U N I V E R Z A V M A R I B O R U

FAKULTETA ZA NARAVOSLOVJE IN MATEMATIKO
Oddelek za matematiko in računalništvo

Diplomsko delo

UVOD V TEORIJO GRUP

Mentor:
dr. Daniel Eremita,
docent

Kandidat:
Matej Kovačec

Maribor, 2008

ZAHVALA

Zahvaljujem se mentorju dr. Danielu Eremiti za pomoč in vodenje pri nastajanju diplomskega dela.

Posebna zahvala velja tudi staršem in mojemu dekletu, ki so mi v času študija stali ob strani in me podpirali.

U N I V E R Z A V M A R I B O R U

FAKULTETA ZA NARAVOSLOVJE IN MATEMATIKO
Koroška cesta 160
2000 Maribor

I Z J A V A

Podpisani *Matej Kovačec*, rojen 27.10. 1981, študent Fakultete za naravoslovje in matematiko Univerze v Mariboru, smer matematika in zgodovina, izjavljam, da je diplomsko delo z naslovom ***Uvod v teorijo grup*** pri mentorju *doc. dr. Danielu Eremiti*, avtorsko delo. V diplomskem delu so uporabljeni viri in literatura korektno navedeni; teksti niso prepisani brez navedbe avtorjev.

Maribor, 2008

PROGRAM DIPLOMSKEGA DELA

Diplomsko delo naj obravnava osnove teorije grup. Obravnava naj bo podkrepljena z različnimi primeri grup.

Osnovna literatura:

J. F. Humphreys, A course in group theory, Oxford University Press, 1997.

doc. dr. Daniel Eremita

Maribor, 2007

POVZETEK

V diplomskem delu je predstavljen uvod v teorijo grup. V prvem poglavju so predstavljene osnovne definicije ter nekaj osnovnih primerov grup. V naslednjem poglavju se osredotočimo na lastnosti grup, ki sledijo iz že omenjenih definicij. V tretjem poglavju obravnavamo podgrupe ter njihove lastnosti. Sledi poglavje, v katerem se ukvarjamo z odseki in dokažemo Lagrangeov izrek. V petem poglavju predstavimo pojem podgrupe edinke in vpeljemo pojem kvocientne grupe. Nato obravnavamo preslikave med grupami, ki ohranjajo grupno operacijo. Sledi izrek o homomorfizmih, medtem ko v sklepnem poglavju predstavimo permutacije.

Ključne besede: grupa, Abelova grupa, podgrupa, red grupe, podgrupa edinka, odsek, Lagrangeov izrek, homomorfizem, izrek o homomorfizmih, permutacija.

ABSTRACT

In this diploma the introduction to the theory of groups is presented. In the first chapter, basic definitions and some basic examples of groups are presented. In the following chapter, we focus on certain properties of groups that follow from already mentioned definitions. In the third chapter, subgroups and their properties are studied. Further, cosets are studied and Lagrange's Theorem is proven. In the fifth chapter, the notion of a normal subgroup is presented and it is also shown how that subgroup is used for construction of quotient groups. Then we consider maps between groups which preserve group operation. Connection between that notion and quotient groups are presented in The Homomorphism Theorem. In concluding chapter we consider permutations of a finite set X ,is studied.

Key words: group, abelian group, subgroup, order of a group, normal subgroup, coset, Lagrange's Theorem, homomorphism, The Homomorphism Theorem, permutation.

Math. Subj. Class. (2000): 20A05, 20B05.

KAZALO

1 UVOD

Definicija 1.1 *Grupa je množica G z binarno operacijo ∘, ki zadošča naslednjim pogojem:*

(G1) za vsak par $g,h \in G,\ g \circ h \in G$;

(G2) za vse elemente $g,h,k \in G$ *velja,* $g \circ (h \circ k) = (g \circ h) \circ k$;

(G3) obstaja tak element $e \in G$, *da je* $g \circ e = e \circ g = g$ *za vsak* $g \in G$;

(G4) za vsak $g \in G$ *obstaja tak* $g^* \in G$, *da je* $g \circ g^* = g^* \circ g = e$.

Opomba 1.2 *Element e imenujemo enota grupe, medtem ko element* g^* *imenujemo inverz (oz. invezni element) elementa g.*

Definicija 1.3 *Grupa G je neskončna, če je število elementov v množici G neskončno, v nasprotnem primeru je grupa končna.*

Definicija 1.4 *Grupa G je Abelova, če za vsak* $g,h \in G$ *velja (zakon komutativnosti)* $g \circ h = h \circ g$.

V tem kontekstu je termin 'Abelova' veliko pogostejši kot pa 'komutativna'. Abelove grupe so dobile ime po norveškem matematiku Nielsu Henrik Abelu (*1802 +1829).

Primer 1.5 Naj bo *G* množica celih števil **Z** in operacija ∘ naj bo operacija seštevanja +. Potem množica **Z** skupaj z operacijo + zadošča zgoraj naštetim štirim aksiomom, če vzamemo za element *e* (G3) število 0, in za element g^* (G4) vzamemo negativno število *–g*. Dejansko je to neskončna Abelova grupa, saj za operacijo + v množici celih števil **Z** velja, da je komutativna. Tudi množica racionalnih števil **Q**, množica realnih števil **R** in množica kompleksnih števil **C**, so Abelove grupe za običajne operacije seštevanja.

Primer 1.6 Če uporabimo operacijo množenja v množici **Z** vidimo, da prvi trije aksiomi držijo pod pogojem, da si za *e* izberemo število 1. Četrti aksiom pa ne drži zaradi naslednjih dveh dejstev. Prvič, število 0 nima inverza, namreč ne obstaja nobeno

število 0^*, da bi veljalo $0 \circ 0^* = 1$. Drugič, za poljubno celo število $h \in Z$ ne obstaja tako celo število h^*, ki zadošča pogoju $h \circ h^* = 1$ (na primer, če je $h = 2$) . Če o operaciji množenja razmislimo tudi za množice števil **Q**, **R** in **C** vidimo, da v nobeni ne obstaja inverz števila nič, vendar obstaja za vsa ostala števila. Naj bo $\mathbf{Q}^\times = \mathbf{Q}\backslash\{0\}$, $\mathbf{R}^\times = \mathbf{R}\backslash\{0\}$ in $\mathbf{C}^\times = \mathbf{C}\backslash\{0\}$. Potem so $\mathbf{Q}^\times$, $\mathbf{R}^\times$, $\mathbf{C}^\times$ neskončne Abelove grupe za operacijo množenja.

Primer 1.7 Končne Abelove grupe lahko konstruiramo na naslednji način. Naj bo *n* naravno število večje od 1 in naj bo ω tako kompleksno število oblike $e^{2\pi i/n}$, da velja $\omega^n = 1$. Naj bo *G* množica različnih kompleksnih števil 1, ω,…, ω^{n-1}. Definirajmo operacijo grupe *G* s predpisom $\omega^j \omega^k = \omega^{j+k}$, ki je enaka operaciji množenja za kompleksna števila. Če preverimo aksiom (G1) vidimo, da tukaj ni vse očitno, saj moramo preveriti ali je ω^{j+k} element množice. Dokazati moramo, da ga lahko zapišemo kot eno od kompleksnih števil $1, \omega, ..., \omega^{n-1}$. Ker je $0 \le j,\ k \le n-1$, obstajata dve možnosti: ali je $j + k < n$, kar pomeni $\omega^{j+k} \in G$, ali $j + k > n - 1$, kar pomeni, da je $j+k$ oblike $n+t$ pri čemer je $t < n$. Ker je $\omega^n = 1$, sledi

$$\omega^j \omega^k = \omega^{j+k} = \omega^{n+t} = \omega^n \omega^t = \omega^t \in G .$$

Zlahka ugotovimo, da je 1 enota in ω^{n-j} inverz elementa ω^j. Ker je

$$\omega^j \omega^k = \omega^{j+k} = \omega^{k+j} = \omega^k \omega^j$$

sledi, da je *G* Abelova grupa. To je primer ciklične grupe. (glej Definicijo 3.11)

Primer 1.8 Naj bo $M_n(\mathbf{R})$ oznaka za množico matrik $n \times n$ z realnimi koeficienti. Ta množica je grupa za običajno seštevanje matrik. Izkaže se, da je enota *e* ničelna matrika(vsi členi so 0) in da je inverz matrike *X* matrika *–X*. Ta množica pa ni grupa za operacijo množenja matrik. To pa zaradi tega, ker je enota za množenje matrik identična matrika

$$I_n = \begin{pmatrix} 1\ 0\ .\ .\ .\ 0 \\ 0\ 1\ .\ .\ \ .0 \\ .\ .\ .\ .\ .\ . \\ .\ .\ .\ .\ .\ . \\ 0\ 0\ \ .\ .\ .1 \end{pmatrix}$$

Inverz za množenje matrike A je potem matrika A^{-1} v običajnem pomenu teorije matrik. Pogoj, da ima A inverzno matriko je ta, da ima A neničelno determinanto, kar pa pomeni, da niso vse matrike obrnljive. Podmnožica $GL(n,\mathbf{R})$ vseh obrnljivih elementov v $M_n(\mathbf{R})$ je grupa za operacijo množenja. Pri tem je enota $e = I_n$, inverz matrike X pa je inverzna matrika X^{-1}. Če zamenjamo množico **R** z drugim številskim obsegom kot je **Q** ali **C**, dobimo drugo grupo matrik za operacijo množenja. Označimo ju z $GL(n, \mathbf{Q})$ in $GL(n, \mathbf{C})$.

Primer 1.9 Naj bo G množica naslednjih 2×2 matrik:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ A = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},\ B = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},\ C = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Trdimo, da je G grupa za operacijo množenja matrik.
To trditev najlažje dokažemo tako, da zapišemo tabelo vseh možnih produktov.

	I	A	B	C
I	I	A	B	C
A	A	I	C	B
B	B	C	I	A
C	C	B	A	I

Iz tabele je razvidno, da drži aksiom (G1), saj je vsak produkt element množice G. Prav tako lahko vidimo, da je I enota in da je vsak od I, A, B in C sam svoj inverz. S to tabelo smo preverili vse aksiome grupe, razen aksioma (G2). Drži pa da je množenje matrik asociativno, zato je temu aksiomu avtomatsko zadoščeno.

Primer 1.10 Naj bosta G in H grupi, sedaj pa pokažimo kako v splošnem konstruiramo novo grupo in podanih dveh. Direktni produkt grup G in H je množica urejenih parov

$$G \times H = \{(g,\ h) : g \in G,\ h \in H\},$$

skupaj z operacijo

$$(g_1,\ h_1) \circ (g_2,\ h_2) = (g_1 \circ_G g_2,\ h_1 \circ_H h_2)$$

pri čemer sta $\circ_G$ in $\circ_H$ oznaki operaciji grup G in H. Da je $G \times H$ grupa za operacijo $\circ$ zlahka dokažemo. Če je $G = H = C_2 = \{1,\ -1\}$, potem ima $G \times H$ štiri elemente $(1,\ 1)$, $(1,\ -1)$, $(-1,\ 1)$ in $(-1,\ -1)$ in naslednjo multiplikacijsko tabelo:

	$(1, 1)$	$(1, -1)$	$(-1, 1)$	$(-1, -1)$
$(1, 1)$	$(1, 1)$	$(1, -1)$	$(-1, 1)$	$(-1, -1)$
$(1, -1)$	$(1, -1)$	$(1, 1)$	$(-1, -1)$	$(-1, 1)$
$(-1, 1)$	$(-1, 1)$	$(-1, -1)$	$(1, 1)$	$(1, -1)$
$(-1, -1)$	$(-1, -1)$	$(-1, 1)$	$(1, -1)$	$(1, 1)$

Opomba 1.11 *Od tega poglavja dalje bomo v večini primerov za grupe uporabljali multiplikativen zapis. Tako bomo zapis* $x \circ y$ *nadomestili z xy. Prav tako zapišemo enoto grupe G z 1 (v primerih, kjer bi lahko prišlo do zmede zaradi oznake 1, uporabljamo za oznako enote grupe G tudi oznaki* 1_G *ali e) in inverz elementa g zapišemo kot* g^{-1}*. S temi oznakami potem aksiomi grupe izgledajo takole:*

(G1) za vsak par $x, y \in G$, $xy \in G$,

(G2) za vse elemente x, y, $z \in G$ *velja,* $(xy)z = x(yz)$*;*

(G3) obstaja tak element $1 \in G$*, da za vsak* $g \in G$ *velja,*

$$1g = g = g1,$$

(G4) za vsak $g \in G$ *obstaja tak* $g^{-1} \in G$*, da je* $gg^{-1} = 1 = g^{-1}g$.

Če je G Abelova grupa, potem je včasih primerneje uporabiti aditivni zapis, v katerem je operacija grupe zapisana s +, enota grupe z 0 in inverz elementa g z –g.

2 Lastnosti grup

V tem poglavju bomo preučili nekaj logičnih posledic aksiomov grupe. Na primer, če imamo podano grupo *G*, nam tretji aksiom zagotavlja obstoj enote v grupi *G*. V tem aksiomu ni ničesar kar preprečuje, da bi grupa imela več kot eno enoto. V nadaljevanju bomo pokazali, da to ni možno.

Trditev 2.1 *Enota grupe je enolično določena.*

Dokaz. Predpostavimo, da sta 1 in *e* enoti grupe *G*. Potem za vsak $g \in G$ velja,

$$1g = g = g1 \text{ in } eg = g = ge .$$

V prvo vstavimo $g = e$, v drugo pa $g = 1$ in dobimo $1e = e = e1$ ter $e1 = 1 = 1e$ od tod pa sledi, da je $1 = e$. □

Trditev 2.2 *Inverzni element vsakega elementa v grupi je enolično določen.*

Dokaz. Recimo, da je *g* element grupe *G*. Če sta g^* in g^{-1} oba inverzna elementa elementa *g*, potem to pomeni

(1) $$gg^* = 1 = g^*g$$

in

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

Od tod sledi

$$\begin{aligned} g^*\left(gg^{-1}\right) &= g^*1 \\ &= g^* \text{ (po aksiomu (G3)).} \end{aligned}$$

Prav tako je

$$\begin{aligned} g^*\left(gg^{-1}\right) &= \left(g^*g\right)g^{-1} \text{ (po aksiomu (G2))} \\ &= 1g^{-1} \\ &= g^{-1} \text{ (po aksiomu (G3)).} \end{aligned}$$

S tem smo pokazali, da je $g^* = g^{-1}$. Kar pomeni, da obstaja enolično določen inverz poljubnega elementa *g* grupe *G*. □

Opomba 2.3 *Inverz elementa g bomo označevali z* g^{-1}.

Trditev 2.4 *Naj bosta a in b elementa grupe G. Potem obstajata enolično določena elementa* $x, y \in G$, *da velja* $ax = b$ *in* $ya = b$.

Dokaz. Dokazati je treba, da ima enačba $ax = b$ vsaj eno rešitev. Torej, da obstaja element *x*, ki zadošča pogoju $ax = b$. Poleg tega je treba pokazali, da obstaja natanko en tak element *x*. Najprej dokažimo enoličnost. Predpostavimo, da ima enačba dve rešitvi *x* in *z* tako, da velja

$$ax = b = az \ .$$

Po aksiomu (G4) ima element *a* inverz a^{-1}. Pomnožimo obe strani enakosti $ax = az$ na levi strani z a^{-1} in dobimo

$$a^{-1}(ax) = a^{-1}(az).$$

Sedaj uporabimo aksiom (G2) in dobimo

$$(a^{-1}a)x = (a^{-1}a)z \ .$$

Aksiom (G4) nam pove, da je $a^{-1}a = 1$, zato sledi $1x = 1z$. Z uporabo aksioma (G3) pa dobimo rezultat $x = z$, kar pomeni, da ima enačba $ax = b$ največ eno rešitev.

Sedaj dokažimo, da ima enačba vsaj eno rešitev. Zato pokažimo, da je element $x = a^{-1}b$ element G in da zadošča enakosti $ax = b$. Ker po predpostavki $a \in G$, po (G4) tudi $a^{-1} \in G$, tako po (G1) tudi $a^{-1}b \in G$. Prav tako pa je

$$\begin{aligned} ax = a(a^{-1}b) &= (aa^{-1})b \text{ po (G2)} \\ &= 1b \text{ po (G4)} \\ &= b \text{ po (G3).} \end{aligned}$$

Da obstaja tak enolično določen element *y*, da velja $ya = b$, dokažemo na podoben način. □

Posledica 2.5 *Naj bosta a in b elementa grupe G. Potem je inverz elementa ab enak* $b^{-1}a^{-1}$.

