Algebra teorija 2023

Jana Vuković

25. februar 2025.

Hvala kolegama Davidu i Željku čije sam beleške pratila.

Sadržaj

1 Algebarske strukture

Skup sa nekim operacijama od interesa (uglavnom prirodne operacije)

Formiramo opisivanjem ili se prirodno pojavljuju. Zgodne su jer mogu da se računaju.

Pr: Osoba; visina, boja kose, dužina kose tj neki parametri

Matematički objekat koji se teško opisuje tako da treba da im dodelimo mu algebarsku strukturu.

Definicija 1.1 *Neka je A neprazan skup i* $n \in N \bigcup 0$. *Algebarska operacije f dužine n ili n-arna operacija je svako preslikavanje* $f : A^n \longrightarrow A$, *pišemo* $\#(f) = n$

$N = \{1, 2, 3, ...\}$ $A^n = A \times A \times .... \times A$

Zanimaće nas n=2 binarne operacije. Umesto $f(a, b)$ pišemo afb.

n=1 Unarna operacija

n= 0 Konstante A_0

Primeri:

1. Sabiranje i množenje su operacije na $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$
2. oduzimanje nije operacija na $\mathbb{N}$ ali jeste na $\mathbb{C}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$
3. deljenje nije operacija na $\mathbb{N}$ $\mathbb{Z}$ $\mathbb{Q}$ (deljenje nulom), $\mathbb{R}$, $\mathbb{C}$ ali jeste na $\mathbb{Q}\{0\}, \mathbb{R}\{0\}, \mathbb{C}\{0\}$ a nije na $\mathbb{Z}\{0\}$
4. NZD je operacija na $\mathbb{N}$. ovde pisemo $NZD(a, b)$
5. Neka je X neprazan skup. Tada su $\bigcup, \bigcap, \Delta$ operacije na $\mathcal{P}$(X)
6. A^A = f: A-¿A — f je funkcija $\circ$ je operacija na A^A (kompozicija) Bitno je da je domen isti kao kodomen.
7. $M_n(\mathbb{R})$ Operacija na $M_n(\mathbb{R})$ je $\cdot$
   $M_{m,n}(\mathbb{R})$ Operacija na $M_{m,n}(\mathbb{R})$ je $+$
8. $Z_n = \{0, 1, ..., n-1\}$ (=$\mathbb{Z}_n$ uskoro)

Za $m \in \mathbb{Z}$ definisemo ostatak pri deljenju m sa n. On je jedinstven:

m = nq + r

$0 \leq r \leq n-1$

i ρ(m, n) = r

Tada na Z_n definisemo operacije $+_n$, $\cdot_n$ sa (za a,b $\in$ Z_n);

a $+_n$ b = ρ(a+b, n)

a $\cdot_n$ b = ρ(a·b, n)

Operacije u 1-8 su binarne. Operacija ‘ na $\mathcal{P}(X)$ je jedna unarna operacija.

Def Algebarska strukture je uređena (n+1)-torka A = (A, f_1, f_2, ..., f_n) gde je A neprazan skup f_1, f_2, ... , f_n operacije na A tada vazi:
$\#(f_i) \leq \#(f_{i+1})$ za $1 \leq i \leq n-1$

Za A kazemo da je nosac algebarske strukture $\mathbb{A}$.

Komentar: Kada je jasno iz konteksta necemo praviti razliku izmedu A i $\mathbb{A}$. Tako cemo pisati $a \in \mathfrak{I}$ ili “A je algebarska struktura”.

Primeri:

1. (ℕ, +, ·, 1) je algebarska struktura
   (ℕ, -, 2) nije algebarska struktura I(ℕ, +, 2) je algebarska struktura.
2. ($\mathcal{P}$(X), $\bigcap, \bigcup, ‘, \emptyset$) je algebarska sturktura

1.1 Grupe

Definicija 1.2 *Algebarska struktura (G, ·) je grupa ako je · binarna operacija na G tada vazi:*

1. *Asocijativnost $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ za svako a, b, c ∈ G*
2. *postoji element e ∈ G tako da $a \cdot e = e \cdot a = a$ za sve a ∈ G*
3. *Za sve a ∈ G postoji $\tilde{a} \in G$ td $\tilde{a} \cdot a = a \cdot \tilde{a} = e$*

Komentar: Grupe mozemo da definisemo. Grupa je algebarska struktura (G, ·, -, e) td vazi 1),

umesto 2) vazi: 2’) a · e = e·a = a (za sve a · G)

umesto 3) vazi 3’) $\tilde{a} \cdot a = a \cdot \tilde{a}$ = e za sve a ∈ G

Imamo vise operacija sa kojima se lakse racuna, suzen skup operacija, olaksane su aksiome.

Komentar: Za element e kazemo da je neutral grupe, dok za element a kazemo da je inverz elementa a.

Stav 1.3 *Neutral u grupi je jedinstven.*

Dokaz: P.S. Neka su e i f, e ≠ f neutrali e je neutral $=_{a=f}$ sledi f·e = e·f = f
f je neutral $=_{a=e}$ sledi e·f = f·e = e
Iz ova dva sledi e = f Kontradikcija

Stav 1.4 *Za svaki a grupe G vazi da mu je inverz jedinstven*

Dokaz: Neka $\tilde{a}$ i $\bar{a}$ zadovoljavaju 3)
a·$\tilde{a}$ = $\tilde{a}$·a = e
i a·$\bar{a}$ = $\bar{a}$ · a = e
Posmatramo: $\bar{a}$·(a · $\tilde{a}$) $=^{3)}$ $\bar{a}$·e $=^{2)}$ $\bar{a}$
($\bar{a}$ · a) · $\tilde{a}$ =3) e·$\tilde{a}$ $=^{2)}$ $\tilde{a}$
$\bar{a}$·(a · $\tilde{a}$) = ($\bar{a}$ · a) · $\tilde{a}$
pa je $\tilde{a}$ = $\bar{a}$

Primeri i komentari:

1. – na Z nije asocijativno (1-2)-3 =/= 1-(2-3)
   Po dogovoru 1-2-3 = (1-2)-3
2. Kada je jasno koja je operacija cesto umesto a·b pisemo ab
3. Cesto umesto grupa (G, ·) kazemo grupa G. Tada je bitno naglasiti o kojoj se operacija radi.
4. $(\mathbb{Z}, +)$ je grupa. O je neutral. Inverz od n je -n.
   $(\mathbb{N}, +)$ nije grupa. $0 \notin \mathbb{N}$ i da jeste $0 \in \mathbb{N}$ ne bi postojao inverz.
5. $(M_n(\mathbb{R}), \cdot)$ nije grupa, jer nema svaka matrica inverz.
   (G $L_n(\mathbb{R})$, ·) je grupa. Proizvod dve matrice je invertibilna matrica
   $(AB)^{-1}=B^{-1} \cdot A^{-1}$
6. $(M_{m,n}(\mathbb{R}), +)$ jeste grupa, neutral nula matrica, inverz je suprotna matrica.
7. $(A^A, \circ)$ nije grupa 1) vazi, neutral je id_A: A $\longrightarrow$ A ; id_A(x) = x
8. BITAN PRIMER !
   $(Z_n, +_n) = \mathbb{Z}_n$ jeste grupa
   $+_n$ je asocijativna (za vezbu, zadatak 1.1)
   Neutral je 0.
   Inverz elementa $a \in \mathbb{Z}_n\{0, 1, 2, ..., n-1\}$ je n-a za $a \neq 0$, dok je a = 0 inverz 0.
9. $(\mathbb{Z}_n, \cdot_n)$ 1 je neutral, nije grupa za n ¿= 2. 0 nema inverz.

1.2 Osobine

Neka je (G, ·) grupa(svuda do kraja casa)

Za $x_1, x_2 ... x_n \in G$ definisemo sa $\prod_{i=1}^{n} x_i$ induktivno sa:

1) $\prod_{i=1}^{1} x_i = x_1$

2) $\prod_{i=1}^{n} x_i = \prod_{i=1}^{n-2} x_i \cdot x_n$

Umesto $\prod_{i=1}^{n} x_i$ pisemo i $(x_1...x_n)$

Stav 1.5 *Neka su* $x_1, ..., x_n, x_{n+1}, ..., x_{n+m}$
Tada vazi:
$\prod_{i=1}^{n} x_i \cdot \prod_{i=n+1}^{n+m} x_i$ *tj* $(x_1..x_n)\cdot(x_{n+1}...x_{n+m})$

Dokaz: indukcijom po m =1
Baza: m = 1 po definicije
Induktivno korak: m $\longrightarrow$ m+1
Vazi: $(x_1..x_n) \cdot (x_{n+1}...x_{n+m+1}) =^{definicija} (x_1..x_n)((x_{n+1}...x_{n+m}) \cdot x_{n+m+1})$
$=(x_1..x_n)(x_{n+1}...x_{n+m}) \cdot x_{n+m+1}$
$=^{IH}=(x_1...x_{n+m}) \cdot x_{n+m+1}$
$=^{podef}= (x_1...x_{n+m+1})$

Komentar: Ovo tvrdjenje dokazuje da u svakom izrazu zagrade mozemo da postavljamo na proizvoljan nacin. Zbog toga zagrade mozemo i da ne pisemo.

Specijalno za $x_1 = x_2 = ... = x_n = x$ umesto $\prod_{i=1}^{n} x_i$ pisemo $x^n = x \cdot x \cdot ... \cdot x$

Def Za binarnu operaciju * na A kazemo da je komutativna ako za sve a, b ∈ A vazi a*b=b*a

Stav 1.6 *Neka je $(G, \cdot)$ grupa td je $\cdot$ komutativna operacija. Tada za $x_1, ..., x_n \in G$ i $i_1, i_2, ..., i_n \in \mathbb{N}$ td $\{i_1, i_2, ..., i_n\}$ vazi $x_1 \cdot x_2 \cdot ... \cdot x_n = x_{i_1} \cdot x_{i_2} \cdot ... \cdot x_{i_n}$*

Dokaz: Indukcijom po n
Baza: n = 1 trivijalno x = x
IK: n $\longrightarrow$ n+1
$x_{i_1} \cdot x_{i_1} \cdot ... \cdot x_{i_{n+1}}$
Neka je $i_{n+1} = k$ Tada je $\{i_1, ..., i_n\} = \{1, ..., k-1, k+1, ...n+1\}$ Imamo n elemenata pa po IH:
$x_{i_1} \cdot x_{i_1} \cdot ... \cdot x_{i_n} \cdot x_{i_{n+1}} =^{IH}= x_1 \cdot x_2 \cdot ... \cdot x_{k-1} \cdot x_{k+1} \cdot ... \cdot x_{n+1} \cdot x_k$
Posmatramo $x_1 \cdot x_2 \cdot ... \cdot x_{k-1}$ kao jedan, $x_{k+1} \cdot ... \cdot x_{n+1}$ kao drugi element.
$= x_1 \cdot x_2 \cdot ... \cdot x_{k-1} \cdot ((x_{k+1} \cdot ... \cdot x_{n+1}) \cdot x_k) =^{komutativnost}= x_1 \cdot x_2 \cdot ... \cdot x_{k-1} \cdot (x_k \cdot (x_{k+1} \cdot ... \cdot x_{n+1}))$
$= x_1 \cdot x_2 \cdot ... \cdot x_{k-1} \cdot x_k \cdot x_{k+1} \cdot ... \cdot x_{n+1}$

Inverz elementa oznacavamo sa $x^{-1} (= \overline{x})$

Tvrdjenje 1.7 *Neka su $x, y \in G$ Tada vazi:*

1. $(x^{-1})^{-1} = x$
2. $(xy)^{-1} = y^{-1}x^{-1}$

Dokaz:

1. Kako je $x \cdot x^{-1} = x^{-1} \cdot x = e$ Kada gledamo iz ugla x^{-1}, x je njegov inverz, iz jedinstvenog inverza sledi $(x^{-1})^{-1} = x$
2. Slicno $(xy)^{-1} = y^{-1}x^{-1}$ sledi iz:
   $xyy^{-1}x^{-1} =^{3)}= x \cdot e \cdot x^{-1} =^{2)}= x \cdot x^{-1} = e$
   $y^{-1}x^{-1}xy =^{3)}= y^{-1} \cdot e \cdot y =^{2)}= y \cdot y^{-1} = e$

Tvrdjenje 1.8 $(x_1 \cdot ... \cdot x_n)^{-1} = x_n^{-1} \cdot ... \cdot x_2^{-1} \cdot x_1^{-1}$

Stav 1.9 *Za $n \geq 1$ sada definisemo:*
$n^{-n} = (x^n)^{-1} =^{prethodno}= (x^{-1})^n$

Stav 1.10 *Za $a, x, y \in G$ vazi $a \cdot x = a \cdot y \Rightarrow x = y$*

Dokaz:
Vazi $a \cdot x = a \cdot y \ / a^{-1} \cdot \sqcup$
$\Rightarrow a^{-1} \cdot a \cdot x = a^{-1} \cdot a \cdot y$
$e \cdot x = e \cdot y$
$x = y$

Definicija 1.11 $x^0 := e$

Teorema 1.12 *Neka je G grupa i $a, b \in G$ tada jednacina:*
$ax = b$ ima jedinstveno resenje u G

Dokaz: Iz $ax = b$ sledi $a^{-1}ax = a^{-1}b$ pa je $ex = x = a^{-1}b$ (Implikacija)
Dakle jednacina ima najvise jedno resenje i potencijalno resenje je $x = a^{-1}b$
Kako je $aa^{-1}b = eb = b$, to $x = a^{-1}b$ jeste resenje i dokaz je zavrsen.

