp_n(F)$ zapravo podgrupa grupe $SL_n(F)$.

U ovom nepotpunom pregledu klasičnih grupa promatramo dva različita tipa ortogonalnih grupa. Prvi tip zovemo ortogonalna grupa i označavamo s $O_n(F)$. To je podgrupa grupe $GL_n(F)$ definirana s

$$O_n(F) = \left\{ A \in GL_n(F) \,:\, {}^tA \cdot J_n \cdot A = J_n \right\}.$$

U ovoj definiciji matrica $J \in M_{n,n}(F)$ iz opće definicije grupe H je jednaka $J = J_n$. Može se pokazati da matrice koje pripadaju ortogonalnoj grupi $O_n(F)$ imaju determinante jednake 1 ili -1. Stoga se definira i specijalna ortogonalna grupa $SO_n(F)$ koja se sastoji od onih matrica iz $O_n(F)$ čija je determinanta jednaka jedan, odnosno

$$SO_n(F) = O_n(F) \cap SL_n(F).$$

Jasno je da je $SO_n(F)$ grupa jer je jednaka presjeku dvije podgrupe od $GL_n(F)$.

Za drugi tip ortogonalne grupe $F = \mathbb{R}$ je skup realnih brojeva, odnosno ona je podgrupa grupe $GL_n(\mathbb{R})$. Ovaj tip ortogonalne grupe zovemo grupa (realnih) ortogonalnih matrica i označavamo s $O(n)$. To je podgrupa grupe $GL_n(\mathbb{R})$ definirana s

$$O(n) = \left\{ A \in GL_n(\mathbb{R}) \,:\, {}^tA \cdot A = I_n \right\}.$$

Ovo je također podgrupa dobivena iz opće konstrukcije grupe H uz matricu $J \in M_{n,n}(\mathbb{R})$ jednaku jediničnoj matrici $J = I_n$. Naime, lijeva strana uvjeta može se zapisati kao

$${}^tA \cdot A = {}^tA \cdot I_n \cdot A$$

jer je I_n neutralni element za množenje matrica. Ponovo ortogonalne matrice iz $O(n)$ imaju determinante jednake 1 ili -1. Stoga se definira i specijalna grupa ortogonalnih matrica $SO(n)$ kao

$$SO(n) = O(n) \cap SL_n(\mathbb{R})$$

To je zaista grupa jer je dobivena kao presjek dvaju podgrupa grupe $GL_n(\mathbb{R})$.

Na kraju navodimo primjer u kojem se koristi konjugirano transponiranje. Neka je sada $F = \mathbb{C}$ skup kompleksnih brojeva. Grupa unitarnih matrica, ili kraće, unitarna grupa $U(n)$ je podgrupa grupe $GL_n(\mathbb{C})$ i definira se s

$$U(n) = \left\{ A \in GL_n(\mathbb{C}) \,:\, {}^*A \cdot A = I_n \right\}.$$

U općoj konstrukciji grupe H' grupa $U(n)$ se dobije za matricu $J \in M_{n,n}(\mathbb{C})$ jednaku jediničnoj matrici $J = I_n$, jer se lijeva strana uvjeta može zapisati kao

$${}^*A \cdot A = {}^*A \cdot I_n \cdot A.$$

Kako je

$$\det({}^*A) = \overline{\det(A)},$$

primjenimo li Binet–Cauchyjev teorem na uvjet iz definicije grupe $U(n)$ dobivamo

$$\overline{\det(A)} \cdot \det A = 1,$$

odnosno $|\det(A)| = 1$. Dakle, determinante unitarnih matrica mogu biti svi kompleksni brojevi apsolutne vrijednosti 1. Stoga se ponovo može definirati specijalna unitarna grupa

$$SU(n) = U(n) \cap SL_n(F)$$

koja se sastoji od unitarnih matrica determinante jedan.

2.23. Modularna grupa i kongruencijske podgrupe. U poglavlju o multiplikativnim grupama promatrali smo opću linearnu grupu $GL_n(F)$ za skup brojeva F jednak $\mathbb{Q}$, $\mathbb{R}$ ili $\mathbb{C}$. Međutim, od velikog interesa, posebno u teoriji brojeva, jesu multiplikativne grupe matrica za skup cijelih brojeva $F = \mathbb{Z}$.

Na isti način kao ranije pokazuje se da skup kvadratnih matrica $M_{n,n}(\mathbb{Z})$ tvori monoid obzirom na operaciju množenja matrica. Stoga je dovoljno da dobijemo grupu promatrati skup invertibilnih elemenata tog monoida. Označimo taj skup s

$$SL_n^{\pm}(\mathbb{Z}) = \{A \in M_{n,n}(\mathbb{Z}) \,:\, A \text{ je invertibilna u } M_{n,n}(\mathbb{Z})\}\,.$$

Ova naizgled neobična oznaka posljedica je opisa invertibilnih matrica u $M_{n,n}(\mathbb{Z})$. Naime, da bi matrica bila invertibilna u $M_{n,n}(\mathbb{Z})$ nije dovoljno da je njena determinanta različita od nule, jer se ta determinanta u poznatoj formuli za inverznu matricu preko adjunkte javlja u nazivniku. Može se pokazati da ta determinanta mora imati multiplikativni inverz unutar cijelih brojeva $\mathbb{Z}$ jer inače inverzna matrica neće imati samo cijele brojeve kao svoje elemente. Međutim, mi smo ranije odredili invertibilne elementa monoida $(\mathbb{Z}, \cdot)$ i to su $\mathbb{Z}^\times = \{1, -1\}$. Stoga je matrica iz $M_{n,n}(\mathbb{Z})$ invertibilna u $M_{n,n}(\mathbb{Z})$ ako i samo ako je njena determinanta jednaka 1 ili -1. Dakle,

$$SL_n^{\pm}(\mathbb{Z}) = \{A \in M_{n,n}(\mathbb{Z}) \,:\, \det A \in \{\pm 1\}\}\,,$$

i to pojašnjava pojavu $\pm$ kao eksponenta u oznaci.

U grupi $SL_n^{\pm}(\mathbb{Z})$ možemo promatrati podgrupu $SL_n(\mathbb{Z})$ invertibilnih matrica u $M_{n,n}(\mathbb{Z})$ determinante jedan. Dakle,

$$SL_n(\mathbb{Z}) = \{A \in M_{n,n}(\mathbb{Z}) \,:\, \det A = 1\}\,.$$

Ovu podgrupu zovemo specijalna linearna grupa nad cijelim brojevima. Dokaz se provodi pomoću kriterija kao i za specijalne linearne grupe nad $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$, pa ga nećemo ponavljati.

Iznimno važan slučaj je $n = 2$. U tom slučaju grupa $SL_2(\mathbb{Z})$ se naziva modularna grupa jer se javlja u teoriji modularnih formi na gornjoj poluravnini. Modularne forme su jedan od centralnih predmeta proučavanja suvremene matematike. Modularna grupa se može zapisati kao

$$SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2,2}(\mathbb{Z}) \,:\, ad - bc = 1 \right\}.$$

U teoriji modularnih formi važne podgrupe modularne grupe su kongruencijske podgrupe. Njihovo ime dolazi od toga što su definirane pomoću kongruencija. Neka je $N > 1$ prirodan broj. Tada definiramo tri kongruencijske podgrupe

$$\begin{aligned}
\Gamma(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \,:\, a \equiv d \equiv 1,\ b \equiv c \equiv 0 \mod N \right\}, \\
\Gamma_1(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \,:\, a \equiv d \equiv 1,\ c \equiv 0 \mod N \right\}, \\
\Gamma_0(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \,:\, c \equiv 0 \mod N \right\}.
\end{aligned}$$

Uočimo da je $\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N)$. Da su to zaista podgrupe grupe $SL_2(\mathbb{Z})$ dokazujemo pomoću kriterija. Neka su matrice

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad \text{i} \quad \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$$

elementi jednog od skupova $\Gamma(N)$, $\Gamma_1(N)$ i $\Gamma_0(N)$. Treba dokazati da je tada i

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}^{-1}$$

opet iz istog skupa. Najprije uočimo da je inverz matrice iz $SL_2(\mathbb{Z})$ jednak

$$\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}^{-1} = \begin{pmatrix} d' & -b' \\ -c' & a' \end{pmatrix}$$

jer je determinanta jednaka jedan. Stoga vrijedi

$$\begin{aligned} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}^{-1} &= \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} d' & -b' \\ -c' & a' \end{pmatrix} \\ &= \begin{pmatrix} ad' - bc' & ba' - ab' \\ cd' - dc' & da' - cb' \end{pmatrix}. \end{aligned}$$

Ako su polazne matrice bile iz $\Gamma(N)$, odnosno

$$\begin{aligned} a \equiv d \equiv a' \equiv d' \equiv 1 \mod N, \\ b \equiv c \equiv b' \equiv c' \equiv 0 \mod N, \end{aligned}$$

onda vrijedi

$$\begin{aligned} ad' - bc' \equiv 1 \cdot 1 - 0 \cdot 0 = 1 \mod N, \\ da' - cb' \equiv 1 \cdot 1 - 0 \cdot 0 = 1 \mod N, \\ ba' - ab' \equiv 0 \cdot 1 - 1 \cdot 0 = 0 \mod N, \\ cd' - dc' \equiv 0 \cdot 1 - 1 \cdot 0 = 0 \mod N. \end{aligned}$$

Dakle,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}^{-1} \in \Gamma(N).$$

Slično, ako su polazne matrice bile u $\Gamma_1(N)$, odnosno

$$\begin{aligned} a \equiv d \equiv a' \equiv d' \equiv 1 \mod N, \\ c \equiv c' \equiv 0 \mod N, \end{aligned}$$

onda vrijedi

$$\begin{aligned} ad' - bc' \equiv 1 \cdot 1 - b \cdot 0 \equiv 1 \mod N, \\ da' - cb' \equiv 1 \cdot 1 - 0 \cdot b' \equiv 1 \mod N, \\ cd' - dc' \equiv 0 \cdot 1 - 1 \cdot 0 = 0 \mod N, \end{aligned}$$

pa je izraz iz kriterija također u $\Gamma_1(N)$. I na kraju, ako su polazne matrice bile iz $\Gamma_0(N)$, odnosno

$$c \equiv c' \equiv 0 \mod N,$$

onda je

$$cd' - dc' \equiv 0 \cdot d' - d \cdot 0 \equiv 0 \mod N,$$

pa je izraz iz kriterija također u $\Gamma_0(N)$.

3. Homomorfizmi grupa, jezgra i slika

3.1. Definicija. Neka su $(G, *)$ i $(H, \bullet)$ dvije grupe. Homomorfizam grupe G u grupu H je funkcija $f : G \to H$ za koju vrijedi

$$f(g_1 * g_2) = f(g_1) \bullet f(g_2)$$

za sve $g_1, g_2 \in G$. Riječima rečeno, slika po funkciji f operacije $*$ iz G primijenjene na dva elementa iz G, jednaka je operaciji $\bullet$ iz grupe H primijenjenoj na slike tih dvaju elemenata. Dakle, isto se dobije neovisno o tome jesmo li najprije primijenili funkciju f ili izvršili operaciju u odgovarajućoj grupi. Kažemo da homomorfizam čuva strukturu grupa.

Ako je homomorfizam $f : G \to H$ injektivan naziva se monomorfizam, ako je surjektivan epimorfizam, a ako je bijektivan izomorfizam. Posebne nazive imaju homomorfizmi grupe u samu sebe. Tako se homomorfizam $f : G \to G$ zove endomorfizam, a izomorfizam $f : G \to G$ automorfizam.

Skup svih homomorfizama grupe G u grupu H označava se $\mathrm{Hom}(G, H)$, a skup izomorfizama $\mathrm{Iso}(G, H)$. Skup endomorfizama grupe G označava se $\mathrm{End}(G)$, a automorfizama $\mathrm{Aut}(G)$.

3.2. Svojstva homomorfizma. Neka je $f : G \to H$ homorfizam. Tada vrijedi

(1) $f(e_G) = e_H$, gdje su e_G i e_H neutralni elementi odgovarajućih grupa,
(2) $f(g^{-1}) = f(g)^{-1}$.

Pritom, u drugom svojstvu je na lijevoj strani invertiranje u grupi G, a na desnoj u H. To svojstvo zapravo kaže da se isto dobije neovisno o tome jesmo li najprije invertirali pa zatim primijenili funkciju f, ili obratno.

Dokaz. Najprije dokazujemo prvo svojstvo. Prema svojstvu neutralnog elementa i definiciji homomorfizma, vrijedi

$$f(e_G) = f(e_G * e_G) = f(e_G) \bullet f(e_G).$$

Primjenimo li na obje stane ove jednakosti operaciju $\bullet$ s inverzom elementa $f(e_G) \in H$ (koji postoji jer je H grupa), dobivamo

$$e_H = f(e_G) \bullet f(e_G)^{-1} = f(e_G) \bullet f(e_G) \bullet f(e_G)^{-1} = f(e_G),$$

što je i trebalo dokazati.

Naglasimo da smo ovdje na gornju jednakost primijenili $\bullet$ s desna. U ovom slučaju isto bi se dobilo i da smo primijenili s lijeva, ali to nije uvijek točno jer nisu sve grupe komutativne. Stoga kad primjenjujemo operaciju iz grupe na obje strane neke jednakosti važno je naglasiti s koje strane to radimo.

Za dokaz drugog svojstva uočimo da prema definiciji homomorfizma, svojstvu inverza i već dokazanom prvom svojstvu, vrijedi

$$f(g^{-1}) \bullet f(g) = f(g^{-1} * g) = f(e_G) = e_H,$$
$$f(g) \bullet f(g^{-1}) = f(g * g^{-1}) = f(e_G) = e_H.$$

Stoga $f(g^{-1})$ ima svojstvo inverza elementa $f(g)$ u grupi H, pa zbog jedinstvenosti inverza dobivamo $f(g)^{-1} = f(g^{-1})$. □

3.3. Jezgra i slika. Neka je $f : G \to H$ homomorfizam grupa. Tada definiramo jezgru homomorfizma f, u oznaci $\mathrm{Ker}f$ (od engleskog kernel), kao

$$\mathrm{Ker}f = \{g \in G \,|\, f(g) = e_H\}\,.$$

Dakle, jezgra je podskup od G koji se sastoji od svih onih elemenata iz G koji se pomoću f preslikaju u neutralni element grupe H. Uočimo da $\mathrm{Ker}f$ nikad nije prazan skup jer svojstvo (1) homomorfizma kaže da je neutralni element $e_G \in \mathrm{Ker}f$.

Slika homomorfizma f, u oznaci $\mathrm{Im}f$ (od engleskog image), se definirao kao uobičajena slika funkcije f, odnosno

$$\begin{aligned}\mathrm{Im}f &= \{h \in H \,|\, \text{postoji } g \in G \text{ takav da } h = f(g)\} \\ &= \{f(g) \,|\, g \in G\}.\end{aligned}$$

Dakle, slika je podskup od H koji se sastoji od svih onih elemenata u H u koje se pomoću H preslika neki element iz G. Kao i jezgra, ni slika nikad nije prazan skup, jer svojstvo (1) homomorfizma pokazuje da je uvijek $e_H \in \mathrm{Im}f$.

3.4. Teorem. Neka je $f : G \to H$ homomorfizam grupa. Tada je jezgra $\mathrm{Ker}f$ podgrupa od G, a slika $\mathrm{Im}f$ podgrupa od H.

Dokaz. Obje tvrdnje dokazujemo pomoću kriterija za podgrupe. Neka su $g_1, g_2 \in \mathrm{Ker}f$, odnosno $f(g_1) = f(g_2) = e_H$. Koristeći definiciju i svojstva homomorfizma računamo

$$f(g_1 * g_2^{-1}) = f(g_1) \bullet f(g_2^{-1}) = f(g_1) \bullet f(g_2)^{-1} = e_H \bullet e_H^{-1} = e_H.$$

Dakle, $g_1 * g_2^{-1} \in \mathrm{Ker}f$, pa je $\mathrm{Ker}f$ grupa.

Neka su sada $h_1, h_2 \in \mathrm{Im}f$. Tada postoje $g_1, g_2 \in G$ takvi da je $h_1 = f(g_1)$ i $h_2 = f(g_2)$. Stoga, prema definiciji i svojstvima homomorfizma, dobivamo

$$h_1 \bullet h_2^{-1} = f(g_1) \bullet f(g_2)^{-1} = f(g_1) \bullet f(g_2^{-1}) = f(g_1 * g_2^{-1}),$$

a budući da je $g_1 * g_2^{-1} \in G$, slijedi $h_1 \bullet h_2^{-1} \in \mathrm{Im}f$. Dakle, $\Im f$ je grupa. □

3.5. Slika i praslika podgrupe. Neka je $f : G \to H$ homomorfizam grupa. Neka je G' podgrupa od G. Tada je slika podgrupe G' naprosto slika restrikcije homomorfizma f s G na G', odnosno

$$f(G') = \{f(g') \,|\, g' \in G'\} = \mathrm{Im}(f|_{G'}).$$

Budući da je restrikcija homomorfizma na podgrupu opet homomorfizam, $f(G')$ je podgrupa od H kao slika homomorfizma.

Neka je sada H' podgrupa od H. Tada se praslika podgrupe H' definira kao

$$f^{-1}(H') = \{g \in G \,|\, f(g) \in H'\}.$$

Uočimo da je jezgra zapravo praslika trivijalne podgrupe $\{e_H\}$. Dokaz da je $f^{-1}(H')$ podgrupa od G je potpuno analogan dokazu da je jezgra homomorfizma podgrupa. Neka su $g_1, g_2 \in f^{-1}(H')$. Dakle, $f(g_1) \in H'$ i $f(g_2) \in H'$. Tada je, prema definiciji i svojstvima homomorfizma

$$f(g_1 * g_2^{-1}) = f(g_1) \bullet f(g_2)^{-1} \in H',$$

gdje smo koristili kriterij za podgrupe i činjenicu da je H' podgrupa. Dakle, $g_1 g_2^{-1} \in f^{-1}(H')$ pa je praslika zaista podgrupa od G.

3.6. Teorem (kriterij za monomorfizam). Neka je $f : G \to H$ homomorfizam grupa. Tada je f monomorfizam ako i samo ako je jezgra trivijalna, odnosno $\mathrm{Ker} f = \{e_G\}$.

Dokaz. Pretpostavimo najprije da je f monomorfizam, te neka je $g \in \mathrm{Ker} f$, odnosno $f(g) = e_H$. S druge strane, prema svojstvima homomorfizma, $f(e_G) = e_H$. Dakle, $f(g) = f(e_G)$, pa zbog injektivnosti mora biti $g = e_G$. Time smo dokazali da je jezgra trivijalna.

Obratno, pretpostavimo da je jezgra trivijalna, te da je $f(g_1) = f(g_2)$ za neke elemente $g_1, g_2 \in G$. Primjenimo li na obje strane te jednakosti operaciju $*$ s elementom $f(g_2)^{-1}$, dobivamo

$$f(g_1) * f(g_2)^{-1} = e_H.$$

Prema svojstvima homomorfizma, izraz na lijevoj strani jednak je

$$f(g_1) * f(g_2)^{-1} = f(g_1) * f(g_2^{-1}) = f(g_1 * g_2^{-1}),$$

pa vrijedi

$$f(g_1 * g_2^{-1}) = e_H.$$

To pokazuje, prema definiciji jezgre, da je $g_1 * g_2^{-1} \in \mathrm{Ker} f$. Ali po pretpostavci jezgra je trivijalna, pa

$$g_1 * g_2^{-1} = e_G.$$

Primjenom operacije $*$ s elementom g_2 na obje strane te jednakosti dobije se $g_1 = g_2$, što pokazuje da je f injektivna, odnosno monomorfizam. □

3.7. Teorem. Neka je $(G, *)$ grupa.

(1) Skup $\mathrm{End}\, G$ svih endomorfizama grupe G uz operaciju $\circ$ kompozicije funkcija čini monoid.
(2) Skup $\mathrm{Aut}\, G$ svih automorfizama grupe G uz operaciju $\circ$ kompozicije funkcija čini grupu.

Dokaz. Najprije dokazujemo prvu tvrdnju. Treba provjeriti svojstva iz definicije monoida. Neka su $f_1, f_2 : G \to G$ endomorfizmi, odnosno $f_1, f_2 \in \mathrm{End}\, G$. Njihova kompozicija $f_1 \circ f_2$ je opet funkcija iz G u G, te prema svojstvima homomorfizama f_1 i f_2 vrijedi

$$\begin{aligned}(f_1 \circ f_2)(g_1 * g_2) &= f_1\big(f_2(g_1 * g_2)\big) = f_1\big(f_2(g_1) * f_2(g_2)\big) \\ &= f_1\big(f_2(g_1)\big) * f_1\big(f_2(g_2)\big) = (f_1 \circ f_2)(g_1) * (f_1 \circ f_2)(g_2)\end{aligned}$$

za sve $g_1, g_2 \in G$, pa je $f_1 \circ f_2$ također endomorfizam, odnosno $f_1 \circ f_2 \in \mathrm{End}\, G$. Time je dokazana zatvorenost.

Kompozicija funkcija je uvijek asocijativna, što smo provjerili u primjerima grupa funkcija. Iz tih primjera znamo i da je neutralni element za kompoziciju funkcija identiteta id_G na G, a budući da je

$$id_G(g_1 * g_2) = g_1 * g_2 = id_G(g_1) * id_G(g_2),$$

za sve $g_1, g_2 \in G$, vidimo da je id_G endomorfizam. Stoga, $\mathrm{End}\, G$ ima identitetu id_G za neutralni element. Dakle, $(\mathrm{End}\, G, \circ)$ je zaista monoid.

Uočimo da to nije grupa jer inverznu funkciju, a to je inverz obzirom na operaciju kompozicije, imaju samo bijekcije, a endomorfizam ne mora nužno biti bijektivan.

Za drugu tvrdnju, primjetimo najprije da je kompozicija bijekcija bijekcija, te da je identiteta id_G bijekcija. Stoga, ako su $f_1, f_2 : G \to G$ automorfizmi, odnosno $f_1, f_2 \in \mathrm{Aut}\, G$, onda je i $f_1 \circ f_2 \in \mathrm{Aut}\, G$, jer smo svojstvo iz definicije homomorfizma provjerili u dokazu prve

tvrdnje. Asocijativnost kompozicije uvijek vrijedi. Neutralni element u $\operatorname{Aut} G$ je identiteta id_G budući da je ona automorfizam.

Preostaje provjeriti postojanje inverza. Neka je $f : G \to G$ automorfizam, odnosno $f \in \operatorname{Aut} G$. Inverz od f obzirom na operaciju kompozicije funkcija je inverzna funkcija koju označavamo s f^{-1}. Ona postoji jer je f bijekcija i sigurno je također bijekcija. Stoga, da bi dokazali da je inverzna funkcija f^{-1} automorfizam, treba provjeriti svojstvo iz definicije homomorfizma. Neka su $g_1, g_2 \in G$ proizvoljni. Zbog bijektivnosti automorfizma f postoje i jedinstveni su $g_1', g_2' \in G$ takvi da vrijedi $g_1 = f(g_1')$ i $g_2 = f(g_2')$. Prema definiciji homomorfizma vrijedi

$$g_1 * g_2 = f(g_1') * f(g_2') = f(g_1' * g_2').$$

Budući da je f^{-1} inverzna funkcija od f, dobivamo

$$f^{-1}(g_1 * g_2) = f^{-1}\big(f(g_1' * g_2')\big) = g_1' * g_2'.$$

S druge strane,

$$f^{-1}(g_1) * f^{-1}(g_2) = f^{-1}(f(g_1')) * f^{-1}(f(g_2')) = g_1' * g_2'.$$

Desne strane u posljednje dvije jednakosti su međusobno jednake, pa moraju biti i lijeve, odnosno

$$f^{-1}(g_1 * g_2) = f^{-1}(g_1) * f^{-1}(g_2).$$

Time smo dokazali da je f^{-1} homomorfizam, pa onda i $f^{-1} \in \operatorname{Aut} G$. □

3.8. Unutarnji automorfizmi. Neka je $(G, *)$ grupa. Unutarnji automorfizmi su posebna vrsta automorfizama grupe G koji se definiraju na sljedeći način. Neka je $g \in G$ fiksirani element grupe g. Tada definiramo unutarnji automorfizam $I_g : G \to G$, određen elementom g, formulom

$$I_g(x) = g * x * g^{-1},$$

za sve $x \in G$. Izraz na desnoj strani je toliko važan u teoriji grupa da ima i poseban naziv, a to je konjugiranje. Kažemo da smo element x konjugirali elementom g. Skup svih unutarnjih automorfizama grupe G se označava $\operatorname{Int} G$.

