Normalne podgrupe i kvocijentne grupe

Brzić, Lucija

Master's thesis / Diplomski rad

2023

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, School of Applied Mathematics and Informatics / Sveučilište Josipa Jurja Strossmayera u Osijeku, Fakultet primijenjene matematike i informatike**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:126:516704

Sveučilište J.J. Strossmayera u Osijeku
Fakultet primijenjene matematike i informatike
Sveučilišni diplomski studij matematike
Smjer: Financijska matematika i statistika

Lucija Brzić

Normalne podgrupe i kvocijentne grupe

Diplomski rad

Osijek, 2023.

Sveučilište J.J. Strossmayera u Osijeku
Fakultet primijenjene matematike i informatike
Sveučilišni diplomski studij matematike
Smjer: Financijska matematika i statistika

Lucija Brzić

Normalne podgrupe i kvocijentne grupe

Diplomski rad

Mentor: prof.dr.sc. Ivan Matić

Sumentorica: dr.sc. Darija Brajković Zorić

Osijek, 2023.

Sadržaj

Uvod **1**

1 Osnovne algebarske strukture **2**
1.1 Grupa 2
1.2 Podgrupa 6

2 Normalne podgrupe **12**

3 Kvocijentne grupe **22**

Literatura **31**

Sažetak **32**

Summary **33**

Životopis **34**

Uvod

Matematika čini temelj za razumijevanje i analizu različitih fenomena te se koristi u svim znanstvenim i tehničkim disciplinama. U svijetu apstraktnih struktura, algebra se ističe kao grana matematike koja omogućuje duboko razumijevanje matematičkih koncepata i njihovih međuodnosa. Bez obzira na područje matematike - analizu, geometriju, teoriju brojeva ili druge discipline - algebra se pokazuje nezamjenjivom. Ova grana matematike ima duboke korijene koji sežu od antičkih Babilonaca, a poručavali su je Grci, Egipćani, Kinezi i Perzijanci. No, kao samostalna grana matematike, algebra se pojavljuje u Europi tek krajem 16. stoljeća. Jedan od ključnih koncepta moderne algebre je teorija grupa koja se primjenjuje u svim njezinim aspektima. Grupa predstavlja središnju točku moderne algebre. Njezin apstraktan karakter omogućuje da se promatraju mnogi specifični primjeri, a u svom osnovnom obliku, grupa je skup elemenata koji se mogu kombinirati kroz neku operaciju, poput zbrajanja ili množenja, podložnih određenim pravilima. Iako se elementi grupe često shvaćaju kao brojevi, grupa omogućuje apstraktnu analizu i primjenu na različitim matematičkim strukturama. Prva istraživanja grupa pojavljuju se u znanstvenim radovima J.L. Lagrangea krajem 18.-tog stoljeća.

U ovom diplomskom radu usredotočujemo se na proučavanje normalnih podgrupa i kvocijentnih grupa. Normalne podgrupe igraju ključnu ulogu u teoriji grupa, koriste se za konstrukciju kvocijentnih grupa i predstavljaju važan alat za analizu struktura grupa i njihovih svojstava. Kvocijentne grupe, pak, predstavljaju još jedan način dobivanja manje grupe. Kao kod normalnih podgrupa, kvocijentne grupe će nam omogućiti proučavanje i razumijevanje strukture grupe.

Cilj ovog rada je pružiti jasno i sustavno razumijevanje normalnih podgrupa i kvocijentnih grupa, te njihovih međusobnih odnosa kroz primjere, definicije i dokaze ključnih teorema. Ukratko ćemo opisati sadržaj ovog rada.

Prvo poglavlje obuhvaća fundametnalne definicije grupoida, polugrupe, monoida, grupe i podgrupe. U drugom poglavlju uvodi se pojam normalne podgrupe te se navode važne leme i teoremi poput Lagrangeovog teorema. Posljednje poglavlje opisuje kvocijentne grupe i izrazito bitan Prvi teorem o izmorfizmu.

1 Osnovne algebarske strukture

Krenut ćemo s uvodom u osnovne algebarske strukture, koje će nam poslužiti kao temelj za daljnje konstrukcije.

1.1 Grupa

Definicija 1. *Neka je G neprazan skup. Svako preslikavanje iz Kartezijevog produkta $G \times G$ u skup G naziva se binarna operacija na skupu G.*

U nastavku ćemo navesti nekoliko različitih notacija za binarnu operaciju, a za početak označimo ju sa $*$. Dakle, binarna operacija je preslikavanje

$$*\colon G \times G \to G.$$

Na uređenom paru $(a, b) \in G \times G$ vrijednost binarne operacije $*$ označavat ćemo s $a * b$ te je po definiciji to također element iz G. Stoga kažemo da je skup G zatvoren s obzirom na binarnu operaciju $*$.

Definicija 2. *Grupoid se sastoji od nepraznog skupa G zajedno sa zadanom binarnom operacijom $*$. Grupoid označavamo kao uređeni par $(G, *)$.*

Primijetimo da uvijek zahtijevamo da algebarske strukture budu neprazne. To ćemo označavati na sljedeći način $G \neq \emptyset$. Kod definiranja binarnih operacija koristimo različite načine zapisivanja ili notacija:

1. $(a, b) \mapsto a \cdot b$ ili jednostavnije $(a, b) \mapsto ab$ (multiplikativna notacija)
   (čitamo: produkt elemenata a i b iz G)

2. $(a, b) \mapsto a + b$ (aditivna notacija)
   (čitamo: suma elmenata a i b iz G).

   Neke specifične notacije:

3. $(a, b) \mapsto a^b$ (eksponencijalna notacija koja se koristi za potenciranje).

4. $(a, b) \mapsto a \cdot_G b$ (posebna notacija množenja kada želimo naglasiti u kojem skupu promatramo).

Primjer 1. *Neki od primjera grupoida su uređeni parovi $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Z}, -)$. Primjer uređenog para koji ne predstavlja grupoid je $(\mathbb{N}, -)$. Taj uređeni par nije grupoid zbog toga što razlika dva prirodna broja ne mora biti prirodan broj, npr. $3 - 5 = -2 \notin \mathbb{N}$.*

Neka je uređeni par $(G, *)$ grupoid. Ako su $a, b, c \in G$, onda možemo formirati njihov produkt na dva načina: $(a * b) * c$ i $a * (b * c)$. Ako je $(a * b) * c = a * (b * c)$ za sve $a, b, c \in G$, tada kažemo da je binarna operacija $*$ asocijativna.
Radi jednostavnosti zapisa, uređeni par $(G, \cdot)$ koji je grupoid označavat ćemo samo s G. Podrazumijeva se da se koristi multiplikativna notacija.

Definicija 3. *Grupoid G u kojem je binarna operacija asocijativna zove se polugrupa, odnosno za sve $a, b, c \in G$ vrijedi $(ab)c = a(bc)$.*

Primjer 2. *Iz prethodnog primjera možemo zaključiti da su grupoidi $(\mathbb{N}, +)$ i $(\mathbb{Z}, +)$ polugrupe, dok uređeni par $(\mathbb{N}, -)$ nije grupoid pa onda nije ni polugrupa. Primjer grupoida koji nije polugrupa je uređeni par $(\mathbb{Z}, -)$ jer ne zadovoljava svojstvo asocijativnosti za $c \neq 0$.*

U grupoidu G lijeva jedinica se definira kao svaki element $e_L \in G$ koji zadovoljava svojstvo da je $e_L a = a, \forall a \in G$. Slično, u grupoidu G desna jedinica je svaki element $e_R \in G$ koji zadovoljava svojstvo da je $ae_R = a, \forall a \in G$.

Definicija 4. *Neka je G grupoid. Ako postoji element $e \in G$ takav da je*

$$ea = a = ae, \forall a \in G,$$

onda e zovemo obostrana jedinica grupoida G.

Ovisno o kontekstu koriste se određene oznake za obostranu jedinicu: e ili 1 (u slučaju multiplikativne notacije) kojeg još nazivamo neutralni element ili kraće jedinica grupoida G te 0 (u slučaju aditivne notacije), pri čemu se taj neutralni element obično naziva nula u grupoidu G. Ukoliko se istovremeno promatraju drugi grupoidi, radi preciznosti, koriste se oznake $e_G, 1_G$ i 0_G.

Definicija 5. *Monoid je polugrupa G koja sadrži jedinicu.*

Iz navedene definicije vidimo da ako je skup G monoid, onda je on uvijek neprazan skup jer sadrži neutralni element.

Primjer 3. *Monoidi s neutralnim elementom 1 su polugrupe $(\mathbb{N}, \cdot), (\{-1, 1\}, \cdot)$. Monoid s neutralnim elementom 0 je polugrupa $(\mathbb{Z}, +)$. Primjer polugrupe koja nije monoid je $(\mathbb{N}, +)$ jer $0 \notin \mathbb{N}$, ali možemo doći do monoida definiranjem nove polugrupe oblika $(\mathbb{N} \cup \{0\}, +)$*

Neka je G monoid s jedinicom e i neka je $a \in G$. Element $b \in G$ naziva se lijevim inverzom elementa a ako je $ba = e$ dok je element $c \in G$ desni inverz elementa a ako je $ac = e$.

Definicija 6. *Neka je G monoid s jedinicom e i neka je $a \in G$. Ako postoji element $b \in G$ takav da je*

$$ba = e = ab,$$

onda b nazivamo obostrani inverz elementa a.

U pravilu izostavljamo izraz "obostrani". Oznaka za inverz elementa a prilikom korištenja multiplikativne notacije je a^{-1} dok prilikom primjene aditivne notacije oznaka za inverz elementa a je $-a$. Također, umjesto izraza $a + (-b)$, često koristimo kraći zapis $a - b$.

Definicija 7. *Ako element a monoida G ima inverz, onda kažemo da je on invertibilan, odnosno ako postoji $a^{-1} \in G$ takav da je $aa^{-1} = a^{-1}a = e$, pri čemu je e jedinica u G.*

Neka je G monoid. Označimo s G^* skup svih elemenata monoida G koji su invertibilni.

Definicija 8. *Grupa je monoid G u kojem je svaki element invertibilan i zadovoljena su sljedeća svojstva (aksiomi grupe):*

1. *Zatvorenost: $\forall a, b \in G$ vrijedi $ab \in G$.*
2. *Asocijativnost: $\forall a, b, c \in G$ vrijedi $a(bc) = (ab)c$.*
3. *Postojanje neutralnog elementa: $\exists e \in G$ takav da vrijedi $ea{=}ae{=}a$, $\forall a \in G$.*
4. *Postojanje inverznog elementa: $\forall a \in G$, $\exists a^{-1} \in G$ takav da vrijedi $aa^{-1} = a^{-1}a = e$.*

Primjer 4. *Navedimo neke primjere grupe. Monoid $(\mathbb{Z}, +)$ je grupa i zovemo ga aditivna grupa cijelih brojeva, također $(\mathbb{Q}, +)$ je aditivna grupa racionalnih brojeva i $(\mathbb{R}, +)$ je aditivna grupa realnih brojeva. Monoidi $(\{-1, 1\}, \cdot)$, $(\{1\}, \cdot)$, $(\{0\}, +)$ su također grupe jer zadovoljavaju aksiome grupe.*
Postoje monoidi koji nisu grupe, a neki od njih su $(\mathbb{N}, \cdot)$ jer je $\mathbb{N}^* = \{1\}$, odnosno svi brojevi osim 1 u skupu prirodnih brojeva nemaju inverzni element uz množenje. Idući primjer je monoid $(\mathbb{Z}, \cdot)$ koji nije grupa jer je $\mathbb{Z}^* = \{-1, 1\}$.

Teorem 1. ([7, Chapter I: Groups, Theorem 1.2.]) *Ako je G monoid, tada je neutralni element e jedinstven. Ako je G grupa, tada vrijede sljedeće tvrdnje:*

i) Ako je $c \in G$ i $cc = c$, onda je $c = e$.

ii) Za sve $a, b, c \in G$, $ac = bc \Rightarrow a = b$ i $ca = cb \Rightarrow a = b$. Ovo svojstvo se naziva pravilo poništavanja s desna i s lijeva.

iii) Za svaki $a \in G$, inverzni element a^{-1} je jedinstven.

iv) Za svaki $a \in G$ vrijedi $(a^{-1})^{-1} = a$.

v) Za $a, b \in G$ vrijedi $(ab)^{-1} = b^{-1}a^{-1}$.

