UNIVERZA V LJUBLJANI
PEDAGOŠKA FAKULTETA
FAKULTETA ZA MATEMATIKO IN FIZIKO

# DIPLOMSKO DELO

ANJA SMRTNIK

UNIVERZA V LJUBLJANI
PEDAGOŠKA FAKULTETA
FAKULTETA ZA MATEMATIKO IN FIZIKO
**študijski program: Matematika in fizika**

# Klasifikacija grup majhnih redov

**DIPLOMSKO DELO**

**Mentor:**
**doc. dr. Primož Šparl**

**Kandidatka:**
**Anja Smrtnik**

**Ljubljana, junij 2013**

# Zahvala

Najprej bi se rada zahvalila mentorju doc. dr. Primožu Šparlu, ker me je sprejel pod svoje mentorstvo in me spretno vodil v pravo smer. Hvala za vso strokovno pomoč in potrpežljivost pri nastajanju diplomskega dela.

Predvsem iskrena hvala staršema za vso finančno pomoč in moralno podporo v času študija. Hvala tudi mojima sestrama in bratoma, ker verjamejo vame, me spodbujajo in mi vedno priskočijo na pomoč. Brez vas mi ne bi uspelo.

Hvala tudi vsem ostalim, ki ste kakorkoli pripomogli k mojemu uspehu.

# PROGRAM DIPLOMSKEGA DELA

V diplomskem delu obravnavajte grupe majhnih redov. Pokažite, da lahko s pomočjo rezultatov teorije grup, ki ste jih spoznali pri predmetu Algebra 2, klasificirate vse grupe vsaj do reda vključno 15, seveda le do izomorfizma grup natančno. Grupe, ki ne pripadajo kaki dobro znani družini grup, predstavite kot podgrupe ustrezne simetrične grupe, podajte pa tudi njihove tabele produktov.

Ljubljana, november 2011 Mentor: doc. dr. Primož Šparl

# Povzetek

V diplomskem delu obravnavamo algebrske strukture, imenovane grupe. Grupa je množica skupaj z dvočleno operacijo na njej, ki je asociativna, ima nevtralni element, poleg tega pa za vsak element obstaja ustrezni inverz. Običajno jih študiramo do izomorfizma natančno.
S pomočjo osnovnih rezultatov teorije grup, ki smo jih spoznali tekom študija, klasificiramo vse grupe majhnih redov do vključno reda 23, z izjemo grup reda 16, seveda le do izomorfizma grup natančno. Določimo, koliko je vseh grup določenega reda in jih poimenujemo. Prav tako določimo število elementov vsakega možnega reda. Nestandardne grupe predstavimo tudi kot grupe ustreznih permutacij in zanje zapišemo ustrezno tabelo produktov.

**Ključne besede:** grupa, končna grupa, red grupe, izomorfizem grup, izreki Sylowa, klasifikacija grup, tabela produktov

**Klasifikacija MSC (2010):** 20A05, 20D20, 20K01, 20E99

# Abstract

In the present BsC thesis we deal with algebraic structures, called groups. A group is a set closed under a binary operation which is associative, has an identity and in which each element has an inverse. Groups are usually studied up to group isomorphisms.
Using basic results of group theory, encountered during our undergraduate studies, we classify all groups of small orders up to order 23, with the exception of groups of order 16, of course only up to isomorphism of groups. We determine how many groups of a particular order there are and name them. Furthermore, we also determine the number of elements of each possible order. We present all nonstandard groups as groups of corresponding permutations for which a corresponding multiplication table is written.

**Key words:** group, finite group, order of a group, isomorphism of groups, Sylow theorems, classification of groups, group table

**MSC (2010) Classification:** 20A05, 20D20, 20K01, 20E99okok

# Kazalo

**1 Uvod** **1**

**2 Teorija grup** **3**

2.1 Grupa . . . . . 3
2.2 Podgrupa . . . . . 5
2.3 Odseki in Lagrangev izrek . . . . . 6
2.4 Podgrupe edinke in kvocientne grupe . . . . . 10
2.5 Homomorfizem grup . . . . . 11
2.6 Družine grup . . . . . 12
2.7 Direktni produkt grup . . . . . 17
2.8 Center grupe . . . . . 20
2.9 Normalizator podgrupe . . . . . 22
2.10 Cauchyjev izrek in izreki Sylowa . . . . . 23

**3 Klasifikacija grup** **31**

3.1 Grupe reda 1 . . . . . 32
3.2 Grupe reda 2 . . . . . 32
3.3 Grupe reda 3 . . . . . 32
3.4 Grupe reda 4 . . . . . 32
3.5 Grupe reda 5 . . . . . 33
3.6 Grupe reda 6 . . . . . 33

3.7 Grupe reda 7 . . . . . 34
3.8 Grupe reda 8 . . . . . 34
3.9 Grupe reda 9 . . . . . 37
3.10 Grupe reda 10 . . . . . 38
3.11 Grupe reda 11 . . . . . 38
3.12 Grupe reda 12 . . . . . 38
3.13 Grupe reda 13 . . . . . 44
3.14 Grupe reda 14 . . . . . 44
3.15 Grupe reda 15 . . . . . 44
3.16 Grupe reda 16 . . . . . 44
3.17 Grupe reda 17 . . . . . 45
3.18 Grupe reda 18 . . . . . 46
3.19 Grupe reda 19 . . . . . 50
3.20 Grupe reda 20 . . . . . 50
3.21 Grupe reda 21 . . . . . 54
3.22 Grupe reda 22 . . . . . 56
3.23 Grupe reda 23 . . . . . 56

**4 Zaključek** **57**

# Poglavje 1

# Uvod

Grupa je v matematiki eden od osnovnih pojmov sodobne algebre. Teorija grup, ki se z njimi ukvarja, je ena izmed bolj bogatih matematičnih teorij. Eden izmed najbolj markantnih dosežkov te teorije je klasifikacija končnih enostavnih grup. Hkrati pa so grupe tudi temelj drugim algebrskim strukturam, kot so na primer obsegi in vektorski prostori.

Grupa je množica skupaj z dvočleno operacijo na njej, ki je asociativna, ima nevtralni element, poleg tega pa za vsak element obstaja ustrezni inverz. Običajno jih študiramo do izomorfizma natančno.

Namen tega diplomskega dela je klasificirati grupe majhnih redov in določiti vse paroma neizomorfne grupe takšnih redov.

Diplomsko delo je razdeljeno na teoretični del in raziskovalni del. Za začetek bralca seznanimo z osnovnimi pojmi in definicijami teorije grup, ki jih potrebuje za razumevanje nadaljnje vsebine. Nato definiramo pojme direktni produkt, homomorfizem in izomorfizem grup, center grupe in normalizator grupe, ki jih uporabimo v raziskovalnem delu diplomskega dela. Predstavimo še vse družine grup, ki se pojavijo v naši raziskavi. Za konec teoretičnega dela pa predstavimo še Cauchyjev izrek in izreke Sylowa, ki so pri naši raziskavi

zelo pomembni.

V raziskovalnem delu diplomskega dela klasificiramo vse grupe do reda 23, z izjemo grup reda 16. Določimo torej vse paroma neizomorfne grupe do reda 23, pri čemer izpustimo grupe reda 16. Za vse grupe določimo še zaporedje redov. Grupe, ki ne pripadajo kaki dobro znani družini grup, predstavimo kot podgrupe ustrezne simetrične grupe in podamo njihove tabele produktov.

# Poglavje 2

# Teorija grup

V tem poglavju bomo predstavili osnovne pojme in rezultate, ki jih potrebujemo za razumevanje 3. poglavja, v katerem je predstavljena klasifikacija vseh končnih grup do vključno reda 23, z izjemo grup reda 16. Snov tega poglavja je povzeta po [2] in [3].

## 2.1 Grupa

Definirajmo najprej pojem grupe, ki igra osrednjo vlogo v tem diplomskem delu.

**Binarna operacija** na množici $S$ je vsaka preslikava, ki slika iz kartezičnega produkta $S \times S$ nazaj v množico $S$. Običajno jo označimo z oznako $\cdot$, to je

$$\cdot : S \times S \to S.$$

Dogovorimo se, da za $a, b, c \in S$ namesto $c = \cdot(a, b)$ pišemo $c = a \cdot b$.

**Grupa** je urejen par $(G, \cdot)$, kjer je $G$ neprazna množica in $\cdot : G \times G \longrightarrow G$ binarna operacija na $G$, ki zadošča naslednjim aksiomom:

(i) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$, za vse $a, b, c \in G$ ; operacija $\cdot$ je torej **asociativna**,

(ii) obstaja element $e \in G$, tako da za vsak $a \in G$ velja $a \cdot e = e \cdot a = a$; elementu $e$ pravimo **nevtralni element** grupe $G$,

(iii) za vsak $a \in G$ obstaja element $a^{-1}$, da velja $a \cdot a^{-1} = a^{-1} \cdot a = e$; elementu $a^{-1}$ pravimo **inverz** elementa $a$ glede na operacijo $\cdot$.
Iz teh treh aksiomov takoj sledi, da ima grupa $G$ natanko en nevtralni element in da ima poljuben element $a \in G$ natanko en inverz. Oznaki $e$ in $a^{-1}$ sta zato upravičeni.

Dogovorimo se, da za $a \in G$ in nenegativno celo število $n$ namesto $\underbrace{a \cdot a \cdots a}_{n}$ pišemo $a^n$, namesto $\underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{n}$ pa $a^{-n}$.

Če imamo opravka s splošno grupo, se običajno namesto na grupo $(G, \cdot)$ nanašamo kar na grupo $G$ z razumevanjem, da je na $G$ definirana binarna operacija za katero je $G$ grupa.

**Kardinalnost** ali **red** grupe $G$ je enaka kardinalnosti pripadajoče množice $G$. Če je torej $G$ končna množica, gre za število elementov v grupi $G$. Grupa, ki vsebuje neskončno elementov, je neskončnega reda. Red grupe $G$ označimo z $|G|$.

Naj bo $G$ grupa in $g \in G$. **Red** elementa $g$ je najmanjše pozitivno naravno število $n$, da je $g^n = e$. Red elementa $g$ označimo z $|g|$. Če tako število $n$ ne obstaja, pravimo, da je $g$ neskončnega reda. Nevtralni element je edini element reda 1.

Grupa $G$ je **ciklična**, če obstaja tak element $g \in G$, da je $G = \{g^n \mid n \in \mathbb{Z}\}$. V tem primeru element $g$ imenujemo **generator** ciklične grupe $G = \langle g \rangle$. Končna grupa reda $n$ je torej ciklična natanko tedaj, ko premore element reda n.

Kot bomo kmalu videli imajo ciklične grupe zelo posebno lastnost.

Grupa $G$ je **abelska** ali **komutativna**, če za vsak par elementov $a, b \in G$ velja $a \cdot b = b \cdot a$.

**Trditev 2.1** *Vsaka ciklična grupa je abelska.*

Dokaz: Naj bo $G$ ciklična grupa in naj bo $g \in G$ generator grupe $G$. Vzemimo poljubna $x \in G$ in $y \in G$. Tedaj obstajata $i, j \in \mathbb{Z}$, da je $x = g^i$ in $y = g^j$. Izračunajmo produkt teh dveh elementov: $x \cdot y = g^i \cdot g^j = g^{i+j} = g^{j+i} = g^j \cdot g^i = y \cdot x$. Torej je $x \cdot y = y \cdot x$ za vsak $x, y \in G$.
Grupa $G$ je tako res abelska. □

## 2.2 Podgrupa

Neka neprazna podmnožica dane grupe $G$ lahko sama zase tvori grupo za podedovano operacijo. V tem primeru tej podmnožici rečemo **podgrupa** grupe $G$. Tak primer je na primer grupa $(\mathbb{Z}, +)$, ki jo najdemo v grupi $(\mathbb{Q}, +)$.

Da za neko podmnožico $H$ dane grupe $G$ ugotovimo, če je njena podgrupa, ni potrebno preverjati vseh zahtevanih lastnosti. Dovolj se je prepričati, da je množica $H$ neprazna $H \neq \emptyset$ ter da je zaprta za produkte $ab \in H$ in inverze $a^{-1} \in H$, za vse $a, b \in H$. Da je $H$ podgrupa grupe $G$, označimo s $H \leq G$.

Vsaka grupa $G$ ima vsaj dve podgrupi in sicer **trivialno podgrupo** $\{e\}$ in **nepravo** podgrupo $G$. Vse morebitne ostale podgrupe grupe $G$ imenujemo **prave netrivialne** podgrupe grupe $G$.

Naj bo $G$ grupa in $a \in G$. Grupa $H = \{a^n \,|\, n \in \mathbb{Z}\}$ je očitno podgrupa grupe $G$. Pravimo ji **ciklična podgrupa** $\langle a \rangle$ grupe $G$ generirana z elementom $a$.

## 2.3 Odseki in Lagrangev izrek

V tem razdelku bomo dokazali Lagrangev izrek. Gre za pomemben izrek, ki pove, da red podgrupe v dani končni grupi vedno deli red te grupe. Najprej bomo vpeljali pojem odseka, na katerem temelji dokaz Lagrangevega izreka.

Naj bo $H$ podgrupa grupe $G$ in naj bo $a$ poljuben element iz $G$. Množico $aH = \{ah \mid h \in H\}$ imenujemo **levi odsek** podgrupe $H$ v grupi $G$. Podobno je množica $Ha = \{ha \mid h \in H\}$ desni odsek podgrupe $H$ v grupi $G$. Vsakemu elementu $a \in G$ pripada po en levi odsek $aH$ in en desni odsek $Ha$ podgrupe $H$ v grupi $G$.

Kot pokaže naslednja trditev nam levi (desni) odseki podgrupe $H$ v grupi $G$ dajo particijo oziroma razbitje množice $G$.

**Trditev 2.2** *Naj bo $G$ grupa in $H \leq G$ njena podgrupa. Leva odseka $aH$ in $bH$ sta bodisi enaka ali pa nimata nobenega skupnega elementa. Podobno velja za desna odseka $Ha$ in $Hb$.*

Dokaz: Denimo, da imata odseka $aH$ in $bH$ kak skupen element, na primer $ah_1 = bh_2$. Elementa $h_1$ in $h_2$ seveda pripadata podgrupi $H$. Enakost $ah_1 = bh_2$ pomnožimo na desni s $h_2^{-1}$. Dobimo $b = (ah_1)h_2^{-1} = a(h_1h_2^{-1}) = ah$, kjer je $h = h_1h_2^{-1}$ seveda element podgrupe $H$. Poljuben element $bx$ odseka $bH$ lahko sedaj zapišemo v obliki $bx = (ah)x = a(hx)$. Ker je produkt $hx$ v podgrupi $H$, leži $bx$ v odseku $aH$. Tako smo ugotovili, da je $bH \subset aH$. Podobno dokažemo, da je tudi $aH \subset bH$, torej velja $aH = bH$. Če imata torej dva leva odseka kak skupen element, sta enaka. □

Naslednja trditev pokaže, da gre pri particiji grupe $G$ na odseke podgrupe $H$ v grupi $G$ za prav posebno particijo. Vsi deli so namreč enake kardinalnosti.

**Trditev 2.3** *Naj bo $G$ grupa in $H$ njena podgrupa. Poljubna dva leva odseka grupe $G$ po podgrupi $H$ imata enako kardinalnost, ki je enaka kardinalnosti podgrupe $H$. Isto velja za dva desna odseka.*

DOKAZ: Naj bo $aH$ levi odsek podgrupe $H$ v grupi $G$. Poiskali bomo bijekcijo med $aH$ in $H$. Iz tega sledi, da obstaja bijekcija med poljubnima levima odsekoma.
Definirajmo preslikavo $\phi : H \to aH$ s predpisom $\phi(h) = ah$ za vsak $h \in H$. Preslikava $\phi$ je očitno surjektivna. Sedaj predpostavimo, da je $\phi(h_1) = \phi(h_2)$, torej $ah_1 = ah_2$. Pomnožimo enakost $ah_1 = ah_2$ na levi z $a^{-1}$ in dobimo $h_1 = h_2$. Zato je preslikava $\phi$ injektivna. Sklepamo, da je $\phi$ bijekcija. □

Naslednji preprost izrek je fundamentalnega pomena za teorijo grup.

**Izrek 2.4 (Lagrangev izrek)** *Naj bo $G$ končna grupa in $H$ njena podgrupa. Tedaj red podgrupe $H$ deli red grupe $G$.*

DOKAZ: Po trditvi 2.2 sta dva leva odseka $aH$ in $bH$ bodisi enaka bodisi disjunktna. Ker je grupa $G$ končna, tako za primeren nabor elementov $a_1, a_2, \ldots, a_k \in G$ velja

$$G = a_1H \cup a_2H \cup \ldots \cup a_kH, \quad a_iH \cap a_jH = \{\} \quad za \quad 1 \leq i < j \leq k.$$

Po trditvi 2.3 je kardinalnost vsakega odseka $a_iH$ enaka kardinalnosti $|H|$. Torej je $|G| = k|H|$ in zato $|H|$ deli $|G|$. □

Če je $G$ grupa in $H$ njena podgrupa, število levih odsekov podgrupe $H$ v grupi $G$ imenujemo **indeks** podgrupe $H$ v grupi $G$ in ga označimo z $[G : H]$. V primeru, ko je $G$ končna, je seveda $[G : H] = \frac{|G|}{|H|}$.

**Posledica 2.5** *Če je $G$ končna grupa in $g \in G$, potem red elementa $g$ deli red grupe $G$.*

DOKAZ: Ker je grupa $G$ končna, je tudi red elementa $g$ končen. Tedaj je $\langle g \rangle = \{e, g, g^2, g^3 \ldots, g^{|g|-1}\}$ podgrupa grupe $G$ in velja $|\langle g \rangle| = |g|$. Po Lagrangevem izreku 2.4 kardinalnost podgrupe $\langle g \rangle$ deli kardinalnost grupe $G$. Torej red elementa $g$ res deli red grupe $G$. □

**Trditev 2.6** *Če je $G$ grupa praštevilske moči $p$, potem je grupa $G$ ciklična.*

DOKAZ: Naj bo $G$ grupa praštevilske moči $p$ in naj bo $g \in G$, $g \neq e$. Torej mora biti $|g| \geq 2$. Po posledici Lagranegovega izreka 2.5 vemo, da $|g|$ deli moč grupe $G$. Torej je $|g| = |G|$, saj je $|G| = p$. To pa pomeni, da je $\langle g \rangle = G$. Torej je grupa $G$ ciklična. □

**Trditev 2.7** *Naj bo $G$ grupa in naj bosta $a, b \in G$ taka elementa, da je $ab = ba$ in $\langle a \rangle \cap \langle b \rangle = \{e\}$. Potem je red elementa $ab$ enak najmanjšemu skupnemu večkratniku redov elementov $a$ in $b$.*

DOKAZ: Naj bosta $a, b \in G$ taka, da velja $|a| = n$ in $|b| = m$. Trdimo, da je $|ab| = v(|a|, |b|) = v$. Označimo $k = |ab|$. Ker je $v$ najmanjši skupni večkratnik števil $m$ in $n$, lahko zapišemo $v = n \cdot v_1$ in $v = m \cdot v_2$, kjer je $D(v_1, v_2) = 1$.
Torej velja

$$(ab)^v = a^v b^v = a^{n \cdot v_1} b^{m \cdot v_2} = (a^n)^{v_1} (b^m)^{v_2} = e^{v_1} e^{v_2} = e,$$

in tako je $k \leq v$.

Po drugi strani, ker je $(ab)^k = e$, je $a^k = b^{-k}$.

Ker je $a^k \in \langle a \rangle$, $b^{-k} \in \langle b \rangle$ in $\langle a \rangle \cap \langle b \rangle = \{e\}$, je $a^k = b^{-k} = e$.
Po posledici 2.5 sledi $n|k$ in $m|k$. Torej je $k$ skupni večkratnik števil $m$ in $n$. Ker pa je $v$ najmanjši skupni večkratnik teh dveh števil, je $v \leq k$. Torej velja $v = k$, kot smo trdili. □

**Lema 2.8** *Naj bosta $H$ in $K$ končni podgrupi grupe $G$. Potem je*

$$|HK| = \frac{|H||K|}{|H \cap K|}.$$

Dokaz: Enakost $|HK| = \frac{|H||K|}{|H \cap K|}$ zapišimo takole: $|HK| = [H : H \cap K] \cdot |K|$. Presek $H \cap K$ označimo s $C$, indeks $[H : C]$ pa z $n$. Podgrupa $H$ je torej unija disjunktnih odsekov $H = h_1C \cup h_2C \cup \cdots \cup h_nC$ za primerne elemente $h_i \in H$. Zapišemo $HK = (h_1C \cup h_2C \cup \cdots \cup h_nC)K = h_1CK \cup h_2CK \cup \cdots \cup h_nCK$. Podgrupa $C$ je vsebovana v podgrupi $K$, zato je $CK = K$, odtod pa $HK = h_1K \cup h_2K \cup \cdots \cup h_nK$. Odseki $h_1K, h_2K, \ldots, h_nK$ so paroma disjunktni. Prepričajmo se, da to res drži. Ker po trditvi 2.2 vemo, da sta dva odseka bodisi enaka bodisi disjunktna, je dovolj videti, da se za noben $i, j$ ne more zgoditi $h_iK = h_jK$. Predpostavimo, da to velja, torej $h_iK = h_jK$. To pomeni, da je $h_ik_i = h_jk_j$ za neka $k_i, k_j \in K$. Torej je $k_ik_j^{-1} = h_i^{-1}h_j$. Ker je element $k_ik_j^{-1} \in K$, sledi, da je element $h_i^{-1}h_j$ ravno tako element grupe $K$. V tem primeru vidimo, da je element $h_i^{-1}h_j$ hkrati v grupi $H$ in grupi $K$. To pa pomeni, da je $h_iC = h_jC$, kar je v protislovju s predpostavko, da so $h_1C, h_2C, \ldots, h_nC$ ravno vsi odseki grupe $H$ po grupi $C$.
Torej je

$$|HK| = n \cdot |K| = [H : C] \cdot |K| = [H : H \cap K] \cdot |K| = \frac{|H||K|}{|H \cap K|}$$

. □

## 2.4 Podgrupe edinke in kvocientne grupe

Nekatere podgrupe so posebnega pomena, saj omogočajo študij lastnosti dane grupe preko precej manjše, tako imenovane kvocientne grupe.