Provjerimo najprije da je unutarnji automorfizam zaista automorfizam, odnosno $I_g \in \operatorname{Aut} G$. Najprije provjeravamo svojstvo iz definicije homomorfizma. Vrijedi

$$I_g(x_1 * x_2) = g * x_1 * x_2 * g^{-1} = g * x_1 * e * x_2 * g^{-1} = (g * x_1 * g^{-1}) * (g * x_2 * g^{-1}) = I_g(x_1) * I_g(x_2)$$

za sve $x_1, x_2 \in G$. Injektivnost od I_g provjeravamo pomoću kriterija. Po definiciji, jezgra je jednaka

$$\begin{aligned} \operatorname{Ker} I_g &= \{x \in G \mid I_g(x) = e_G\} \\ &= \{x \in G \mid g * x * g^{-1} = e_G\} \\ &= \{x \in G \mid x = g^{-1} * e_G * g = e_G\}, \end{aligned}$$

gdje smo u posljednjem koraku na jednakost $g * x * g^{-1} = e_G$ primjenili operaciju $*$ i to s lijeva s elementom g^{-1} te s desna s elementom g. Dakle, $\operatorname{Ker} I_g = \{e_G\}$ je trivijalna, pa je I_g monomorfizam. Na kraju provjerimo surjektivnost. Neka je $h \in G$ proizvoljan. Pitamo se postoji li $x \in G$ takav da vrijedi $I_g(x) = h$, odnosno

$$g * xg^{-1} = h.$$

Primjenom opearacije $*$ i to s lijeva s elementom g^{-1} te s desna s elementom g, dobivamo

$$x = g^{-1} * h * g.$$

Time smo dokazali da traženi x postoji (čak smo ga i eksplicitno izračunali), pa je I_g i epimorfizam. Dakle, I_g je automorfizam.

3.9. Svojstva unutarnjih automorfizama. Neka je $(G, *)$ grupa. Za element $g \in G$, neka je I_g unutarnji automorfizam određen njime. Tada vrijedi

(1) $I_{g_1} \circ I_{g_2} = I_{g_1 * g_2}$ za sve $g_1, g_2 \in G$,
(2) $I_g^{-1} = I_{g^{-1}}$ za sve $g \in G$,
(3) $(\operatorname{Int} G, \circ)$ je grupa.

Dokaz. Najprije dokazujemo prvo svojstvo. Kompozicija unutarnjih automorfizama, izračunata na proizvoljnom elementu $x \in G$, jednaka je

$$\begin{aligned}(I_{g_1} \circ I_{g_2})(x) &= I_{g_1}\big(I_{g_2}(x)\big) = I_{g_1}(g_2 * x * g_2^{-1}) = g_1 * (g_2 * x * g_2^{-1}) * g_1^{-1} \\ &= (g_1 * g_2) * x * (g_1 * g_2)^{-1} = I_{g_1 * g_2}(x),\end{aligned}$$

pri čemu smo koristili formulu $(g_1 * g_2)^{-1} = g_2^{-1} * g_1^{-1}$. Time je dokazano prvo svojstvo.

Za drugo svojstvo treba odrediti inverznu funkciju unutarnjeg automorfizma I_g. Neka je $x \in G$ proizvoljan. Budući da je I_g bijekcija, postoji i jedinstven je x' takav da

$$x = I_g(x') = g * x' * g^{-1}.$$

Sada, prema definiciji inverzne funkcije, $I_g^{-1}(x) = x'$. S druge strane primjenjujući operaciju $*$ na gornju jednakost s lijeva s elementom g^{-1}, te s desna s elementom g, dobivamo

$$g^{-1} * x * g = x'$$

Uspoređujući dvije formule za x' slijedi

$$I_g^{-1}(x) = g^{-1} * x * g = I_{g^{-1}}(x).$$

Time smo dokazali i drugo svojstvo.

Treće svojstvo se dokazuje pomoću kriterija za podgrupe, jer je skup unutarnjih automorfizama $\operatorname{Int} G$ podskup skupa svih automorfizama $\operatorname{Aut} G$, za koji znamo da je grupa. Neka su $I_{g_1}, I_{g_2} \in \operatorname{Int} G$. Tada, koristeći već dokazana prva dva svojstva, dobivamo

$$I_{g_1} \circ I_{g_2}^{-1} = I_{g_1} \circ I_{g_2^{-1}} = I_{g_1 * g_2^{-1}}.$$

Dakle, $I_{g_1} \circ I_{g_2}^{-1} \in \operatorname{Int} G$, jer je jednak unutarnjem automorfizmu određenom elementom $g_1 * g_2^{-1} \in G$, pa je $\operatorname{Int} G$ grupa prema kriteriju. □

Prethodni dokaz svojstava unutarnjih automorfizama direktnim računom može se bitno pojednostaviti ako tražena svojstva unutarnjih automorfizama interpretiramo malo apstraktnije, odnosno algebarskije. To ćemo napraviti u sljedećem teoremu. Iako je nakon dokaza sljedećeg teorema prethodni dokaz zapravo suvišan, uključili smo ga da bi čitaoc mogao uočiti prednosti algebarskog pristupa.

3.10. Teorem. Neka je $(G, *)$ grupa, te neka je $(\mathrm{Aut}\, G, \circ)$ grupa njenih automorfizama. Neka je $\Phi : G \to \mathrm{Aut}\, G$ preslikavanje definirano sa

$$\Phi(g) = I_g$$

za $g \in G$, gdje je I_g unutarnji automorfizam grupe G određen njenim elementom g.

Tada je Φ homomorfizam grupa, pa stoga vrijede svojstva (1) i (2) unutarnjih automorfizama. Slika homomorfizma Φ je $\mathrm{Int}\, G$. Posebno, vrijedi svojstvo (3) unutarnjih automorfizama, odnosno skup svih unutarnjih automorfizama $\mathrm{Int}\, G$ čini podgrupu grupe svih automorfizama $\mathrm{Aut}\, G$ grupe G. Jezgra homomorfizma Φ je centar $Z(G)$ grupe G, koji se definira kao skup onih elemenata iz G koji komutiraju sa svim elementima iz G, odnosno

$$Z(G) = \{g \in G \,|\, g * x = x * g \text{ za sve } x \in G\}.$$

Posebno, centar $Z(G)$ grupe G je podgrupa od G.

Dokaz. Najprije dokažimo da je preslikavanje Φ homomorfizam. Koristeći formulu za Φ, uvjet $\Phi(g_1 * g_2) = \Phi(g_1) \circ \Phi(g_2)$ iz definicije homomorfizma glasi

$$I_{g_1 * g_2} = I_{g_1} \circ I_{g_2},$$

za sve $g_1, g_2 \in G$. Uočimo da je to upravo svojstvo (1) unutarnjih automorfizama. Njega i u ovom dokazu moramo dokazati direktnim računom, na isti način kao prije. Međutim, interpretacija svojstva (1) preko homomorfizma Φ iz grupe G u $\mathrm{Aut}\, G$ odmah daje preostala svojstva, jer možemo primijeniti općenite činjenice o homomorfizmima koje smo već dokazali.

Zaista, svojstvo (2) koje glasi $I_g^{-1} = I_{g^{-1}}$, za sve $g \in G$, se pomoću Φ zapisuje kao

$$\Phi(g)^{-1} = \Phi(g^{-1}),$$

za sve $g \in G$, a to je svojstvo (2) homomorfizama grupa koje upravo kaže da je slika inverza jednaka inverzu slike.

Svojstvo (3) unutarnjih automorfizama slijedi iz činjenice da je slika homomorfizma grupa. Naime, $\mathrm{Im}\Phi = \mathrm{Int}\, G$, jer se unutarnji automorfizam određen elementom $g \in G$ dobije upravo kao $\Phi(g)$.

Budući da je jezgra homomorfizma uvijek podgrupa, preostaje, za dokaz posljednje tvrnje teorema, izračunati jezgru od Φ. Po definiciji jezgre (podsjećamo da je identiteta id_G neutralni element u $\mathrm{Aut}\, G$), formulama za funkciju Φ i unutarnji automorfizam I_g dobivamo

$$\begin{aligned}
\mathrm{Ker}\Phi &= \{g \in G \,|\, \Phi(g) = id_G\} \\
&= \{g \in G \,|\, I_g = id_G\} \\
&= \{g \in G \,|\, I_g(x) = id_G(x) \text{ za svaki } x \in G\} \\
&= \left\{g \in G \,|\, g * x * g^{-1} = x \text{ za svaki } x \in G\right\} \\
&= \{g \in G \,|\, g * x = x * g \text{ za svaki } x \in G\}\,,
\end{aligned}$$

a to je upravo definicija centra $Z(G)$ grupe G. Pritom smo u zadnjem koraku na obje strane jednakosti primijenili operaciju $*$ s elementom g s desna. □

LIJEPO Ovim dokazom smo ujedno jednostavnije dokazali i ranije dokazana svojstva unutarnjih automorfizama. Ključna stvar u ovom dokazu je interpretacija svojstva (1) unutarnjih automorfizama kao homomorfizma iz grupe G u $\mathrm{Aut}\, G$. Takva interpretacija je lijepi primjer algebraizacije u samoj algebri. Na neki način, iako se bavimo samim algebarskim

strukturama (grupama i grupama njihovih automorfizama), moguće je preći na višu razinu apstrakcije i uočiti da neki objekt koji proučavamo i sam ima neka svojstva algebarske strukture te na taj način iskoristiti općenite činjenice o tim strukturama da bismo donijeli zaključke o proučavanom objektu. Ovakav način razmišljanja prisutan je i često se koristi u čitavoj matematici. Algebra daje općenite tvrdnje o algebarskim strukturama, a u konkretnim problemima drugih područja matematike (kao i unutar same algebre) pokazuje se iznimno korisnim uočiti neku algebarsku strukturu te primjeniti te općentite tvrdnje i time riješiti polazni problem. Kažemo da smo time algebraizirali polazni problem. Čitavo dvadeseto stoljeće u povijesti matematike može se na neki način smatrati stoljećem algebraizacije.

4. Primjeri homomorfizama

4.1. Homomorfizmi aditivne grupe cijelih brojeva. Neka je m prirodan broj. Promatramo aditivnu grupu cijelih brojeva $(\mathbb{Z}, +)$ i funkciju $f : \mathbb{Z} \to \mathbb{Z}$ definiramo formulom

$$f(k) = mk$$

za sve $k \in \mathbb{Z}$, gdje je množenje na desnoj strani uobičajeno množenje cijelih brojeva. Pokažimo da je f homomorfizam. Zaista, vrijedi

$$f(k + l) = m(k + l) = mk + ml = f(k) + f(l)$$

za sve $k, l \in \mathbb{Z}$.

Odredimo jezgru tog homomorfizma. Po definiciji jezgre dobivamo

$$\begin{aligned} \mathrm{Ker} f &= \{k \in \mathbb{Z} : f(k) = 0\} \\ &= \{k \in \mathbb{Z} : mk = 0\} \\ &= \{k \in \mathbb{Z} : k = 0\} \\ &= \{0\}. \end{aligned}$$

Dakle, jezgra je trivijalna, pa je prema kriteriju f monomorfizam.

Slika homomorfizma f je po definiciji jednaka

$$\begin{aligned} \mathrm{Im} f &= \{f(k) : k \in \mathbb{Z}\} \\ &= \{mk : k \in \mathbb{Z}\} \\ &= m\mathbb{Z}. \end{aligned}$$

Dakle, slika homomorfizma f je podgrupa $m\mathbb{Z}$ grupe $(\mathbb{Z}, +)$ koju smo već susreli u primjerima grupa. Uočimo da za sve $m \geq 2$ ta podgrupa nije jednaka čitavom $\mathbb{Z}$ pa tada f nije epimorfizam. Za $m = 1$ vrijedi $1 \cdot \mathbb{Z} = \mathbb{Z}$, pa je tada f epimorfizam. Ali u tom slučaju $f(k) = 1 \cdot k = k$ za sve $k \in \mathbb{Z}$, pa je tada f zapravo identiteta.

4.2. Kanonski epimorfizam cijelih brojeva na klase ostataka. Neka je $m > 1$ prirodan broj. Promatramo aditivnu grupu cijelih brojeva $(\mathbb{Z}, +)$ i aditivnu grupu klasa ostataka $(\mathbb{Z}_m, +_m)$. Funkciju $f : \mathbb{Z} \to \mathbb{Z}_m$ definiramo formulom

$$f(k) = \text{ostatak koji daje } k \text{ pri dijeljenju s } m.$$

Ako grupu $\mathbb{Z}_m$ shvatimo kao grupu klasa ekvivalencije obzirom na relaciju kongruencije modulo m, onda se ta formula može zapisati u obliku

$$f(k) = [k]$$

za sve $k \in \mathbb{Z}$. Pritom koristimo oznaku $[k]$ za klasu ekvivalencije cijelog broja k. Koristeći definiciju zbrajanja klasa dobivamo

$$f(k+l) = [k+l] = [k] + [l] = f(k) + f(l)$$

za sve $k, l \in \mathbb{Z}$. Dakle, f je homomorfizam.

Odredimo sada jezgru homomorfizma f. Po definiciji jezgre vrijedi

$$\begin{aligned} \mathrm{Ker} f &= \{k \in \mathbb{Z} : f(k) = [0]\} \\ &= \{k \in \mathbb{Z} : [k] = [0]\} \\ &= \{k \in \mathbb{Z} : k \equiv 0 \mod m\} \\ &= \{k \in \mathbb{Z} : k \text{ je djeljiv s } m\} \\ &= m\mathbb{Z}. \end{aligned}$$

Dakle, po kriteriju f nije monomorfizam.

Budući da za svaki $r \in \mathbb{Z}_m$ postoji cijeli broj koji daje ostatak r pri dijeljenju s m, zaključujemo da je slika homomorfizma f jednaka

$$\mathrm{Im} f = \mathbb{Z}_m.$$

Dakle, f je epimorfizam. Ovakav epimorfizam se naziva kanonski jer šalje svaki cijeli broj u njegovu klasu ekvivalencije.

4.3. Eksponencijalna funkcija. Uobičajena eksponencijalna funkcija $f : \mathbb{R} \to \mathbb{R}$ je definirana formulom

$$f(x) = e^x,$$

gdje je e baza prirodnog logaritma. Međutim, dobro je poznato da ova funkcija nikada ne poprima vrijednost nula. Stoga se eksponencijalna funkcija može promatrati kao funkcija

$$f : \mathbb{R} \to \mathbb{R}^\times,$$

gdje je $\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$. U primjerima grupa vidjeli smo da je $(\mathbb{R}, +)$ aditivna grupa realnih brojeva, a $(\mathbb{R}, \cdot)$ je multiplikativna grupa realnih brojeva. Prema tome, eksponencijalnu funkciju možemo shvatiti kao preslikavanje

$$f : \mathbb{R} \to \mathbb{R}^\times$$

između te dvije grupe definirano formulom

$$f(x) = e^x.$$

Pokažimo da je tako shvaćena eksponencijalna funkcija homomorfizam. Zaista, prema dobro poznatim svojstvima eksponencijalne funkcije vrijedi

$$f(x+y) = e^{x+y} = e^x \cdot e^y = f(x) \cdot f(y)$$

za sve $x, y \in \mathbb{R}$. To je upravo uvjet iz definicije homomorfizma.

Odredimo još jezgru i sliku tog homomorfizma. Prema definiciji, jezgra je jednaka

$$\begin{aligned} \mathrm{Ker} f &= \{x \in \mathbb{R} : f(x) = 1\} \\ &= \{x \in \mathbb{R} : e^x = 1\} \\ &= \{0\}. \end{aligned}$$

Pritom smo koristili činjenicu da je $e^x = 1$ ako i samo ako je $x = 0$. Budući da je e^x uvijek pozitivan broj, te da se svaki pozitivan broj y može dobiti kao

$$e^{\ln y} = y,$$

zaključujemo da je slika jednaka

$$\begin{aligned} \mathrm{Im} f &= \{y \in \mathbb{R}, : \, y = f(x) \text{ za neki } x \in \mathbb{R}\} \\ &= \{y \in \mathbb{R}, : \, y = e^x \text{ za neki } x \in \mathbb{R}\} \\ &= \{y \, : \, y > 0\} \\ &= \mathbb{R}_{>0}, \end{aligned}$$

gdje je $\mathbb{R}_{>0}$ skup pozitivnih realnih brojeva.

Prema kriteriju za monomorfizam zaključujemo da je eksponencijalna funkcija $f : \mathbb{R} \to \mathbb{R}^\times$ monomorfizam, ali nije epimorfizam jer slika nije čitav $\mathbb{R}^\times$. Također, kako je $\mathbb{R}_{>0}$ slika eksponencijalne funkcije, zaključujemo da je $(\mathbb{R}_{>0}, \cdot)$ podgrupa grupe $(\mathbb{R}^\times, \cdot)$.

4.4. Namatanje pravca na kružnicu. Namatanje pravca na jediničnu kružnicu je preslikavanje

$$f : \mathbb{R} \to S^1$$

iz aditivne grupe $(\mathbb{R}, +)$ u grupu $(S^1, \cdot)$ koje realnom broju x pridružuje točku na jediničnoj kružnici koja odgovara kutu od x radijana. Iz definicije sinusa i kosinusa poznato je da su koordinate te točke $(\cos x, \sin x)$. Ako te koordinate zapišemo kao kompleksan broj dobivamo formulu

$$f(x) = \cos x + i \sin x = e^{ix},$$

za sve $x \in \mathbb{R}$. Uočimo da je

$$|e^{ix}| = |\cos x + i \sin x| = \sqrt{\cos^2 x + \sin^2 x} = 1,$$

pa je zaista $f(x) \in S^1$ za svaki $x \in \mathbb{R}$. Tada je f homomorfizam jer po svojstvima eksponencijalne funkcije vrijedi

$$f(x + y) = e^{i(x+y)} = e^{ix+iy} = e^{ix} \cdot e^{iy} = f(x) \cdot f(y)$$

za sve $x, y \in \mathbb{Z}$.

Prema definiciji, jezgra homomorfizma f je jednaka

$$\begin{aligned} \mathrm{Ker} f &= \{x \in \mathbb{R} \, : \, f(x) = 1\} \\ &= \left\{x \in \mathbb{R} \, : \, e^{ix} = 1\right\} \\ &= \{x \in \mathbb{R} \, : \, \cos x = 1 \text{ i } \sin x = 0\} \\ &= \{x \in \mathbb{R} \, : \, x = 2k\pi \text{ za neki } k \in \mathbb{Z}\} \\ &= \{2k\pi \, : \, k \in \mathbb{Z}\} \\ &= 2\pi\mathbb{Z}, \end{aligned}$$

gdje smo s $2\pi\mathbb{Z}$ označili skup svih "višekratnika" od 2π, odnosno brojeva oblika $2\pi k$, gdje je $k \in \mathbb{Z}$. Budući da jezgra nije trivijalna, zaključujemo da f nije monomorfizam. Također, kako je jezgra homomorfizma uvijek podgrupa, dobivamo da je $(2\pi\mathbb{Z}, +)$ podgrupa od $(\mathbb{R}, +)$.

Slika namatanja na kružnicu je čitava kružnica jer se svaki kompleksan broj apsolutne vrijednosti jedan može prikazati u kompleksnom obliku kao $\cos x + i \sin x$. Drugim riječima, za svaki $z \in S^1$ postoji kut $x \in \mathbb{R}$ takav da vrijedi

$$f(x) = e^{ix} = \cos x + i \sin x = z.$$

Stoga je $\mathrm{Im} f = S^1$, pa je f epimorfizam.

4.5. Izomorfizam grupe klasa ostataka $\mathbb{Z}_m$ i grupe korijena iz jedinice μ_m. Neka je $m > 1$ prirodan broj. Ovim primjerom pokazujemo da je aditivna grupa $(\mathbb{Z}_m, +_m)$ klasa ostataka modulo m izomorfna grupi m–tih korijena iz jedinice $(\mu_m, \cdot)$. Neka je funkcija

$$f : \mathbb{Z}_m \to \mu_m$$

definirana formulom

$$f([k]) = e^{\frac{2k\pi i}{m}} = \cos\left(\frac{2\pi k}{m}\right) + i \sin\left(\frac{2k\pi}{m}\right)$$

za sve klase $[k] \in \mathbb{Z}_m$, gdje je $i = \sqrt{-1}$.

Budući da je funkcija f definirana na klasama ostataka $[k] \in \mathbb{Z}_m$, a u formuli se koristi predstavnik klase k, najprije je potrebno utvrditi je li definicija dobra, odnosno ovisi li o izboru predstavnika. Neka su k i k' dva predstavnika iste klase ostataka modulo m. To znači da vrijedi

$$k \equiv k' \mod m,$$

što je ekvivalentno tome da je $k - k'$ djeljivo s m. Dakle, postoji $a \in \mathbb{Z}$ takav da je

$$k - k' = am.$$

Sada je jasno da vrijedi

$$e^{\frac{2k\pi i}{m}} = e^{\frac{2(k'+am)\pi i}{m}} = e^{\frac{2k'\pi i}{m} + 2a\pi i} = e^{\frac{2k'\pi i}{m}} \cdot e^{2a\pi i} = e^{\frac{2k'\pi i}{m}},$$

pri čemu smo koristili činjenicu da je

$$e^{2a\pi i} = \cos(2a\pi) + i \sin(2a\pi) = 1 + i \cdot 0 = 1$$

za sve $a \in \mathbb{Z}$. Time smo dokazali da definicija funkcije f zaista ne ovisi o izboru predstavnika.

Za sve $[k], [l] \in \mathbb{Z}_m$ vrijedi

$$f([k] + [l]) = f([k + l]) = e^{\frac{2(k+l)\pi i}{m}} = e^{\frac{2k\pi i}{m}} \cdot e^{\frac{2l\pi i}{m}} = f([k]) \cdot f([l]).$$

Stoga je f homomorfizam.

Odredimo jezgru homomorfizma f. Po definiciji jezgre dobivamo

$$\begin{aligned}
\mathrm{Ker}f &= \{[k] \in \mathbb{Z}_m \,:\, f([k]) = 1\} \\
&= \left\{[k] \in \mathbb{Z}_m \,:\, e^{\frac{2k\pi i}{m}} = 1\right\} \\
&= \left\{[k] \in \mathbb{Z}_m \,:\, \cos\left(\frac{2k\pi}{m}\right) + i\sin\left(\frac{2k\pi}{m}\right) = 1\right\} \\
&= \left\{[k] \in \mathbb{Z}_m \,:\, \cos\left(\frac{2k\pi}{m}\right) = 1 \text{ te } \sin\left(\frac{2k\pi}{m}\right) = 0\right\} \\
&= \left\{[k] \in \mathbb{Z}_m \,:\, \frac{2k\pi}{m} = 2a\pi \text{ za neki } a \in \mathbb{Z}\right\} \\
&= \{[k] \in \mathbb{Z}_m \,:\, k = am \text{ za neki } a \in \mathbb{Z}\} \\
&= \{[k] \in \mathbb{Z}_m \,:\, k \equiv 0 \mod m\} \\
&= \{[0]\}.
\end{aligned}$$

Dakle, jezgra $\mathrm{Ker}f$ je trivijalna jer se sastoji samo od neutralnog elementa $[0] \in \mathbb{Z}_m$. Prema kriteriju za monomorfizam, zaključujemo da je f monomorfizam.

Slika homomorfizma f je

$$\mu_m.$$

Naime, proizvoljni m–ti korijen iz jedinice

$$e^{\frac{2k\pi i}{m}} \in \mu_m,$$

gdje je $k \in \mathbb{Z}$, se dobiva upravo kao slika klase ostataka $[k] \in \mathbb{Z}_m$ jer vrijedi

$$f([k]) = e^{\frac{2k\pi i}{m}}.$$

Dakle, f je i epimorfizam, pa onda i izomorfizam.

4.6. Trag matrice. Trag kvadratne matrice je zbroj elemenata na njenoj glavnoj (padajućoj) dijagonali. Trag matrice $A \in M_{n,n}(F)$, gdje je F jedan od skupova brojeva $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$, označavamo s $\mathrm{tr}(A)$. Ako je

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ a_{2,1} & a_{2,2} & \dots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \dots & a_{n,n} \end{pmatrix} \in M_{n,n}(F),$$

onda je trag jednak

$$\mathrm{tr}(A) = a_{1,1} + a_{2,2} + \ldots + a_{n,n} = \sum_{k=1}^{n} a_{k,k} \in F.$$

Dokažimo da je trag homomorfizam s aditivne grupe matrica $(M_{n,n}(F), +)$ u aditivnu grupu brojeva $(F, +)$. Zaista, za proizvoljne matrice $A = (a_{i,j}) \in M_{n,n}(F)$ i $B = (b_{i,j}) \in M_{n,n}(F)$,

gdje $i, j = 1, \ldots, n$, vrijedi

$$\begin{aligned}\operatorname{tr}(A+B) &= \operatorname{tr}\big((a_{i,j})+(b_{i,j})\big) = \operatorname{tr}\big((a_{i,j}+b_{i,j})\big)\\ &= \sum_{k=1}^{n}(a_{k,k}+b_{k,k}) = \sum_{k=1}^{n}a_{k,k}+\sum_{k=1}^{n}b_{k,k}\\ &= \operatorname{tr}\big((a_{i,j})\big)+\operatorname{tr}\big((b_{i,j})\big) = \operatorname{tr}(A)+\operatorname{tr}(B).\end{aligned}$$

Jezgra traga je prema definiciji jednaka

$$\begin{aligned}\operatorname{Ker}(\operatorname{tr}) &= \{A \in M_{n,n}(F) \,:\, \operatorname{tr}(A) = 0\}\\ &= \left\{A = (a_{i,j}) \in M_{n,n}(F) \,:\, \sum_{k=1}^{n} a_{k,k} = 0\right\}.\end{aligned}$$

Dakle, jezgra se sastoji od svih matrica kojima je zbroj dijagonalnih elemenata jednak nuli, pa takve matrice čine podgrupu aditivne grupe matrica $M_{n,n}(F)$. Prema kriteriju zaključujemo da trag nije monomorfizam.