Dokaz. Ako postoji obostrani neutralni element e', tada vrijedi:

$$e = ee' = e'.$$

Ovo pokazuje da je neutralni element e jednak obostrano neutralnom elementu e'.

i) Neka je $cc = c$, $c \in G$. Pomnožimo obje strane jednakosti s c^{-1} slijeva te dobivamo $c^{-1}(cc) = c^{-1}c$. Sada primjenimo svojstvo asocijativnosti, $(c^{-1}c)c = c^{-1}c$. Iz definicije inverznog elementa dolazimo do $ec = e$, a budući da e predstavlja neutralni element, dokazujemo da je $c = e$.

ii) U prvom slučaju pomnožimo obje strane jednakosti s c^{-1} zdesna te iskoristimo asocijativnost. Dolazimo do zapisa oblika $a(cc^{-1}) = b(cc^{-1})$, gdje primjenjujemo definiciju neutralnog elementa i dobivamo da je $a = b$. Analogno se dokazuje i drugi slučaj tvrdnje pri čemu svaku stranu jednakosti pomnožimo slijeva s c^{-1}.

iii) Da bismo dokazali da je $\forall a \in G$, inverzni element jedinstven pretpostavit ćemo suprotno, tj. da postoje dva inverzna elementa a^{-1} i b^{-1} za isti element $a \in G$. Zbog pretpostavke važi: $aa^{-1} = e$ i $ab^{-1} = e$. Sada pomnožimo drugu jednakost s a^{-1} slijeva: $a^{-1}(ab^{-1}) = a^{-1}e$, odnosno $a^{-1}(ab^{-1}) = a^{-1}(aa^{-1})$. Koristeći svojstvo asocijativnosti dobivamo $(a^{-1}a)b^{-1} = (a^{-1}a)a^{-1}$, te po definiciji inverznog elementa slijedi: $eb^{-1} = ea^{-1}$. Budući da je e neutralan element dobivamo $b^{-1} = a^{-1}$.

iv) Želimo dokazati da $\forall a \in G$ vrijedi $(a^{-1})^{-1} = a$, koristeći svojstva inverznih elmenata. Prema definiciji inverznog elementa, $\forall a \in G$, a^{-1} je inverzni element od a ako vrijedi: $aa^{-1} = e$ i $a^{-1}a = e$. Sada razmotrimo inverzni element $(a^{-1})^{-1}$ koji je inverz od a^{-1}, stoga vrijedi: $a^{-1}(a^{-1})^{-1} = e$ i $(a^{-1})^{-1}a^{-1} = e$. Pomnožimo prvu jednakost s a s lijeve strane te dobivamo $a(a^{-1}(a^{-1})^{-1}) = ae$, iskoristimo asocijativnost i dolazimo do $(aa^{-1})(a^{-1})^{-1} = a$. Kako je $aa^{-1} = e$, a množenje s neutralnim elementom ne mijenja ništa, dobivamo: $(a^{-1})^{-1} = a$. Dakle, $\forall a \in G$ vrijedi $(a^{-1})^{-1} = a$.

v) Budući da su $a, b \in G$, a G je grupa, onda je i $ab \in G$. Također ti elementi iz grupe G posjeduju svoje inverzne elemente: $a^{-1}, b^{-1}, (ab)^{-1} \in G$. Važi da je $(ab)(ab)^{-1} = e$ i $(ab)^{-1}(ab) = e$. Na prvu jednakost primjenimo svojstvo asocijativnosti i pomnožimo s a^{-1} s lijeve strane te dobivamo $a^{-1}a(b(ab)^{-1}) = a^{-1}e$. Nadalje, kako je $a^{-1}a = e$, a e je neutralan element slijedi: $b(ab)^{-1} = a^{-1}$. To pomnožimo slijeva s b^{-1} i lako dobijemo traženu tvrdnju.

□

Binarna operacija $*$ je komutativna na skupu G ako za svaki $a, b \in G$ vrijedi $a * b = b * a$.

Definicija 9. *Za grupoid, polugrupu, monoid ili grupu G kažemo da su komutativni ako je binarna operacija na G komutativna, tj. $\forall a, b \in G$ vrijedi $ab = ba$.*

Tada govorimo o komutativnom grupoidu, polugrupi, monoidu i grupi. Komutativna grupa još se naziva i Abelova grupa. Ime je dobila po Nielsu Henriku Abelu, norveškom matematičaru. Postoje i grupe koje nisu komutativne, a njih nazivamo nekomutativne ili ne-Abelove grupe.

Definicija 10. *Broj elemenata skupa G (kardinalni broj) nazivamo red grupe G i označavamo s $|G|$. Kažemo da je grupa G konačnog reda ili konačna ako je skup G konačan. Za grupu koja nije konačna kažemo da je beskonačna.*

Definicija 11. *Neka je G grupa i $a \in G$. Ako postoji $n \in \mathbb{N}$ takav da vrijedi $a^n = e$, onda se takav najmanji n zove red elementa a. Ukoliko takav n ne postoji, tada je red elementa a beskonačan.*

Često se koriste sljedeće činjenice o redu elemenata: jedini element reda 1 je uvijek neutralni element, te element a i njegov inverz a^{-1} uvijek su istog reda.

Primjer 5. *U Primjeru 4 naveli smo grupe $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ koje su beskonačne i Abelove. Nakon definiranja Abelove grupe i grupe konačnoga reda, navedimo još neke primjere.*

- *Grupa $(\{-1, 1\}, \cdot)$ je konačna Abelova grupa reda 2.*

- *Neka je $n \in \mathbb{N}$ i označimo s $M_n(\mathbb{R})$ skup svih kvadratnih $n \times n$ matrica s elementima iz $\mathbb{R}$. U monoidu $(M_n(\mathbb{R}), +)$ neutralni element je nul-matrica, a inverzni element matrice $A \in M_n(\mathbb{R})$ je matrica $-A$. Monoid $(M_n(\mathbb{R}), +)$ je beskonačna Abelova grupa. S obzirom na množenje matrica skup $M_n(\mathbb{R})$ je monoid. Raspišimo to malo: neka su $A, B \in M_n(\mathbb{R})$. Tada je prema samoj definiciji množenja i produkt $AB \in M_n(\mathbb{R})$ jer elementi produkta ostaju u $\mathbb{R}$. Dakle, zadovoljeno je svojstvo zatvorenosti s obzirom na množenje. Asocijativnost množenja matrica također vrijedi. Jedinična matrica I_n neutralni je element za množenje matrica. Jedinična matrica na glavnoj dijagonali ima jedinice dok su svi ostali elementi jednaki nula. Time smo zadovoljili svojstva da uređeni par $(M_n(\mathbb{R}), \cdot)$ bude monoid, no on nije grupa jer za nul-matricu ne postoji inverzna matrica. Osim toga, za $n \geq 2$ promjena redoslijeda množenja matrica ne daje isti rezultat, odnosno ovaj monoid nije komutativan. Lako je pronaći matrice koje ne komutiraju. Neka su $A, B \in M_2(\mathbb{R})$:*

$$AB = \begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 2 \\ 0 & 2 \end{bmatrix} = \begin{bmatrix} 2 & 6 \\ 0 & 2 \end{bmatrix}$$

$$BA = \begin{bmatrix} 1 & 2 \\ 0 & 2 \end{bmatrix} \cdot \begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 2 & 3 \\ 0 & 2 \end{bmatrix}$$

- *Označimo s $GL_n(\mathbb{R})$ skup svih regularnih matrica u $M_n(\mathbb{R})$ (regularna matrica je matrica kojoj je determinanta različita od 0), $GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \colon detA \neq 0\}$. Uređeni par $(GL_n(\mathbb{R}), \cdot)$ je grupa, koja je nekomutativna za $n \geq 2$ te je nazivamo opća linearna grupa.*

- *Uvedimo još jedan skup: $SL_n(\mathbb{R}) = \{A \in GL_n(\mathbb{R}) \colon detA = 1\}$. Uređeni par $(SL_n(\mathbb{R}), \cdot)$ je grupa. Za $A, B \in SL_n(\mathbb{R})$ vrijedi $det(AB) = (detA)(detB) = 1, AB \in M_n(\mathbb{R})$, iz čega slijedi da je $AB \in SL_n(\mathbb{R})$, te je time pokazana zatvorenost. Asocijativnost također vrijedi. Neutralni element za množenje matrica je jedinična matrica I_n i očito je $det(I_n) = 1$, pa je stoga $I_n \in SL_n(\mathbb{R})$. Nadalje i A^{-1} je element iz $SL_n(\mathbb{R})$ jer vrijedi $det(A^{-1}) = (detA)^{-1} = 1$ i $A^{-1} \in M_n(\mathbb{R})$. Skup $SL_n(\mathbb{R})$ zovemo specijalna linearna grupa, a za $n \geq 2$ ova grupa je nekomutativna.*

1.2 Podgrupa

Jedan od osnovnih načina istraživanja strukture matematičkih objekata koji su definirani skupom aksioma je proučavanje podskupova tih objekata koji također zadovoljavaju iste aksiome. U ovom potpoglavlju razmotrit ćemo podgrupe grupe.

Definicija 12. *Neka je G grupa i $H \subseteq G$. Neprazan skup H zove se podgrupa grupe G ako je H grupa s obzirom na istu binarnu operaciju kao i G. Pišemo $H \leq G$ (čitamo: H je podgrupa od G). Ako je $H \neq G$ i $H \leq G$, onda kažemo da je H prava podgrupa od G i pišemo $H < G$.*

Kada kažemo da je H podgrupa od G, uvijek podrazumijevamo da je operacija za grupu H ista operacija kao i za grupu G (općenito je moguće da podskup H ima strukturu grupe s nekom drugom operacijom osim operacije na G).
Iz prethodne definicije proizlazi da podgrupa H ispunjava zatvorenost u odnosu na operaciju množenja i zatvorenost s obzirom na postojanje inverznog elementa. Drugim riječima, $\forall a, b \in H$ je i umnožak $ab \in H$ te je inverz a^{-1} također u H.

Napomena 1. ([10, Osnovne algebarske strukture]) *Ako je G grupa, tada su G i $\{e\}$ (e je neutralni element u G) podgrupe od G. Dakle, svaka grupa predstavlja svoju vlastitu podgrupu. Te podgrupe nazivamo trivijalne.*

Lako se primjećuje da neutralni element podgrupe mora biti isti kao i neutralni element grupe, odnosno $e_H = e_G$.

Primjer 6. *Navedimo nekoliko primjera podgrupe:*

- *$\mathbb{Z} \leq \mathbb{Q}$ i $\mathbb{Q} \leq \mathbb{R}$ s operacijom zbrajanja. Relacija "biti podgrupa" je tranzitivna: ako je H podgrupa grupe K i K je podgrupa grupe G, tada je H također podgrupa grupe G. U našem primjeru onda slijedi da je $\mathbb{Z} \leq \mathbb{R}$.*
- *Skup parnih cijelih brojeva je podgrupa grupe svih cijelih brojeva u odnosu na zbrajanje.*
- *Neka je $n \in \mathbb{N}$ te definiramo $n\mathbb{Z} = \{nx \colon x \in \mathbb{Z}\}$ što predstavlja skup svih višekratnika od n. Uređeni par $(n\mathbb{Z}, +)$ zadovoljava svojstva grupe i $n\mathbb{Z} \subseteq \mathbb{Z}$, iz čega slijedi $n\mathbb{Z} \leq \mathbb{Z}$.*

Navedimo još primjer skupa koji nije podgrupa:

- *$\mathbb{Z}^+$ u odnosu na zbrajanje nije podgrupa od $\mathbb{Z}$ u odnosu na zbrajanje. Uviđamo da je $\mathbb{Z}^+ \subseteq \mathbb{Z}$, ali ne sadrži neutralan element 0 za zbrajanje, niti inverzan element za svaki element iz $\mathbb{Z}^+$.*

Čak i za jednostavne primjere, provjera ispunjavanja svih aksioma grupe za bilo koju zadanu binarnu operaciju može biti zamorna. Međutim, kada znamo da imamo grupu, provjera je li neki njezin podskup (ili nije) podgrupa znatno je lakši zadatak jer samo treba provjeriti zatvorenost u odnosu na množenje i postojanje inverza. Sljedeći teorem pokazuje mogućnost kombiniranja ovih provjera u jedno što pruža kriterij za određivanje postojanja podgrupe, odnosno kriterij za egzistenciju podgrupe.

Teorem 2. ([7, Chapter I: Groups, Theorem 2.5.]) *Neka je G grupa i $H \subseteq G$, $H \neq \emptyset$. H je podgrupa od G ako i samo ako je*

$$ab^{-1} \in H, \forall a, b \in H. \tag{1.1}$$

Dokaz. Neka je G grupa i $H \subseteq G$, $H \neq \emptyset$. Pokažimo nužnost: ako je $H \leq G$, onda je po definiciji H grupa, odnosno H je zatvoren na množenje i invertiranje. To znači da za sve $a, b \in G$ vrijedi $b^{-1} \in H$ i $ab^{-1} \in H$. Time je dokazana nužnost.
S druge strane, pretpostavimo da vrijedi $ab^{-1} \in H, \forall a, b \in H$. Budući da je $H \neq \emptyset$, onda postoji $a \in H$. Ako uzmemo $a = b$ i primijenimo svojstvo (1.1), slijedi $aa^{-1} = e \in H$ te zaključujemo da H sadrži neutralni element. Nadalje, uzmemo li da je $a = e$, onda na svaki $b \in H$ primijenimo (1.1) te vrijedi $eb^{-1} = b^{-1} \in H$. Skup H je zatvoren i na postojanje inverza. Još pokažimo zatvorenost na množenje. Za $a, b \in H$ i zbog toga što smo sada pokazali da je $b^{-1} \in H$, vrijedi $ab = a(b^{-1})^{-1} \in H$. U konačnici, recimo nešto o asocijativnosti. Kako je navedeno da je $H \subseteq G$, a G je grupa i vrijedi asocijativnost, onda je i binarna operacija u H asocijativna. Iz pokazanog slijedi da je H grupa i H je podgrupa od G. □

Nakon ovog teorema navedimo primjere u kojima ćemo iskoristiti svojstvo (1.1).