Dokaz. Obravnavajmo produkt

$$\begin{aligned} (ab)(b^{-1}a^{-1}) &= a(b(b^{-1}a^{-1})) \text{ po (G2)} \\ &= a((bb^{-1})a^{-1}) \text{ spet po (G2)} \\ &= a(1a^{-1}) \text{ po (G4)} \\ &= aa^{-1} \text{ po (G3)} \\ &= 1 \text{ po (G4).} \end{aligned}$$

Za vsak *g* iz *G* ima enačba $gx = 1$ eno samo rešitev. Vemo, da je g^{-1} rešitev te enačbe, tako nam argument zgoraj pokaže, da je inverz od *ab* resnično $b^{-1}a^{-1}$. □

Posledica 2.6 *Naj bo g element grupe G. Potem je inverz od* g^{-1} *enak g.*

Dokaz. Enačba

$$gg^{-1} = 1 = g^{-1}g$$

pravi, da je g^{-1} inverz od g, in tako je tudi g inverz od g^{-1}. □

Posledica 2.7 *Inverz od 1 je enak 1.*

Dokaz. $1^{-1} = 1$, ker je $1 = 1 \cdot 1$. □

Trditev 2.8 *(Pravilo krajšanja.) Naj bodo g, x, y elementi grupe G. Potem iz enačbe* $gx = gy$ *sledi da je* $x = y$. *Tudi iz enačbe* $xg = yg$ *sledi* $x = y$.

Dokaz. Enačbo $gx = gy$ pomnožimo na levi, enačbo $xg = yg$ pa na desni z elementom g^{-1}. V prvem primeru dobimo

$\left(g^{-1}g\right)x = \left(g^{-1}g\right)y$. Tako je $1x = 1y$, torej $x = y$.

V drugem primeru dobimo

$x\left(gg^{-1}\right) = y\left(gg^{-1}\right)$. Zato je $x1 = y1$, torej $x = y$. □

Definicija 2.9 *Naj bo g element grupe G. Definirajmo, da je* $g^0 = 1$, $g^1 = g$, g^2 *naj bo* gg, *in induktivno, za naravno število n naj bo* $g^n = gg^{n-1}$. *Če je n negativno celo število definiramo* g^n *kot inverz elementa* g^{-n}.

Trditev 2.10 *Naj bo g element grupe G in naj bosta r, s celi števili. Potem velja:*

(1) $g^r g^s = g^{r+s} = g^s g^r$,

(2) $\left(g^r\right)^s = g^{rs}$,

(3) $g^{-r} = \left(g^{-1}\right)^r = \left(g^r\right)^{-1}$, *kar pomeni, da je inverz od* g^r *enak* g^{-r}.

Dokaz. (1) Najprej bomo obravnavali primer, ko sta *r* in *s* naravni števili. V tem primeru bomo trditev (1) dokazali z indukcijo po *r*.

Če je $r = 1$, potem je po definiciji $gg^s = g^{1+s}$. Po indukcijski predpostavki je

$$g^r g^s = g^{r+s}.$$

Dokazati moramo, da izraz velja tudi za $r+1$. Poglejmo izraz $g^{r+1}g^s$:

$$g^{r+1}g^s = \left(gg^r\right)g^s = g\left(g^r g^s\right) = gg^{r+s} = g^{r+s+1}.$$

Sedaj obravnavajmo primer, ko je eno izmed števil *r* in *s* enako nič. Če je $r = 0$, potem je

$$g^0 g^s = 1g^s = g^s = g^{0+s}.$$

Dokaz za $s = 0$ je podoben.

Nadalje predpostavimo, da sta *r* in *s* negativni števili. Sedaj uporabimo definicijo negativne potence z negativnim eksponentom in ugotovitev, ki smo jo pokazali v prvem primeru. Tako je

$$\begin{aligned} g^r g^s &= \left(g^{-r}\right)^{-1}\left(g^{-s}\right)^{-1} \\ &= \left(g^{-s}g^{-r}\right)^{-1} \text{ po posledici 2.5} \\ &= \left(g^{-s-r}\right)^{-1}, \text{ ker sta } -r \text{ in } -s \text{ pozitivni števili} \\ &= \left(g^{-r-s}\right)^{-1}, \text{ ker } -r-s = -s-r \\ &= g^{r+s} \text{ po definiciji.} \end{aligned}$$

Ker je $r+s = s+r$, iz tega dokaza sledi, da je $g^r g^s = g^s g^r$.

Za zaključek tega dela dokaza nam je še ostala možnost, ko je eno izmed števil *r* in *s* pozitivno drugo pa negativno. Ker sta v obeh primerih dokaza podobna se bomo omejili na enega t.j., ko je $r > 0$ in $s < 0$. Sedaj obstajajo tri možnosti, ki jih moramo upoštevati.

(λ_1) $r+s > 0$. Po primeru, ko sta obe števili pozitivni,

$$g^{r+s}g^{-s} = g^{(r+s)-s} = g^r.$$

Ker je po definiciji g^{-s} inverz od g^s, lahko pomnožimo obe strani z g^s in dobimo $g^{r+s} = g^r g^s$ kot je zahtevano.

(λ_2) $r+s = 0$. V tem primeru je $s = -r$, tako da je g^s, po definiciji, inverz od g^r in tako je $g^r g^s = 1 = g^0$.

(λ_3) $r+s<0$. Uporabimo primer, ko sta obe števili pozitivni,

$$g^{-(r+s)}g^r = g^{-r-s+r} = g^{-s}.$$

Pomnožimo obe strani z g^{-r}, inverzom od g^r, in dobimo

$$g^{-(r+s)} = g^{-s}g^{-r}.$$

Sedaj vzemimo inverza obeh strani, da dobimo želeni rezultat.

$$\left.\begin{aligned}\left(g^{-(r+s)}\right)^{-1} &= \left(g^{-r-s}\right)^{-1} = g^{-(-r-s)} = g^{r+s} = g^r g^s \\ \left(g^{-s}g^{-r}\right)^{-1} &= \left(g^{-s}\right)^{-1}\left(g^{-r}\right)^{-1} = g^s g^r\end{aligned}\right\} \Rightarrow g^r g^s = g^s g^r$$

(2) Tudi tukaj bomo najprej obravnavali primer, ko sta *r* in *s* naravni števili. V tem primeru bomo trditev (2) dokazali z indukcijo po *r*.

Če je $r=1$, potem je po definiciji $g^s = g^s$. Po indukcijski predpostavki je $\left(g^r\right)^s = g^{rs}$.

Dokazati moramo, da izraz velja tudi za $r+1$. Poglejmo izraz $\left(g^{r+1}\right)^s$:

$$\left(g^{r+1}\right)^s = \left(g^r g\right)^s = \left(g^r\right)^s g^s = g^{rs}g^s = g^{rs+s} = g^{(r+1)s}.$$

Sedaj obravnavajmo primer, ko je eno izmed števil *r* in *s* enako nič. Če je $r=0$, potem je

$$\left(g^0\right)^s = 1^s = 1 = g^{0s}.$$

Če je $s=0$, potem je $\left(g^r\right)^0 = 1 = g^{r0}$.

Nadalje predpostavimo, da sta r in s negativni števili. Tako je

$$\left(g^r\right)^s = \left(g^{-r}\right)^{-s}.$$

Za zaključek tega dela dokaza nam je še ostala možnost, ko je eno izmed števil *r* in *s* pozitivno, drugo pa negativno.

Če je $r>0$ in $s<0$ velja, da je $rs<0$.

Če je $r<0$ in $s>0$ prav tako velja, da je $rs<0$.

Ker sta dokaza podobna se bomo omejili na primer (a)

$$\left(g^r\right)^{-s} = g^{-rs}$$

$$\left(\left(g^r\right)^{-s}\right)^{-1} = \left(g^{-rs}\right)^{-1}$$

$$\left(g^r\right)^s = g^{rs}.$$

Za dokaz trditve (3) najprej predpostavimo, da je *r* pozitiven, tako da je po definiciji $g^{-r} = \left(g^r\right)^{-1}$. Preprosta indukcija nam dokaže, da je $\left(g^{-1}\right)^r$ inverz od g^r. Če je $r=0$, potem je

$$g^{-r} = \left(g^{-1}\right)^r = \left(g^r\right)^{-1} = 1.$$

Če je r negativen, potem je *–r* pozitiven in spet lahko uporabimo indukcijo: ko je $r = -1$,

$$g^{-r} = g^1 = \left(g^{-1}\right)^{-1} = \left(g^{-1}\right)^r = \left(g^r\right)^{-1}.$$

Naj bo sedaj $-r > 1$ in predpostavimo, da je

$$g^{-r} = \left(g^{-1}\right)^r = \left(g^r\right)^{-1},$$

tako da je

$$\begin{aligned} g^{-r+1} &= g^{-r}g = \left(g^{-1}\right)^r g \\ &= \left(g^{-1}\right)^r \left(g^{-1}\right)^{-1} = \left(g^{-1}\right)^{r-1} \text{ z uporabo (1).} \end{aligned}$$

Prav tako je

$$\begin{aligned} g^{-r+1} &= \left(g^r\right)^{-1} g \text{ po indukcijski predpostavki} \\ &= \left(g^r\right)^{-1}\left(g^{-1}\right)^{-1} \\ &= \left(g^{-1}g^r\right)^{-1} \text{ po posledici 2.5} \\ &= \left(g^{r-1}\right)^{-1} \text{ z uporabo (1).} \end{aligned}$$

S čimer zaključimo dokaz. □

Definicija 2.11 *Naj bo g element grupe G. Red elementa g je najmanjše naravno število n, ki zadošča pogoju* $g^n = 1$. *Če ne obstaja nobeno tako naravno število n, potem rečemo, da je g element reda neskončno.*

Opomba 2.12 *V poljubni končni grupi ima vsak element nujno končni red. Da to vidimo, upoštevamo potence* $g, g^2, g^3, \ldots$ *in tako naprej za vsak element g končne grupe G. Ker so to vsi elementi grupe in grupa ima končno število elementov, mora ta seznam vsebovati ponavljajoče se elemente. Predpostavimo, da je* $g^r = g^s$ *za nek r in s, ker je* $r > s$. *Ker je inverz od* g^s *enak* g^{-s}, *sledi* $g^{r-s} = g^s g^{-s} = 1$. *Tako ima g končni red. Primer grupe z elementom neskončnega reda grupa GL(2,* ***R****). Namreč, če je* $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, *potem je* $A^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$. *To pomeni, da matrika A nima končnega reda.*

Opomba 2.13 *Če je g element reda n sledi, da je* g^{n-1} *inverz elementa g. Še več opišemo lahko, kdaj sta poljubni dve potenci istega elementa enaki.*

Trditev 2.14 *Naj bo g element reda n v grupi G. Potem je* $g^r = g^s$ *natanko tedaj, ko* $n|r-s$. *Tako je* $g^k = 1$ *natanko takrat, ko* $n|k$.

Dokaz. Predpostavimo, da *n* deli $r-s$. Tako je $r-s=nt$ za neko celo število *t*. Potem je

$$\begin{aligned} g^r = g^{s+nt} &= g^s g^{nt} \text{ po trditvi 2.10(1)} \\ &= g^s \left(g^n\right)^t \text{ po trditvi 2.10(2)} \\ &= g^s (1)^t \text{, ker je } g^n = 1 \\ &= g^s \text{, ker je } 1^t = 1. \end{aligned}$$

Obratno, predpostavimo, da je $g^r = g^s$. Po trditvi 2.10(3) je inverz od g^s enak g^{-s} in tako je

$$g^{r-s} = g^r g^{-s} = g^s g^{-s} = 1.$$

Sedaj zapišimo celo število $r-s$ v obliki $qn+t$ pri čemer je $0 \le t < n$. To sledi iz izreka o deljenju z ostankom: za poljubni celi števili *a* in *b*, pri čemer je $b > 0$, obstajata taki celi števili *c* in *d*, da je $a = cb + d$ in $0 \le d < b$. Potem dobimo

$$1 = g^{r-s} = g^{nq+t} = \left(g^n\right)^q g^t = 1^q g^t = g^t.$$

Ker je *n* najmanjše naravno število z lastnostjo $g^n = 1$ sledi, da je *t* enak 0. To pomeni, da $n|r-s$. □

3 Podgrupe

Definicija 3.1 *Naj bo* $(G,\circ)$ *grupa. Neprazni podmnožici H grupe G pravimo podgrupa grupe G, če je tudi* $(H,\circ)$ *grupa. Če je H podgrupa grupe G, bomo to označili s simbolom* $H \leq G$. *Če pa je H podgrupa grupe G in* $H \neq G$, *pišemo* $H < G$.

Trditev 3.2 *Naj bo H podmnožica grupe G. Naslednji pogoji so ekvivalentni:*

(1) H je podgrupa grupe G;

(2) H zadošča trem zahtevam:

(a) enota grupe G je tudi v H;

(b) če sta x in y iz H, potem je tudi xy;

(c) če je h iz H, potem je tudi h^{-1};

(3) H zadošča pogojema:

(i) enota grupe G je tudi v H;

(ii) če sta a in b v H , potem je tudi ab^{-1}.

Dokaz. Ekvivalenco teh izjav dokažemo na sledeč način:

(1) $\Rightarrow$ *(2)* Če je *H* podgrupa pomeni, da je neprazna in zadošča zahtevama (b) in (c). Prav tako ima *H* enoto 1_H. Zato je $1_H h = h = h1_H$ za vsak $h \in H$. Ker je vsak $h \in H$ hkrati tudi iz *G*, velja $h1_G = h$. Iz česar sledi

$$h1_G = h1_H$$

$$1_G = 1_H \text{ po trditvi 2.2.}$$

(2) $\Rightarrow$ *(3)* Pogoj *(i)* iz *(3)* in pogoj *(a)* iz *(2)* pravita, da je enota grupe *G* tudi v *H*, zato moramo samo pokazati zakaj drži *(ii)*. Naj bosta *a* in *b* iz *H*. Po *(c)* je $b^{-1} \in H$. Tako po *(b)* sledi $ab^{-1} \in H$.

(3) $\Rightarrow$ *(1)* Predpostavimo, da pogoja *(i)* in *(ii)* držita. Pokažimo, da je *H* podgrupa grupe *G*. Ker je H neprazna množica z enoto, kar nam zagotavlja (*i*), v njej velja asociativnostni zakon (G2). Naj bo *h* iz *H*. Uporabimo *(ii)* tako, da je $a = 1$ in $b = h$ in vidimo, da je tudi $h^{-1} \in H$. S tem smo pokazali, da drži tudi *(G4)*. Končno drži tudi lastnost *(G1)*, saj če sta *x* in *y* iz *H*, potem (kot smo že videli) sta tudi *x* in y^{-1} iz *H*. Sedaj ponovno uporabimo *(ii)*, tako da je $a = x$ in $b = y^{-1}$ in dobimo

$x\left(y^{-1}\right)^{-1} = xy \in H$. □

Opomba 3.3 *Da je podmnožica podgrupa, lahko preverimo samo z aksiomom (2) trditve 3.2.*

Opomba 3.4 *Dokaz trditve 3.2 nam pokaže, da vsaka podgrupa grupe G vsebuje enoto grupe G.*

Opomba 3.5 *Pogoja (a) iz (2) in (i) iz (3) smo vključili le zato, da zagotavljata nepraznost H. Če vemo, da je naša podmnožica neprazna, potem ta dva podatka postaneta odvečna. Na primer, če vsebuje H vsaj en element, potem z vpeljavo pogoja (ii) iz (3) in a = b pokažemo, da 1 je v H.*

Opomba 3.6 *Če je G končna grupa, po opombi 2.13 sledi, da je za vsak* $g \in G$, g^{-1} *tudi oblike* g^k *za neko naravno število k. Potem po opombi 3.5 sledi, da če je H taka podmnožica G, da je (i)' H neprazna in (ii)' za vsak* $x, y \in H$ *, velja* $xy \in H$ *, potem je H podgrupa G. Obratno, vsaka podgrupa H grupe G zadošča pogojema (i)' in (ii)'.*

Primer 3.7 Vrnimo se na primer 1.5 in 1.6. Zlahka opazimo, da je **Z** podgrupa **Q** in **Q** je podgrupa **R**. Iz definicije preprosto sledi, da je podgrupa podgrupe podgrupa. Tako dobimo verigo aditivnih Abelovih grup

$$\mathbf{Z} \leq \mathbf{Q} \leq \mathbf{R} \leq \mathbf{C},$$

in verigo multiplikativnih grup

$$\mathbf{Q}^{\times} \leq \mathbf{R}^{\times} \leq \mathbf{C}^{\times} \ .$$

Primer 3.8 Naj bo *SL*(*n*, **R**) množica vseh matrik z determinanto 1. Potem je *SL*(*n*, **R**) podgrupa grupe *GL*(*n*, **R**). To velja, ker ima enotska matrika determinanto enako 1; če imata matriki *X* in *Y* determinanto 1, potem jo ima tudi matrika *XY*; obstaja pa tudi inverzna matrika matrike z determinanto 1, ki pa ima prav tako determinanto enako 1.