Slika traga jednaka je

$$\operatorname{Im}(\operatorname{tr}) = F$$

jer je svaki broj $x \in F$ jednak tragu neke matrice iz $M_{n,n}(F)$. Primjerice, matrica koja na presjeku prvog retka i prvog stupca ima broj x, a na svim ostalim mjestima nule, ima trag jednak upravo x. Dakle, trag je epimorfizam.

4.7. Determinanta matrice. Determinanta se može definirati za sve kvadratne matrice iz $M_{n,n}(F)$, gdje je F jedan od skupova brojeva $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$. Podsjetimo da je matrica iz $M_{n,n}$ regularna ako i samo ako njena determinanta nije jednaka nuli. Regularne matrice tvore grupu obzirom na množenje matrica koju smo označili $GL_n(F)$ i zvali opća linearna grupa. Stoga mi promatramo determinantu kao preslikavanje

$$\det : GL_n(F) \to F^\times$$

iz grupe $(GL_n(F), \cdot)$ u grupu $(F^\times, \cdot)$ invertibilnih elemenata u F obzirom na operaciju množenja. Uočimo da za sve skupove brojeva koje koristimo u ovom primjeru vrijedi $F^\times = F \setminus \{0\}$.

Determinanta, shvaćena kao preslikavanje iz $GL_n(F)$, je homomorfizam jer prema Binet–Cauchyjevom teoremu vrijedi

$$\det(A \cdot B) = \det A \cdot \det B$$

za sve $A, B \in GL_n(F)$. Zapravo, Binet–Cauchyjev teorem vrijedi za sve matrice iz $M_{n,n}(F)$, ali nama je dovoljno $GL_n(F)$.

Prema definiciji, jezgra determinante je jednaka

$$\begin{aligned}\operatorname{Ker}(\det) &= \{A \in GL_n(F) \,:\, \det A = 1\}\\ &= SL_n(F).\end{aligned}$$

Podsjetimo da je specijalna linearna grupa $SL_n(F)$ upravo tako i definirana kao skup matrica determinante jedan. Prema kriteriju slijedi da determinanta nije monomorfizam.

Slika determinante je jednaka

$$\operatorname{Im}(\det) = F^\times.$$

Naime, svaki broj $x \in F^\times$ jednak je determinanti neke regularne matrice. Primjerice, determinanta matrice koja na presjeku prvog retka i prvog stupca ima taj broj $x \neq 0$, na svim ostalim mjestima na dijagonali broj 1, a na svim mjestima izvan dijagonale nule, jednaka je x. Dakle, determinanta je epimorfizam.

4.8. Homomorfizam aditivne grupe realnih brojeva i opće linearne grupe $GL_2(\mathbb{R})$. Neka je $(\mathbb{R}, +)$ aditivna grupa realnih brojeva, a $(GL_2(\mathbb{R}), \cdot)$ opća linearna grupa regularnih matrica reda 2. Definiramo preslikavanje

$$f : \mathbb{R} \to GL_2(\mathbb{R})$$

formulom

$$f(\theta) = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}$$

za sve $\theta \in \mathbb{R}$. Uočimo da je

$$\det \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} = \cos^2\theta + \sin^2\theta = 1$$

pa je $f(\theta)$ zaista regularna matrica.

Dokažimo da je f homomorfizam. Koristeći adicione formule za trigonometrijske funkcije, dobivamo

$$\begin{aligned} f(\theta_1) \cdot f(\theta_2) &= \begin{pmatrix} \cos\theta_1 & \sin\theta_1 \\ -\sin\theta_1 & \cos\theta_1 \end{pmatrix} \cdot \begin{pmatrix} \cos\theta_2 & \sin\theta_2 \\ -\sin\theta_2 & \cos\theta_2 \end{pmatrix} \\ &= \begin{pmatrix} \cos\theta_1\cos\theta_2 - \sin\theta_1\sin\theta_2 & \cos\theta_1\sin\theta_2 + \sin\theta_1\cos\theta_2 \\ -\sin\theta_1\cos\theta_2 - \cos\theta_1\sin\theta_2 & -\sin\theta_1\sin\theta_2 + \cos\theta_1\cos\theta_2 \end{pmatrix} \\ &= \begin{pmatrix} \cos(\theta_1+\theta_2) & \sin(\theta_1+\theta_2) \\ -\sin(\theta_1+\theta_2) & \cos(\theta_1+\theta_2) \end{pmatrix} \\ &= f(\theta_1 + \theta_2) \end{aligned}$$

za sve $\theta_1, \theta_2 \in \mathbb{R}$. Dakle, f je zaista homomorfizam.

Odredimo jezgru homomorfizma f. Prema definiciji, jezgra je jednaka

$$\begin{aligned} \mathrm{Ker} f &= \{\theta \in \mathbb{R} : f(\theta) = I_2\} \\ &= \left\{\theta \in \mathbb{R} : \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right\} \\ &= \{\theta \in \mathbb{R} : \cos\theta = 1, \sin\theta = 0\} \\ &= \{\theta \in \mathbb{R} : \theta = 2k\pi \text{ za neki } k \in \mathbb{Z}\} \\ &= 2\pi\mathbb{Z}. \end{aligned}$$

Dakle, jezgru čine svi "višekratnici" broja 2π u $\mathbb{R}$. Prema kriteriju, f nije monomorfizam.

Pokazuje se da je slika homomorfizma f jednaka

$$\mathrm{Im} f = SO(2)$$

specijalnoj grupi ortogonalnih matrica reda 2. Već smo vidjeli da je matrica

$$f(\vartheta) = \begin{pmatrix} \cos\vartheta & \sin\vartheta \\ -\sin\vartheta & \cos\vartheta \end{pmatrix} \in SL_2(\mathbb{R}),$$

jer ima determinantu jednaku jedan. Također vrijedi

$$\begin{aligned}
{}^t f(\vartheta)\cdot f(\vartheta) &= {}^t\begin{pmatrix} \cos\vartheta & \sin\vartheta \\ -\sin\vartheta & \cos\vartheta \end{pmatrix}\cdot\begin{pmatrix} \cos\vartheta & \sin\vartheta \\ -\sin\vartheta & \cos\vartheta \end{pmatrix} \\
&= \begin{pmatrix} \cos\vartheta & -\sin\vartheta \\ \sin\vartheta & \cos\vartheta \end{pmatrix}\cdot\begin{pmatrix} \cos\vartheta & \sin\vartheta \\ -\sin\vartheta & \cos\vartheta \end{pmatrix} \\
&= \begin{pmatrix} \cos^2\vartheta+\sin^2\vartheta & \cos\vartheta\sin\vartheta-\sin\vartheta\cos\vartheta \\ \sin\vartheta\cos\vartheta-\cos\vartheta\sin\vartheta & \sin^2\vartheta+\cos^2\vartheta \end{pmatrix} \\
&= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\
&= I_2
\end{aligned}$$

Dakle, matrica $f(\vartheta)$ pripada podgrupi $O(2)$, pa stoga i $SO(2) = O(2)\cap SL_2(\mathbb{R})$.

Treba dokazati da je $SO(2)$ čitava slika. Neka je

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SO(2)$$

proizvoljna. Tada vrijedi ${}^tA\cdot A = I_2$, ali budući da je $SO(2)$ grupa, to znači da je $A^{-1} = {}^tA$ inverz matrice A, pa je

$$A\cdot {}^tA = {}^tA\cdot A = I_2.$$

Množenjem matrica dobivamo

$$\begin{aligned}
A\cdot {}^tA &= \begin{pmatrix} a & b \\ c & d \end{pmatrix}\cdot {}^t\begin{pmatrix} a & b \\ c & d \end{pmatrix} \\
&= \begin{pmatrix} a & b \\ c & d \end{pmatrix}\cdot\begin{pmatrix} a & c \\ b & d \end{pmatrix} \\
&= \begin{pmatrix} a^2+b^2 & ac+bd \\ ac+bd & c^2+d^2 \end{pmatrix}.
\end{aligned}$$

Kako je $A\in SO(2)$, ova posljednja matrica je jednaka jediničnoj matrici. Time smo dobili tri uvjeta

$$a^2+b^2=1,\quad c^2+d^2=1,\quad ac+bd=0,$$

a zbog determinante koja je jednaka jedan, dobivamo i četvrti uvjet

$$\det A = ad-bc = 1.$$

Prva dva uvjeta pokazuju da točke (a,b) i (c,d) leže na jediničnoj kružnici sa središtem u ishodištu koordinatnog sustava. Stoga postoje realni brojevi $\vartheta,\varphi\in\mathbb{R}$ takvi da je

$$a=\cos\vartheta,\quad b=\sin\vartheta,\quad c=\cos\varphi,\quad d=\sin\varphi.$$

Preostala dva uvjeta određuju vezu između ϑ i φ. Naime, prema adicionim formulama vrijedi

$$\begin{aligned}
ac+bd &= \cos\vartheta\cos\varphi+\sin\vartheta\sin\varphi \\
&= \cos(\varphi-\vartheta),
\end{aligned}$$

$$\begin{aligned}
ad-bc &= \cos\vartheta\sin\varphi-\sin\vartheta\cos\varphi \\
&= \sin(\varphi-\vartheta),
\end{aligned}$$

pa je razlika $\varphi - \vartheta$ određena uvjetima

$$\cos(\varphi - \vartheta) = 0, \quad \sin(\varphi - \vartheta) = 1.$$

Dakle,

$$\varphi - \vartheta = \frac{\pi}{2} + 2k\pi, \quad k \in \mathbb{Z}.$$

Izrazimo li φ i uvrstimo u izraze za c i d dobivamo

$$c = \cos\varphi = \cos(\vartheta + \frac{\pi}{2} + 2k\pi) = -\sin\vartheta,$$

$$d = \sin\varphi = \sin(\vartheta + \frac{\pi}{2} + 2k\pi) = \cos\vartheta.$$

Dakle, za proizvoljnu matricu $A \in SO(2)$, pokazali smo da postoji $\vartheta \in \mathbb{R}$ takav da je

$$f(\vartheta) = \begin{pmatrix} \cos\vartheta & \sin\vartheta \\ -\sin\vartheta & \cos\vartheta \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} = A.$$

To znači da je proizvoljna matrica $A \in SO(2)$ u slici homomorfizma f, pa je njegova slika zaista jednaka $SO(2)$.

4.9. Homomorfizmi grupa malog reda. U poglavlju o primjerima grupa proučavali smo Cayleyjeve tablice konačnih grupa i to posebno grupa malog reda. Kako još nismo uveli pojam homomorfizma, tamo smo govorili o apstraktnoj strukturi grupe i njenim realizacijama. To sada možemo preformulirati.

Naime, ako se dvije Cayleyjeve tablice konačnih grupa mogu jedna iz druge dobiti preimenovanjem elemenata, to znači da postoji bijekcija između elemenata koja je ujedno i homomorfizam jer šalje jednu Cayleyjevu tablicu u drugu. Dakle, u novoj terminologiji, takve dvije tablice su Cayleyjeve tablice izomorfnih grupa. Ako promatramo apstraktnu strukturu svake dvije izomorfne grupe imaju jednaku strukturu, ali mogu se razlikovati u oznakama i poretku elemenata. To smo ranije zvali realizacijama iste apstraktne strukture grupe.

Vidjeli smo da postoji samo jedna struktura grupe reda dva i reda tri. To znači da su sve grupe reda dva, te sve grupe reda tri, međusobno izomorfne. Za grupu reda četiri vidjeli smo da postoje dvije Cayleyjeve tablice koje se jedna iz druge ne mogu dobiti preimenovanjem elemenata. Jedna je Cayleyjeva tablica grupe ostataka $\mathbb{Z}_4$, a druga direktnog produkta $\mathbb{Z}_2 \times \mathbb{Z}_2$. Dakle, svaka grupa reda četiri je izomorfna jednoj od te dvije grupe.

5. Lijeve i desne klase, Lagrangeov teorem

5.1. Napomena o oznaci operacije. Od ovog mjesta prestajemo koristiti $*$ kao oznaku za binarnu operaciju u grupi. Umjesto toga, radi kratkoće, koristimo oznaku $\cdot$, kao za množenje. Od sada kad kažemo "neka je G grupa" podrazumijevamo da je $\cdot$ operacija na G. Prednost ove oznake je u tome što umjesto $g_1 \cdot g_2$ možemo pisati $g_1 g_2$, i time u potpunosti ispuštati oznaku operacije. Ovaj način pisanja je uobičajen za množenje brojeva, primjerice ako su $a, b \in \mathbb{R}$, njihov produkt se piše ab. Stoga ćemo ponekad za neku općenitu binarnu operaciju čak i reći množenje, a za rezultat binarne operacije produkt. Na primjer, frazu "primjenimo na obje strane jednakosti operaciju $*$ s elementom g s lijeva" ćemo od sada zamijeniti frazom "pomnožimo s lijeva obje strane jednakosti elementom g".

5.2. Definicija. Neka je G grupa (podrazumijevamo da je operacija $\cdot$). Neka je H podgrupa od G. Neka je element $a \in G$ fiksiran. Lijeva klasa grupe G po podgrupi H predstavljena elementom a je skup

$$aH = \{ah \,|\, h \in H\},$$

a desna klasa grupe G po podgrupi H predstavljena elementom a je skup

$$Ha = \{ha \,|\, h \in H\}.$$

Element a zovemo predstavnikom lijeve klase aH, odnosno desne klase Ha. Predstavnik je uvijek element i lijeve i desne klase koju predstavlja jer je $e \in H$. Budući da sve tvrdnje o lijevim klasama vrijede i za desne klase, te se dokazuju na isti način, u ovom ćemo poglavlju sve dokaze detaljno napraviti samo za lijeve klase. Odgovarajuće tvrdnje i dokaze za desne klase ćemo samo komentirati.

5.3. Operacija na podskupovima grupe. Neka je G grupa. Neka su S i T podskupovi od G, koji mogu, ali ne moraju, biti grupe. Slično kao lijeve i desne klase, možemo definirati i operaciju na podskupovima

$$ST = \{st \,|\, s \in S, t \in T\}.$$

Produkt ST je naprosto novi podskup od G. Čak i ako su S i T podgrupe, njihov produkt ST nije uvijek podgrupa od G. Međutim, za podgrupu H od G vrijedi $HH = H$, jer zbog zatvorenosti je $HH \subseteq H$, a obratna inkluzija se dobije jer je neutralni element e u H, pa se svaki element $h \in H$ može zapisati kao $h = eh \in HH$. Kao zadatak čitaocu ostavljamo da odredi koju algebarsku strukturu čini partitivni skup $\mathcal{P}(G)$ grupe G uz operaciju množenja podskupova.

Množenjem skupova čuvaju se njihove inkluzije. Preciznije, za podskupove S, S_1, S_2 i T grupe G, te elemente $a, b \in G$ vrijede sljedeće tvrdnje:

(1) ako je $S_1 \subseteq S_2$, onda je $TS_1 \subseteq TS_2$ i $S_1T \subseteq S_2T$,
(2) ako je $S_1 \subseteq S_2$, onda je $aS_1 \subseteq aS_2$ i $S_1a \subseteq S_2a$,
(3) ako je $a \in S$, onda je $ba \in bS$ i $ab \in Sb$,
(4) ako je $a \in S$, onda je $Ta \in TS$ i $aT \in ST$.

Dovoljno je dokazati tvrdnju (1) jer je ona najopćenitija. Preostale tvrdnje su posebni slučajevi tvrdnje (1) u kojima ulogu nekih od skupova iz tvrdnje (1) preuzima element grupe G kojeg možemo interpretirati kao jednočlani skup. Za dokaz tvrdnje (1) uočimo da je proizvoljni element skupa TS_1 oblika ts, gdje je $t \in T$ i $s \in S_1$. Ali $S_1 \subseteq S_2$, pa je $s \in S_2$, odnosno $ts \in TS_2$. Slučaj množenja s T s desna se dokazuje na potpuno jednak način.

5.4. Svojstva lijevih klasa. Neka je G grupa i H njena podgrupa. Neka su $a, b \in G$. Tada vrijedi

(1) $a^{-1}b \in H$ ako i samo ako $aH = bH$, odnosno a i b su predstavnici jedne te iste lijeve klase.
(2) $a^{-1}b \notin H$ ako i samo ako $aH \cap bH = \emptyset$, odnosno lijeve klase predstavljene elementima a i b su disjunktne.

Dakle, dvije lijeve klase su ili jednake ili disjunktne, obzirom da za proizvoljne $a, b \in G$ element $a^{-1}b$ ili je u H ili nije u H.

Dokaz. Najprije dokazujemo prvo svojstvo. Pretpostavimo da je $a^{-1}b \in H$. Množenjem s lijeva s elementom a te s desna s podgrupom H, prema tvrdnjama (3) i (4) o množenju podskupova dobivamo

$$bH = a(a^{-1}b)H \subseteq aHH = aH.$$

Time smo dokazali jednu inkluziju. Za drugu iskoristimo činjenicu da je H grupa pa je inverz od $a^{-1}b$ također u H, odnosno

$$(a^{-1}b)^{-1} = b^{-1}a \in H. \quad [1]$$

Množeći s lijeva elementom b, te s desna podgrupom H, dobivamo

$$aH = b(b^{-1}a)H \subseteq bHH = bH,$$

a to je upravo druga inkluzija.

Za obrat prvog svojstva, pretpostavimo da je $aH = bH$, odnosno da su a i b predstavnici iste lijeve klase. Posebno to znači da je $b \in aH$ (također i $a \in bH$, ali to nam neće trebati). Množeći s lijeva elementom a^{-1} dobivamo

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

što smo i trebali dokazati.

Za drugo svojstvo, dokažimo najprije da ako vrijedi $a^{-1}b \notin H$, onda je $aH \cap bH = \emptyset$. Pretpostavimo suprotno, odnosno da vrijedi $a^{-1}b \notin H$ i da postoji element $x \in aH \cap bH$. Moramo dobiti kontradikciju. Tada, zato što je $x \in aH$, postoji $h_1 \in H$ takav da $x = ah_1$, te zato što je $x \in bH$, postoji $h_2 \in H$ takav da je $x = bh_2$. Izjednačiv si dvije formule za x dobivamo

$$ah_1 = bh_2.$$

Pomnožimo tu jednakost elementom a^{-1} s lijeva i elementom h_2^{-1} s desna. Dobiva se

$$h_1h_2^{-1} = a^{-1}(ah_1)h_2^{-1} = a^{-1}(bh_2)h_2^{-1} = a^{-1}b.$$

Budući da je H podgrupa, lijeva strana ove jednakosti je iz H, dok desna strana nije iz H po pretpostavci. Time smo došli do kontradikcije.

Za obrat drugog svojstva, pretpostavimo da je $aH \cap bH = \emptyset$. Kad bi tada $a^{-1}b \in H$, onda bi množenjem s lijeva elementom a dobili

$$b = a(a^{-1}b) \in aH.$$

Ali b je predstavnik lijeve klase bH, pa stoga i element te klase. Dakle, dobili smo kontradikciju jer je $b \in aH \cap bH$, koji je prazan skup po pretpostavci. □

[1] U ovoj formuli je mali Mak Grbac dana 22. srpnja 2010. godine, kao beba od samo 14 mjeseci i 8 dana, nadopisao "$(a^{-1}b)^{-1} = b^{-1}a \in, kzzzkjzt2H$.". Mi ne znamo što to znači, ali sigurno je nešto jako važno što mi odrasli ne možemo razumjeti. Mislimo da je ključan za razumjevanje faktor 2 koji se javlja ispred H, a k ispred trostrukog z bi mogao značiti "keksić prije spavanja".

5.5. Lijeve klase kao klase ekvivalencije. Lijeve klase se mogu interpretirati kao klase ekvivalencije za pogodno definiranu relaciju ekvivalencije na grupi G. Neka je $\sim_l$ relacija na grupi G, definirana za $a, b \in G$ sa

$$a \sim_l b \text{ ako je } a^{-1}b \in H.$$

To je relacija ekvivalencije. Zaista,

(1) $a \sim_l a$ za sve $a \in G$ jer $a^{-1}a = e \in H$,
(2) ako je $a \sim_l b$, onda $a^{-1}b \in H$, pa je i inverz $(a^{-1}b)^{-1} = b^{-1}a \in H$, te stoga $b \sim_l a$,
(3) ako je $a \sim_l b$ i $b \sim_l c$, onda je $a^{-1}b \in H$ i $b^{-1}c \in H$, pa je i njihov produkt $(a^{-1}b)(b^{-1}c) = a^{-1}c \in H$, te stoga $a \sim_l c$.

Odredimo klase ekvivalencije za relaciju $\sim_l$. Klasa $[a]$ predstavljena elementom $a \in G$ je po definiciji klase ekvivalencije jednaka

$$\begin{aligned} [a] &= \{g \in G \,|\, a \sim_l g\} \\ &= \left\{g \in G \,|\, a^{-1}g \in H\right\} \\ &= \{g \in G \,|\, g \in aH\} \\ &= aH, \end{aligned}$$

pri čemu smo u drugom koraku uvjet pomnožili s lijeva elementom a. Dakle, klase ekvivalencije relacije $\sim_l$ su upravo lijeve klase. Stoga ćemo relaciju $\sim_l$ zvati lijeva relacija. Od tuda dolazi indeks l u oznaci relacije.

Činjenica da su lijeve klase zapravo klase ekvivalencije relacije $\sim_l$ daje jednostavniji dokaz prethodnih svojstava lijevih klasa. Naime, prvo svojstvo kaže da je $a \sim_l b$ ako i samo ako su klase aH i bH jednake, a drugo da je $a \not\sim_l b$ ako i samo ako su klase aH i bH disjunktne. Ali to su upravo osnovna svojstva klasa ekvivalencije. One su jednake ako i samo ako su im predstavnici u relaciji, a disjunktne ako i samo ako nisu u relaciji.

5.6. Teorem. Neka je G grupa i H njena podgrupa. Tada vrijedi

$$|aH| = |H| = |Ha|$$

za sve $a \in G$, gdje $|\ |$ označava kardinalni broj skupa (broj elemenata za konačne skupove). Dakle, sve lijeve i sve desne klase imaju jednak kardinalni broj (broj elemenata), i on je jednak kardinalnom broju (broju elemenata) same podgrupe H.

Dokaz. Jednakost kardinalnih brojeva dvaju skupova po definiciji znači postojanje bijekcije između njih. Dakle, treba odrediti bijekcije

$$\varphi_l : H \to aH \text{ i } \varphi_d : H \to Ha,$$

a onda pomoću njih dobivamo i bijekciju $\varphi_d \circ \varphi_l^{-1} : aH \to Ha$ (to je zapravo tranzitivnost jednakosti kardinalnih brojeva).

Funkciju $\varphi_l : H \to aH$ definiramo formulom

$$\varphi_l(h) = ah$$

za sve $h \in H$. Tada je φ_l injekcija zato što jednakost slika $\varphi_l(h_1) = \varphi_l(h_2)$, za neke $h_1, h_2 \in H$, povlači da je $ah_1 = ah_2$, pa množenjem elementom a^{-1} s lijeva dobivamo $h_1 = h_2$. Također, φ_l je surjekcija, jer je proizvoljni element lijeve klase aH oblika ah za neki $h \in H$, pa se dobije kao slika $\varphi_l(h)$ tog elementa h.

Analogan dokaz bijektivnosti za funkciju $\varphi_d : H \to Ha$, definiranu formulom

$$\varphi_d(h) = ha$$

za sve $h \in H$, prepuštamo čitaocu. □

5.7. Napomena o desnim klasama. Nije teško odrediti analogna svojstva desnih klasa, te interpretaciju tih klasa kao klasa ekvivalencije za relaciju na G koju ćemo zvati desna relacija i označavati $\sim_d$. U svojstvima lijevih klasa valja promijeniti uvjete $a^{-1}b \in H$ i $a^{-1}b \notin H$ uvjetima $ab^{-1} \in H$ i $ab^{-1} \notin H$, te naravno lijeve zamijeniti desnim klasama. Iz toga je odmah jasno da se desna relacija definira kao

$$a \sim_d b \text{ ako } ab^{-1} \in H$$

za $a, b \in G$.