Primjer 7. *Pogledajmo:*

- *Već smo naveli kako je skup* $n\mathbb{Z} = \{nx \colon x \in \mathbb{Z}\}$, $n \in \mathbb{N}$, *podgrupa od* $\mathbb{Z}$, *a sada to i pokažimo koristeći Teorem 2. Skup* $n\mathbb{Z}$ *je neprazan podskup skupa* $\mathbb{Z}$. *Nadalje, neka su* $a, b \in n\mathbb{Z}$. *Iz definicije skupa slijedi:* $a = nx, b = ny$ *za neke* $x, y \in \mathbb{Z}$. *Postoji inverz od* b *i definiran je kao* $-b = -ny$. *Kako se radi o skupu* $n\mathbb{Z}$ *zajedno s aditivnom operacijom, primjenom svojstva (1.1) dobije se:*

$$a + (-b) = a - b = nx - ny = n(x - y) \in n\mathbb{Z}$$

  jer je $x - y \in \mathbb{Z}$. *Time je zadovoljen Teorem 2 te je* $n\mathbb{Z} \leq \mathbb{Z}$.

- ([2, 1.2 Podgrupe, Zadatak 1.2.2.]) *Pokažimo da je* $SL_n(\mathbb{R})$ *podgrupa od* $GL_n(\mathbb{R})$. *Za skup* $SL_n(\mathbb{R})$ *znamo da je neprazan skup jer je naprimjer,* $I_n \in SL_n(\mathbb{R})$, *a iz definicije skupova* $SL_n(\mathbb{R})$ *i* $GL_n(\mathbb{R})$ *slijedi da je skup* $SL_n(\mathbb{R}) \subseteq GL_n(\mathbb{R})$. *Sada uzmimo proizvoljne matrice* $A, B \in SL_n(\mathbb{R})$. *Prema tome,* $detA = 1$ *i* $detB = 1$ *pa je onda*

$$det(AB^{-1}) = (detA)(detB^{-1}) = (detA)(detB)^{-1} = 1$$

  i $AB^{-1} \in M_n(\mathbb{R})$, *iz čega slijedi* $AB^{-1} \in SL_n(\mathbb{R})$ *te je* $SL_n(\mathbb{R}) \leq GL_n(\mathbb{R})$.

Napomena 2. *Ako je* G *Abelova grupa i* $H \leq G$ *tada je i* H *Abelova grupa. Obrat ne mora vrijediti.*

Teorem 3. ([6, 2.7. Podgrupa, Teorem 5.]) *Neka je* G *grupa te neka je* $H_1 \leq G$ *i* $H_2 \leq G$. *Onda je* $H_1 \cap H_2$ *također podgrupa od* G.

Dokaz. Uočimo da je $H_1 \cap H_2$ neprazan podskup skupa G. Treba pokazati da vrijedi (1.1), tj. da za $a, b \in H_1 \cap H_2$ vrijedi $ab^{-1} \in H_1 \cap H_2$.
Neka je $a, b \in H_1 \cap H_2$ bilo koji par elemenata. Iz pretpostavke slijedi da su $a, b \in H_1$, pa je onda i $ab^{-1} \in H_1$, jer je H_1 grupa. Također, kako su $a, b \in H_2$, slijedi da je $ab^{-1} \in H_2$, jer je H_2 isto grupa. Dobivamo da je $ab^{-1} \in H_1 \cap H_2$ što je trebalo dokazati. □

Korolar 1. ([7, Chapter I: Groups, Corollary 2.6.]) *Neka je* G *grupa i neka je* $\{H_i \colon i \in I\}$ *neprazna familija podgrupa od* G, *gdje je* I *proizvoljan skup indeksa. Tada je presjek*

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

također podgrupa grupe G.

Naglasimo da unija podgrupa grupe G ne mora biti podgrupa od G.
U apstraktnoj teoriji grupa, zanimaju nas svojstva koja proizlaze iz strukture definirane binarnom operacijom unutar grupe. Ova svojstva ne ovise o prirodi elemenata ili karakteru operacije. Istražimo preslikavanja između grupa koja čuvaju svojstva binarnih operacija.

Definicija 13. *Neka su* $(G_1, \cdot_1)$ *i* $(G_2, \cdot_2)$ *grupe. Preslikavanje* $\varphi \colon G_1 \to G_2$ *nazivamo homomorfizam grupa ako* $\forall a, b \in G_1$ *vrijedi*

$$\varphi(a \cdot_1 b) = \varphi(a) \cdot_2 \varphi(b). \tag{1.2}$$

Govoreći jednostavno, slika funkcije φ po operaciji $\cdot_1$ primijenjena na dva elementa iz G_1 jednaka je operaciji $\cdot_2$ iz G_2 primijenjenoj na slike tih dvaju elemenata. Zaključujemo da homomorfizam čuva strukturu grupa. Označimo s $Hom(G_1, G_2)$ skup svih homomorfizama s G_1u G_2.
Ako podrazumijevamo o kojim se binarnim operacijama radi, zapis (1.2) možemo pisati jednostavnije $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

Navedimo još neke posebne pojmove vezane uz homomorfizam grupa:

- Ako je φ injektivni homomorfizam grupa, onda kažemo da je φ monomorfizam grupa.
- Ako je φ surjektivni homomorfizam grupa, onda kažemo da je φ epimorfizam grupa.
- Ako je φ bijektivni homomorfizam grupa, onda kažemo da je φ izomorfizam grupa. Oznaka za skup svih izmorofizama je $Iso(G_1, G_2)$.
- Ako je $\varphi\colon G_1 \to G_2$ dano s $\varphi(a) = e$, za $e \in G_2$ i $\forall a \in G_1$ homomorfizam grupa, onda kažemo je φ trivijalni ili nul-homomorfizam grupa.
- Ako je $\varphi\colon G \to G$ homomorfizam grupa, onda kažemo da je φ endomorfizam grupa. Oznaka za skup svih ednomorfizama od G je $End(G)$.
- Ako je $\varphi\colon G \to G$ bijektivni homomorfizam grupa (izomorfizam), onda kažemo da je φ automorfizam grupa. Oznaka za skup svih automorfizama od G je $Aut(G)$.

Kažemo da su grupe G_1 i G_2 izomorfne te pišemo $G_1 \simeq G_2$ ako postoji izomorfizam $\varphi\colon G_1 \to G_2$.
Svojstvo "biti izomorfan" je relacije ekvivalencije.
Pokažimo da se zaista radi o relaciji ekvivalencije, odnosno da su zadovoljena svojstva refleksivnosti, simetričnosti i tranzitivnosti.

1. Refleksivno: Identiteta $id_G\colon G \to G$, gdje je $id_G(a) = a, \forall a \in G$ je izomorfizam. Stoga imamo $G \simeq G$, što ispunjava svojstvo refleksivnosti.
2. Simetričnost: ako imamo izomorfizam $\varphi\colon G_1 \to G_2$, tada također postoji inverzni izomorfizam $\varphi^{-1}\colon G_2 \to G_1$. Inverzni izomorfizam također zadržava strukturalne karakteristike grupe, samo u obrnutom smjeru. Dakle, ako je $G_1 \simeq G_2$, tada će također biti $G_2 \simeq G_1$ te je time ispunjeno svojstvo simetričnosti.
3. Tranzitivnost: ako postoji izomorfizam $\varphi_1\colon G_1 \to G_2$ i izomorfizam $\varphi_2\colon G_2 \to G_3$, tada je kompozicija izomorfizama $\varphi_2 \circ \varphi_1\colon G_1 \to G_3$ izomorfizam između G_1 i G_3. Ovo je zato što kompozicija izomorfizama također čuva strukturalne karakteristike grupe. Prema tome, ako je $G_1 \simeq G_2$ i $G_2 \simeq G_3$, onda možemo zaključiti da je $G_1 \simeq G_3$. Dakle, ispunjeno je i svojstvo tranzitivnosti.

U sljedećoj propoziciji navedena su svojstva homomorfizama.

Propozicija 1. ([3, Chapter 3, Proposition 1.]) *Neka su G_1 i G_2 grupe i neka je $\varphi\colon G_1 \to G_2$ homomorfizam. Tada vrijedi:*

i) $\varphi(e_{G_1}) = e_{G_2}$, gdje su e_{G_1} i e_{G_2} redom neutralni elementi od G_1 i G_2.

ii) $\varphi(a^{-1}) = \varphi(a)^{-1}, \forall a \in G_1$.

iii) $\varphi(a^n) = \varphi(a)^n, \forall n \in \mathbb{Z}, a \in G_1$.

Dokaz. Dokažimo svojstva redom:

i) Zbog svojstva neutralnog elementa i definicije homomorfizma grupe, vrijedi

$$\varphi(e_{G_1}) = \varphi(e_{G_1} \cdot e_{G_1}) = \varphi(e_{G_1}) \cdot \varphi(e_{G_1}), \tag{1.3}$$

odakle, zbog toga što je G_2 grupa i element $\varphi(e_{G_1}) \in G_2$ ima inverzni element, slijedi

$$e_{G_2} = \varphi(e_{G_1})[\varphi(e_{G_1})]^{-1} = \varphi(e_{G_1})\varphi(e_{G_1})[\varphi(e_{G_1})]^{-1} = \varphi(e_{G_1})e_{G_2} = \varphi(e_{G_1}).$$

Navedimo da smo u jednakost (1.3) na obje strane primjenili operaciju iz grupe G_2 s desna. Važno je naglasiti s koje strane se primjenjuje operacija iz grupe zbog komutativnosti i činjenice da nisu sve grupe komutativne.

ii) Da bi dokazali drugo svojstvo koristit ćemo se definicijom homomorfizma, svojstvom inverza i prethodno dokazanim prvim svojstvom. Za $a \in G_1$ imamo:

$$e_{G_2} = \varphi(e_{G_1}) = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1}),$$

analogno

$$e_{G_2} = \varphi(e_{G_1}) = \varphi(a^{-1}a) = \varphi(a^{-1})\varphi(a).$$

Ove dvije jednakosti prikazuju da je $\varphi(a^{-1})$ inverz od $\varphi(a)$.

iii) Zadnje svojstvo pokaže se koristeći metodu matematičke indukcije i svojstvo *ii)*.

□

Definicija 14. *Neka je* $\varphi\colon G_1 \to G_2$ *homomorfizam grupa. Tada skup*

$$Im\varphi = \{\varphi(a)\colon a \in G_1\}$$

zovemo slika homomorfizma φ*, dok skup*

$$Ker\varphi = \{a \in G_1\colon \varphi(a) = e_{G_2}\}$$

zovemo jezgra homomorfizma φ*.*

Riječima rečeno, jezgru homomorfizma čini skup svih elemenata iz G_1 koji se preslikavaju u neutralni element grupe G_2 pomoću preslikavanja φ. Važno je primijetiti da je jezgra homomorfizma φ uvijek neprazan skup ($Ker\varphi \neq \emptyset$) jer svojstvo *i)* prethodne propozicije jamči da neutralni element e_{G1} pripada jezgri homomorfizma. Slika homomorfizma je skup elemenata u skupu G_2 koji su rezultat preslikavanja nekog elementa iz skupa G_1 pomoću φ. Slično kao i kod jezgre homomorfizma, slika homomorfizma φ nije neprazan skup tj. $e_{G_2} \in Im\varphi$.