Teorema 1.13 *Neka je G grupa $a, x \in G$ i $n \in \mathbb{N}$ Tada vazi:*
$(a \cdot x \cdot a^{-1})^n = a \cdot x^n \cdot a^{-1}$

Dokaz: Vazi $(axa^{-1})^n = axa^{-1}axa^{-1}a...a^{-1}axa^{-1}$
$= axexe...exa^{-1} = ax...xa^{-1} = ax^n a^{-1}$

Stav 1.14 *Neka je G grupa, $x \in G$ i $m, n \in \mathbb{Z}$ Tada vazi:*

1. $x^{m+n} = x^m \cdot x^n$
2. $(x^m)^n = x^{m \cdot n}$

Dokaz:

1. (a) Ako je $m = 0$ ili $n = 0$ tvrdjenje lako sledi $x^{0+n} = e \cdot x^n$
   (b) slucaj $m, n > 0$
   $x^{m+n} = x \cdot ..._{m+nputa}... \cdot x = x \cdot ..._{mputa}... \cdot x \cdot x \cdot ..._{nputa}... \cdot x = x^m \cdot x^n$
   (c) slucaj $m, n < 0$
   $x^{m+n} = (x^{-1})^{-m-n} = x^{-1} \cdot ..._{-m-nputa}... \cdot x^{-1} = x^{-1} \cdot ..._{-mputa}... \cdot x^{-1} \cdot x^{-1} \cdot ..._{-nputa}... \cdot x^{-1} = (x^{-1})^{-m} \cdot (x^{-1})^{-n} = x^m x^n$
   (d) $m > 0, n < 0$
      i. $m + n \geq 0$ Vazi: $x^m \cdot x^n = x \cdot ..._m ...x \cdot x^{-1} \cdot ..._{-n}... \cdot x^{-1} = x \cdot ..._{m+n}... \cdot x = x^{m+n}$
      ii. $m + n < 0$ Slicno kao iznad
2. Ako je $m = 0$ ili $n = 0$ tvrdjenje lako sledi
   (a) $m, n > 0$ Vazi: $x^{mn} = x \cdot ..._{mn}... \cdot x =$
   $x \cdot ..._m... \cdot x \cdot x \cdot ..._m... \cdot x \cdot ..._{nputasve} \cdot x \cdot ..._m... \cdot x = x^m \cdot ..._n ...x^m = (x^m)^n$
   (b) $m > 0, n < 0$ Vazi:
   $(x^m)^n = ((x^m)^{-n})^{-1} =^{odgore}= (x^{-mn})^{-1} = x^{mn}$
   (c) Oba slucaja kao gore

1.3 Primeri grupa

$\mathbb{C}_n = \{z \in \mathbb{C} | z^n = 1\} n \in \mathbb{N}$

Npr: $\mathbb{C}_2 = \{1, -1\}$

$\mathbb{C}_3 = \{1, \frac{-1+i\sqrt{3}}{2}, \frac{-1-i\sqrt{3}}{2}\}$

$\mathbb{C}_4 = \{1, -1, i, -i\}$

Podsetnik: Za $z \in \mathbb{C}$ postoje jedinstveni $\rho \in \mathbb{R}$, $\rho \geq 0$ i $\phi \in [0, 2\pi]$ takvi da vazi: $z = \rho(\cos\phi + i\sin\phi)$

Tada za $z_1 = \rho_1(\cos\phi_1 + i\sin\phi_1)$ i $z_2 = \rho_2(\cos\phi_2 + i\sin\phi_2)$

Vazi $z_1 z_2 = \rho_1\rho_2(\cos(\phi_1 + \phi_2) + i\sin(\phi_1 + \phi_2))$

Problem $\phi_1 + \phi_2 \geq 2\pi$ onda zbog periodicnosti mozemo da namestimo.

Specijalno $z^n = \rho^n(\cos(n\phi) + i\sin(n\phi))$

Iz ovoga resavamo: $z^n = 1$ vazi

$z^n = \rho^n(\cos(n\phi) + i\sin(n\phi)) = 1(\cos 0 + i\sin 0) = 1$

pa je $\rho^n = 1$ tj $\rho = 1$, a $n\phi = 2k\pi$ za $k \in \mathbb{Z}$

Uz to, $n\phi \in [0, 2n\pi)$ pa je $n\phi = 2k\pi$ za neko $k \in \{0, 1, ..., n-1\}$ Dakle $\phi = \frac{2k\pi}{n}$ tj.

$\mathbb{C}_n = \{\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} | 0 \leq k \leq n-1\}$

Stav 1.15 *$\mathbb{C}_n$ u odnosu na mnozenje kompleksnih brojeva je grupa.*

Dokaz: $\cdot$ je zatvoreno. Vazi: $(\cos\frac{2k\pi}{n} ii \sin\frac{2k\pi}{n})(\cos\frac{2l\pi}{n} ii \sin\frac{2l\pi}{n}) = cos\frac{2\pi(k+l)}{n} + i\sin\frac{2\pi(k+l)}{n} \in \mathbb{C}_n$
$\cos\frac{2(k+n)\pi}{n} + i\sin\frac{2(k+n)\pi}{n} = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$
Asocijativnost: ✓
Neutral: $1 = \cos 0 + i\sin 0$
Inverz elementa $\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$ za $k \neq 0$, a inverz za $k = 0$ je 1.
Neka je $\epsilon = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ Tada je:
$\mathbb{C}_n = \{\epsilon^k | 0 \leq k \leq n-1\}$ Jasno $\epsilon^n = 1$ pa je i $\epsilon^m \in \mathbb{C}_n$ za svako $m \in \mathbb{Z}$
Za $m = nq + r$ tkd $0 \leq r \leq n-1$ tada je $\epsilon^m = \epsilon^r \in \mathbb{C}_n$

1.4 Ciklicna grupa

Definicija 1.16 *Grupa G je ciklina ako postoji $x \in G$ td.*
$G = \{x^m | m \in \mathbb{Z}\}$

Tada za x kazemo da je generator grupe G.

Primeri:

1. $(\mathbb{C}_n, \cdot)$ je ciklicna grupa.
2. $(\mathbb{Z}_n, +_n)$ je ciklicna. Generator je 1 (Svaki element mozemo dobiti sabiranjem jedinica '$3 = 1^3$' po gornjoj def.
3. $(\mathbb{Z}, +)$ je ciklicna. Generator je 1 (ili -1)
4. $(\mathbb{Q}, +)$ nije ciklicna grupa. (iz $\frac{p}{q}k$ ne mozemo dobiti $\frac{1}{q+1}$ ili vece ni uzajamno proste manje od q)

1.5 Grupe formirane od bijekcija

Neka je $\mathcal{F}$ figura u ravni. Posmatramo skup: $\mathcal{S}(\mathcal{F}) = \{\sigma : \mathbb{R}^2 \longrightarrow \mathbb{R}^2 | \sigma$ je simetrija od $\mathcal{F}\}$

Transformacije ravni koje cuvaju rastojanja i pritom ne pomeraju figuru $\mathcal{F}$

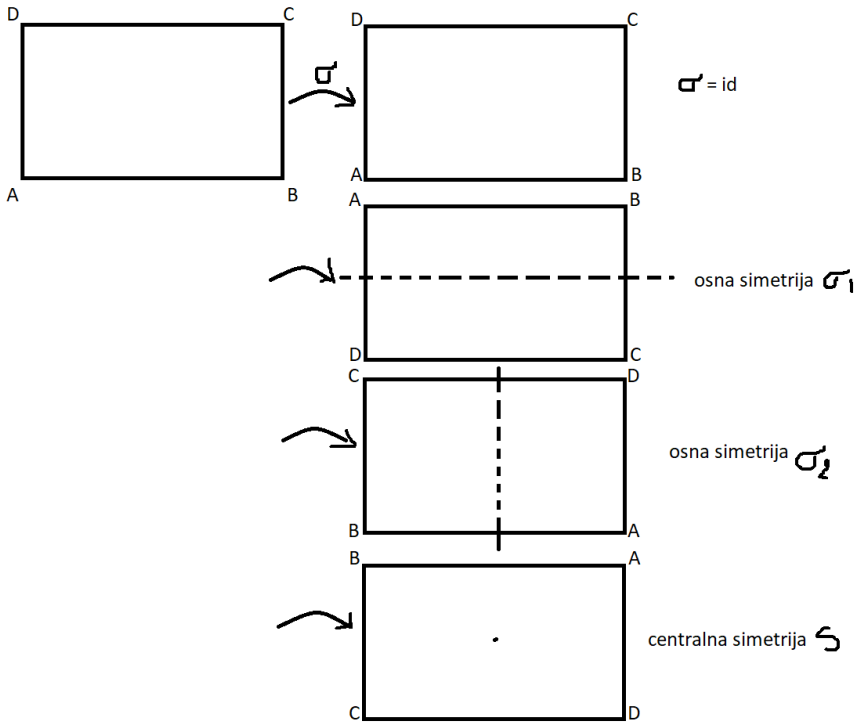
Stav 1.17 *$(\mathcal{S}(\mathcal{F}), \circ)$ je grupa.*

Neutral je *id*. Dokaz sledi iz tvrdjenja da je kompozicija simetrija isto neutral.inverz ce postojati i bice izometrija.

Primeri:

1.