5.8. Lema. Neka je G grupa i H njena podgrupa. Neka su $\sim_l$ i $\sim_d$ lijeva i desna relacija na G ranije definirane pomoću podgrupe H. Tada vrijedi

$$a \sim_l b \text{ ako i samo ako } a^{-1} \sim_d b^{-1},$$

za sve $a, b \in G$.

Dokaz. Po definiciji lijeve relacije $a \sim_l b$ ako i samo ako $a^{-1}b \in G$. Taj uvjet možemo zapisati kao $a^{-1}(b^{-1})^{-1} \in H$ i shvatiti ga, po definiciji desne relacije, kao $a^{-1} \sim_d b^{-1}$. □

5.9. Teorem. Neka je G grupa i H njena podgrupa. Označimo s G/H skup svih lijevih klasa, a s $H\backslash G$ skup svih desnih klasa grupe G po podgrupi H. Tada vrijedi

$$|G/H| = |H\backslash G|.$$

Dakle, kardinalni broj skupa lijevih klasa jednak je kardinalnom broju skupa desnih klasa, odnosno lijevih i desnih klasa ima jednako mnogo. Indeks podgrupe H u grupi G, u oznaci $[G : H]$, definiramo kao taj kardinalni broj ako je konačan, odnosno kao beskonačno ako je taj kardinalni broj beskonačan.

Dokaz. Da bi dokazali jednakost kardinalnih brojeva treba odrediti bijekciju između G/H i $H\backslash G$. Funkciju $\varphi : G/H \to H\backslash G$ definiramo formulom

$$\varphi(aH) = Ha^{-1}$$

za sve $aH \in G/H$. **PAZI** Pritom valja biti oprezan. Iako smo naizgled napisali eksplicitnu formulu za funkciju φ, nije odmah jasno da je φ time dobro definirana. Problem je u tome što se u našoj formuli za vrijednost funkcije φ na nekoj lijevoj klasi aH javlja predstavnik te klase a koji zapravo nije jedinstven. Ako je b neki drugi predstavnik iste lijeve klase, odnosno $aH = bH$, onda bi prema našoj formuli vrijednost funkcije φ na toj lijevoj klasi bila jednaka desnoj klasi Ha^{-1} ako se računa pomoću predstavnika a, odnosno desnoj klasi Hb^{-1} ako se računa pomoću predstavnika b. Stoga, uvijek kada pokušamo definirati funkciju na klasama ekvivalencije koristeći u formuli predstavnika klase prije svega treba provjeriti da je takva funkcija dobro definirana, odnosno da formula koju smo napisali ne ovisi o tome kojeg predstavnika klase izaberemo.

U našem slučaju, neka su $a, b \in G$ dva predstavnika iste lijeve klase, odnosno $aH = bH$. Interpretirajući lijeve klase kao klase ekvivalencije lijeve relacije, to znači da je $a \sim_l b$. Prema

lemi je onda i $a^{-1} \sim_d b^{-1}$, pa stoga $Ha^{-1} = Hb^{-1}$. Dakle, a^{-1} i b^{-1} su predstavnici iste desne klase, pa je φ dobro definirana.

Za injektivnost, pretpostavimo da je $\varphi(aH) = \varphi(bH)$ za neke $a, b \in G$. To znači da je $Ha^{-1} = Hb^{-1}$, odnosno $a^{-1} \sim_d b^{-1}$. Opet prema lemi, onda je $a \sim_l b$, odnosno $aH = bH$. Time smo dokazali injektivnost funkcije φ.

Surjektivnost funkcije φ također vrijedi, zato što je proizvoljna desna klasa oblika Ha za neki $a \in G$, pa se dobije kao

$$\varphi(a^{-1}H) = H(a^{-1})^{-1} = Ha.$$

Dakle, φ je zaista bijekcija. □

5.10. Teorem. Neka je G grupa i H njena podgrupa. Tada vrijedi

$$|G| = [G : H] \cdot |H|,$$

gdje su $|G|$ i $|H|$ redovi grupa G i H, respektivno, a $[G : H]$ indeks podgrupe H u grupi G. Pritom produkt na desnoj strani smatramo beskonačnim ako je barem jedan od faktora beskonačan.

Dokaz. Neka je najprije G konačna grupa. Tada je i H konačna. Budući da su lijeve klase zapravo klase ekvivalencije lijeve relacije, one čine particiju grupe G. Dakle, unija svih lijevih klasa po podgrupi H je čitava grupa G i svake dvije različite klase su disjunktne. Broj lijevih klasa je stoga konačan i po definiciji jednak indeksu $[G : H]$. Ranije smo već dokazali da svaka lijeva klasa ima točno $|H|$ elemenata. Dakle, budući da je unija $[G : H]$ u parovima disjunktnih skupova, od kojih svaki ima $|H|$ elemenata, jednaka čitavoj grupi G, zaključujemo da zaista vrijedi $|G| = [G : H] \cdot |H|$.

Neka je sada G beskonačna grupa. Treba dokazati da je red podgrupe H ili indeks $[G : H]$ beskonačan. Zaista, kad bi i red grupe G i indeks $[G : H]$ bili konačni, onda isti argument kao u prvom dijelu dokaza pokazuje da bi onda i red grupe G bio konačan. □

5.11. Korolar (Lagrangeov teorem).[2] Neka je G konačna grupa. Tada, za svaku podgrupu H od G vrijedi

$$|H| \,\big|\, |G|,$$

odnosno red svake podgrupe dijeli red čitave grupe. Posebno, red svakog elementa dijeli red čitave grupe.

Dokaz. Iz prethodnog teorema je očito da red $|H|$ dijeli red $|G|$. Red elementa $g \in G$ jednak je redu podgrupe $\langle g \rangle$ generirane tim elementom, a prema prethodnom taj red dijeli red čitave grupe. □

6. Normalne podgrupe i kvocijentne grupe

6.1. Motivacija. Jedan od ciljeva teorije grupa je odrediti strukturu grupa. To se može raditi na način da se pronalaze podgrupe, koje su manje od čitave grupe pa se u principu može njihova struktura jednostavnije odrediti. Međutim, da bi se iz toga moglo doći do informacija o strukturi čitave grupe, potrebno je na neki način poznavati i strukturu dijela grupe koji nije u podgrupi. Drugim riječima, potrebno je poznavati skupove lijevih i desnih klasa grupe G po podgrupi H. Stoga bi bilo korisno na neki način prenijeti binarnu operaciju

[2] Lagrange je bio...

iz grupe na te skupove lijevih i desnih klasa. Međutim, to se ne može napraviti za klase po bilo kakvoj podgrupi. Podgrupe za koje je to moguće se zovu normalne podgrupe, a grupa lijevih i desnih klasa, koje su u slučaju normalne podgrupe jednake, zove se kvocijentna grupa.

6.2. Uvjet dvije zvjezdice za lijeve klase. Podsjetimo se uvjeta dvije zvjezdice $(**)$, kojeg smo prvi put susreli kod primjera aditivnih i multiplikativnih grupa klasa ostataka cijelih brojeva pri dijeljenju. U tom slučaju promatrali smo skup klasa ekvivalencije za relaciju $\equiv \pmod m$ kongruencije modulo neki prirodni broj m. Da bi mogli prenijeti operaciju zbrajanja i množenja cijelih brojeva na te skup tih klasa trebalo je provjeriti uvjet $(**)$ koji osigurava da operacija čuva relaciju. Općenito, ako je G grupa i $\sim$ relacija ekvivalencije na G, uvjet $(**)$ glasi

$(**)$ ako za $a, b, a', b' \in G$ vrijedi $a \sim a'$ i $b \sim b'$, onda vrijedi i $ab \sim a'b'$.

U slučaju lijevih klasa grupe G po podgrupi H relacija ekvivalencije je lijeva relacija $\sim_l$. Stoga, da bi prenijeli operaciju s grupe G na lijeve klase, mora vrijediti uvjet dvije zvjezdice za relaciju $\sim_l$, odnosno

$(**)$ ako za $a, b, a', b' \in G$ vrijedi $aa'^{-1} \in H$ i $bb'^{-1} \in H$, onda vrijedi i $ab(a'b')^{-1} \in H$.

Raspišimo taj uvjet eksplicitnije.

Izraz $ab(a'b')^{-1} \in H$ se može zapisati u obliku

$$ab(a'b')^{-1} = abb'^{-1}a'^{-1} = a(bb'^{-1})a^{-1}(aa'^{-1}) \in H.$$

Po pretpostavci je $aa'^{-1} \in H$, pa je gornji izraz element podgrupe H ako i samo ako je

$$a(bb'^{-1})a^{-1} \in H,$$

pri čemu je, također po pretpostavci, $bb'^{-1} \in H$. Proizvoljni element $h \in H$ možemo napisati u obliku bb'^{-1}, gdje su b i b' pogodno izabrani elementi grupe G (na primjer $b = h$ i $b' = e$).

Time smo dokazali da je uvjet $(**)$ za lijevu relaciju $\sim_l$ ekvivalentan uvjetu

$(**_l)$ $ghg^{-1} \in H$ za svaki $h \in H$ i za svaki $g \in G$, odnosno konjugat svakog elementa podgrupe H proizvoljnim elementom grupe G je opet element podgrupe H.

Pritom smo oznaku a za proizvoljni element grupe G zamijenili oznakom g.

Koristeći zapis operacije na skupovima uvjet $(**_l)$ se može zapisati u obliku

$(**_l)$ $gHg^{-1} \subseteq H$ za svaki $g \in G$,

što ćemo koristiti u definiciji normalne podgrupe.

6.3. Normalna podgrupa. Neka je G grupa i N njena podgrupa. Tada su sljedeći uvjeti ekvivalentni:

(1) $gNg^{-1} \subseteq N$ za svaki $g \in G$,
(2) $gNg^{-1} = N$ za svaki $g \in G$,
(3) $gN = Ng$ za svaki $g \in G$.

Ako podgupa N zadovoljava te ekvivalentne uvjete, naziva se normalna podgrupa, u oznaci $N \trianglelefteq G$. Uočimo da je uvjet (1) zapravo uvjet $(**_l)$.

Dokaz. Dokažimo najprije da uvjet (1) implicira uvjet (2). Budući da uvjet (1) vrijedi za svaki $g \in G$, možemo umjesto proizvoljnog elementa g uvrstiti njegov inverz g^{-1}. Stoga vrijedi

$$g^{-1}Ng \subseteq N$$

za svaki $g \in G$. Pomnožimo li tu inkluziju s lijeva elementom g, a s desna elementom g^{-1} dobivamo

$$N = g(g^{-1}Ng)g^{-1} \subseteq gNg^{-1}$$

za svaki $g \in G$. Prema uvjetu (1), desna strana ove inkluzije je podskup od N, odnosno

$$gNg^{-1} \subseteq N$$

za svaki $g \in G$. Posljednje dvije inkluzije pokazuju da vrijedi

$$gNg^{-1} = N$$

za svaki $g \in G$. Obrat, odnosno da uvjet (2) implicira uvjet (1), je očigledan jer jednakost skupova uvijek implicira jednu inkluziju. Time smo dokazali da su uvjeti (1) i (2) ekvivalentni.

Ekvivalencija uvjeta (2) i (3) slijedi množenjem s desna elementom g, odnosno g^{-1}. Zaista, množenjem jednakosti iz uvjeta (2) elementom g s desna dobivamo

$$gN = (gNg^{-1})g = Ng$$

za svaki $g \in G$, što je upravo uvjet (3). Obratno, množenjem jednakosti iz uvjeta (3) elementom g^{-1} s desna, dobivamo

$$gNg^{-1} = (Ng)g^{-1} = N$$

za svaki $g \in G$, što je upravo uvjet (2). □

6.4. Napomene. U definiciji normalne podgrupe koristimo oznaku N kao oznaku podgrupe grupe G. To je uobičajena oznaka za podgrupe koje su normalne.

Među ekvivalentnim uvjetima iz definicije normalne podgrupe, uvjet (3) nam kaže da su lijeva i desna klasa grupe G po normalnoj podgrupi N predstavljene proizvoljnim elementom $g \in G$ međusobno jednake. To svojstvo ne vrijedi za proizvoljne podgrupe. Budući da su lijeve i desne klase po podgrupi zapravo klase ekvivalencije za lijevu i desnu relaciju na grupi G, jednakost klasa pokazuje jednakost tih relacija u slučaju normalne podgrupe, odnosno $\sim_l = \sim_d$.

Uvjet (2) ćemo malo detaljnije komentirati jer je to dobar primjer za objasniti važnost razlikovanja jednakosti i izomorfnosti dviju podgrupa. Dvije podgrupe su jednake ako su jednake kao skupovi, odnosno ako se baš sastoje od istih elemenata velike grupe. S druge strane, dvije podgrupe su izomorfne ako postoji izomorfizam između njih, što ne znači da moraju nužno biti jednake kao skupovi, odnosno sastojati se od istih elemenata. Dakle, jednakost je jači uvjet od izomorfnosti.

Uvjet (2) baš traži da su gNg^{-1} i N jednake, a ne samo izomorfne. Drugim riječima, proizvoljni konjugat podgrupe N mora biti baš jednak podgrupi N. Uvjet izomorfnosti podgrupe i njenog proizvoljnog konjugata je ispunjen za bilo koju podgrupu H grupe G, pa ne donosi ništa novo. Zaista, ako je H podgrupa od G i $g \in G$ proizvoljan, onda možemo definirati funkciju $f : H \to gHg^{-1}$ formulom

$$f(h) = ghg^{-1}$$

za svaki $h \in H$. Uočimo da je f zapravo restrikcija unutarnjeg automorfizma I_g sa grupe G na njenu podgrupu H, pa je stoga f monomorfizam. Pri tome smo i za kodomenu umjesto G uzeli gHg^{-1} što je upravo slika te restrikcije, pa je f i epimorfizam. Dakle, f je izomorfizam.

6.5. Teorem. Neka su G i H grupe, te $f : G \to H$ homomorfizam grupa. Tada je jezgra $\mathrm{Ker}f$ normalna podgrupa grupe G.

Dokaz. Provjerimo da uvjet (1) iz definicije normalne podgrupe vrijedi za jezgru $\mathrm{Ker}f$. Točnije, treba provjeriti da vrijedi

$$g(\mathrm{Ker}f)g^{-1} \subseteq \mathrm{Ker}f$$

za sve $g \in G$. Neka je $x \in \mathrm{Ker}f$ proizvoljan element jezgre. Tada je $f(x) = e_H$, pa prema svojstvima homomorfizma vrijedi

$$f(gxg^{-1}) = f(g)f(x)f(g)^{-1} = f(g)e_H f(g)^{-1} = f(g)f(g)^{-1} = e_H$$

za svaki $g \in G$. Stoga je i $gxg^{-1} \in \mathrm{Ker}f$ za svaki $g \in G$. Kako je $x \in \mathrm{Ker}f$ bio proizvoljan, dokazali smo da zaista vrijedi

$$g(\mathrm{Ker}f)g^{-1} \subseteq \mathrm{Ker}f,$$

za sve $g \in G$. □

6.6. Primjer (trivijalna podgrupa). Neka je G grupa s neutralnim elementom e. Njena trivijalna podgrupa $\{e\}$ je normalna jer za svaki $g \in G$ vrijedi

$$g\{e\}g^{-1} = \{geg^{-1}\} = \{e\},$$

pa je ispunjeno svojstvo (2) iz definicije normalne podgrupe. Dakle, trivijalna podgrupa je normalna podgrupa svake grupe.

6.7. Primjer (Abelova grupa). Svaka podgrupa N Abelove grupe G je normalna. Zaista, u Abelovoj grupi vrijedi

$$gNg^{-1} = gg^{-1}N = e_G N = N$$

za svaki $g \in G$, jer N i g^{-1} mogu zamijeniti mjesta. To pokazuje da vrijedi uvjet (2) iz definicije normalne podgrupe.

6.8. Primjer (podgrupa indeksa 2). Neka je N podgrupa grupe G indeksa $[G : N] = 2$. Tada je N normalna podgrupa. Naime, grupa G ima dvije lijeve klase obzirom na podgrupu N. Jedna od njih je sama podgrupa N, a druga sadrži sve elemente koji nisu iz N. Dakle,

$$gN = \begin{cases} N, & \text{ako } g \in N, \\ G \setminus N, & \text{ako } g \notin N. \end{cases}$$

Isto vrijedi i za desne klase, odnosno

$$Ng = \begin{cases} N, & \text{ako } g \in N, \\ G \setminus N, & \text{ako } g \notin N. \end{cases}$$

Dakle, lijeve i desne klase se podudaraju $gN = Ng$ za sve $g \in G$. Prema uvjetu (3) iz definicije normalne podgrupe vidimo da je N zaista normalna podgrupa.

$\circ$	id	ρ_1	ρ_2	ρ_3	σ_1	σ_2	σ_3	σ_4
id	id	ρ_1	ρ_2	ρ_3	σ_1	σ_2	σ_3	σ_4
ρ_1	ρ_1	ρ_2	ρ_3	id	σ_2	σ_3	σ_4	σ_1
ρ_2	ρ_2	ρ_3	id	ρ_1	σ_3	σ_4	σ_1	σ_2
ρ_3	ρ_3	id	ρ_1	ρ_2	σ_4	σ_1	σ_2	σ_3
σ_1	σ_1	σ_4	σ_3	σ_2	id	ρ_3	ρ_2	ρ_1
σ_2	σ_2	σ_1	σ_4	σ_3	ρ_1	id	ρ_3	ρ_2
σ_3	σ_3	σ_2	σ_1	σ_4	ρ_2	ρ_1	id	ρ_3
σ_4	σ_4	σ_3	σ_2	σ_1	ρ_3	ρ_2	ρ_1	id

TABLICA 2. Cayleyjeva tablica grupe izometrija kvadrata

6.9. Primjer. Neka je G grupa i N njena normalna podgrupa. Ako je H podgrupa od G koja sadrži N, onda je N normalna podgrupa i u H. To je jasno iz definicije, jer ako uvjeti iz definicije normalne podgrupe vrijede za svaki $g \in G$, onda će sigurno vrijediti i za svaki $g \in H$.

Međutim, obrat ne vrijedi. Neka je G grupa, K i H njene podgrupe takve da je $K \leqslant H \leqslant G$. Ako je sada K normalna podgrupa od H, ona ne mora biti normalna podgrupa od G. Čak i ako je K normalna u H i H normalna u G, ipak K ne mora biti normalna u G. To zapravo znači da relacija "biti normalna podgrupa" nije tranzitivna.

Kao primjer takve situacije, neka je G grupa izometrija kvadrata. Numerirajmo vrhove kvadrata brojevima 1, 2, 3, 4 u pozitivnom smjeru (suprotno od kazaljke na satu). Osim identitete id, izometrije kvadrata su tri rotacije ρ_1, ρ_2 i ρ_3 oko središta kvadrata u pozitivnom smjeru za 90°, 180° i 270°, respektivno, te četiri osne simetrije σ_1, σ_2, σ_3, σ_4 obzirom na pravce kroz vrhove 1 i 3, kroz polovišta stranica $\overline{12}$ i $\overline{34}$, kroz vrhove 2 i 4, kroz polovišta stranica $\overline{23}$ i $\overline{41}$, respektivno. Dakle,

$$G = \{id, \rho_1, \rho_2, \rho_3, \sigma_1, \sigma_2, \sigma_3, \sigma_4\}$$

je grupa reda osam. Kao u primjeru grupe izometrija peterokuta, određujemo Cayleyjevu tablicu grupe G navedenu u tablici 2. Detalje računa prepuštamo čitaocu.

Promotrimo podskup

$$H = \{id, \rho_2, \sigma_1, \sigma_3\}$$

grupe G. Iz Cayleyjeve tablice možemo isčitati da je H podgrupa od G. Naime, ako izdvojimo iz Cayleyjeve tablice za grupu G retke i stupce koji odgovaraju elementima iz H, dobivamo tablicu 3. Vidimo da se u tablici 3 javljaju samo elementi iz H, pa je to zaista Cayleyjeva tablica podgrupe H. To je podgrupa reda četiri, pa uspoređivanjem s tablicama koje smo ranije dobili, vidimo da je H izomorfna grupi $\mathbb{Z}_2 \times \mathbb{Z}_2$. To se najlakše vidi po tome što je red sva tri elementa koji nisu neutralni jednak 2. Također, budući da je prema Lagrangeovom teoremu

$$[G : H] = \frac{G}{H} = \frac{8}{4} = 2,$$

zaključujemo iz prethodnog primjera da je H normalna podgrupa od G.

Cayleyjeva tablica podgrupe H je simetrična obzirom na glavnu (padajuću) dijagonalu. To pokazuje da je H komutativna, pa su sve njene podgrupe normalne u H. Neka je

$$K = \{id, \sigma_1\}.$$

$\circ$	id	ρ_2	σ_1	σ_3
id	id	ρ_2	σ_1	σ_3
ρ_2	ρ_2	id	σ_3	σ_1
σ_1	σ_1	σ_3	id	ρ_2
σ_3	σ_3	σ_1	ρ_2	id

TABLICA 3. Cayleyjeva tablica podgrupe H grupe izometrija kvadrata

Budući da je σ_1 reda 2, to je podgrupa od H, pa stoga i normalna u H.

Time smo konstruirali grupu G i njene podgrupe K i H takve da vrijedi

$$K \leqslant H \leqslant G$$

i pritom je K normalna podgrupa u H, te H normalna u G. Međutim, K nije normalna podgrupa u čitavoj grupi G jer, iz Cayleyjeve tablice za grupu G vidimo, primjerice, da je lijeva klasa

$$\sigma_2 K = \{\sigma_2, \rho_1\},$$

dok je desna klasa

$$K\sigma_2 = \{\sigma_2, \rho_3\},$$

pa ne vrijedi svojstvo (3) iz definicije normalne podgrupe. Dakle, ovaj primjer pokazuje da relacija biti normalna podgrupa nije tranzitivna.

6.10. Primjeri dobiveni kao jezgra homomorfizma. Dokazali smo da je jezgra homomorfizma normalna podgrupa. Stoga iz primjera homomorfizama dobivamo primjere normalnih podgrupa. Tako je primjerice specijalna linearna grupa $SL_n(F)$ normalna podgrupa u općoj linearnoj grupi $GL_n(F)$ kao jezgra determinante definirane na $GL_n(F)$.

U svakoj grupi G centar grupe $Z(G)$ je normalna podgrupa. Naime, vidjeli smo da je centar $Z(G)$ jezgra homomorfizma

$$\Phi : G \to \operatorname{Aut} G$$

definiranog za $g \in G$ s $\Phi(g) = I_g$, gdje je I_g unutarnji automorfizam određen konjugiranjem elementom g.

6.11. Kvocijentna grupa. Neka je G grupa i N njena normalna podgrupe. Kao što smo već uočili, uvjet (1) iz definicije normalne podgrupe je ekvivalentan uvjetu $(**)$ za lijevu relaciju. Stoga se operacija iz grupe G može prenijeti na skup lijevih klasa G/N koristeći predstavnike klasa. Točnije, operacija na lijevim klasama je definirana kao

$$(g_1N)(g_2N) = g_1g_2N,$$

za sve $g_1N, g_2N \in G/N$. Pritom uvjet $(**)$ osigurava da je ta definicija dobra, odnosno neovisna o odabiru predstavnika lijevih klasa. Zaista, ako je $g_1 \sim_l g_1'$ i $g_2 \sim_l g_2'$, odnosno $g_1N = g_1'N$ i $g_2N = g_2'N$, onda svojstvo $(**)$ za $\sim_l$ daje $g_1g_2 \sim_l g_1'g_2'$, pa stoga i $g_1g_2N = g_1'g_2'N$. Dakle,

$$(g_1N)(g_2N) = g_1g_2N = g_1'g_2'N = (g_1'N)(g_2'N).$$

Time smo dokazali da definicija ne ovisi o izboru predstavnika lijevih klasa. Budući da je G grupa, ovako prenesena operacija s G na G/N zadržava svojstva iz definicije grupe zahvaljujući uvjetu $(**)$. Zaista, zatvorenost operacije na G/N je očigledna, asocijativnost

slijedi iz asocijativnosti u grupi G, neutralni element je lijeva klasa koju predstavlja neutralni element iz grupe G, a to je klasa

$$e_{G/N} = e_G N = N,$$

inverz klase $gN \in G/N$ je klasa

$$(gN)^{-1} = g^{-1}N.$$

Stoga je G/N grupa. Ta grupa se naziva kvocijentna grupa grupe G po normalnoj podgrupi N.

Na isti način mogli smo definirati operaciju na skupu $N\backslash G$ desnih klasa grupe G po normalnoj podgrupi N i time dobiti strukturu grupe. Međutim, kako se za normalne podgrupe, prema uvjetu (3) iz definicije, lijeve i desne klase podudaraju, grupe G/N i $N\backslash G$ su zapravo jedna te ista grupa. Mi smo odlučili pisati kvocijentnu grupu kao grupu lijevih klasa.