Naj bo $G$ grupa in $H$ njena podgrupa. Podgrupa $H$ je **podgrupa edinka** grupe $G$, če za vsak $g \in G$ in $h \in H$ velja $g^{-1}hg \in H$ za vsak $g \in G$ in za vsak $h \in H$. To je ekvivalentno z zahtevo, da za vsak $g \in G$ velja $gH = Hg$. Dejstvo, da je $H$ podgrupa edinka v grupi $G$, označimo z $H \triangleleft G$.

V vsaki grupi $G$ sta vsaj dve podgrupi edinki. To sta trivialna podgrupa $\{e\}$ in neprava podgrupa $G$.

Kot pokažeta naslednji trditvi, v določenih primerih velja, da je dana podgrupa avtomatsko tudi njena edinka.

**Trditev 2.9** *Če je grupa $G$ komutativna, potem je vsaka njena podgrupa tudi edinka.*

Dokaz: Naj bo $G$ komutativna grupa. To pomeni, da za vsak $a, b \in G$ velja $ab = ba$. Naj bo $H \leq G$ poljubna podgrupa in $a \in G$ poljuben. Pa poglejmo čemu je enak levi odsek podgrupe $H$.

$$aH = \{ah \mid h \in H\} = \{ha \mid h \in H\} = Ha$$

Torej za vsak $a \in G$ velja $aH = Ha$ in tako je res $H \triangleleft G$. □

**Trditev 2.10** *Naj bo $G$ grupa in $H$ njena podgrupa, ki je indeksa 2. Tedaj je $H \triangleleft G$.*

DOKAZ: Izberimo v $G$ element $a$, ki ne leži v $H$. Grupa $G$ sestoji iz dveh levih odsekov, $H$ in $aH$ oziroma iz dveh desnih odsekov $H$ in $Ha$, to je

$$H \cup aH = G = H \cup Ha.$$

Oba odseka $aH$ in $Ha$ sta komplementa množice $H$ v množici $G$ . Torej sta enaka, to je $aH = Ha$ in tako je $H$ res edinka v $G$. □

Naj bo sedaj $G$ grupa in $H \triangleleft G$ njena edinka. Tedaj lahko na množici $G/H = \{gH \mid g \in G\}$ levih odsekov podgrupe $H$ v grupi $G$ definiramo binarno operacijo s predpisom $(g_1H) \cdot (g_2H) = (g_1 \cdot g_2)H$. Prepričajmo se, da je definicija dobra. Preveriti moramo, da če $g_1H = \widetilde{g_1}H$ in $g_2H = \widetilde{g_2}H$, potem velja $g_1g_2H = \widetilde{g_1}\widetilde{g_2}H$. Odseka $g_1H$ in $\widetilde{g_1}H$ sta enaka natanko tedaj, ko je ${g_1}^{-1}\widetilde{g_1} \in H$. Prav tako velja, da je ${g_2}^{-1}\widetilde{g_2} \in H$. Da preverimo enakost odsekov $g_1g_2H$ in $\widetilde{g_1}\widetilde{g_2}H$, je dovolj videti, da je $(g_1g_2)^{-1}\widetilde{g_1}\widetilde{g_2} \in H$.

$$\begin{aligned}(g_1g_2)^{-1}\widetilde{g_1}\widetilde{g_2} &= {g_2}^{-1}{g_1}^{-1}\widetilde{g_1}\widetilde{g_2} \\ &= {g_2}^{-1}h\widetilde{g_2}, \text{ kjer je } h = {g_1}^{-1}\widetilde{g_1} \in H \\ &= {g_2}^{-1}\widetilde{g_2}({\widetilde{g_2}}^{-1}h\widetilde{g_2})\end{aligned}$$

Ker je $H$ podgrupa edinka, je ${\widetilde{g_2}}^{-1}h\widetilde{g_2} \in H$ in ${g_2}^{-1}\widetilde{g_2} \in H$, tako je tudi $(g_1g_2)^{-1}\widetilde{g_1}\widetilde{g_2} \in H$.

Lahko je preveriti, da na ta način množica $G/H$ postane grupa. Imenujemo jo **kvocientna grupa** grupe $G$ po edinki $H$.

## 2.5 Homomorfizem grup

Kot smo omenili, je grupa neprazna množica skupaj z dvočleno operacijo, ki tej množici da strukturo grupe. Vendar pa se lahko zgodi, da se dve grupi na različnih množicah po strukturi bistveno ne razlikujeta. V tem razdelku bomo definirali, kdaj sta dve grupi bistveno različni.

Naj bosta $(G, \cdot)$ in $(H, \circ)$ grupi. Preslikava $\varphi : G \to H$ je **homomorfizem grup**, če za poljubna $a, b \in G$ velja $\varphi(a \cdot b) = \varphi(a) \circ \varphi(b)$.

Če je homomorfizem $\varphi$ bijektiven, gre za **izomorfizem grup**. Če med grupama $G$ in $H$ obstaja izomorfizem grup, sta grupi **izomorfni**, kar zapišemo z $G \cong H$. Nekoliko ohlapno torej lahko rečemo, da sta dve grupi izomorfni, če lahko eno dobimo iz druge z ustreznim preimenovanjem elementov.

Grupe običajno preučujemo do izomorfizma natančno.

## 2.6 Družine grup

Oglejmo si sedaj nekaj najbolj standardnih družin grup.

### Grupa ostankov pri deljenju z n

Naj bo $n$ naravno število. Na množici $\mathbb{Z}$ vpeljemo ekvivalenčno relacijo $\sim^n$ tako, da je $a \sim^n b \iff n \mid (b - a)$. Namesto $a \sim^n b$ običajno pišemo $a \equiv b \, (mod \, n)$.

Za vsak $a \in \mathbb{Z}$ označimo ekvivalenčni razred elementa $a$ z $[a]$ in ga imenujemo **razred ostankov** elementa $a$ po modulu n. Vsebuje seveda ravno vsa cela števila, ki se razlikujejo od $a$ za večkratnik od $n$:

$$[a] = \{a + kn | \, k \in \mathbb{Z}\} = \{a, a \pm n, a \pm 2n, a \pm 3n, \ldots\}.$$

Kvocient množice $\mathbb{Z}$ po ekvivalenčni relaciji $\sim^n$ je množica ekvivalenčnih razredov $\mathbb{Z} \backslash \sim^n = \{[a]; a \in \mathbb{Z}\}$, ki jo označimo z $\mathbb{Z}_n$.

$$\mathbb{Z}_n = \{[0], [1], [2], \ldots, [n-1]\}$$

Na $\mathbb{Z}_n$ lahko definiramo seštevanje

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

**Trditev 2.11** *Za vsak $n \in \mathbb{Z}$ je $\mathbb{Z}_n$ ciklična grupa reda $n$ za seštevanje po modulu $n$.*

DOKAZ: Najprej moramo preveriti, da je operacija seštevanje po modulu n sploh dobro definirana.
Naj za $a_1, a_2 \in \mathbb{Z}$ in $b_1, b_2 \in \mathbb{Z}$ velja $[a_1] = [b_1]$ in $[a_2] = [b_2]$. Ker je $a_1 \equiv b_1 \pmod{n}$, je število $a_1 - b_1$ deljivo z n. Potem je $a_1 = b_1 + sn$ za nek $s \in \mathbb{Z}$. Prav tako zaradi $a_2 \equiv b_2 \pmod{n}$ velja $a_2 = b_2 + tn$ za nek $t \in \mathbb{Z}$. Potem je $a_1 + a_2 = b_1 + sn + b_2 + tn = (b_1 + b_2) + (s + t)n$. Torej je $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$, od koder sledi, da je vsota kongruenčnih razredov neodvisna od izbranih predstavnikov.

Preverimo še vse aksiome, katerim mora zadoščati grupa.

i) asociativnost se deduje iz $\mathbb{Z}$.

ii) nevtralni element je razred $[0]$.

iii) inverzni element za $[a]$ je $[n - a]$.

Torej je $\mathbb{Z}_n$ res grupa za seštevanje po modulu n. Jasno je, da gre za ciklično grupo, saj je $[1]$ njen generator. □

Dogovorimo se, da v grupi $\mathbb{Z}_n$ namesto $[i]$ pišemo kar $i$. Torej je

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n - 1\}.$$

Trditev 2.6 torej v resnici pokaže, da je do izomorfizma natančno edina grupa reda $p$ ciklična grupa $\mathbb{Z}_p$.

### Simetrična grupa

Naj bo $I_n$ končna množica $\{1, 2, \ldots, n\}$. Množico vseh permutacij množice $I_n$ označimo z $S_n$. Ta množica, opremljena z operacijo komponiranja preslikav, je grupa, ki jo imenujemo **simetrična grupa**. Dogovorimo se, da bomo za operacijo grupe $S_n$ vedno vzeli komponiranje z leve proti desni. Grupa $S_n$ ima $n!$ elementov, kjer je

$$n! = n \cdot (n-1) \cdot (n-2) \cdots 3 \cdot 2 \cdot 1.$$

Vsako permutacijo $\pi \in S_n$ lahko zapišemo v obliki dvovrstičnega simbola

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

Permutaciji $\pi \in S_n$, za katero za neke $1 \leq k \leq n$ in paroma različne $i_1, i_2, \ldots, i_k \in I_n$ velja: $\pi(i_1) = i_2, \pi(i_2) = i_3, \ldots, \pi(i_{k-1}) = i_k, \pi(i_k) = i_1$, za vse $i \in I_n \setminus \{i_1, i_2, \ldots, i_k\}$ pa velja $\pi(i) = i$, imenujemo **cikel** dolžine k. V tem primeru $\pi$ krajše zapišemo kot $(i_1 i_2 i_3 \ldots i_k)$.

Dva cikla sta si tuja, če ne vsebujeta nobenega skupnega elementa. Izkaže se, da lahko vsako permutacijo iz $S_n$ zapišemo kot produkt tujih si ciklov. Na primer permutacijo

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 4 & 3 & 1 & 7 & 6 & 5 & 8 \end{pmatrix} \in S_8$$

lahko zapišemo kot produkt naslednjih tujih si ciklov $\pi = (124)(3)(57)(6)(8)$. Cikle dolžina 1 ponavadi izpuščamo, saj so ta števila fiksirana s $\pi$. Torej $\pi$ skrajšano zapišemo kot $\pi = (124)(57)$.

**Transpozicija** je permutacija, ki zamenja dva elementa, vse ostale pa pusti pri miru. Gre torej za cikel dolžine 2. Vsak cikel in s tem vsaka permutacija je produkt samih transpozicij.

Na primer cikel $\pi = (1354)$ lahko zapišemo kot produkt naslednjih transpozicij $\pi = (13)(15)(14)$.

Izkaže se, da pri tem velja naslednje. Če za neko dano permutacijo $\pi$ velja, da ima v nekem zapisu na produkt samih transpozicij sodo mnogo transpozicij, potem ima vsak zapis $\pi$ na produkt samih transpozicij sodo mnogo transpozicij. Zato sta smiselna naslednja dva pojma.

**Soda permutacija** je permutacija, ki se jo da zapisati kot produkt sodega števila transpozicij. **Liha permutacija** je permutacija, ki se jo da zapisati kot produkt lihega števila transpozicij.

### Alternirajoča grupa

Produkt dveh sodih permutacij je očitno soda permutacija, prav tako pa je soda permutacija tudi inverz poljubne sode permutacije. Označimo množico vseh sodih permutacij iz $S_n$ z $A_n$. Tedaj velja naslednja trditev.

**Trditev 2.12** *Množica $A_n$ je za podedovano operacijo podgrupa edinka v $S_n$.*

Dokaz: Indeks podgrupe $A_n$ v grupi $S_n$ je enak

$$[S_n : A_n] = \frac{|S_n|}{|A_n|} = n! : \frac{n!}{2} = 2.$$

Ker je $[S_n : A_n] = 2$, je po trditvi 2.10 podgrupa $A_n$ res edinka v grupi $S_n$. □

Grupo $A_n$ imenujemo **alternirajoča grupa** na n elementih.

### Diedrska grupa

Oglejmo si grupo $D_{2n}$ vseh simetrij pravilnega n-kotnika. Ker je vsaka simetrija natanko določena s tem, da povemo kam se preslika n oglišč pravilnega n-kotnika, je $D_{2n}$ očitno podgrupa simetrične grupe $S_n$. Diedrska grupa $D_{2n}$ je torej grupa z elementi:

$$id, \rho, \rho^2, \ldots, \rho^{n-1}, \tau, \rho\tau, \rho^2\tau, \ldots, \rho^{n-1}\tau,$$

kjer

$\rho = (1 \quad 2 \quad 3 \quad \ldots \quad n-1 \quad n)$; $\rho : i \mapsto i+1$ , za vsak $i \in I_n \setminus \{n\}$ in $\rho(n) = 1$,

$\tau = (1 \quad n-1)(2 \quad n-2)\cdots(n)$; $\tau : i \mapsto n-i$ , za vsak $i \in I_n \setminus \{n\}$.

**Trditev 2.13** *Naj bo $G$ grupa generirana z dvema elementoma $a, b \in G$. Če je $|b| = 2$ in velja $b \notin \langle a \rangle$ ter $bab = a^{-1}$, potem je $G \cong D_{2n}$, kjer je $|a| = n$.*

Dokaz: Iz zgornje definicije razberemo, da je $D_{2n} = \langle \rho, \tau \rangle$, kjer velja $|\rho| = n$, $|\tau| = 2$, $\tau\rho\tau = \rho^{-1}$.

Ker je grupa $G$ generirana z elementoma $a$ in $b$, lahko vsak element grupe $G$ zapišemo kot produkt elementov $a$, $b$, $a^{-1}$, $b^{-1}$. V grupi $G$ velja $a^n = 1$ in $b^2 = 1$, $a^{-1} = a^{n-1}$ in $b^{-1} = b$, zato je vsak element grupe $G$ produkt samih $a$ in $b$. Z uporabo enačbe $ba = a^{-1}b = a^{n-1}b$ lahko premaknemo vse $a$-je v produktu na levo stran izraza in tako dobimo produkt $a^i b^j$ za $i \in \{0, 1, \ldots, n-1\}$ in za $j \in \{0, 1\}$. Torej smo pokazali, da je

$$G = \{a^i b |\ 0 \leq i \leq n-1, \} \cup \{a^i |\ 0 \leq i \leq n-1\},$$

tako kot v grupi $D_{2\cdot n}$.

Torej se nam ponuja izomorfizem

$$\varphi : G \longrightarrow D_{2n}$$
$$\varphi : a^i b^j \longmapsto \rho^i \tau^j$$

za vsak $i \in \{0, 1, \ldots, n-1\}$ in za $j \in \{0, 1\}$.
Po večkratni uporabi enačbe $ba = a^{-1}b$ dobimo, da je

$$ba^i = baa^{i-1} = a^{-1}ba^{i-1} = a^{-1}baa^{i-2} = a^{-1}a^{-1}ba^{i-2} = a^{-2}ba^{i-2} = \cdots = a^{-i}b$$

za vsak $i \geq 0$ in ker je $a^{-i} = a^{n-i}$, dobimo $ba^i = a^{n-i}b$ za vsak $0 \leq i \leq n-1$.
V grupi $G$ torej velja:
$(a^i)(a^{i'}) = a^{i+i'}$
$(a^i)(a^{i'}b) = a^{i+i'}b$
$(a^ib)(a^{i'}) = a^ia^{n-i'}b = a^{i+n-i'}b$
$(a^ib)(a^{i'}b) = a^ia^{n-i'}bb = a^{i+n-i'}$
Povsem enake zveze veljajo v diedrski grupi $D_{2\cdot n}$, kjer $a$ nadomestimo z $\rho$, $b$ pa s $\tau$. Zato je $\varphi(a^ib^j) = \rho^i\tau^j$ res izomorfizem iz $G$ v $D_{2\cdot n}$. □

## 2.7 Direktni produkt grup

Družine grup, ki smo jih spoznali do sedaj, nam dajo neskončno mnogo grup. Kaj kmalu pa ugotovimo, da obstajajo še druge. V tem razdelku bomo predstavili operacijo na grupah, s katero lahko iz poznanih grup tvorimo povsem nove grupe.

Naj bosta $G$ in $H$ grupi. **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 operacij grup $G$ in $H$.

**Trditev 2.14** *Direktni produkt $G \times H$ grup $G$ in $H$ je grupa za binarno operacijo $(g_1, h_1)(g_2, h_2) = (g_1 g_2, h_1 h_2)$.*

DOKAZ: Preveriti moramo vse aksiome, katerim mora zadoščati grupa. Ker operacijo izvajamo po komponentah in sta $G$ in $H$ grupi, je očitno, da je operacija notranja in asociativna. Prav tako je jasno, da je netvralni element direktnega produkta element $(e_G, e_H)$, kjer sta $e_G \in G$, $e_H \in H$ nevtralna elementa grup $G$ in $H$, in da je $(g, h)^{-1} = (g^{-1}, h^{-1})$, kjer sta $g^{-1}$ in $h^{-1}$ inverza elementov $g$ in $h$ v pripadajočih grupah.

Torej je direktni produkt $G \times H$ res grupa. □

**Trditev 2.15** *Naj bo $(g, h) \in G \times H$. Red elementa $(g, h)$ je enak najmanjšemu skupnemu večkratniku redov elementov $g$ in $h$.*

DOKAZ: Ker je $(g, h) = (g, e_H)(h, e_G)$, elementa $(g, e_H)$ in $(h, e_G)$ pa očitno komutirata, je element $(g, h)$ element komutativne grupe $\langle (g, e_H), (e_G, h) \rangle$. Torej po trditvi 2.7 sledi, da je red elementa $(g, h)$ enak najmanjšemu skupnemu večkratniku redov elementov $(g, e_H)$ in $(e_G, h)$, torej najmanjšemu skupnemu večkratniku redov elementov $g$ in $h$.

□

**Trditev 2.16** *Grupa $\mathbb{Z}_m \times \mathbb{Z}_n$ je izomorfna ciklični grupi $\mathbb{Z}_{m \cdot n}$ natanko tedaj, ko sta $m$ in $n$ tuji si števili.*

DOKAZ: Naj bo $d$ največji skupni deljitelj števil $m$ in $n$. Po trditvi 2.15 je red elementa $(1,1)$ v grupi $\mathbb{Z}_m \times \mathbb{Z}_n$ enak $\frac{mn}{d}$. Po drugi strani za vsak element $(a,b) \in \mathbb{Z}_m \times \mathbb{Z}_n$ velja

$$\frac{mn}{d}(a,b) = (\frac{n}{d}(ma), \frac{m}{d}(nb)) = (0,0).$$

Torej so redi elementov iz te grupe manjši ali enaki $\frac{mn}{d}$. Od tod sledi, da je maksimalen red elementa iz $\mathbb{Z}_m \times \mathbb{Z}_n$ enak $\frac{mn}{d}$.
Grupa $\mathbb{Z}_m \times \mathbb{Z}_n$ je izomorfna ciklični grupi $\mathbb{Z}_{m \cdot n}$ natanko tedaj, ko premore element $(a,b)$ reda $mn$. To pa je možno le, če je $d = 1$, torej ko sta si števili $m$ in $n$ tuji. □

Zgornjo trditev zlahka posplošimo na več faktorjev. Dokaz prepuščamo bralcu.