Grupa simetrija $V = \{\text{id}, \sigma_1, \sigma_2, S\}$



Definicija 1.18 *Kejlijeva tablica grupe V je tablica kojom je prikazana operacija u konacnoj grupi*

	id	σ_1	σ_2	S
id	id	σ_1	σ_2	S
σ_1	σ_1	id	S	$\sigma_1 \circ S = \sigma_2$
σ_2	σ_2	S	id	σ_1
S	S	σ_2	σ_1	id

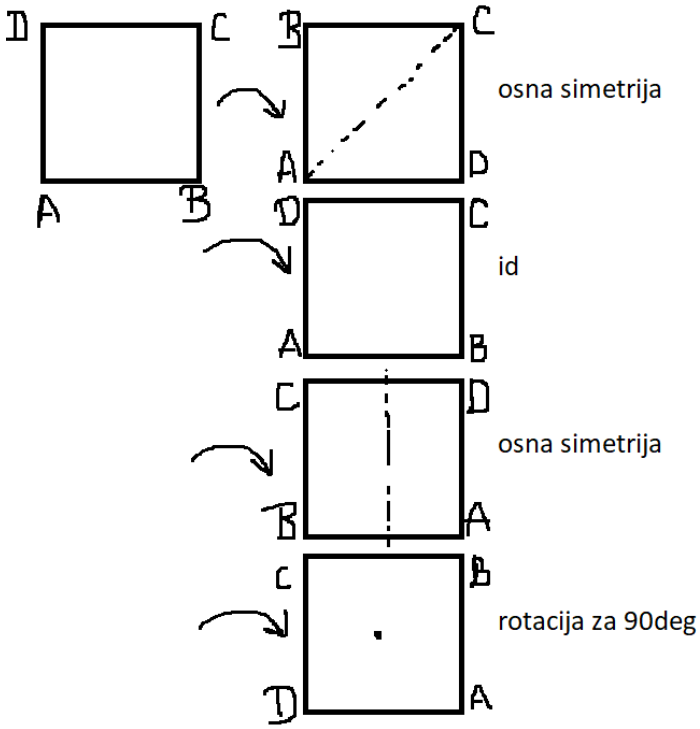
Simetrija u odnosu na glavnu dijagonalu $\Leftrightarrow$ grupa je komutativna

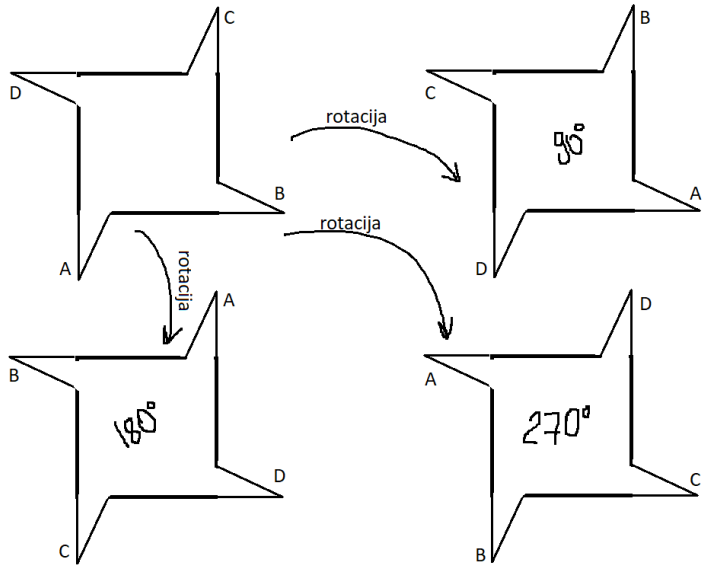
2. $\mathcal{F}$ = kvadrat

Ukupno 8 simetrija kvadrata

3. $\mathcal{F}$ = ovajOblik

$\{\mathrm{id}, \rho_{90^{\mathrm{deg}}}, \rho_{180^{\mathrm{deg}}}, \rho_{270^{\mathrm{deg}}}\} = \{\mathrm{id}, \rho_{90^{\mathrm{deg}}}, \rho^2_{90^{\mathrm{deg}}}, \rho^3_{90^{\mathrm{deg}}}\}$ i ona je ciklicna


D
C
A
B
osna simetrija
id
osna simetrija
rotacija za 90deg


C
D
B
A
rotacija
90°
rotacija
rotacija
180°
270°

1.6 Diedarske grupe

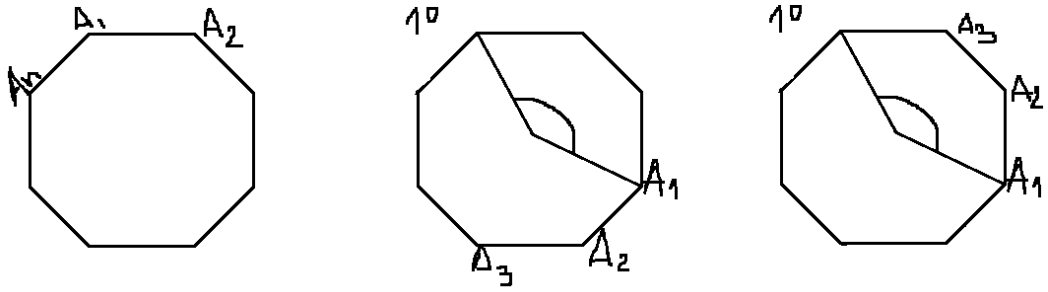
Definicija 1.19 *Diedarska grupa, u oznaci $\mathbb{D}_n$, je grupa simetrija pravilnog n-touglao.*

Neka se A_1 slika u A_k $(A_1 \longmapsto A_k)$

Tada je $A_2 \longmapsto A_{k+1}$ ili $A_2 \longmapsto A_{k-1}$

U prvom slucaju vazi $A_3 \longmapsto A_{k+2}$

U drugom vazi $A_3 \longmapsto A_{k-2}$



Izometrija slike zahteva 3 tacke. Zato je 1. rotacija oko centra za $\frac{2\pi}{n} \cdot (k-1)$ dok je 2. osna simetrija.

Stav 1.20 $|\mathbb{D}_n| = 2n$

Neka je ρ rotacija za $\frac{2\pi}{n}$ (oko O). Neka je σ neka od simetrija. Tada je

$\mathbb{D}_n = \{id, \rho, ..., \rho^{n-1}, \sigma, ...\sigma\rho^{n-1}\}$

Uz to $\rho^n = id$

$\sigma^2 = id$

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

$\rho^i \cdot \rho^j = \rho^{i+j}$

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

Vazi: $\rho^i\sigma = \sigma\rho^{n-i}$ (indukcijom po i

1.7 Podgrupa

Definicija 1.21 *Neka su $(G, \cdot)$ i $(H, *)$ grupa. Tada je $(H, *)$ podgrupa grupe $(G, \cdot)$ ako vazi $H \subseteq G$ i $x * y = x \cdot y$ za sve $x, y \in H$. Pisemo $(H, *) \leq (G, \cdot)$ ili samo $H \leq G$*

Primer: $(\mathbb{G}, +) \leq (\mathbb{R}, +)$ Te operacije nisu iste formalno, ali se na manjem skupu isto izvrsavaju.

1. $(\mathbb{Z}, +) \leq (\mathbb{Q}, +) \leq (\mathbb{R}, +) \leq (\mathbb{C}, +)$
2. $(\mathbb{C}_n, \cdot) \leq (\mathbb{C}\backslash\{0\}, \cdot)$
3. $(\mathbb{Z}, +_n) \not\leq (\mathbb{Z}, +)$

1.7.1 Osobine podgrupa

Neka je $H \leq G$. Tada je:

1. za neutral ϵ grupe H, i neutral e iz grupe G vazi $\epsilon = e$

   Dokaz: Neka je $x \in H$ Tada je $(x \cdot \epsilon =) x * \epsilon = x / x^{-1} \cdot \bigsqcup$ gde je x^{-1} inverz u G

   $x^{-1}x\epsilon = x^{-1}x = e$

2. Ako je $x \in H$ i $\tilde{x}$ njegov inverz u H, a $\overline{x}$ njegov inverz u G tada je $\tilde{x} = \overline{x}$

   Dokaz: Vazi $\tilde{x} * x = \epsilon = e$ iz 1)

   $x * \tilde{x} = \tilde{x} * x = \epsilon = e$ pa je zbog jedinstvenosti inverza u G $\overline{x} = \tilde{x}$

Stav 1.22 *Neka je $(G, \cdot)$ grupa. Preslikavanje $* : H \times H \longrightarrow H$ je restrikcija operacije $\cdot$ ako za sve $x, y \in H$ vazi $x * y = x \cdot y$ (Ovde je $H \subseteq G$).*

Stav 1.23 *Neprazan podskup H grupe G je podgrupa u G u odnosu na restrikciju operacije iz G ako za sve $x, y \in H$ vazi $xy^{-1} \in H$ (ovaj izraz racunamo u G). Ovaj stav menja ona tri uslova.*

Dokaz: Neka je $(G, \cdot)$ data grupa i restrikcija operacije $\cdot$ na H.
($\Rightarrow$) Dakle $(H, *) \leq (G, \cdot)$. Neka su $x, y \in H$. Tada je y^{-1} inverz od y i u H, pa je $xy^{-1} = x * y^{-1} \in H$ zbog zatvorenosti.
($\Leftarrow$) Sada dokazujemo da je $(H, *) \leq (G, \cdot)$. Vec vazi $x * y = x \cdot y$ za $x, y \in H$

1. * je operacija na H. Drugim recima dokazujemo da za $x, y \in H$ vazi $x * y = xy \in H$ Za ovo je dovoljno dokazati implikaciju:

   $y \in H \Rightarrow y^{-1} \in H$ jer tada imamo $x, y \in H \Rightarrow x, y^{-1} \in H$ po uslovu $\Rightarrow x(y^{-1})^{-1} = xy \in H$

   Za implikaciju $y \in H \Rightarrow y^{-1} \in H$ je dovoljno dokazati $e \in H$ jer je tada $y \in H \Rightarrow e, y \in H \Rightarrow ey^{-1} = y^{-1} \in H$

   Uzmimo proizvoljan element iz H ($x \in H$) on postoji jer $H \neq \emptyset$ Tada iz:

   $x, x \in H \Rightarrow x \cdot x^{-1} = e \in H$ cime je dokaz zavrsen.

2. $(H, *)$ je grupa.

   - $x * (y * z) = x \cdot (y \cdot z) =^{\cdot asocijativno} = (x \cdot y) \cdot z = (x * y) * z$ je asocijativna $(x, y, z \in H)$
   - $x \in H$

     $x * e = x \cdot e = e \cdot x = e * x = x$ pa je e neutral u H.
   - $x \in H$ Tada je $x^{-1} \in H$ i vazi:

     $x * x^{-1} = x \cdot x^{-1} = x^{-1} \cdot x = x^{-1} * x = e$ pa je x^{-1} inverz od x u H

Stav 1.24 *Ako su H i K podgrupe grupe G, tada je i $H \bigcap K$ podgrupa od G.*

Dokaz: Koristimo prethodni stav.

1. $H \bigcap K \neq \emptyset$ Svaka podgrupa sadrzi neutral pa $e \in H \bigcap K$.
2. $x, y \in H \bigcap K \Rightarrow xy^{-1} \in H \bigcap K$

   Vazi: $x, y \in H \bigcap K \Rightarrow x, y \in H$ i $x, y \in K$ po prethodnom stavu $\Rightarrow x \cdot y^{-1} \in H$, $xy^{-1} \in K \Rightarrow xy^{-1} \in H \bigcap K$.

Komentar: Ako vazi $H, K \leq G$ tada je $H \bigcup K \leq G$ (jedino u trivijalnim slucajevima) ako je $H \subseteq K$ ili $K \subseteq H$.

$x \in H \Rightarrow yxx^{-1} = y \in H$

Definicija 1.25 *Neka je G grupa i $S \subseteq G$. Tada sa $< S >$ oznacavamo minimalnu podgrupu (u odnosu na inkluziju) koja sadrzi S. Za $< S >$ kazemo da je podgrupa generisana sa S.*

Vazi: $< S >= \bigcap_{H \leq G \ S \subseteq H}$, $A \bigcup B \subseteq A$ ne moze da se formira manja grupa. Podgrupa je zbog preseka.