6.12. Primjer (grupe klasa ostataka kao kvocijentna grupa). Promotrimo aditivnu grupu cijelih brojeva $(\mathbb{Z}, +)$. Neka je $m > 1$ prirodni broj. Podgrupa $m\mathbb{Z}$ grupe $\mathbb{Z}$ je normalna jer je $\mathbb{Z}$ Abelova grupa. Stoga možemo definirati kvocijentnu grupu $\mathbb{Z}/m\mathbb{Z}$. Lijeve klase su oblika $k + m\mathbb{Z}$, gdje je $k \in \mathbb{Z}$, a operacija zbrajanja na kvocijentnoj grupi je definirana s

$$(k + m\mathbb{Z}) + (l + m\mathbb{Z}) = (k + l) + m\mathbb{Z}$$

za sve $k, l \in \mathbb{Z}$.

Uočimo da su klase ekvivalencije ostataka pri dijeljenju s m upravo jednake lijevim klasama ove kvocijentne grupe. Naime, za svaki $k \in \mathbb{Z}$, klasa $[k] \in \mathbb{Z}_m$ je jednaka

$$\begin{aligned}
[k] &= \{l \in \mathbb{Z} : l \equiv k \mod m\} \\
&= \{l \in \mathbb{Z} : l - k \text{ je djeljivo s } m\} \\
&= \{l \in \mathbb{Z} : l - k \in m\mathbb{Z}\} \\
&= \{l \in \mathbb{Z} : l \in k + m\mathbb{Z}\} \\
&= k + m\mathbb{Z}.
\end{aligned}$$

Stoga možemo definirati preslikavanje

$$f : \mathbb{Z}_m \to \mathbb{Z}/m\mathbb{Z}$$

formulom

$$f([k]) = k + m\mathbb{Z}$$

za sve $[k] \in \mathbb{Z}_m$. To preslikavanje je očito bijekcija jer smo vidjeli da se klase ostataka podudaraju s lijevim klasama. Također, f je homomorfizam jer vrijedi

$$f([k] + [l]) = f([k + l]) = (k + l) + m\mathbb{Z} = (k + m\mathbb{Z}) + (l + m\mathbb{Z}) = f([k]) + f([l])$$

za sve $[k], [l] \in \mathbb{Z}_m$. Time smo dokazali da je grupa ostataka $(\mathbb{Z}_m, +_m)$ izomorfna kvocijentnoj grupi $(\mathbb{Z}/m\mathbb{Z}, +)$.

Još primjera kvocijentnih grupa ostavljamo za kasnije u poglavlju o teoremima o izomorfizmu jer će nam oni omogućiti da jednostavnije odredimo grupe kojima su te kvocijentne grupe izomorfne.

6.13. Primjer (kvocijentna grupa po trivijalnoj podgrupi). Među primjerima normalnih podgrupa naveli smo da je trivijalna podgrupa normalna u svakoj grupi G. To znači da možemo formirati kvocijentnu grupu.

Međutim, sve lijeve klase obzirom na trivijalnu podgrupu $\{e\}$ su jednočlane jer za svaki $g \in G$ vrijedi

$$g\{e\} = \{g\}.$$

Stoga se množenje u kvocijentnoj grupi podudara s množenjem u G jer možemo jednočlane lijeve klase poistovjetiti s elementima iz G. Preciznije, možemo definirati funkciju

$$f : G \to G/\{e\}$$

naprosto formulom

$$f(g) = g\{e\} = \{g\}.$$

Funkcija f je očito izomorfizam. Time smo dokazali da je kvocijentna grupa po trivijalnoj podgrupi izomorfna s polaznom grupom.

6.14. Teorem (podgrupe kvocijentne grupe). Neka je G grupa i N njena normalna podrupa. Tada postoji bijekcija između skupa svih podgrupa grupe G koje sadrže N i skupa svih podgrupa grupe G/N. Pritom ta bijekcija podgrupi H grupe G koja sadrži podgrupu N pridružuje kvocijentnu grupu H/N.

Dokaz. Traženu bijekciju dobivamo iz kanonskog epimorfizma za kvocijentnu grupu. To je homomorfizam $\pi : G \to G/N$ definiran kao

$$\pi(g) = gN$$

za sve $g \in G$. To je zaista homomorfizam jer vrijedi

$$\pi(g_1 g_2) = g_1 g_2 N = (g_1 N)(g_2 N) = \pi(g_1)\pi(g_2)$$

za sve $g_1, g_2 \in G$. Homomorfizam π je surjektivan jer za proizvoljnu klasu gN za predstavnika g vrijedi

$$\pi(g) = gN.$$

Uočimo da je jezgra

$$\begin{aligned} \mathrm{Ker}\pi &= \{g \in G \,:\, \pi(g) = e_{G/N}\} \\ &= \{g \in G \,:\, gN = N\} \\ &= \{g \in G \,:\, g \in N\} \\ &= N. \end{aligned}$$

Neka je S skup svih podgrupa grupe G koji sadrže N, a T skup svih podgrupa od G/N. Koristeći π definiramo funkciju $\varphi : S \to T$ kao

$$\varphi(H) = \pi(H)$$

za sve $H \in S$. Budući da je slika podgrupe pri homomorfizmu opet podgrupa, ova funkcije je dobro definirana.

Dokažimo da je φ bijekcija. Za dokaz surjektivnosti neka je H' proizvoljna podgrupa od G/N. Označimo s $H = \pi^{-1}(H')$. Tada je H podgrupa od G kao praslika podgrupe pri

homomorfizmu. Također H sadrži N jer je N jezgra od π pa je sadržana u praslici svake podgrupe. Dakle, $H \in S$ i vrijedi

$$\varphi(H) = \pi(\pi^{-1}(H')) = H'$$

jer je π surjektivan.

Za dokaz injektivnost pretpostavimo da su $H_1, H_2 \in S$ takve da je $\varphi(H_1) = \varphi(H_2)$. Po definiciji funkcije φ to znači da je $\pi(H_1) = \pi(H_2)$. Uočimo da za proizvoljnu podgrupu K grupe G vrijedi

$$\pi(K) = \{kN \,:\, k \in K\},$$

što znači da se $\pi(K)$ sastoji točno od onih lijevih klasa iz G/N čijeg barem jednog predstavnika sadrži podgrupa K. Dakle, H_1 i H_2 imaju svojstvo da za iste lijeve klase u G/N sadrže barem jednog predstavnika. Međutim, podgrupe H_1 i H_2 sadrže N. Ako takva podgrupa sadrži predstavnika g neke lijeve klase gN iz G/N, onda sadrži i čitavu lijevu klasu jer se ona dobije množenjem tog predstavnika s elementima iz N za koje znamo da su u toj podgrupi. Zaključujemo da se H_1 i H_2 sastoje od istih lijevih klasa, pa su stoga jednake. Time smo dokazali injektivnost. □

6.15. Prosta grupa. Definirati... možda par riječi o Aschbacherovoj klasifikaciji za konačne grupe, Janku i njegovim sporadičnim grupama itd. Povezati s idejom da se grupe koje nisu proste mogu proučavati kroz proučavanje normalnih podgrupa i kvocijentnih grupa... Primjere...

7. Teoremi o izomorfizmu

7.1. Motivacija. Teoremi o izomorfizmu daju izomorfizme kvocijentnih grupa koji se dobivaju polazeći od homomorfizama. Iz toga vidimo da homomorfizmi omogućuju usporedbe strukture dvaju grupa. Obično se navode tri teorema o izomorfizmu koji se nazivaju prvi, drugi i treći teorem o izomorfizmu. Zapravo, drugi i treći teorem slijede iz prvog.

7.2. Prvi teorem o izomorfizmu. Neka su G i H grupe te neka je $f : G \to H$ homomorfizam grupa. Tada vrijedi

$$G/\mathrm{Ker}f \cong \mathrm{Im}f,$$

odnosno kvocijentna grupa grupe G po jezgri homomorfizma je izomorfna slici tog izomorfizma.

Dokaz. Za dokaz tražene izomorfnosti grupa potrebno je definirati jedan izomorfizam među njima. Stoga definiramo funkciju

$$\Phi : G/\mathrm{Ker}f \to \mathrm{Im}f$$

na sljedeći način. Elementi kvocijentne grupe $G/\mathrm{Ker}f$ su lijeve klase oblika $g\mathrm{Ker}f$, gdje je $g \in G$ predstavnik te klase. Vrijednost funkcije Φ na takvoj lijevoj klasi mora na neki način ovisiti o homomorfizmu f. Stoga je prirodno pokušati s najjednostavnijom definicijom, a to je

$$\Phi(g\mathrm{Ker}f) = f(g).$$

Uočimo odmah da je desna strana zaista element $\mathrm{Im}f$. **PAZI** Pritom smo, u formuli na desnoj strani definicije funkcije Φ, koristili predstavnika g lijeve klase $g\mathrm{Ker}f$.

Kao i u dokazu teorema 5.9, postavlja se pitanje je li ta definicija dobra, odnosno ovisi li formula na desnoj strani o odabiru predstavnika lijeve klase. Neka su $g, g' \in G$ dva predstavnika jedne te iste lijeve klase $g\mathrm{Ker}f = g'\mathrm{Ker}f \in G/\mathrm{Ker}f$. Posebno to znači da je $g \in g'\mathrm{Ker}f$, pa postoji $x \in \mathrm{Ker}f$ takav da je $g = g'x$. Tada,

$$f(g) = f(g'x) = f(g')f(x) = f(g')e_H = f(g').$$

Iz toga vidimo da bez obzira kojeg predstavnika lijeve klase koristimo, izraz na desnoj strani definicije funkcije Φ se neće promijeniti, a to pokazuje da je definicija funkcije Φ dobra.

Dokažimo da je Φ homomorfizam. Neka su $g_1\mathrm{Ker}f$ i $g_2\mathrm{Ker}f$ dvije proizvoljne lijeve klase iz kvocijentne grupe $G/\mathrm{Ker}f$. Tada, prema definiciji operacije u kvocijentnoj grupi i svojstvu iz definicije za homomorfizam f, vrijedi

$$\Phi\big((g_1\mathrm{Ker}f)(g_2\mathrm{Ker}f)\big) = \Phi(g_1g_2\mathrm{Ker}f) = f(g_1g_2) = f(g_1)f(g_2) = \Phi(g_1\mathrm{Ker}f)\Phi(g_2\mathrm{Ker}f),$$

čime smo dokazali da je Φ homomorfizam.

Da bi dokazali injektivnost od Φ, odnosno da je Φ monomorfizam, koristimo kriterij za monomorfizam. Treba dokazati da je jezgra $\mathrm{Ker}\Phi$ trivijalna, a to znači da se sastoji samo od neutralnog elementa $\mathrm{Ker}f$ kvocijentne grupe $G/\mathrm{Ker}f$. Prema definiciji jezgre i formuli za funkciju Φ vrijedi

$$\begin{aligned}\mathrm{Ker}\Phi &= \{g\mathrm{Ker}f \in G/\mathrm{Ker}f \,:\, \Phi(g\mathrm{Ker}f) = e_H\}\\ &= \{g\mathrm{Ker}f \in G/\mathrm{Ker}f \,:\, f(g) = e_H\}\\ &= \{g\mathrm{Ker}f \in G/\mathrm{Ker}f \,:\, g \in \mathrm{Ker}f\}.\end{aligned}$$

Dakle, jezgra $\mathrm{Ker}\Phi$ se sastoji od svih onih lijevih klasa $g\mathrm{Ker}f$ iz kvocijentne grupe $G/\mathrm{Ker}f$ čiji predstavnik g je element jezgre $\mathrm{Ker}f$. Ali ako je $g \in \mathrm{Ker}f$, onda je $g\mathrm{Ker}f = \mathrm{Ker}f$, pa je $\mathrm{Ker}f$ jedina lijeva klasa u jezgri $\mathrm{Ker}\Phi$. Stoga je

$$\mathrm{Ker}\Phi = \{\mathrm{Ker}f\},$$

pa je Φ zaista monomorfizam.

Surjektivnost od Φ je očigledna, jer je svaki element $h \in \mathrm{Im}f$ oblika $h = f(g)$ za neki element $g \in G$, a tada je vrijednost funkcije Φ na odgovarajućoj lijevoj klasi $g\mathrm{Ker}f$ jednaka upravo

$$\Phi(g\mathrm{Ker}f) = f(g) = h.$$

Stoga je Φ epimorfizam, a onda i izomorfizam. Time je teorem dokazan. □

7.3. Primjeri. Prvi teorem o izomorfizmu daje izomorfizme kvocijentne grupe po jezgri sa slikom homomorfizma. Stoga svaki primjer homomorfizma koji smo ranije naveli daje po jedan takav izomorfizam. Kako smo za sve primjere homomorfizma već ranije izračunali jezgru i sliku, sada navodimo posljedice prvog teorema o izomorfizmu samo za neke interesantnije situacije.

Homomorfizam aditivne grupe cijelih brojeva $f : \mathbb{Z} \to \mathbb{Z}$ definiran formulom

$$f(k) = mk$$

za sve $k \in \mathbb{Z}$, gdje je $m > 1$ prirodan broj, daje izomorfizam aditivne grupe $\mathbb{Z}$ i njene podgrupe $m\mathbb{Z}$. Pritom koristimo činjenicu da je kvocijentna grupa po trivijalnoj podgrupi izomorfna polaznoj grupi.

Kanonski epimorfizam $f : \mathbb{Z} \to \mathbb{Z}_m$, definiran s

$$f(k) = [k]$$

za sve $k \in \mathbb{Z}$, daje izomorfizam kvocijentne grupe $\mathbb{Z}/m\mathbb{Z}$ i aditivne grupe klasa ostataka $\mathbb{Z}_m$. Ovaj izomorfizam smo dokazali već ranije, kao primjer kvocijentne grupe, ali bez korištenja teorema o izomorfizmu.

Homomorfizam $f : \mathbb{R} \to S^1$ namatanja pravca na kružnicu, definiran formulom

$$f(x) = e^{ix}$$

za sve $x \in \mathbb{R}$, pokazuje da je kvocijentna grupa $\mathbb{R}/2\pi\mathbb{Z}$ izomorfna s grupom S^1. S druge strane, homomorfizam $f : \mathbb{R} \to GL_2(\mathbb{R})$ koji realnom broju $\vartheta \in \mathbb{R}$ pridružuje odgovarajuću matricu iz $SO(2)$ pokazuje da je $\mathbb{R}/2\pi\mathbb{Z}$ izomorfna i sa grupom $SO(2)$. Iz ta dva izomorfizma zaključujemo da su grupe $SO(2)$ i S^1 izomorfne.

Determinanta matrica, shvaćena kao homomorfizam

$$\det : GL_n(F) \to F^\times,$$

pokazuje da je kvocijentna grupa $GL_n(F)/SL_n(F)$ izomorfna multiplikativnoj grupi $F^\times$.

I na kraju, za proizvoljnu grupu G, homomorfizam $\Phi : G \to \operatorname{Aut} G$, definiran s

$$\Phi(g) = I_g$$

za sve $g \in G$, gdje je I_g unutarnji automorfizam, pokazuje da je kvocijentna grupa $G/Z(G)$ po centru izomorfna s grupom $\operatorname{Int} G$ unutarnjih automorfizama. Iz ovog izomorfizma vidimo i odakle naziv unutarnji automorfizam. Naime, unutarnje automorfizme možemo na neki način opisati elementima same grupe do na centar.

7.4. Drugi teorem o izomorfizmu. Neka je G grupa, H podgrupa od G, te N normalna podgrupa od G. Tada je NH podgrupa od G, presjek $N \cap H$ normalna podgrupa od H, te vrijedi

$$NH/N \cong H/(N \cap H).$$

Ovaj teorem možemo vizualno pamtiti usporedbom s kraćenjem razlomka, s time da kraćenjem N na lijevoj strani ne ostaje samo H, nego treba još podijeliti H s dijelom koji je zajednički s N, a to je $N \cap H$ koji se javi na desnoj strani.

Dokaz. Najprije dokažimo da je

$$NH = \{nh : n \in N, h \in H\}$$

podgrupa od G. Koristimo kriterij za podgrupe. Neka su n_1h_1 i n_2h_2, gdje su $n_1, n_2 \in N$ i $h_1, h_2 \in H$, dva proizvoljna elementa iz NH. Treba provjeriti da je tada i

$$n_1h_1(n_2h_2)^{-1} \in NH.$$

Taj izraz možemo zapisati u obliku

$$\begin{aligned} n_1h_1(n_2h_2)^{-1} &= n_1h_1h_2^{-1}n_2^{-1} \\ &= n_1h_1h_2^{-1}n_2^{-1}(h_1h_2^{-1})^{-1}h_1h_2^{-1} \\ &= n_1\left[h_1h_2^{-1}n_2^{-1}(h_1h_2^{-1})^{-1}\right] \cdot h_1h_2^{-1}. \end{aligned}$$

Označimo s $h = h_1h_2^{-1} \in H$ te s $n = n_2^{-1} \in N$. Tada je izraz u uglatoj zagradi oblika hnh^{-1}, gdje $h \in H$ i $n \in N$. Budući da je N normalna podgrupa u grupi G, po definiciji

normalne podgrupe dobivamo da je taj izraz $hnh^{-1} \in N$. Stoga je i produkt $n_1 \in N$ s uglatom zagradom koja je iz N također iz N. Nadalje, $h_1 h_2^{-1} \in H$, pa možemo pisati

$$n_1 h_1 (n_2 h_2)^{-1} = \underbrace{n_1 \left[h_1 h_2^{-1} n_2^{-1} (h_1 h_2^{-1})^{-1} \right]}_{\in N} \cdot \underbrace{h_1 h_2^{-1}}_{\in H},$$

iz čega vidimo da je zaista $n_1 h_1 (n_2 h_2)^{-1} \in NH$. Time smo dokazali da je NH podgrupa od G.

Sada primjenimo prvi teorem o izomorfizmu na sljedeći način. Uočimo da je N normalna podgrupa u NH, obzirom da je normalna u još većoj grupi G. Dakle, može se definirati kvocijentna grupa NH/N. Neka je

$$f : H \to NH/N$$

preslikavanje definirano formulom

$$f(h) = hN$$

za sve $h \in H$. Desna strana te formule je lijeva klasa s predstavnikom h u kvocijentnoj grupi NH/N.

Pokazuje se da je f homomorfizam jer vrijedi

$$f(h_1 h_2) = h_1 h_2 N = (h_1 N)(h_2 N) = f(h_1) f(h_2)$$

za sve $h_1, h_2 \in H$. Na taj homomorfizam primjenjujemo prvi teorem o izomorfizmu.

Homomorfizam f je surjektivan, odnosno $\mathrm{Im} f = NH/N$. Naime, proizvoljna lijeva klasa nhN iz kvocijentne grupe NH/N, gdje su $n \in N$ i $h \in H$, može se zapisati kao

$$nhN = h(h^{-1} n h)N = hN.$$

Pritom smo koristili činjenicu da je N normalna podgrupa od G pa je izraz $h^{-1} n h \in N$, odnosno $h^{-1} n h N = N$. Stoga vrijedi

$$f(h) = hN = nhN,$$

što pokazuje da je proizvoljna lijeva klasa nhN iz NH/N u slici od f.

Odredimo jezgru $\mathrm{Ker} f$. Po definiciji jezgre dobivamo

$$\begin{aligned} \mathrm{Ker} f &= \{h \in H \,:\, f(h) = N\} \\ &= \{h \in H \,:\, hN = N\} \\ &= \{h \in H \,:\, h \in N\} \\ &= H \cap N. \end{aligned}$$

Dakle, prema prvom teoremu o izomorfizmu dobivamo

$$H/H \cap N \cong NH/N,$$

što je i trebalo dobiti. □

7.5. Treći teorem o izomorfizmu. Neka je G grupa, a H i K njene normalne podgrupe takve da vrijedi $K \leqslant H \leqslant G$. Tada je H/K normalna podgrupa u G/K i vrijedi

$$(G/K)\Big/(H/K) \cong G/H.$$

Pritom je K normalna u H jer je normalna u većoj grupi G.

Ovaj teorem se može pamtiti usporedbom s dvojnim razlomkom u kojem pokratimo nazivnike, a to je grupa K.

Dokaz. U ovom dokazu također primjenjujemo prvi teorem o izomorfizmu. Neka je

$$f : G/K \to G/H$$

preslikavanje definirano formulom

$$f(gK) = gH,$$

za sve lijeve klase gK iz kvocijentne grupe G/K. Kako na desnoj strani formule koristimo predstavnika g klase gK, treba provjeriti je li f dobro definirano. Neka su g i g' dva predstavnika iste klase u G/K, odnosno $gK = g'K$. To znači da su g i g' u lijevoj relaciji obzirom na grupu K, odnosno $g^{-1}g' \in K$. Međutim, $K \leqslant H$, pa je $g^{-1}g' \in H$, odnosno g i g' su u lijevoj relaciji obzirom na grupu H. Dakle, $gH = g'H$. Iz toga vidimo da desna strana formule za f ne ovisi o izboru predstavnika g.

Preslikavanje f je homomorfizam jer

$$f((g_1K)(g_2K)) = f(g_1g_2K) = g_1g_2H = (g_1H)(g_2H) = f(g_1K)f(g_2K),$$

za sve $g_1, g_2 \in G$. Na homomorfizam f primjenjujemo prvi teorem o izomorfizmu.

Pokažimo da je f surjektivan, odnosno $\mathrm{Im}f = G/H$. Neka je gH, gdje je $g \in G$, proizvoljna lijeva klasa iz kvocijentne grupe G/H. Tada vrijedi

$$f(gK) = gH,$$

gdje je gK lijeva klasa iz kvocijentne grupe G/K s istim predstavnikom g kao i klasa gH. Time je dokazana surjektivnost jer je proizvoljna lijeva klasa $gH \in G/H$ u slici od f.

Odredimo na kraju jezgru $\mathrm{Ker}f$. Po samoj definiciji jezgre i preslikavanja f dobivamo

$$\begin{aligned} \mathrm{Ker}f &= \{gK \in G/K \,:\, f(gK) = H\} \\ &= \{gK \in G/K \,:\, gH = H\} \\ &= \{gK \in G/K \,:\, g \in H\} \\ &= H/K. \end{aligned}$$

Primjenom prvog teorema o izomorfizmu dobivamo

$$(G/K)\Big/(H/K) \cong G/H,$$

što je i tvrdnja teorema. □

8. Djelovanje grupe na skup

8.1. Definicija djelovanja. Neka je G grupa, a S skup. Djelovanje grupe G na skup S je preslikavanje

$$G \times S \to S,$$

čiju vrijednost na uređenom paru $(g, x) \in G \times S$ označavamo sa $g \,.\, x$, te koje zadovoljava uvjete

(D1) $e \,.\, x = x$ za svaki $x \in S$, gdje je e neutralni element grupe G,
(D2) $g_1 \,.(g_2 \,.\, x) = (g_1 g_2) \,.\, x$ za sve $g_1, g_2 \in G$ i svaki $x \in S$.

Oznaka za djelovanje je točkica dolje . (koju uvijek pišemo) i valja ju razlikovati od oznake točkica u sredini $\cdot$ (koju obično ne pišemo) za binarnu operaciju u grupi. Tako $g \,.\, x$ je djelovanje elementa g grupe G na element x skupa S, a $gg' = g \cdot g'$ je binarna operacija između dva elementa g i g' grupe G.

Na primjer, u uvjetu (D2) na lijevoj strani imamo djelovanje elementa $g_2 \in G$ na element $x \in S$. Rezultat je element skupa S na kojeg zatim djelujemo elementom $g_1 \in G$. Na desnoj strani imamo najprije operaciju između elemenata $g_1, g_2 \in G$. Rezultat je element grupe G kojim zatim djelujemo na element $x \in S$.

8.2. Orbita. Orbita je podskup skupa S koji se dobije djelovanjem svih elemenata grupe na jedan izabrani i fiksirani element skupa S. Ako je $x \in S$ taj fiksirani element, onda se orbita koja se dobije pomoću njega zove orbita elementa x i označava $\overline{x}$. Ona je jednaka

$$\overline{x} = \{g \,.\, x \,|\, g \in G\}.$$

Element x zovemo predstavnik orbite. Kardinalni broj orbite, odnosno broj elemenata u orbiti ako je konačna, zove se duljina orbite.

8.3. Orbite kao klase ekvivalencije. Kao i kod lijevih klasa, svojstva orbita se najlakše dokazuju ako se orbite shvate kao klase ekvivalencije za neku relaciju ekvivalencije. Za orbite relacija $\sim$ se definira na skupu S kao

$$x \sim y \text{ ako } y = g \,.\, x \text{ za neki } g \in G,$$

gdje su $x, y \in S$. Drugim riječima, x je u relaciji sa y ako postoji $g \in G$ takav da djelovanje g na x daje y.