Primer 3.9 Pokažimo, da je množica $n\mathbf{Z}$= { $nz \mid n \in \mathbf{N},\ z \in \mathbf{Z}$} podgrupa grupe **Z**.

Drži, da je $n\mathbf{Z} \subseteq \mathbf{Z}$. Preveriti bi še morali, če velja:

$$a,\ b \in n\mathbf{Z} \Rightarrow a \circ b^{-1} \in n\mathbf{Z},$$

vendar to sledi kar iz pogoja (3) (*ii*) trditve 3.2.

Zato iz pogoja (2) (b) trditve 3.2 sledi, da $nz \in \mathbf{Z}$. Kar pomeni, da je $n\mathbf{Z} \leq \mathbf{Z}$.

Trditev 3.10 *Naj bo I množica indeksov in naj bo* H_i *podgrupa grupe* G *za vsak* $i \in I$. *Potem je*

$$\bigcap H_i = \{g \in G \mid g \in H_i \text{ za vsak } i \in I\}$$

podgrupa grupe G.

Dokaz. Naj bo $K = \bigcap H_i$. Da pokažemo, da je K podgrupa moramo preveriti pogoj (2) iz trditve 3.2.

(a) Ker je vsak H_i podgrupa sledi, da je $1 \in H_i$ za vsak $i \in I$. Zato je 1 tudi v *K*.

(b) Predpostavimo, da $x, y \in K$. Potem, sta $x, y \in H_i$ za vsak *i*. Zato ker je H_i podgrupa, je $xy \in H_i$. Ker to velja za vsak *i* sledi $xy \in K$.

(c) Naj bo $h \in K$. Ker je $h \in H_i$ in je H_i podgrupa sledi $h^{-1} \in H_i$ za vsak $i \in I$. Zato je $h^{-1} \in K$. □

Definicija 3.11 *Naj bo X poljubna podmnožica grupe G. Presek vseh podgrup grupe G, ki vsebujejo množico X imenujmo podgrupa generirana z X in jo označimo z* $\langle X \rangle$. *Dejstvo, da je* $\langle X \rangle$ *podgrupa sledi iz trditve 3.10. Potemtakem je* $\langle X \rangle$ *najmanjša podgrupa grupe G, ki vsebuje X.*

Opomba 3.12 *Ko je* $X = \{x_1, \ldots, x_n\}$ *in so* $x_1, \ldots, x_n$ *elementi grupe G, potem namesto zapisa* $\langle \{ \} \rangle$ *uporabljamo kar zapis* $\langle \ \rangle$. *V primeru, ko X vsebuje samo en element iz G, recimo x, pravimo, da je grupa* $\langle x \rangle$ *ciklična. Tako podgrupa* $\langle x \rangle$ *sestoji iz vseh možnih potenc (pozitivne, negativne in nič) elementa x. V splošnem so elementi grupe* $\langle X \rangle$ *produkti potenc elementov množice X. Namreč grupa* $\langle X \rangle$ *vsebuje vse take produkte, in nadalje je množica vseh takih produktov podgrupa od G.*

Primer 3.13 Aditivna grupa celih števil **Z** je neskončna ciklična. Katerokoli naravno število m lahko zapišemo kot vsoto $1+1+\cdots+1$ $(m-krat)$; to je *m*-ta potenca elementa 1. Negativna cela števila so inverzi pozitivnih, oziroma negativne potence elementa 1. Tudi 0 je generirana z elementom 1: $0 = 1 + (-1) \in \mathbf{Z}$.

Primer 3.14 V primeru 1.7 smo videli, da je $\langle e^{2\pi i/n} \rangle$ ciklična podgrupa grupe **C** z *n* elementi.

Trditev 3.15 *Naj bo G grupa in g naj bo element grupe G. Če je g neskončnega reda, potem je* $\langle g \rangle$ *neskončna ciklična grupa. Če pa je g reda n, potem ima grupa* $\langle g \rangle$ *n elementov.*

Dokaz. Predpostavimo, da je *g* neskončnega reda. Recimo, da je $\langle g \rangle$ končna grupa, ki je sestavljena iz vseh možnih potenc elementa *g.* Torej sledi, da ima lahko končno število elementov le v primeru, če bi bili nekateri od teh enaki. Potem, če je $g^i = g^j$ in $i < j$, bi dosegli

$$g^{j-i} = g^{i-i} = g^0 = 1,$$

tako bi bil *g* končnega reda. Ker je to v nasprotju s predpostavko, zaključimo, da $\langle g \rangle$ ni končna grupa.

Če sedaj predpostavimo, da je *g* končnega reda *n*, potem po trditvi 2.14 sledi, da obstaja natanko *n* različnih elementov grupe G oblike g^i. To pomeni, da je $g^i = g^j$ natanko tedaj, ko $n \mid i - j$, takrat je tudi $g^{i-j} = 1$. Iz česar sledi, da ima grupa $\langle g \rangle$ *n* elementov.□

Trditev 3.16 *Ciklična grupa je Abelova.*

Dokaz. Naj bo grupa *G* generirana z elementom *g*. Zato je vsak element grupe *G* oblike g^i za nek *i*. Potemtakem, če sta *x* in *y* v *G*,obstajata taka *i* in *j*, da je $x = g^i$ in $y = g^j$. Potem je

$$\begin{aligned} xy &= g^i g^j = g^{i+j} \text{ po trditvi 2.10} \\ &= g^{j+i} = g^j g^i = yx. \end{aligned}$$

To pomeni, da je *G* Abelova grupa. □

Trditev 3.17 *Podgrupa ciklične grupe je ciklična grupa.*

Dokaz. Naj bo *G* ciklična grupa generirana z elementom g in recimo, da je *H* podgrupa grupe *G*. Ker je *H* podmnožica *G*, so vsi elementi *H* oblike g^k za nek $k \in Z$. Če je $H = \{1\}$, potem je *H* ciklična. Zato predpostavimo, da $H \neq \{1\}$ in izberemo tak element iz *H*, da je *k* je najmanjše možno pozitivno število. Sedaj naj bo g^s drug element grupe H. Uporabimo izrek o deljenju z ostankom in *s* zapišimo v obliki $qk + r$, kjer je $0 \leq r < k$. Potem sta g^s in $\left(g^k\right)^{-1} = g^{-k}$ v *H*, zato ker je *H* podgrupa, je tudi $g^s\left(g^{-k}\right)^q = g^{s-kq} = g^r$ v *H*. To je v nasprotju z definicijo *k*, razen v primeru, ko je $r = 0$, potem $k|s$. Pokazali smo, da je vsak element podgrupe *H* oblike $\left(g^k\right)^q$ za neko celo število *q*, tako da je *H* ciklična in generirana z g^k. □

Trditev 3.18 *Naj bo G končna ciklična grupa reda n. Če d|n potem obstaja natanko ena podgrupa grupe G z d elementi, označimo jo z* G_d. *Število elementov grupe G, ki zadoščajo pogoju* $x^d = 1$, *je d in natanko ti elementi so elementi podgrupe* G_d.

Dokaz. Naj bo grupa *G* generirana z *g*, in *g* naj bo reda *n*. Jasno je, da ima $g^{n/d}$ *d* različnih moči, tako ima $\left\langle g^{n/d} \right\rangle$ *d* elementov. Če bi bila *H* druga podgrupa reda *d*, po trditvi 3.16, bi *H* bila ciklična in generirana npr. z elementom *y*. Potem je $y = x^r$ za nek *r* in ker je *y* reda d vidimo, da je $x^{rd} = 1$. Potem, po trditvi 2.14, *n*|*rd*. Potemtakem je $kn = k(n/d)d = rd$ za nek *k*. Iz tega sledi, da je $r = k(n/d)$, od to pa, da *n/d*|*r*. To pomeni, da je *y* potenca elementa $g^{n/d}$, tako da je *H* podgrupa ciklične grupe $\left\langle g^{n/d} \right\rangle$. Ker sta obe grupi reda *d*, morata biti enaki.

Zgornji argument nam pokaže, da *x* zadošča enačbi $x^d = 1$ natanko tedaj, ko je *x* potenca elementa $g^{n/d}$. Iz česar sledi, da je d rešitev te enačbe. □

4 Odseki in Lagrangeov izrek

V tem poglavju bomo dokazali Lagrangeov izrek. Ta pomemben rezultat nam pove, da število elementov podgrupe končne grupe *G* deli število elementov grupe *G*. Najprej bomo vpeljali pojem odseka, na katerem temelji dokaz Lagrangeovega izreka.

Definicija 4.1 *Naj bo H podgrupa grupe G in naj bo g poljubni element grupe G. Levi odsek gH grupe G po podgrupi H je definiran kot množica elementov grupe, ki so oblike gh, kjer je h poljubni element grupe H:*

$$gH = \{gh : h \in H\}.$$

Opomba 4.2 *Desni odsek grupe G po podgrupi H definiramo analogno.*

Opomba 4.2 *Odsek* $1H$ *je preprosto podgrupa H. Še več, za vsak h iz grupe H je* $hH = H$ *, saj je H zaprta za operacijo množenja.*

Opomba 4.3 *Element g je v odseku gH, ker je* $g = g1$.

Primer 4.4 Naj bo *G* dihedralna grupa $D(3)$ reda 6, grupa simetrij enakostraničnega trikotnika. Potemtakem, ima grupa G obliko

$$G = \langle a,\ b \mid b^2 = 1 = a^3,\ ab = ba^{-1} \rangle.$$

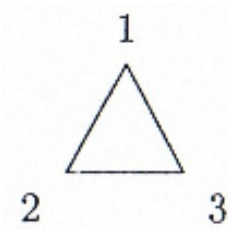
Ker ima *b* red 2 ima podgrupa $H = \langle b \rangle$ dva elementa. Šest elementov grupe *G* je $1,\ a,\ a^2,\ b,\ ba,\ ba^2$. Sedaj izračunamo šest možnih levih odsekov grupe *G* po podgrupi *H*:

$$\begin{aligned}
1H = 1\{1,\ b\} &= \{1,\ b\} = H;\\
bH = b\{1,\ b\} &= \{b,\ 1\} = H;\\
aH = a\{1,\ b\} &= \{a,\ ab\} = \{a,\ ba^2\};\\
a^2H = a^2\{1,\ b\} &= \{a^2,\ a^2b\} = \{a^2,\ ba\};\\
baH = ba\{1,\ b\} &= \{ba,\ bab\} = \{ba,\ a^2\};\\
ba^2H = ba^2\{1,\ b\} &= \{ba^2,\ ba^2b\} = \{ab,\ a\}.
\end{aligned}$$

Če dobro pogledamo vidimo, da so v resnici samo trije različni levi odseki, ker so ostali trije enaki temu:

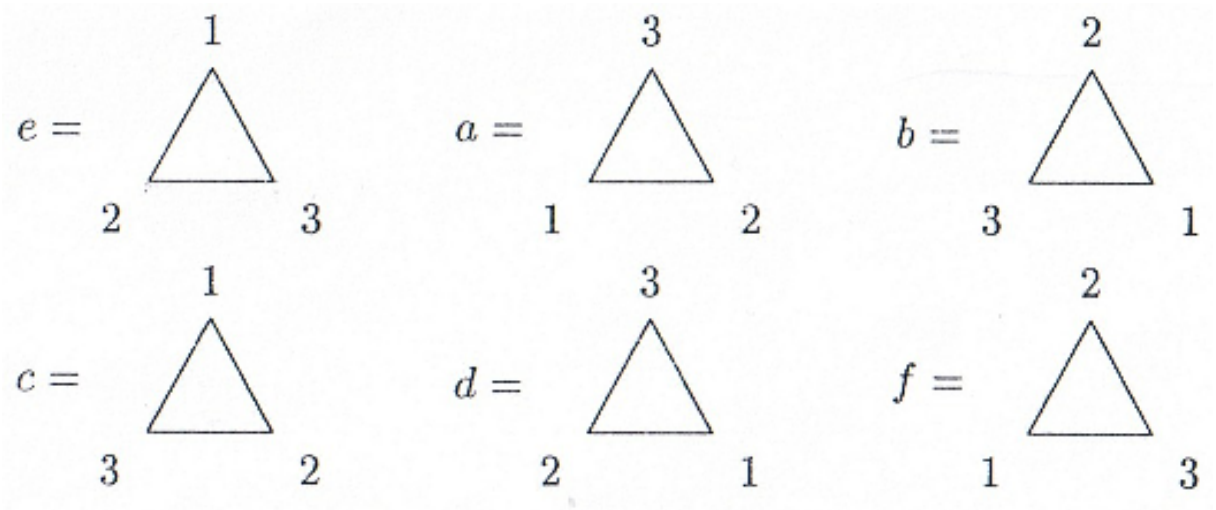
$$1H = bH;\ \ aH = ba^2H;\ \ a^2H = baH\ .$$

Primer 4.5 Preučili bomo grupo simetrij geometrijskih likov v ravnini. Elementi te grupe so transformacije ravnine, ki pustijo geometrijski lik nespremenjen. Ta pojem bomo predstavili v primeru, ko je geometrijski lik enakostranični trikotnik. Za poenostavitev poznejše diskusije, bomo točke trikotnika označili z naravnimi števili 1, 2 in 3.



Obstaja več transformacij ravnine, ki ohranijo enakostranični trikotnik. Na primer rotacija ravnine za 120° v nasprotni smeri urinega kazalca s središčem v težišču trikotnika. Potem ga lahko rotiramo še za nadaljnjih 120° , še ena taka rotacija pa trikotnik vrne v začetno stanje. Kar je enako, kot pa da sploh nebi vrteli, zato se imenuje identiteta. Naslednje tri simetrije so rezultat zrcaljenja trikotnika preko simetrale stranice. Iz tega sledi, da zrcaljenje preko simetrale stranice, s krajiščema 2 in 3, zamenja oglišči 2 in 3, medtem ko oglišče 1 ostaja fiksno. Potemtakem naslednjih šest simetrij predstavlja vse možne simetrije enakostraničnega trikotnika.

Označimo jih takole:



Na množici simetrij $\{e,\ a,\ b,\ c,\ d,\ f\}$ definirajmo naslednjo operacijo: za poljubna $x,\ y \in \{e,\ a,\ b,\ c,\ d,\ f\}$ naj bo $x \circ y$ simetrija, ki jo dobimo tako, da najprej uporabimo *y,* nato pa vpeljemo še *x*. Ker a označuje rotacijo za 120 stopinj in *c* označuje zrcaljenje čez nosilko višine na osnovnico, potem je $a \circ c$ zrcaljenje preko nosilke višine na stranico, ki jo omejujeta točki 1 in 2 (=*f*). Na podoben način lahko preverimo sledečo tabelo za operacijo $\circ$:

	e	*a*	*b*	*c*	*d*	*f*
e	*e*	*a*	*b*	*c*	*d*	*f*
a	*a*	*b*	*e*	*f*	*c*	*d*
b	*b*	*e*	*a*	*d*	*f*	*c*
c	*c*	*d*	*f*	*e*	*a*	*b*
d	*d*	*f*	*c*	*b*	*e*	*a*
f	*f*	*c*	*d*	*a*	*b*	*e*

Ta tabela preveri vsak aksiom grupe razen aksioma asociativnosti (*G2*). Vendar bomo v poglavju 3 pokazali, da je kompozicija transformacij asociativna in zato grupa.

Na podoben način lahko, za poljubno liho naravno število *n* $(n \geq 3)$, konstruiramo grupo simetrij pravilnih *n*-kotnikov. Izkaže se, da ima taka grupa 2*n* elementov (*n* rotacij in *n* zrcaljenj preko simetral stranic). Če pa je *n* sodo število, ima grupa simetrij pravilnega *n*-kotnika prav tako 2*n* elementov, *n* rotacij in *n* zrcaljenj preko simetrale stranice.

Ta grupa je poznana pod imenom grupa simetrij pravilnega *n*-kotnika in jo označimo z $D(n)$(uporabljata pa se tudi oznaki D_n ali pa D_{2n}). Kot bo razvidno iz poznejših poglavij, so lastnosti te grupe pogosto odvisne od *n*. Prav tako pa je mogoče simetrijo drugih oblik v ravnini in prav tako tri-dimenzionalnih predmetov.

Grupa simetrij enakostraničnega trikotnika je grupa D(3) in hkrati Abelova grupa s šestimi elementi.

Primer 4.6 Uporaben način določanja grupe *G* je z generatorji in relacijami podanimi pri predstavitvi grupe *G*. V tem primeru imamo podano listo takšnih generatorjev, ki se ujemajo s produkti moči teh generatorjev…

Na primer predstavitev $\langle a : a^n = 1 \rangle$ definira ciklično grupo z *n* elementi.