**Trditev 2.17** *Grupi $\mathbb{Z}_{m_1 \cdot m_2 \cdots m_k}$ in $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k}$ sta izomorfni natanko tedaj, ko so si števila $m_1, m_2, \ldots, m_k$ paroma tuja.*

DOKAZ: Dokaz prepuščamo bralcu. □

**Trditev 2.18** *Naj bosta $H$ in $K$ podgrupi edinki grupe $G$ za kateri velja, da je $HK = G$. Če je nevtralni element edini skupni element podgrup $H$ in $K$, potem je grupa $G$ izomorfna grupi $H \times K$.*

DOKAZ: Poiskati moramo izomorfizem med grupo $G$ in grupo $H \times K$. Definirajmo

$$\varphi : H \times K \to G$$

s predpisom

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

za vsak $x \in H$ in $y \in K$. Preveriti moramo, da je preslikava $\varphi$ homomorfizem in da je bijekcija.

Naj bosta $h \in H$ in $k \in K$ poljubna elementa. Tedaj je $hkh^{-1} \in K$ in $kh^{-1}k^{-1} \in H$, saj sta $H$ in $K$ edinki grupe $G$. Torej je $hkh^{-1}k^{-1} \in H \cap K$ in zato je $hkh^{-1}k^{-1} = e$, to je $hk = kh$. Vsak element iz $H$ torej komutira z vsakim elementom iz $K$.

Za vsak $x, x' \in H$ in za vsak $y, y' \in K$ torej velja

$$\varphi((x,y)(x',y')) = \varphi((xx',yy')) = xx'yy' = xyx'y' = \varphi((x,y))\varphi((x',y')),$$

zato je $\varphi$ homomorfizem grup.

Da preverimo injektivnost privzemimo, da velja $\varphi((x,y)) = \varphi((x',y'))$. Torej je $xy = x'y'$ in zato $x'^{-1}x = y'y^{-1}$. Leva stran pripada grupi $H$, desna stran pa grupi $K$. Torej obe strani pripadata $H \cap K$ in zato sta obe enaki nevtralnemu elementu. To pomeni, da je $x = x'$ in $y = y'$ in zato $(x,y) = (x',y')$. Torej je $\varphi$ injektivna preslikava.

Vemo tudi, da je $HK = G$, kar pomeni, da je vsak element iz grupe $G$ oblike $xy$ za nek $x \in H$ in nek $y \in K$. Zato je preslikava $\varphi$ surjektivna.

Dokazali smo, da je $\varphi$ izomorfizem grup , kar pomeni, da je $H \times K \cong G$. $\square$

## 2.8 Center grupe

V tem razdelku si bomo ogledali posebej odlikovano podgrupo edinko, ki jo premore vsaka grupa in igra pomembno vlogo pri strukturi grupe.

**Center grupe** $G$, ki ga označimo z $Z(G)$, je podmnožica tistih elementov grupe $G$, ki komutirajo z vsemi elementi te grupe:

$$Z(G) = \{a \in G \mid ax = xa, \quad \forall x \in G\}.$$

Center grupe $G$ vedno vsebuje nevtralni element $e$. Če je $Z(G) = \{e\}$, potem rečemo, da je center grupe $G$ trivialen.

**Trditev 2.19** *$Z(G)$ je komutativna podgrupa edinka v $G$.*

DOKAZ: Da je center $Z(G)$ neprazna množica, smo opazili že zgoraj.
Naj bodo $z, u \in Z(G)$ in $a \in G$ poljubni. Potem je

$$a(zu) = (az)u = (za)u = z(au) = z(ua) = (zu)a.$$

Tu smo upoštevali, da je $az = za$ in $au = ua$, saj sta $z, u \in Z(G)$. Torej produkt $zu$ komutira z vsakim elementom grupe $G$ in zato pripada centru $Z(G)$.
Naj bo sedaj $z \in Z(G)$ in $a \in G$. Tedaj velja $za = az$. Pomnožimo z desne in z leve z $z^{-1}$ in dobimo $az^{-1} = z^{-1}a$. Torej tudi inverzni element $z^{-1}$ komutira z $a$. To pomeni, da je hkrati z elementom $z$ tudi $z^{-1}$ v centru $Z(G)$. Torej je center $Z(G)$ grupa.
Ker pa je $aza^{-1} = zaa^{-1} = z$ za vsak $z \in Z(G)$, velja $aZ(G)a^{-1} = Z(G)$ za vse elemente $a \in G$. Zato je center $Z(G)$ edinka v $G$. □

**Trditev 2.20** *Grupa $G$ je abelska natanko tedaj, ko je $Z(G) = G$.*

DOKAZ: Če je $G$ abelska, potem vsi elementi grupe $G$ komutirajo. Torej je $Z(G) = G$. Obratno, če velja $Z(G) = G$, potem vsi elementi grupe $G$ komutirajo. Torej je grupa $G$ abelska. □

**Trditev 2.21** *Grupa $G$ je abelska natanko tedaj, ko je kvocientna grupa $G/Z(G)$ ciklična.*

DOKAZ: Po trditvi 2.19 vemo, da je $Z(G) \triangleleft G$, torej je $G/Z(G)$ res grupa.

Če je $G$ abelska, potem je po trditvi 2.20 $Z(G) = G$. Torej je $G/Z(G) = G/G$ grupa reda 1. V tem primeru je torej grupa $G/Z(G)$ izomorfna $\mathbb{Z}_1$ in je tako res ciklična.

Denimo sedaj, da je kvocientna grupa $G/Z(G)$ ciklična. Torej je

$$G/Z(G) = \langle aZ(G) \rangle = \{Z(G), aZ(G), a^{-1}Z(G), a^2Z(G), a^{-2}Z(G), ...\}$$

in tako

$$G = Z(G) \cup aZ(G) \cup a^{-1}Z(G) \cup a^2Z(G) \cup a^{-2}Z(G) \cup ...$$

Naj bosta $g, h \in G$ poljubna. Radi bi dokazali, da je $gh = hg$. Obstajata $i, j \in \mathbb{Z}$, da je $g \in a^iZ(G)$ in $h \in a^jZ(G)$. Torej obstajata $z_1, z_2 \in Z(G)$, da je $g = a^iz_1$ in $h = a^jz_2$. Ker je $z_1, z_2 \in Z(G)$, sledi

$$gh = a^iz_1a^jz_2 = a^ia^jz_1z_2 = a^ja^iz_1z_2 = a^ja^iz_2z_1 = a^jz_2a^iz_1 = hg.$$

Torej je $G$ res komutativna grupa. □

## 2.9 Normalizator podgrupe

V tem razdelku si bomo ogledali posebno podgrupo, ki nam lahko zagotovi vpogled v strukturo grupe in njenih podgrup.

Naj bo $G$ grupa in $H$ njena podgrupa. **Normalizator** $N_G(H)$ podgrupe $H$ v grupi $G$ je množica vseh tistih elementov grupe $G$, ki pri konjugiranju ohranjajo podgrupo $H$, to je

$$N_G(H) = \{x \in G : x^{-1}Hx = H\}.$$

**Trditev 2.22** *Naj bo $G$ grupa in naj bo $H \leq G$. Tedaj je normalizator $N_G(H)$ podgrupa grupe $G$, ki vsebuje podgrupo $H$. Še več, $H \triangleleft N_G(H)$.*

DOKAZ: Pokažimo najprej, da je normalizator $N_G(H)$ podgrupa grupe $G$. V ta namen je treba pokazati, da je $N_G(H)$ neprazna množica, ki je zaprta za produkte in inverze.
1. $N_G(H)$ ni prazna:
Nevtralni element $e \in G$ je zagotovo vsebovan v $N_G(H)$, saj očitno velja $eHe = H$. Torej množica $N_G(H)$ ni prazna.
2.$N_G(H)$ je zaprta za produkte:
Naj bosta $x, y \in N_G(H)$. Poglejmo, kaj dobimo pri produktu.

$$(xy)^{-1}Hxy = y^{-1}x^{-1}Hxy = y^{-1}Hy = H \Rightarrow xy \in N_G(H)$$

3. $N_G(S)$ je zaprta za inverze:
Naj bo $x \in N_G(H)$. Ker je $x^{-1}Hx = H$, je $H = xHx^{-1} = (x^{-1})^{-1}Hx^{-1}$. Torej je tudi $x^{-1} \in N_G(H)$.

Torej res $N_G(H) \leq G$.

Pokažimo sedaj še, da je $H \triangleleft N_G(H)$.
Ker za vsak $h \in H$ velja $h^{-1}Hh = H$, je $H \leq N_G(H)$. Da je $H \triangleleft N_G(H)$ sedaj sledi po definiciji normalizatorja $N_G(H)$. □

Naj bo $G$ grupa. Elementa $x, y \in G$ sta **konjugirana**, če obstaja tak element $g \in G$, da velja $y = g^{-1}xg$. Lahko se je prepričati, da smo s tem na grupi $G$ vpeljali ekvivalenčno relacijo. Njenim ekvivalenčnim razredom rečemo **razredi konjugiranosti**.

## 2.10 Cauchyjev izrek in izreki Sylowa

V zadnjem razdelku tega poglavja si oglejmo še Cauchyjev izrek ter izreke Sylowa, ki igrajo ključno vlogo v naši klasifikaciji v naslednjem poglavju. Gre

za izreke, ki zagotavljajo obstoj podgrup določenih redov v vsaki grupi.

Bodi p praštevilo. Grupa $G$ je **p-grupa**, če je red vsakega elementa grupe $G$ potenca praštevila p. Podgrupa grupe $G$ je p-podgrupa grupe $G$, če je podgrupa sama p-grupa.

Dokazi Cauchyjevega izreka in izrekov Sylowa so nekoliko daljši in zahtevajo vpeljavo dodatnih pojmov, kot so na primer delovanja grup, orbite in stabilizatorji in podobno. Dokaze je moč najti v skoraj vsaki knjigi, ki vsebuje osnovne teorije grup. Zainteresiranemu bralcu priporočamo knjigo [3].

**Izrek 2.23 (Cauchyjev izrek)** *Naj bo $G$ grupa, katere red je deljiv s praštevilom p. Tedaj $G$ vsebuje vsaj en element reda p.*

DOKAZ: Dokaz najdemo v knjigi [3] na strani 219. □

**Trditev 2.24** *Center končne netrivialne p-grupe $G$ je netrivialen.*

DOKAZ: Grupa $G$ razpade na razrede konjugiranosti. Če z $g_1, g_2, \ldots, g_k$ označimo predstavnike teh razredov, sledi

$$|G| = \sum_{i=1}^{k} |[g_i]|.$$

Izračunajmo, kdaj je $|[g_i]| = 1$, torej, kdaj je $[g_i] = \{g_i\}$.

$$\begin{aligned} & [g_i] = \{g_i\} \\ \iff & \{h^{-1}g_ih : h \in G\} = \{g_i\} \\ \iff & hg_i = g_ih \quad \forall h \in G \\ \iff & g_i \in Z(G). \end{aligned}$$

Recimo, da so predstavniki $g_1, g_2, \ldots, g_l$ centralni, ostali pa ne. Torej velja:

$$|G| = |Z(G)| + \sum_{i=l+1}^{k} |[g_i]|. \tag{2.1}$$

Naj bo $h_1^{-1} g_i h_1 = h_2^{-1} g_i h_2$. Od tod dobimo $g_i = h_1 h_2^{-1} g_i h_2 h_1^{-1} = (h_2 h_1^{-1})^{-1} g_i h_2 h_1^{-1}$. Torej element $h_2 h_1^{-1}$ pripada normalizatorju $N_G(\langle g_i \rangle)$. Od tod sledi $h_2 \in N_G(\langle g_i \rangle) h_1$, zato ležita elementa $h_1$ in $h_2$ v istem desnem odseku $N_G(\langle g_i \rangle) h_1$. Vsi elementi iz istega odseka nam dajo en sam konjugirani element, elementi iz različnih odsekov pa različne konjugirane elemente. Torej ima $[g_i]$ toliko konjugiranih elementov, kolikor je desnih odsekov po podrgupi $N_G(\langle g_i \rangle)$. Število odsekov je enako indeksu podgrupe $N_G(\langle g_i \rangle)$, indeks pa je enak kvocientu med močjo grupe in močjo podgrupe. Torej velja $|[g_i]| = \frac{|G|}{|N_G(\langle g_i \rangle)|}$.

Če je $|G| = p^n$ in vemo, da $g_i \notin Z(G)$, je $|N_G(\langle g_i \rangle)| < p^n$. Ker je $N_G(\langle g_i \rangle) \leq G$ po Lagrangevem izreku 2.4 sledi, da $|N_G(\langle g_i \rangle)| \mid p^n$. Torej je $|N_G(\langle g_i \rangle)| = p^i$ za nek $i < n$.
Iz tega sledi, da je $\frac{|G|}{|N_G(\langle g_i \rangle)|} = \frac{p^n}{p^i} = p^{n-i}$ in $n - i > 0$. To pomeni, da v vsoti na desni strani enačbe 2.1 nastopajo sama števila, dejiva s $p$, zato je celotna vsota deljiva s $p$. Potemtakem $p$ deli tudi $|Z(G)|$ in tako je $|Z(G)| \geq p > 1$.

□

Zgornja trditev ima naslednjo zanimivo posledico.

**Trditev 2.25** *Vsaka grupa $G$, ki je reda $p^2$, kjer je $p$ praštevilo, je abelska.*

Dokaz: Po trditvi 2.20 je grupa $G$ komutativna natanko tedaj, ko je $G = Z(G)$. Po trditvi 2.19 je $Z(G) \triangleleft G$, in tako po Lagrangevem izreku 2.4 velja $|Z(G)| \in \{1, p, p^2\}$. Po trditvi 2.24 je center netrivialen.

Denimo, da je $|Z(G)| = p$. Tedaj je $G/Z(G)$ grupa reda p, ki je torej po trditvi 2.6 ciklična. Tedaj pa je po trditvi 2.21 grupa $G$ komutativna, kar je zaradi $|Z(G)| = p$ nemogoče.

Torej je $|Z(G)| = p^2$, posledično pa je $G = Z(G)$ in zato je grupa $G$ komutativna. □

**Izrek 2.26 (Prvi izrek Sylowa)** *Naj bo $G$ končna grupa in naj bo $|G| = mp^n$, kjer je $n \geq 1$ in je $p$ praštevilo, ki ne deli $m$. Potem $G$ vsebuje podgrupo moči $p^i$ za vsak $1 \leq i \leq n$.*

Dokaz: Dokaz najdemo v knjigi [3] na strani 221. □

V grupi $G$ moči $mp^n$, kjer $(m, p) = 1$ po prvem izreku Sylowa obstajajo tudi podgrupe moči $p^n$. Vsaki taki podgrupi pravimo **sylowska podgrupa** ali **p-Sylowka**.

Število vseh $p$-Sylowk v dani grupi označimo z $n_p$.

**Izrek 2.27 (Drugi izrek Sylowa)** *Naj bo $G$ grupa končnega reda deljivega s praštevilom $p$. Tedaj so vse $p$-Sylowke grupe $G$ konjugirane med seboj.*

Dokaz: Dokaz najdemo v knjigi [3] na strani 221. □

**Posledica 2.28** *Naj bo $G$ grupa in naj bo $P$ njena $p$-Sylowka. Tedaj je $P$ edinka v grupi $G$ natanko tedaj, ko grupa $G$ premore eno samo $p$-Sylowko.*

DOKAZ: Naj bo $P$ $p$-Sylowka v grupi $G$ in naj bo $g$ poljuben element grupe $G$. Tedaj je $g^{-1}Pg$ podgrupa grupe $G$ in velja $|g^{-1}Pg| = |P|$, torej je $g^{-1}Pg$ $p$-Sylowka grupe $G$. 2. izrek Sylowa 2.27 pravi, da so vse $p$-Sylowke med seboj konjugirane. Torej dobimo vse, če izberemo eno in pogledamo vse njene konjugirance. To pa pomeni, da je $n_p = 1$ natanko tedaj, ko velja $g^{-1}Pg = P$ za vse $g \in G$. To pa je le v primeru, ko je $P$ edinka v grupi $G$. □

**Izrek 2.29 (Tretji izrek Sylowa)** *Bodi $G$ grupa moči $mp^n$, kjer $n \geq 1$ in je $p$ praštevilo, ki ne deli $m$. Število $n_p$ vseh $p$-Sylowk v grupi $G$ deli $m$ in je kongruentno 1 po modulu $p$. Če je $H$ poljubna $p$-Sylowka, potem je $n_p = [G : N_G(H)]$.*

DOKAZ: Dokaz najdemo v knjigi [3] na strani 221. □

Izreki Sylowa so zelo močno orodje. Ena izmed njihovih posledic je naslednja zanimiva trditev.

**Trditev 2.30** *Bodita $p > q$ praštevili za kateri velja, da $p \not\equiv 1 (mod\, q)$ in naj bo $G$ grupa moči $pq$. Potem je grupa $G$ ciklična.*

DOKAZ: Naj bo $|G| = pq$, kjer sta $p > q$ praštevili in $p \not\equiv 1 (mod\, q)$. Določimo število p-Sylowk in število q-Sylowk grupe $G$.

p-Sylowke:

Po 1. izreku Sylowa obstaja vsaj ena. Po 3. izreku Sylowa velja:

$n_p \equiv 1 \,(mod\, p) \quad \wedge \quad n_p \mid q.$

Sledi $n_p \in \{1, p+1, \ldots\}$ in $n_p \in \{1, q\}$, od koder zaradi $p+1 > q$ sledi $n_p = 1$.

q-Sylowke:

Po 1. izreku Sylowa obstaja vsaj ena. Po 3. izreku Sylowa velja:

$n_q \equiv 1 \,(mod\, q) \quad \wedge \quad n_q \mid p.$

Sledi $n_q \in \{1, q+1, \ldots\}$ in $n_q \in \{1, p\}$, od koder zaradi $p \not\equiv 1(mod\, q)$ sledi $n_q = 1$.

Po Lagrangevem izreku 2.4 so v grupi $G$ lahko le elementi redov 1, $p$, $q$ in $pq$. Vsak element reda $p$ generira podgrupo reda $p$ in je zato v neki $p$-Sylowki. Ker je $n_p = 1$, ima torej grupa $G$ $p-1$ elementov reda $p$. Prav tako je vsak element reda $q$ v neki $q$-Sylowki. To pomeni, da ima grupa $G$ natanko $q-1$ elementov reda q, saj je $n_q = 1$. Skupaj z nevtralnim elementom je to $1 + p - 1 + q - 1 = p + q - 1$ elementov grupe $G$.

Ker je $p > q$ je $pq \geq 2p = p + p > p + q > p + q - 1$. Torej morajo v grupi $G$ obstajati tudi elementi reda pq. Iz tega sledi, da je $G \cong \mathbb{Z}_{pq}$. □

**Izrek 2.31** *Naj bo $p \geq 3$ praštevilo. Do izomorfizma natančno tedaj obstajata natanko dve grupi reda $2p$ in sicer ciklična grupa $\mathbb{Z}_{2p}$ ter diederska grupa $D_{2p}$.*

Dokaz: Naj bo $G$ grupa reda $2p$. Po Cauchyjevem izreku 2.23 obstaja v grupi $G$ element $a$ reda $p$ in element $b$ reda 2. Podgrupa $\langle a \rangle$ je podgrupa edinka v grupi $G$, saj je indeksa 2. Sledi $b^{-1}ab = a^i$ za nek $0 \leq i \leq p-1$.

$$\begin{aligned} & b^{-1}ab = a^i \\ \Rightarrow\ & b^{-1}b^{-1}abb = b^{-1}a^ib \\ \Rightarrow\ & b^{-2}ab^2 = (b^{-1}ab)^i \\ \Rightarrow\ & eae = (a^i)^i \end{aligned}$$

$$\Rightarrow a = a^{i^2}$$
$$\Rightarrow i^2 \equiv 1 \pmod{p}$$
$$\Rightarrow i \in \{1, p-1\}$$

Dobimo dve možnosti:

1. $b^{-1}ab = a$

V tem primeru torej elementa $a$ in $b$ komutirata. Ker je $a$ reda $p \geq 3$, $b$ pa reda 2, je seveda $\langle a \rangle \cap \langle b \rangle = \{e\}$ in tako je po trditvi 2.7 element $ab$ reda $2p$. Torej je $ab$ generator grupe $G$ in tako je $G$ ciklična grupa, to je $G \cong \mathbb{Z}_{2p}$.

2. $b^{-1}ab = a^{p-1} = a^{-1}$

Po trditvi 2.13 v tem primeru velja $G \cong D_{2.p}$.

Torej sta ciklična grupa $\mathbb{Z}_{2p}$ ter diederska grupa $D_{2p}$ do izomorfizma natančno res edini grupi reda $2p$. □

# Poglavje 3

# Klasifikacija grup

V tem poglavju bomo klasificirali vse grupe dovolj majhnih redov. Raziskali bomo grupe do vključno reda 23, pri čemer bomo izpustili grupe reda 16. Za klasifikacijo grup reda 16 namreč doslej osvojeno znanje ne zadošča. Določili bomo koliko je vseh grup določenega reda, do izomorfizma natančno, jih poimenovali in zapisali zaporedje redov za vsako izmed njih. **Zaporedje redov grupe** je zaporedje, katerega i-ti člen je število elementov reda i, pri čemer navedemo le člene do zadnjega neničelnega. Nekatere grupe, predvsem nestandardne, bomo predstavili tudi kot grupe ustreznih permutacij.