Dokažimo da je $\sim$ zaista relacija ekvivalencije. Refleksivnost je očita jer, prema svojstvu (D1) iz definicije djelovanja, za svaki $x \in S$ vrijedi $x = e \,.\, x$, pa je $x \sim x$. Za simetričnost, pretpostavimo da je $x \sim y$ za neke $x, y \in S$. To znači da je $y = g \,.\, x$ za neki $g \in G$. Na obje strane te jednakosti djelujemo elementom g^{-1}. Koristeći svojstva (D2) i (D1) iz definicije djelovanja dobiva se

$$g^{-1} \,.\, y = g^{-1} \,.(g \,.\, x) = (g^{-1} g) \,.\, x = e \,.\, x = x,$$

pa je $y \sim x$ jer se x dobije djelovanjem $g^{-1} \in G$ na y. Time je dokazana simetričnost. Za tranzitivnost pretpostavimo da je $x \sim y$ i $y \sim z$ za neke $x, y, z \in S$. To znači da je $y = g \,.\, x$ za neki $g \in G$ te $z = g' \,.\, y$ za neki $g' \in G$. Uvrstimo li izraz za y u izraz za z, koristeći svojstvo (D2) iz definicije djelovanja dobivamo

$$z = g' \,.\, y = g' \,.(g \,.\, x) = (g' g) \,.\, x,$$

pa je $x \sim z$ jer se z dobije djelovanjem elementa $g'g \in G$ na x. Time je dokazana i tranzitivnost pa je $\sim$ relacija ekvivalencije.

Klasu ekvivalencije elementa $x \in S$ za relaciju $\sim$ označimo s $[x]$. Tada vrijedi

$$\begin{aligned}[x] &= \{y \in S \,:\, x \sim y\} \\ &= \{y \in S \,:\, y = g\,.\,xhboxzanekig \in G\} \\ &= \{g\,.\,x \,:\, g \in G\} \\ &= \overline{x}.\end{aligned}$$

Dakle, klase ekvivalencije za $\sim$ su upravo orbite.

Sada je jasno zbog općih svojstava klasa ekvivalencije da orbite djelovanja čine particiju skupa S, odnosno da su disjunktne i u uniji daju čitav S. Drugim riječima, svaki element iz S pripada točno jednoj orbiti.

8.4. Stabilizator. Neka je $x \in S$. Stabilizator elementa x se definira kao

$$G_x = \{g \in G \,:\, g\,.\,x = x\}.$$

Dakle, stabilizator elementa $x \in S$ čine svi oni elementi grupe G koji "stabiliziraju" x, odnosno ne promijene ga pri djelovanju. Uočimo da je G_x podskup od G koji je neprazan za bilo koji $x \in S$ jer prema svojstvu (D1) iz definicije djelovanja $e\,.\,x = x$, za svaki $x \in S$, pa je $e \in G_x$ za svaki $x \in S$.

Zapravo, G_x je podgrupa od G za svaki $x \in S$. To dokazujemo prema kriteriju za podgrupe. Neka su $g_1, g_2 \in G_x$ proizvoljni. Treba dokazati da je onda i $g_1 g_2^{-1} \in G_x$. Najprije, budući da je $g_2 \in G_x$, vrijedi $g_2\,.\,x = x$. Djelovanjem s g_2^{-1} na obje strane te jednakosti dobije se

$$g_2^{-1}\,.\,x = g_2^{-1}\,.(g_2\,.\,x) = (g_2^{-1}g_2)\,.\,x = e\,.\,x = x,$$

što pokazuje da je i $g_2^{-1} \in G_x$. Sada je jasno da vrijedi

$$(g_1 g_2^{-1})\,.\,x = g_1\,.(g_2^{-1}\,.\,x) = g_1\,.\,x = x,$$

odnosno $g_1 g_2^{-1} \in G_x$, pa je G_x podgrupa prema kriteriju.

Stabilizator G_x elementa $x \in S$ još se naziva i grupa izotropije od x.

8.5. Teorem. Neka grupa G djeluje na skup S. Tada je orbita $\overline{x}$ elementa $x \in S$ u bijekciji sa skupom G/G_x lijevih klasa stabilizatora G_x u grupi G. Dakle, duljina orbite $\overline{x}$ je jednaka indeksu $[G : G_x]$.

Dokaz. Funkciju $\varphi : G/G_x \to \overline{x}$ definiramo formulom

$$\varphi(gG_x) = g\,.\,x,$$

za sve $g \in G$. Jasno je da je desna strana element orbite od x jer se dobije djelovanjem elementa g na x. Budući da se u formuli na desnoj strani koristi predstavnik g lijeve klase gG_x valja provjeriti da je definicija dobra, odnosno da formula ne ovisi o odabiru predstavnika. Neka su g i g' dva predstavnika iste lijeve klase. To znači da je $gG_x = g'G_x$. Posebno, $g' \in gG_x$, pa postoji element $g_0 \in G_x$ takav da je $g' = gg_0$. Stoga, koristeći svojstvo (D2), vrijedi

$$g'\,.\,x = (gg_0)\,.\,x = g\,.(g_0\,.\,x) = g\,.\,x,$$

što pokazuje da desna strana formule za φ ne ovisi o odabiru predstavnika za lijevu klasu gG_x.

Dokažimo da je φ bijekcija. Najprije dokazujemo injektivnost. Pretpostavimo da je $\varphi(gG_x) = \varphi(g'G_x)$ za neke dvije lijeve klase gG_x i $g'G_x$. Tada, prema definiciji funkcije φ, vrijedi $g \,.\, x = g' \,.\, x$. Djelovanjem g^{-1} na obje strane te jednakosti, te korištenjem definicije djelovanja, dobiva se

$$\begin{aligned} g^{-1} \,.(g' \,.\, x) &= g^{-1} \,.(g \,.\, x) \\ (g^{-1}g') \,.\, x &= (g^{-1}g) \,.\, x \\ (g^{-1}g') \,.\, x &= e \,.\, x \\ (g^{-1}g') \,.\, x &= x. \end{aligned}$$

Dakle, $g^{-1}g' \in G_x$. Prema definiciji lijeve relacije obzirom na podgrupu G_x to znači da je $g \sim_l g'$, odnosno $gG_x = g'G_x$. Time je dokazana injektivnost.

Za dokaz surjektivnosti, neka je $y \in \overline{x}$ proizvoljan element orbite od x. Tada vrijedi $y = g \,.\, x$ za neki $g \in G$. Za taj g vrijedi

$$\varphi(gG_x) = g \,.\, x = y,$$

pa je y u slici od φ. Time smo dokazali i surjektivnost.

Zadnja tvrdnja teorema odmah slijedi iz dokazane bijektivnosti jer skupovi među kojima postoji bijekcija imaju jednak kardinalni broj, a duljina orbite je kardinalni broj orbite, dok je indeks $[G : G_x]$ kardinalni broj skupa lijevih klasa. □

NEVEN: pazi kad su g i g' dva predstavnika iste klase onda odmah slijedi da su $g, g' \in gG_x = g'G_x$. To treba vidjeti kroz cijeli tekst da nisam previse komplicirao.

8.6. Teorem. Neka grupa G djeluje na skup S. Neka je G_x stabilizator elementa $x \in S$. Neka je $y \in S$ element orbite $\overline{x}$ elementa x. Tada je stabilizator G_y elementa y jednak

$$G_y = g_0 G_x g_0^{-1},$$

gdje je $g_0 \in G$ takav da je $y = g_0 \,.\, x$. Posebno, $G_x \cong G_y$, odnosno stabilizatori svih elemenata orbite su međusobno izomorfni.

Dokaz. Prema definiciji stabilizatora, $g \in G_y$ ako i samo vrijedi $g \,.\, y = y$. Uvrstimo li $y = g_0 \,.\, x$ dobivamo

$$g \,.(g_0 \,.\, x) = g_0 \,.\, x.$$

Djelovanjem s g_0 na obje strane i koristeći svojstva iz definicije djelovanja dobivamo

$$(g_0^{-1} g g_0) \,.\, x = x.$$

Dakle, $g \in G_y$ ako i samo ako je $g_0^{-1} g g_0 \in G_x$. Množenjem posljednjeg uvjeta elementom g_0 slijeva i elementom g_0^{-1} sdesna dobivamo da je $g \in G_y$ ako i samo ako

$$g \in g_0 G_x g_0^{-1}.$$

Time smo dokazali da je $G_y = g_0 G_x g_0^{-1}$. Svi stabilizatori elemenata jedne orbite su stoga međusobno konjugirani, pa onda i izomorfni, jer su konjugirane podgrupe uvijek izomorfne kao što smo već ranije dokazali. □

8.7. Fiksne točke. Fiksna točka djelovanja grupe G na skup S je element $x \in S$ za koji vrijedi $g \,.\, x = x$ za sve $g \in G$. Drugim riječima, $x \in S$ je fiksna točka ako ju stabiliziraju svi elementi grupe G, odnosno ako je njen stabilizator čitava grupa G. Skup svih fiksnih točaka označimo s S_0. Tada

$$\begin{aligned} S_0 &= \{x \in S \,:\, g \,.\, x = x \text{ za sve } g \in G\} \\ &= \{x \in S \,:\, G_x = G\}. \end{aligned}$$

8.8. Primjer: djelovanje $SL_2(\mathbb{R})$ na prošireni skup kompleksnih brojeva. Neka je za početak $S = \mathbb{C}$ skup kompleksnih brojeva. Za matricu

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R})$$

promatramo funkciju koja kompleksnom broju $z \in \mathbb{C}$ pridružuje

$$\frac{az+b}{cz+d}.$$

Funkcija definirana ovom formulom naziva se Möbiusova transformacija. Međutim, ta funkcija nije definirana na čitavom skupu $\mathbb{C}$. Naime, za sve matrice za koje je $c \neq 0$ uvrstimo li $z = -d/c$ u gornju formulu dobivamo da je nazivnik jednak nuli.

Problem s definiranjem Möbiuseve transformacije može se riješiti na sljedeći način. Skup kompleksnih brojeva se proširi još jednom točkom koju označavamo s ∞ i zovemo točka u beskonačnosti. Neka je

$$\widehat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$$

prošireni skup kompleksnih brojeva. Sada se Möbiusovu transformaciju može definirati kao funkciju iz $\widehat{\mathbb{C}}$ u $\widehat{\mathbb{C}}$. Naime, ako je

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R})$$

takva da je $c \neq 0$, onda odgovarajuću Möbiusovu transformaciju

$$f_g : \widehat{\mathbb{C}} \to \widehat{\mathbb{C}}$$

definiramo kao

$$f_g(z) = \frac{az+b}{cz+d}$$

ako je $z \in \widehat{\mathbb{C}}$ te $z \neq -d/c$ i $z \neq \infty$. Za problematičnu točku $z = -d/c$ definiramo

$$f_g(-d/c) = \infty,$$

dok za točku u beskonačnosti $z = \infty$ definiramo

$$f_g(\infty) = a/c.$$

Ako je pak u matrici g element $c = 0$, onda je $d \neq 0$ jer bi inače matrica imala nulredak pa ne bi bila regularna. Tada odgovarajuću Möbiusovu transformaciju

$$f_g : \widehat{\mathbb{C}} \to \widehat{\mathbb{C}}$$

možemo za sve $z \in \mathbb{C}$ definirati formulom

$$f_g(z) = \frac{az+b}{cz+d} = \frac{az+b}{d},$$

jer sada nema problema s nulom u nazivniku. Za točku u beskonačnosti $z = \infty$ definiramo

$$f_g(\infty) = \infty.$$

Time smo za svaku matricu $g \in SL_2(\mathbb{R})$ definirali odgovarajuću Möbiusovu transformaciju $f_g : \widehat{\mathbb{C}} \to \widehat{\mathbb{C}}$. Sada definiramo djelovanje grupe $SL_2(\mathbb{R})$ na skup $\widehat{\mathbb{C}}$ formulom

$$g \,.\, z = f_g(z)$$

za sve $g \in SL_2(\mathbb{R})$ i $z \in \widehat{\mathbb{C}}$, pri čemu je $f_g : \widehat{\mathbb{C}} \to \widehat{\mathbb{C}}$ Möbiusova transformacija određena s g.

Dokažimo da je time zaista definirano djelovanje. Za svojstvo (1) podsjetimo da je neutralni element u grupi $SL_2(\mathbb{R})$ jedinična matrica

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Za jediničnu matricu vrijedi

$$I \,.\, z = f_I(z) = \frac{1 \cdot z + 0}{0 \cdot z + 1} = z$$

za sve $z \in \mathbb{C}$, te

$$I \,.\, \infty = f_I(\infty) = \infty.$$

Dakle,

$$I \,.\, z = z$$

za sve $z \in \widehat{\mathbb{C}}$, pa je svojstvo (1) iz definicije djelovanja ispunjeno.

Za svojstvo (2), neka su $g_1, g_2 \in SL_2(\mathbb{R})$. Tada vrijedi

$$g_1 \,.(g_2 \,.\, z) = g_1 \,.\, \big(f_{g_2}(z)\big) = f_{g_1}\big(f_{g_2}(z)\big) = (f_{g_1} \circ f_{g_2})(z),$$

te

$$(g_1 g_2) \,.\, z = f_{g_1 g_2}(z),$$

za sve $z \in \widehat{\mathbb{C}}$. Stoga je svojstvo (2) iz definicije djelovanja ispunjeno ako i samo ako vrijedi

$$f_{g_1} \circ f_{g_2} = f_{g_1 g_2}$$

za sve $g_1, g_2 \in SL_2(\mathbb{R})$. Neka su

$$g_1 = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}, g_2 = \begin{pmatrix} a_2 & b_2 \\ c_2 & d_2 \end{pmatrix} \in SL_2(\mathbb{R}).$$

Tada je

$$g_1 g_2 = \begin{pmatrix} a_1 a_2 + b_1 c_2 & a_1 b_2 + b_1 d_2 \\ c_1 a_2 + d_1 c_2 & c_1 b_2 + d_1 d_2 \end{pmatrix}.$$

Ako je $z \in \mathbb{C}$ takav da su svi nazivnici u sljedećem računu različiti od nule, onda vrijedi

$$\begin{aligned}(f_{g_1} \circ f_{g_2})(z) = f_{g_1}\big(f_{g_2}(z)\big) &= f_{g_1}\left(\frac{a_2 z + b_2}{c_2 z + d_2}\right) \\ &= \frac{a_1 \cdot \frac{a_2 z + b_2}{c_2 z + d_2} + b_1}{c_1 \cdot \frac{a_2 z + b_2}{c_2 z + d_2} + d_1} \\ &= \frac{\frac{a_1(a_2 z + b_2) + b_1(c_2 z + d_2)}{c_2 z + d_2}}{\frac{c_1(a_2 z + b_2) + d_1(c_2 z + d_2)}{c_2 z + d_2}} \\ &= \frac{(a_1 a_2 + b_1 c_2) z + (a_1 b_2 + b_1 d_2)}{(c_1 a_2 + d_1 c_2) z + (c_1 b_2 + d_1 d_2)} \\ &= f_{g_1 g_2}(z).\end{aligned}$$

Ostaje provjeriti što se dešava u posebnim slučajevima za koje gornji račun ne vrijedi zbog nule u nekom od nazivnika, te u točki u beskonačnosti. Nazivnici koji se javljaju su

$$c_2 z + d_2$$

te

$$(c_1 a_2 + d_1 c_2) z + (c_1 b_2 + d_1 d_2).$$

Stoga problemi mogu nastati jedino u točkama

$$\begin{aligned} z &= -\tfrac{d_2}{c_2}, && \text{ako je } c_2 \neq 0, \\ z &= -\tfrac{c_1 b_2 + d_1 d_2}{c_1 a_2 + d_1 c_2}, && \text{ako je } c_1 a_2 + d_1 c_2 \neq 0. \end{aligned}$$

Promatramo posebno svaki od mogućih slučajeva, ali, radi kratkoće, preskačemo same račune koji se ionako svode na uvrštavanje posebnih slučajeva u formule Möbiusovih transformacija.

Pretpostavimo najprije da je $c_2 = 0$. Tada je

$$c_1 a_2 + d_1 c_2 = c_1 a_2.$$

Uočimo da je $a_2 \neq 0$ jer bi inače matrica g_2 imala nulstupac pa ne bi bila regularna. Stoga je

$$c_1 a_2 = 0 \text{ ako i samo ako } c_1 = 0.$$

Ako je i $c_1 = 0$, onda niti jedan nazivnik nije jednak nuli, pa jedino treba provjeriti što je s točkom u beskonačnosti. Budući da je $c_1 = c_2 = 0$, vrijedi

$$(f_{g_1} \circ f_{g_2})(\infty) = f_{g_1}\big(f_{g_2}(\infty)\big) = f_{g_1}(\infty) = \infty,$$

a zbog $c_1 a_2 + d_1 c_2 = 0 \cdot a_2 + d_1 \cdot 0 = 0$ vrijedi i

$$f_{g_1 g_2}(\infty) = \infty.$$

Dakle, u ovom slučaju vrijedi

$$f_{g_1} \circ f_{g_2}(z) = f_{g_1 g_2}(z)$$

za sve $z \in \widehat{\mathbb{C}}$.

Neka je i dalje $c_2 = 0$, ali sada neka je $c_1 \neq 0$. To znači da je $c_1 a_2 + d_1 c_2 \neq 0$. Stoga je problematična točka jednaka

$$z = -\frac{c_1 b_2 + d_1 d_2}{c_1 a_2 + d_1 c_2} = -\frac{c_1 b_2 + d_1 d_2}{c_1 a_2} = -\frac{b_2}{a_2} - \frac{d_1 d_2}{c_1 a_2}.$$

Račun, čije detalje prepuštamo čitaocu, daje

$$(f_{g_1} \circ f_{g_2}) \left(-\frac{b_2}{a_2} - \frac{d_1 d_2}{c_1 a_2} \right) = f_{g_1} \left(-\frac{d_1}{c_1} \right) = \infty$$

dok s druge strane,

$$f_{g_1 g_2} \left(-\frac{b_2}{a_2} - \frac{d_1 d_2}{c_1 a_2} \right) = \infty,$$

budući da je nazivnik transformacije $f_{g_1 g_2}$ jednak nuli u toj točki. Što se tiče točke u beskonačnosti,

$$(f_{g_1} \circ f_{g_2})(\infty) = f_{g_1}(\infty) = \frac{a_1}{c_1},$$

$$f_{g_1 g_2}(\infty) = \frac{a_1 a_2 + b_1 c_2}{c_1 a_2 + d_1 c_2} = \frac{a_1}{c_1}.$$

Dakle, i u ovom slučaju

$$f_{g_1} \circ f_{g_2}(z) = f_{g_1 g_2}(z)$$

za sve $z \in \widehat{\mathbb{C}}$.

Neka je sada $c_2 \neq 0$, ali $c_1 a_2 + d_1 c_2 = 0$. Tada je jedina problematična točka jednaka

$$z = -d_2/c_2.$$

Uočimo da je u ovom slučaju i $c_1 \neq 0$, jer kad bi bilo $c_1 = 0$, onda bi iz uvjeta $c_1 a_2 + d_1 c_2 = 0$ slijedilo da je $d_1 = 0$. To bi značilo da matrica g_1 nije regularna jer ima nulredak. Stoga vrijedi

$$(f_{g_1} \circ f_{g_2})\,(-d_2/c_2) = f_{g_1}(\infty) = a_1/c_1,$$

te koristeći uvjet $c_1 a_2 + d_1 c_2 = 0$, odnosno $d_1 c_2 = -c_1 a_2$, nakon računa koji prepuštamo čitaocu, dobivamo

$$f_{g_1 g_2}\,(-d_2/c_2) = a_1/c_1$$

Za točku u beskonačnosti vrijedi

$$(f_{g_1} \circ f_{g_2})(\infty) = f_{g_1}\big(f_{g_2}(\infty)\big) = f_{g_1}(a_2/c_2) = \infty,$$

jer je u točki a_2/c_2 nazivnik Möbiusove transformacije f_{g_1} jednak nuli, te

$$f_{g_1 g_2}(\infty) = \infty$$

jer je $c_1 a_2 + d_1 c_2 = 0$. Dakle, i u ovom slučaju je

$$f_{g_1} \circ f_{g_2}(z) = f_{g_1 g_2}(z)$$

za sve $z \in \widehat{\mathbb{C}}$.

Na kraju, neka je $c_2 \neq 0$ i $c_1 a_2 + d_1 c_2 \neq 0$. Tada su obje točke problematične. Najprije, za točku $z = -d_2/c_2$, računamo

$$(f_{g_1} \circ f_{g_2})\,(-d_2/c_2) = f_{g_1}\,(f_{g_2}\,(-d_2/c_2)) = f_{g_1}(\infty) = \begin{cases} a_1/c_1, & \text{ako je } c_1 \neq 0, \\ \infty, & \text{ako je } c_1 = 0. \end{cases}$$

S druge strane, ako je $c_1 \neq 0$, onda račun koji prepuštamo čitaocu daje

$$f_{g_1 g_2}\,(-d_2/c_2) = a_1/c_1,$$

a ako je $c_1 = 0$, onda je nazivnik Möbiusove transformacije $f_{g_1g_2}$ u točki $z = -d_2/c_2$ jednak nuli pa je

$$f_{g_1g_2}\left(-d_2/c_2\right) = \infty.$$

Zatim, za točku $z = -\frac{c_1b_2+d_1d_2}{c_1a_2+d_1c_2}$, račun za $c_1 \neq 0$ koji prepuštamo čitaocu daje

$$(f_{g_1} \circ f_{g_2}) \left(-\frac{c_1b_2 + d_1d_2}{c_1a_2 + d_1c_2}\right) = f_{g_1}(-d_1/c_1) = \infty.$$

Za $c_1 = 0$, nazivnik transformacije f_{g_2} u toj točki jednak je nuli. Stoga je i tada

$$(f_{g_1} \circ f_{g_2}) \left(-\frac{c_1b_2 + d_1d_2}{c_1a_2 + d_1c_2}\right) = f_{g_1}(\infty) = \infty.$$

S druge strane, nazivnik Möbiusove transformacije $f_{g_1g_2}$ je nula u toj točki pa je

$$f_{g_1g_2}\left(-\frac{c_1b_2 + d_1d_2}{c_1a_2 + d_1c_2}\right) = \infty.$$

Preostaje provjeriti točku u beskonačnosti. Za nju vrijedi

$$(f_{g_1} \circ f_{g_2})(\infty) = f_{g_1}(a_2/c_2) = \frac{a_1a_2 + b_1c_2}{c_1a_2 + d_1c_2},$$

te

$$f_{g_1g_2}(\infty) = \frac{a_1a_2 + b_1c_2}{c_1a_2 + d_1c_2}.$$

Dakle, u ovom slučaju također vrijedi

$$(f_{g_1} \circ f_{g_2})(z) = f_{g_1g_2}(z)$$

za sve $z \in \widehat{\mathbb{C}}$. Time smo provjerili sve moguće posebne slučaje pa zaista vrijedi svojstvo (2) iz definicije djelovanja.

Pokažimo sada da ovo djelovanje grupe $SL_2(\mathbb{R})$ na skup $\widehat{\mathbb{C}}$ ima tri orbite i to

$$\begin{aligned}
\mathcal{H} &= \{z \in \mathbb{C} : \mathrm{im}(z) > 0\},\\
\widehat{\mathbb{R}} &= \mathbb{R} \cup \{\infty\} = \{z \in \mathbb{C} : \mathrm{im}(z) = 0\} \cup \{\infty\},\\
\overline{\mathcal{H}} &= \{z \in \mathbb{C} : \mathrm{im}(z) < 0\},
\end{aligned}$$

gdje im označava imaginarni dio kompleksnog broja. Obično se $\mathcal{H}$ naziva gornja, a $\overline{\mathcal{H}}$ donja poluravnina, dok je $\widehat{R}$ proširena realna os. U dokazu prvo fiksiramo po jednu točku u svakom od skupova $\mathcal{H}$, $\widehat{R}$ i $\overline{\mathcal{H}}$. Neka su te fiksirane točke

$$i \in \mathcal{H}, \quad 0 \in \widehat{\mathbb{R}}, \quad -i \in \overline{\mathcal{H}}.$$

Treba dokazati da su orbite određene tim točkama redom jednake skupovima $\mathcal{H}$, $\widehat{R}$ i $\overline{\mathcal{H}}$.

Uočimo najprije da za

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R})$$

i $z \in \mathbb{C}$ vrijedi formula

$$\mathrm{im}\,(g\,.\,z) = \frac{\mathrm{im}(z)}{|cz + d|^2},$$

gdje $z \neq -d/c$ ako je $c = 0$. Naime,

$$\begin{aligned} g\,.\,z = f_g(z) &= \frac{az+b}{cz+d}\cdot\frac{c\overline{z}+d}{c\overline{z}+d} \\ &= \frac{ac|z|^2+bd+adz+bc\overline{z}}{|cz+d|^2} \\ &= \frac{ac|z|^2+bd+ad\,\mathrm{re}(z)+bc\,\mathrm{re}(z)}{|cz+d|^2}+i\frac{(ad-bc)\,\mathrm{im}(z)}{|cz+d|^2} \\ &= \frac{ac|z|^2+bd+ad\,\mathrm{re}(z)+bc\,\mathrm{re}(z)}{|cz+d|^2}+i\frac{\mathrm{im}(z)}{|cz+d|^2}, \end{aligned}$$

gdje re označava realni dio kompleksnog broja.