Kot naslednji primer, naj bo n naravno število in

$$G = \langle a, b : b^2 = 1 = a^n \ \wedge \ ab = ba^{-1} \rangle .$$

Jasno je, če hočemo, da je *G* grupa, potem mora vsebovati *n* moči elementa *a*, skupaj z elementom *b* in produkt kot je $ba^i \ \ (0 \le i \le n-1)$. Prav tako mora vsebovati produkt $a^i b$. Enakost $a^i b = ba^{-i}$ dobimo po indukciji, saj velja, da de $ab = ba^{-1}$. Rešitev v eno smer je trivialna, saj je podana s samo relacijo. V nasprotno smer pa predpostavimo, da velja $a^i b = ba^{-i}$ potem iz tega sledi zahtevano

$a^{i+1}b = aa^i b = a(ba^{-i}) = ba^{-1}a^{-i} = ba^{-i-1}$.

Če hočemo pokazati, da sta elementa $\{a^i, ba^j : 0 \le i, j \le n-1\}$ zaprta za množenje, moramo upoštevati štiri različne primere:

(1) produkt elementov oblike a^i in a^j je a^{i+j} in ta pripada grupi *G* (po menjavi a^{i+j} z a^{i+j-n}, če je $(i+j) \ge n$);

(2) produkt elementov oblike ba^i in a^j je ba^{i+j} kar pripada grupi *G* (spet po menjavi a^{i+j} z a^{i+j-n}, če je $(i+j) \ge n$);

(3) produkt elementov oblike a^j in ba^i je ba^{-i+j} in ta pripada grupi *G* (po menjavi a^{-i+j} z a^{n-i+j}, če je $i > j$); in nazadnje

(4) produkt elementov oblike ba^i in ba^j je

$ba^i ba^j = bba^{-i}a^j = a^{-i+j}$,

ker je $b^2 = 1$ sledi, da ta produkt prav tako pripada grupi G (spet po menjavi a^{-i+j} z a^{n-i+j}, če je $i > j$).

To nam pokaže, da elementa $\{a^i, ba^j : 0 \le i, j \le n-1\}$ tvorita grupo.

Še vedno pa nam preostane problem za razmislek, kako mi lahko vemo, da nas več primerov relacij ne bo pripeljalo do nepričakovanega zaključka, kot je $a = 1$? Grupa $\langle w : w^2 = 1, \ w^3 = 1 \rangle$ vsebuje samo en element, zaradi relacije to pomeni $1 = w^3 = w^2 w = w$. Eden od načinov za dokaz, da ima naša grupa $2n$ različnih elementov je, da najdemo 'primer' zanjo. To lahko naredimo, ko je $n > 2$ z razlago

grupe kor simetrične grupe pravilnega *n*-stranega mnogokotnika, kjer *a* označuje $360/n$ -stopinjsko rotacijo v nasprotni smeri urinega kazalca in *b* označuje partikularne preslikave. Preprosto lahko preverimo, da simetrije zadoščajo relacija podanim za grupo *G*. Ker ima simetrija grupe *n* zrcaljenj in *n* rotacij, lahko vidimo, da ima zgoraj predstavljena grupa $2n$ elementov. Ta grupa je poznana pod imenom dihedralna grupa $D(n)$.

Definicija 4.7 *Relacija R na množici X je ekvivalenčna relacija na X, če R zadošča sledečim trem pogojem za vsak x, y, z iz X,*

(1) xRx (refleksivnost);

(2) če je xRy potem je yRx (simetričnost); in

(3) če je xRy in je yRz potem je xRz (tranzitivnost).

Trditev 4.8 *Naj bo H podgrupa grupe G. Potem je relacija R na G, definirana s predpisom*

$$xRy \;\Leftrightarrow\; x^{-1}y \in H\,,$$

ekvivalenčna relacija.

Dokaz. Preverimo tri zahteve na *R*, kot je podano v definiciji 4.7.

(1) Ker je *H* podgrupa, je tudi $x^{-1}x = 1_G$ v *H* za vsak $x \in H$. Zato je *xRx,* kar pokaže, da je relacija *R* refleksivna.

(2) Če je *xRy* potem $x^{-1}y \in H$. Ker je *H* podgrupa, velja

$y^{-1}x = \left(x^{-1}y\right)^{-1} \in H$.

Zato je *yRx*, kar pomeni, da je *R* simetrična.

(3) Če je *xRy* in *yRz*, potem sta $x^{-1}y$ in $y^{-1}z$ iz *H*. Tako je $x^{-1}z = \left(x^{-1}y\right)\left(y^{-1}z\right) \in H$, kar pomeni, da je *xRz*. Skratka relacija *R* je tranzitivna. □

Definicija 4.9 *Naj bo R ekvivalenčna relacija na množici X. Ekvivalenčni razred* $[x]_R$ *elementa x iz množice X je množica vseh elementov množice X , ki so v relaciji R z elementom x:*

$$[x]_R = \{y \in X \mid xRy\}.$$

Definicija 4.10 *Naj bo X neprazna množica. Pravimo, da je množica vseh nepraznih podmnožic množice X razbitje množice X, če je vsak element množice X v natanko eni podmnožici.*

Iz tega sledi, da je unija vseh podmnožic v razbitju množice *X* enaka množici *X*, medtem ko je presek poljubnih dveh podmnožic prazna množica.

Trditev 4.11 *Množica ekvivalenčnih razredov poljubne ekvivalenčne relacije na množici X je razbitje množice X.*

Dokaz. Najprej upoštevajmo, da je *R* refleksivna relacija (Definicija 4.5). Vsak element *x* iz *X* je v ekvivalenčnem razredu $[x]_R$ in tako je unija ekvivalenčnih razredov enaka množici *X*. Če je *z* v obeh $[x]_R$ in $[y]_R$, potem je *xRz* in *yRz*. Ker je R simetrična vidimo, da je *zRy*. Zaradi tranzitivnosti sedaj sledi, da je *xRy*. Potemtakem je $y \in [x]_R$. Torej *xRy* ter *yRx* in zato je $[x]_R = [y]_R$. □

Trditev 4.12 *Naj bo H podgrupa grupe G in naj bo R ekvivalenčna relacija iz trditve 4.8. Potem je ekvivalenčni razred elementa g iz G levi odsek gH.*

Dokaz. Najprej pokažimo, da je $[g]_R \subseteq gH$. Naj bo $x \in [g]_R$. Potem je $g^{-1}x = h$ za nek $h \in H$. Potemtakem je $x = gh$ in tako $x \in gH$.
Nasprotno pokažemo, da je vsak element odseka *gH* vsebovan v ekvivalenčnem razredu $[g]_R$. Naj bo $gh \in gH$. Potem je $g^{-1}(gh) = h \in H$ in tako je $gR(gh)$. Torej $gh \in [g]_R$. □

Posledica 4.13 *Naj bo H podgrupa grupe G. Potem sta dva leva odseka xH in yH grupe G po podgrupi H, enaka ali disjunktna. Namreč xH = yH drži natanko tedaj, ko je* $y^{-1}x \in H$. *Če sta xH in yH različna, potem je* $xH \cap yH$ *prazna množica. Vsak element grupe G pripada nekemu levemu odseku grupe G po podgrupi H.*

Dokaz. To sledi iz trditve 4.11 in trditve 4.12. □

Primer 4.14 Ta rezultat lahko predstavimo z uporabo primera 4.4. Ugotovili smo, da je

$$1H = bH, \quad aH = ba^2H, \quad a^2H = baH .$$

Te enakosti lahko sedaj izpeljemo tudi kot posledice sledečih dejstev

$$b^{-1}1 = b^{-1} \quad = \quad b \in H ;$$

$$\left(ba^2\right)^{-1} a = a^{-2}b^{-1}a \quad = \quad aba = b \in H \text{ ; in}$$

$$\left(ba\right)^{-1} a^2 = a^{-1}b^{-1}a^2 \quad = \quad a^2ba^2 = b \in H .$$

Primer 4.15 Naj bo G aditivna grupa celih števil $\mathbf{Z}$ in naj bo n poljubno naravno število. Za množico vseh večkratnikov števila n $n\mathbf{Z}=\{ nz \mid z \in \mathbf{Z} \}$ je jasno, da je podgrupa grupe $\mathbf{Z}$ (primer 3.9). Operacija grupe $n\mathbf{Z}$ je seštevanje, zato je enota grupe 0. Izberimo poljubno celo število k. Levi odsek grupe $\mathbf{Z}$ po podgrupi $n\mathbf{Z}$ v označimo s simbolom $k+n\mathbf{Z}$. Torej

$$k+n\mathbf{Z}= \{k+nz \mid n \in \mathbf{N},\ k,\ z \in \mathbf{Z}\}.$$

Trditev 4.16 *Naj bo H podgrupa grupe G. Za poljuben element g iz G, ostaja bijekcija* α *med H in gH.*

Dokaz. Definiramo preslikavo α iz H v gH po pravilu $\alpha(h) = gh$ za vsak $h \in H$. Da dokažemo bijektivnost preslikave α, moramo pokazati, da je injektivna in surjektivna.
Da pokažemo, da je α injektivna: predpostavimo, da za $x,\ y \in H$ velja $\alpha(x) = \alpha(y)$, tako da je $gx = gy$. Potem obe strani enakosti pomnožimo z g^{-1} z leve strani, iz česa dobimo $x = y$.
Da pokažemo da je α surjektivna: poljubni element odseka grupe G po podgrupi H je oblike gh za nek $h \in H$. Tako imamo $gh = \alpha(h)$. □

Opomba 4.17 Za vsako množico X, moč množice X zapišemo kot $|X|$. Ko je X končna grupa G, številu $|G|$ pravimo red grupe G. V tem zapisu nam trditev 4.16 pokaže, da če je H podgrupa grupe G, potem za vsak $g \in G$, velja $|H| = |gH|$.

Izrek 4.18 *(Lagrange) Naj bo G končna grupa in naj bo H podgrupa grupe G. Če je r število različnih levih (ali desnih) odsekov grupe G po podgrupi H, potem je* $r = \frac{|G|}{|H|}$.

Zato velja, da obe števili $|H|$ *in r delita* $|G|$.

Dokaz. Naj bo *G* končna grupa. Vsaka njena podgrupa je potem tudi končna grupa Prav tako je končno tudi število odsekov *aH*. Naj bo različnih odsekov *r*, in sicer

(*) $H,\ a_2H,\ a_3H,\ ...,\ a_rH$.

Na te odseke razpade grupa *G*. Tu smo vzeli $a_1 = e$ in dobili prvi odsek, ki je kar *H*. Moč grupe *G* zaznamujmo z *m*, moč podgrupe *H* pa z *n*. V vsakem odseku *aH* je prav toliko elementov, kolikor jih je v podgrupi *H*. V zaporedju (*) je *r* odsekov, vsak izmed njih vsebuje po *n* elementov in posamezni odseki nimajo skupnih elementov. Od tod sklepamo, da je v vseh odsekih zaporedja (*) ravno *nr* elementov. Ker drugih elementov v grupi *G* ni, je $m = nr$. To pomeni, da $|H|$ deli $|G|$. □

Definicija 4.19 *Število različnih levih odsekov grupe G po podgrupi H se imenuje indeks podgrupe H v G. Indeks označujemo z* $|H : G|$.

Primer 4.20 Kot preprosto aplikacijo tega rezultata, določimo vse podgrupe grupe $G = C_2 \times C_2$. Štiri elemente grupe G lahko zapišemo v obliki $(1,\ 1)$, $(x,\ 1)$, $(1,\ y)$, in $(x,\ y)$ (kjer je $x^2 = 1 = y^2$). Potem sta grupa G sama in podgrupa $\{(1,\ 1)\}$ podgrupi s štirimi oziroma enim elementom. Prav tako je jasno, da je edina podgrupa s štirimi elementi sama grupa G in da je edina podgrupa z enim elementom podgrupa $\{(1,\ 1)\}$. Po Lagrangeovem izreku red vsake druge podgrupe deli 4 in tako mora biti 2. Podgrupa z dvema elementoma je sestavljena z enoto in elementom, ki mora imeti red 2. Potemtakem obstajajo tri take podgrupe z dvema elementoma:

$$\{(1,\ 1),\ (x,\ 1)\},\ \{(1,\ 1),\ (1,\ y)\}, \text{ in } \{(1,\ 1),\ (x,\ y)\},$$

in tako obstaja pet podgrup grupe *G*.

Besedo 'red' smo uporabili v dveh pomenih: red grupe *G* (število elementov grupe *G*), in red elementa *g* v grupi *G* (najmanjše naravno število *k*, da velja $g^k = 1$). Po trditvi 3.15 sledi, da je red elementa *g* enaka redu podgrupe $\langle g \rangle$.

Posledica 4.21 *Naj bo g element končne grupe G. Potem red elementa g deli red grupe G.*

Dokaz. Uporabimo Lagrangeov izrek za podgrupo $\langle g \rangle$ grupe *G*. Nato uporabimo še trditev 3.15, ki pove, da je število elementov v tej podgrupi enako redu elementa *g*. □

Izrek 4.22 *Naj bo m red končne grupe G. Vsak element* $x \in G$ *ustreza enačbi* $x^m = 1$.

Dokaz. Naj bo *s* red elementa *x*. Ker je *m* deljiv z *s*, lahko pišemo $m = rs$, pri čemer je tudi r celo število. Od tod dobimo

$$x^m = x^{rs} = \left(x^s\right)^r = 1^r = 1.$$ □

Sledeča pomembna posledica Lagrangeovega izreka se glasi:

Posledica 4.23 *Naj bosta H in K podgrupi končne grupe G. Če je H podgrupa grupe K, potem velja*

$$|G : H| = |G : K||K : H|.$$

Dokaz. Kot smo videli je

$$|G : H| = |G|/|H| = \left(|G|/|K|\right)\left(|K|/|H|\right) = |G : K| \ |K : H|.$$

□

Trditev 4.24 *Naj bo H podgrupa grupe G. Preslikava* α *definirana s predpisom* $\alpha(gH) = Hg^{-1}$ *je bijekcija med množico različnih levih odsekov grupe G po podgrupi H in množico različnih desnih odsekov grupe G po podgrupi H. Tako je število različnih levih odsekov grupe G po podgrupi H enako številu različnih desnih odsekov grupe G po podgrupi H.*

Dokaz. Za dokaz injektivnosti α predpostavimo, da je $\alpha(xH)=\alpha(yH)$ za neka $x,\ y\in G$. Potem je $Hx^{-1}=Hy^{-1}$, tako je tudi $x^{-1}=1x^{-1}$ enako hy^{-1} za nek h iz H. Potemtakem je $h=x^{-1}y$ in tako je $h^{-1}=y^{-1}x$. Ker je H podgrupa, je h^{-1} v H in hkrati sta tudi leve odseka xH in yH enaka (posledica 4.13). Kar nam pove, da je α injektivna. Za dokaz surjektivnosti α pa, naj bo Hx desni odsek H v G. Ker je $x=\left(x^{-1}\right)^{-1}$ in ker je $Hx=\alpha\left(x^{-1}H\right)$, je α surjektivna. □

Primer 4.25 Vrnimo se na primer 4.4. Naj bo

$$G=\left\langle b,\ a:\ b^2=1=a^3,\ ab=ba^{-1}\right\rangle \text{ in } H=\left\langle b\right\rangle .$$

Različni desni odseki *grupe G po podgrupi H* so

$$H=H1=Hb;\ \ Ha=\{a,ab\}=Hba \text{ in } Ha^2=\left\{a^2,ba^2\right\}=Hba^2 .$$

Pripomnimo še, da elementi desnih odsekov nisi enaki tistim v levih odsekih: $\{a,ba\}$ je desni odsek, ni pa tudi levi odsek. Preslikava α v trditvi 4.24 je povezava med levimi in desnimi odseki, ki nam pokaže, da obstaja enako število obojih. Vendar so elementi v teh odsekih lahko popolnoma različni.

Definicija 4.26 *Za poljubni dve podmnožici A in B grupe G, definiramo podmnožico AB, ki je množica vseh elementov oblike ab, kjer je* $a\in A$ *in* $b\in B$

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

Trditev 4.27 *Naj bosta A in B podgrupi grupe G. Potem je AB podgrupa G natanko tedaj, ko je* $AB=BA$. *V tem primeru rečemo, da sta A in B zamenljivi.*

Dokaz.

$(AB\subseteq BA)$Predpostavimo, da je AB podgrupa G in naj bo ab iz AB. Potem je ab inverz nekega elementa c, recimo, iz AB. c lahko zapišemo kot a_1b_1 za nek a_1 iz A in b_1 iz B. Odtod je

$$ab=c^{-1}=\left(a_1b_1\right)^{-1}=b_1^{-1}a_1^{-1},$$

in tako je ab iz BA. To nam pokaže da je $AB\subseteq BA$.