Za nestandardne grupe bomo njihovo grupno strukturo predstavili z grupno tabelo produktov, v kateri so podani vsi produkti po dveh elementov grupe. V grupni tabeli začetna vodoravna vrsta vsebuje vse elemente grupe v določenem vrstnem redu. Prav tako so ti elementi v istem vrstnem redu navedeni v prvem stolpcu. Produkt dveh elementov stoji na križišču ustrezne vrstice in ustreznega stolpca. Vsak element grupe se zaradi pravil krajšanja v vsaki vrstici in v vsakem stolpcu pojavi natanko enkrat. Ta tabela povsem določa strukturo grupe $G$.

## 3.1 Grupe reda 1

Vsaka grupa mora imeti vsaj en element, namreč nevtralni element, zato je najmanjša množica, ki lahko s primerno operacijo tvori grupo, množica z enim elementom $\{e\}$. Edina možna binarna operacija $\cdot$ na $\{e\}$ je definirana kot $e \cdot e = e$. Vsi aksiomi grupe držijo, saj je nevtralni element vedno sam svoj inverz v vsaki grupi. Gre seveda za ciklično grupo $\mathbb{Z}_1$.

zaporedje redov za $\mathbb{Z}_1$: 1

## 3.2 Grupe reda 2

Kot smo že omenili mora vsaka grupa vsebovati nevtralni element, torej $e$. Potrebujemo še en element grupe, ki ga bomo imenovali $a$. Torej bo grupa na dveh elementih oblike $G = \{e, a\}$. Ker pa je moč grupe $|G| = 2$, ki je praštevilo, je po trditvi 2.6 grupa $G$ izomorfna grupi $\mathbb{Z}_2$, ki je potemtakem do izomorfizma natančno edina grupa reda 2.

zaporedje redov za $\mathbb{Z}_2$: 1, 1

## 3.3 Grupe reda 3

Naj bo $G$ grupa reda 3. Podobno kot v prejšnjem primeru gre za grupo praštevilskega reda. Po trditvi 2.6 torej velja $G \cong \mathbb{Z}_3$.

zaporedje redov za $\mathbb{Z}_3$: 1, 0, 2

## 3.4 Grupe reda 4

Naj bo $G$ grupa reda $4 = 2^2$. Po posledici 2.5 so možni redi elementov grupe $G$ 1, 2 in 4. Po trditvi 2.25 je grupa $G$ abelska, saj je red grupe oblike $p^2$,

kjer je p praštevilo.

Denimo, da grupa $G$ premore element reda 4. Potem je $G$ ciklična grupa in tako je $G \cong \mathbb{Z}_4$.

Ostane nam še primer, ko v grupi $G$ nimamo elementa reda 4. Potem so vsi elementi, razen nevtralnega elementa, reda 2. Naj bosta $a, b \in G$ poljubna elementa reda 2, pri čemer $b \notin \langle a \rangle$. Po trditvi 2.9 sta tedaj $\langle a \rangle$ in $\langle b \rangle$ edinki grupe $G$. Ker velja še $\langle a \rangle \cap \langle b \rangle = \{e\}$, je po trditvi 2.18 $G \cong \langle a \rangle \times \langle b \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Po trditvi 2.16 grupi $\mathbb{Z}_4$ in $\mathbb{Z}_2 \times \mathbb{Z}_2$ nista izomorfni.

Torej obstajata do izomorfizma natančno natanko dve grupi reda 4: $\mathbb{Z}_4$ in $\mathbb{Z}_2 \times \mathbb{Z}_2$.

zaporedje redov za $\mathbb{Z}_4$: 1, 1, 0, 2

zaporedje redov za $\mathbb{Z}_2 \times \mathbb{Z}_2$: 1, 3

## 3.5 Grupe reda 5

Naj bo $G$ grupa reda 5. V tem primeru gre zopet za grupo praštevilskega reda. Zato upoštevamo trditev 2.6 in dobimo, da je edina grupa reda 5 ciklična grupa $\mathbb{Z}_5$.

zaporedje redov za $\mathbb{Z}_5$: 1, 0, 0, 0, 4

## 3.6 Grupe reda 6

Naj bo $G$ grupa reda $6 = 2 \cdot 3$. Grupa je reda $2p$, kjer je $p \geq 3$ praštevilo, torej po trditvi 2.31 obstajata natanko 2 grupi reda 6 do izomorfizma natančno in sicer ciklična grupa $\mathbb{Z}_6$ in diederska grupa $D_{2 \cdot 3}$.

zaporedje redov za $\mathbb{Z}_6$: 1, 1, 2, 0, 0, 2

zaporedje redov za $D_{2\cdot 3}$: 1, 3, 2

## 3.7 Grupe reda 7

Naj bo $G$ grupa reda 7. V tem primeru gre zopet za grupe praštevilskega reda. Upoštevamo trditev 2.6 in ugotovimo, da je edina grupa reda 7 ciklična grupa $\mathbb{Z}_7$.

zaporedje redov za $\mathbb{Z}_7$: 1, 0, 0, 0, 0, 0, 6

## 3.8 Grupe reda 8

Naj bo $G$ grupa reda $8 = 2^3$. Po posledici 2.5 so možni redi elementov 1, 2, 4 in 8. Ločimo dva primera glede na to ali je $G$ komutativna grupa ali ne.

1. Naj bo $G$ komutativna grupa.

Denimo najprej, da imamo v grupi $G$ element reda 8. Potem je $G$ ciklična grupa in tako velja $G \cong \mathbb{Z}_8$.

Denimo sedaj, da v grupi $G$ nimamo elementa reda 8, imamo pa element reda 4. Označimo nek element reda 4 z $a$. Če obstaja element $b \in G$ reda 2, različen od $a^2$, je po trditvi 2.18 $G \cong \langle a \rangle \times \langle b \rangle \cong \mathbb{Z}_4 \times \mathbb{Z}_2$. Denimo torej, da je $a^2$ edini element reda 2 v grupi $G$. Vzemimo tedaj poljuben element $b \in G \setminus \langle a \rangle$. Ker je $b$ reda 4, je $b^2 = a^2$. Tedaj je $(ab)^2 = a^2b^2 = e$. Vendar $ab \neq a^2$, ker je nemogoče, saj je $a^2$ edini element reda 2.

Torej je edina možna grupa $G \cong \mathbb{Z}_4 \times \mathbb{Z}_2$.

Denimo sedaj, da v grupi $G$ nimamo elementa reda 4. Torej so, razen nevtralnega elementa, vsi elementi reda 2. Tedaj v grupi $G$ obstajajo različni

elementi $a$, $b$, $c$ reda 2, da je $G = \{e, a, b, c, ab, ac, bc, abc\}$. Ker je $c \neq ab$, je $\langle a, b\rangle \cap \langle c\rangle = e$ in tako je po trditvi 2.18 $G \cong \langle a, b\rangle \times \langle c\rangle$. Prav tako je $\langle a, b\rangle \cong \langle a\rangle \times \langle b\rangle$ in tako sledi $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

2. Naj bo $G$ nekomutativna grupa.

Ker grupa $G$ ni abelska, ni ciklična in tako nima nobenega elementa reda 8. Torej so vsi elementi, razen nevtralnega elementa, reda 2 ali 4. Če bi bili vsi elementi reda 2, potem bi za vsak $a, b \in G$ veljalo $(ab)^2 = e$, to je $abab = e$. Ker pa velja tudi $a^2 = e$, $b^2 = e$, dobimo

$$ba = a^2bab^2 = aababb = a(abab)b = ab.$$

Pridemo do protislovja, saj je grupa $G$ nekomutativna. Torej mora grupa $G$ vsebovati vsaj en element reda 4.
Naj bo $a \in G$ reda 4. Tedaj je $\langle a\rangle$ podgrupa edinka grupe $G$, saj je indeksa 2. Kvocientna grupa $G/\langle a\rangle$ je izomorfna edini grupi reda 2, torej $\mathbb{Z}_2$. Vzemimo nek element $b \notin \langle a\rangle$. Odseka $\langle a\rangle$ in $b\langle a\rangle$ tedaj pokrivata celo grupo. Torej je $b^2 \in \langle a\rangle$. Če je $b^2 = a$ ali $b^2 = a^3$, potem je $b$ reda 8, kar je nemogoče. Torej je $b^2 = e$ ali $b^2 = a^2$.

Ker je $\langle a\rangle$ edinka v grupi $G$, je $b^{-1}ab \in \langle a\rangle$. Ker se pri konjugiranju redi elementov ohranjajo, je $b^{-1}ab = a$ ali $b^{-1}ab = a^3$. Če je $b^{-1}ab = a$, potem velja $ba = ab$. Pridemo do protislovja, saj $G$ ni komutativna grupa. Torej je $b^{-1}ab = a^3$ in $ba = a^3b$.

Za grupo $G$ dobimo dve možnosti glede na to ali je $b$ reda 2 ali 4.

Denimo najprej, da je $b$ reda 2. Tedaj je $G = \langle a, b\rangle$, kjer je $|a| = 4$, $|b| = 2$ in velja $b^{-1}ab = a^3 = a^{-1}$. Torej po trditvi 2.13 velja $G \cong D_{2\cdot 4}$.

Denimo sedaj, da je $b$ reda 4. Tedaj je $G = \langle a, b\rangle$, kjer je $|a| = 4$, $|b| = 4$, $b^2 = a^2$ in velja $ba = a^3b$. Sedaj lahko sestavimo ustrezno grupno tabelo. Da

takšna grupa zares obstaja, ni težko videti. Če vzamemo $a = (1234)(5678) \in S_8$ in $b = (1537)(2846) \in S_8$, je $|a| = |b| = 4$, $a^2 = b^2$ in $b^{-1}ab = a^{-1}$. Za grupo $\langle a, b\rangle$ torej veljajo ravno vse zgornje lastnosti. Tej grupi običajno rečemo kvaternionska grupa, ki jo označimo s $Q_8$ in definiramo kot

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

z naslednjimi produkti:

$$1 \cdot a = a \cdot 1 = a, \qquad \text{za vse } a \in Q_8$$
$$(-1) \cdot (-1) = 1, \qquad (-1) \cdot a = a \cdot (-1) = -a, \qquad \text{za vse } a \in Q_8$$
$$i \cdot i = j \cdot j = k \cdot k = -1$$
$$\begin{aligned} i \cdot j &= k, & j \cdot i &= -k \\ j \cdot k &= i, & k \cdot j &= -i \\ k \cdot i &= j, & i \cdot k &= -j \end{aligned}$$

Pripadajoča grupna tabela je torej

| | $1$ | $-1$ | $i$ | $-i$ | $j$ | $-j$ | $k$ | $-k$ |
|---|---|---|---|---|---|---|---|---|
| $1$ | $1$ | $-1$ | $i$ | $-i$ | $j$ | $-j$ | $k$ | $-k$ |
| $-1$ | $-1$ | $1$ | $-i$ | $i$ | $-j$ | $j$ | $-k$ | $k$ |
| $i$ | $i$ | $-i$ | $-1$ | $1$ | $k$ | $-k$ | $-j$ | $j$ |
| $-i$ | $-i$ | $i$ | $1$ | $-1$ | $-k$ | $k$ | $j$ | $-j$ |
| $j$ | $j$ | $-j$ | $-k$ | $k$ | $-1$ | $1$ | $i$ | $-i$ |
| $-j$ | $-j$ | $j$ | $k$ | $-k$ | $1$ | $-1$ | $-i$ | $i$ |
| $k$ | $k$ | $-k$ | $j$ | $-j$ | $-i$ | $i$ | $-1$ | $1$ |
| $-k$ | $-k$ | $k$ | $-j$ | $j$ | $i$ | $-i$ | $1$ | $-1$ |

Torej obstaja do izomorfizma natančno natanko 5 grup reda 8: $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $D_{2\cdot 4}$ in $Q_8$.

zaporedje redov za $\mathbb{Z}_8$: 1, 1, 0, 2, 0, 0, 0, 4

zaporedje redov za $\mathbb{Z}_4 \times \mathbb{Z}_2$: 1, 3, 0, 4

zaporedje redov za $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$: 1, 7

zaporedje redov za $D_{2\cdot 4}$: 1, 5, 0, 2

zaporedje redov za $Q_8$: 1, 1, 0, 6

## 3.9 Grupe reda 9

Naj bo $G$ grupa reda $9 = 3^2$. Po posledici 2.5 so možni redi elementov grupe $G$ 1, 3 in 9. Po trditvi 2.25 je grupa $G$ abelska, saj je red grupe oblike $p^2$, kjer je p praštevilo.

Denimo, da grupa $G$ premore element reda 9. Potem je $G$ ciklična grupa in tako je $G \cong \mathbb{Z}_9$.

Ostane nam še primer, ko v grupi $G$ nimamo elementa reda 9. Potem so vsi elementi, razen nevtralnega elementa, reda 3. Naj bosta $a, b \in G$ poljubna elementa reda 3, pri čemer $b \notin \langle a \rangle$. Tedaj sta $\langle a \rangle$ in $\langle b \rangle$ edinki grupe $G$, saj je vsaka podgrupa komutativne grupe njena edinka. Po trditvi 2.18 je $G \cong \langle a \rangle \times \langle b \rangle \cong \mathbb{Z}_3 \times \mathbb{Z}_3$.

Po trditvi 2.16 ti dve grupi nista izomorfni.

Torej obstajata do izomorfizma natančno natanko dve grupi reda 9: $\mathbb{Z}_9$ in $\mathbb{Z}_3 \times \mathbb{Z}_3$.

zaporedje redov za $\mathbb{Z}_9$: 1, 0, 2, 0, 0, 0, 0, 0, 6

zaporedje redov za $\mathbb{Z}_3 \times \mathbb{Z}_3$: 1, 0, 8

## 3.10 Grupe reda 10

Naj bo $G$ grupa reda $10 = 2 \cdot 5$. Grupa je reda $2p$, kjer je $p \geq 3$ praštevilo. Po trditvi 2.31 torej obstajata natanko 2 grupi reda 10, do izomorfizma natančno, in sicer ciklična grupa $\mathbb{Z}_{10}$ in diederska grupa $D_{2\cdot 5}$.

zaporedje redov za $\mathbb{Z}_{10}$: 1, 1, 0, 0, 4, 0, 0, 0, 0, 4

zaporedje redov za $D_{2\cdot 5}$: 1, 5, 0, 0, 4

## 3.11 Grupe reda 11

Naj bo $G$ grupa reda 11. V tem primeru gre zopet za grupe praštevilskega reda. Po trditvi 2.6 torej velja $G \cong \mathbb{Z}_{11}$.

zaporedje redov za $\mathbb{Z}_{11}$: 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 10

## 3.12 Grupe reda 12

Naj bo $G$ grupa reda $12 = 3 \cdot 2^2$. Po posledici 2.5 so možni redi elementov v grupi $G$ 1, 2, 3, 4, 6 in 12.

Določimo število 2-Sylowk in 3-Sylowk grupe $G$.

2-Sylowke:

Po 1. izreku Sylowa obstaja vsaj ena. Po 3. izreku Sylowa velja:

$n_2 \equiv 1 \,(mod\, 2) \quad \wedge \quad n_2 \mid 3$

$\Rightarrow n_2 \in \{1, 3, 5, 7, \ldots\} \wedge n_2 \in \{1, 3\}$

$\Rightarrow n_2 \in \{1, 3\}$.

3-Sylowke:

Po 1. izreku Sylowa obstaja vsaj ena. Po 3. izreku Sylowa velja:

$n_3 \equiv 1 \,(mod\, 3) \quad \wedge \quad n_3 \mid 4$

$\Rightarrow n_3 \in \{1, 4, 7, \ldots\} \wedge n_3 \in \{1, 2, 4\}$

$\Rightarrow n_3 = \{1, 4\}.$

3-Sylowke so reda 3 in zato so izomorfne edini grupi reda 3, torej $\mathbb{Z}_3$. 2-Sylowka so reda 4. Ker sta edini grupi reda 4 do izomorfizma natančno $\mathbb{Z}_4$ in $\mathbb{Z}_2 \times \mathbb{Z}_2$, so 2-Sylowke izomorfne eni izmed njiju.

Poglejmo, kaj dobimo pri različnih kombinacijah.

1. $n_3 = 1$ in $n_2 = 1$.

Naj bo $Q$ edina 3-Sylowka in $P$ edina 2-Sylowka. Ker sta $P$ in $Q$ po posledici 2.28 edinki v grupi $G$ in velja $Q \cap P = \{e\}$, po trditvi 2.18 sledi $G \cong Q \times P$. Dobimo dve možnosti, saj je $P \cong \mathbb{Z}_4$ ali $P \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

i) Naj bo $P \cong \mathbb{Z}_4$. Torej je $G \cong \mathbb{Z}_3 \times \mathbb{Z}_4 \cong \mathbb{Z}_{12}$ po trditvi 2.16.

ii) Naj bo $P \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Torej je $G \cong \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \cong \mathbb{Z}_6 \times \mathbb{Z}_2$ po trditvi 2.16.

Po trditvi 2.16 ti dve grupi nista izomorfni.

2. $n_3 = 4$ in $n_2 = 3$.

Ker so vse 3-Sylowke praštevilskega reda 3, imajo po Lagrangevem izreku 2.4 trivialen presek. Tako štiri 3-Sylowke vsebujejo $4 \cdot 2 = 8$ elementov reda 3. To pa pomeni, da grupa $G$ premore natanko štiri elemente redov 1, 2 in 4. Posledično ima grupa $G$ lahko kvečjemu eno 2-Sylowko, kar je v protislovju z $n_2 = 3$. Torej mora biti nujno vsaj ena od Sylowk edinka.

3. $n_3 = 4$, $n_2 = 1$, edina 2-Sylowka pa je izomorfna grupi $\mathbb{Z}_4$.

Naj bo $a \in G$ poljuben element reda 4, $b \in G$ pa poljuben element reda 3. Ker je $\langle a \rangle$ edina 2-Sylowka, je po posledici 2.28 $\langle a \rangle \triangleleft G$ in tako je $b^{-1}ab \in \{a, a^{-1}\}$.

i. $b^{-1}ab = a$

V tem primeru elementa $a$ in $b$ komutirata. Ker je $a$ reda 4, $b$ pa reda 3, je seveda $\langle a \rangle \cap \langle b \rangle = \{e\}$ in tako je po trditvi 2.7 element $ab$ reda 12. Torej je $ab$ generator grupe $G$ in tako je $G$ ciklična grupa. To pa je seveda nemogoče, saj potem velja $n_3 = 1$.

ii. $b^{-1}ab = a^{-1}$
$\Rightarrow b^{-1}b^{-1}abb = b^{-1}a^{-1}b = (b^{-1}ab)^{-1}$
$\Rightarrow b^{-2}ab^2 = a$
$\Rightarrow b^{-3}ab^3 = b^{-1}ab$
$\Rightarrow eae = a^{-1}$
$\Rightarrow a = a^{-1}$
Pridemo do protislovja, saj je $|a| = 4$, torej je $a^{-1} = a^3 \neq a$.

Torej taka grupa ne obstaja.

4. $n_3 = 1$, $n_2 = 3$, 2-Sylowke pa so izomorfne grupi $\mathbb{Z}_4$.

Naj bo $a$ poljuben element reda 3. Edina 3-Sylowka je torej $Q = \langle a \rangle$. Ker so 2-Sylowke ciklične, obstaja element $b \in G$ reda 4. Ker je $\langle a \rangle \triangleleft G$, velja $b^{-1}ab \in \{a, a^{-1}\}$.
Če velja $b^{-1}ab = a$, je $ba = ab$. Kot zgoraj ugotovimo, da je $G$ ciklična grupa, kar je v nasprotju z $n_2 = 3$.

Torej velja $b^{-1}ab = a^{-1}$.