Definicija 1.26 $< S >= \{a_1 \cdot ... \cdot a_n | n \in \mathbb{N}, a_i \in S \bigcup S^{-1}\}$ *gde je* $S^{-1} \in \{x^{-1} | x \in S\}$

Skica: Mora sve da pripada da bi bilo zatvoreno u odnosu na $\cdot$.
Koristimo stav 1.23
$(a_1, ..., a_n)(b_1, ..., b_n)^{-1}$ $a_i, b_j \in S \bigcup S^{-1}$
$= a_1 ... a_n b_m^{-1} ... b_1^{-1}$ $a_i \in S \bigcup S^{-1}, b_j \in S \bigcup S^{-1}$

Primeri:

1. $S = x$
   $< S >= \{x^k | k \in \mathbb{Z}\}$ ciklicna grupa generisana sa x
2. $\mathbb{D}_n =< \rho, \sigma >$

2 Red elemnta i red grupe

Definicija 2.1 *Ako je grupa G konacna, onda je njen red jednak $|G|$. Ako je G beskonacna, kazemo da je beskonacnog reda*

Neka je a element grupe G. Tada je red od a u oznaci $\omega(a)$ najmanje $n \in \mathbb{N}$ td $a^n = e$ (ako postoji). AKo ovakvo $n \in \mathbb{N}$ ne postoji kazemo da je a beskonacnog reda.

Primeri:

1. $(\mathbb{Z}_n, +_n)$ n = 6, $\omega(1) = n$, $\omega(4) = 3$
2. $(\mathbb{D}_n, \circ)$ $\omega(\rho) = n$, $\omega(\sigma) = 2$
3. $(G, \cdot)$ $\omega(e) = 1$, $\omega(x) = 1$ akko x = e.
4. $(\mathbb{Z}, +)$ svako $n \neq 0$ je beskonacnog reda

Stav 2.2 *Red ma kog elementa jednak je redu podgrupe koju taj element generise.*

Dokaz: Neka je G grupa i $x \in G$ Dokazujemo da vazi:

1. Ako je x konacnog reda, tada je $\omega(x) = | < x > |$
2. Ako je x beskonacnog reda, tada je i $< x >$ beskonacnog reda

1. : Neka je $\omega(x) = n$ Dokazujemo da vazi $< x >= \{e, x, x^2, ..., x^{n-1}\}(\#)$

   Po definiciji $< x >= \{x^n | n \in \mathbb{Z}\}$, pa vazi $\supseteq$. Dokazimo i $\subseteq$.

   Neka je $y \in < x >$. Tada je $y = x^m$ za neko $m \in \mathbb{Z}$. Kako je $\omega(x) = n$, to je $x^n = e$. Postoje $q, r \in \mathbb{Z}$ takvi da je $m = nq + r$, $0 \leq r \leq n-1$ i tada vazi $x^m = x^{nq+r} = (x^n)^q \cdot x^r = x^r$, cime je dokaz # zavrsen. Sada je dovoljno dokazati da je $x_i \neq x^j$ za sve $0 \leq i \leq j \leq n-1$ (tada $< x >$ ima n elemenata).

   PPS. $x^i = x^j / x^{-i} \Rightarrow e = x^{j-i}$, a $0 < j - i < n = \omega(x)$ Kontradikcija (definicija: n najmanji)

2. : PPS. $< x >= \{x^m | m \in \mathbb{Z}\}$ je konacan skup. Tada postoje i, j td $i < j$ i $x^i = x^j \ x^{-i}$ Sledi da je $e = x^{j-i}$, $j - i \in \mathbb{N}$ tj x je konacnog reda. Kontradikcija.

Stav 2.3 *Neka je G grupa i $a \in G$. Ako je a beskonacnog reda i $m \in \mathbb{Z}\backslash\{0\}$, tada je i a^m beskonacnog reda. AKo je a konacnog reda i $m \in \mathbb{Z}\backslash\{0\}$, tada je $\omega(a^m) = \frac{\omega(a)}{NZD(\omega(a), m0)}$*

Dokaz:

I PPS a^m je reda $n \in \mathbb{N}$. Tada je $(a^m)^n = a^{mn} = e$ i $a^{-mn} = e$ pa kako je $mn > 0$ ili $-mn > 0$, to je a konacnog reda. Kontradikcija.

II Odredimo najmanje $k \in \mathbb{N}$ takvo da $(a^m)^k = e$ (tada je $\omega(a^m) = k$). Pre ovoga dokazimo sledece:

Stav 2.4 *Neka je G grupa i a konacnog reda. Tada za $l \in \mathbb{Z}$ vazi $a^l = e$ akko $\omega(a)|l$*

Dokaz:

$\Leftarrow$ Tada je $l = \omega(a) \cdot m$ pa je $a^l = a^{\omega(a) \cdot m} = (a^{\omega(a)})^m = e$

$\Rightarrow$ Neka je $\omega(a) = n$. Postoje $q, r \in \mathbb{Z}$ td. $l = nq + r$, $0 \leq r \leq n-1$. Tada je $e = a^l = a^{nq+r} = (a^n)^q \cdot a^r = a^r$ pa kako je $r < n$, mora biti $r \notin \mathbb{N}$ tj. r = 0 i $n|l$.

Nastavak dokaza stava2: Vazi $a^{mk} = e$ akko $\omega(a)|mk$ tj akko $\frac{\omega(a)}{NZD(\omega(a),m)} | \frac{m}{NZD(\omega(a),m)} k$.
$NZD(\frac{\omega(a)}{NZD(\omega(a),m)}, \frac{m}{NZD(\omega(a),m)}) = 1$ pa:
1deg: Akko $\frac{\omega(a)}{NZD(\omega(a),m)} | k$, najmanje ovakvo $k \in \mathbb{N}$ je bas $\omega(a^m)$ i jednako je $\frac{\omega(a)}{NZD(\omega(a),m)}$

Primer: U $\mathbb{Z}_{24}$: $\omega(14) = \frac{\omega(1)}{NZD(\omega(1),14)} = \frac{24}{NZD(24,14)} = \frac{24}{2} = 12$

Teorema 2.5 *1. Svaka podgrupa ciklicne grupe je ciklicna*

2. Ako je G ciklicna grupa reda n, tada za svako $k \in \mathbb{N}$ takvo da $k|n$ postoji jedinstvena podgrupa reda k od G.

Dokaz:

1. Neka je G ciklicna grupa tj $G =< a >$ i $H \leq G$. Ako je $H = \{e\}$, tada je $H =< e >$. U suprotnom neka je $k \in \mathbb{N}$ najmanje takvo da je $a^k \in H$ (ovo postoji jer $H \neq \{e\}$). Dokazimo da je $H =< a^k >$.

   $\supseteq$: Iz $a^k \in H$ zbog zatvorenosti sledi $(a^k)^m \in H$ pa $< a^k > \subseteq H$

   $\subseteq$: Neka je $x \in H \subseteq G$ Tada je $x = a^l$ za neko $l \in \mathbb{Z}$. Postoje $q, r \in \mathbb{Z}$ tkd je $l = kq + r$, $0 \leq r \leq k-1$ pa je $a^l = a^{kq+r} = (a^k)^q \cdot a^r \in H$. Iz $a^k \in H$ sledi $(a^k)^q \in H$, pa je $a^r = (a^k)^{-q} \cdot a^l \in H$. Odavde sledi (zbog nacina odabira k) tj $k|l$ pa je $a^l \in < a^k >$.

2. Neka je $G =< a >$. Tada je $\omega(a) = | < a > | = |G| = n$. Vazi: $\omega(a^{\frac{n}{k}}) = \frac{\omega(a)}{NZD(\omega(a), \frac{n}{k})} = \frac{n}{NZD(n, \frac{n}{k})} = \frac{n}{\frac{n}{k}} = k$, pa je $| < a^{\frac{n}{k}} > | = \omega(a^{\frac{n}{k}}) = k$. Neka je $H \leq G$ td $|H| = k$. Po delu 1 H je ciklicna, pa je $H =< a^l >$. Iz ovoga sledi $k = |H| = | < a^l > | = \omega(a^l) = \frac{\omega(a)}{NZD(\omega(a), l)} = \frac{n}{NZD(n,l)}$, pa je $\text{NZD}(n, l) = \frac{n}{k}$.

   Odavde $\frac{n}{k}|l$ pa $a^l \in < a^{\frac{n}{k}} >$, a dalje sledi $(a^l)^n \in < a^{\frac{n}{k}} >$ tj $H =< a^l > \subseteq < a^{\frac{n}{k}} >$.

   Kako $| < a^l > | = | < a^{\frac{n}{k}} > |$, sledi $H =< a^{\frac{n}{k}} >$

3 Izomorfizmi grupa

Definicija 3.1 *Neka su $(G, \cdot)$ i $(H, *)$ grupe. Kazemo da su ove grupe izomorfne ako postoji bijekcija $f : G \longrightarrow H$ td. za sve $x, y \in G$ vazi: $f(x \cdot y) = f(x) * f(y)$*

Za preslikavanje f kazemo da je izomorfizam grupa G i H. Kada su G i H izomorfne, pisemo $G \cong H$

Komentar: 1, 2, 3, 4... $\longrightarrow$ I, II, III, IV...

Primer:$\mathbb{C}_4 = \{1, -1, i, -i\}$ i $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ i imamo:

$f : \mathbb{Z}_4 \longrightarrow \mathbb{C}_4$ zadato sa:

f(0) = 1, f(1) = i, f(2) = -1, f(3) = -i.

$f(2 +_4 3) =^? = f(2) \cdot f(3)$

$f(1) =^? = -1 \cdot (-1)$ ovo je $i = i$ tacno.

Stav 3.2 *Ako je e neutral u $(G, \cdot)$, ϵ neutral u $(H, *)$ i $f : G \longrightarrow H$ izomorfizam grupa, onda je $f(e) = \epsilon$. Takodje za svako $x \in G$ je $f(x^{-1}) = (f(x))^{-1}$.*

Dokaz: Vazi $f(e) = f(e \cdot e) =^{def} = f(e) * f(e) / \bigsqcup * f(e)^{-1} \Rightarrow \epsilon = f(e)$
Vazi $\epsilon = f(e) = f(x \cdot x^{-1}) =^{-1} = f(x) * f(x^{-1}) / (f(x))^{-1} * \bigsqcup$
$\Rightarrow (f(x))^{-1} = (f(x))^{-1} * f(x) * f(x^{-1}) = f(x^{-1})$
Komentar: U dokazu nismo koristili da je f-bijekcija (vazi za svaku izomorfnu grupu). Neutral cemo uglavnom oznacavati sa e, cak i kada imamo vise grupa.

Stav 3.3 *Ako je $f : G \longrightarrow H$ izomorfizam grupa, tada je $f^{-1} : H \longrightarrow G$ takodje izomorfizam.*

Dokaz: Kako je f bijekcija, to f^{-1} postoji i bijekcija je. Zato je dovoljno dokazati da za $x, y \in H$ vazi: $f^{-1}(x * y) = f^{-1}(x) \cdot f^{-1}(y)$ gde je * operacija u H, a $\cdot$ u G. Kako je f bijekcija, to postoje $a, b \in G$ td $x = f(a)$ i $y = f(b)$ pa je: $f^{-1}(x) \cdot f^{-1}(y) = f^{-1}(f(a)) \cdot f^{-1}(f(b)) = a \cdot b$, dok je $f^{-1}(x * y) = f^{-1}(f(a) * f(b)) =^{def} = f^{-1}(f(a \cdot)) = ab$

Stav 3.4 *Neka je $f : G \longrightarrow H$ izomorfizam grupa i $x \in G$.*

1. *Ako je x beskonacnog reda, tada je i f(x) beskonacnog reda.*
2. *Ako je x konacnog reda, tada je i $\omega(x) = \omega(f(x))$*

Dokaz:

1. PPS f(x) je konacnog reda. Neka je $\omega(f(x)) = n$. Tada je $(f(x))^n = e$ pa je $f(x^n) = (f(x))^n$ (f je izomorfizam) $= e = f(e)$. Kako je f "1-1šledi $x^n = e$ Kontradikcija.
2. Neka je $\omega(x) = n$. Tada je $x^n = e$ pa je $f(x^n) = (f(x))^n = f(e) = e$ tj. $\omega(f(x))|n$. Neka je $\omega(f(x)) = m$. Tada je $f(e) = e = (f(x))^m = f(x^m)$, pa je kao i u 1. $x^m = e$ tj $n = \omega(x)|m$ Sledi n = m.