$(BA \subseteq AB)$ Sedaj naj bo $x \in BA$. Tako je $x = ba$ za nek $a \in A$ in $b \in B$. Potem je $ba = \left(a^{-1}b^{-1}\right)^{-1} \in AB$, medtem ko je *AB* podgrupa. Iz tega sledi zahtevano $BA \subseteq AB$. Nasprotno predpostavimo, da je $AB = BA$. Da pa pokažemo, da je AB podgrupa G, moramo preveriti zahteve trditve 3.2(2). Potemtakem je 1 v *AB*, ker je 1 v *A* in v *B*. Če sta a_1, a_2 iz *A* in b_1, b_2 iz *B*, potem

$$(a_1b_1)(a_2b_2) = a_1(b_1a_2)b_2.$$

Ker je $AB = BA$ vidimo, da je $b_1a_2 = ab$ za nek *a* iz *A* in *b* iz *B*. Odtod je

$$(a_1b_1)(a_2b_2) = (a_1a)(bb_2).$$

Ker sta *A* in *B* podgrupi, preprosto sledi, da je $(a_1b_1)(a_2b_2)$ v *AB*. Končno velja, če je *ab* iz *AB*, potem je $(ab)^{-1} = b^{-1}a^{-1}$, tako je $(ab)^{-1}$ iz $AB = BA$ in *AB* je zaprta pod inverzom. Potemtakem je *AB* podgrupa *G*. □

Trditev 4.28 *Naj bosta A in B končni podgrupi grupe G. Potem je*

$$|AB| = \frac{|A|\ |B|}{|A \cap B|}.$$

Dokaz. Naj bodo

$$x_1(A \cap B),\ x_2(A \cap B),\ \ldots,\ x_k(A \cap B)$$

različni levi odseki $A \cap B$ v *A*. Potemtakem je tudi vsak element *A* v $x_i(A \cap B)$ za $1 \le i \le k$ in prav tako, če je $i \neq j$, potem $x_j x_i^{-1}$ ni element $A \cap B$. Naj bo *ab* poljuben element iz *AB*. potem lahko zapišemo a v obliki $x_i g$ za nek $1 \le i \le k$ in nek $g \in A \cap B$. Potemtakem je $ab = x_i(gb)$. Ker sta *g* in *b* iz *B*, je potem *ab* iz odseka $x_i B$. Razen tega se odseki $x_i B$ $(i = 1,\ldots,k)$ razdelijo, saj je drugače (posledica 4.11) $x_i B = x_j B$ za nek *i* in *j*. Zato je (trditev 4.10) $x_j^{-1}x_i$ element iz *B*. Ker sta x_i in x_j iz podgrupe A, in v nasprotju z definicijo je $x_j^{-1}x_i$ iz $A \cap B$. Smo pokazali, da

$$r = |A|/|A \cap B| = |AB|/|B|$$

in tako tudi

$$|AB| = \frac{|A|\ |B|}{|A \cap B|}.$$

□

Trditev 4.29 *Naj bo p praštevilo in G grupa s p elementi. Potem je grupa G ciklična.*

Dokaz. Predpostavimo, da je *G* grupa s *p* elementi in naj bo g element iz *G*, ki je različen od enote. Po posledici 4.21 red *g* deli *p*. Ker je *p* praštevilo, sta njegova edina delitelja 1 in *p*. Red *g* pa ni 1, saj je $g \neq e$, potemtakem je *p* red elementa *g*. Po trditvi 3.15 sledi, da ima podgrupa $\langle g \rangle$ *p* elementov in tako zajame celotno grupo *G*. Potemtakem je *G* ciklična grupa. □

5 Podgrupe edinke in kvocientne grupe

V tem poglavju bomo predstavili pojem podgrupe edinke in pokazali kako je ta podgrupa uporabljena pri konstrukciji kvocientne grupe.

Definicija 5.1 *Naj bo x element grupe G. Pravimo, da je poljubni element grupe G oblike* gxg^{-1} *konjugirani element elementa x. Za poljubno podgrupo H grupe G pravimo, da je množica* $gHg^{-1} = \{gxg^{-1} : x \in H\}$ *konjugiranka podgrupe H.*

Trditev 5.2 *Naj bo H podgrupa grupe G. Potem je vsake konjugiranka* gHg^{-1} *tudi podgrupa grupe G.*

Dokaz. Za dokaz, da je gHg^{-1} podgrupa G, moramo preveriti pogoj 2 iz trditve 3.2. Enota grupe G je tudi v grupi gHg^{-1}, ker je $g1g^{-1} = 1 \in gHg^{-1}$. Če sta $a = gxg^{-1}$ in $b = gyg^{-1}$ iz gHg^{-1}, potem je tudi

$$ab = (gxg^{-1})(gyg^{-1}) = g(xy)g^{-1} \in gHg^{-1}.$$

Končno za poljuben $gxg^{-1} \in gHg^{-1}$ vidimo, da je

$$(gxg^{-1})^{-1} = (g^{-1})^{-1}x^{-1}g^{-1} = gx^{-1}g^{-1} \in gHg^{-1}. \qquad \square$$

Definicija 5.3 *Podgrupa N grupe G je edinka, če za vsak* $g \in G$ *velja, da je* $gNg^{-1} \subseteq N$ *(to pomeni, da za vsak* $x \in N$ *in vsak* $g \in G$*, velja* $gxg^{-1} \in N$*).*

Opomba 5.4 *V poljubni grupi G sta* $\{1\}$ *in G podgrupi edinki.*

Trditev 5.5 *Naslednji pogoji so za vsako podgrupo N grupe G ekvivalentni:*

(a) N je podgrupa edinka grupe G;

(b) za vsak $g \in G$ *velja, da je* $g^{-1}Ng \subseteq N$*;*

(c) za vsak $g \in G$ *velja, da je* $g^{-1}Ng = N = gNg^{-1}$*;*

(d) za vsak $g \in G$ *velja, da je* $gN = Ng$*; in*

(e) vsak desni odsek grupe G po podgrupi N je tudi levi odsek grupe G po podgrupi N.

Dokaz. (a)$\Rightarrow$(b) Ker je N podgrupa edinka grupe G, je $yNy^{-1} \subseteq N$ za vsak $y \in G$. Če namesto y vstavimo g^{-1}, nam potem to pove, da je $g^{-1}N\left(g^{-1}\right)^{-1} = g^{-1}Ng \subseteq N$.

(b)$\Rightarrow$(c) Po (b) za vsak $g \in G$ velja, da je $gNg^{-1} = \left(g^{-1}\right)^{-1} Ng^{-1} \subseteq N$, tako je

$$gN = gNg^{-1}g \subseteq Ng.$$

Iz tega sledi, da je $N = g^{-1}\left(gN\right)$ vsebovan v $g^{-1}Ng$. Zato je potemtakem $N = g^{-1}Ng$ in $N = gNg^{-1}$.

(c)$\Rightarrow$(d) Če je $gNg^{-1} = N$ za vsak $g \in G$ vidimo, da je

$$gN = g\left(g^{-1}Ng\right) = Ng \text{ za vsak } g \in G.$$

(d)$\Rightarrow$(e) Ta implikacija je očitna.

(e)$\Rightarrow$(a) Za vsak $g \in G$ nam pogoj (e) pove, da je desni odsek Ng levi odsek, recimo $Ng = g'N$ za nek g'. Potem pa, ker je 1 iz $g^{-1}Ng = g^{-1}g'N$, je $1 = g^{-1}g'n$ za nek $n \in N$. Iz tega sledi, da je $N \subseteq g^{-1}Ng$ od to pa nadalje preprosto sledi, da $g^{-1}Ng \subseteq N$ tako, da podgrupa edinka grupe *G*. □

Primer 5.6 Če je *G* Abelova grupa, potem za vsako podgrupo *N* grupe *G* in vsak element *g* iz *G* velja, da je $gNg^{-1} = N$, ker je $gng^{-1} = gg^{-1}n = n$. Potemtakem je vsaka podgrupa Abelove grupe podgrupa edinka.

Primer 5.7 Predpostavimo, da je *H* podgrupa grupe *G* z indeksom 2. Potem ima *H* dva leva (in dva desna) odseka v *G*. Če je $g \in H$, je levi odsek gH enak *H*, prav tako kot desni odsek Hg. Za vsak g, ki ni v *H*, mora biti levi odsek gH enak *G\H*, ker obstajata samo dva leva odseka in ta odseka tvorita razbitje grupe *G*. Tudi desni odsek Hg mora zaradi istega razloga biti enak *G\H*. Potemtakem je vsak levi odsek enak desnemu odseku in tako je po trditvi 5.5(e) *H* podgrupa edinka grupe *G*.

Trditev 5.8 *Naj bo N podgrupa edinka grupe G in naj bo H poljubna podgrupa grupe G. Potem je* $H \cap N$ *podgrupa edinka grupe H.*

Dokaz. Za poljuben $x \in H \bigcap N$ in poljuben $g \in H$ velja, da $gxg^{-1} \in H$, ker je H podgrupa G. Vendar, ker je $x \in N$ in je N podgrupa edinka grupe G, je prav tako $gxg^{-1} \in N$. Zato, kot je zahtevano, tudi $gxg^{-1} \in N \bigcap H$. □

Trditev 5.9 *Naj bo I množica indeksov in* $\{N_i : i \in I\}$ *naj bo množica podgrup edink grupe G. Potem sta tudi* $\langle N_i : i \in I \rangle$ *in* $\bigcap_{i \in I} N_i$ *podgrupi edinki grupe G.*

Dokaz. Po definiciji je $\langle N_i \rangle$ presek vseh podgrup grupe G, ki vsebujejo vse N_i. Za poljubno tako podgrupo H velja, da njena konjugiranka podgrupe H vsebuje vsak gN_ig^{-1}. Ker je vsaka N_i podgrupa edinka grupe G, sklepamo, da konjugiran gHg^{-1} vsebuje tudi N_i. Zato sledi, da je

$$\langle N_i : i \in I \rangle$$

podgrupa edinka.

Prav tako, ker je $\bigcap N_i$ podgrupa G (trditev 3.10), in $g(\bigcap N_i)g^{-1} = \bigcap(gN_ig^{-1})$ za vsak $g \in G$, sklepamo, da je $\bigcap N_i$ podgrupa edinka grupe G. □

Trditev 5.10 *Naj bo N podgrupa edinka grupe G in naj bo H poljubna podgrupa grupe G. Potem je* $\langle N, H \rangle = NH$ *tako, da je* $HN = NH$.

Dokaz. Že iz aksioma (G1) definicije 1.1 je jasno, da mora $\langle N, H \rangle$ vsebovati NH. Kajti aksiom pravi za vsak par $g, h \in G$, $g \circ h \in G$. Zato bo dovolj pokazati, da je NH podgrupa G. Saj bo potem rezultat sledil po definiciji $\langle N, H \rangle$. Brez dvoma $1 \in NH$. Predpostavimo, da $n, n_1 \in N$ in $h, h_1 \in H$. Potem je

$$(nh)(n_1h_1) = n(hn_1H^{-1}h)h_1 = n(hn_1h^{-1})(hh_1).$$

Ker je N podgrupa edinka, je hn_1h^{-1} element n_2 recimo iz N, in tako velja:

$$(nh)(n_1h_1) = (nn_2)(hh_1) \in NH.$$

Prav tako je

$(nh)^{-1} = h^{-1}n^{-1} = (h^{-1}n^{-1}h)h^{-1} \in NH$,

kar pomeni, da je NH podgrupa. Dejstvo, da je $HN = NH$ pa sledi iz trditve 4.27. □

Podgrupe edinke so pomembne zaradi tega, ker lahko z levimi odseki grupe po podgrupi edinki konstruiramo kvocientno grupo (to velja tudi za desne odseke, saj je vsak levi odsek enak desnemu).

Trditev 5.11 *Naj bo N podgrupa edinka grupe G. Množica vseh levih odsekov grupe G po podgrupi N, ki jo označujemo z* G/N*, je grupa za operacijo* $(xN)(yN) = xyN$.

Dokaz. Preverimo lahko, da množica levih odsekov zadošča vsem štirim aksiomom grupe za definirano operacijo, vendar pa to ni težava pri našem dokazu. Trditev, da je G/N grupa, ki vsebuje implicirano trditev, da je operacija dobro definirana v sledečem smislu. Videti je, da je pravilo $(xN)(yN) = xyN$ odvisno od izbire tipičnega odseka. Odsek xN je enak uN kadar $u^{-1}x \in N$, in $yN = vN$ kadar $v^{-1}y \in N$. Preveriti moramo, da če $xN = uN$ in $yN = vN$, potem je odsek xyN enak odseku uvN. Da to izvedemo, moramo preveriti, da $(uv)^{-1}(xy) \in N$ (ali z izrazi ekvivalenčnih relacij, če xRu in yRv, potem $xyRuv$). To sledi iz sledečega računa:

$$\begin{aligned}(uv)^{-1}(xy) &= v^{-1}u^{-1}xy \\ &= v^{-1}ny, \text{ kjer } n = u^{-1}x \in N \\ &= v^{-1}y(y^{-1}ny).\end{aligned}$$

Ker je *N* podgrupa edinka, je $y^{-1}ny$ v *N*, in $v^{-1}y$ je element iz *N*, tako je $(uv)^{-1}(xy)$ tudi v N. omeniti moramo, da ta argument uporablja dejstvo, da je *N* podgrupa edinka grupe G. Za dokaz dobre definiranosti operacije, moramo preprosto preveriti aksiome grupe: enota kvocientne grupe G/N je odsek $1N = N$ in inverz od gN je $g^{-1}N$. □

Primer 5.12 Uporabimo aditivno grupo celih števil **Z**. **Z** je Abelova grupa, zato je vsaka podgrupa grupe **Z** podgrupa edinka. Preučimo podgrupo, vseh večkratnikov poljubnega celega števila *n*, *n***Z.** Nadalje definirajmo kvocientno grupo **Z**/*n***Z**.
Elementi te grupe so odseki *x*+*n***Z**. Cela števila v danem odseku *x*+*n***Z** so elementi kongruenčnega razreda $[x] \equiv (\text{mod } n)$. Ker je Z grupa za operacijo seštevanja, je operacija v kvocientni grupi prav tako seštevanje, podano s pravilom:

$$(x+n\mathbf{Z})+(y+n\mathbf{Z}) = (x+y+n\mathbf{Z}).$$

Vprašanje dobre definiranosti lahko formuliramo takole: če je $u \equiv x \pmod{n}$in $v \equiv y \pmod{n}$, potem je $x + y \equiv u + v \pmod{n}$.

V grupi **Z** obstaja *n* različnih odsekov po podgrupi *n***Z**:

$$0+n\mathbf{Z},\ 1+n\mathbf{Z},\ \ldots,\ (n\text{-}1)+n\mathbf{Z},$$

zato je kvocientna grupa **Z**/*n***Z** Abelova grupa z *n* elementi. Ta grupa je ciklična in generirana z $1+n\mathbf{Z}$.

Tako smo videli, da je kvocientna grupa **Z**/*n***Z** v resnici grupa $\mathbf{Z}_n$.

Primer 5.13 Naj bo *G* grupa simetrij kvadrata *D*(4):

$$G = \left\langle a, b : a^4 = 1 = b^2 \ in\ ab = ba^{-1} \right\rangle.$$

Naj bo *N* podgrupa generirana z a^2, tako da je *N* sestavljena iz dveh elementov 1 in a^2. Potem je *N* podgrupa edinka grupe *G*. To lahko vidimo na več načinov, eden od teh je, da naštejemo štiri leve odseke grupe G po podgrupi N:

$1N = \{1, a^2\},\ bN = \{b, ba^2\},\ aN = \{a, a^3\}$ in $baN = \{ba, ba^3\}$.

Ker $ba^2 = a^2b$ in $ba^3 = a^2ba$, je lahko videti, da je vsak od teh desni odsek.:

$1N = N1,\ bN = Nb,\ aN = Na$ in $baN = Nba$.

Nadalje konstruiramo tabelo produktov za G/N, da to lažje naredimo bomo odseke preimenovali, recimo $E = N,\ A = aN,\ B = bN$ in $C = abN$.

Tabela izpolnimo z izračuni kot so

$$AB = (aN)(bN) = abN = C;$$

$$AC = (aN)(abN) = a^2bN = bN = B,$$

tako dobimo sledečo tabelo

	E	A	B	C
E	E	A	B	C
A	A	E	C	B
B	B	C	E	A
C	C	B	A	E

Da je $G/N \cong C_2 \times C_2$ vidimo, če dobljeno tabelo primerjamo s tabelo primera 1.9.

Izrek 5.14 *Naj bo N podgrupa edinka grupe G. Potem je vsaka podgrupa kvocientne grupe* G/N *oblike* H/N, *za neko podgrupo H grupe G, kjer je* $N \le H$.