Za grupo $G$ tako velja $G = \langle a, b \rangle$, kjer je $|a| = 3$, $|b| = 4$ in $b^{-1}ab = a^{-1}$. S tem je struktura grupe $G$ natanko določena. Sestoji iz elementov

$$G = \{e, a, a^2, b, b^2, b^3, ab, a^2b, ab^2, a^2b^2, ab^3, a^2b^3\},$$

njena grupna tabela pa je

| | $e$ | $a$ | $a^2$ | $b$ | $b^2$ | $b^3$ | $ab$ | $a^2b$ | $ab^2$ | $a^2b^2$ | $ab^3$ | $a^2b^3$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $e$ | $e$ | $a$ | $a^2$ | $b$ | $b^2$ | $b^3$ | $ab$ | $a^2b$ | $ab^2$ | $a^2b^2$ | $ab^3$ | $a^2b^3$ |
| $a$ | $a$ | $a^2$ | $e$ | $ab$ | $ab^2$ | $ab^3$ | $a^2b$ | $b$ | $a^2b^2$ | $b^2$ | $a^2b^3$ | $b^3$ |
| $a^2$ | $a^2$ | $e$ | $a$ | $a^2b$ | $a^2b^2$ | $a^2b^3$ | $b$ | $ab$ | $b^2$ | $ab^2$ | $b^3$ | $ab^3$ |
| $b$ | $b$ | $a^2b$ | $ab$ | $b^2$ | $b^3$ | $e$ | $a^2b^2$ | $ab^2$ | $a^2b^3$ | $ab^3$ | $a^2$ | $a$ |
| $b^2$ | $b^2$ | $ab^2$ | $a^2b^2$ | $b^3$ | $e$ | $b$ | $ab^3$ | $a^2b^3$ | $a$ | $a^2$ | $ab$ | $a^2b$ |
| $b^3$ | $b^3$ | $a^2b^3$ | $ab^3$ | $e$ | $b$ | $b^2$ | $a^2$ | $a$ | $a^2b$ | $ab$ | $a^2b^2$ | $ab^2$ |
| $ab$ | $ab$ | $b$ | $a^2b$ | $ab^2$ | $ab^3$ | $a$ | $b^2$ | $a^2b^2$ | $b^3$ | $a^2b^3$ | $e$ | $a^2$ |
| $a^2b$ | $a^2b$ | $ab$ | $b$ | $a^2b^2$ | $a^2b^3$ | $a^2$ | $ab^2$ | $b^2$ | $ab^3$ | $b^3$ | $a$ | $e$ |
| $ab^2$ | $ab^2$ | $a^2b^2$ | $b^2$ | $ab^3$ | $a$ | $ab$ | $a^2b^3$ | $b^3$ | $a^2$ | $e$ | $a^2b$ | $b$ |
| $a^2b^2$ | $a^2b^2$ | $b^2$ | $ab^2$ | $a^2b^3$ | $a^2$ | $a^2b$ | $b^3$ | $ab^3$ | $e$ | $a$ | $b$ | $ab$ |
| $ab^3$ | $ab^3$ | $b^3$ | $a^2b^3$ | $a$ | $ab$ | $ab^2$ | $e$ | $a^2$ | $b$ | $a^2b$ | $b^2$ | $a^2b^2$ |
| $a^2b^3$ | $a^2b^3$ | $ab^3$ | $b^3$ | $a^2$ | $a^2b$ | $a^2b^2$ | $a$ | $e$ | $ab$ | $b$ | $ab^2$ | $b^2$ |

Da ta tabela zares predstavlja grupo, se prepričamo z eksplicitno konstrukcijo. Vzemimo $a = (123) \in S_7$ in $b = (23)(4567) \in S_7$ in naj bo $T = \langle a, b \rangle \leq S_7$. Tedaj je $|a| = 3$, $|b| = 4$ in velja $b^{-1}ab = a^{-1}$. Grupa $T$ je reda 12 in ima prav takšno grupno tabelo kot smo jo opisali zgoraj. Taka grupa torej res obstaja.

5. $n_3 = 1$, $n_2 = 3$, 2-Sylowke pa so izomorfne grupi $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Naj bo $a$ poljuben element reda 3 in naj bo $P = \{e, b, c, bc\}$ poljubna 2-Sylowka.

Ker je $\langle a \rangle \triangleleft G$, velja $bab$, $cac$, $bcabc \in \langle a \rangle$. Če $b$, $c$ in $bc$ vsi komutirajo z $a$, je $G$ komutativna grupa. Pridemo do protislovja, saj so pri komutativnih grupah vse podgrupe edinke, v našem primeru pa 2-Sylowke niso edinke. Torej vsaj eden od elementov $b$, $c$, $bc$ ne komutira z $a$. Brez škode za splošnost lahko privzamemo $b^{-1}ab = a^{-1}$.

Če velja še $c^{-1}ac = a^{-1}$, je $(bc)^{-1}abc = c^{-1}b^{-1}abc = c^{-1}a^{-1}c = a$. Če pa je $cac^{-1} = a$, je $bca(bc)^{-1} = bcac^{-1}b^{-1} = bab^{-1} = a^{-1}$. Torej natanko eden od

elementov $b$, $c$, $bc$ komutira z $a$. Brez škode za splošnost smemo privzeti, da je $ca = ac$. Element $ac \in G$ ima torej po trditvi 2.7 red 6.
Ker je $|b| = 2$ in je $c$ edini element reda 2 v grupi $\langle ac \rangle$, sledi $b \notin \langle ac \rangle$.

Torej je grupa $G$ generirana z dvema elementoma in sicer $G = \langle ac, b \rangle$. Pri tem velja $|ac| = 6$ in $|b| = 2$. Poglejmo si še, čemu je enak konjugirani element $b^{-1}acb$.
$b^{-1}(ac)b = b^{-1}acb = b^{-1}abc = a^{-1}c = (ac)^{-1}$. Torej v grupi $G$ še velja, da je $b^{-1}acb = (ac)^{-1}$.

Po trditvi 2.13 je torej $G \cong D_{2 \cdot 6}$.

6. $n_3 = 4$, $n_2 = 1$, edina 2-Sylowka pa je izomorfna grupi $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Naj bo $Q$ poljubna 3-Sylowka, naj bo $a \in G$ tak, da je $\langle a \rangle = Q$ in naj bo $P = \{e, b, c, bc\}$ edina 2-Sylowka.

Ker je $P \triangleleft G$, je $a^{-1}ba \in P$. Torej je $a^{-1}ba = \{b, c, bc\}$.
Če je $a^{-1}ba = b$, je $a^{-1}ca = bc$ (sicer je $G$ komutativna grupa), in tako $a^{-1}bca = a^{-1}baa^{-1}ca = bbc = c$. Torej je $c = a^{-3}ca^3 = a^{-1}a^{-2}ca^2a = a^{-1}ca = bc$, kar je nemogoče.

Brez škode za splošnost smemo torej privzeti, da je $a^{-1}ba = c$.

Poglejmo si, čemu je enak element $a^{-1}ca$.
$a^{-1}ca \neq c$, saj je $a^{-1}ba = c$ in $b \neq c$.
$a^{-1}ca \neq b$, saj je v tem primeru $a^{-1}a^{-1}caa = a^{-1}(a^{-1}ca)a = a^{-1}ba = c$, torej je $c = a^{-3}ca^3 = a^{-1}a^{-2}ca^2a = a^{-1}ca = b$, kar ni mogoče.

Torej je $a^{-1}ca = bc$. Po lemi 2.8 je $|\langle a \rangle \cdot \langle b, c \rangle| = \frac{3 \cdot 4}{1} = 12$, in tako je $G = \langle a, b, c \rangle$.

Dobimo torej grupo $G = \langle a, b, c \rangle$, kjer je $a^3 = e$, $b^2 = e$, $c^2 = e$, $bc = cb$, $a^{-1}ba = c$, $a^{-1}ca = bc$. S tem je struktura grupe $G$ natanko določena. Sestoji iz elementov

$$G = \{e, b, c, bc, a, a^2, a^2bc, ac, abc, a^2b, a^2c, ab\},$$

njena grupna tabela pa je

| | $e$ | $b$ | $c$ | $bc$ | $a$ | $a^2$ | $a^2bc$ | $ac$ | $abc$ | $a^2b$ | $a^2c$ | $ab$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $e$ | $e$ | $b$ | $c$ | $bc$ | $a$ | $a^2$ | $a^2bc$ | $ac$ | $abc$ | $a^2b$ | $a^2c$ | $ab$ |
| $b$ | $b$ | $e$ | $bc$ | $c$ | $ac$ | $a^2bc$ | $a^2$ | $a$ | $ab$ | $a^2c$ | $a^2b$ | $abc$ |
| $c$ | $c$ | $bc$ | $e$ | $b$ | $abc$ | $a^2b$ | $a^2c$ | $ab$ | $a$ | $a^2$ | $a^2bc$ | $ac$ |
| $bc$ | $bc$ | $c$ | $b$ | $e$ | $ab$ | $a^2c$ | $a^2b$ | $abc$ | $ac$ | $a^2bc$ | $a^2$ | $a$ |
| $a$ | $a$ | $ab$ | $ac$ | $abc$ | $a^2$ | $e$ | $bc$ | $a^2c$ | $a^2bc$ | $b$ | $c$ | $a^2b$ |
| $a^2$ | $a^2$ | $a^2b$ | $a^2c$ | $a^2bc$ | $e$ | $a$ | $abc$ | $c$ | $bc$ | $ab$ | $ac$ | $b$ |
| $a^2bc$ | $a^2bc$ | $a^2c$ | $a^2b$ | $a^2$ | $b$ | $ac$ | $ab$ | $bc$ | $c$ | $abc$ | $a$ | $e$ |
| $ac$ | $ac$ | $abc$ | $a$ | $ab$ | $a^2bc$ | $b$ | $c$ | $a^2b$ | $a^2$ | $e$ | $bc$ | $a^2c$ |
| $abc$ | $abc$ | $ac$ | $ab$ | $a$ | $a^2b$ | $c$ | $b$ | $a^2bc$ | $a^2c$ | $bc$ | $e$ | $a^2$ |
| $a^2b$ | $a^2b$ | $a^2$ | $a^2bc$ | $a^2c$ | $c$ | $abc$ | $a$ | $e$ | $b$ | $ac$ | $ab$ | $bc$ |
| $a^2c$ | $a^2c$ | $a^2bc$ | $a^2$ | $a^2b$ | $bc$ | $ab$ | $ac$ | $b$ | $e$ | $a$ | $abc$ | $c$ |
| $ab$ | $ab$ | $a$ | $abc$ | $ac$ | $a^2c$ | $bc$ | $e$ | $a^2$ | $a^2b$ | $c$ | $b$ | $a^2bc$ |

Vzemimo sedaj elemente $a = (123)$, $b = (13)(24)$ in $c = (12)(34)$ grupe $A_4$. Tedaj je seveda $A_4 = \langle a, b, c \rangle$, poleg tega pa za te elemente veljajo vse zgornje relacije. Zgornja tabela torej ustreza ravno grupni tabeli grupe $A_4$.

S tem je klasifikacija grup reda 12 končana. Obstaja 5 grup reda 12 do izomorfizma natančno: $\mathbb{Z}_{12}$, $\mathbb{Z}_6 \times \mathbb{Z}_2$, $T$, $D_{2\cdot 6}$ in $A_4$.

zaporedje redov za $\mathbb{Z}_{12}$: 1, 1, 2, 2, 0, 2, 0, 0, 0, 0, 0, 4

zaporedje redov za $\mathbb{Z}_6 \times \mathbb{Z}_2$: 1, 3, 2, 0, 0, 6

zaporedje redov za $T$: 1, 1, 2, 6, 0, 2

zaporedje redov za $D_{2\cdot 6}$: 1, 7, 2, 0, 0, 2

zaporedje redov za $A_4$: 1, 3, 8

## 3.13 Grupe reda 13

Naj bo $G$ grupa reda 13. V tem primeru gre za grupo praštevilskega reda. Po trditvi 2.6 torej velja $G \cong \mathbb{Z}_{13}$.

zaporedje redov za $\mathbb{Z}_{13}$: 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 12

## 3.14 Grupe reda 14

Naj bo $G$ grupa reda $14 = 2 \cdot 7$. Grupa je reda $2p$, kjer je $p \geq 3$ praštevilo. Po trditvi 2.31 torej obstajata natanko dve grupi reda 14, do izomorfizma natančno, in sicer ciklična grupa $\mathbb{Z}_{14}$ in diederska grupa $D_{2\cdot 7}$.

zaporedje redov za $\mathbb{Z}_{14}$: 1, 1, 0, 0, 0, 0, 6, 0, 0, 0, 0, 0, 0, 6

zaporedje redov za $D_{2\cdot 7}$: 1, 7, 0, 0, 0, 0, 6

## 3.15 Grupe reda 15

Naj bo $G$ grupa reda $15 = 5 \cdot 3$. Ker sta 5 in 3 praštevili in velja $5 \not\equiv 1 (mod 3)$, po trditvi 2.30 vemo, da je grupa $G$ ciklična. Torej je $G \cong \mathbb{Z}_{15}$.

zaporedje redov za $\mathbb{Z}_{15}$: 1, 0, 2, 0, 4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 8

## 3.16 Grupe reda 16

Kot smo omenili že na začetku tega poglavja, klasifikacije grup reda 16 ne bomo navedli. Znanje, ki smo ga osvojili tekom študija, namreč za kaj takega ni zadostno. Izkaže se, da obstaja 14 paroma neizomorfnih grup reda 16. Od tega je 5 komutativnih grup: $\mathbb{Z}_{16}$, $\mathbb{Z}_8 \times \mathbb{Z}_2$, $\mathbb{Z}_4 \times \mathbb{Z}_4$, $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ in $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Poiskati znamo še tri nekomutativne grupe, in sicer $D_{2\cdot 8}$,

$\mathbb{Z}_2 \times D_{2\cdot 4}$ in $\mathbb{Z}_2 \times Q_8$. Preostalih šest nekomutativnih grup je nekoliko težje konstruirati.

zaporedje redov za $\mathbb{Z}_{16}$: 1, 1, 0, 2, 0, 0, 0, 4, 0, 0, 0, 0, 0, 0, 0, 8

zaporedje redov za $\mathbb{Z}_8 \times \mathbb{Z}_2$: 1, 3, 0, 4, 0, 0, 0, 8

zaporedje redov za $\mathbb{Z}_4 \times \mathbb{Z}_4$: 1, 3, 0, 12

zaporedje redov za $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$: 1, 7, 0, 8

zaporedje redov za $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$: 1, 15

zaporedje redov za $D_{2\cdot 8}$: 1, 9, 0, 2, 0, 0, 0, 4

zaporedje redov za $\mathbb{Z}_2 \times D_{2\cdot 4}$: 1, 11, 0, 4

zaporedje redov za $\mathbb{Z}_2 \times Q_8$: 1, 3, 0, 12

Opazimo, da imata grupa $\mathbb{Z}_4 \times \mathbb{Z}_4$ in grupa $\mathbb{Z}_2 \times Q_8$ enako zaporedje redov. Grupi sta očitno neizomorfni, saj je grupa $\mathbb{Z}_4 \times \mathbb{Z}_4$ abelska grupa $\mathbb{Z}_2 \times Q_8$ pa je neabelska.

## 3.17 Grupe reda 17

Naj bo $G$ grupa reda 17. V tem primeru gre za grupo praštevilskega reda, torej po trditvi 2.6 velja $G \cong \mathbb{Z}_{17}$.

zaporedje redov za $\mathbb{Z}_{17}$: 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 16

## 3.18 Grupe reda 18

Naj bo $G$ grupa reda $18 = 2 \cdot 3^2$. Po posledici 2.5 so možni redi elementov 1, 2, 3, 6, 9 in 18.

Določimo število 2-Sylowk in 3-Sylowk grupe $G$.

2-Sylowke:

Po 1. izreku Sylowa obstaja vsaj ena. Po 3. izreku Sylowa velja:

$n_2 \equiv 1 \, (mod \, 2) \quad \wedge \quad n_2 \mid 9$

$\Rightarrow n_2 \in \{1, 3, 5, 7, 9, 11 \ldots\} \wedge n_2 \in \{1, 3, 9\}$

$\Rightarrow n_2 \in \{1, 3, 9\}$.

3-Sylowke:

Po 1. izreku Sylowa obstaja vsaj ena. Po 3. izreku Sylowa velja:

$n_3 \equiv 1 \, (mod \, 3) \quad \wedge \quad n_3 \mid 2$

$\Rightarrow n_3 \in \{1, 4, 7, \ldots\} \wedge n_3 \in \{1, 2\}$

$\Rightarrow n_3 = 1$.

Torej je 3-Sylowka edinka; označimo jo s $Q$. Naj bo $P$ poljubna 2-Sylowka. Ker je $|P| = 2$, je $P \cong \mathbb{Z}_2$.
Velja tudi $|Q| = 9$. Ker sta, do izomorfizma natančno, edini grupi reda 9 $\mathbb{Z}_9$ in $\mathbb{Z}_3 \times \mathbb{Z}_3$, je grupa $Q$ izomorfna eni izmed njiju.

Poglejmo, kaj dobimo pri različnih kombinacijah.

1. $n_2 = 1$

V tem primeru je $Q$ edina 3-Sylowka, $P$ pa edina 2-Sylowka. Tako $P$ kot $Q$ sta tedaj edinki grupe $G$. Po Lagrangevem izreku 2.4 je $P \cap Q = \{e\}$

in tako je po lemi 2.8 $|PQ| = \frac{2 \cdot 9}{1} = 18$. Iz tega sledi, da je $PQ = G$. Po trditvi 2.18 sledi $G \cong P \times Q$. Dobimo dve možnosti glede na to ali je $Q \cong \mathbb{Z}_9$ ali $Q \cong \mathbb{Z}_3 \times \mathbb{Z}_3$.

i) Naj bo $Q \cong \mathbb{Z}_9$. Torej je $G \cong \mathbb{Z}_2 \times \mathbb{Z}_9 \cong \mathbb{Z}_{18}$ po trditvi 2.16.

ii) Naj bo $Q \cong \mathbb{Z}_3 \times \mathbb{Z}_3$. Torej je $G \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \cong \mathbb{Z}_6 \times \mathbb{Z}_3 \ncong \mathbb{Z}_{18}$ po trditvi 2.16.

2. $n_2 = 9$

Ker so 2-Sylowke praštevilskega reda, se po Lagrangevem izreku 2.4 trivialno sekajo. Torej nam 2-Sylowke dajo 9 elementov reda 2. Ker je 3-Sylowka $Q$ reda 9 in je $G$ reda 18, podgrupa $Q$ sestoji ravno iz preostalih devetih elementov grupe $G$. Naj bo $b \in G$ tak, da je $|b| = 2$. Tedaj seveda velja $b \notin Q$. Ker je $[G : Q] = 2$, je $G = Q \cup Qb$. Če je $a \in Q$, potem ima element $ab$ red 2, saj $ab \notin Q$.

Torej $(ab)^2 = 1$

$$\Rightarrow abab = 1$$
$$\Rightarrow bab = a^{-1}.$$

2.1) $Q \cong \mathbb{Z}_9$

V tem primeru za nek $a \in G$ velja $Q = \langle a \rangle$. Ker velja še $G = Q \cup Qb$, je potem $G = \{e, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, b, ab, a^2b, a^3b, a^4b, a^5b, a^6b, a^7b, a^8b\}$.

Torej v grupi $G$ velja $|a| = 9$, $|b| = 2$ in $bab = a^{-1}$. Po trditvi 2.13 je $G \cong D_{2 \cdot 9}$.

2.2) $Q \cong \mathbb{Z}_3 \times \mathbb{Z}_3$

V tem primeru v grupi $G$ obstajata elementa $a, c$ reda 3, da je $ac = ca$ in velja $Q = \{e, a, a^2, c, c^2, ac, a^2c, ac^2, a^2c^2\}$. Ker je $G = Q \cup Qb$, je potem

$$G = \{e, a, a^2, c, c^2, ac, a^2c, ac^2, a^2c^2, b, ab, a^2b, cb, c^2b, acb, a^2cb, ac^2b, a^2c^2b\}$$

in za vsak $q \in Q$ velja $bq = q^{-1}b$. S tem je struktura take grupe natanko določena. Grupno tabelo najdemo v prilogi, in sicer je to tabela 1. Take grupe do sedaj še nismo spoznali. Prepričajmo se, da taka grupa zares obstaja.

Oglejmo si naslednje elemente simetrične grupe $S_6$. Naj bo $a = (123)$, $c = (456)$ in $b = (23)(56)$. Velja $|a| = |c| = 3$, $|b| = 2$, $ac = ca$ in $bab = a^{-1}$ ter $bcb = c^{-1}$. Grupa $G_{18} = \langle a, b, c \rangle \leq S_6$ je torej grupa reda 18 z zgoraj opisanimi lastnostmi, torej tabela 1 res podaja grupo.

3. $n_2 = 3$

Po 3. izreku Sylowa je število vseh 2-Sylowk enako indeksu normalizatorja $N_G(P)$ v grupi $G$, kjer je $P$ poljubna 2-Sylowka grupe $G$. Velja torej $[G : N_G(P)] = 3$ in tako je $|N_G(P)| = 6$. Analizirajmo oba primera glede na to kateri grupi je izomorfna 3-Sylowka $Q$.

3.1.) $Q \cong \mathbb{Z}_9$

Naj bo $a \in G$ reda 9. Torej je $Q \cong \langle a \rangle$. Naj bo $b$ reda 2. Torej je $bab \in \langle a \rangle$, to je

$$
\begin{aligned}
& bab = a^i \text{ za nek } i \in \{1, 2, 4, 5, 7, 8\}. \text{ Sledi} \\
& bbabb = b(bab)b \\
& \Rightarrow b^2ab^2 = ba^ib \\
& \Rightarrow eae = (bab)^i \\
& \Rightarrow a = (a^i)^i \\
& \Rightarrow a = a^{i^2} \\
& \Rightarrow i^2 \equiv 1 \pmod 9 \\
& \Rightarrow i \in \{1, 8\}.
\end{aligned}
$$

3.1.1) $i = 1$

Če je $b^{-1}ab = a$, pridemo do protislovja, saj je potem grupa $G$ abelska.