Teorema 3.5 *Svaka ciklicna grupa izomorfna je ili grupi $\mathbb{Z}$ ili $\mathbb{Z}_n$ za neko $n \in \mathbb{N}$.*

Dokaz: Neka je G ciklicna grupa i $x \in G$ njen generator. Tadaje $G =< x >= \{x^m | m \in \mathbb{Z}\}$

I G je beskonacnog reda.

Dokazujemo da je $f : \mathbb{Z} \Longrightarrow G$ zadato sa $f(m) = x^m$ za $m \in \mathbb{Z}$ izomorfizam.

1. f je bijekcija: f je "na-trivijalno; f je "1-1"
   vazi $f(n) = f(m)$ Odavde $x^n = x^m$ tj $x^{n-m} = e$
2. $f(n + m) = f(n) \cdot f(m)$ Vazi $f(n + m) = x^{n+m}$, a $f(n) \cdot f(m) = x^n x^m = x^{n+m}$.

II G je reda n

Tada je $G = \{e, x, x^2, ..., x^n\}$ (dokazano ranije). Dokazujemo da je $f : \mathbb{Z}_n \longrightarrow G$ zadato sa: $f(k) = x^k$ za $k \in \mathbb{Z}_n$ izomorfizam.

1. f je bijekcija. Sledi iz ovoga gore.
2. $f(kk_nm) = f(k) \cdot f(m)$ Vazi $f(k +_n m) = x^{k+_n m}$ dokje $f(k) \cdot f(m) = x^n \cdot x^m = x^{k+m}$. Dalje $\omega(x) = | < x > | = |G| = n$, pa je $x^n = e$ i ako zapisemo $k + m = nq + (k +_n m), q \in \mathbb{Z}$. Dobijamo $x^{k+m} = x^{nq+(k+_n m)} = (x^n)^q \cdot x^{k+_n m} = x^{k+_n m}$

4 Grupe Permutacija

Stav 4.1 *Neka je X neprazan skup. Posmatrajmo skup $\mathbb{S}_x$ zadat sa $\mathbb{S}_x = \{f : X \Longrightarrow X | f je bijekcija\}$. Tada je $(\mathbb{S}_x, \circ)$ gde je $\circ$ kompozicija funkcija, grupa. Nazivamo je grupa permutacija skupa X.*

Dokaz:

I $\circ$ je operacija. Za $f, g \in \mathbb{S}_x$ je $f \circ g : X \longrightarrow X$ dobro definisano, a kako su f i g bijekcije, to je i $f \circ g$ bijekcija, pa je $f \circ g \in \mathbb{S}_x$.

II $\circ$ je asocijativna.

III Neutral $id_x : X \longleftarrow X$ ($id_x(x) = x$, pa $id_x \in \mathbb{S}_x$)

IV Inverz: za $f \in \mathbb{S}_x$ inverz je f^{-1} (kako je f bijekcija to f^{-1} postoji i bijekcija je).

Stav 4.2 *Ako postoji bijekcija izmedju X i Y, tada je $\mathbb{S}_x \cong \mathbb{S}_y$.*

Neka je $f : X \longrightarrow Y$ bijekcija. Dokazujemo da je $\Phi : \mathbb{S}_x \longrightarrow \mathbb{S}_y$ zadato sa $\Phi(\pi) = f \circ \pi \circ f^{-1}$ za $\pi \in \mathbb{S}_x$ izomorfizam.

1. Φ je dobro definisana

   Dokazujemo da je $f \circ \pi f^{-1} \in \mathbb{S}_y$. Ovo je tacno jer je $f \circ \pi f^{-1} : Y \longrightarrow Y$ bijekcija kao kompozicija bijekcija.

2. Φ je bijekcija.

   Φ je "1-1": Vazi $\phi(\pi_1) = \phi(\pi_2) \Rightarrow f \circ \pi_1 \circ f^1 f \circ \pi_2 \circ f^1 / f^{-1} \circ \bigsqcup \circ f \Rightarrow \pi_1 = \pi_2$

   Φ je "na": Neka je $\sigma \in \mathbb{S}_y$. Tada vazi: $\Phi(f^{-1} \circ \sigma \circ f) = f \circ f^{-1} \circ \sigma \circ f \circ f^{-1} = \sigma$, a $f^{-1} \circ f$ pripada $\mathbb{S}_x$ (kao u 1)

3. $\Phi(\pi_1 \circ \pi_2) = \Phi(\pi_1) \circ \Phi(\pi_2)$

   Vazi $\Phi(\pi_1) \circ \Phi(\pi_2) = f \circ \pi + 1 \circ f^{-1} \circ f \circ \pi_2 \circ f^{-1} = f \circ \pi_1 \circ \pi_2 \circ f^{-1} = \Phi(\pi_1 \circ \pi_2)$

U nastavku X ce uglavnom biti konacan. Ako $|X| = n$ tada je $\mathbb{S}_x \cong \mathbb{S}_{\{1,2,...,n\}}$ pa zato uvodimo $\mathbb{S}_n$ kao $\mathbb{S}_{\{1,2,...,n\}}$.

Za $\pi \in \mathbb{S}_n$ cesto pisemo (i definisemo sa): $\pi = \begin{pmatrix} 1 & 2 & 3 & ... & n \\ \pi(1) & \pi(2) & \pi(3) & ... & \pi(n) \end{pmatrix}$

Primer: $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 5 & 4 & 3 \end{pmatrix}$

$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 4 & 1 & 5 & 2 \end{pmatrix}$

$\pi \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 5 & 2 & 4 & 6 \end{pmatrix}$

$\sigma \circ \pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 6 & 5 & 1 & 4 \end{pmatrix}$

$\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 2 & 3 & 5 & 1 \end{pmatrix}$

$|\mathbb{S}_n| = n!$

Neka su $a_1, a_2, ..., a_n \in \{1, 2, ..., n\}$ razliciti. Tada cikl ili ciklus $(a_1, a_2, ..., a_k)$ u $\mathbb{S}_n$ definisemo kao permutaciju tako da $\pi(a_i) = a_{i+1}$ za $1 \leq i \leq k-1$, $\quad \pi(a_k) = a_1 \quad \pi(b) = b$ za $b \notin \{a_1, ..., a_k\}$

Primer: U $\mathbb{S}_7$: $(4 \quad 7 \quad 1 \quad 2) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 3 & 7 & 5 & 6 & 1 \end{pmatrix}$

Skup $\{a_1, a_2, ..., a_k\}$ je nosac ciklusa $(a_1, a_2, ..., a_k)$

Za dva cirklusa kazemo da su disjunktni ako imaju disjunktne nosace.

Tvrdjenje 4.3 *Neka su σ i π disjunktni ciklusi iz $\mathbb{S}_n$. Tada je $\sigma \circ \pi = \pi \circ \sigma$.*

Dokaz: Neka je S nosac ciklusa σ, a P nosac ciklusa π. Dokazujemo da za svako $x \in \{1, 2, ..., n\}$ vazi $(\sigma \circ \pi)(x) = (\pi \circ \sigma)(x)$

I $x \in P$. Tada $x \notin S$ Vazi $(\sigma \circ \pi)(x) = \sigma(\pi(x)) = \pi(x)$, pa $\pi(x) \notin S$ kao i $(\pi \circ \sigma)(x) = \pi(\sigma(x)) = \pi(x)$

II $x \in S$ kao I

III $x \notin S \bigcup P$ Vazi $(\sigma \circ \pi)(x) = \sigma(\pi(x)) = \sigma(x) = x$ i slicno $(\pi \circ \sigma)(x) = x$

Teorema 4.4 *Svaka permutacija iz $\mathbb{S}_n$ moze se na jedinstven nacin, do na redosled faktora, predstaviti kao proizvod disjunktnih ciklusa.*

Primer: $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 4 & 1 & 3 & 2 & 8 & 7 \end{pmatrix}$
$\pi = (1 \quad 5 \quad 3 \quad 4)(2 \quad 6)(7 \quad 8)$

Stav 4.5 *Neka je $\sigma = \pi_1\pi_2...\pi_k$ gde su $\pi_1, \pi_2..., \pi_k$ disjunktni ciklusi. Tada je $\sigma^m = \pi_1^m\pi_2^m...\pi_k^m$. Ako je $\sigma = \pi_1\pi_2...\pi_k$, gde su $\pi_1, \pi_2, ...\pi_k$ disjunktni ciklusi tada je $\omega(\sigma) = NZS(\omega(\pi_1), \omega(\pi_2), ..., \omega(\pi_k))$. Za $\sigma = (\sigma_1, \sigma_2, ...\sigma_k)$ je $\omega(\sigma) = k$.*

Dokaz: Neka je $l \in \mathbb{N}$ td. $\pi^l = id$. Vazi: $\pi^l = id \Leftrightarrow (\sigma_1...\sigma_k)^l = id \Leftrightarrow \sigma_1^l...\sigma_k^l = id \quad (*)$, jer su σ_i medjusobno disjunktni. Neka je $x \in \{1, 2, ..., n\}$ u nosacu σ_i. Tada je $(\sigma_1^l...\sigma_k^l)(x) = \sigma_i^l(x) = id(x) = x$, pa zakljucujemo da (*) vazi akko $\sigma_i^l = id$ za $1 \leq l \leq k$ akko $\omega(\sigma_i)|l$ za $1 \leq i \leq k$ akko $NZS(\omega(\sigma_1), ..., \omega(\sigma_k))|l$. Najmanje ovakvo l je $\omega(\pi)$, a to je bas $NZS(\omega(\sigma_1), ..., \omega(\sigma_k))$
Vazi: $(a_1a_2...a_k) = (a_1...a_{l-1}a_l)(a_la_{l+1}...a_k)$ za $1 \leq l \leq k$. Sada vazi: $(a_1a_2...a_k) = (a_1a_2)(a_2a_3...a_k) = (a_1a_2)(a_2a_3)(a_3...a_k) = (a_1a_2)(a_2a_3)...(a_{k-1}a_k)$
Ciklusi duzine 2 su transpozicije. Ovim smo dokazali sledeci stav:

Stav 4.6 *Svaka permutacija iz $\mathbb{S}_n$ moze se zapisati kao proizvod transpozicija.*

Komentar:

a) Zapis iz prethodnog stava nije jedinstven. $(ab)(ab) = id$

b) Ono sto za svaki zapis jeste jedinstveno je parnost broja transpozicija. Ako se permutacija $\pi \in \mathbb{S}_n$ moze zapisati kao proizvod parnog broja transpozicija kazemo da je parna, a u suprotnom kazemo da je neparna.

Skup parnih permutacija oznacavamo sa $\mathbb{A}_n$.

Stav 4.7 *Neka je $n \geq 2$. Tada je $\mathbb{A}_n \leq \mathbb{S}_n$ i vazi $|\mathbb{A}_n| = \frac{|\mathbb{S}_n|}{2}$.*

Komentar: Za $n = 1$ je $\mathbb{A}_1 = \mathbb{S}_n = \{id\}$
Dokaz: Pokazimo prvo da je $\mathbb{A}_n \leq \mathbb{S}_n$. Vazi $id \in \mathbb{A}_n \neq \emptyset$, pa je dovoljno dokazati da za $\sigma, \pi \in \mathbb{A}_n$ vazi $\sigma\pi^{-1} \in \mathbb{A}_n$. $\sigma = \sigma_1...\sigma_{2k}$, $\pi = \pi_1...\pi_{2l}$, gde su σ_i, π_j transpozicije. Tada je: $\sigma\pi^{-1} = \sigma_1...\sigma_{2k}(\pi_1...\pi_{2l})^{-1} = \sigma_1...\sigma_{2k}\pi_{2l}^{-1}...\pi_1^{-1} = \sigma_1...\sigma_{2k}\pi_{2l}...\pi_1$ (vazi $\pi_i^{-1} = \pi_i$) $\rightarrow \sigma\pi^{-1} \in \mathbb{A}_n$.
Za drugi deo je dovoljno dokazati $|\mathbb{A}_n| = |\mathbb{S}_n \backslash \mathbb{A}_n|$. Za ovo je dovoljno dokazati da je $f : \mathbb{A}_n \longrightarrow \mathbb{S}_n \backslash \mathbb{A}_n$ zadato sa $f(\pi) = \tau\pi$, gde je π neka fiksirana neparna permutacija (npr. mozemo uzeti da je τ jedna transpozicija) bijekcija.