Obratno, če je H podgrupa grupe G, ki vsebuje N, potem je H/N *podgrupa grupe* G/N. *Med množico podgrup grupe* G/N *in množico podgrup grupe G, ki vsebujejo N obstaja bijektivna preslikava. Ta bijektivna preslikava slika podgrupe edinke grupe* G/N *v podgrupe edinke grupe G, ki vsebujejo N.*

Dokaz. Naj bo H^* podgrupa grupe G/N tako, da se ujema z neko množico $\{hN\}$ levih odsekov grupe N v G. Definirajmo podmnožico $\beta(H^*)$ množice G, da bo $\{g \in G : gN \in H^*\}$. Potem $\beta(H^*)$ vsebuje N in je podgrupa grupe G:

$1 \in N$, tako $1 \in \beta(H^*)$;

če $x, y \in \beta(H^*)$, potem xN in $yN \in H^*$, tako $(xN)(yN) = xyN \in H^*$, in tako $xy \in \beta(H^*)$; in

ker je $(xN)^{-1} = x^{-1}N$ sledi, da $x^{-1} \in \beta(H^*)$.

Na ta način je $\beta(H^*)$ podgrupa grupe G, ki vsebuje N.

Nasprotno, če je H poljubna podgrupa grupe G, ki vsebuje N, naj bo $\alpha(H)$ podmnožica $\{hn : h \in H\}$ množice G/N. Preprost lahko preverimo, da je $\alpha(H)$ podgrupa grupe G/N.

Za zaključek dokaza pokažemo, daje preslikava α, iz množice podgrup X grupe G, ki vsebujejo N, v množico podgrup Y grupe G/N, bijektivna. To bo končano po preveritvi, da je preslikava $\beta : Y \to X$ inverzna preslikava preslikave α. Da to storimo, moramo pokazati, da sta kompozituma preslikav $\alpha \circ \beta$ in $\beta \circ \alpha$ identična. Predpostavimo, da $H \le G$ in $N \le H$, potem je

$$\beta \circ \alpha(H) = \beta(H/N) = \{g \in G : gN \in H/N\} = H .$$

Nasprotno, na bo H^* podgrupa grupe G/N. , potem je

$$\alpha \circ \beta(H^*) = \alpha(\{g \in G : gN \in H^*\}) = \{gN \in H^*\} = H^* .$$

Sedaj naj bo H podgrupa edinka grupe G, ki vsebuje N. Pokazati moramo, da je $\alpha(H)$ podgrupa edinka grupe G/N. To sledi, ker

$$(gN)(hN)(gN)^{-1} = ghg^{-1}N \in H/N .$$

Obratno, če je H^* podgrupa edinka grupe G/N, brez težav preverimo, da je $\beta(H^*) = \{g \in G : gN \in H^*\}$ podgrupa edinka grupe G. □

Trditev 5.15 *Naj bo N podgrupa edinka grupe G in naj bosta A, B taki podgrupi grupe G, da velja* $N \leq A, B$. *Potem za bijektivno preslikavo* α *iz izreka 5.14 velja:*

(i) $\alpha(A \cap B) = \alpha(A) \cap \alpha(B)$;

(ii) $\alpha(\langle A, B \rangle) = \langle \alpha(A), \alpha(B) \rangle$.

Dokaz. (i) Imamo, da je

$$\alpha(A) \cap \beta(B) = \{gN : g \in A \cap B\} = (A \cap B)/N = \alpha(A \cap B).$$

(ii) Rezultat sledi, ker je

$$\begin{aligned} \alpha(\langle A, B \rangle) &= \{hN : h \in \langle A, B \rangle\} \\ &= \{hN \in \langle A/N, B/N \rangle\} \\ &= \langle \alpha(A), \alpha(B) \rangle. \end{aligned}$$

□

6 Homomorfizmi

V tem poglavju bomo raziskali preslikave med grupami, ki ohranjajo grupno operacijo. Povezava med to idejo in kvocientnimi grupami, ki smo jih spoznali v prejšnjem poglavju, je predstavljena v izreku 6.14 znanem pod imenom »Izrek o homomorfizmih«.

Definicija 6.1 *Naj bosta G in H grupi. Homomorfizem iz G v H je taka preslikava* $\phi : G \to H$ *, da za vsak x, y iz G velja,* $\phi(xy) = \phi(x)\phi(y)$.

Primer 6.2 Naj bo *G*=*GL*(*n*, **R**) grupa vseh obrnljivih $n \times n$ matrik z realnimi členi, kjer za operacijo vzamemo običajno množenje matrik. Naj bo H multiplikativna grupa vseh neničelnih realnih števil. Za matriko *X* v *G* definiramo, da je $\phi(X)$ determinanta matrike *X*. Ker je *X* obrnljiva, je determinanta različna od nič. Splošna lastnost determinant je, da je

$$\det(XY) = \det(X)\det(Y).$$

Iz česar sledi, da je ϕ homomorfizem.

Trditev 6.3 *Naj bosta G in H grupi in* $\phi : G \to H$ *naj bo homomorfizem. Potem za vsak x in y iz G velja:*

$$\phi(xy^{-1}) = \phi(x)\phi(y)^{-1} \text{ in } \phi(y^{-1}x) = \phi(y)^{-1}\phi(x).$$

Dokaz. Ker je ϕ homomorfizem velja

$$\begin{aligned}\phi(xy^{-1})\phi(y) &= \phi((xy^{-1})y)\\ &= \phi(x).\end{aligned}$$

Sedaj pomnožimo obe strani te enakosti na desni z $\phi(y)^{-1}$, da dobimo želeni rezultat.

Ker je ϕ homomorfizem velja

$$\begin{aligned}\phi(y)\phi(y^{-1}x) &= \phi(y(y^{-1}x))\\ &= \phi(x).\end{aligned}$$

Sedaj pomnožimo obe strani te enakosti na levi z $\phi(y)^{-1}$, da dobimo želeni rezultat. □

Posledica 6.4 *Naj bosta G in H grupi in* $\phi : G \to H$ *naj bo homomorfizem. Potem velja:*

(i) $\phi(1_G) = 1_H$ *; in*

(ii) za vsak $g \in G, \phi(g^{-1}) = \phi(g)^{-1}$.

Dokaz. (i) sledi iz trditve 6.3, ko vzamemo $x = y$.

(ii) sledi, ko vzamemo $x = 1_G$ in $y = g$. □

Za poljubno množico X, je identična preslikava preslikava $id_X : X \to X$ definirana s predpisom $id_X(x) = x$ za vsak $x \in X$. Iz definicije je jasno, da če je $f : X \to Y$ poljubna preslikava, potem je $f \circ id_X = f$ in $id_Y \circ f = f$.

Definicija 6.5 *Za podano preslikavo* $f : X \to Y$ *pravimo, da ima inverzno preslikavo, če obstaja taka preslikava* $g : Y \to X$*, da velja* $g \circ f = id_X$ *in* $f \circ g = id_Y$.

Trditev 6.6 *Preslikava* $f : X \to Y$ *ima inverzno preslikavo natanko tedaj, ko je f bijektivna.*

Dokaz. Najprej predpostavimo, da je *f* bijektivna. Definirajmo preslikavo $g : Y \to X$ po pravilu:

$$g(y) = x \text{ natanko tedaj, ko je } f(x) = y.$$

Upoštevajmo, da je *g* preslikava, ker obstaja vsaj en element iz X, ki je določen nekemu *y* po *g* (ker je *f* injektivna), vendar vsak element iz *Y* je določen nekemu *x* iz *X* (ker je *f* surjektivna). Zato direktno iz definicije sledi, da so kompozitumi preslikav $g \circ f$ in $f \circ g$ enaki identični preslikavi.

Obratno predpostavimo, da ima *f* inverzno funkcijo f^{-1}. Najprej pokažimo, da je *f* injektivna. Predpostavimo, da je $f(x_1) = f(x_2)$. Vpeljimo f^{-1} na obe strani in dobimo

$$x_1 = id_X(x_1) = f^{-1}(f(x_1)) = f^{-1}(f(x_2)) = id_X(x_2) = x_2,$$

tako da *f* je injektivna. Za dokaz surjektivnosti *f*, vzemimo poljuben *y* iz *Y*. Potem je

$$y = id_Y(y) = f \circ f^{-1}(y) = f(f^{-1}(y)) = f(x)$$

kjer je $x = f^{-1}(y)$. □

Posledica 6.7 *Če sta preslikavi* $f : X \to Y$ *in* $g : Y \to Z$ *bijektivni, potem je bijektivna tudi preslikava* $g \circ f$.

Dokaz. Uporabimo trditev 6.7. *f* in *g* imata inverzni preslikavi f^{-1} in g^{-1}. Za dokaz je dovolj opazovati, da

$$(g \circ f)(f^{-1} \circ g^{-1}) = id_Z \text{ in } (f^{-1} \circ g^{-1})(g \circ f) = id_X,$$

tako da je inverz od $g \circ f$ enak $f^{-1} \circ g^{-1}$. Potem pa iz trditve 6.7 vidimo, da je $g \circ f$ bijektivna. □

Definicija 6.8 *Bijektivni homomorfizem iz grupe G v grupo H se imenuje izomorfizem. V tem primeru pravimo, da sta grupi G in H izomorfni in pišemo* $G \cong H$.

Trditev 6.9 *Izomorfizem je ekvivalenčna relacija na množici grup.*

Dokaz. Preslikava $id_G : G \to G$, definirana kot $id_G(g) = g$ za vsak $g \in G$, je brez dvoma bijektivni homomorfizem, kar pomeni $G \cong G$. Če je ϕ izomorfizem in *G* v *H*, potem, ker je ϕ bijektivna, obstaja ϕ^{-1}. Da pa pokažemo, da je ϕ^{-1} izomorfizem iz *H* v *G*, se spomnimo, da je $\phi^{-1}(y) = x$ kadarkoli je $\phi(x) = y$. Na ta način, če je tudi $\phi(x_1) = y_1$ in je $\phi(xx_1) = yy_1$, imamo

$$\phi^{-1}(y)\phi^{-1}(y_1) = xx_1 = \phi^{-1}(yy_1),$$

kar nam pokaže, da je ϕ^{-1} homomorfizem. Končno, če sta $\phi : G \to H$ in $\vartheta : H \to K$ izomorfizma, lahko preprosto preverimo, da je $\vartheta \circ \phi$ homomorfizem med *G* in *K*, ker

$$\begin{aligned} \vartheta \circ \phi(xy) &= \vartheta(\phi(xy)) \\ &= \vartheta(\phi(x)\phi(y)), \text{ ker je } \phi \text{ homomorfizem} \\ &= \vartheta(\phi(x))\vartheta(\phi(y)), \text{ ker je } \vartheta \text{ homomorfizem} \\ &= \vartheta(\phi(x)\phi(y)). \end{aligned}$$

Dejstvo, da je $\vartheta \circ \phi$ bijektivna, lahko preprosto preverimo, vendar smo ga že prej v posledici 6.8 natančno dokazali. □

Definicija 6.10 *Bijektivni homomorfizem ϕ grupe same vase imenujemo avtomorfizem.*

Množico vseh avtomorfizmov grupe G označimo z $Avt(G)$.

Trditev 6.11 *Množica $Avt(G)$ je skupaj z operacijo komponiranja ($\circ$) grupa.*

Dokaz. Preverimo aksiome grupe. Če $\vartheta, \phi \in Avt(G)$, smo videli že v dokazu trditve 6.9, da je kompozitum $\vartheta \circ \phi$ bijektivni homomorfizem, saj sta tudi ϕ in ϑ. Znano je, da je kompozitum asociativna operacija. Identična preslikava je bijektivna. Če je ϕ v $Avt(G)$, potem ker je ϕ bijektivna, obstaja tudi ϕ^{-1} in je homomorfizem kot v dokazu trditev 6.9. □

Definicija 6.12 *Naj bo $\phi : G \to H$ homomorfizem grup. Jedro* $\ker\phi$ *je množica elementov iz G, ki jih homomorfizem ϕ preslika v enoto grupe H:*

$$\ker\phi = \{g \in G : \phi(g) = 1_H\}$$

Slika $im\phi$ pa je množica elementov iz H, ki so slike elementov iz G:

$$im\phi = \{h \in H : h = \phi(g) \text{ za nek } g \in G\}.$$

Izrek 6.13 (Izrek o homomorfizmih) *Naj bo ϕ homomorfizem iz grupe G v grupo H. Potem velja:*

(1) $\ker\phi$ *je podgrupa edinka grupe G;*

(2) $im\phi$ je podgrupa grupe H; in

(3) $G/\ker\phi \cong im\phi$.

Dokaz. (1) Najprej pokažemo, da je $\ker\phi$ podgrupa grupe G. Po posledici 6.4(i) je 1_G v $\ker\phi$; če sta x in y v $\ker\phi$, potem je

$$\phi(xy) = \phi(x)\phi(y) = 1_H 1_H = 1_H$$

in $xy \in \ker\phi$; in če je g v $\ker\phi$, potem $g^{-1} \in \ker\phi$ po posledici 6.4(ii). Da pokažemo, da je $\ker\phi$ podgrupa edinka, naj bo $g \in G$ in $x \in \ker\phi$, potem je

$$\begin{aligned}\phi\left(g^{-1}xg\right) &= \phi(g)^{-1}\phi(x)\phi(g) \text{ po trditvi 6.3}\\ &= \phi(g)^{-1}1_H\phi(g), \text{ ker } x\in\ker\phi\\ &= 1_H,\end{aligned}$$

tako je $g^{-1}xg$ iz $\ker\phi$; in $\ker\phi$ je podgrupa edinka grupe *G*.

(2) Posledica 6.4 nam pokaže, da je 1_H v $im\phi$. Če sta $y=\phi(x)$ in $y_1=\phi(x_1)$ v $im\phi$ za poljubna $x, x_1\in G$, potem je

$$yy_1=\phi(x)\phi(x_1)=\phi(xx_1)$$

v $im\phi$. Prav tako, če je $y=\phi(x)$ v $im\phi$, potem je po posledici 6.4(ii) $y^{-1}=\phi\left(x^{-1}\right)$. Potemtakem je $im\phi$ podgrupa grupe *H*.

(3) Zaradi lažjega zapisa namesto $\ker\phi$ pišimo *K*. Definirajmo preslikavo $\vartheta: G/K\to H$ po pravilu

$$\vartheta(gK)=\phi(g) \text{ za vsak } g\in G.$$

Za dokaz, da je ϑ izomorfizem moramo preveriti kar nekaj stvari: da je ϑ dobro definirana, da je ϑ homomorfizem in končno, da je ϑ bijektivna preslikava iz G/K v $im\phi$. Definicija ϑ ,e zdi odvisna od izbire reprezentativnega odseka, zato da je ϑ dobro definirana predpostavimo, da je $xK=yK$, tako da je $x=yk$ za nek $k\in K$, potem je

$$\vartheta(xK)=\phi(x)=\phi(xk)=\phi(y)\phi(k)=\phi(y)1_H=\phi(y)=\vartheta(yK),$$

tako da je ϑ dobro definirana. Nadalje za vsak $x, y\in G$ velja,

$$\vartheta(xK)\vartheta(yK)=\phi(x)\phi(y)=\phi(xy)=\vartheta(xyK),$$

da je ϑ homomorfizem. Ker je vsak element iz $im\phi$ oblike $\phi(x)=\vartheta(xK)$ za nek $x\in G$ velja, da je ϑ surjektivna iz G/K v $im\phi$. Preostane nam še dokaz, da je ϑ injektivna: če je $\vartheta(xK)=\vartheta(yK)$, sklepamo, da je $\phi(x)=\phi(y)$ in tako je z uporabo trditve 6.3

$$1_H=\phi(y)^{-1}\phi(x)=\phi\left(y^{-1}x\right).$$

Potemtakem $y^{-1}x\in K$ in tako je $xK=yK$. □

Primer 6.14 Naj bo det : $GL(n, \mathbf{R})\to\mathbf{R}^{\times}$ homomorfizem, ki vsaki obrnljivi matriki priredi njeno determinanto. Jedro te preslikave je množica $SL(n, \mathbf{R})$ matrik z determinanto 1. Preslikava je surjektivna, ker obstajajo obrnljive matrike z vsemi možnimi neničelnimi determinantami, tako nam izrek o homomorfizmu pokaže, da

$GL(n, \mathbf{R})/SL(n, \mathbf{R}) \cong \mathbf{R}^{\times}$.

Opomba 6.15 Izrek o homomorfizmih nam pove, da je jedro poljubnega homomorfizma podgrupa edinka. Velja tudi obratno. Če je N podgrupa edinka grupe G, potem lahko vidimo, da je preslikava $\phi : G \to G/N$ definirana s $\phi(g) = gN$ homomorfizem. Imenujemo ga *naravni homomorfizem*. Jedro te preslikave je podgrupa edinka N. Zato obstaja povezava med množico podgrup edink grupe G in jedri homomorfizmov na grupi G.