Teorem 4. ([1, Chapter 4, 2.3 Theorem]) *Homomorfizam $\varphi\colon G_1 \to G_2$ je injektivan ako i samo ako je $Ker\varphi = \{e_{G_1}\}$.*

Dokaz. Pretpostavimo da je φ injektivni homomorfizam, odnosno monomorfizam i neka je $a \in Ker\varphi$. Tada je po definiciji jezgre homomorfizma φ i svojstva i) iz Propozicije 1, $\varphi(a) = e_{G_2} = \varphi(e_{G_1})$. Stoga, kako smo pretpostavili da je φ injekcija, slijedi da je $a = e_{G_1}$, odnosno $Ker\varphi = \{e_{G_1}\}$. Za obratnu implikaciju pretpostavimo da je $Ker\varphi = \{e_{G_1}\}$. Uzmimo $a, b \in G_1$ takve da vrijedi $\varphi(a) = \varphi(b)$. Tada je

$$\varphi(ab^{-1}) = \varphi(a)\varphi(b^{-1}) = \varphi(a)\varphi(b)^{-1} = \varphi(a)\varphi(a)^{-1} = e_{G_2} \Rightarrow ab^{-1} \in Ker\varphi.$$

Kako samo pokazali da se ab^{-1} nalazi u jezgri homomorfizma φ, onda je $ab^{-1} = e_{G_1}$. Množenjem te jednakosti zdesna s b dobivamo da je $a = b$ i tada je φ injekcija. □

Propozicija 2. ([1, Chapter 4, 3.3 Theorem]) *Neka je $\varphi\colon G_1 \to G_2$ homomorfizam grupa. U tom slučaju je $Ker\varphi \leq G_1$ i $Im\varphi \leq G_2$.*

Dokaz. Za dokaz ćemo koristiti Teorem 2. Jezgra homomorfizma φ je neprazan podskup od G_1, te neka su a i b elementi jezgre homomorfizma φ . Onda je

$$\varphi(ab^{-1}) = \varphi(a)\varphi(b^{-1}) = \varphi(a)\varphi(b)^{-1} = e_{G_2}e_{G_2}^{-1} = e_{G_2}e_{G_2} = e_{G2}$$

pa je $ab^{-1} \in Ker\varphi$ te smo time pokazali da je $Ker\varphi$ podgrupa od G_1.
Pokažimo sada da je $Im\varphi$ podgrupa grupe G_2. Slika homomorfizma φ neprazan je podskup od G_1 i neka su $a, b \in Im\varphi$. U tom slučaju postoje $c, d \in G_1$ takvi da je $a = \varphi(c)$ i $b = \varphi(d)$ te slijedi

$$ab^{-1} = \varphi(c)[\varphi(d)]^{-1} = \varphi(c)\varphi(d^{-1}) = \varphi(cd^{-1}).$$

Budući da je $cd^{-1} \in G_1$, slijedi da je $ab^{-1} \in Im\varphi$. Na taj način je dokazano da je slika homomorfizma φ podgrupa od G_2. □

Primjer 8. ([2, 1.3 Homomorfizmi grupa, Zadatak 1.3.1.]) *Netrivijalan primjer homomorfizma je determinanta. Determinantu možemo definirati za sve kvadratne matrice iz $M_n(\mathbb{R})$. U Primjeru 5 naveli smo da $GL_n(\mathbb{R})$ označava opću linearnu grupu i želimo pokazati da je preslikavanje $\varphi\colon GL_n(\mathbb{R}) \to \mathbb{R}^*$ dano s*

$$\varphi(A) = det(A)$$

homomorfizam grupa. Uočimo da je $\mathbb{R}^* = \mathbb{R}\backslash\{0\}$. Za izbor proizvoljnih matrica $A, B \in GL_n(\mathbb{R})$ vrijedi

$$\varphi(AB) = det(AB) = detA \cdot detB = \varphi(A) \cdot \varphi(B)$$

pri čemu smo na drugoj jednakosti iskoristili Binet-Cauchyjev teorem. Prema tome, pokazano je da je preslikavanje φ homomorfizam grupa.
No, nećemo stati samo na tome, možemo pokazati i da se radi o epimorfizmu grupa tj., pokazat ćemo da je preslikavanje $\varphi\colon GL_n(\mathbb{R}) \to \mathbb{R}^*$ surjektivno. Neka je $y \in \mathbb{R}^*$. Potražimo matricu A čija je determinanta jednaka y. Primjerice, dijagonalna matrica koja na presjeku prvog retka i prvog stupca ima x, a na svim ostalim dijagonalnim mjestima ima jedinicu je primjer takve matrice, odnosno vrijedi $detA = x$. Slijedi da je matrica $A \in GL_n(\mathbb{R})$ te je preslikavanje φ epimorfizam grupa.

2 Normalne podgrupe

Postoje različite vrste grupa i podgrupa kao što su simetrične, cikličke, normalne, kvocijentne itd. U ovom poglavlju opisat ćemo normalne podgrupe i navesti definicije, teoreme i ključna svojstva. Ta specijalna vrsta podgrupe od iznimne je važnosti za daljne konstrukcije.

Na početku se upoznajmo s pojmom kongruencije koju je u matematiku uveo jedan od najznačajnijih matematičara u povijesti Carl Friedrich Gauss.

Definicija 15. *Neka su $a, b \in \mathbb{Z}$ i neka je $n \in \mathbb{N}$. Kažemo da je a kongruentan b modulo n ako n dijeli razliku $a - b$ i pišemo*

$$a \equiv b \ (mod\ n).$$

U suprotnom, ako a nije kongruentan b modulo n, onda pišemo $a \not\equiv b \ (mod\ n)$ što znači da n ne dijeli razliku $a - b$.

Definicija 16. *Neka je G grupa i H podgrupa grupe G. Neka su $a, b \in G$. Kažemo da je a desno kongruentan b modulo H ako je*

$$b^{-1}a \in H. \tag{2.1}$$

Tada pišemo $a \sim_H b$.

Primjer 9. *Neka grupa G predstavlja grupu realnih brojeva s aditivnom operacijom i neka je H skup cijelih brojeva. Iz Primjera 6 znamo da je grupa cijelih brojeva sa zbrajanjem podgrupa grupe realnih brojeva sa zbrajanjem. Ukoliko su $a = 10$ i $b = 6$ elementi grupe G, tada vrijedi $-b + a = a - b = 10 - 6 = 4$, što je sadržano u podgrupi H. To znači da je $a = 10$ desno kongruentan $b = 6$ modulo $H = \mathbb{Z}$.*

Definicija 17. *Neka je G grupa i H podgrupa grupe G. Neka su $a, b \in G$. Kažemo da je a lijevo kongruentan b modulo H ako je*

$$ab^{-1} \in H. \tag{2.2}$$

Tada pišemo $a \ {}_H\!\sim b$.

Primjer 10. *Neka je G grupa cijelih brojeva s aditivnom operacijom i neka je $H = \{2k : k \in \mathbb{Z}\}$ (skup parnih cijelih brojeva). Lako se može pokazati da je ovako definirani H podgrupa grupe G. Razmotrimo dva elementa $a = 6, b = 10$ iz G. Istaknimo da je a lijevo kongruentan b modulo H ako $a - b$ pripada podgrupi H. U ovom slučaju, $a - b = 6 - 10 = -4$ pripada podgrupi H pa je $a = 6$ lijevo kongruentan $b = 10$ modulo $H = \{2k : k \in \mathbb{Z}\}$.*

Ako je G Abelova grupa, tada se desna i lijeva kongruencija modulo H podudaraju. To je zbog toga jer je $ab^{-1} \in H$ ako i samo ako je $(ab^{-1})^{-1} \in H$ i $(ab^{-1})^{-1} = ba^{-1} = a^{-1}b$. Također, postoje i ne-Abelove grupe G i podgrupe H takve da se desna i lijeva kongruencija modulo H podudaraju, ali to općenito nije istina.

Lema 1. ([10, Normalne podgrupe i kvocijentne grupe, Lema.]) *Neka je H podgrupa grupe G.*

i) "Biti desno kongruentan modulo H" je relacije ekvivalencije na G.

ii) Za klasu ekvivalencije elementa $a \in G$ uvedimo oznaku $[a]$, te je tada

$$[a] = \{ah \colon h \in H\}$$

i pišemo $[a] = aH$.

Dokaz. Potvrdimo taj teorem dokazom.

i) Relacija ekvivalencije je relacija koja je refleksivna, simetrična i tranzitivna pa pokažimo da je to zaista zadovoljeno.

1. Refleksivnost: Neka je $a \in G$. Postoji neutralni element grupe G i označimo ga s e te postoji inverzni element od a i označimo ga s a^{-1}. Budući da je H podgrupa od G, onda po Teoremu 2 vrijedi $a^{-1}a = e$ te je $a \sim_H a$. U toj situaciji smo pokazali da je relacija $\sim_H$ refleksivna.
2. Simetričnost: Nadalje, neku su $a, b \in G$ i neka je $a \sim_H b$. Po definiciji desne kongruencije modulo H je $b^{-1}a \in H$, a budući da je H grupa, onda imamo $(b^{-1}a)^{-1} = a^{-1}b \in H$ te je time pokazano da je b desno kongruentan a modulo H, tj. $b \sim_H a$. Dakle, simetričnost je zadovoljena.
3. Tranzitivnost: Na kraju, neka su $a, b, c \in G$ i neka vrijedi $a \sim_H b$ i $b \sim_H c$. Ponovno, po Definiciji 16 slijedi da je $b^{-1}a \in H$ i $c^{-1}b \in H$. Iskoristit ćemo svojstvo asocijativnosti i činjenicu da grupa H sadrži produkt svojih elemenata te dobivamo sljedeće:

$$(c^{-1}b)(b^{-1}a) = c^{-1}(bb^{-1})a = c^{-1}a \in H.$$

Time je pokazano da je zadovoljeno i svojstvo tranzitivnosti.

ii) Neka je $a \in G$.

$$[a] = \{b \in G \colon a \sim_H b\} \overset{*}{=} \{b \in G \colon b \sim_H a\} \overset{**}{=} \{b \in G \colon a^{-1}b \in H\} =$$

$$= \{b \in G \colon a^{-1}b = h, \text{ za neki } h \in H\} = \{b \in G \colon b = ah, \text{ za neki } h \in H\} =$$

$$= \{ah \colon h \in H\} = aH.$$

Navedimo da smo kod $(*)$ koristili svojstvo simetričnosti, a kod $(**)$ Definiciju 16.

□

Relacija biti lijevo kongruentan modulo H također je relacija ekvivalencije na G. Dokaz slijedi analogno kao u Lemi 1 pod *i)*.
Prethodno navedene klase ekvivalencije $[a] = aH$, za $a \in G$, poznate su kao desne klase u G u odnosu na podgrupu H ili skraćeno desne H–klase u G. Kao skup grupa G je jednaka disjunktnoj uniji svih svojih desnih H–klasa.
Klase ekvivalencije elemenata $a \in G$, $[a] = \{ha \colon h \in H\} = Ha$, poznate su kao lijeve klase u G u odnosu na H, tj. lijeve H–klase u G. Također vrijedi da je grupa G disjunktna unija svih svojih lijevih H–klasa.

Korolar 2. ([6, 3.6. Susjedne klase. Lagrangeov teorem, Korolar 3.]) *Neka su $a, b \in G$ i neka je H podgrupa grupe G. Onda je:*

i) $aH = bH$, *ako je* $a \sim_H b$.

ii) $aH \cap bH = \emptyset$, *ako* $a \nsim_H b$.

Analogan iskaz korolara vrijedi i u slučaju lijevih klasa i lijeve kongruencije.

Između svake dvije H–klase u grupi G postoji bijektivno preslikavanje. Doista, definiramo sljedeća preslikavanja za element p iz grupe G, $\varphi_p, \chi_p, \psi_p \colon G \to G$:

$$\varphi_p(a) = pap^{-1}, \quad \chi_p(a) = ap, \quad \psi_p(a) = pa, \quad a \in G.$$

Navedena preslikavanja koristimo u sljedećoj propoziciji.

Propozicija 3. ([8, Poglavlje 2., Propozicija 2.1.]) *Neka je G grupa, H pogrupa od G i $p \in G$. Tada vrijedi:*

i) φ_p *je izomorfizam grupe G na G. Restrikcija $\varphi_p|Hp$ je bijekcija lijeve H–klase Hp na desnu H–klasu pH.*

ii) χ_p *je bijekcija s G na G. Za $a, b \in G$ restrikcija $\chi_{a^{-1}b}|Ha$ je bijekcija s Ha na Hb.*

iii) ψ_p *je bijekcija s G na G. Za $a, b \in G$ restikcija $\psi_{ba^{-1}}|aH$ je bijekcija s aH na bH.*

Dokaz. Dokažimo tvrdnje redom:

i) φ_p je homomorfizam jer je

$$\varphi_p(ab) = pabp^{-1} = pap^{-1}pbp^{-1} = \varphi_p(a)\varphi_p(b).$$

Pokažimo da je φ_p injekcija. Pod pretpostavkom da su elementi $a, b \in G$ takvi da vrijedi $\varphi_p(a) = \varphi_p(b)$, onda to podrazumijeva da je

$$\begin{aligned} pap^{-1} &= pbp^{-1} \ / \cdot p \\ pap^{-1}p &= pbp^{-1}p \\ pae &= pbe \\ pa &= pb \\ p^{-1} \cdot / \ pa &= pb \\ p^{-1}pa &= p^{-1}pb \\ ea &= eb \\ a &= b. \end{aligned}$$

Također, zaključujemo da je φ_p surjekcija s G na G. Pokažimo to: za bilo koji element $a \in G$ vrijedi $\varphi_p(p^{-1}ap) = pp^{-1}app^{-1} = a$. Prema tome, kako smo pokazali da je φ_p bijektivni homomorfizam, pokazali smo da je φ_p izomorfizam grupe G na samu sebe. Konačno, očigledno je $\varphi_p(Hp) = pHpp^{-1} = pH$.

ii) Za drugu tvrdnju pokažimo da je χ_p bijekcija, tj. da imamo injekciju i surjekciju. Pokažimo da je χ_p injekcija:

$$\begin{aligned} \chi_p(a) &= \chi_p(b) \\ ap &= bp \ / \cdot p^{-1} \\ app^{-1} &= bpp^{-1} \\ ae &= be \\ a &= b. \end{aligned}$$

Sada pokažimo da je χ_p surjekcija. Za bilo koji element $a \in G$ vrijedi

$$\chi_p(ap^{-1}) = ap^{-1}p = a.$$

Na kraju slijedi:

$$\chi_{a^{-1}b}(Ha) = Haa^{-1}b = Hb.$$

iii) Dokažimo još da je ψ_p bijekcija. Lako vidimo da je ψ_p injekcija:

$$\begin{aligned} \psi_p(a) &= \psi_p(b) \\ p^{-1} \cdot /pa &= pb \\ p^{-1}pa &= p^{-1}pb \\ ea &= eb \\ a &= b. \end{aligned}$$

Također, lako se vidi da je ψ_p surjekcija. Za bilo koji element $a \in G$ vrijedi

$$\psi_p(p^{-1}a) = pp^{-1}a = a.$$

Napokon,

$$\psi_{ba^{-1}}(aH) = ba^{-1}aH = bH.$$

□

Dakle, za sve H–klase u grupi G (bilo da se radi o desnim ili lijevim) postoji bijektivno preslikavanje između njih.