3.1.2) $i = 8 = -1$

V tem primeru je $G = \langle a, b \rangle$, kjer je $|a| = 9$, $|b| = 2$ in velja $bab = a^{-1}$. Po trditvi 2.13 je tedaj $G \cong D_{2\cdot 9}$, kar pa je nemogoče zaradi $n_2 = 3$.

3.2.) $Q \cong \mathbb{Z}_3 \times \mathbb{Z}_3$

Naj bosta $a, b \in G$ taka, da je $|a| = |b| = 3$, $ab = ba$ in $Q = \langle a, b \rangle$. Naj bo $c$ poljuben element reda 2. Ker je $|N_G(\langle c \rangle)| = 6$ in podgrupa $\langle a, b \rangle$ vsebuje vse elemente reda 3, obstaja $x \in \langle a, b \rangle$, da je $xc = cx$. Brez škode za splošnost smemo privzeti $x = a$. Torej velja $cac = a$.
Ker je $\langle a, b \rangle \triangleleft G$, je $cbc = a^i b^j$ za neka $0 \leq i, j \leq 2$. Iz tega sledi, da je $b = c^2 bc^2 = ca^i b^j c = a^i cb^j c = a^i (a^i b^j)^j = a^{i+ij} b^{j^2}$.
Torej je $i(1 + j) \equiv 0 \pmod 3$ in $j^2 \equiv 1 \pmod 3$. Iz tega sledi, da je $j \in \{1, -1\}$ in da je $i = 0$ ali $j = -1$ ali pa velja oboje.

Dobimo dve možnosti.

1. $i = 0$ in $j \in \{1, -1\}$
Če je $j = 1$, $c$ komutira tudi z $b$, kar pa bi pomenilo, da je grupa $G$ abelska. Torej velja $j = -1$ in tako $cac = a$ in $cbc = b^{-1}$. Potem je $cabc = acbc = ab^{-1}$.

2. $i \neq 0$ in $j = -1$.
Brez škode za splošnost lahko tedaj privzamemo $i = 1$, sicer zamenjamo vlogi $a$ in $a^{-1}$. Torej velja $cac = a$ in $cbc = ab^{-1}$. Potem je $cabc = acbc = aab^{-1} = a^{-1}b^{-1} = (ab)^{-1}$. Brez škode za splošnost lahko torej privzamemo, da je $cbc = b^{-1}$.

V obeh primerih tako ugotovimo, da gre za grupo $G = \langle a, b, c \rangle$, kjer je $|a| = |b| = 3$, $|c| = 2$, $ab = ba$, $ca = ac$ in $cbc = b^{-1}$. S tem je struktura grupe $G$ natanko določena. Sestoji iz elementov

$$G = \{e, a, a^2, b, b^2, ab, a^2b, ab^2, a^2b^2, c, ac, a^2c, bc, b^2c, abc, a^2bc, ab^2c, a^2b^2c\},$$

njeno grupno tabelo najdemo v prilogi pod tabelo 2. Da takšna grupa res obstaja, se brž prepričamo.

Oglejmo si grupo $\mathbb{Z}_3 \times S_3$ in naj bo $a = (1, id)$, $b = (0, (123))$ in $c = (0, (12))$. Tedaj je $|a| = |b| = 3$, $|c| = 2$, $ab = ba$, $ac = ca$ in $cbc = b^{-1}$. Tabela 2 je torej ravno grupna tabela grupe $\mathbb{Z}_3 \times S_3$.

Do izomorfizma natančno torej obstaja 5 grup reda 18 do izomorfizma natančno: $\mathbb{Z}_{18}$, $\mathbb{Z}_6 \times \mathbb{Z}_3$, $D_{2\cdot 9}$, $G_{18}$ in $\mathbb{Z}_3 \times S_3$.

zaporedje redov za $\mathbb{Z}_{18}$: 1, 1, 2, 0, 0, 2, 0, 0, 6, 0, 0, 0, 0, 0, 0, 0, 0, 6

zaporedje redov za $\mathbb{Z}_6 \times \mathbb{Z}_3$: 1, 1, 8, 0, 0, 8

zaporedje redov za $D_{2\cdot 9}$: 1, 9, 2, 0, 0, 0, 0, 0, 6

zaporedje redov za $G_{18}$: 1, 9, 8

zaporedje redov za $\mathbb{Z}_3 \times S_3$: 1, 3, 8, 0, 0, 6

## 3.19 Grupe reda 19

Naj bo $G$ grupa reda 19. V tem primeru gre za grupo praštevilskega reda, torej po trditvi 2.6 velja $G \cong \mathbb{Z}_{19}$.

zaporedje redov za $\mathbb{Z}_{19}$: 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 18

## 3.20 Grupe reda 20

Naj bo $G$ grupa reda $20 = 5 \cdot 2^2$. Po posledici 2.5 so možni redi elementov 1, 2, 4, 5, 10 in 20.

Določimo število 2-Sylowk in 5-Sylowk grupe $G$.

2-Sylowke:

Po 1. izreku Sylowa obstaja vsaj ena. Po 3. izreku Sylowa velja:

$n_2 \equiv 1 \,(mod\, 2) \quad \wedge \quad n_2 \mid 5$

$\Rightarrow n_2 \in \{1, 3, 5, 7, \ldots\} \wedge n_2 \in \{1, 5\}$

$\Rightarrow n_2 \in \{1, 5\}.$

5-Sylowke:

Po 1. izreku Sylowa obstaja vsaj ena. Po 3. izreku Sylowa velja:

$n_5 \equiv 1 \,(mod\, 5) \quad \wedge \quad n_5 \mid 4$

$\Rightarrow n_5 \in \{1, 6, 11, \ldots\} \wedge n_5 \in \{1, 2, 4\}$

$\Rightarrow n_5 = 1.$

Naj bo $Q$ edina 5-Sylowka, ki je potemtakem edinka grupe $G$, in naj bo $P$ poljubna 2-Sylowka.
Ker je $|Q| = 5$, je $Q \cong \mathbb{Z}_5$.
Velja tudi $|P| = 4$. Ker sta edini grupi reda 4 do izomorfizma natančno $\mathbb{Z}_4$ in $\mathbb{Z}_2 \times \mathbb{Z}_2$, je grupa $P$ izomorfna eni izmed njiju.

Poglejmo, kaj dobimo pri različnih kombinacijah.

1. $n_2 = 1$.

Po Lagrangevem izreku 2.4 je $Q \cap P = \{e\}$ in tako velja po lemi 2.8 $|QP| = \frac{5 \cdot 4}{1} = 20$. Iz tega sledi, da je $QP = G$. Ker sta v tem primeru $P$ in $Q$ edinki grupe $G$, velja po trditvi 2.18 $G \cong Q \times P$. Dobimo dve možnosti, saj je $P \cong \mathbb{Z}_4$ ali $P \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

1.1.) Naj bo $P \cong \mathbb{Z}_4$. Torej je $G \cong \mathbb{Z}_5 \times \mathbb{Z}_4 \cong \mathbb{Z}_{20}$, po trditvi 2.16.

1.2.) Naj bo $P \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Torej je $G \cong \mathbb{Z}_5 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \cong \mathbb{Z}_{10} \times \mathbb{Z}_2 \ncong \mathbb{Z}_{20}$, po trditvi 2.16.

2. $n_2 = 5$.

Naj bo $a$ poljuben element reda 5 v grupi $G$. Tedaj je $Q = \langle a \rangle \cong \mathbb{Z}_5$. Ločimo dva primera glede na to ali so 2-Sylowke ciklične ali ne.

2.1.) 2-Sylowke so izomorfne ciklični grupi $\mathbb{Z}_4$.

Naj bo $b \in G$ poljuben element reda 4. Ker je $\langle a \rangle \triangleleft G$, je $b^{-1}ab \in \langle a \rangle$, to je $b^{-1}ab = a^i$ za nek $1 \leq i \leq 4$.

Najprej opazimo, da v primeru, ko je $b^{-1}ab = a^3$, velja $b^{-1}a^2b = a$ in od tod $(b^{-1})^{-1}ab^{-1} = a^2$. Ker tako $b$ kot $b^{-1}$ generirata grupo $\langle b \rangle$, lahko torej privzamemo, da je $i \in \{1, 2, 4\}$.

2.1.1) $i = 1$.
V tem primeru $a$ in $b$ komutirata, kar je nemogoče, saj je potem grupa $G$ abelska, to pa je v nasprotju z $n_2 = 5$.

2.1.2) $i = 2$
V tem primeru gre za grupo $G = \langle a, b \rangle$, kjer je $|a| = 5$, $|b| = 4$ in velja $b^{-1}ab = a^2$. S tem je struktura grupe $G$ natanko določena. Njeno grupno tabelo najdemo v prilogi pod tabelo 3. Pokažimo, da taka grupa zares obstaja.

Oglejmo si podgrupo $F_{20} = \langle a, b \rangle$ grupe $S_5$, kjer je $a = (12345)$ in $b = (2354)$. Velja $|a| = 5$, $|b| = 4$ in $b^{-1}ab = (13524) = a^2$. $F_{20}$ je torej grupa reda 20 z grupno tabelo 3, kar dokazuje, da grupa s to grupno tabelo zares obstaja. Gre za tako imenovano Frobeniusovo grupo reda 20.

2.1.3) $i = 4 = -1$
V tem primeru gre za grupo $G = \langle a, b \rangle$, kjer je $|a| = 5$, $|b| = 4$ in velja $b^{-1}ab = a^{-1}$. S tem je struktura grupe $G$ natanko določena. Njeno grupno tabelo najdemo v prilogi pod tabelo 4. Pokažimo, da obstaja tudi takšna grupa.

Oglejmo si sedaj podgrupo $G_{20} = \langle a, b \rangle$ grupe $S_9$, kjer je $a = (12345)$ in $b = (25)(34)(6789)$. Velja $|a| = 5$, $|b| = 4$ in $b^{-1}ab = (15432) = a^{-1}$, torej je

$G_{20}$ grupa reda 20, katere grupna tabela je tabela 4. To dokazuje, da taka grupa reda 20 zares obstaja.

2.2.) 2-Sylowke niso ciklične.

Naj bo $P = \{e, b, c, bc\}$ poljubna 2-Sylowka. To pomeni, da sta $b$ in $c$ različna elementa reda 2, ki komutirata. Ker je $\langle a \rangle \triangleleft G$, velja $bab, cac \in \langle a \rangle$.

$$
\begin{aligned}
& b^{-1}ab = a^i \\
\Rightarrow\ & b^{-1}b^{-1}abb = b^{-1}a^ib \\
\Rightarrow\ & b^{-2}ab^2 = (b^{-1}ab)^i \\
\Rightarrow\ & eae = (a^i)^i \\
\Rightarrow\ & a = a^{i^2} \\
\Rightarrow\ & i^2 \equiv 1 \pmod 5 \\
\Rightarrow\ & i \in \{1, 4\} = \{1, -1\}
\end{aligned}
$$

Torej je $bab \in \{a, a^{-1}\}$. Na podoben način ugotovimo tudi, da je $cac \in \{a, a^{-1}\}$ in $bcabc \in \{a, a^{-1}\}$.
Če je $bab = a$ in $cac = a$, pridemo do protislovja, saj je potem grupa $G$ abelska.

Torej lahko brez škode za splošnost privzamemo $bab = a^{-1}$.
Če velja še $cac = a^{-1}$, je $bcabc = bcacb = ba^{-1}b = a$. Če pa je $cac = a$, je $bcabc = bcacb = bab = a^{-1}$. Torej natanko eden od elementov $b$, $c$, $bc$ komutira z $a$. Brez škode za splošnost smemo privzeti, da velja $ca = ac$. Element $ac \in G$ ima po trditvi 2.7 tedaj red 10.

Ker je $|b| = 2$, edini element reda 2 v $\langle a, c \rangle$ pa je $c$, sledi $b \notin \langle ac \rangle$.

Torej je grupa $G$ generirana z dvema elementoma in sicer $G = \langle ac, b \rangle$, pri čemer velja $|ac| = 10$ in $|b| = 2$. Poglejmo si še, čemu je enak konjugirani element $b^{-1}acb$.

Velja $b^{-1}(ac)b = bacb = babc = a^{-1}c = (ac)^{-1}$. Torej v grupi $G$ velja tudi, da je $b^{-1}acb = (ac)^{-1}$, od koder po trditvi 2.13 sledi $G \cong D_{2 \cdot 10}$.

Do izomorfizma natančno torej obstaja 5 grup reda 20: $\mathbb{Z}_{20}$, $\mathbb{Z}_{10} \times \mathbb{Z}_2$, $G_{20}$, $F_{20}$ in $D_{2\cdot 10}$.

zaporedje redov za $\mathbb{Z}_{20}$: 1, 1, 0, 2, 4, 0, 0, 0, 0, 4, 0, 0, 0, 0, 0, 0, 0, 0, 0, 8

zaporedje redov za $\mathbb{Z}_{10} \times \mathbb{Z}_2$: 1, 3, 0, 0, 4, 0, 0, 0, 0, 12

zaporedje redov za $G_{20}$: 1, 1, 0, 10, 4, 0, 0, 0, 0, 4

zaporedje redov za $F_{20}$: 1, 5, 0, 10, 4

zaporedje redov za $D_{2\cdot 10}$: 1, 11, 0, 0, 4, 0, 0, 0, 0, 4

## 3.21 Grupe reda 21

Naj bo $G$ grupa reda $21 = 7 \cdot 3$. Po posledici 2.5 so možni redi elementov 1, 3, 7 in 21.

Določimo število 3-Sylowk in 7-Sylowk grupe $G$.

3-Sylowke:

Po 1. izreku Sylowa obstaja vsaj ena. Po 3. izreku Sylowa velja:

$n_3 \equiv 1 \,(mod\, 3) \quad \wedge \quad n_3 \mid 7$

$\Rightarrow n_3 \in \{1, 4, 7, \ldots\} \wedge n_3 \in \{1, 7\}$

$\Rightarrow n_3 \in \{1, 7\}$.

7-Sylowke:

Po 1. izreku Sylowa obstaja vsaj ena. Po 3. izreku Sylowa velja:

$n_7 \equiv 1 \,(mod\, 7) \quad \wedge \quad n_7 \mid 3$

$\Rightarrow n_7 \in \{1, 8, 15, \ldots\} \wedge n_7 \in \{1, 3\}$

$\Rightarrow n_7 = 1$.

Naj bo $Q$ edina 7-Sylowka in $P$ poljubna 3-Sylowka.
Ker je $|Q| = 7$, je $Q \cong \mathbb{Z}_7$, podobno pa je $P \cong \mathbb{Z}_3$.

Edina 7-Sylowka je edinka v grupi $G$. Naj bo $a$ reda 7. Tedaj je seveda $Q = \langle a \rangle$. Po Cauchyjevem izreku 2.23 obstaja $b \in G$ reda 3. Ker je $\langle a \rangle \triangleleft G$, sledi $b^{-1}ab \in \langle a \rangle$.

$$\begin{aligned}
&b^{-1}ab = a^i \\
&\Rightarrow b^{-1}b^{-1}abb = b^{-1}a^ib \\
&\Rightarrow b^{-2}ab^2 = (b^{-1}ab)^i \\
&\Rightarrow bb^{-2}ab^2b = b^{-1}(a^i)^ib \\
&\Rightarrow b^{-3}ab^3 = (a^{i^2})^i \\
&\Rightarrow eae = a^{i^3} \\
&\Rightarrow i^3 \equiv 1 (mod\, 7) \\
&\Rightarrow i \in \{1, 2, 4\}.
\end{aligned}$$

Opazimo, da v primeru, ko je $b^{-1}ab = a^4$, velja $b^{-1}a^2b = a$ in od tod $(b^{-1})^{-1}ab^{-1} = a^2$. Brez škode za splošnost torej lahko privzamemo $i \in \{1, 2\}$.

1. $b^{-1}ab = a$

Velja torej $ba = ab$. To je, elementa $a$ in $b$ komutirata. Po trditvi 2.7 je element $ab$ reda 21 in tako je grupa $G$ ciklična. Sledi $G \cong \mathbb{Z}_{21}$.

2. $b^{-1}ab = a^2$
V tem primeru gre za grupo $G = \langle a, b \rangle$, kjer je $|a| = 7$, $|b| = 3$ in velja $b^{-1}ab = a^2$. S tem je struktura grupe $G$ natanko določena. Sestoji iz elementov

$$G = \{e, a, a^2, a^3, a^4, a^5, a^6, b, b^2, ab, a^2b, a^3b, a^4b, a^5b, a^6b, ab^2, a^2b^2, a^3b^2, a^4b^2, a^5b^2, a^6b^2\},$$

njeno grupno tabelo pa najdemo v prilogi pod tabelo 5. Pokažimo, da taka grupa zares obstaja.

Oglejmo si podgrupo $G_{21} = \langle a, b \rangle$ grupe $S_7$, kjer je $a = (1234567)$ in $b = (235)(476)$. Velja $|a| = 7$, $|b| = 3$ in $b^{-1}ab = (1357246) = a^2$. Torej je $G_{21}$ grupa reda 21, katere grupna tabela je tabela 5. To dokazuje, da taka grupa reda 21 zares obstaja.

Do izomorfizma natančno torej obstajata dve grupi reda 21: $\mathbb{Z}_{21}$ in $G_{21}$.

zaporedje redov za $\mathbb{Z}_{21}$: 1, 0, 2, 0, 0, 0, 6, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 12

zaporedje redov za $G_{21}$: 1, 0, 14, 0, 0, 0, 6

## 3.22 Grupe reda 22

Naj bo $G$ grupa reda $22 = 2 \cdot 11$. Grupa je reda $2p$, kjer je $p \geq 3$ praštevilo. Po trditvi 2.31 torej obstajata natanko dve grupi reda 22, do izomorfizma natančno, in sicer ciklična grupa $\mathbb{Z}_{22}$ in diederska grupa $D_{2\cdot 11}$.

zaporedje redov za $\mathbb{Z}_{22}$: 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 10, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 10

zaporedje redov za $D_{2\cdot 11}$: 1, 11, 0, 0, 0, 0, 0, 0, 0, 0, 10

## 3.23 Grupe reda 23

Naj bo $G$ grupa reda 23. V tem primeru gre za grupe praštevilskega reda, torej po trditvi 2.6 velja $G \cong \mathbb{Z}_{23}$.

zaporedje redov za $\mathbb{Z}_{23}$: 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 22

# Poglavje 4

# Zaključek

V diplomskem delu smo se posvetili klasifikaciji končnih grup do reda 23, seveda do izomorfizma natančno. Izkazalo se je, da so rezultati, ki smo jih spoznali tekom študija pri predmetu Algebra 2, dovolj močno orodje za klasifikacijo grup majhnih redov. Določili smo vse paroma neizomorfne grupe določenega reda in jih poimenovali. Osvojeno znanje ni zadostno le za klasifikacijo vseh grup reda 16, zato smo klasifikacijo grup tega reda izpustili. Za grupe reda 16 smo zapisali le tiste, ki jih z rezultati iz predmeta Algebra 2 znamo določiti. Vsem grupam smo določili tudi zaporedje redov. Ugotovili smo, da imata lahko dve neizomorfni grupi enako zaporedje redov, kar priča o tem, da enako zaporedje redov ni zadosten kriterij za izomorfnost dveh grup. Med klasifikacijo so se pojavile tudi nekatere nestandardne grupe. Te grupe smo predstavili tudi kot grupe ustreznih permutacij in zanje zapisali ustrezno tabelo produktov.