Izrek 6.16 (1. izrek o izomorfizmih**)** *Naj bo H podgrupa grupe G in naj bo N podgrupa edinka grupe G. Potem je N podgrupa edinka grupe* $\langle N, H \rangle = HN$ *in* $N \cap H$ *je podgrupa edinka grupe H. Nadalje velja*

$$\frac{H}{N \cap H} \cong \frac{HN}{N}.$$

Dokaz. Dejstvo, da je $\langle N, H \rangle = HN$ sledi iz trditve 5.8, in iz dejstva, da je N podgrupa edinka od G sledi, da je N podgrupa edinka od HN. Sedaj definirajmo preslikavo $\phi : H \to HN/N$ po pravilu $\phi(h) = hN$. (Opomba. H mora vsebovati N, tako da je odsek hN prej element grupe HN/N kot pa H/N.) Potem je ϕ homomorfizem, ker je $\phi(xy) = xyN = (xN)(yN) = \phi(x)\phi(y)$.

Jedro preslikave ϕ je podano e enačbo

$$\begin{aligned} \ker\phi &= \{h \in H : \phi(h) = 1_{HN/N}\} \\ &= \{h \in H : hN = N\} \\ &= \{h \in H : h = N\} \\ &= H \cap N. \end{aligned}$$

ϕ je surjektivna, ker je element $hnN = hN$ iz HN/N enak $\phi(h)$. Rezultat sedaj sledi po izreku o homomorfizmih. □

Izrek 6.17 (2. izrek o izomorfizmih**)** *Naj bosta H in N podgrupi edinki grupe G in N naj bo vsebovana v H. Potem je* H/N *podgrupa edinka grupe* G/N *in*

$$(G/N)/(H/N) \cong G/H.$$

Dokaz. Definirajmo preslikavo $\phi : G/N \to G/H$ po pravilu $\phi(gN) = gH$. Ker je ϕ definirana na odsekih, bomo preverili, ali je dobro definirana. Predpostavimo, da je $xN = yN$, tako da $y^{-1}x \in N$. Potem ker je $N \leq H$ vidimo, da $y^{-1}x \in H$ in tako je $xH = yH$, tako da je $\phi(xN) = \phi(yN)$. Naprej, ϕ je homomorfizem, ker je $\phi(xN) = \phi(yN) = (xH)(yH) = xyH = \phi(xyN)$.

ϕ je jasno tudi surjektivna in

$$\begin{aligned} \ker\phi &= \{gN \in G/N : \phi(gN) = 1_{G/N}\} \\ &= \{gN \in G/N : gH = H\} \\ &= \{gN \in G/N : g \in H\} \\ &= H/N. \end{aligned}$$

Rezultat sedaj sledi po izreku 6.13. □

Naj bo *x* poljubni element grupe *G*. Definirajmo preslikavo $\phi_x : G \to G$ s predpisom $\phi_x(g) = xgx^{-1}$ za vsak $g \in G$. Množico vseh takih preslikav označimo z Inn(*G*). Definirajmo še množico $Z(G) = \{x \mid x \in G\}$.

Trditev 6.18 *Naj bo x element grupe G. Potem velja, da je* ϕ_x *avtomorfizem grupe G. Množica* Inn(*g*) je *podgrupa grupe* Avt(*G*), $Z(G)$ *je podgrupa edinka grupe G, in* $G/Z(G) \cong$ Inn(*G*).

Dokaz. Za dokaz, da je ϕ_x avtomorfizem potrebujemo tri korake:

(a) ϕ_x je homomorfizem: za vsak $g, h \in G$

$$\phi_x(g)\phi_x(h) = (xgx^{-1})(xhx^{-1}) = x(gh)x^{-1} = \phi_x(gh);$$

(b) ϕ_x je injektivna:

če je $\phi_x(g) = \phi_x(h)$, potem je $xgx^{-1} = xhx^{-1}$ in tako je $g = h$;

(c) ϕ_x je surjektivna:

za poljuben *h* iz *G* velja, $\phi_x(x^{-1}hx) = x(x^{-1}hx)x^{-1} = h$.

Sedaj definirajmo preslikavo $\vartheta : G \to Aut(G)$ s predpisom $\vartheta(x) = \phi_x$. Upoštevajmo, da za vsak *g* iz *G* velja,

$$(\phi_x \circ \phi_y)(g) = \phi_x(\phi_y(g)) = \phi_x(ygy^{-1}) = xygy^{-1}x^{-1} = \phi_{xy}(g),$$

tako je $\phi_x \circ \phi_y = \phi_{xy}$. Ker je ϑ homomorfizem, potem sledi

$$\vartheta(x)\vartheta(y) = \phi_x \circ \phi_y = \phi_{xy} = \vartheta(xy).$$

Jasno je, da je slika funkcije ϑ enaka Inn(G) in

$$\begin{aligned}
\ker \vartheta &= \{x \in G : \phi_x = id_G\} \\
&= \{x \in G : \phi_x(g) = id_G(g) \ za \ vsak \ g \in G\} \\
&= \{x \in G : xgx^{-1} = g \ za \ vsak \ g \in G\} \\
&= \{x \in G : xg = gx \ za \ vsak \ g \in G\} \\
&= Z(G).
\end{aligned}$$

Izrek o homomorfizmu nam pove, da je $Z(G)$ podgrupa edinka grupe G, da je Inn(G) podgrupa od Avt(G), in prav tako da je kvocientna grupa $G/Z(G)$ izomorfna z Inn(G).

□

Opomba 6.19 *Avtomorfizem ϕ_x imenujemo motranji avtomorfizem. Z(G) imenujemo center grupe G.*

7 Permutacije

Definicija 7.1 *Bijekcijo* π *iz množice X na množico X imenujemo permutacija množice X.*

Z *S(X)* bomo označevali množico vseh permutacij $f : X \to X$.

Trditev 7.2 *Naj bo X poljubna množica. Potem je množica* $S(X)$*, skupaj z operacijo komponiranja, grupa.*

Dokaz. Preveriti moramo aksiome grupe za $S(X)$, če želimo pokazati, da je grupa. (G1) sledi iz posledice 6.7. (G2) sledi iz asociativnosti kompozituma. (G3) sledi, če za enoto vzamemo preslikavo id_X. Končno, definicija inverzne funkcije nam pokaže, da če je f^{-1} inverz od f, potem je f inverz od f^{-1}, in tako je f^{-1} bijektivna. □

Nas bodo zanimali samo primeri v katerih je *X* končna množica z *n* elementi. Zato bomo v tem primeru *X*, ki predstavlja množico $\{1,\ 2,\ ...,\ n\}$, v zapisu $S(X)$ zamenjali z $S(n)$. Zaradi boljše preglednosti bijektivno funkcijo $\pi : X \to X$ zapišemo v dvovrstičnem zapisu, v katerem zgornja vrstica matrike $2 \times n$ vsebuje naravna števila 1, 2, ..., n. V drugi vrstici pod posameznim naravnim številom $i \in \{1,\ 2,\ ...,\ n\}$ zapišemo njegovo funkcijsko vrednost $\pi(i)$:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & ... & n \\ \pi(1) & \pi(2) & \pi(3) & ... & \pi(n) \end{pmatrix}.$$

Ker druga vrstica vsebuje vsak element množice *X* natanko enkrat, obstaja *n* možnosti za vpis pod 1, kar pomeni $n-1$ možnosti za vpis pod 2 itn.. Vse skupaj nam da *n*! bijekcij. Potemtakem, ko je $n = 3$, obstaja 6 permutacij:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Za elemente množice $S(n)$ se pogosto uporablja kompaktnejši zapis, imenovan ciklični zapis, ki se izogiba ponavljanju prve vrstice v vsaki permutaciji. Teoretična osnova za ta zapis je predstavljena v nadaljevanju.

Trditev 7.3 *Naj bo* π *element množice* $S(n)$ *in naj bo i poljubno število iz množice* $\{1,...,n\}$. *Naj bo k najmanjše naravno število, za katero je* $\pi^k(i)$ *element množice* $\{i, \pi(i),..., \pi^{k-1}(i)\}$. *Potem je* $\pi^k(i) = i$.

Dokaz. Predpostavimo, da je $\pi^k(i) = \pi^r(i)$ za nek $r > 0$. Potem, ker ima π inverz, je $\pi^{k-r}(i) = i$. To je v nasprotju definicijo števila *k*, zato je $r = 0$. □

Definicija 7.4 *Permutacija* ρ *je k-cikel, če obstajata taki naravni števili k in i, da velja*

(1) k je tako najmanjše naravno število, da je $\rho^k(i) = i$ *; in*

(2) $\rho(j) = j$ *za vsak j, ki ni v* $\{i, \rho(i),..., \rho^{k-1}(i)\}$.

k-cikel ρ *ponavadi označujemo* $(i\ \rho(i)\ ...\ \rho^{k-1}(i))$.

Primer 7.5 Vseh pet elementov grupe $S(3)$, ki so različni od identitete so cikli, in jih lahko zapišemo kot

$$(1\ 2\ 3),\ (1\ 3\ 2),\ (2\ 3),\ (1\ 3) \text{ in } (1\ 2).$$

Identična permutacija, ki fiksira vsakega od elementov 1, 2 in 3, je ponavadi označena z 1. Permutacija

$$\begin{pmatrix} 1\ 2\ 3\ 4 \\ 2\ 1\ 4\ 3 \end{pmatrix}$$

v $S(4)$ ni cikel.

Definicija 7.6 *Permutaciji* $\rho,\ \sigma$ *sta disjunktni, če za vsak* $i \in \{1, ...,\ n\}$ *velja*

$$\rho(i) = i \ \textit{in}\ \sigma(i) \neq i$$

ali obratno

$$\rho(i) \neq i \ \textit{in}\ \sigma(i) = i.$$

Trditev 7.7 *Vsako permutacijo lahko zapišemo kot produkt disjunktnih ciklov.*

Dokaz. Za zapis danega elementa π iz $S(n)$, kot produkt disjunktnih ciklov, začnimo s pridobivanjem dela množice $X = \{1,2,...,n\}$. Najprej naj bo podmnožica množice X določena s π označena s $\mathrm{Fix}(\pi)$, in oblikujmo cikle dolžine 1, kjer vsak $i \in \mathrm{Fix}(\pi)$. Nadalje izberimo najmanjše pozitivno celo število *i*, recimo tak, da ni iz $\mathrm{Fix}(\pi)$. Naj bo r tako najmanjše pozitivno celo število in $r > 1$, da je $\pi^r(i)$ množica $\{i, \pi(i),..., \pi^{r-1}(i)\}$. Potemtakem je, po trditvi 7.3, $\pi^r(i) = i$, tako oblikujemo cikel

$$(i \ \pi(i) \ ... \ \pi^{k-1}(i)).$$

Če obstaja kakšno celo število j, recimo, nedoločeno s π, ki prav tako ni v množici $\{i, \pi(i),..., \pi^{r-1}(i)\}$, in naj bo *s* tako najmanjše pozitivno celo število, da $\pi^s(j)$ pripada množici $\{j, \pi(j),..., \pi^{s-1}(j)\}$. Nadaljujmo v tej smeri in izdelajmo del množice $\{1,...,n\}$ v razčlenjene množice. Če nadaljujemo v tej smeri za množice v delih, lahko pišemo π ko produkt njegovih razčlenjenih ciklov. □

Primer 7.8 Permutacijo

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

lahko zapišemo kot produkt naslednjih ciklov $\pi = (1)(2\ 4)(3\ 6\ 9)(5\ 8)$. Ponavadi cikle dolžine 1 izpuščamo, saj so ta števila fiksirana s π, tako π skrajšano zapišemo $(2\ 4)(3\ 6\ 9)(5\ 8)$.

Po dogovoru se najmanjše število v vsakem ciklu piše na prvem mestu. Tako so cikli $(3\ 6\ 9)$, $(6\ 9\ 3)$ in $(9\ 3\ 6)$ enaki, saj vsak cikel 3 priredi 6, 6 priredi 9 in 9 priredi 3. Pa vendar so različni od cikla $(3\ 9\ 6)$.

Če imamo podan produkt dveh disjunktnih ciklov, ni popolnoma jasno kateri simetrični grupi pripadata permutaciji. Na primer ne vemo, kateri $S(n)$ pripada 2-cikel $(1\ 2)$. Disjunktne cikle lahko množimo, ne da bi navedli, kateri simetrični grupi pripadajo.

Primer 7.9 Poglejmo produkt

$$\pi = (1\ 2\ 4)(3\ 5\ 7\ 9)(1\ 3\ 9)(2\ 3\ 4\ 5\ 6\ 8).$$

Najprej poglejmo vrednost $\pi(1)$. Vrednost dobimo, če začnemo na desni strani zapisa in se 'premikamo' proti levi, s seboj pa 'nesemo' 1, kot aktivni simbol in iščemo prvo 1-ko. Ko jo najdemo, naravno število desno od 1 (v našem primeru 3), postane aktivni simbol. Nadalje se 'premikamo' proti levi in iščemo prvi pojav 3 in v tem primeru postane 5 aktivni simbol. Ker pa se 5 več ne pojavi, levo od te točke, produkt 1 spremeni v 5, tako da je $\pi(1) = 5$. Sedaj računamo vrednost $\pi(5)$, začnemo na desni s 5 kot aktivnim simbolom, tako dobimo spremembo $5 \to 6$. Spet ponovimo in dobimo $6 \to 8$. V nadaljevanju postopek ponovimo z 8 kot aktivnim simbolom. 8 se ponovno spet pojavi na desni strani cikla, tako se pri konstruiranju cikla 8 preslika v 2 oz. v naravno število na levem koncu njegovega cikla, zato vzamemo 2 kot aktivni simbol in nadaljujemo levo od levega konca prvega cikla in dobimo $8 \to 2 \to 4$. Ko nadaljujemo na tak način, vidimo, da je podana permutacija 9-cikel $(1\ 5\ 6\ 8\ 4\ 7\ 9\ 2\ 3)$.
Kot posledica tega pravila sledi naslednja trditev.

Trditev 7.10 *Naj bosta σ in ρ disjunktni permutaciji. Potem je $\sigma\rho = \rho\sigma$ in za vsako naravno število k velja, da je $(\sigma\rho)^k = \sigma^k \rho^k$. Naj bo π produkt disjunktnih ciklov dolžin $k_1,\ k_2,\ ...,\ k_r$, potem je red permutacije π najmanjši skupni večkratnik naravnih števil $k_1,\ k_2,\ ...,\ k_r$.*

Dokaz. Najprej pokažemo, da disjunktne permutacije komutirajo. Če ρ določa *i* potem je $\sigma\rho(i) = \sigma(i)$, medtem ko je $\rho\sigma(i) = \rho(\sigma(i))$. Ker sta ρ in σ razčlenjeni, mora ρ določati $\sigma(i)$ in tako je $\sigma\rho(i) = \rho\sigma(i)$. Po drugi strani pa, če ρ ne določa *i*, potem dejstvo, da sta ρ in σ razčlenjeni pomeni, da mora σ določati *i* in od tod znova sledi, da je $\sigma\rho(i) = \rho\sigma(i)$.
Ker σ in ρ komutirata, nam indukcijski dokaz pokaže, da za vsako pozitivno število *k* velja $(\sigma\rho)^k = \sigma^k \rho^k$. To naredimo v dveh korakih. Najprej pokažemo z indukcijo po *k*, da če je $\sigma\rho = \rho\sigma$ potem je $\sigma\rho^k = \rho^k\sigma$: ko je $k = 1$ sledi iz hipoteze; če predpostavimo, da je $\sigma\rho^k = \rho^k\sigma$, potem

$$\begin{aligned} \sigma\rho^{k+1} &= \sigma\rho^k\rho = \rho^k\sigma\rho \\ &= \rho^k\rho\sigma = \rho^{k+1}\sigma \end{aligned}$$

Potem sledi, prav tako z indukcijo po *k*, da je $(\sigma\rho)^k = \sigma^k \rho^k$: to je jasno, ko je $k = 1$; če je $(\sigma\rho)^k = \sigma^k \rho^k$, potem je

$$\begin{aligned}(\sigma\rho)^{k+1} &= (\sigma\rho)^k \sigma\rho = \sigma^k \rho^k \sigma\rho \\ &= \sigma^k \sigma\rho^k \rho = \sigma^{k+1} \rho^{k+1}.\end{aligned}$$

Upoštevamo, da je red *k*-cikla gotovo *k*. Sedaj predpostavimo, da je π produkt razčlenjenih ciklov

$$\rho_1,\ \rho_2,\ ...,\ \rho_r$$

dolžin $k_1,\ k_2,\ ...,\ k_r$. Naj bo *t* najmanjši skupni večkratnik $k_1,\ k_2,\ ...,\ k_r$. Potem iz tega zgoraj sledi, da je

$$\pi^t = \rho_1^t \rho_2^t ... \rho_r^t,$$

in tako je $\pi^t = 1$. Zaradi tega red π deli *t*. Če je $\pi^s = 1$ potem, ker so cikli razčlenjeni, je vsak $\rho_i^s = 1$ in tako je *s* deljiv z vsakim k_i iz česar sledi, da je s deljiv s *t*. Potemtakem je red π enak *t*. □

Definicija 7.11 *Vsak 2-cikel imenujemo transpozicija.*

Trditev 7.12 *Vsak k-cikel v* $S(n)$ *lahko zapišemo kot produkt* $(k-1)$ *transpozicij.*

Dokaz. Cikel $\pi = (1\ 2\ ...\ k)$ ima faktorizacijo

$$\pi = (1\ k)\ ...\ (1\ 3)(1\ 2).$$

Tako vidimo, da lahko splošni *k*-cikel zapišemo kot,

$$(i_1\ i_k)\ ...\ (i_1\ i_3)(i_1\ i_2).$$ □

Posledica 7.13 *Vsako permutacijo lahko zapišemo kot produkt transpozicij.*

Faktorizacija cikla na transpozicije ni enolično določena. Niti ni res, da je število transpozicij v poljubni faktorizaciji podanega cikla vedno enako, npr. $(1\ 3) = (2\ 3)(1\ 2)(2\ 3)$. Zato je naš naslednji cilj pokazati, da je število transpozicij v poljubnih dveh faktorizacijah podane permutacije v obeh primerih sodo ali v obeh liho.