1. f je dobro definisana.

   Zelimo da dokazemo da je za svaku parnu permutaciju π permutacija $\tau\pi$ neparna. Ovo radimo kao u dokazuje da je $\mathbb{A}_n \leq \mathbb{S}_n$.

2. f je "1-1"

   Vazi $f(\pi_1) = f(\pi_2) \rightarrow \tau\pi_1 = \tau\pi_2 \rightarrow \pi_1 = \pi_2$

3. f je "na"

   Neka je $\sigma \in \mathbb{S}_n \backslash \mathbb{A}_n$. Tada je $f(\tau^{-1}\sigma) = \tau\tau^{-1}\sigma = \sigma$, a vazi $\tau^{-1}\sigma \in \mathbb{A}_n$ (isto kao $\mathbb{A}_n \leq \mathbb{S}_n$.

Teorema 4.8 *Neka je $\pi \in \mathbb{S}_n$ i $(a_1a_2...a_k) \in \mathbb{S}_n$.*
Tada vazi: $\pi(a_1a_2...a_k)\pi^{-1} = (\pi(a_1)\pi(a_2)...\pi(a_k))$.

Dokaz: Oznacimo sa $\sigma = \pi(a_1a_2...a_k)\pi^{-1}$ i $\tau = (\pi(a_1)...\pi(a_k))$ Neka je $x \in \{1, 2, ..., n\}$.

1. $x \in \{\pi(a_1), ..., \pi(a_k)\}$

   Neka je $x = \pi(a_i)$ za neko $1 \leq i \leq k$. Uzecemo da je $i \neq k$ (za $i = k$ dokaz je slican). Tada je $\sigma(x) = (\pi \circ (a_1...a_k) \circ \pi^{-1})(\pi(a_i))$

   $= \pi((a_1...a_k)(\pi(\pi(a_i)))) = \pi((a_i...a_k)(a_i)) = \pi(a_{i+1})$

   $\tau(x) = \pi(a_{i+1}$

2. $x \notin \{\pi(a_1), .., \pi(a_k)\}$

   Tada je $\sigma(x) = \pi((a_1...a_k)(\pi^{-1}(x))) = \pi(\pi^{-1}(x)) = x$

Teorema 4.9 *(Kejlijeva): Svaka grupa G izomorfna je podgrupi grupe $\mathbb{S}_G$.*

Dokaz: Za $g \in G$ definisemo $Lg : G \longrightarrow G$ sa $Lg(x) = gx$. Dokazimo da je $Lg \in \mathbb{S}_G$ tj da je Lg bijekcija.

1. Lg je "1-1"
   Vaı$Lg(x_1) = Lg(x_2) \to gx_1 = gx_2 / g^{-1} \cdot \bigsqcup \quad \to x_1 = x_2$
2. Lg je "na"
   Neka je $x \in G$. Tada vazi $Lg(g^{-1}x) = gg^{-1}x = x$ pa je Lg "na".

Posmatrajmo $\mathcal{L}(G) = \{Lg | g \in G\}$. Dokazimo da je $\mathcal{L}(G) \leq \mathbb{S}_G$. Vazi $L_e \in \mathcal{L}(G)$, pa $\mathcal{L}(G) \neq \emptyset$. Zato je dovoljno da za $Lg, Lh \in \mathcal{L}(G)$ vazi:
$Lh^{-1}(Lh(x)) = x$ tj $Lh^{-1}(hx) = x$ pa je $Lh^{-1}(x) = Lh^{-1}(x) = Lh^{-1}(hh^{-1}x) = h^{-1}x = Lh^{-1}(x)$
$\to (Lg \circ Lh^{-1})(x) = Lg(Lh^{-1}(x)) = Lg(Lh^{-1}(x)) = Lg(h^{-1}x) = gh^{-1}x = Lgh^{-1}(x)$ pa je $Lg \circ Lh^{-1} = Lgh^{-1} \in \mathcal{L}(G)$
Dakle dovoljno je dokazati da je $G \cong \mathcal{L}(G)$, a za to je dovoljno dokazati da je $F \circ G \longrightarrow \mathcal{L}(G)$ zadato sa $F(g) = Lg$ izomorfizam.

1. F je bijekcija
   (a) F je "na- po definiciji $\mathcal{L}(G)$
   (b) F je "1-1"
   Vazi: $F(g_1) = F(g_2) \to Lg_1 = Lg_2 \to Lg_1(x) = Lg_2(x)$.
   Za svako $x \in G$: $g_1 x = g_2 \to g_1 = g_2$
2. $F(g_1g_2) = F(g_1) \circ F(g_2)$: za $x \in G$ vazi: $(F(g_1) \circ F(g_2))(x) = (Lg_1 \circ Lg_2)(x) = Lg_1(Lg_2(x)) = Lg_1(g_2x) = g_1g_2x = Lg_1g_2(x) = F(g_1g_2)(x)$

4.1 Direktan proizvod grupa

Definicija 4.10 *Neka su $(G_1, *_1), (G_2, *_2), ..., (G_n, *_n)$ grupe. Definisemo direktan proizvod $(P, *)$ svih grupa sa:*

1. $P = G_1 \times G_2 \times ... \times G_n$
2. *za $(g_1, ..., g_n), (h_1, ..., h_n) \in P$ je:* $(g_1, ..., g_n)(h_1, ..., h_n) = (g_1 *_1 h_1, ..., g_n *_n h_n)$

Teorema 4.11 *$(P, *)$ je grupa.*

Dokaz:

I Asocijativnost
Neka je $(g_1...g_n), (h_1...h_n), (l_1...l_n) \in P$. Tada je $((g_1...g_n) * (h_1...h_n)) * (l_1...l_n) = (g_1 *_1 h_1....g_n *_n h_n) * (l_1...l_n) = ((g_1 *_1 h_1) *_1 l_1....(g_n *_n h_n) *_n l_n) = (g_1 *_1 (h_1 *_1 l_1)...g_n *_n (h_n *_n l_n)) = (g_1...g_n) * (h_1 *_1 l_1...h_n *_n l_n) = (g_1...g_n) * ((h_1...h_n) * (l_1...l_n))$

II Neutral $e = (e_1, ..., e_n)$ gde je e_i neutral u $(G_i, *_i)$. Zaista vazi:
$(g_1, ..., g_n) * (e_1, ..., e_n) = (g_1, ..., g_n)$ i slicno za $(e_1, ..., e_n) * (g_1, ..., g_n)$.

III Inverz elementa $(g_1, ..., g_n) \in P$ je $(g_1^{-1}, ..., g_n^{-1})$ gde je g_i^{-1} inverz od g_i u $(G_i, *_i)$

Primer: U $\mathbb{Z}_5 \times \mathbb{Z}_7$ je $(3, 5) + (4, 1) = (3 +_5 4, 5 +_7 1) = (2, 6)$

Tvrdjenje 4.12 *Neka su G i H grupe, i $g \in G, h \in H$. Tada u $G \times H$ vazi $\omega(g,h) = NZS(\omega(g), \omega(h))$.*

Dokaz: Za $k \in \mathbb{N}$ vazi: $(g,h)^k = (e,e)$ akko $(g^k, h^k) = (e,e)$ akko je $g^k = e$ i $h^k = e$ akko $\omega(g)|k$ i $\omega(h)|k$
Akko $NZS(\omega(g), \omega(h))|k \to \omega(g,h) = NZS(\omega(g), \omega(h))$

Primer: U $\mathbb{Z}_5 \times \mathbb{Z}_7$: $\omega(1,1) = NZS(\omega(1), \omega(1)) = NZS(5,7) = 35$

Stav 4.13 *Grupa $\mathbb{Z}_n \times \mathbb{Z}_m$ je ciklicna grupa akko $NZD(n,m) = 1$.*

$\to$ Neka je $\mathbb{Z}_n \times \mathbb{Z}_m =< (a,b) >$ za neke $a \in \mathbb{Z}_n, b \in \mathbb{Z}_m$. Tada je $nm = |\mathbb{Z}_n \times \mathbb{Z}_m| = \omega((a,b)) = NZS(\omega(a), \omega(b)) \leq \omega(a)\omega(b) = \frac{n}{NZD(a,n)} \cdot \frac{m}{NZD(b,m)} \leq nm$

Pa svuda moraju da vaze jednakosti; specijalno $\omega(a) = n, \omega(b) = m$ i $NZS(\omega(a), \omega(b)) = \omega(a)\omega(b)$ tj $nm = NZS(n,m) = \frac{nm}{NZD(n,m)}$ pa je $NZD(n,m) = 1$

$\leftarrow$ Posmatramo $< (1,1) >$. Vazi $< (1,1) > \leq \mathbb{Z}_n \times \mathbb{Z}_m$, kao i $| < (1,1) > | = \omega(1,1) = NZS(\omega(1), \omega(2)) = NZS(n,m) = \frac{nm}{NZD(n,m)} = nm$

pa je $< (1,1) > = \mathbb{Z}_n \times \mathbb{Z}_m$ (jer $|\mathbb{Z}_n \times \mathbb{Z}_m| = nm$)

Komentar: Ako je $NZD(n,m) = 1$ tada je $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$

Neka su $H, K \subseteq G$, gde je G grupa. Tada definisemo $HK = \{hk | h \in H, k \in K\}$

Stav 4.14 *Neka je G grupa i $H, K \leq G$ takve da vazi:*

a) $HK = G$

b) $H \bigcap K = \{e\}$

c) $(\forall h \in H)(\forall k \in K)hk = kh$

Tada vazi $G \cong H \times K$

Dokaz: Dokazujemo da je $F : H \times K \longrightarrow G$ zadato sa
$F(h,k) = hk$ izomorfizam.

1. F je bijekcija.
   (a) F je "na"po uslovu a)
   (b) F je "1-1": vazi $F(h_1,k_1) = F(h_2,k_2) \quad h_2^{-1} \backslash h_1 k_1 = h_2 k_2 / k_1^{-1}$
   $h_2^{-1} h_{1(\in H)} = h_2 k_{1(\in H)}^{-1} = g \quad \to g \in H \bigcup K \to g = e = h_2^{-1} h_1 = k_2 k_1^{-1} \to h_1 = h_2$ i $k_1 = k_1$
2. $F(h_1,k_1)F(h_2,k_2) = F((h_1,k_1)(h_2,k_2))$
   vazi: $F(h_1,k_1)F(h_2,k_2) = h_1k_1 \cdot h_2k_2 =^{v)}$
   $= h_1h_2k_1k_2 = F(h_1h_2, k_1k_2) = F((h_1,k_1)(h_2,k_2))$

4.2 Lagranzova teorema

Definicija 4.15 *Neka je G grupa, $x \in G, H \leq G$. Tada je skup $xH = \{xh | h \in H\}$ levi koset (polozaj) podgrupe H u grupi G. Slicno $Hx = \{hx | h \in H\}$ je desni koset (polozaj) podgrupe H u grupi G.*

Primer: $G = D_4 = \{id, \rho, \rho^2, \rho^3, \sigma, \sigma\rho, \sigma\rho^2, \sigma\rho^3\}$

$H =< \rho >= \{id, \rho, \rho^2, \rho^3\} \quad \sigma H = \{\sigma, \sigma\rho, \sigma\rho^2, \sigma\rho^3\}$

$\sigma\rho H = \{\sigma\rho, \sigma\rho^2, \sigma\rho^3, \sigma\}$

Stav 4.16 *Vazi sledece:*

1. $xH = yH$ *akko* $x^{-1}y \in H$
2. *ako* $xH \neq yH$, *tada je* $xH \bigcap yH = \emptyset$

Dokaz:

1.(=>) Kako je $e \in H$, to je $ye \in yH$ pa kako je $yH = xH$ to je $y \in xH$ Dakle postoji $h \in H$ takvo da je $y = xh \quad / x^{-1} \cdot \bigsqcup$ Sledi $x^{-1}y = h \in H$.