Dokažimo sada da je orbita određena elementom $i \in \mathcal{H}$ jednaka $\mathcal{H}$. Svaka točka $z \in \mathcal{H}$ je u relaciji $\sim$ s točkom $i \in \mathcal{H}$. Zaista, ako je $z = x + iy \in \mathcal{H}$ proizvoljan, gdje je $x \in \mathbb{R}$ i $y > 0$, onda za matricu

$$\begin{pmatrix} y^{1/2} & xy^{-1/2} \\ 0 & y^{-1/2} \end{pmatrix} \in SL_2(\mathbb{R})$$

vrijedi

$$\begin{pmatrix} y^{1/2} & xy^{-1/2} \\ 0 & y^{-1/2} \end{pmatrix}.i = \frac{y^{1/2}i + xy^{-1/2}}{y^{-1/2}} = x + iy = z.$$

Dakle, $i \sim z$ za svaki $z \in \mathcal{H}$. S druge strane, za proizvoljnu matricu

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R})$$

vidjeli smo da je

$$\mathrm{im}(g\,.\,i) = \frac{\mathrm{im}(i)}{|ci+d|^2} = \frac{1}{c^2+d^2} > 0,$$

pa i nije u relaciji s kompleksnim brojevima koji nisu u $\mathcal{H}$ niti s točkom ∞. Time smo dokazali da je orbita kompleksnog broja i jednaka $\mathcal{H}$.

Dokaz da je orbita kompleksnog broja $-i$ jednaka $\overline{\mathcal{H}}$ vrlo je sličan prethodnom. Naime, za proizvoljni $z = x - iy \in \overline{\mathcal{H}}$, gdje je $x \in \mathbb{R}$ i $y > 0$, vrijedi

$$\begin{pmatrix} y^{1/2} & xy^{-1/2} \\ 0 & y^{-1/2} \end{pmatrix}.-i = \frac{y^{1/2}(-i) + xy^{-1/2}}{y^{-1/2}} = x - iy = z,$$

a s druge strane za proizvoljnu matricu $g \in SL_2(\mathbb{R})$, oblika kao u prethodnom dokazu, vrijedi

$$\mathrm{im}\left(g\,.(-i)\right) = \frac{\mathrm{im}(-i)}{|c(-i)+d|^2} = \frac{-1}{c^2+d^2} < 0.$$

Dakle, svi kompleksni brojevi iz $\overline{\mathcal{H}}$ su u relaciji s $-i$, dok svi koji nisu iz $\overline{\mathcal{H}}$ i točka ∞ nisu u relaciji s $-i$. Time smo dokazali da je orbita od $-i$ jednaka $\overline{\mathcal{H}}$.

Na kraju za $0 \in \widehat{\mathbb{R}}$ već smo vidjeli da niti jedan element izvan $\widehat{\mathbb{R}}$ nije u relaciji s 0. S druge strane, proizvoljni $x \in \mathbb{R}$ dobivamo kao

$$\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}.0 = \frac{1\cdot 0 + x}{1} = x,$$

pa je $0 \sim x$. Točku ∞ dobivamo kao

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} . 0 = \infty$$

jer je nazivnik te Möbiusove transformacije u točki 0 jednak $1 \cdot 0 + 0 = 0$. Time smo dokazali da je orbita broja 0 zaista jednaka $\widehat{\mathbb{R}}$.

Da bi odredili stabilizatore dovoljno je odrediti stabilizator po jednog elementa svake orbite jer smo dokazali teorem koji kaže da ostale dobivamo konjugiranjem. Stabilizator elementa $i \in \mathcal{H}$ računamo prema definiciji. Za

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R})$$

vrijedi

$$g \,.\, i = \begin{pmatrix} a & b \\ c & d \end{pmatrix} . i = \frac{ai+b}{ci+d} \cdot \frac{-ci+d}{-ci+d} = \frac{ac+bd+i(ad-bc)}{c^2+d^2} = \frac{ac+bd}{c^2+d^2} + i\frac{1}{c^2+d^2}.$$

Stoga je $g \,.\, i = i$ ako i samo ako je

$$\frac{ac+bd}{c^2+d^2} = 0 \quad \text{i} \quad \frac{1}{c^2+d^2} = 1,$$

što je ekvivalentno uvjetima

$$ac + bd = 0 \quad \text{i} \quad c^2 + d^2 = 1.$$

Treći uvjet daje determinanta jer

$$\det g = ad - bc = 1.$$

Iz ta tri uvjeta može se odrediti $a^2 + b^2$. Promatramo dva slučaja ovisno o tome je li $c = 0$ ili $c \neq 0$. Ako $c \neq 0$, onda iz prvog uvjeta možemo izraziti $a = -bd/c$. Uvrstimo li to u treći uvjet, dobivamo

$$\frac{-bd}{c} \cdot d - bc = 1,$$

što nakon množenja s c daje

$$-b(d^2 + c^2) = c,$$

pa zbog drugog uvjeta slijedi $b = -c$. Vratimo li b u izraz za a dobivamo da je $a = d$. Dakle,

$$a^2 + b^2 = d^2 + (-c)^2 = 1.$$

Ako je $c = 0$, onda se tri uvjeta pojednostavljaju i postaju

$$bd = 0, \quad d^2 = 1, \quad ad = 1.$$

Iz drugog uvjeta vidimo da je $d = \pm 1$, pa preostala dva uvjeta daju $b = 0$ i $a = 1/d = \mp 1$. Dakle, i u ovom slučaju je

$$a^2 + b^2 = 1.$$

Zaključujemo da je stabilizator elementa i jednak podgrupi

$$\left\{ g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R}) \,:\, a^2 + b^2 = c^2 + d^2 = 1, \text{ te } ac + bd = 0 \right\}.$$

S druge strane, vidjeli smo u primjerima homomorfizama da je to specijalna grupa $SO(2)$ ortogonalnih matrica reda 2. Dakle, stabilizator broja $i \in \mathcal{H}$ jednak je grupi $SO(2)$, pa se

čitava orbita $\mathcal{H}$ može poistovjetiti s lijevim razredima $SL_2(\mathbb{R})/SO(2)$ kao što je općenito dokazano u jednom ranije dokazanom teoremu.

Za donju poluravninu, odnosno točku $-i$, na potpuno jednak način dokazujemo da je stabilizator $SO(2)$. Za stabilizatore elemenata orbite $\widehat{\mathbb{R}}$ najelegantnije je odrediti stabilizator točke ∞. Naime, za nju je po samoj definiciji Möbiusevih transformacija

$$g\,.\,\infty = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.\infty = \begin{cases} a/c, & \text{ako je } c \neq 0, \\ \infty, & \text{ako je } c = 0, \end{cases}$$

za $g \in SL_2(\mathbb{R})$. Dakle, stabilizator točke ∞ je jednak

$$\left\{ g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R}) \,:\, c = 0 \right\} = \left\{ g = \begin{pmatrix} a & b \\ 0 & a^{-1} \end{pmatrix} \,:\, a \in \mathbb{R}^\times, b \in \mathbb{R} \right\},$$

a to je podgrupa gornjetrokutastih matrica u $SL_2(\mathbb{R})$.

8.9. Primjer: djelovanje modularne grupe $SL_2(\mathbb{Z})$ na gornju poluravninu. Neka grupa G djeluje na skup S. Za $g \in G$ i $x \in S$ neka $g\,.\,x$ označava djelovanje elementa g grupe na element x skupa. Neka je S' podskup skupa S koji je jednak uniji nekih od orbita. Tada djelovanje grupe G na skup S definira djelovanje grupe G na skup S'. Naime, za $g \in G$ i $x \in S'$ naprosto definiramo djelovanje s $g\,.\,x$. Kako je S' unija orbita, vidimo da $g\,.\,x \in S'$, a svojstva (1) i (2) iz definicije djelovanja se nasljeđuju.

Posebno, za djelovanje grupe $SL_2(\mathbb{R})$ na skup $\widehat{\mathbb{C}}$ iz prethodnog primjera, možemo promatrati djelovanje grupe $SL_2(\mathbb{R})$ na gornju poluravninu $\mathcal{H}$, obzirom da je $\mathcal{H}$ orbita. Formula tog djelovanja ostaje ista. Za $g \in SL_2(\mathbb{R})$ i $z \in \mathcal{H}$ djelovanje je definirano formulom

$$g\,.\,z = f_g(z),$$

gdje je f_g Möbiusova transformacija određena s g.

Ako grupa djeluje na skup, onda i svaka njena podgrupa djeluje na taj isti skup. Tako djelovanje grupe $SL_2(\mathbb{R})$ na gornju poluravninu $\mathcal{H}$ možemo restringirati na djelovanje njenih podgrupa, kao što su modularna grupa i kongruencije podgrupe. Na taj način dobivamo djelovanje tih podgrupa na gornju poluravninu Möbiusovim transformacijama. Mi ćemo promatrati jedino djelovanje modularne grupe $SL_2(\mathbb{Z})$, iako je i djelovanje kongruencijskih podgrupa iznimno važno, posebice u teoriji brojeva. Ta djelovanja se javljaju u definiciji modularnih formi, što je jedan od najvažnijih objekata izučavanja u matematici uopće.

Za razliku od djelovanja veće grupe $SL_2(\mathbb{R})$, djelovanje modularne grupe $SL_2(\mathbb{Z})$ na gornju poluravninu $\mathcal{H}$ Möbiusovim transformacijama ima puno orbita. Opisujemo ih tako da odredimo po jednog predstavnika svake orbite. Neka je

$$\mathcal{F}^\circ = \{ z \in \mathcal{H} \,:\, |z| > 1,\, |\operatorname{re}(z)| < 1/2 \}\,.$$

To je otvorena pruga (rub nije uključen) u $\mathcal{H}$ između okomitih pravaca kroz točke $1/2$ i $-1/2$ na x osi i s donje strane omeđena lukom jedinične kružnice sa središtem u ishodištu. Neka je, nadalje,

$$\mathcal{F}_1 = \{ z \in \mathcal{H} \,:\, |z| \geq 1,\, \operatorname{re}(z) = -1/2 \}$$

polupravac koji tvori lijevi rub skupa $\mathcal{F}^\circ$, te

$$\mathcal{F}_2 = \{ z \in \mathcal{H} \,:\, |z| = 1,\, -1/2 < \operatorname{re}(z) \leq 0 \}$$

lijeva polovica luka jediniče kružnice koji tvori donji rub skupa $\mathcal{F}^\circ$. Definiramo podskup $\mathcal{F}$ gornje poluravnine $\mathcal{H}$ kao uniju ova tri skupa, odnosno

$$\mathcal{F} = \mathcal{F}^\circ \cup \mathcal{F}_1 \cup \mathcal{F}_2.$$

Pokazuje se da su elementi skupa $\mathcal{F}$ predstavnici međusobno različitih orbita djelovanja $SL_2(\mathbb{Z})$ na $\mathcal{H}$, te da na taj način dobijemo sve orbite, odnosno da svaka orbita ima predstavnika u skupu $\mathcal{F}$.

Što se tiče stabilizatora, uočimo da, osim jedinične matrice I_2, i matrica $-I_2 \in SL_2(\mathbb{Z})$ stabilizira sve $z \in \mathcal{H}$, jer za nju vrijedi

$$-I_2 \,.\, z = \frac{-1 \cdot z + 0}{0 \cdot z - 1} = z$$

za svaki $z \in \mathcal{H}$. Pokazuje se da je to čitav stabilizator za sve točke $z \in \mathcal{F}$, osim točaka i te $\rho = -1/2 + i\sqrt{3}/2$. Dakle, stabilizator svih točaka $z \in \mathcal{F}$, osim dvije navedene, je grupa reda 2, pa stoga izomorfna grupi $\mathbb{Z}_2$.

Za točku $i \in \mathcal{F}$, pokazuje se da je stabilizator jednak podgrupi od $SL_2(\mathbb{Z})$ generiranoj matricom

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in SL_2(\mathbb{Z}).$$

Ta matrica je reda 4, pa je stabilizator od i ciklička grupa reda 4. Stoga je izomorfan grupi $\mathbb{Z}_4$.

Za točku $\rho \in \mathcal{F}$, pokazuje se da je stabilizator jednak podgrupi od $SL_2(\mathbb{Z})$ generiranoj matricom

$$S' = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \in SL_2(\mathbb{Z}).$$

To je matrica reda 6, pa je stabilizator od ρ ciklička grupa reda 6. Stoga je izomorfan grupi $\mathbb{Z}_6$.

Dokaz ovih činjenica o orbitama i stabilizatorima, iako elementaran, preskačemo zbog njegove duljine[3].

8.10. Primjer: djelovanje grupe bijekcija skupa S na skup S. Neka je S skup i G grupa svih bijekcija skupa S. Tada možemo definirati djelovanje grupe G na skup S kao

$$f \,.\, x = f(x)$$

za sve bijekcije $f \in G$ i sve $x \in S$. Drugim riječima, bijekcija $f : S \to S$ djeluje na $x \in S$ tako što izračunamo vrijednost funkcije f na elementu x. Dokažimo da je time zaista definirano djelovanje grupe na skup. Neutralni element u grupi bijekcija je identiteta. Za identitetu id na skupu S vrijedi

$$id \,.\, x = id(x) = x$$

za sve $x \in S$, pa vrijedi svojstvo (1) iz definicije djelovanja. Neka su sada $f_1, f_2 \in G$ dvije bijekcije. Tada, prema definiciji kompozicije funkcija, vrijedi

$$f_1 \,.(f_2 \,.\, x) = f_1 \,.\, \big(f_2(x)\big) = f_1\big(f_2(x)\big) = (f_1 \circ f_2)(x) = (f_1 \circ f_2) \,.\, x$$

za sve $x \in S$. Kako su f_1 i f_2 bile proizvoljne, time smo dokazali i svojstvo (2) iz definicije djelovanja.

[3]Serre: A course in arithmetic...

Odredimo orbite ovog djelovanja. Neka su $x_1, x_2 \in S$ proizvoljni. Tada možemo definirati $f \in G$, odnosno bijekciju $f : S \to S$, formulom

$$f(x) = \begin{cases} x_2, & \text{za } x = x_1, \\ x_1, & \text{za } x = x_2, \\ x, & \text{za } x \in S \setminus \{x_1, x_2\}. \end{cases}$$

Dakle, preslikavanje f zamijeni elemente x_1 i x_2, a na svim ostalim elementima djeluje kao identiteta. To je očito bijekcija. Za tako definiranu $f \in G$ vrijedi

$$f \,.\, x_1 = f(x_1) = x_2,$$

pa je $x_1 \sim x_2$. Time smo dokazali da su proizvoljna dva elementa skupa S u relaciji koja definira orbite. Dakle, djelovanje grupe bijekcija skupa S na skup S ima samo jednu orbitu, a to je čitav S.

Neka je sada $x \in S$. Prema definiciji, stabilizator G_x elementa x u grupi G bijekcija skupa S jednak je

$$\begin{aligned} G_x &= \{f \in G \,:\, f \,.\, x = x\} \\ &= \{f \in G \,:\, f(x) = x\}. \end{aligned}$$

Drugim riječima, stabilizator G_x se sastoji od onih bijekcija $f : S \to S$ kojima je x fiksna točka. Posebno, takve bijekcije tvore podgrupu grupe G.

8.11. Primjer: djelovanje permutacija. Ako je u prethodnom primjeru skup S konačan onda je grupa bijekcija zapravo simetrična grupa permutacija tog konačnog skupa. Ako S ima n elemenata, možemo uzeti da je jednak

$$X_n = \{1, 2, \ldots, n\}.$$

Na njega djeluje simetrična grupa S_n permutacija od n elemenata na isti način kao grupa bijekcija u prethodnom primjeru. Dakle,

$$\sigma \,.\, k = \sigma(k)$$

za sve $\sigma \in S_n$ i sve $k \in X_n$. Prema prethodnom primjeru, to djelovanje ima jednu orbitu i to cijeli X_n, a stabilizator elementa $k \in X_n$ čine sve permutacije kojima je k fiksna točka.

U poglavlju o primjerima grupa dokazali smo da se svaka permutacija $\sigma \in S_n$ može zapisati kao kompozicija disjunktnih ciklusa i to na jedinstven način do na poredak tih ciklusa. Pritom disjunktni ciklusi komutiraju. Sada kad smo definirali djelovanje grupe na skup, taj dokaz se može elegantnije zapisati.

Naime, u tom dokazu promatramo podgrupu H simetrične grupe S_n generiranu zadanom permutacijom σ. Ako je n_0 red te permutacije σ, onda je

$$H = \langle \sigma \rangle = \{id, \sigma, \sigma^2, \ldots, \sigma^{n_0 - 1}\}.$$

Uvijek kad grupa djeluje na skup, onda istim djelovanjem djeluje i svaka njena podgrupa, jer se svojstva (1) i (2) iz definicije djelovanja očito nasljeđuju. Stoga podgrupa H djeluje na skup X_n formulom

$$\sigma^l \,.\, k = \sigma^l(k)$$

za sve $\sigma^l \in H$ i sve $k \in X_n$.

Orbitu elementa $k \in X_n$ pri tom djelovanju označimo s $[k]$. Ona je, prema definiciji, jednaka

$$\begin{aligned}[k] &= \{\sigma^l \,.\, k \,:\, \sigma^l \in H\} \\ &= \{\sigma^l(k) \,:\, \sigma^l \in H\} \\ &= \{k, \sigma(k), \sigma^2(k), \ldots, \sigma^{n_0-1}(k)\}.\end{aligned}$$

Pri tome u ovom zapisu orbite $[k]$ može biti i ponavljanja. Stoga promotrimo stabilizator H_k elementa k. Budući da je H_k podgrupa cikličke grupe H, ona je također ciklička. To znači da postoji prirodni broj m_0 koji dijeli red n_0 grupe H takav da je

$$H_k = \langle \sigma^{m_0} \rangle = \{id, \sigma^{m_0}, \sigma^{2m_0}, \ldots, \sigma^{(d-1)m_0}\},$$

gdje je d prirodni broj takav da je $n_0 = dm_0$. Kako je $\sigma^{m_0}(k) = k$, jer je $\sigma^{m_0} \in H_k$, slijedi da su međusobno različiti elementi orbite od k upravo

$$[k] = \{k, \sigma(k), \ldots, \sigma^{m_0-1}(k)\}.$$

Sada, na isti način kao u ranijem dokazu, definira se ciklus

$$\sigma_{[k]} = (k, \sigma(k), \ldots, \sigma^{m_0-1}(k)) \in S_n,$$

te se zatim provjerava da ta definicija ne ovisi o odabiru predstavnika orbite, te da je

$$\sigma = \prod_{[k]} \sigma_{[k]},$$

gdje produkt ide po svim orbitama i zapravo predstavlja kompoziciju.

8.12. Djelovanje lijevim translacijama. Neka je G grupa i H njena podgrupa. Neka je najprije $S = G$. Tada definiramo djelovanje grupe H na skup G lijevim translacijama kao

$$h \,.\, x = hx$$

za sve $h \in H$, $x \in G$. Na desnoj strani ove definicije je operacija iz grupe G između elemenata h i x. Može se reći da je ovo djelovanje naprosto množenje s lijeva. Provjerimo da je time zaista definirano djelovanje. Svojstvo (D1) iz definicije djelovanja je očito ispunjeno jer

$$e \,.\, x = ex = x$$

za sve $x \in G$. Svojstvo (D2) se svodi na asocijativnost u grupi G jer

$$h_1 \,.(h_2 \,.\, x) = h_1 \,.(h_2 x) = h_1(h_2 x) = (h_1 h_2)x = (h_1 h_2) \,.\, x$$

za sve $h_1, h_2 \in H$, $x \in G$.

Neka je sada K još jedna podgrupa od G. Neka je $S = G/K$ skup svih lijevih klasa od G obzirom na K. Naglasimo da ovdje K ne mora biti normalna podgrupa od G, već naprosto promatramo skup lijevih klasa koje ne moraju činiti grupu. Tada se djelovanje grupe H lijevim translacijama na S definira formulom

$$h \,.\, xK = hxK$$

za sve $h \in H$, $x \in G$. Opet je na desnoj strani naprosto množenje s lijeva elementom h. Provjerimo da je ovime zaista definirano djelovanje. Svojstvo (D1) opet očito vrijedi jer

$$e \,.\, xK = exK = xK$$

za svaki $x \in G$. Svojstvo (D2) također vrijedi jer

$$h_1 .(h_2 \,.\, xK) = h_1 \,.\, h_2 xK = h_1(h_2 x)K = (h_1 h_2)xK = (h_1 h_2) \,.\, xK$$

za sve $h_1, h_2 \in H$, $x \in G$.

8.13. Napomena o desnim translacijama. Neka je G grupa i H njena podgrupa. Htjeli bismo po uzoru na lijeve definirati desne translacije. Prvi pokušaj bio bi

$$h \,.\, x = xh$$

za sve $h \in H$, $x \in G$. Međutim, ta definicija nije dobra jer ne vrijedi svojstvo (D2). Točnije,

$$h_1 .(h_2 \,.\, x) = h_1 .(xh_2) = xh_2 h_1,$$

dok je

$$(h_1 h_2) \,.\, x = xh_1 h_2,$$

za sve $h_1, h_2 \in H$, $x \in G$. Stoga, osim u slučaju kad je H komutativna, ovo nije djelovanje.

Prava definicija djelovanja desnim translacijama je

$$h \,.\, x = xh^{-1}$$

za sve $h \in H$, $x \in G$. Svojstvo (D2) sada vrijedi jer

$$h_1 .(h_2 \,.\, x) = h_1 .(xh_2^{-1}) = xh_2^{-1}h_1^{-1} = x(h_1 h_2)^{-1} = (h_1 h_2) \,.\, x$$

za sve $h_1, h_2 \in H$, $x \in G$. Svojstvo (D1) je očito.

8.14. Djelovanje konjugiranjem. Neka je G grupa i H njena podgrupa. Najprije neka je skup $S = G$. Tada se djelovanje grupe H na skup S konjugiranjem definira kao

$$h \,.\, x = hxh^{-1}$$

za sve $h \in H$, $x \in G$. Podsjetimo da je izraz na desnoj strani jednak $I_h(x)$, gdje je I_h unutarnji automorfizam grupe G određen elementom h. Pri dokazu da je time doista definirano djelovanje koristimo svojstva unutarnjih automorfizama. Svojstvo (D1) vrijedi jer

$$e \,.\, x = exe^{-1} = x$$

za sve $x \in G$. Svojstvo (D2) vrijedi jer

$$\begin{aligned} h_1 .(h_2 \,.\, x) &= h_1 .(h_2 x h_2^{-1}) = h_1 \,.\, I_{h_2}(x) = h_1 I_{h_2}(x) h_1^{-1} = I_{h_1}(I_{h_2}(x)) \\ &= I_{h_1 h_2}(x) = (h_1 h_2)x(h_1 h_2)^{-1} = (h_1 h_2) \,.\, x \end{aligned}$$

za sve $h_1, h_2 \in H$, $x \in G$.

Neka je i dalje H podgrupa od G. Neka je sada S skup svih podrupa grupe G. Tada se djelovanje grupe H na skup S konjugiranjem definira formulom

$$h \,.\, K = hKh^{-1}$$

za sve $h \in H$ i sve $K \in S$ podgrupe od G. Izraz na desnoj strani jednak je slici unutarnjeg automorfizma I_h primjenjenog na podgrupu K, a to je

$$I_h(K) = \{I_h(k) \,:\, k \in K\}.$$

Time je zaista definirano djelovanje. Naime, (D1) vrijedi očito jer

$$e \,.\, K = eKe^{-1} = K$$

za sve $K \in S$. Svojstvo (D2) dobivamo koristeći svojstva unutarnjih automorfizama jer

$$\begin{aligned} h_1 .(h_2 \,.\, K) &= h_1 .(h_2 K h_2^{-1}) = h_1 \,.\, I_{h_2}(K) = h_1 I_{h_2}(K) h_1^{-1} = I_{h_1}(I_{h_2}(K)) \\ &= I_{h_1 h_2}(K) = (h_1 h_2) K (h_1 h_2)^{-1} = (h_1 h_2) \,.\, K \end{aligned}$$

za sve $h_1, h_2 \in H$, $K \in S$.

8.15. Klasa konjugiranosti elementa, centralizator. Djelovanje konjugiranjem je toliko važno da orbite i stabilizatori imaju posebno ime. U slučaju kad podgrupa H djeluje na skup $S = G$ konjugiranjem, orbite se nazivaju klase H-konjugiranosti elemenata. Tako se orbita elementa $x \in G$ naziva klasa H-konjugiranosti elementa x. Ako je $H = G$, odnosno G djeluje na samu sebe konjugiranjem, onda u nazivu ispustimo grupu i orbite kratko zovemo klase konjugiranosti.