Naše ugotovitve in rezultati so zbrani v naslednji tabeli. V tabeli je za vsak red grupe najprej podano število vseh grup do izomorfizma natančno, nato so grupe še poimenovane, seveda ločeno na abelske in neabelske.

| red | št. | abelske grupe | neabelske grupe |
|---|---|---|---|
| 2 | 1 | $\mathbb{Z}_2$ | |
| 3 | 1 | $\mathbb{Z}_3$ | |
| 4 | 2 | $\mathbb{Z}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$ | |
| 5 | 1 | $\mathbb{Z}_5$ | |
| 6 | 2 | $\mathbb{Z}_6$ | $D_{2\cdot 3}$ |
| 7 | 1 | $\mathbb{Z}_7$ | |
| 8 | 5 | $\mathbb{Z}_8$, $\mathbb{Z}_4 \times \mathbb{Z}_2$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ | $D_{2\cdot 4}$, $Q_8$ |
| 9 | 2 | $\mathbb{Z}_9$, $\mathbb{Z}_3 \times \mathbb{Z}_3$ | |
| 10 | 2 | $\mathbb{Z}_{10}$ | $D_{2\cdot 5}$ |
| 11 | 1 | $\mathbb{Z}_{11}$ | |
| 12 | 5 | $\mathbb{Z}_{12}$, $\mathbb{Z}_6 \times \mathbb{Z}_2$ | $T$, $D_{2\cdot 6}$, $A_4$ |
| 13 | 1 | $\mathbb{Z}_{13}$ | |
| 14 | 2 | $\mathbb{Z}_{14}$ | $D_{2\cdot 7}$ |
| 15 | 1 | $\mathbb{Z}_{15}$ | |
| 17 | 1 | $\mathbb{Z}_{17}$ | |
| 18 | 5 | $\mathbb{Z}_{18}$, $\mathbb{Z}_6 \times \mathbb{Z}_3$ | $D_{2\cdot 9}$, $G_{18}$, $S_3 \times \mathbb{Z}_3$ |
| 19 | 1 | $\mathbb{Z}_{19}$ | |
| 20 | 5 | $\mathbb{Z}_{20}$, $\mathbb{Z}_{10} \times \mathbb{Z}_2$ | $G_{20}$, $F_{20}$, $D_{2\cdot 10}$ |
| 21 | 2 | $\mathbb{Z}_{21}$ | $G_{21}$ |
| 22 | 2 | $\mathbb{Z}_{22}$ | $D_{2\cdot 11}$ |
| 23 | 1 | $\mathbb{Z}_{23}$ | |

# Literatura


[1] Clark, A. *Elements of abstract algebra*. New York: Dover Publications, cop., 1984. ISBN 0-486-64725-0

[2] Dummit, D. S., Foote, R. M. *Abstract algebra*. 3th ed. Hoboken: John Wiley and sons, 2004. ISBN 0-471-45234-3

[3] Fraleigh, J. B. *A first course in abstract algebra*. 6th ed. Massachusetts: Addison - Wesley, 1999. ISBN 0-201-33596-4

[4] Malnič, A., Marušič, D. *Uvod v teorijo grup*: študijsko gradivo. Ljubljana: Pedagoška fakulteta, 1997

[5] Marušič, D. *Zapiski iz predavanj*. 2006/2007

[6] Vidav, I. *Algebra*. 3. natis. Ljubljana: Društvo matematikov, fizikov in astronomov SRS; Zveza organizacij za tehnično kulturo Slovenije, 1987.

[7] Zgrablić, B. *Grupe: svitek nalog iz teorije in rabe*. Ljubljana: Pedagoška fakulteta, 1999

| | $e$ | $a$ | $a^2$ | $c$ | $c^2$ | $ac$ | $a^2c$ | $ac^2$ | $a^2c^2$ | $b$ | $ab$ | $a^2b$ | $cb$ | $c^2b$ | $acb$ | $a^2cb$ | $ac^2b$ | $a^2c^2b$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $e$ | $e$ | $a$ | $a^2$ | $c$ | $c^2$ | $ac$ | $a^2c$ | $ac^2$ | $a^2c^2$ | $b$ | $ab$ | $a^2b$ | $cb$ | $c^2b$ | $acb$ | $a^2cb$ | $ac^2b$ | $a^2c^2b$ |
| $a$ | $a$ | $a^2$ | $e$ | $ac$ | $ac^2$ | $a^2c$ | $c$ | $a^2c^2$ | $c^2$ | $ab$ | $a^2b$ | $b$ | $acb$ | $ac^2b$ | $a^2cb$ | $cb$ | $a^2c^2b$ | $c^2b$ |
| $a^2$ | $a^2$ | $e$ | $a$ | $a^2c$ | $a^2c^2$ | $c$ | $ac$ | $c^2$ | $ac^2$ | $a^2b$ | $b$ | $ab$ | $a^2cb$ | $a^2c^2b$ | $cb$ | $acb$ | $c^2b$ | $ac^2b$ |
| $c$ | $c$ | $ac$ | $a^2c$ | $c^2$ | $e$ | $ac^2$ | $a^2c^2$ | $a$ | $a^2$ | $cb$ | $acb$ | $a^2cb$ | $c^2b$ | $b$ | $ac^2b$ | $a^2c^2b$ | $ab$ | $a^2b$ |
| $c^2$ | $c^2$ | $ac^2$ | $a^2c^2$ | $e$ | $c$ | $a$ | $a^2$ | $ac$ | $a^2c$ | $c^2b$ | $ac^2b$ | $a^2c^2b$ | $b$ | $cb$ | $ab$ | $a^2b$ | $acb$ | $a^2cb$ |
| $ac$ | $ac$ | $a^2c$ | $c$ | $ac^2$ | $a$ | $a^2c^2$ | $c^2$ | $a^2$ | $e$ | $acb$ | $a^2cb$ | $cb$ | $ac^2b$ | $ab$ | $a^2c^2b$ | $c^2b$ | $a^2b$ | $b$ |
| $a^2c$ | $a^2c$ | $c$ | $ac$ | $a^2c^2$ | $a^2$ | $c^2$ | $ac^2$ | $e$ | $a$ | $a^2cb$ | $cb$ | $acb$ | $a^2c^2b$ | $a^2b$ | $c^2b$ | $ac^2b$ | $b$ | $ab$ |
| $ac^2$ | $ac^2$ | $a^2c^2$ | $c^2$ | $a$ | $ac$ | $a^2$ | $e$ | $a^2c$ | $c$ | $ac^2b$ | $a^2c^2b$ | $c^2b$ | $ab$ | $acb$ | $a^2b$ | $b$ | $a^2cb$ | $cb$ |
| $a^2c^2$ | $a^2c^2$ | $c^2$ | $ac^2$ | $a^2$ | $a^2c$ | $e$ | $a$ | $c$ | $ac$ | $a^2c^2b$ | $c^2b$ | $ac^2b$ | $ab$ | $a^2cb$ | $b$ | $ab$ | $cb$ | $acb$ |
| $b$ | $b$ | $a^2b$ | $ab$ | $c^2b$ | $cb$ | $a^2c^2b$ | $ac^2b$ | $a^2cb$ | $acb$ | $e$ | $a^2$ | $a$ | $c^2$ | $c$ | $a^2c^2$ | $ac^2$ | $a^2c$ | $ac$ |
| $ab$ | $ab$ | $b$ | $a^2b$ | $ac^2b$ | $acb$ | $c^2b$ | $a^2c^2b$ | $cb$ | $a^2cb$ | $a$ | $e$ | $a^2$ | $ac^2$ | $ac$ | $c^2$ | $a^2c^2$ | $c$ | $a^2c$ |
| $a^2b$ | $a^2b$ | $ab$ | $b$ | $a^2c^2b$ | $a^2cb$ | $ac^2b$ | $c^2b$ | $acb$ | $cb$ | $a^2$ | $a$ | $e$ | $a^2c^2$ | $a^2c$ | $ac^2$ | $c^2$ | $ac$ | $c$ |
| $cb$ | $cb$ | $a^2cb$ | $acb$ | $b$ | $c^2b$ | $a^2b$ | $ab$ | $a^2c^2b$ | $ac^2b$ | $c$ | $a^2c$ | $ac$ | $e$ | $c^2$ | $a^2$ | $a$ | $a^2c^2$ | $ac^2$ |
| $c^2b$ | $c^2b$ | $a^2c^2b$ | $ac^2b$ | $cb$ | $b$ | $a^2cb$ | $acb$ | $a^2b$ | $ab$ | $c^2$ | $a^2c^2$ | $ac^2$ | $c$ | $e$ | $a^2c$ | $ac$ | $a^2$ | $a$ |
| $acb$ | $acb$ | $cb$ | $a^2cb$ | $ab$ | $ac^2b$ | $b$ | $a^2b$ | $c^2b$ | $a^2c^2b$ | $ac$ | $c$ | $a^2c$ | $a$ | $ac^2$ | $e$ | $a^2$ | $c^2$ | $a^2c^2$ |
| $a^2cb$ | $a^2cb$ | $acb$ | $cb$ | $a^2b$ | $a^2c^2b$ | $ab$ | $b$ | $ac^2b$ | $c^2b$ | $a^2c$ | $ac$ | $c$ | $a^2$ | $a^2c^2$ | $a$ | $e$ | $ac^2$ | $c^2$ |
| $ac^2b$ | $ac^2b$ | $c^2b$ | $a^2c^2b$ | $acb$ | $ab$ | $cb$ | $a^2cb$ | $b$ | $a^2b$ | $ac^2$ | $c^2$ | $a^2c^2$ | $ac$ | $a$ | $c$ | $a^2c$ | $e$ | $a^2$ |
| $a^2c^2b$ | $a^2c^2b$ | $ac^2b$ | $c^2b$ | $a^2cb$ | $a^2b$ | $acb$ | $cb$ | $ab$ | $b$ | $a^2c^2$ | $ac^2$ | $c^2$ | $a^2c$ | $a^2$ | $ac$ | $c$ | $a$ | $e$ |

Tabela 1: Grupna tabela grupe $G_{18}$.

| | $e$ | $a$ | $a^2$ | $b$ | $b^2$ | $ab$ | $a^2b$ | $ab^2$ | $a^2b^2$ | $c$ | $ac$ | $a^2c$ | $bc$ | $b^2c$ | $abc$ | $a^2bc$ | $ab^2c$ | $a^2b^2c$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $e$ | $e$ | $a$ | $a^2$ | $b$ | $b^2$ | $ab$ | $a^2b$ | $ab^2$ | $a^2b^2$ | $c$ | $ac$ | $a^2c$ | $bc$ | $b^2c$ | $abc$ | $a^2bc$ | $ab^2c$ | $a^2b^2c$ |
| $a$ | $a$ | $a^2$ | $e$ | $ab$ | $ab^2$ | $a^2b$ | $b$ | $a^2b^2$ | $b^2$ | $ac$ | $a^2c$ | $c$ | $abc$ | $ab^2c$ | $a^2bc$ | $bc$ | $a^2b^2c$ | $b^2c$ |
| $a^2$ | $a^2$ | $e$ | $a$ | $a^2b$ | $a^2b^2$ | $b$ | $ab$ | $b^2$ | $ab^2$ | $a^2c$ | $c$ | $ac$ | $a^2bc$ | $a^2b^2c$ | $bc$ | $abc$ | $b^2c$ | $ab^2c$ |
| $b$ | $b$ | $ab$ | $a^2b$ | $b^2$ | $e$ | $ab^2$ | $a^2b^2$ | $a$ | $a^2$ | $bc$ | $abc$ | $a^2bc$ | $b^2c$ | $c$ | $ab^2c$ | $a^2b^2c$ | $ac$ | $a^2c$ |
| $b^2$ | $b^2$ | $ab^2$ | $a^2b^2$ | $e$ | $b$ | $a$ | $a^2$ | $ab$ | $a^2b$ | $b^2c$ | $ab^2c$ | $a^2b^2c$ | $c$ | $bc$ | $ac$ | $a^2c$ | $abc$ | $a^2bc$ |
| $ab$ | $ab$ | $a^2b$ | $b$ | $ab^2$ | $a$ | $a^2b^2$ | $b^2$ | $a^2$ | $e$ | $abc$ | $a^2bc$ | $bc$ | $ab^2c$ | $ac$ | $a^2b^2c$ | $b^2c$ | $a^2c$ | $c$ |
| $a^2b$ | $a^2b$ | $b$ | $ab$ | $a^2b^2$ | $a^2$ | $b^2$ | $ab^2$ | $e$ | $a$ | $a^2bc$ | $bc$ | $abc$ | $a^2b^2c$ | $a^2c$ | $b^2c$ | $ab^2c$ | $c$ | $ac$ |
| $ab^2$ | $ab^2$ | $a^2b^2$ | $b^2$ | $a$ | $ab$ | $a^2$ | $e$ | $a^2b$ | $b$ | $ab^2c$ | $a^2b^2c$ | $b^2c$ | $ac$ | $abc$ | $a^2c$ | $c$ | $a^2bc$ | $bc$ |
| $a^2b^2$ | $a^2b^2$ | $b^2$ | $ab^2$ | $a^2$ | $a^2b$ | $e$ | $a$ | $b$ | $ab$ | $a^2b^2c$ | $b^2c$ | $ab^2c$ | $a^2c$ | $a^2bc$ | $c$ | $ac$ | $bc$ | $a^2bc$ |
| $c$ | $c$ | $ac$ | $a^2c$ | $b^2c$ | $bc$ | $ab^2c$ | $a^2b^2c$ | $abc$ | $a^2bc$ | $e$ | $a$ | $a^2$ | $b^2$ | $b$ | $ab^2$ | $a^2b^2$ | $ab$ | $a^2b$ |
| $ac$ | $ac$ | $a^2c$ | $c$ | $ab^2c$ | $abc$ | $a^2b^2c$ | $b^2c$ | $a^2bc$ | $bc$ | $a$ | $a^2$ | $e$ | $ab^2$ | $ab$ | $a^2b^2$ | $b^2$ | $a^2b$ | $b$ |
| $a^2c$ | $a^2c$ | $c$ | $ac$ | $a^2b^2c$ | $a^2bc$ | $b^2c$ | $ab^2c$ | $bc$ | $abc$ | $a^2$ | $e$ | $a$ | $a^2b^2$ | $a^2b$ | $b^2$ | $ab^2$ | $b$ | $ab$ |
| $bc$ | $bc$ | $abc$ | $a^2bc$ | $c$ | $b^2c$ | $ac$ | $a^2c$ | $ab^2c$ | $a^2b^2c$ | $b$ | $ab$ | $a^2b$ | $e$ | $b^2$ | $a$ | $a^2$ | $ab^2$ | $a^2b^2$ |
| $b^2c$ | $b^2c$ | $ab^2c$ | $a^2b^2c$ | $bc$ | $c$ | $abc$ | $a^2bc$ | $ac$ | $a^2c$ | $b^2$ | $ab^2$ | $a^2b^2$ | $b$ | $e$ | $ab$ | $a^2b$ | $a$ | $a^2$ |
| $abc$ | $abc$ | $a^2bc$ | $bc$ | $ac$ | $ab^2c$ | $a^2c$ | $c$ | $a^2b^2c$ | $b^2c$ | $ab$ | $a^2b$ | $b$ | $a$ | $ab^2$ | $a^2$ | $e$ | $a^2b^2$ | $b^2$ |
| $a^2bc$ | $a^2bc$ | $bc$ | $abc$ | $a^2c$ | $a^2b^2c$ | $c$ | $ac$ | $b^2c$ | $ab^2c$ | $a^2b$ | $b$ | $ab$ | $a^2$ | $a^2b^2$ | $e$ | $a$ | $b^2$ | $ab^2$ |
| $ab^2c$ | $ab^2c$ | $a^2b^2c$ | $b^2c$ | $abc$ | $ac$ | $a^2bc$ | $bc$ | $a^2c$ | $c$ | $ab^2$ | $a^2b^2$ | $b^2$ | $ab$ | $a$ | $a^2b$ | $b$ | $a^2$ | $e$ |
| $a^2b^2c$ | $a^2b^2c$ | $b^2c$ | $ab^2c$ | $a^2bc$ | $a^2c$ | $bc$ | $abc$ | $c$ | $ac$ | $a^2b^2$ | $b^2$ | $ab^2$ | $a^2b$ | $a^2$ | $b$ | $ab$ | $e$ | $a$ |

Tabela 2: Grupna tabela grupe $\mathbb{Z}_3 \times S_3$.

| | $e$ | $a$ | $a^2$ | $a^3$ | $a^4$ | $b$ | $b^2$ | $b^3$ | $ab$ | $a^2b$ | $a^3b$ | $a^4b$ | $ab^2$ | $a^2b^2$ | $a^3b^2$ | $a^4b^2$ | $ab^3$ | $a^2b^3$ | $a^3b^3$ | $a^4b^3$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $e$ | $e$ | $a$ | $a^2$ | $a^3$ | $a^4$ | $b$ | $b^2$ | $b^3$ | $ab$ | $a^2b$ | $a^3b$ | $a^4b$ | $ab^2$ | $a^2b^2$ | $a^3b^2$ | $a^4b^2$ | $ab^3$ | $a^2b^3$ | $a^3b^3$ | $a^4b^3$ |
| $a$ | $a$ | $a^2$ | $a^3$ | $a^4$ | $e$ | $ab$ | $ab^2$ | $ab^3$ | $a^2b$ | $a^3b$ | $a^4b$ | $b$ | $a^2b^2$ | $a^3b^2$ | $a^4b^2$ | $b^2$ | $a^2b^3$ | $a^3b^3$ | $a^4b^3$ | $b^3$ |
| $a^2$ | $a^2$ | $a^3$ | $a^4$ | $e$ | $a$ | $a^2b$ | $a^2b^2$ | $a^2b^3$ | $a^3b$ | $a^4b$ | $b$ | $ab$ | $a^3b^2$ | $a^4b^2$ | $b^2$ | $ab^2$ | $a^3b^3$ | $a^4b^3$ | $b^3$ | $ab^3$ |
| $a^3$ | $a^3$ | $a^4$ | $e$ | $a$ | $a^2$ | $a^3b$ | $a^3b^2$ | $a^3b^3$ | $a^4b$ | $b$ | $ab$ | $a^2b$ | $a^4b^2$ | $b^2$ | $ab^2$ | $a^2b^2$ | $a^4b^3$ | $b^3$ | $ab^3$ | $a^2b^3$ |
| $a^4$ | $a^4$ | $e$ | $a$ | $a^2$ | $a^3$ | $a^4b$ | $a^4b^2$ | $a^4b^3$ | $b$ | $ab$ | $a^2b$ | $a^3b$ | $b^2$ | $ab^2$ | $a^2b^2$ | $a^3b^2$ | $b^3$ | $ab^3$ | $a^2b^3$ | $a^3b^3$ |
| $b$ | $b$ | $a^3b$ | $ab$ | $a^4b$ | $a^2b$ | $b^2$ | $b^3$ | $e$ | $a^3b^2$ | $ab^2$ | $a^4b^2$ | $a^2b^2$ | $a^3b^3$ | $ab^3$ | $a^4b^3$ | $a^2b^3$ | $a^3$ | $a$ | $a^4$ | $a^2$ |
| $b^2$ | $b^2$ | $a^4b^2$ | $a^3b^2$ | $a^2b^2$ | $ab^2$ | $b^3$ | $e$ | $b$ | $a^4b^3$ | $a^3b^3$ | $a^2b^3$ | $ab^3$ | $a^4$ | $a^3$ | $a^2$ | $a$ | $a^4b$ | $a^3b$ | $a^2b$ | $ab$ |
| $b^3$ | $b^3$ | $a^2b^3$ | $a^4b^3$ | $ab^3$ | $a^3b^3$ | $e$ | $b$ | $b^2$ | $a^2$ | $a^4$ | $a$ | $a^3$ | $a^2b$ | $a^4b$ | $ab$ | $a^3b$ | $a^2b^2$ | $a^4b^2$ | $ab^2$ | $a^3b^2$ |
| $ab$ | $ab$ | $a^4b$ | $a^2b$ | $b$ | $a^3b$ | $ab^2$ | $ab^3$ | $a$ | $a^4b^2$ | $a^2b^2$ | $b^2$ | $a^3b^2$ | $a^4b^3$ | $a^2b^3$ | $b^3$ | $a^3b^3$ | $a^4$ | $a^2$ | $e$ | $a^3$ |
| $a^2b$ | $a^2b$ | $b$ | $a^3b$ | $ab$ | $a^4b$ | $a^2b^2$ | $a^2b^3$ | $a^2$ | $b^2$ | $a^3b^2$ | $ab^2$ | $a^4b^2$ | $b^3$ | $a^3b^3$ | $ab^3$ | $a^4b^3$ | $e$ | $a^3$ | $a$ | $a^4$ |
| $a^3b$ | $a^3b$ | $ab$ | $a^4b$ | $a^2b$ | $b$ | $a^3b^2$ | $a^3b^3$ | $a^3$ | $ab^2$ | $a^4b^2$ | $a^2b^2$ | $b^2$ | $ab^3$ | $a^4b^3$ | $a^2b^3$ | $b^3$ | $a$ | $a^4$ | $a^2$ | $e$ |
| $a^4b$ | $a^4b$ | $a^2b$ | $b$ | $a^3b$ | $ab$ | $a^4b^2$ | $a^4b^3$ | $a^4$ | $a^2b^2$ | $b^2$ | $a^3b^2$ | $ab^2$ | $a^2b^3$ | $b^3$ | $a^3b^3$ | $ab^3$ | $a^2$ | $e$ | $a^3$ | $a$ |
| $ab^2$ | $ab^2$ | $b^2$ | $a^4b^2$ | $a^3b^2$ | $a^2b^2$ | $ab^3$ | $a$ | $ab$ | $b^3$ | $a^4b^3$ | $a^3b^3$ | $a^2b^3$ | $e$ | $a^4$ | $q^3$ | $a^2$ | $b$ | $a^4b$ | $a^3b$ | $a^2b$ |
| $a^2b^2$ | $a^2b^2$ | $ab^2$ | $b^2$ | $a^4b^2$ | $a^3b^2$ | $a^2b^3$ | $a^2$ | $a^2b$ | $ab^3$ | $b^3$ | $a^4b^3$ | $a^3b^3$ | $a$ | $e$ | $a^4$ | $a^3$ | $ab$ | $b$ | $a^4b$ | $a^3b$ |
| $a^3b^2$ | $a^3b^2$ | $a^2b^2$ | $ab^2$ | $b^2$ | $a^4b^2$ | $a^3b^3$ | $a^3$ | $a^3b$ | $a^2b^3$ | $ab^3$ | $b^3$ | $a^4b^3$ | $a^2$ | $a$ | $e$ | $a^4$ | $a^2b$ | $ab$ | $b$ | $a^4b$ |
| $a^4b^2$ | $a^4b^2$ | $a^3b^2$ | $a^2b^2$ | $ab^2$ | $b^2$ | $a^4b^3$ | $a^4$ | $a^4b$ | $a^3b^3$ | $a^2b^3$ | $ab^3$ | $b^3$ | $a^3$ | $a^2$ | $a$ | $e$ | $a^3b$ | $a^2b$ | $ab$ | $b$ |
| $ab^3$ | $ab^3$ | $a^3b^3$ | $b^3$ | $a^2b^3$ | $a^4b^3$ | $a$ | $ab$ | $ab^2$ | $a^3$ | $e$ | $a^2$ | $a^4$ | $a^3b$ | $b$ | $a^2b$ | $a^4b$ | $a^3b^2$ | $b^2$ | $a^2b^2$ | $a^4b^2$ |
| $a^2b^3$ | $a^2b^3$ | $a^4b^3$ | $ab^3$ | $a^3b^3$ | $b^3$ | $a^2$ | $a^2b$ | $a^2b^2$ | $a^4$ | $a$ | $a^3$ | $e$ | $a^4b$ | $ab$ | $a^3b$ | $b$ | $a^4b^2$ | $ab^2$ | $a^3b^2$ | $b^2$ |
| $a^3b^3$ | $a^3b^3$ | $b^3$ | $a^2b^3$ | $a^4b^3$ | $ab^3$ | $a^3$ | $a^3b$ | $a^3b^2$ | $e$ | $a^2$ | $a^4$ | $a$ | $b$ | $a^2b$ | $a^4b$ | $ab$ | $b^2$ | $a^2b^2$ | $a^4b^2$ | $ab^2$ |
| $a^4b^3$ | $a^4b^3$ | $ab^3$ | $a^3b^3$ | $b^3$ | $a^2b^3$ | $a^4$ | $a^4b$ | $a^4b^2$ | $a$ | $a^3$ | $e$ | $a^2$ | $ab$ | $a^3b$ | $b$ | $a^2b$ | $ab^2$ | $a^3b^2$ | $b^2$ | $a^2b^2$ |