Lema 2. ([10, Normalne podgrupe i kvocijentne grupe, Lema.]) *Neka je G konačna grupa i $H \leq G$. Za svaki $a \in G$ vrijedi*

$$|aH| = |H| = |Ha|.$$

Dokaz. Vidjeti u 10. □

Interpretacija leme: kardinalnost svake desne i lijeve klase je jednaka i ta kardinalnost odgovara redu podgrupe H.
Idući teorem jedan je od najvažnijih rezultata u teoriji grupa.

Teorem 5. ([8, Poglavlje 2., Teorem 2.1.]) (Lagrangeov teorem) *Neka je G konačna grupa i H podgrupa od G. Tada je red $|G|$ grupe G djeljiv s redom $|H|$ grupe H, odnosno $|H|$ dijeli $|G|$. Konkretnije, ako je $|G| = n$, $|H| = k$ i ako je r broj desnih H–klasa u G, onda je $n = rk$ (r je također i broj lijevih H–klasa u G).*

Dokaz. Neka su $a_1, a_2, \ldots, a_r$ predstavnici svih desnih H–klasa u G. Tada je

$$G = a_1H \cup a_2H \cup \cdots \cup a_rH$$

(G je disjunktna unija desnih H–klasa). Stoga je,

$$\begin{aligned} |G| &= |a_1H \cup a_2H \cup \cdots \cup a_rH| \\ &= |a_1H| + |a_2H| + \cdots + |a_rH| \end{aligned}$$

pa zbog Leme 2 slijedi

$$|G| = |H| + |H| + \cdots + |H| = r|H|.$$

Dobili smo da je $n = rk$, te zaključujemo da $|H|$ dijeli $|G|$. □

Korolar 3. ([4, Section 17, Corollary 5.]) *Ako je G konačna grupa prostog reda, tada su čitava G i $\{e\}$ jedine podgrupe od G.*

Dokaz. Ovo je izravna posljedica Lagrangeovog teorema, budući da prost broj nema pozitivnih djelitelja osim 1 i samoga sebe. □

Primjer 11. *Neka je G konačna grupa i neka je $H \leq G$. Neka je $|G| = 8$. Mogući redovi podgrupe H su iz skupa $\{1, 2, 4, 8\}$, tj. $|H| \in \{1, 2, 4, 8\}$.*

Definicija 18. *Neka je G grupa i H je podgrupa od G. Ako postoji konačno mnogo različitih desnih H–klasa u G, onda kažemo da je H podgrupa konačnog indeksa. U tom slučaju broj desnih H–klasa u G označavamo s $[G : H]$. Broj $[G : H]$ nazivamo indeks od H u G.*

Svejedno je koristimo li u prethodnoj definiciji desne ili lijeve H–klase jer znamo da je broj desnih H–klasa jednak broju lijevih H–klasa. Ako je $G = H$, onda je $[G : H] = 1$. Ako je $H = \{e\}$, onda je desna (lijeva) klasa u G u odnosu na podgrupu H jednočlana. Dakle, indeks od H u G jednak je redu grupe G. Ako za trivijalnu podgrupu $H = \{e\}$ pišemo 1, dobivamo $|G| = [G : 1]$.

Napomena 3.

- ([1, Chapter 4]) *Neka je G konačna grupa i H podgrupa grupe G. Tada je*

$$[G : H][H : 1] = [G : 1].$$

- ([7, Chapter I: Groups, Theorem 4.5.]) *Općenito, neka su H i K podgrupe od G i neka je $K \leq H$. Tada je*

$$[G : H][H : K] = [G : K].$$

Ako su bilo koja dva od ovih indeksa konačna, onda je konačan i treći indeks.

- ([2, 1.5 Normalne i kvocijentne podgrupe, Napomena 1.5.8.]) *Ako je G konačna grupa i ako je H bilo koja podgrupa grupe G, tada prema Lagrangeovom teoremu vrijedi:*

$$[G : H] = \frac{|G|}{|H|}.$$

Primjer 12. *Već smo naveli u Primjeru 6 da je $n\mathbb{Z}$ podgrupa od $\mathbb{Z}$. Uzmimo da je $n = 12$. Indeks podgrupe $12\mathbb{Z}$ u grupi $\mathbb{Z}$ jest 12, tj. $[\mathbb{Z} : 12\mathbb{Z}] = 12$.*

Definicija 19. *Za podgrupa H grupe G kažemo da je normalna podgrupa ako je*

$$aH = Ha, \text{ za sve } a \in G.$$

Ako je H normalna podgrupa od G, onda to obično zapisujemo ovako: $H \trianglelefteq G$. Očito, podgrupe $\{e\}$ i G su normalne podgrupe grupe G . Navedenu jednakost $aH = Ha$ pišemo također kao jednakost skupova $\{ah \colon h \in H\} = \{ha \colon h \in H\}$. Zbog toga nam slijedi da je u Abelovoj grupi svaka podgrupa normalna. Obrat općenito ne vrijedi: grupa u kojoj su sve podgrupe normalne nije nužno Abelova.
Sljedeći teorem daje nekoliko karakterizacija normalne podgrupe.

Teorem 6. ([5, 6. Normalne podgrupe i kvocijentne grupe, 6.3. Normalna podgrupa.]) *Neka je G grupa i $H \trianglelefteq G$. Sljedeći su uvjeti ekvivalentni:*

i) $aHa^{-1} \subseteq H, \forall a \in G,$

ii) $aHa^{-1} = H, \forall a \in G,$

iii) $aH = Ha, \forall a \in G.$

Dokaz. Za početak pokažimo da prvi uvjet implicira drugi uvjet. Kako prvi uvjet vrijedi za svaki $a \in G$, onda umjesto njega možemo uvrstiti njegov inverzni element a^{-1}. Tada imamo

$$a^{-1}Ha \subseteq H, \forall a \in G.$$

Sada pomnožimo taj izraz slijeva elementom a te zdesna elementom a^{-1} i dobivamo

$$\begin{aligned} a(a^{-1}Ha)a^{-1} &\subseteq aHa^{-1} \\ eHe &\subseteq aHa^{-1} \\ H &\subseteq aHa^{-1}, \forall a \in G. \end{aligned}$$

Vidimo da je

$$H \subseteq aHa^{-1} \subseteq H,$$

tj. $aHa^{-1} = H, \forall a \in G$.
Pokažimo da drugi uvjet implicira treći. Drugi uvjet pomnožimo zdesna s elementom a:

$$\begin{aligned} (aHa^{-1})a &= Ha \\ a(Ha^{-1}a) &= Ha \\ aHe &= Ha \\ aH &= Ha, \forall a \in G. \end{aligned}$$

Još preostaje pokazati da treći uvjet implicira prvi uvjet. Tada izraz $aH = Ha$ pomnožimo s a^{-1} zdesna i dobijemo $aHa^{-1} = H \subseteq H, \forall a \in G$. □

Teorem 7. ([4, Section 21, Theorem 21.2.]) *Neka su G_1 i G_2 grupe i neka je $\varphi\colon G_1 \to G_2$ homomorfizam grupa. Tada je $Ker\varphi$ normalna podgrupa grupe G_1.*

Dokaz. Iz Propozicije 2 znamo da je $Ker\varphi$ podgrupa grupe G_1. Dakle, dovoljno je pokazati da je jezgra homomorfizma φ normalna podgrupa od G_1. Treba pokazati da je $a(Ker\varphi)a^{-1} = Ker\varphi, \forall a \in G_1$. Prvo provjerimo je li

$$a(Ker\varphi)a^{-1} \subseteq Ker\varphi, \forall a \in G_1. \tag{2.3}$$

Neka je $a \in G_1$ i neka je $h_1 \in Ker\varphi$ proizvoljan element jezgre homomorfizma. Tada je prema definiciji jezgre homomorfizma $\varphi(h_1) = e_{G_2}$, te prema svojstvima homomorfizma možemo reći da vrijedi:

$$\varphi(ah_1a^{-1}) = \varphi(a)\varphi(h_1)\varphi(a)^{-1} = \varphi(a)e_{G_2}\varphi(a)^{-1} = \varphi(a)\varphi(a)^{-1} = e_{G_2}, \forall a \in G_1.$$

Iz toga zaključujemo da je i $ah_1a^{-1} \in Ker\varphi$ za svaki $a \in G_1$. Kako je izbor elementa h_1 iz jezgre homomorfizma φ bio proizvoljan, zaista je pokazano da vrijedi (2.3). Nadalje, pokažimo da vrijedi druga inkluzija, odnosno

$$Ker\varphi \subseteq a(Ker\varphi)a^{-1}, \forall a \in G_1. \tag{2.4}$$

Možemo umjesto a uzeti a^{-1} (to je moguće jer, kako je navedeno, relacija (2.3) vrijedi za svaki element grupe G_1) te tada postoji $h_2 \in Ker\varphi$ takav da je $a^{-1}h_1a = h_2$. Sada ako pomnožimo tu jednakost s a slijeva i zdesna s a^{-1} dobivamo $h_1 = ah_2a^{-1}$ te je $Ker\varphi \subseteq a(Ker\varphi)a^{-1}$. Iz pokazanih inkluzija dolazimo do zaključka da je $a(Ker\varphi)a^{-1} = Ker\varphi, \forall a \in G_1$, odnosno $Ker\varphi$ je normalna podgrupa grupe G_1. □

Lako se pokaže da ako je G grupa s podgrupama N i M takvim da je $N \trianglelefteq M$ i $M \trianglelefteq G$, onda ne slijedi da je $N \trianglelefteq G$. Međutim, ako je N normalna podgrupa grupe G, tada je N normalna u svakoj podgrupi od G koja sadrži N.

Propozicija 4. ([6, 3.5. Normalne podgrupe, Propozicija 1]) *Neka je $M \trianglelefteq G$ i $N \trianglelefteq G$. Onda je i $M \cap N$ normalna podgrupa od G.*

Dokaz. Kako su M i N podgrupe od G, onda je po Teoremu 3 i $M \cap N \leq G$. Nadalje, neka su $x \in M \cap N$ i $a \in G$. Treba pokazati da je $axa^{-1} \in M \cap N$. S obzirom na činjenicu da je x element presjeka, onda je $x \in M$, a kako je M prema pretpostavci normalna podgrupa od G, onda slijedi $axa^{-1} \in M$. Slično, $x \in N$ i N je normalna podgrupa od G pa imamo $axa^{-1} \in N$. Dokazali smo što je trebalo, odnosno $axa^{-1} \in M \cap N$. □

Analogno se može dokazati da je presjek bilo kojeg proizvoljnog broja normalnih podgrupa od G ponovno normalna podgrupa od G.

Primjer 13. *Navedimo dva zanimljiva primjera normalnih podgrupa:*

- ([5, 6. Normalne podgrupe i kvocijentne grupe, 6.8. Primjer (podgrupa indeksa 2).]) *Neka je H podgrupa grupe G takva da je indeks $[G : H] = 2$. Pokažimo da je H normalna podgrupa od G. S obzirom na podgrupu H, grupa G ima dvije lijeve klase, od kojih je jedna od njih sama podgrupa H, dok je druga klasa $G \setminus H$, odnosno obuhvaća sve elemente koji se nalaze izvan skupa H. Dakle,*

$$aH = \begin{cases} H, & ako\ a \in H, \\ G \setminus H, & ako\ a \notin H. \end{cases}$$

Analogno vrijedi i za desne klase,

$$Ha = \begin{cases} H, & ako\ a \in H, \\ G \setminus H, & ako\ a \notin H. \end{cases}$$

Pokazali smo da se lijeve i desne klase podudaraju, tj. $aH = Ha, \forall a \in G$ te je prema tome H normalna podgrupa od G.