Stabilizator elementa $x \in G$ naziva se centralizator elementa x u grupi H i označava $Z_H(x)$. Prema definiciji stabilizatora

$$\begin{aligned} Z_H(x) &= \{h \in H \,:\, h \,.\, x = x\} \\ &= \{h \in H \,:\, hxh^{-1} = x\} \\ &= \{h \in H \,:\, hx = xh\}. \end{aligned}$$

Dakle, stabilizator od x u H se sastoji od svih onih elemenata iz H koji komutiraju s x. Posebno, ako je $H = G$, onda je

$$Z_G(x) = \{g \in G \,:\, gx = xg\},$$

pa na neki način centralizator mjeri koliko je element x blizu tome da bude u centru $Z(G)$ grupe G. Naime, $x \in Z(G)$ ako i samo x komutira sa svim $g \in G$, a to je ako i samo ako $Z_G(x) = G$.

8.16. Jednadžba klasa konjugiranosti. Uočimo da je, prema općem teoremu koji daje vezu orbite i lijevih klasa stabilizatora, kardinalni broj klase konjugiranosti elementa $x \in G$ jednak indeksu njegovog centralizatora $[G : Z_G(x)]$. Ako je G konačna grupa, to ima za posljedicu formulu

$$|G| = |Z(G)| + \sum_x [G : Z_G(x)],$$

gdje suma ide po elementima x iz skupa koji se sastoji od po jednog predstavnika svake netrivijalne konjugacijske klase. Pritom konjugacijsku klasu zovemo netrivijalnom ako se sastoji od barem dva elementa. Ova formula se obično naziva jednadžba klasa konjugiranosti.

Dokaz ove formule polazi od činjenice da je grupa G disjunktna unija klasa konjugiranosti, obzirom da su orbite općenito klase ekvivalencije. Stoga je red grupe G jednak sumi duljina svojih klasa konjugiranosti. Dakle,

$$|G| = \sum_x |\overline{x}|,$$

gdje suma ide po skupu koji se sastoji od po jednog predstavnika svake klase konjugiranosti, a $|\overline{x}|$ označava duljinu klase konjugiranosti. Prema prethodno navedenoj tvrdnji,

$$|\overline{x}| = [G : Z_G(x)].$$

Podsjetimo da je $x \in Z(G)$ ako i samo ako $Z_G(x) = G$. Međutim, to je ako i samo ako je

$$|\overline{x}| = [G : Z_G(x)] = [G : G] = 1,$$

odnosno ako i samo ako je klasa konjugiranosti od x trivijalna. To znači da ako u gornjem izrazu za $|G|$ preko sume duljina klasa konjugiranosti izdvojimo trivijalne klase, njih ima upravo koliko i elemenata u centru $Z(G)$ i svaka je duljine jedan. Stoga je suma duljina trivijalnih klasa jednaka redu centra $Z(G)$. Preostale klase su netrivijalne i njihove duljine su jednake indeksu centralizatora. Time je formula dokazana.

Kao primjer primjene jednadžbe klasa konjugiranosti dokažimo tvrdnju da svaka grupa G čiji red je jednak potenciji prostog broja ima netrivijalan centar. Neka je $|G| = p^n$, gdje je p prost i n pozitivan cijeli broj. Ako je x predstavnik netrivijalne klase konjugiranosti, onda je indeks $[G : Z_G(x)] > 1$. S druge strane, iz Lagrangeovog teorema znamo da indeks $[G : Z_G(x)]$ dijeli red grupe G, pa slijedi da je $[G : Z_G(x)]$ djelitelj od p^n. Svi djelitelji od p^n veći od jedan su djeljivi s p. Stoga je $[G : Z_G(x)]$ djeljiv s p za svaki predstavnik x netrivijalne klase konjugiranosti. Time smo pokazali da su, u slučaju $|G| = p^n$, svi sumandi u jednadžbi klasa konjugiranosti, osim $|Z(G)|$, djeljivi s p. Tada i $|Z(G)|$ mora biti djeljiv s p. Kako je neutralni element uvijek u centru grupe, $|Z(G)| \geq 1$. Ali kako je $|Z(G)|$ djeljiv s p, dobivamo da je $|Z(G)| \geq p$. Svaki prost broj je veći od jedan, pa smo time dokazali netrivijalnost centra. Ali zapravo smo dokazali i više, a to je da centar u grupi reda p^n ima barem p elemenata.

8.17. Klasa konjugiranosti podgrupe, normalizator. U slučaju kada podgrupa H djeluje konjugiranjem na skup S svih podgrupa grupe G, orbite se zovu klase H-konjugiranosti podgrupa. Tako se orbita podrupe $K \in S$ zove klasa H-konjugiranosti grupe K i sastoji od svih podgrupa oblika hKh^{-1}, gdje je $h \in H$. Ako je $H = G$, onda se grupa ispušta iz naziva i orbite zovu klase konjugiranosti.

Stabilizator podgrupe K naziva se normalizator grupe K u grupi H i označava $N_H(K)$. Iz definicije stabilizatora slijedi da je

$$\begin{aligned} N_H(K) &= \{h \in H \,:\, h\,.\,K = K\} \\ &= \{h \in H \,:\, hKh^{-1} = K\}. \end{aligned}$$

Uvjet $hKh^{-1} = K$ je upravo uvjet normalnosti podgrupe K za element h. Stoga se normalizator podgrupe K u H sastoji od svih onih $h \in H$ za koje je uvjet normalnosti podgrupe K ispunjen. Posebno, ako je $H = G$, onda

$$N_G(K) = \{g \in G \,:\, gKg^{-1} = K\}.$$

To znači da normalizator na neki način mjeri koliko je K blizu tome da bude normalna. U stvari, K je normalna podgrupa od G ako i samo ako je $N_G(K) = G$.

9. Sylowljevi teoremi

9.1. Motivacija. Lagrangeov teorem za konačnu grupu G kaže da je red svake njene podgrupe djelitelj reda čitave grupe. Tako nam Lagrangeov teorem olakšava određivanje svih podgrupa od G jer daje ograničenje na njihov red. Prirodno je postaviti pitanje obrata: ako je d pozitivni djelitelj reda grupe G, postoji li podgrupa reda d?

Cilj Sylowljevih teorema je odgovoriti na to pitanje, ali ne općenito, nego za slučaj kada je d potencija prostog broja. U tom specijalnom slučaju oni daju afirmativan odgovor.

9.2. Osnovna lema. Neka je p prosti broj te H konačna grupa reda p^n za neki pozitivan cijeli broj n. Neka H djeluje na konačan skup S. Tada vrijedi

$$|S| \equiv |S_0| \mod p,$$

gdje je S_0 skup fiksnih točaka djelovanja.

Dokaz. Dokaz je vrlo sličan primjeni jednadžbe klasa konjugiranosti. Naime, kako su orbite klase ekvivalencije, skup S je disjunktna unija orbita. Posebno vrijedi

$$|S| = \sum_x |\overline{x}|$$

gdje suma ide po elementima x skupa koji se sastoji od po jednog predstavnika svake orbite.

Orbitu zovemo trivijalnom ako se sastoji od samo jednog elementa. Takvi elementi su zapravo fiksne točke djelovanja. Stoga, trivijalnih orbita ima $|S_0|$ i sve su duljine jedan. Dakle, ako izdvojimo iz gornje sume trivijalne orbite, suma njihovih duljina je $|S_0|$, pa dobivamo

$$|S| = |S_0| + \sum_x |\overline{x}|,$$

gdje sada suma ide po elementima x iz skupa koji se sastoji od po jednog predstavnika svake netrivijalne orbite.

Na kraju, sjetimo se da općenito vrijedi

$$|\overline{x}| = [G : G_x].$$

Prema Lagrangeovom teoremu taj indeks $[G : G_x]$ dijeli red grupe G. Kako je $|G| = p^n$, za netrivijalne orbite duljina $|\overline{x}|$ je djeljiva s p. To pokazuje da se $|S|$ i S_0 razlikuju za broj djeljiv s p, pa su kongruentni modulo p. □

9.3. Cauchyjev teorem. Neka je p prost broj i G grupa čiji red je djeljiv s p. Tada u grupi G postoji element reda p.

Dokaz. Dokaz ovog teorema bazira se na zgodnoj primjeni prethodne leme. Treba pametno odabrati, kao u lemi, skup S, grupu H i definirati djelovanje grupe H na skup S, na takav način da su u skupu S_0 elementi reda p.

Neka je S skup uređenih p–torki elemenata iz G takvih da je produkt svih elemenata u p–torci neutralni element. Dakle,

$$S = \{(g_1, g_2, \ldots, g_p) \,:\, g_1, g_2, \ldots, g_p \in G,\ g_1 g_2 \ldots g_p = e\}.$$

Broj elemenata u skupu S računamo pomoću teorema o uzastopnom prebrojavanju. Prvi element p–torke iz S može se izabrati na $|G|$ načina jer to može biti bilo koji element grupe G. Nakon toga, drugi element p–torke također možemo izabrati na $|G|$ načina, jer i on može biti bilo koji element grupe G. I sve ostale elemente do predzadnjeg $(p-1)$–ti možemo izabrati na $|G|$ načina. Na kraju, posljednji p–ti element možemo izabrati samo na jedan način jer uvjet $g_1 g_2 \ldots g_p = e$ pokazuje da je g_p jedinstveno određen prethodnim elementima formulom

$$g_p = (g_1 g_2 \ldots g_{p-1})^{-1}.$$

Stoga je

$$|S| = \underbrace{|G| \cdot |G| \cdot \ldots \cdot |G|}_{p-1 \text{ faktor}} \cdot 1 = |G|^{p-1}$$

prema teoremu o uzastopnom prebrojavanju. Kako je $|G|$ djeljiv s p, a p prost pa $p-1 \geq 1$, slijedi da je $|G|^{p-1}$ djeljiv s p. Dakle, $|S|$ je djeljiv s p.

Neka je $H = \mathbb{Z}_p$ grupa (klasa) ostataka modulo p obzirom na operaciju $+_p$ zbrajanja modulo p. To je grupa reda p pa zadovoljava uvjete prethodne leme. Podsjetimo da klasu cijelog broja k označavamo s $[k]$ pri čemu predstavnika klase možemo odabrati iz skupa $\{0, 1, \ldots, p-1\}$. Operacija zbrajanja klasa je definirana s

$$[k] +_p [l] = [k + l]$$

za sve cijele brojeve k i l.

Djelovanje grupe H na skup S definiramo formulom

$$[k] .(g_1, g_2, \ldots, g_p) = (g_{k+1}, g_{k+2}, \ldots, g_p, g_1, g_2, \ldots, g_k)$$

za sve $[k] \in H$, pri čemu je predstavnik $k \in \{0, 1, \ldots, p-1\}$, i sve $(g_1, \ldots, g_p) \in S$. Drugim riječima, prvih k elemenata p–torke prebacimo na kraj. Dokažimo da je time zaista definirano djelovanje. Svojstvo (D1) očito vrijedi jer

$$[0] .(g_1, g_2, \ldots, g_p) = (g_1, g_2, \ldots, g_p)$$

za sve $(g_1, g_2, \ldots, g_p) \in S$. Za svojstvo $(D2)$ uočimo da

$$[k] .([l] .(g_1, g_2, \ldots, g_p))$$

je p–torka koja se dobije prebacivanjem najprije prvih l elemenata na kraj, a zatim u tako dobivenoj p–torki prvih k elemenata na kraj. To znači da smo ukupno $k + l$ elemenata prebacili na kraj. Kako prebacivanje p elemenata na kraj daje ponovo polaznu p–torku, prebacivanje $k + l$ elemenata je isto kao i prebacivanje $k + l$ modulo p elemenata. To je upravo

$$[k + l] .(g_1, g_2, \ldots, g_p).$$

Dakle, vrijedi svojstvo (D2) jer

$$[k] .([l] .(g_1, g_2, \ldots, g_p)) = [k + l] .(g_1, g_2, \ldots, g_p)$$

za sve $[k], [l] \in H$ i sve $(g_1, \ldots, g_p) \in S$.

Odredimo skup S_0 fiksnih točaka tog djelovanja. Uvjet da je $(g_1, \ldots, g_p) \in S_0$ se može pisati u obliku

$$\begin{aligned} [k] .(g_1, g_2, \ldots, g_p) &= (g_1, g_2, \ldots, g_p) \\ (g_{k+1}, g_{k+2}, \ldots, g_p, g_1, g_2, \ldots, g_k) &= (g_1, g_2, \ldots, g_p) \end{aligned}$$

za sve $[k] \in H$, gdje je $k \in \{0, 1, \ldots, p-1\}$. Već uspoređivanjem prvog elementa p–torke dobivamo da je $g_1 = g_{k+1}$ za svaki $k \in \{0, 1, \ldots, p-1\}$, odnosno

$$g_1 = g_2 = \ldots = g_p.$$

Isti uvjet se dobije uspoređivanjem ostalih elemenata p–torke. Dakle, skup fiksnih točaka

$$S_0 = \{\underbrace{(g, g, \ldots, g)}_{p\text{–torka}} : g \in G,\, g^p = e\}$$

ima onoliko elemenata koliko u grupi G ima elemenata g za koje vrijedi $g^p = e$. Uočimo da iz uvjeta $g^p = e$ slijedi da red elementa g dijeli p. Kako je p prost, takav g je ili reda p ili neutralni element koji je uvijek jedini element reda 1. Posebno, S_0 je neprazan jer sigurno sadrži p–torku $(e, e, \ldots, e)$.

Sad primijenimo prethodnu lemu koja kaže da $|S|$ i $|S_0|$ daju isti ostatak pri dijeljenju s p. Kako je $|S|$ djeljivo s p, zaključujemo da je i $|S_0|$ djeljivo s p. Vidjeli smo da je S_0 neprazan, pa mora biti $|S_0| \geq p$. Kako je p prost broj, to znači da S_0 sadrži barem dva elementa. Stoga, osim neutralnog elementa, postoji još barem jedan $g \in G$ takav da je $g^p = e$. Takav g je traženi element reda p. □

9.4. Definicija i kriterij za p–grupe. Neka je p prosti broj. Po definiciji, p–grupa je grupa u kojoj je red svakog elementa potencija od p. Za konačnu grupu G ova definicija se može pojednostaviti. Konačna grupa G je p–grupa ako i samo ako je red grupe G potencija od p.

Da bismo to dokazali, pretpostavimo najprije da je G konačna p–grupa i da prost broj q dijeli red grupe G. Tada, prema Cauchyjevom teoremu, postoji element reda q. Kako je po pretpostavci G p–grupa, slijedi da je $q = p$. Dakle, jedini prost broj koji dijeli red grupe G je p, pa je red grupe G potencija od p. Obrat je očigledan, jer red elementa dijeli red grupe, pa u grupi čiji red je potencija od p, red svakog elementa je potencija od p.

Neka je G grupa i H njena podgrupa. Ako je H p–grupa, onda kažemo da je H p–podgrupa grupe G. Trivijalna podgrupa $\{e\}$ je p–podgrupa za svaki p jer je red neutralnog elementa jednak $p^0 = 1$.

9.5. Lema. Neka je G konačna grupa i H njena p–podgrupa. Tada

$$[G : H] \equiv [N_G(H) : H] \mod p,$$

gdje je $N_G(H)$ normalizator od H u G.

Dokaz. Promatramo djelovanje lijevim translacijama p–podgrupe H na skup $S = G/H$ svih lijevih klasa određenih podgrupom H. Tada je

$$|S| = [G : H].$$

Odredimo skup fiksnih točaka tog djelovanja. Po definiciji fiksne točke vrijedi

$$\begin{aligned} S_0 &= \{gH \in G/H \,:\, h\,.\,gH = gH \text{ za sve } h \in H\} \\ &= \{gH \in G/H \,:\, hgH = gH \text{ za sve } h \in H\} \\ &= \{gH \in G/H \,:\, g^{-1}hgH = H \text{ za sve } h \in H\} \\ &= \{gH \in G/H \,:\, g^{-1}hg \in H \text{ za sve } h \in H\} \\ &= \{gH \in G/H \,:\, g^{-1}Hg \subset H\} \\ &= \{gH \in G/H \,:\, g^{-1} \in N_G(H)\} \\ &= \{gH \in G/H \,:\, g \in N_G(H)\} \\ &= N_G(H)/H. \end{aligned}$$

Stoga je

$$|S_0| = [N_G(H) : H].$$

Sada primjena osnovne leme daje traženu kongruenciju. □

9.6. Prvi Sylowljev teorem. Neka je G konačna grupa reda $p^n \cdot m$, gdje je p prost broj, n i m pozitivni cijeli brojevi, te p ne dijeli m. Tada za svaki $k \in \{1, \ldots, n\}$ postoji podgrupa od G reda p^k, a pri tome je svaka podgrupa reda p^k normalna u nekoj podgrupi reda p^{k+1} za $k \in \{1, \ldots, n-1\}$.

Dokaz. Dokaz provodimo matematičkom indukcijom. Baza indukcije za $k = 1$ je posljedica Cauchyjevog teorema. Naime, on garantira postojanje elementa reda p u grupi G, pa je podgrupa generirana tim elementom reda p.

Neka je k takav da $1 < k \leq n$ i pretpostavimo da postoji podgrupa H_{k-1} grupe G reda p^{k-1}. Uočimo da je tada

$$[G : H_{k-1}] = \frac{|G|}{|H_{k-1}|} = \frac{p^n \cdot m}{p^{k-1}} = p^{n-k+1} \cdot m,$$

pa je taj indeks djeljiv s p jer $n - k + 1 \geq 1$. Neka je $N_G(H_{k-1})$ normalizator od H_{k-1} u grupi G. Prema prethodnoj lemi

$$[N_G(H_{k-1}) : H_{k-1}] \equiv [G : H_{k-1}] \mod p,$$

što znači da p dijeli i indeks $[N_G(H_{k-1}) : H_{k-1}]$. Budući da je svaka podgrupa normalna u svom normalizatoru, može se formirati kvocijentna grupa $N_G(H_{k-1})/H_{k-1}$. Njen red je jednak indeksu $[N_G(H_{k-1}) : H_{k-1}]$, pa je djeljiv s p. Stoga, prema Cauchyjevom teoremu, postoji element reda p u toj kvocijentnoj grupi $N_G(H_{k-1})/H_{k-1}$. Element reda p generira podgrupu reda p u toj kvocijentnoj grupi. Prema opisu podgrupa kvocijentne grupe, postoji jedinstvena podgrupa H_k grupe $N_G(H_{k-1})$, a time i grupe G, takva da je H_k/H_{k-1} ta podgrupa reda p. Posebno, H_{k-1} je normalna podgrupa u H_k. Red podgrupe H_k jednak je

$$|H_k| = |H_k/H_{k-1}| \cdot |H_{k-1}| = p \cdot p^{k-1} = p^k.$$

Dakle, H_k je tražena podgrupa od G reda p^k. Iz koraka indukcije je vidljivo da je H_{k-1} normalna u H_k. □

9.7. Sylowljeva p–podgrupa. Neka je G grupa. Svaka p–podgrupa od G koja nije sadržana u niti jednoj drugoj p–podgrupi od G naziva se Sylowljeva p–podgrupa. U slučaju konačne grupe G reda $p^n \cdot m$, gdje p ne dijeli m, svaka podgrupa reda p^n je Sylowljeva p–podgrupa. Prvi Sylowljev teorem daje obrat. Svaka Sylowljeva p–podgrupa takve grupe G je reda p^n. To je jasno jer je svaka p–podgrupa reda p^k, gdje $k < n$, sadržana u nekoj p–podgrupi reda p^{k+1}, pa ne može biti Sylowljeva.

Drugi i treći Sylowljev teorem govori o Sylowljevim p–podgrupama konačne grupe. Drugi Sylowljev teorem pokazuje da su sve Sylowljeve p–podgrupe konačne grupe konjugirane, a stoga i izomorfne. Treći Sylowljev teorem daje informacije o broju različitih Sylowljevih p–podgrupa konačne grupe (sve su izomorfne, ali ne sastoje se sve od istih elemenata).

9.8. Drugi Sylowljev teorem. Neka je G konačna grupa. Neka je H p–podgrupa od G, a P Sylowljeva p–podgrupa od G. Tada, postoji $x \in G$ takav da vrijedi

$$H \leqslant xPx^{-1}.$$

Posebno, svake dvije Sylowljeve p–podgrupe od G su konjugirane.

Dokaz. Promatramo djelovanje grupe H lijevim translacijama na skup $S = G/P$ lijevih klasa obzirom na podgrupu P. Po definiciji $|S| = [G : P]$, što nije djeljivo s p jer prema prvom Sylowljevom teoremu red od P je najveća potencija od p koja dijeli red grupe G. Prema osnovnoj lemi slijedi da

$$|S_0| \equiv |S| = [G : P] \mod p.$$

Vidjeli smo da p ne dijeli $|S|$, pa p ne dijeli ni $|S_0|$. Posebno $|S_0| \neq 0$, odnosno S_0 je neprazan. Neka je $xP \in S_0$. Po definiciji fiksne točke tada vrijedi

$$hxP = xP \text{ za sve } h \in H.$$

Po definiciji lijevih klasa, x i hx su predstavnici iste klase ako i samo ako su u lijevoj relaciji $x \sim_l hx$, odnosno $x^{-1}hx \in P$. Stoga $xP \in S_0$ ako i samo ako $x^{-1}hx \in P$ za sve $h \in H$, a to znači da je $x^{-1}Hx \leqslant P$. Množenjem elementom x s lijeva te elementom x^{-1} s desna dobivamo traženu tvrdnju $H \leqslant xPx^{-1}$. Sve Sylowljeve podgrupe su konjugirane jer sve imaju jednak broj elemenata po prvom Sylowljevom teoremu, pa ne može konjugat jedne biti prava podgrupa drugoj. □

9.9. Treći Sylowljev teorem. Neka je G konačna grupa i p prost broj. Tada je broj različitih Sylowljevih p–podgrupa od G djelitelj reda grupe G i oblika $kp + 1$ za neki nenegativan cijeli broj k.

Dokaz. Promatramo djelovanje grupe G konjugiranjem na skup S svih podgrupa od G. Budući da drugi Sylowljev teorem pokazuje da su sve Sylowljeve p–podgrupe konjugirane, one su sve u istoj orbiti tog djelovanja. S druge strane, svaka podgrupa koje je konjugirana, a time i izomorfna, Sylowljevoj mora i sama biti Sylowljeva. Dakle, jednu orbitu djelovanja tvore upravo Sylowljeve p–podgrupe. Kako je općenito duljina orbite jednaka indeksu stabilizatora u G nekog njenog elementa, zaključujemo da duljina orbite dijeli red grupe $|G|$ jer indeks podgrupe uvijek dijeli red grupe po Lagrangeovom teoremu. Ali duljina orbite Sylowljevih p–podgrupa je upravo njihov broj, pa je time dokazana prva tvrdnja teorema.

Za drugu tvrdnju, neka je P jedna Sylowljeva podgrupa od G, a S skup svih Sylowljevih podgrupa od G. Promatramo djelovanje grupe P na skup S konjugiranjem. Odredimo skup S_0 fiksnih točaka tog djelovanja. Po definiciji

$$\begin{aligned} S_0 &= \{Q \in S : x \,.\, Q = Q \text{ za sve } x \in P\} \\ &= \{Q \in S : xQx^{-1} = Q \text{ za sve } x \in P\}. \end{aligned}$$

Uvjet $xQx^{-1} = Q$ je uvjet iz definicije normalizatora. Stoga je ispunjen za svaki $x \in P$, ako i samo ako je grupa P podgrupa normalizatora $N_G(Q)$. Dakle,

$$S_0 = \{Q \in S : P \leqslant N_G(Q)\}.$$

S druge strane, Q je normalna podgrupa u svom normalizatoru $N_G(Q)$. Budući da su P i Q Sylowljeve p–podgrupe u G, one su također Sylowljeve p–podgrupe u svakoj podgrupi od G koja ih sadrži. To vrijedi jer je njihov red najveća potencija od p s kojom je djeljiv red grupe. Dakle, P i Q su Sylowljeve p–podgrupe u $N_G(Q)$. Kao takve moraju biti konjugirane unutar $N_G(Q)$ po drugom Sylowljevom teoremu, pa postoji $x \in N_G(Q)$ takav da je $P = xQx^{-1}$. Ali x je iz normalizatora od Q pa vrijedi $xQx^{-1} = Q$. Stoga je $P = Q$. Time smo dokazali da je

$$S_0 = \{P\}.$$

Sada primjenimo osnovnu lemu na ovo djelovanje. Dobivamo da je

$$|S| \equiv |S_0| = 1 \mod p.$$

Skup S je upravo skup Sylowljevih p–podgrupa, pa smo time dokazali da je njihov broj kongruentan 1 modulo p, a to je upravo druga tvrdnja teorema. □