Tabela 3: Grupna tabela grupe $F_{20}$.

| | $e$ | $a$ | $a^2$ | $a^3$ | $a^4$ | $b$ | $b^2$ | $b^3$ | $ab$ | $a^2b$ | $a^3b$ | $a^4b$ | $ab^2$ | $a^2b^2$ | $a^3b^2$ | $a^4b^2$ | $ab^3$ | $a^2b^3$ | $a^3b^3$ | $a^4b^3$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $e$ | $e$ | $a$ | $a^2$ | $a^3$ | $a^4$ | $b$ | $b^2$ | $b^3$ | $ab$ | $a^2b$ | $a^3b$ | $a^4b$ | $ab^2$ | $a^2b^2$ | $a^3b^2$ | $a^4b^2$ | $ab^3$ | $a^2b^3$ | $a^3b^3$ | $a^4b^3$ |
| $a$ | $a$ | $a^2$ | $a^3$ | $a^4$ | $e$ | $ab$ | $ab^2$ | $ab^3$ | $a^2b$ | $a^3b$ | $a^4b$ | $b$ | $a^2b^2$ | $a^3b^2$ | $a^4b^2$ | $b^2$ | $a^2b^3$ | $a^3b^3$ | $a^4b^3$ | $b^3$ |
| $a^2$ | $a^2$ | $a^3$ | $a^4$ | $e$ | $a$ | $a^2b$ | $a^2b^2$ | $a^2b^3$ | $a^3b$ | $a^4b$ | $b$ | $ab$ | $a^3b^2$ | $a^4b^2$ | $b^2$ | $ab^2$ | $a^3b^3$ | $a^4b^3$ | $b^3$ | $ab^3$ |
| $a^3$ | $a^3$ | $a^4$ | $e$ | $a$ | $a^2$ | $a^3b$ | $a^3b^2$ | $a^3b^3$ | $a^4b$ | $b$ | $ab$ | $a^2b$ | $a^4b^2$ | $b^2$ | $ab^2$ | $a^2b^2$ | $a^4b^3$ | $b^3$ | $ab^3$ | $a^2b^3$ |
| $a^4$ | $a^4$ | $e$ | $a$ | $a^2$ | $a^3$ | $a^4b$ | $a^4b^2$ | $a^4b^3$ | $b$ | $ab$ | $a^2b$ | $a^3b$ | $b^2$ | $ab^2$ | $a^2b^2$ | $a^3b^2$ | $b^3$ | $ab^3$ | $a^2b^3$ | $a^3b^3$ |
| $b$ | $b$ | $a^4b$ | $a^3b$ | $a^2b$ | $ab$ | $b^2$ | $b^3$ | $e$ | $a^4b^2$ | $a^3b^2$ | $a^2b^2$ | $ab^2$ | $a^4b^3$ | $a^3b^3$ | $a^2b^3$ | $ab^3$ | $a^4$ | $a^3$ | $a^2$ | $a$ |
| $b^2$ | $b^2$ | $ab^2$ | $a^2b^2$ | $a^3b^2$ | $a^4b^2$ | $b^3$ | $e$ | $b$ | $ab^3$ | $a^2b^3$ | $a^3b^3$ | $a^4b^3$ | $a$ | $a^2$ | $a^3$ | $a^4$ | $ab$ | $a^2b$ | $a^3b$ | $a^4b$ |
| $b^3$ | $b^3$ | $a^4b^3$ | $a^3b^3$ | $a^2b^3$ | $ab^3$ | $e$ | $b$ | $b^2$ | $a^4$ | $a^3$ | $a^2$ | $a$ | $a^4b$ | $a^3b$ | $a^2b$ | $ab$ | $a^4b^2$ | $a^3b^2$ | $a^2b^2$ | $ab^2$ |
| $ab$ | $ab$ | $b$ | $a^4b$ | $a^3b$ | $a^2b$ | $ab^2$ | $ab^3$ | $a$ | $b^2$ | $a^4b^2$ | $a^3b^2$ | $a^2b^2$ | $b^3$ | $a^4b^3$ | $a^3b^3$ | $a^2b^3$ | $e$ | $a^4$ | $a^3$ | $a^2$ |
| $a^2b$ | $a^2b$ | $ab$ | $b$ | $a^4b$ | $a^3b$ | $a^2b^2$ | $a^2b^3$ | $a^2b^4$ | $ab^2$ | $b^2$ | $a^4b^2$ | $a^3b^2$ | $ab^3$ | $b^3$ | $a^4b^3$ | $a^3b^3$ | $a$ | $e$ | $a^4$ | $a^3$ |
| $a^3b$ | $a^3b$ | $a^2b$ | $ab$ | $b$ | $a^4b$ | $a^3b^2$ | $a^3b^3$ | $a^3b^4$ | $a^2b^2$ | $ab^2$ | $b^2$ | $a^4b^2$ | $a^2b^3$ | $ab^3$ | $b^3$ | $a^4b^3$ | $a^2$ | $a$ | $e$ | $a^4$ |
| $a^4b$ | $a^4b$ | $a^3b$ | $a^2b$ | $ab$ | $b$ | $a^4b^2$ | $a^4b^3$ | $a^4b^4$ | $a^3b^2$ | $a^2b^2$ | $ab^2$ | $b^2$ | $a^3b^3$ | $a^2b^3$ | $ab^3$ | $b^3$ | $a^3$ | $a^2$ | $a$ | $e$ |
| $ab^2$ | $ab^2$ | $a^2b^2$ | $a^3b^2$ | $a^4b^2$ | $b^2$ | $ab^3$ | $a$ | $ab$ | $a^2b^3$ | $a^3b^3$ | $a^4b^3$ | $b^3$ | $a^2$ | $a^3$ | $a^4$ | $e$ | $a^2b$ | $a^3b$ | $a^4b$ | $b$ |
| $a^2b^2$ | $a^2b^2$ | $a^3b^2$ | $a^4b^2$ | $b^2$ | $ab^2$ | $a^2b^3$ | $a^2$ | $a^2b$ | $a^3b^3$ | $a^4b^3$ | $b^3$ | $ab^3$ | $a^3$ | $a^4$ | $e$ | $a$ | $a^3b$ | $a^4b$ | $b$ | $ab$ |
| $a^3b^2$ | $a^3b^2$ | $a^4b^2$ | $b^2$ | $ab^2$ | $a^2b^2$ | $a^3b^3$ | $a^3$ | $a^3b$ | $a^4b^3$ | $b^3$ | $ab^3$ | $a^2b^3$ | $a^4$ | $e$ | $a$ | $a^2$ | $a^4b$ | $b$ | $ab$ | $a^2b$ |
| $a^4b^2$ | $a^4b^2$ | $b^2$ | $ab^2$ | $a^2b^2$ | $a^3b^2$ | $a^4b^3$ | $a^4$ | $a^4b$ | $b^3$ | $ab^3$ | $a^2b^3$ | $a^3b^3$ | $e$ | $a$ | $a^2$ | $a^3$ | $b$ | $ab$ | $a^2b$ | $a^3b$ |
| $ab^3$ | $ab^3$ | $b^3$ | $a^4b^3$ | $a^3b^3$ | $a^2b^3$ | $a$ | $ab$ | $ab^2$ | $e$ | $a^4$ | $a^3$ | $a^2$ | $b$ | $a^4b$ | $a^3b$ | $a^2b$ | $b^2$ | $a^4b^2$ | $a^3b^2$ | $a^2b^2$ |
| $a^2b^3$ | $a^2b^3$ | $ab^3$ | $b^3$ | $a^4b^3$ | $a^3b^3$ | $a^2$ | $a^2b$ | $a^2b^2$ | $a$ | $e$ | $a^4$ | $a^3$ | $ab$ | $b$ | $a^4b$ | $a^3b$ | $ab^2$ | $b^2$ | $a^4b^2$ | $a^3b^2$ |
| $a^3b^3$ | $a^3b^3$ | $a^2b^3$ | $ab^3$ | $b^3$ | $a^4b^3$ | $a^3$ | $a^3b$ | $a^3b^2$ | $a^2$ | $a$ | $e$ | $a^4$ | $a^2b$ | $ab$ | $b$ | $a^4b$ | $a^2b^2$ | $ab^2$ | $b^2$ | $a^4b^2$ |
| $a^4b^3$ | $a^4b^3$ | $a^3b^3$ | $a^2b^3$ | $ab^3$ | $b^3$ | $a^4$ | $a^4b$ | $a^4b^2$ | $a^3$ | $a^2$ | $a$ | $e$ | $a^3b$ | $a^2b$ | $ab$ | $b$ | $a^3b^2$ | $a^2b^2$ | $ab^2$ | $b^2$ |

Tabela 4: Grupna tabela grupe $G_{20}$.

| | $e$ | $a$ | $a^2$ | $a^3$ | $a^4$ | $a^5$ | $a^6$ | $b$ | $b^2$ | $ab$ | $a^2b$ | $a^3b$ | $a^4b$ | $a^5b$ | $a^6b$ | $ab^2$ | $a^2b^2$ | $a^3b^2$ | $a^4b^2$ | $a^5b^2$ | $a^6b^2$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $e$ | $e$ | $a$ | $a^2$ | $a^3$ | $a^4$ | $a^5$ | $a^6$ | $b$ | $b^2$ | $ab$ | $a^2b$ | $a^3b$ | $a^4b$ | $a^5b$ | $a^6b$ | $ab^2$ | $a^2b^2$ | $a^3b^2$ | $a^4b^2$ | $a^5b^2$ | $a^6b^2$ |
| $a$ | $a$ | $a^2$ | $a^3$ | $a^4$ | $a^5$ | $a^6$ | $e$ | $ab$ | $ab^2$ | $a^2b$ | $a^3b$ | $a^4b$ | $a^5b$ | $a^6b$ | $b$ | $a^2b^2$ | $a^3b^2$ | $a^4b^2$ | $a^5b^2$ | $a^6b^2$ | $b^2$ |
| $a^2$ | $a^2$ | $a^3$ | $a^4$ | $a^5$ | $a^6$ | $e$ | $a$ | $a^2b$ | $a^2b^2$ | $a^3b$ | $a^4b$ | $a^5b$ | $a^6b$ | $b$ | $ab$ | $a^3b^2$ | $a^4b^2$ | $a^5b^2$ | $a^6b^2$ | $b^2$ | $ab^2$ |
| $a^3$ | $a^3$ | $a^4$ | $a^5$ | $a^6$ | $e$ | $a$ | $a^2$ | $a^3b$ | $a^3b^2$ | $a^4b$ | $a^5b$ | $a^6b$ | $b$ | $ab$ | $a^2b$ | $a^4b^2$ | $a^5b^2$ | $a^6b^2$ | $b^2$ | $ab^2$ | $a^2b^2$ |
| $a^4$ | $a^4$ | $a^5$ | $a^6$ | $e$ | $a$ | $a^2$ | $a^3$ | $a^4b$ | $a^4b^2$ | $a^5b$ | $a^6b$ | $b$ | $ab$ | $a^2b$ | $a^3b$ | $a^5b^2$ | $a^6b^2$ | $b^2$ | $ab^2$ | $a^2b^2$ | $a^3b^2$ |
| $a^5$ | $a^5$ | $a^6$ | $e$ | $a$ | $a^2$ | $a^3$ | $a^4$ | $a^5b$ | $a^5b^2$ | $a^6b$ | $b$ | $ab$ | $a^2b$ | $a^3b$ | $a^4b$ | $a^6b^2$ | $b^2$ | $ab^2$ | $a^2b^2$ | $a^3b^2$ | $a^4b^2$ |
| $a^6$ | $a^6$ | $e$ | $a$ | $a^2$ | $a^3$ | $a^4$ | $a^5$ | $a^6b$ | $a^6b^2$ | $b$ | $ab$ | $a^2b$ | $a^3b$ | $a^4b$ | $a^5b$ | $b^2$ | $ab^2$ | $a^2b^2$ | $a^3b^2$ | $a^4b^2$ | $a^5b^2$ |
| $b$ | $b$ | $a^4b$ | $ab$ | $a^5b$ | $a^2b$ | $a^6b$ | $a^3b$ | $b^2$ | $e$ | $a^4b^2$ | $ab^2$ | $a^5b^2$ | $a^2b^2$ | $a^6b^2$ | $a^3b^2$ | $a^4$ | $a$ | $a^5$ | $a^2$ | $a^6$ | $a^3$ |
| $b^2$ | $b^2$ | $a^2b^2$ | $a^4b^2$ | $a^6b^2$ | $ab^2$ | $a^3b^2$ | $a^5b^2$ | $e$ | $b$ | $a^2$ | $a^4$ | $a^6$ | $a$ | $a^3$ | $a^5$ | $a^2b$ | $a^4b$ | $a^6b$ | $ab$ | $a^3b$ | $a^5b$ |
| $ab$ | $ab$ | $a^5b$ | $a^2b$ | $a^6b$ | $a^3b$ | $b$ | $a^4b$ | $ab^2$ | $a$ | $a^5b^2$ | $a^2b^2$ | $a^6b^2$ | $a^3b^2$ | $b^2$ | $a^4b^2$ | $a^5$ | $a^2$ | $a^6$ | $a^3$ | $e$ | $a^4$ |
| $a^2b$ | $a^2b$ | $a^6b$ | $a^3b$ | $b$ | $a^4b$ | $ab$ | $a^5b$ | $a^2b$ | $a^2$ | $a^6b^2$ | $a^3b^2$ | $b^2$ | $a^4b^2$ | $ab^2$ | $a^5b^2$ | $a^6$ | $a^3$ | $e$ | $a^4$ | $a$ | $a^5$ |
| $a^3b$ | $a^3b$ | $b$ | $a^4b$ | $ab$ | $a^5b$ | $a^2b$ | $a^6b$ | $a^3b$ | $a^3$ | $b^2$ | $a^4b^2$ | $ab^2$ | $a^5b^2$ | $a^2b^2$ | $a^6b^2$ | $e$ | $a^4$ | $a$ | $a^5$ | $a^2$ | $a^6$ |
| $a^4b$ | $a^4b$ | $ab$ | $a^5b$ | $a^2b$ | $a^6b$ | $a^3b$ | $b$ | $a^4b$ | $a^4$ | $ab^2$ | $a^5b^2$ | $a^2b^2$ | $a^6b^2$ | $a^3b^2$ | $b^2$ | $a$ | $a^5$ | $a^2$ | $a^6$ | $a^3$ | $e$ |
| $a^5b$ | $a^5b$ | $a^2b$ | $a^6b$ | $a^3b$ | $b$ | $a^4b$ | $ab$ | $a^5b$ | $a^5$ | $a^2b^2$ | $a^6b^2$ | $a^3b^2$ | $b^2$ | $a^4b^2$ | $ab^2$ | $a^2$ | $a^6$ | $a^3$ | $e$ | $a^4$ | $a$ |
| $a^6b$ | $a^6b$ | $a^3b$ | $b$ | $a^4b$ | $ab$ | $a^5b$ | $a^2b$ | $a^6b$ | $a^6$ | $a^3b^2$ | $b^2$ | $a^4b^2$ | $ab^2$ | $a^5$ | $a^2b^2$ | $a^3$ | $e$ | $a^4$ | $a$ | $a^5$ | $a^2$ |
| $ab^2$ | $ab^2$ | $a^3b^2$ | $a^5b^2$ | $b^2$ | $a^2b^2$ | $a^4b^2$ | $a^6b^2$ | $a$ | $ab$ | $a^3$ | $a^5$ | $e$ | $a^2$ | $a^4$ | $a^6$ | $a^3b$ | $a^5b$ | $b$ | $a^2b$ | $a^4b$ | $a^6b$ |
| $a^2b^2$ | $a^2b^2$ | $a^4b^2$ | $a^6b^2$ | $ab^2$ | $a^3b^2$ | $a^5b^2$ | $b^2$ | $a^2$ | $a^2b$ | $a^4$ | $a^6$ | $a$ | $a^3$ | $a^5$ | $e$ | $a^4b$ | $a^6b$ | $ab$ | $a^3b$ | $a^5b$ | $b$ |
| $a^3b^2$ | $a^3b^2$ | $a^5b^2$ | $b^2$ | $a^2b^2$ | $a^4b^2$ | $a^6b^2$ | $ab^2$ | $a^3$ | $a^3b$ | $a^5$ | $e$ | $a^2$ | $a^4$ | $a^6$ | $a$ | $a^5b$ | $b$ | $a^2b$ | $a^4b$ | $a^6b$ | $ab$ |
| $a^4b^2$ | $a^4b^2$ | $a^6b^2$ | $ab^2$ | $a^3b^2$ | $a^5b^2$ | $b^2$ | $a^2b^2$ | $a^4$ | $a^4b$ | $a^6$ | $a$ | $a^3$ | $a^5$ | $e$ | $a^2$ | $a^6b$ | $ab$ | $a^3b$ | $a^5b$ | $b$ | $a^2b$ |
| $a^5b^2$ | $a^5b^2$ | $b^2$ | $a^2b^2$ | $a^4b^2$ | $a^6b^2$ | $ab^2$ | $a^3b^2$ | $a^5$ | $a^5b$ | $e$ | $a^2$ | $a^4$ | $a^6$ | $a$ | $a^3$ | $b$ | $a^2b$ | $a^4b$ | $a^6b$ | $ab$ | $a^3b$ |
| $a^6b^2$ | $a^6b^2$ | $ab^2$ | $a^3b^2$ | $a^5b^2$ | $b^2$ | $a^2b^2$ | $a^4b^2$ | $a^6$ | $a^6b$ | $a$ | $a^3$ | $a^5$ | $e$ | $a^2$ | $a^4$ | $ab$ | $a^3b$ | $a^5b$ | $b$ | $a^2b$ | $a^4b$ |

Tabela 5: Grupna tabela grupe $G_{21}$.

**UNIVERZA V LJUBLJANI**

**PEDAGOŠKA FAKULTETA**

**FAKULTETA ZA MATEMATIKO IN FIZIKO**

**študijski program: Matematika in fizika**

# IZJAVA

Spodaj podpisana Anja Smrtnik, rojena 26. decembra 1985, študentka Pedagoške fakultete Univerze v Ljubljani, smer matematika in fizika, izjavljam, da je diplomsko delo z naslovom

**KLASIFIKACIJA GRUP MAJHNIH REDOV**

pri mentorju doc. dr. Primožu Šparlu avtorsko delo. V diplomskem delu so uporabljeni viri in literatura korektno navedeni; teksti niso uporabljeni brez navedbe avtorjev.

Ljubljana, junij 2013 Anja Smrtnik