(<=) Dokazi prvo da je $xH \subseteq yH$. Neka je $g \in xH$. Tada postoji $h \in H$ td. $g = yh$ pa je $g = yy^{-1}xh = y(x^{-1}y_{(\in H)}h \in yH)$.
Dokazimo i da je $yH \subseteq xH$. Neka je $g \in H$. Tada postoji $h \in H$ td $g = yh$, pa je $g = xx^{-1}yh \in xH$

2. PPS. Neka je $g \in xH \bigcap yH$. Kako je $g \in xH$, postoji $h \in H$ td. $g = xh$. Slicno, postoji $h' \in H$ td $g = yh'$. Tada je $xh = yh' \quad / x^{-1} \cdot \bigsqcup \cdot h'^{-1}$, pa vazi: $x^{-1}y = hh'^{-1}$, pa je po delu 1) $xH = yH$ sto je kontradikcija.

Komentar: Vazi $x \in xH$. Samim tim, svi razliciti levi koseti podgrupe H u grupi G cine particiju skupa G.

Ovim je dokazano sledece:

Stav 4.17 *Neka je G grupa i* $H \leq G$. *Tada je G disjunktna unija razlicitih levih koseta podgrupe H.*

Definicija 4.18 *Neka je G grupa i* $H \leq G$. *tada skup levih koseta od H u G oznacavamo sa* $G/G = \{xH | x \in G\}$ *i nazivamo kolicnickim skupom.*

Ako je $G \backslash H$ konacan tada za $|G \backslash H|$ kazemo da je indeks podgrupe H u grupi G i oznacamo ga sa $[G : H]$. Ako je $G \backslash H$ beskonacan, kazemo da je H beskonacnog indeksa u G.

Teorema 4.19 *(Langranzova): Neka je G konacna grupa i* $H \leq G$. *Tada vazi:* $|G| = |H| \cdot [G : H]$. *Specijalno, red podgrupe deli red (konacne) grupe.*

Dokaz: Neka su $x_1H, x_2H, ..., x_kH$ svi razliciti levi koseti podgrupe H u G. Tada je $[G : H] = k$. Dokazimo da za svako i, $1 \leq i \leq k$ vazi $|H| = |x_iH|$. Za ovo je dovoljno dokazati da je $f : H \longrightarrow x_iH$ zadato sa $f(h) = x_ih$, bijekcija.

1. f je "na- na osnovu definicije x_iH.
2. f je "1-1- vazi $f(h_1) = f(h_2) \rightarrow x_ih_1 = x_ih_2 / x_i^{-1} \cdot \sqcup \rightarrow h_1 = h_2$

Kako vazi $G = x_1H \sqcup h_2H \sqcup ... \sqcup x_kH$, to je $|G| = |x_1H| + ... + |x_kH| = k \cdot |H|$.
$\sqcup$ je disjunktna unija.

Teorema 4.20 *(posledica) Red svakog elementa konacne grupe deli red te grupe.*

Dokaz: Neka je G konacna grupa i $x \in G$. Kako je $\omega(x) = | < x > |$, a $< x > \leq G$, to $\omega(x)$ deli $|G|$ po Lagranzovoj teoremi.

Teorema 4.21 *(posledica) Svaka grupa prostog reda je ciklicna.*

Dokaz: Neka je p prost broj i G grupa reda p. Tada za svako $x \in G$ vazi $\omega(x)|p$, pa $\omega(x) \in \{1, p\}$. Dakle za svako $x \neq e$ je $\omega(x) = | < x > | = p = |G|$ pa je $G =< x >$.

Komentar: Ako je $|G| = p$ gde je p prost broj, tada je $G \cong \mathbb{Z}_p$.

Teorema 4.22 *(posledica) Ako je G konacna grupa i $x \in G$, tada je $x^{|G|} = e$.*

Dokaz: Kako $\omega(x)|G$, to je $x^{|G|} = e$.

4.3 Ojlerova grupa, funkcija i teorema

$\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$
$\Phi(n) = \{k | 1 \leq k \leq n, \text{NZD}(k, n) = 1\}$ za $n \geq 2$, $\Phi(n) \subseteq \mathbb{Z}_n$.

Stav 4.23 *Za $n \geq 2$ $(\Phi(n), \cdot_n)$ je komutativna grupa.*

Dokaz: $\cdot_n$ je operacija na $\Phi(n)$: Neka su $x, y \in \Phi(n)$. Kako je $\text{NZD}(x, n) = \text{NZD}(y, n) = 1$, postoje $u', v', u", v" \in \mathbb{Z}$ takvi da je $xu' + nv' = 1$, $yu" + nv - 1$. Mnozenjem dobijamo: $(xu'+nv')(xu"+nv") = 1$, tj $xyu'u"+n(xu'v"+yu"v'+nv'v") = 1$. Odavde sledi $\text{NZD}(xy, n) = 1$. Dakle, ako je $xy = nq + (x \cdot_n y) \quad (q \in \mathbb{Z})$, tada iz $\text{NZD}(x \cdot_n y, n) = d$, sledi $d|nq + x \cdot_n y = xy$, pa je $d = 1$. Sledi $x \cdot_n y \in \Phi(n)$.
$\cdot_n$ je asocijativna.
Neutral: $1 \in \Phi(n)$
Dokazimo da za svako $k \in \Phi(n)$ ima iverz, tj da postoji $l \in \Phi(n)$ td. $k \cdot_n l = 1$. Kako je $k \in \Phi(n)$, to postoje $u, v \in \mathbb{Z}$ td. $ku + nv = 1$. Neka je l ostatak pri deljenju i sa n. Tada iz prethodne jednakosti sledi $k \cdot_n l = 1$.
Dokazimo i da je $l \in \Phi(n)$, tj da je $\text{NZD}(l, n) = 1$. Zapisimo $(q' \in \mathbb{Z}) : kl = nq' + (k \cdot_n l) = nq' + 1$, pa ako je $\text{NZD}(l, n) = d$, vazi $d|kl$, $d|n$ te $d|kl - nq' = 1$ tj $d = 1$.
$\cdot_n jekomutativna$

Definicija 4.24 *Grupa $(\Phi(n), \cdot_n)$ je Ojlerova grupa.*
Definisemo $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ sa $\varphi(n) = |\Phi(n)|$

Teorema 4.25 *(Ojlerova teorema) Ako je $n \geq 2$ i $x \in \mathbb{Z}$ td. $NZD(x, n) = 1$, tada je $x^{\varphi(n)} \equiv q(modn)$.*

Dokaz: Neka je $\overline{x}$ ostatak pri deljenju x sa n. Tada je $x^{\varphi(n)} \equiv \overline{x}^{\phi(n)}(\text{mod}n)$, a kako vazi $\text{NZD}(x, n) = 1$, to je $\text{NZD}(\overline{x}, n) = 1$ tj $\overline{x} \in \Phi(n)$. Kako u $\Phi(n)$ vazi $\overline{x}^{|\Phi(n)|} = \overline{x}^{\varphi(n)} = 1$, tvrdjenje sledi.

Teorema 4.26 *(Mala Fermaova teorema) Ako je p prost broj i $x \in \mathbb{Z}$ td. $p \nmid x$, tada je $x^{p-1} \equiv 1(modp)$*

Dokaz:Kako $p \nmid x$, to je $\text{NZD}(x, p) = 1$, a $\Phi(p) = \{1, 2, ..., p-1\}$ pa je $\varphi(p) = p - 1$, te tvrdjenje sledi iz prethodnog.

? Kako odrediti $\varphi(n)$?

1. Za $m, n \in \mathbb{N}$ td $\text{NZD}(m, n) = 1$ vazi $\varphi(m, n) = \varphi(m) \cdot \varphi(n)$
   Dokaz: kasnije

2. Ako je p prost broj i $k \in \mathbb{N}$, tada je $\varphi(p^k) = p^{k-1}(p-1)$.
   Dokaz: Za $x \in \mathbb{Z}$ vazi NZD$(x, p^k) = 1$. Akko x nije deljiv sa p. Sledi $\varphi(p^k) = p^k - \frac{p^k}{p} = p^{k-1}(p-1)$.
   p^k su svi, a $\frac{p^k}{p}$ samo deljivi sa p.
   Dakle ako je $n = p_1^{\alpha_1} \cdot ... \cdot p_k^{\alpha_k}$ gde su p_i razliciti prosti brojevi, vazi:
   $\varphi(n) = \varphi(p_1^{\alpha_1} \cdot ... \cdot p_k^{\alpha_k}) =^{1.} = \varphi(p_1^{\alpha_1} \cdot ... \cdot p_{k-1}^{\alpha_{k-1}}) \cdot \varphi(p_k^{\alpha_k}) = ... = \varphi(p_1^{\alpha_1}) \cdot ... \cdot \varphi(p_k^{\alpha_k}) =^{2.} = p_1^{\alpha_1 - 1}(p_1 - 1) \cdot ... \cdot p_k^{\alpha_k - 1}(p_k - 1)$

Primer: Odrediti ostatak pri deljenju broja $3^{2024} sa 10$.
$3^1 = 3 \quad 3^2 = 9 \quad 3^3 \equiv_{10} 1 \quad 3^5 \equiv_{10} 3...$
$\omega(3) = 4$ u $\Phi(10)$
$3^{2024} = 1$ u Φ_{10}, jer $\omega(3) | 2024$

Teorema 4.27 *(Košijeva) Ako je G konacna grupa i p prost broj koji deli njen red, tada u G postoji element reda p.*

Dokaz: Neka je G grupa reda 6. Tada postoje $x, y \in G$ td $\omega(x) = 3$, $\omega(y) = 2$. Oznacimo: $H =< x >= \{e, x, x^2\}$, $K =< y >= \{e, y\}$. Kako $y \notin H$, to $eH \neq yH \quad (e^{-1}y \notin H)$,pa je $H \bigcap yH = \emptyset$. Dakle $G = H \sqcup yH$ tj. $G = \{e, x, x^2, y, yx, yx^2\}$. Posmatrajmo xy. Vazi $xy \neq e$ (jer $y \neq x^2$), $xy \neq x$ (jer $y \neq e$), $xy \neq x^2$ (jer $y \neq x$), $xy \neq y$ (jer $x \neq e$).

I $xy = yx$: Vazi $KH = H, K \bigcap H = \{e\}$ i za sve $k \in K, h \in H$ vazi $kh = hk$.
$(k \in \{e, y\}, \quad h \in \{e, x, x^2\})$
Sledi: $G \cong K \times H \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$

II $xy = yx^2$: Tada je $G \cong \mathbb{D}_3$ uz izomorfizam $f(y^i x^j = \sigma^i \delta^j$??

4.4 Normalne Podgrupe

Definicija 4.28 *Neka je G grupa i $x, y \in G$. Tada kazemo da je y konjugovan elementu x ako postoji $g \in G$ td $y = gxg^{-1}$.*

Ako na G uvedemo relaciju sa: $x\ y$ akko y konjugovan sa x, tada je relacije ekvivalencije.
Zaista:
Refleksivnost: $x\ x$ jer je $x = exe^{-1}$
Simetricnost: Neka je $x\ y$. Tada postoji $g \in G$ td $y = gxg^{-1}$. Sledi: $x = g^{-1}xg = g^{-1}y(g^{-1})^{-1}$, pa je $y\ x$.
Tranzitivnost: Neka je $x\ y$ i $y\ z$. Tada postoje $g, h \in G$ td. $y = gxg^{-1}$ i $= hyh^{-1}$. Sledi $z = hgxg^{-1}h^{-1} = (hg)x(hg)^{-1}$, pa je $x\ z$.