- ([2, 1.5 Normalne i kvocijentne podgrupe, Zadatak 1.5.4.]) *Pokažimo da je specijalna linearna grupa normalna podgrupa opće linearne grupe. Ranije smo argumentirali u Primjeru 10 da je $SL(n, \mathbb{R})$ podgrupa od $GL(n, \mathbb{R})$. Da bi smo još pokazali normalnost uzmimo $A \in SL(n, \mathbb{R})$ i $B \in GL(n, \mathbb{R})$. Koristeći Binet-Cauchyjev teorem i činjenicu da je $detA = 1$ imamo*

$$det(BAB^{-1}) = (detB) \cdot (detA) \cdot (detB)^{-1} = (detB) \cdot (detB)^{-1} = 1$$

i $BAB^{-1} \in M_n(\mathbb{R})$. Iz toga slijedi da je $BAB^{-1} \in SL(n, \mathbb{R})$, pa preciznije zaključujemo da je $SL(n, \mathbb{R})$ normalna podgrupa od $GL(n, \mathbb{R})$.

Definicija 20. *Neka je S podskup grupe G. Centralizator skupa S u G je skup svih elemenata iz G koji komutiraju sa svim elementima iz S, tj.*

$$C_G(S) = \{a \in G \colon as = sa, \forall s \in S\}.$$

Definicija 21. *Centar grupe G je skup svih elemenata u G koji komutiraju sa svakim elementom od G. Označava se s*

$$Z(G) = \{a \in G \colon ag = ga, \forall g \in G\}.$$

Uočimo da je $C_G(G) = Z(G)$.

Teorem 8. ([1, Chapter 4, 3.4 Theorem]) *Centar grupe G podgrupa je od G.*

Dokaz. Pokažimo da je $Z(G) \leq G$. Prije svega, skup $Z(G) \neq \emptyset$ jer je $eg = g = ge, \forall g \in G$ pa je $e \in Z(G)$. Neka su $a, b \in Z(G)$. Zatim, za svaki $g \in G$ je

$$ab^{-1}g = ab^{-1}ge = ab^{-1}gbb^{-1} = ab^{-1}bgb^{-1} = aegb^{-1} = agb^{-1} = gab^{-1}$$

Stoga je $ab^{-1} \in Z(G)$, te po Teoremu 2 slijedi da je $Z(G)$ pogrupa od grupe G. □

Uočimo da je $Z(G)$ normalna podgrupa od G jer za $a \in Z(G)$ i $g \in G$ imamo $gag^{-1} = a$, a to znači da je $gZ(G)g^{-1} = Z(G), \forall g \in G$.

Napomena 4. ([10, Normalne podgrupe i kvocijentne grupe]) *Uz centar grupe G vežemo sljedeće napomene:*

- *Grupa G je Abelova ako i samo ako je $G = Z(G)$.*
- *Ako je $H \leq G$ takva da je $H \subseteq Z(G)$, onda je $H \trianglelefteq G$. Takva se podgrupa naziva centralna podgrupa grupe G.*

Definicija 22. *Neka je G grupa i neka je S neprazan podskup od G. Normalizator od S u G je skup*

$$N(S) = \{a \in G \colon aSa^{-1} = S\}.$$

Normalizator jednočlanog skupa $\{a\}$ označava se s $N(a)$.

Teorem 9. ([1, Chapter 5, 1.3 Theorem]) *Neka je G grupa.*

i) Za bilo koji neprazan podskup S od G, $N(S)$ je podgrupa od G.

ii) Za bilo koju podgrupu H od G, $N(H)$ je najveća podgrupa od G u kojoj je H normalna podgrupa.

Dokaz.

i) Očito je $e \in N(S)$. Ako su $a, b \in N(S)$, onda po definiciji normalizatora i kriteriju za određivanje podgrupe vrijedi

$$(ab^{-1})S(ab^{-1})^{-1} = (ab^{-1})S(ba^{-1}) = a(b^{-1}Sb)a^{-1} \overset{*}{=} aSa^{-1} = S,$$

pri čemu smo kod $(*)$ iskoristili da bSb^{-1}=S implicira $S = b^{-1}Sb$. Dakle, $ab^{-1} \in N(S)$ i zaključujemo da je $N(S) \leq G$.

ii) Prvo pokažimo da je H normalna podgrupa od $N(H)$. Neka je $H \leq G$ i tada je $hHh^{-1} = H, \forall h \in H$. Stoga je $H \subseteq N(H)$ i H je onda podgrupa od $N(H)$. Kako prema definiciji normalizatora za svaki $a \in N(H)$ vrijedi $aHa^{-1} = H$, onda je $H \trianglelefteq N(H)$. Preostaje još pokazati da je $N(H)$ najveća podgrupa od G u kojoj je H normalna podgrupa. Neka je K bilo koja podgrupa od G takva da je H normalna podgrupa od K. Kako je $H \trianglelefteq K$, onda je $kHk^{-1} = H, \forall k \in K$ te po definiciji normalizatora slijedi da je K podskup od normalizatora skupa H u G. To pokazuje da je $N(H)$ najveća podgrupa od G koja sadrži H kao normalnu podgrupu.

□

Propozicija 5. ([3, Chapter 2]) *Neka je G grupa i neka je $S \subseteq G$, $S \neq \emptyset$. Tada je $C_G(S)$ podgrupa od $N(S)$.*

Dokaz. Neka je $aSa^{-1} = \{asa^{-1} \colon s \in S\}$. Primjećujemo da ako je a element centralizatora skupa S u G, onda je $asa^{-1} = s \in S$, za svaki $s \in S$. To povlači da je a element normalizatora skupa S u G te je $C_G(S) \subseteq N(S)$. Navedimo još da je $C_G(S) \neq \emptyset$ jer je $e \in C_G(S)$. Centralizator skupa S u G zatvoren je s obzirom na množenje: ako su $a, b \in C_G(S)$, onda za svaki $s \in S$ vrijedi

$$(ab)s = a(bs) = a(sb) = (as)b = (sa)b = s(ab) \Rightarrow ab \in C_G(S)$$

i zatvoren je s obzirom na postojanje inverznog elementa: ako je $a \in C_G(S)$, onda za svaki $s \in S$ vrijedi

$$\begin{aligned} a^{-1}/as &= sa \\ s &= a^{-1}sa/a^{-1} \\ sa^{-1} &= a^{-1}s \Rightarrow a^{-1} \in C_G(S). \end{aligned}$$

Tako je pokazano da je $C_G(S)$ grupa i uzimajući u obzir da je $C_G(S) \subseteq N(S)$ zaključujemo da je $C_G(S) \leq N(S)$. □

Kako smo u Teoremu 6 naveli ekvivalentne uvjete za karakterizaciju normalne podgrupe i definirali smo normalizator, onda zaključujemo da su normalne podgrupe grupe G one podgrupe grupe G kod kojih je normalizator cijela grupa G. Zapišimo to malo detaljnije. Neka je G grupa i neka je H normalna podgrupa od G. Tada vrijedi da je $aH = Ha$, za $a \in G$, a taj je uvjet ekvivalentan s uvjetom

$$aHa^{-1} = H, \ \forall a \in G,$$

te se normalne podgrupe mogu okarakterizirati kao podgrupe kod kojih je $N(H) = G$.

3 Kvocijentne grupe

U ovom poglavlju uvodimo pojam kvocijentne grupe grupe G. Kvocijentne grupe predstavljaju još jedan način da se iz grupe G dobije manja grupa. Slično kao što smo proučavali podgrupe, kvocijentne grupe će nam pomoći da dublje razumijemo strukturu grupe G. Struktura grupe G odražava se u strukturi njezinih kvocijentnih grupa i podgrupa. Proučavanje kvocijentnih grupa je suštinski ekvivalentno proučavanju homomorfizama.

Neka je G grupa i neka je H normalna podgrupa od G. Označimo s G/H skup svih H–klasa u G. Važno je napomenuti da nije potrebno specificirati govorimo li skupu svih lijevih ili svih desnih H–klasa u G. To je posljedica definicije normalne podgrupe koja nam govori da su lijeve i desne H–klasa u G zapravo iste. Definirajmo na skupu G/H binarnu operaciju:

$$(aH)(bH) = abH, \qquad aH, bH \in G/H,\ a, b \in G. \tag{1}$$

Za početak provjerimo je li ova binarna operacija dobro definirana, to jest da rezultat abH ne ovisi o tome koji su predstavnici odabrani iz dviju H–klasa. Neka su $a, b \in G$ i neka su $a', b' \in G$ redom novi predstavnici istih H–klasa. Tada je

$$\begin{aligned} aH &= a'H, \\ bH &= b'H. \end{aligned} \tag{2}$$

Prva jednakost iz (2) ekvivalentna je s $a \sim_H a'$ ili $a' \sim_H a$. Po Definiciji 16 slijedi da je $a^{-1}a' \in H$, odnosno postoji $h_1 \in H$ takav da je $a^{-1}a' = h_1$. Ako slijeva pomnožimo tu jednakost s a, slijedi izraz $a' = ah_1$.
Druga jednakost iz (2) ekvivalentna je s $b \sim_H b'$ ili $b' \sim_H b$. Ponovno po Definiciji 16 slijedi da je $b^{-1}b' \in H$, odnosno postoji $h_2 \in H$ takav da je $b^{-1}b' = h_2$. Sada tu jednakost pomnožimo slijeva s b te slijedi izraz $b' = bh_2$.
Provjerimo je li $a'b'H = abH$. Dakle, sada je

$$a'b' = ah_1bh_2 = aeh_1bh_2 = abb^{-1}h_1bh_2,$$

pa slijedi da je $b^{-1}h_1b \in H$ jer je $H \trianglelefteq G$. Tada postoji $h_3 \in H$ takav da je

$$a'b' = (ab)(h_3h_2). \tag{3}$$

Kako su $h_2, h_3 \in H$, onda je i njihov produkt $h_3h_2 \in H$. Pomnožimo jednakost (3) slijeva s $(ab)^{-1}$ te dobivamo

$$(ab)^{-1}(a'b') = h_3h_2,$$

odnosno

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

te po Definiciji 16 slijedi $a'b' \sim_H ab$ pa je $abH = a'b'H$.
Pokazali smo da binarna operacija ne ovisi o izboru predstavnika.

Obzirom na tako definiranu binarnu operaciju (1) skup G/H postaje grupa. Pokažimo da su zadovoljeni aksiomi grupe:

- Zatvorenost: za sve $aH, bH \in G/H$ vrijedi $abH \in G/H$.
- Asocijativnost: za sve $aH, bH, cH \in G/H$ vrijedi

$$((aH)(bH))(cH) = (abH)(cH) = abcH = (aH)(bcH) = (aH)((bH)(cH)).$$

- Postojanje neutralnog elementa: postoji neutralni element u G/H i to je $eH = \{eh \colon h \in H\} = \{h \colon h \in H\} = H$ takav da vrijedi

$$(eH)(aH) = (aH)(eH) = (aH)H = aH, \text{ za svaki } aH \in G/H.$$

- Postojanje inverznog elementa: $\forall aH \in G/H$, $\exists (aH)^{-1} = a^{-1}H \in G/H$ takav da vrijedi

$$(aH)(a^{-1}H) = (a^{-1}H)(aH) = eH.$$

Definicija 23. *Grupa G/H naziva se kvocijentna grupa grupe G po normalnoj podgrupi H.*

Primjer 14. ([6, 3.7. Kvocijentna grupa]) *Uzmimo da je $G = \mathbb{Z}$ i $H = n\mathbb{Z}$, pri čemu je $n \in \mathbb{N}$. U prethodnim poglavljima smo pokazali da je $n\mathbb{Z}$ podgrupa od $\mathbb{Z}$. Također, $n\mathbb{Z}$ je normalna podgrupa od grupe $\mathbb{Z}$ jer je $\mathbb{Z}$ Abelova grupa. Tada je $\mathbb{Z}/n\mathbb{Z}$ kvocijentna grupa koju nazivamo grupa klasa ostataka modulo n. Elementi te grupe su klase oblika*

$$\begin{aligned}
[p] &= \{t \in \mathbb{Z} \colon t \equiv p \ (mod\ n)\} \\
&= \{t \in \mathbb{Z} \colon t - p \text{ je djeljivo s } n\} \\
&= \{t \in \mathbb{Z} \colon t - p \in n\mathbb{Z}\} \\
&= \{t \in \mathbb{Z} \colon t \in p + n\mathbb{Z}\} \\
&= p + n\mathbb{Z},
\end{aligned}$$

pri čemu je $p \in \mathbb{Z}$. Uočimo da među klasama ima samo n različitih:

$$\begin{aligned}
[0] &= n\mathbb{Z} \\
[1] &= 1 + n\mathbb{Z} \\
&\vdots \\
[n-1] &= (n-1) + n\mathbb{Z}.
\end{aligned}$$

To je zbog toga što je npr.

$$\begin{aligned}
[n] &= n + n\mathbb{Z} = n(1 + \mathbb{Z}) = n\mathbb{Z} = [0], \\
[n+1] &= (n+1) + n\mathbb{Z} = 1 + (n + n\mathbb{Z}) = 1 + n\mathbb{Z} = [1], \quad \textit{itd.}
\end{aligned}$$

Dakle, kvocijenta grupa je oblika

$$\mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\} = \{[0], [1], \ldots, [n-1]\}$$

te je na njoj definirana binarna operacija zbrajanja s

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) = a + b + n\mathbb{Z},\ \forall a, b \in \mathbb{Z}.$$

Teorem 10. ([7, Chapter I: Groups, Theorem 5.5.]) *Ako je H normalna podgrupa od G, onda je preslikavanje $\pi\colon G \to G/H$ definirano s $\pi(a) = aH$ epimorfizam s $Ker\pi = H$.*

Dokaz. Treba pokazati da je preslikavanje π epimorfizam, odnosno da je surjektivni homomorfizam grupa. Očigledno je da je preslikavanje $\pi\colon G \to G/H$ definirano s $\pi(a) = aH$ surjekcija. Nadalje, na osnovu definirane binarne operacije kvocijentne grupe G/H slijedi:

$$\pi(ab) = abH = (aH)(bH) = \pi(a)\pi(b)$$

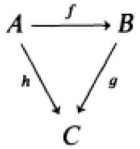
te je π homomorfizam grupa. Pokažimo još čemu je jednaka jezgra homomorfizma φ. Uočimo da je jezgra homomorfizma π dana s

$$\begin{aligned} Ker\pi &= \{a \in G\colon \pi(a) = eH\} \\ &= \{a \in G\colon aH = eH = H\} \\ &= \{a \in G\colon a \in H\} \\ &= H. \end{aligned}$$

□

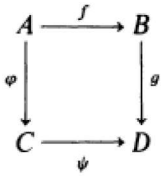
Preslikavanje $\pi\colon G \to G/H$ naziva se kanonski epimorfizam s G na G/H.