Definicija 7.14 *Naj bo n poljubno naravno število in naj bo* $f(x_1, x_2, ..., x_n)$ *polinom z n spremenljivkami* $x_1, x_2, ..., x_n$. *Za podan element* π *iz* $S(n)$, *definirajmo* $\pi \cdot f$, *kot polinom dobljen z delovanjem permutacije* π *na indeksih spremenljivk:*

$$f(x_{\pi(1)},\ x_{\pi(2)},\ ...,\ x_{\pi(n)}).$$

Primer 7.15 Če je $\pi = (1\ 2\ 3)$ iz $S(3)$ in

$$f(x_1, x_2, x_3) = x_1^2 + 2x_1x_2 - 4x_1x_2x_3^3,$$

potem je

$$\pi \cdot f = x_2^2 + 2x_2x_3 - 4x_2x_3x_1^3.$$

Trditev 7.16 *Naj bosta* π *in* ρ *elementa* $S(n)$ *in naj bo f poljuben polinom s spremenljivkami* $x_1,\ x_2,\ ...,\ x_n$. *Potem je*

(a) $id \cdot f = f$ *;*

(b) $\pi\rho \cdot f = \pi \cdot (\rho \cdot f)$.

Dokaz. (a) Če je *f* poljuben polinom s spremenljivkami $x_1,\ x_2,\ ...,\ x_n$ oblike

$$f(x_1,\ x_2,\ ...,\ x_n)$$

potem je

$$id \cdot f(x_1,\ x_2,\ ...,\ x_n) = f(x_1,\ x_2,\ ...,\ x_n).$$

(b) Naj bosta $\pi,\ \rho \in S(n)$ in *f* je poljuben polinom, potem je

$$\begin{aligned} &\pi\rho \cdot f(x_1,\ ...,x_n) \\ &= f(x_{\pi(\rho(1))},\ ...,x_{\pi(\rho(n))}) \\ &= \pi \cdot f(x_{\rho(1)},\ ...,x_{\rho(n)}). \end{aligned}$$

Torej $\pi\rho \cdot f = \pi \cdot (\rho \cdot f)$.

□

Definicija 7.17 *Za poljubno naravno število n, naj bo* Δ_n *polinom z n spremenljivkami* $x_1, x_2, ..., x_n$, *definiran s predpisom*

$$\begin{aligned} &\Delta_n(x_1, x_2, ..., x_n) \\ &= (x_1 - x_2)(x_1 - x_3)...(x_1 - x_n)(x_2 - x_3)...(x_2 - x_n)...(x_{n-1} - x_n) \end{aligned}$$

$$= \prod_{1 \le i < j \le n} (x_i - x_j).$$

Za poljubno permutacijo π iz $S(n)$, je $\pi \cdot \Delta_n$ polinom

$$(x_{\pi(1)} - x_{\pi(2)})(x_{\pi(1)} - x_{\pi(3)}) \ldots (x_{\pi(1)} - x_{\pi(n)})(x_{\pi(2)} - x_{\pi(3)}) \ldots (x_{\pi(2)} - x_{\pi(n)}) \ldots (x_{\pi(n-1)} - x_{\pi(n)})$$
$$= \prod_{1 \le i < j \le n} (x_{\pi(i)} - x_{\pi(j)}).$$

Torej $\Delta_n = \pi\Delta_n$ ali $\Delta_n = -\pi\Delta_n$. Namreč, če je $\pi(i) < \pi(j)$ potem imamo v Δ_n faktor $(x_{\pi(i)} - x_{\pi(j)})$. Če je $\pi(j) < \pi(i)$, pa imamo v Δ_n faktor $-(x_{\pi(i)} - x_{\pi(j)})$.

Definicija 7.18 *Če je* $\Delta_n = \pi \cdot \Delta_n$, *je permutacija* π *soda. Če pa je* $\Delta_n = -\pi \cdot \Delta_n$, *rečemo, da je permutacija* π *liha. Če je* π *soda permutacija pišemo* $\operatorname{sgn}(\pi) = 1$, *če pa je* π *liha pa pišemo* $\operatorname{sgn}(\pi) = -1$. *Torej je* $\pi \cdot \Delta_n = \operatorname{sgn}(\pi) \cdot \Delta_n$. *Številu* $\operatorname{sgn}(\pi)$ *pravimo predznak permutacije* π.

Trditev 7.19 *Preslikava* $\operatorname{sgn} : S(n) \to C_2$ *je homomorfizem.*

Dokaz. Pokazati moramo, da je $\operatorname{sgn}(\pi\rho) = \operatorname{sgn}(\pi)\operatorname{sgn}(\rho)$. Dokaz tega je sledeč:

$$\begin{aligned} \operatorname{sgn}(\pi\rho)\Delta_n &= \pi\rho \cdot (\Delta_n) \\ &= \pi \cdot (\rho \cdot \Delta_n) \\ &= \pi \cdot (\operatorname{sgn}(\rho)\Delta_n) \\ &= \operatorname{sgn}(\rho)(\pi \cdot \Delta_n) \\ &= \operatorname{sgn}(\rho)\operatorname{sgn}(\pi)\Delta_n. \end{aligned}$$

Zato je $\operatorname{sgn}(\pi\rho) = \operatorname{sgn}(\rho)\operatorname{sgn}(\pi) = \operatorname{sgn}(\pi)\operatorname{sgn}(\rho)$. □

Posledica 7.20 *Za poljuben element* π *iz* $S(n)$ *velja, da je* $\operatorname{sgn}(\pi^{-1}) = \operatorname{sgn}(\pi)$. *Za poljubna elementa* π, ρ *iz* $S(n)$ *pa velja,*

$$\operatorname{sgn}(\pi\rho\pi^{-1}) = \operatorname{sgn}(\rho).$$

Dokaz. Le-to takoj sledi iz definicije, saj je $\operatorname{sgn}(id) = 1$. Ker je $id = \pi\pi^{-1}$ in trditev nam pokaže, da je $\operatorname{sgn}(\pi)\operatorname{sgn}(\pi^{-1}) = 1$ iz česar pa sledi, da je $\operatorname{sgn}(\pi^{-1}) = \operatorname{sgn}(\pi)$. Ker je

$$\operatorname{sgn}(\rho)\operatorname{sgn}(\pi) = \operatorname{sgn}(\pi)\operatorname{sgn}(\rho)$$

sledi, da je

$$\operatorname{sgn}(\pi\rho\pi^{-1}) = \operatorname{sgn}(\pi)\operatorname{sgn}(\rho)\operatorname{sgn}(\pi) = \operatorname{sgn}(\rho). \qquad \square$$

Posledica 7.21 *Vsaka transpozicija je liha permutacija. k-cikel je soda permutacija natanko tedaj, ko je k liho naravno število.*

Dokaz. Da je transpozicija liha pokažemo v nekaj korakih. Najprej uporabimo dejstvo, da je transpozicija $(1\ 2)$ liha, kar sledi iz definicije sgn z uporabo Δ_n. Če zamenjamo 1 in 2, nam to prinese le spremembo enega znaka v $(1\ 2)\cdot\Delta_n$, ki se pojavi v faktorju $(x_1 - x_2)$. Naslednjo transpozicijo oblike $(1\ k)$ lahko zapišemo kot

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

ki je tako, po posledici 7.20, liha. Končno nam,

$$(l\ k) = (1\ l)(1\ k)(1\ l)^{-1},$$

druga uporaba posledice 7.20 pokaže, da je poljubna transpozicija liha. Po trditvi 7.12 je *k*-cikel, produkt $k-1$ lihih permutacij, sod natanko tedaj, ko je *k* liho celo število. $\square$

Definicija 7.22 *Jedro preslikave* $\operatorname{sgn} : S(n) \to C_2$ *imenujemo alternirajoča grupa* $A(n)$.

Opomba 7.23 *Po izreku o homomorfizmih in dejstvu, da je preslikava* $\operatorname{sgn} : S(n) \to C_2$ *surjektivna sledi, da je alternirajoča grupa* $A(n)$ *množica sodih permutacij v* $S(n)$. *Prav tako sledi, da je* $A(n)$ *podgrupa edinka indeksa 2, ko je* $n \geq 2$. *Grupa* $A(3)$ *sestoji iz treh permutacij* $\{id, (1\ 2\ 3), (1\ 3\ 2)\}$.

Trditev 7.24 *Naj bosta* π *in* ρ *permutaciji v* $S(n)$. *Faktorizacijo permutacije* $\pi\rho\pi^{-1}$ *na cikle dobimo iz ciklične faktorizacije permutacije* ρ *tako, da v tej faktorizaciji vsako število i zamenjamo s* $\pi(i)$.

Dokaz. Poglejmo kako permutacija $\pi\rho\pi^{-1}$ deluje na število $\pi(i)$:

$$\pi\rho\pi^{-1}(\pi(i)) = \pi(\rho(i)).$$

Drugače povedano, $\pi\rho\pi^{-1}$ preslika $\pi(i)$ v $\pi(\rho(i))$. Zato je v faktorizaciji permutacije $\pi\rho\pi^{-1}$ na cikle, število $\pi(i)$ levo od $\pi(\rho(i))$, medtem ko je v fakrorizaciji permutacije ρ na cikle, število *i* levo od $\rho(i)$. □

Trditev 7.25 *Naj bo n naravno število in* $a_k = (k\ k+1)$ *za vsak* $(1 \le k \le n-1)$. *Potem velja* $\langle a_1, ..., a_{n-1} \rangle = S(n)$

$$\begin{aligned} a_k^2 &= 1, \\ (a_k a_{k+1})^3 &= 1, \\ (a_i a_j)^2 &= 1, \end{aligned}$$

za vse $i,\ j,\ k \in \{1, 2, ..., n-1\}$, *kjer je* $|i-j| > 1$.

Dokaz. Najprej pokažemo, da je vsaka transpozicija $(i\ j)$ $(i < j)$ podgrupa $\langle a_1, a_2, ..., a_{n-1} \rangle$. Sedaj uporabimo trditev 7.24, da vidimo rezultat konjugiranja a_i z a_{i+1}, ki nam da $(i\ i+2)$ ter, da nam konjugiranje a_i s produktom $a_{j-1}a_{j-2}...a_{i+1}$ da $(i\ j)$. Ker je vsak cikel produkt transpozicij (po trditvi 7.12) in ker je vsaka permutacija produkt ciklov (po trditvi 7.7) vidimo, da je

$$\langle a_1, a_2, ..., a_{n-1} \rangle = S(n).$$

Podane relacije za a_1, a_2, ..., a_{n-1} so zlahka preverljive, ker sta a_i in a_j razčlenjena, če je $|i-j| > 1$ in če je $a_i a_{i+1}$ 3-cikel $(i\ i+1\ 1+2)$. □

Trditev 7.26 *Naj bo G grupa in H naj bo podgrupa grupe G. Naj bo X množica različnih levih odsekov grupe G po podgrupi H. Za vsak g v G je preslikava* $\vartheta_g : X \to X$, *definirana s predpisom* $\vartheta_g(xH) = gxH$, *permutacija množice X. Preslikava* ϑ, *definirana s predpisom* $\vartheta(g) = \vartheta_g$, *je homomorfizem iz G v simetrično grupo na* $S(X)$, *in jedro te preslikave je podgrupa*

$$\bigcap_{x \in G} xHx^{-1}.$$

Dokaz. Najprej moramo dokazati, da je ϑ_g dobro definirana: če je $xH = yH$, tako da je $y^{-1}x$ v H, potem je $(gy)^{-1}gx = y^{-1}x \in H$, in tako je $\vartheta_g(yH) = \vartheta_g(xH)$. Če pogledamo korake tega argumenta v nasprotnem vrstnem redu vidimo, da je ϑ_g injektivna. Končno, ϑ_g je surjektivna za poljuben levi odsek xH, je $\vartheta_g(g^{-1}xH) = xH$.

Za dokaz, da je ϑ homomorfizem, uporabimo

$\vartheta_{uv}(xH) = uvxH = \vartheta_u(vxH) = \vartheta_u(\vartheta_v(xH))$.

To nam pokaže, da je $\vartheta_{uv} = \vartheta_u\vartheta_v$, tako velja kot je zahtevano, da je $\vartheta(uv) = \vartheta(u)\vartheta(v)$.

Zadnji korak v dokazu pa je izračun jedra preslikave ϑ.

$$\begin{aligned}
\ker(\vartheta) &= \{g \in G : \vartheta_g = id\} \\
&= \{g \in G : \vartheta_g(xH) = xH \ \ za\ \ vsak\ \ x \in G\} \\
&= \{g \in G : gxH = xH \ \ za\ \ vsak\ \ x \in G\} \\
&= \{g \in G : x^{-1}gxH = H \ \ za\ \ vsak\ \ x \in G\} \\
&= \{g \in G : x^{-1}gx \in H \ \ za\ \ vsak\ \ x \in G\} \\
&= \{g \in G : g \in xHx^{-1} \ \ za\ \ vsak\ \ x \in G\} \\
&= \bigcap_{x \in G} xHx^{-1}\ .
\end{aligned}$$

□

Posledica 7.27 *Naj bo H podgrupa grupe G s končnim indeksom n. Potem obstaja taka podgrupa edinka N grupe G, da velja* $N \subseteq H$, $n \| G : N |$ *in* $|G : N \| n!$.

Dokaz. Uporabimo trditev 7.26 na podgrupi *H* in naj bo *N* jedro preslikave ϑ. Potem je *N* podgrupa edinka grupe *G* in *H* vsebuje *N*, tako da je H/N podgrupa grupe G/N z indeksom *n* (po izreku 5.14). Nadalje sledi, da *n* deli $|G : N|$. Prav tako, po trditvi 7.26, je G/N izomorfna podgrupi simetrične grupe $S(n)$ in tako kot je zahtevano $|G : N|$ deli $n!$. □

Posledica 7.28 *(Cayley-ev izrek) Vsaka grupa je izomorfna podgrupi simetrične grupe.*

Dokaz. Uporabimo trditev v primeru, ko je H podgrupa $\{1\}$. Potem je množica X kar grupa G in jedro preslikave ϑ je $\{1\}$. Rezultat potem sledi iz izreka o homomorfizmih (6.13). □

Naš zadnji rezultat bomo dokazali z uporabo trditve 7.24 in tako posplošili dejstvo, ki smo ga obravnavali v primeru 5.7.

Posledica 7.29 *Naj bo G grupa in predpostavimo, da je p najmanjše praštevilo, ki deli* $|G|$. *Če ima grupa G podgrupo H z indeksom p, potem je H podgrupa edinka grupe G.*

Dokaz. Po posledici 7.28 za podgrupo H, obstaja taka podgrupa edinka N, da $|G:N|$ deli $p!$. Ker $|G:N|$ deli $|G|$, deli tudi največji skupni delitelj od $p!$ in $|G|$. Ker je p najmanjše praštevilo, ki deli $|G|$, je največji skupni delitelj od $p!$ in $|G|$ tudi p. Tako je $|G:N| = p = |G:H|$. Ker je N vsebovana v H sledi, da je N enaka H. □

Literatura

[1] Cameron P. J., Introduction to Algebra, Oxford University Press, 1998.

[2] Humphreys J. F., A course in group theory, Oxford University Press, 1997.

[3] Vidav I., Algebra, DFMA – Založništvo, Ljubljana 2003.