Objasnimo sada pojam komutativnog dijagram kako bismo olakšali razumijevanje sljedećih pojmova i teorema. Za dijagram



Slika 1: Komutativni dijagram, Izvor ([9])

kažemo da je komutativan ako je $g \circ f = h$. Slično, dijagram



Slika 2: Komutativni dijagram, Izvor ([9])

je komutativan ako je $g \circ f = \psi \circ \varphi$. Za složenije dijagrame koji se sastoje od strelica (morfizama) između različitih objekata kažemo da su komutativni ako, kad god je moguće prijeći s jednog objekta na drugi pomoću dva niza strelica, recimo

$$A_1 \xrightarrow{f_1} A_2 \xrightarrow{f_2} \cdots \xrightarrow{f_{n-1}} A_n$$

i

$$A_1 \xrightarrow{g_1} B_2 \xrightarrow{g_2} \cdots \xrightarrow{g_{m-1}} B_m = A_n,$$

tada je

$$f_{n-1} \circ \cdots \circ f_1 = g_{m-1} \circ \cdots \circ g_1,$$

odnosno, kompozicije su jednake. Većina dijagrama sastoji se od trokuta ili kvadrata. Da bismo provjerili da je dijagram koji je sastavljen od trokuta ili kvadrata komutativan, dovoljno je provjeriti da je svaki trokut ili kvadrat unutar njega komutativan.

Definicija 24. *Neka je*

$$G' \xrightarrow{f} G \xrightarrow{g} G''$$

niz homomorfizama. Kažemo da je taj niz egzaktan ako je $Imf = Kerg$.

Na primjer, ako je H normalna podgrupa grupe G, onda je niz

$$H \xrightarrow{j} G \xrightarrow{\pi} G/H$$

egzaktan, pri čemu je j inkluzija i π već navedeno kanonsko preslikavanje.
Općenito, niz homomorfizama s više od jednog člana, kao što je

$$G_1 \xrightarrow{f_1} G_2 \xrightarrow{f_2} G_3 \to \cdots \xrightarrow{f_{n-1}} G_n,$$

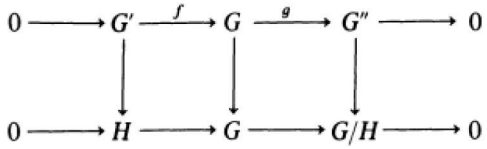
naziva se egzaktan ako vrijedi $Imf_i = Kerf_{i+1}$, za svaki $i = 1, \ldots n-2$.
Promotrimo sljedeći niz:

$$0 \to G' \xrightarrow{f} G \xrightarrow{g} G'' \to 0.$$

Taj niz je egzaktan ako je f injektivno preslikavanje, g surjektivno preslikavanje i $Imf = Kerg$.
Prema tome, ako je $H = Kerg$, onda imamo egzaktan niz

$$0 \to H \to G \to G/H \to 0.$$

Preciznije, tada zapravo postoji komutativni dijagram:



Slika 3: Komutativni dijagram, Izvor ([9])

kod kojeg su vertikalna preslikavanja izomorfizmi, a redovi su egzaktni nizovi.

Kako smo već na početku poglavlja naveli da je pročavanje kvocijentnih grupa u suštini ekvivalento proučavanju homomorfizama, a preko prethodnog Teorema 10 i idućeg Teorema 11 je pokazano da je to zaista tako. Idući teorem jedan je od bitnijih teorema u algebri i nosi poseban naziv. Radi se o fundamentalnom teoremu o homomorfizmu, odnosno nazivamo ga Prvi teorem o izomorfizmu. Postoje još Drugi i Treći teorem o izomorfizmu koji slijede iz Prvog teorema o izomorfizmu.

Teorem 11. ([10, Normalne podgrupe i kvocijentne grupe, Teorem.])(Prvi teorem o izomorfizmu) *Neka je* $\varphi\colon G_1 \to G_2$ *homomorfizam grupa. Preslikavanje* $\Phi\colon G_1/Ker\varphi \to Im\varphi$ *dano s*

$$\Phi(aKer\varphi) = \varphi(a),\ za\ a \in G_1,$$

je izomorfizam kvocijentne grupe $G_1/Ker\varphi$ *na grupu* $Im\varphi$.

Po već uvedenim oznaka to možemo pisati ovako: $G_1/Ker\varphi \simeq Im\varphi$.

Dokaz. Neka je $Ker\varphi = H$. Za dokaz prvog teorema o izomorfizmu najprije treba provjeriti je li preslikavanje Φ dobro definirano, što zapravo znači da ne ovisi o izboru prestavnika H–klase. Neka je

$$aH = a'H, \tag{4}$$

za neke $a, a' \in G_1$, a to možemo interpretirati na način da su aH i $a'H$ predstavnici iste klase ekvivalencije. Jednakost (4) ekvivalentna je s $a \sim_H a'$ ili $a' \sim_H a$. Po Definiciji 16 slijedi da je $a^{-1}a' \in H$, odnosno postoji $h \in H$ za koji je $a^{-1}a' = h$. Ta jednakost pomnožena slijeva s a daje izraz $a' = ah$ pa je

$$\Phi(a'H) = \varphi(a') = \varphi(ah) = \varphi(a)\varphi(h) = \varphi(a)e_{G_2} = \varphi(a) = \Phi(aH).$$

Time je pokazano da je preslikavanje Φ ispravno definirano.
Pokažimo da je Φ homomorfizam grupa: za $aH, bH \in G_1/Ker\varphi$, $a, b \in G_1$ vrijedi:

$$\Phi((aH)(bH)) = \Phi(abH) = \varphi(ab) = \varphi(a)\varphi(b) = \Phi(aH)\Phi(bH).$$

Za kraj preostaje dokazati da je preslikavanje Φ bijekcija.
Φ je očito surjektivno preslikavanje. Neka je $c \in Im\varphi$. Tada postoji $a \in G_1$ za koji vrijedi da je $c = \varphi(a)$. Zbog načina na koji smo definirali preslikavanje Φ vrijedi $c = \Phi(aH)$.
Lako se pokaže da je Φ injekcija. Neka su $aH, bH \in G_1/Ker\varphi$, $a, b \in G_1$, takvi da je

$$\Phi(aH) = \Phi(bH) \Longrightarrow \varphi(a) = \varphi(b).$$

Sada množenjem obje strane jednakosti slijeva s $\varphi(b)^{-1} = \varphi(b^{-1})$ dobije se:

$$\varphi(b^{-1}a) = e_{G_2}.$$

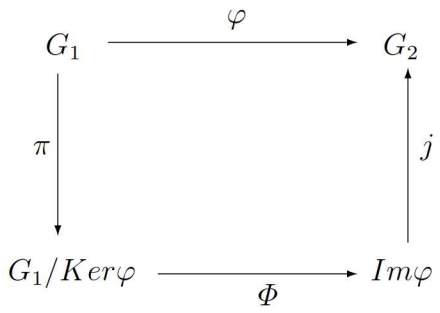
Tada je $b^{-1}a \in Ker\varphi$, tj. $b^{-1}a \in H$ te je $a \sim_H b$ i $aH = bH$. Kako smo pokazali da je preslikavanje Φ dobro definirano i da je bijektivni homomorfizam grupa, zapravo smo pokazali da je Φ izomorfizam kvocijentne grupe $G_1/Ker\varphi$ na grupu $Im\varphi$. □

Sažmimo Prvi teorem o izomorfizmu:

- $\varphi\colon G_1 \to G_2$ homomorfizam grupa,

- $\pi\colon G_1 \to G_1/Ker\varphi$ kanonski epimorfizam grupa,
- $\Phi\colon G_1/Ker\varphi \to Im\varphi \leq G_2$ izomorfizam kvocijentne grupe na grupu $Im\varphi$,
- $j\colon Im\varphi \to G_2$ inkluzija.

Navedimo da je u Teoremu 10 domena preslikavanja π bila G, a kodomena preslikavanja π bila je G/H. Ovdje smo radi konzistentnosti koristili druge oznake. Zapravo, ova četiri navedena preslikavanja međusobno djeluju na sljedeći način: $j \circ \Phi \circ \pi = \varphi$. Idući dijagram sadrži ideju Prvog teorema o izomorfizmu:



Taj dijagram je komutativan jer smo naveli da je $j \circ \Phi \circ \pi = \varphi$.

Primjer 15. *Skup $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ je grupa nenul realnih brojeva uz operaciju množenja i skup $\mathbb{R}^+$ je grupa pozitivnih realnih brojeva uz operaciju množenja. Tada definiramo preslikavanje $\varphi\colon \mathbb{R}^* \to \mathbb{R}^+$ s*

$$\varphi(x) = |x|.$$

Provjerimo je li preslikavanje φ homomorfizam grupa. Za $x, y \in \mathbb{R}^*$ vrijedi:

$$\varphi(xy) = |xy| = |x||y| = \varphi(x)\varphi(y),$$

te zaključujemo da je preslikavanje φ homomorfizam grupa. Idući korak je da odredimo jezgru homomorfizma φ. Dakle, trebamo pronaći sve $x \in \mathbb{R}^*$ za koje vrijedi

$$\varphi(x) = |x| = 1.$$

Rješavanje jednadžbe $|x| = 1$ daje dvije moguće vrijednosti za x: $x = 1$ i $x = -1$. Time smo došli do jezgre homomorfizma koja je

$$Ker\varphi = \{1, -1\}.$$

Sada odredimo sliku homomorfizma φ. Za sve $x \in \mathbb{R}^*$, funkcija $\varphi(x) = |x|$ uvijek će davati pozitivan realan broj. Stoga je slika homomorfizma φ skup pozitivnih realnih brojeva, odnosno $Im\varphi = \mathbb{R}^+$. Iz Prvog teorema o izomorfizmu slijedi:

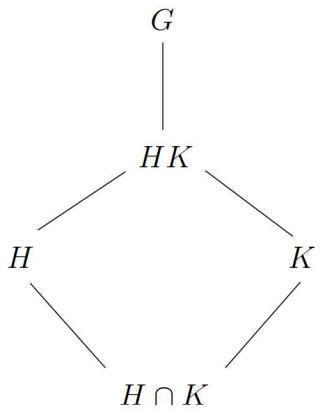
$$\mathbb{R}^*/\{1, -1\} \simeq \mathbb{R}^+.$$

Navedimo još Drugi i Treći teorem o izomorfizmu, pri čemu se Drugi teorem o izomorfizmu naziva i Dijamantni teorem o izomorfizmu, dok je Treći teorem o izomorfizmu poznat kao Teorem o dvostrukom kvocijentu.

Teorem 12. ([1, Chapter 5, 2.3 Theorem]) (Drugi teorem o izomorfizmu) *Neka je G grupa i neka su H i K njezine podgrupe. Neka je $K \trianglelefteq G$. Tada je*

$$H/(H \cap K) \simeq HK/K.$$

Sljedeći dijagram koristan je za vizualizaciju Drugog teorema o izomorfizmu, te je zbog izgleda dijagrama ovaj teorem dobio svoj specifičan naziv.



Navedimo i dokažimo teorem koji ćemo koristiti u dokazu Drugog teorema o izomorfizmu.

Teorem 13. ([1, Chapter 4, 3.5 Theorem]) *Neka su H i K podgrupe grupe G. Tada je skup*

$$HK = \{hk \colon h \in H, k \in K\}$$

podgrupa od G ako i samo ako je $HK = KH$.

Dokaz. Neka je $HK = KH$ i pokažimo da je $HK \leq G$. Kako je $e = ee \in HK$, skup HK je neprazan. Neka su $a, b \in HK$. Onda je $a = h_1k_1$ i $b = h_2k_2$, za neke $h_1, h_2 \in H$ i $k_1, k_2 \in K$. Stoga je

$$ab^{-1} = (h_1k_1)(h_2k_2)^{-1} = (h_1k_1)(k_2^{-1}h_2^{-1}) = h_1(k_1k_2^{-1})h_2^{-1} = h_1k_3h_2^{-1},$$

gdje je $k_3 = k_1k_2^{-1} \in K$. Sada je $k_3h_2^{-1} \in KH = HK$. Zbog toga je $k_3h_2^{-1} = h_3k_4$, za neke $h_3 \in H$ i $k_4 \in K$. Prema tome je

$$ab^{-1} = h_1h_3k_4 = h_4k_4,$$

gdje je $h_4 = h_1h_3 \in H$. Pokazali smo da je $ab^{-1} \in HK$ te je HK podgrupa od G.
Obratno, pretpostavimo da je HK podgrupa grupe G. Neka je $a \in KH$, onda je $a = kh$, za neki $h \in H$ i neki $k \in K$. Tada je $a^{-1} = h^{-1}k^{-1}$ element skupa HK te je $a \in HK$. Time je pokazano da je $KH \subseteq HK$. Na sličan način se pokazuje i druga inkluzija, tj. da je $HK \subseteq KH$ te se na kraju dobije $HK = KH$. □

Dokažimo sada Drugi teorem o izomorfizmu.

Dokaz. Nakon što smo dokazali da je $HK = KH$ podgrupa od G, dokažimo sada da je $K \trianglelefteq HK$. Pretpostavimo da je $k \in K$ i $a \in HK$. Želimo pokazati da je $aka^{-1} \in K$. Primjetimo da kako je $a \in HK$, onda je $a = hk_1$, za $h \in H, k_1 \in K$. Raspišimo sada čemu je jednako aka^{-1}:

$$aka^{-1} = (hk_1)k(k_1^{-1}h^{-1}) = h(k_1kk_1^{-1})h^{-1} = hk_2h^{-1},$$

gdje je $k_2 = k_1kk_1^{-1} \in K$. Tada je $aka^{-1} = hk_2h^{-1} \in K$ jer je $h \in G, k_2 \in K$ i $K \trianglelefteq G$. Tako smo pokazali da je K normalna podgrupa od HK.
Promotrimo sada preslikavanje $\varphi\colon H \to HK/K$ definirano s

$$\varphi(h) = hK, \ \forall h \in H.$$

Cilj je pokazati da je ovo preslikavanje surjektivno, tj. da je $Im\varphi = HK/K$ te da je $Ker\varphi = H \cap K$. Očigledno je da je φ homomorfizam grupa jer je

$$\varphi(ab) = (ab)K = (aK)(bK) = \varphi(a)\varphi(b).$$

Iduće što moramo pokazati jest surjektivnost preslikavanja φ. Pretpostavimo da je $aK \in HK/K$, odnosno $a \in HK$, a to nam pokazuje da je $a = hk$, za $h \in H$ i $k \in K$. Također primijetimo da imamo $aK = (hk)K = hK, \forall k \in K$ pa je sada $\varphi(h) = hK = aK$ te slijedi da je homomorfizam φ surjektivan.
Pokažimo čemu je jednaka jezgra homomorfizma φ:

$$Ker\varphi = \{h \in H\colon \varphi(h) = eK = K\}.$$

Neka je $h \in H$ element jezgre homomorfizma φ, a kako je $\varphi(h) = hK$, onda imamo $hK = K$ i $h \in K$. Dakle, $h \in H \cap K$ i $Ker\varphi \subseteq H \cap K$. Zapravo trebamo pokazati jednakost, a to ćemo napraviti dokazivanjem druge inkluzije. Pretpostavimo da je $a \in H \cap K$, a to znači da je $a \in H$ i $a \in K$ iz čega je $aK = K$, odnosno $\varphi(a) = K$ pa nam to na kraju govori da je $a \in Ker\varphi$. Pokazali smo da je $H \cap K \subseteq Ker\varphi$. Iz obje inkluzije dobivamo da je jezgra homomorfizma φ jednaka $H \cap K$. Sada primjenom Prvog teorema o izomorfizmu dobivamo:

$$H/(H \cap K) \simeq HK/K.$$

□

Teorem 14. ([1, Chapter 5, 2.4 Theorem]) (Treći teorem o izomorfizmu) *Neka su H i K normalne podgrupe grupe G i neka je $K \subseteq H$. Tada je*

$$(G/K)/(H/K) \simeq G/H.$$

Dokaz. Neka je definirano preslikavanje $\varphi\colon G/K \to G/H$ s

$$\varphi(gK) = gH.$$

Trebamo provjeriti je li preslikavanje φ dobro definirano. Pretpostavimo da je $gK = g'K$. Onda je $g^{-1}g' \in K$, a kako je u iskazu teorema navedeno da je $K \subseteq H$ slijedi da je $g^{-1}g' \in H$. Iz toga dobivamo $gH = g'H$ i preslikavanje φ je dobro definirano. Jednostavno se pokaže da je preslikavanje φ homomorfizam jer za sve $g, g' \in G$ vrijedi

$$\varphi((gK)(g'K)) = \varphi(gg'K) = (gg')H = (gH)(g'H) = \varphi(gK)\varphi(g'K).$$

Pokažimo da je to preslikavanje i surjekcija. Očito je

$$Im\varphi = \{gH : gK \in G/K\} = \{gH : g \in G\} = G/H.$$

Jezgra homomorfizma φ dana je s

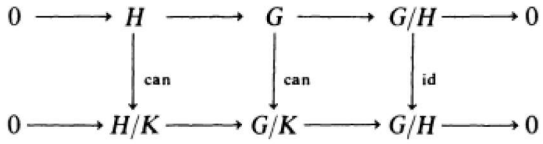
$$Ker\varphi = \{gK : gH = H\} = \{gK : g \in H\} = H/K.$$

Sada, primjenom Prvog teorema o izomorfizmu slijedi:

$$(G/K)/(H/K) \simeq G/H.$$

□

I ovdje također imamo komutativni dijagram kod kojeg su redovi egzaktni:



Slika 4: Komutativni dijagram, Izvor ([9])

Primjer 16. *Promotrimo grupu* $\mathbb{Z}$ *i njezine podgrupe* $12\mathbb{Z}$ *i* $6\mathbb{Z}$. *Uočimo da je* $12\mathbb{Z} \subseteq 6\mathbb{Z}$. *Navedene podgrupe su normalne podgrupe grupe* $\mathbb{Z}$ *jer je* $\mathbb{Z}$ *Abelova grupa. U Primjeru 14 pokazali smo da je* $\mathbb{Z}/n\mathbb{Z}$ *kvocijentna grupa. Koristeći Treći teorem o izomorfizmu možemo vidjeti da je*

$$(\mathbb{Z}/12\mathbb{Z})/(6\mathbb{Z}/12\mathbb{Z}) \simeq \mathbb{Z}/6\mathbb{Z}.$$

Sljedeći terem pokazuje da je direktan produkt dviju kvocijentnih grupa izomorfan kvocijentnoj grupi.

Teorem 15. ([1, Chapter 5, 2.5 Theorem]) *Neka su* G_1 *i* G_2 *grupe i neka je* $K_1 \trianglelefteq G_1$, $K_2 \trianglelefteq G_2$. *Tada je*

$$(G_1 \times G_2)/(K_1 \times K_2) \simeq (G_1/K_1) \times (G_2/K_2). \tag{5}$$

Dokaz. Promotrimo preslikavanje $\varphi : G_1 \times G_2 \to (G_1/K_1) \times (G_2/K_2)$ dano s

$$\varphi(g_1, g_2) = (g_1K_1, g_2K_2).$$

Može se jednostavno dokazati da je preslikavanje φ surjektivni homomorfizam grupa i da je $Ker\varphi = K_1 \times K_2$. Tada rezultat (5) slijedi po Prvom teoremu o izomorfizmu. □

Literatura

[1] P.B. BHATTACHARYA, S.K. JAIN, S.R. NAGPAUL, *Basic abstract algebra, second ed.*, Cambridge University Press, Cambridge, 1995.

[2] D. BRAJKOVIĆ, *Algebra kroz primjere, priručnik za vježbe*, Sveučilište J.J. Strossmayera u Osijeku, Odjel za matematiku, 2018, web izvor dostupan na `https://www.mathos.unios.hr/images/uploads/774.pdf`

[3] D.S. DUMMIT, R.M. FOOTE, *Abstract algebra-3th ed.*, John Wiley & Sons, Inc., Hoboken, New Jersey, 2004.

[4] J.R. DURBIN, *Modern Algebra An Introductionn-6th ed.*, John Wiley & Sons, Inc., Hoboken, New Jersey, 2009.

[5] N. GRBAC, V.M. CRNKOVIĆ, *Algebarske strukture-prva verzija skripte*, Sveučilište u Rijeci, Fakultet za matematiku, ak. god. 2010-2011, web izvor dostupan na `https://www.math.uniri.hr/~ngrbac/alg_str_web.pdf`

[6] K. HORVATIĆ, *Linearna algebra*, Golden marketing - Tehnička knjiga, Zagreb, 2004.

[7] T.W. HUNGERFORD, *Algebra*, Springer-Verlag New York, Inc., New York, 1974.

[8] H. KRALJEVIĆ, Algebra, Sveučilište J.J. Strossmayera u Osijeku, Odjel za matematiku, 2007, web izvor dostupan na `https://web.math.pmf.unizg.hr/~hrk/nastava/2006-07/algebra_Osijek_2006_7.pdf`

[9] S. LANG, *Algebra*, Springer-Verlag New York, Inc., New York, 2002.

[10] I. MATIĆ, Predavanja iz kolegija Algebra, Sveučilište J.J. Strossmayera u Osijeku, Odjel za matematiku, ak. god. 2019-2020, web izvor dostupan na `https://www.mathos.unios.hr/images/homepages/imatic/Algebra_predavanja.pdf`

Sažetak

U ovom radu definirali smo pojmove grupoida, monoida, grupe i podgrupe te naveli važne tvrdnje vezane uz njih. Upoznali smo se s pojmom Abelove grupe, pokazali kako odrediti podgrupu grupe i definirali pojmove homomorfizma, monomorfizma, epimorfizma i izomorfizma grupe. Definirali smo normalne podgrupe, naveli primjere i važne teoreme, a najvažniji među njima je Lagrangeov teorem. Uz to smo uveli i objasnili pojmove centralizatora i normalizatora skupa u grupi te centra grupe. Na kraju smo rekli nešto o kvocijentnim grupama, komutativnom dijagramu, egzaktnom nizu te o Prvom, Drugom i Trećem teoremu o izomorfizmu.

Ključne riječi

grupoid, monoid, grupa, podgrupa, normalna podgrupa, kvocijentna grupa, Lagrangeov teorem, Prvi teorem o izomorfizmu, Drugi teorem o izomorfizmu, Treći teorem o izomorfizmu

Normal Subgroups and Quotient Groups

Summary

In this thesis, we have defined the concepts of groupoid, monoid, group and subgroup and stated important claims related to them. We were acquainted with the concept of Abelian group, showed how to determine a subgroup of a group and defined the concepts of group homomorphism, monomorphism, epimorphism and isomorphism. We have defined normal subgroups, given examples and important theorems, the most important of which is Lagrange's theorem. In addition, we introduced and explained the concepts of the centralizer and normalizer of a set in a group and center of a group. Finally, we said something about quotient groups, commutative diagram, exact sequence and about the First, Second and Third isomorphism theorem.

Keywords

groupoid, monoid, group, subgroup, normal subgroup, quotient group, Lagrange's theorem, First isomorphism theorem, Second isomorphism theorem, Third isomorphism theorem

Životopis

Rođena sam 5. studenog 1997. godine u Požegi. Pohađala sam Osnovnu školu fra Kaje Adžića u Pleternici. Po završetku osnovne škole 2012. godine upisala sam Opću gimnaziju u Požegi koju završavam 2016. godine. Te godine upisujem preddiplomski studij matematike u Osijeku na Odjelu za matematiku tj. današnjem Fakultetu primijenjene matematike i informatike na Sveučilištu J.J. Strossmayera. Sveučilišna prvostupnica matematike postajem 2020. godine s temom završnog rada *Jacobijeva i Gauss-Seidelova metoda za rješavanje sustava linearnih jednadžbi* pod mentorstvom izv. prof. dr. sc. Tomislava Marošević. Na istom fakultetu upisala sam diplomski studij matematike, smjer Financijska matematika i statistika. Tijekom diplomskog studija obavila sam stručnu praksu u PPD d.o.o. u Odjelu za upravljanje portfeljom u Vukovaru. Također, bila sam zaposlena na poziciji nastavnice matematike u srednjoj školi za primjenjenu umjetnost i dizajn u Osijeku te u osnovnoj školi Augusta Šenoe u Osijeku.