Klase ekvivalencije u odnosu na su $K_x = \{y | x\ y\} = \{gxg^{-1} | g \in G\}$ i nazivamo ih klasama konjugacije ili konjugvanosti.
Osobine:

1. $x \in K_x$
2. za sve $x, y \in G$ je $K_x = K_y$ ili $K_x \bigcap K_y = \emptyset$
3. $\bigcup_{x \in G} K_x = G$

Definicija 4.29 *Neka je G grupa i $H \leq G$. Tada je H normalna podgrupa od G ako je H unija nekih klasa konjugacije. U tom slucaju pisemo $H \Delta G$*

Komentar: Ako je $x \in H$ i $H \Delta G$, tada je $K_x \subseteq G$.
Komentar: $K_e = \{geg^{-1} | g \in G\}$, tj. $K_e = \{e\}$. Sledi $\{e\} \Delta G$, a vazi i $G \Delta G$.
Primer: $\mathbb{D}_3 = \{id, \rho, \rho^2, \sigma, \sigma\rho, \sigma\rho^2\}$ $H =< \rho >= \{id, \rho, \rho^2\} \leq \mathbb{D}_3$
$K =< \sigma >= \{id, \sigma\} \leq \mathbb{D}_3$
$K_\sigma = \{g\sigma g^{-1} | g \in \mathbb{D}_3\}$, pa $\rho\sigma\rho^{-1} = \sigma\rho^2\rho^{-1} = \sigma\rho \in K_\sigma$, ali $\sigma\rho \notin K$, pa Knije$\delta\mathbb{D}_3$.
Sa druge strane, $H \Delta \mathbb{D}_3$, jer je $H = K_{\text{id}} \bigcup K_\rho$
Komentar: Ako je G komutativna grupa, tada za svako $H \leq G$ vazi $H \Delta G$ (jer je $K_x = \{x\}$).

Stav 4.30 *Neka je $H \leq G$. Tada je sledece ekvivalentno:*

1. $H \Delta G$
2. *za sve* $g \in G$ *je* $gHg^{-1} \subseteq H$
3. *za sve* $g \in G$ *je* $gH = Hg$

Dokaz: $1 \to 2 \to 3 \to 1$

$1 \to 2$: Neka je $y \in gHg^{-1}$, Tada je $y = ghg^{-1}$ za neko $h \in H$. Kako je $ghg^{-1} \in K_h$, to iz $K_h \subseteq H$ sledi $ghg^{-1} \in H$.

$2 \to 3$: $\subseteq$: Neka je $y \in gH$. Tada postoji $h \in H$ takvo da je $y = gh$. Sledi $y = ghg^{-1}g \in HG$

$\supseteq$: Neka je $y \in HG$. Tada postoji $h \in H$ takvo da je $y = hg$. Sledi: $y = gg^{-1}hg = gg^{-1}h(g^{-1})^{-1} \in gH$

$3 \to 1$: Dovoljno je dokazati da za svako $x \in H$ vazi $K_x \subseteq H$, jer je tada $H = \bigcup_{x \in H} K_x$.

Neka je $y \in K_x$. Tada je $y = gxg^{-1}$ za neko $g \in G$. Kako je $gx \in gH = Hg$, to postoji $x_1 \in H$ td $gx = x_1 g$. Sledi $y = gxg^{-1} = x_1 gg^{-1} = x_1 \in H$.

Stav 4.31 *Svaka grupa indeksa 2 je normalna.*

Dokaz: Neka je G grupa i $H \leq G$ td $[G : H] = 2$. Tada postoji $a \in G$ td. su $eH = H$ i aH levi koseti od H i G. Kako $H \neq aH$, to $a \notin H$. Da bismo dokazali da je $H \Delta G$, po prethodnom stavu dovoljno je dokazati da je $gH = Hg$ za svako $g \in G$. Pre svega, kako $H \neq Ha$ (jer $a \notin H$), pa je $G = H \sqcup aH = H \sqcup Ha$ i sledi $aH = Ha$. Razmotrimo sledeca dva slucaja:

1.$g \in H$: Tada je $gH = H$ i slicno $Hg = H$, pa je $gH = Hg$.

1.$g \notin H$: Tada $gH \neq H$, pa je $gH = aH$. Slicno $Hg \neq H$, pa je $Hg = Ha$. Sledi: $gH = aH = Ha = Hg$.

Primer: $\mathbb{D}_n, |\mathbb{D}_n| = 2n, | < \rho > | = n$, pa je $[\mathbb{D}_n, < \rho >] =^{\text{Lagranz}} = \frac{|\mathbb{D}_n|}{|<\rho>|} = 2$ i sledi $< \rho > \Delta \mathbb{D}_n$.
Primer: $\mathbb{A}_n \Delta \mathbb{S}_n$ za $n \geq 2$ jer $[\mathbb{S}_n : \mathbb{A}_n] = 2$
Primer: U $\mathbb{D}_3$ je $[\mathbb{D}_n :< \sigma >] = \frac{|\mathbb{D}_n|}{<\sigma>} = \frac{6}{2} = 3$, a $< \sigma >$nije$\Delta \mathbb{D}_3$.

4.5 Kolicnicke grupe

* Neka je G grupa i $X, Y \subseteq G$. Tada definisemo $X \cdot Y = \{xy | x \in X, y \in Y\}$
Podsetnik: Za $H \leq G$ je $G \backslash H = \{aH | a \in G\}$

Stav 4.32 *Neka je G grupa i $H \Delta G$. Tada je $(G/H, \cdot)$ grupa u odnosu na prethodno definisano mnozenje podskupova od G.*

Dokaz:

1. $\cdot$ je operacija
   Neka su $a, b \in G$. Zelimo da dokazemo da je $aH \cdot bH$ takodje levi koset od H. Zato dokazujemo da vazi: $aH \cdot bH = (ab)H$.
   Vazi: $aH \cdot bH = \{ah \cdot bk | h, k \in H\} = \{ahb | h \in H\} \cdot \{k | k \in H\} = (a(Hb)) \cdot H =^{H \Delta G} = (a(bH)) \cdot H = \{abh | h \in H\} \cdot \{k | k \in H\} = \{abhk | h, k \in H\} = (ab) \cdot (H \cdot H)$
   Dakle, dovolljno je dokazati da je $H \cdot H = H$. Ovo sledi iz:
   1 $H \cdot H \subseteq H$, jer je $H \leq G$
   2 $H \subseteq H \cdot H$ jer je $H = He \subseteq H \cdot H$
2. $\cdot$ je asocijativna.
   $((aH) \cdot (bH)) \cdot (cH) = (ab)H \cdot cH = ((ab)c)H = (a(bc))H = aH(bc)H = (aH)((bH)(cH))$
3. Neutral je $eH = H$ jer je $aH \cdot eH = (ae)H = aH$ i $eH \cdot aH = (ea)H = aH$
4. Inverz od aH je $a^{-1}H$ jer je $aH \cdot a^{-1}H = (aa^{-1})H = eH$ i $a^{-1}H \cdot aH = (a^{-1}a)H = eH$

Primer: $G = \mathbb{Z}$, $H =< 3 >= \{0, 3, -3, 6, -6...\} = 3\mathbb{Z}$
Odredimo $G/H = \mathbb{Z}/3\mathbb{Z} \quad (\cong \mathbb{Z}_3)$
$0 + 3\mathbb{Z} = 3\mathbb{Z} = \{0, 3, -3, 6, -6...\}$
$1 + 3\mathbb{Z} = \{1, 4, -2, 7, -5...\}$
$2 + 3\mathbb{Z} = \{2, 5, -1, 8, -4...\}$
$(1 + 3\mathbb{Z}) + (2 + 3\mathbb{Z}) = (1 + 2) + 3\mathbb{Z} = 3 + 3\mathbb{Z} = 0 + 3\mathbb{Z}$

4.6 Homomorfizmi grupa

Definicija 4.33 *Neka su $(G, \cdot)$ i $(H, *)$ grupe. Tada je $g : G \longrightarrow H$ homomorfizam grupa ako za sve $x, y \in G$ vazi $f(x \cdot y) = f(x) * f(y)$*

izomorfizam = bijekcija + homomorfizam

Komentar: Uz dokaz kao kod izomorfizma, dokazuje se da za homomorfizam $f : G \longrightarrow H$ vazi: $f(e) = e$ i $f(x^{-1}) = f(x)^{-1}$

Definicija 4.34 *Neka je $f : G \longrightarrow H$ homorfizam grupa. Jezgro ovog homomorfizma je $Ker(f) = \{a \in G | f(a) = e\}$, a slika je $Im(f) = \{f(a) | a \in G\}$*

Stav 4.35 *Jezgro homomorfizma $f : G \longrightarrow H$ je normalna podgrupa od G.*

Dokaz:
$\text{Ker}(f) \leq G$. Važi $e \in \text{Ker}(f)$, jer je $f(e) = e$, pa $\text{Ker}(f) \neq \emptyset$. Zato je dovoljno dokazati da za $x, y \in \text{Ker}(f)$ važi $xz^{-1} \in \text{Ker}(f)$. Za $x, y \in \text{Ker}(f)$ važi: $f(x) = f(y) = e$, pa je $f(xy^{-1}) = f(x)f(y^{-1}) = f(x)f(y)^{-1} = e$ tj $xy^{-1} \in \text{Ker}(f)$.
$\text{Ker}(f) \lhd G$: Dovoljno je dokazati da za svako $g \in G$ važi $g\text{Ker}(f)g^{-1} \subseteq \text{Ker}(f)$.
Neka je $y \in g\text{Ker}(f)g^{-1}$. Tada postoji $x \in \text{Ker}(f)$ td $y = gxg^{-1}$ i $f(x) = e$. Sledi:
$f(y) = f(gxg^{-1}) = f(g)f(x)f(g)^{-1} = f(g)f(g^{-1}) = e$, tj $y \in \text{Ker}(f)$.

Stav 4.36 *Homomorfizam grupa $f : G \longrightarrow H$ je "1-1"akko je $Ker(f) = \{e\}$*

Dokaz:

=> Neka je $x \in \text{Ker}(f)$. Tada je $f(x) = e = f(e)$, pa kako je f "1-1šledi $x = e$

¡= Iz $f(x) = f(y) \quad /f(y)^{-1}$ sledi $e = f(x)f(y)^{-1} = f(xy^{-1})$, pa kako je $\text{Ker}(f) = \{e\}$, važi $xy^{-1} = e$ tj $x = y$

Stav 4.37 *Slika homomorfizma grupa $f : G \longrightarrow H$ je podgrupa od H.*

Dokaz: Važi $f(e) \in \text{Im}(f)$, pa $\text{Im}(f) \neq \emptyset$. Zato je dovoljno dokazati da za $x, y \in \text{Im}(f)$ važi $xy^{-1} \in \text{Im}(f)$. Iz $x, y \in \text{Im}(f)$ sledi da postoje $a, b \in G$ td $x = f(a), y = f(b)$ pa je $xy^{-1} = f(a)f(b)^{-1} = f(ab^{-1}) \in \text{Im}(f)$.

Teorema 4.38 ***teorema o izomorfizmu za grupa:*** *Neka je $f : G \longrightarrow H$ homomorfizam grupa. Tada je $\tilde{f} : G/Ker(f) \longrightarrow Im(f)$, zadato sa $\tilde{f}(aKer(f)) = f(a)$ je izomorfizam grupe. Specijalno, $G\backslash Ker(f) \cong Im(f)$.*

Dokaz:

1. $\tilde{f}$ je dobro definisano i "1-1":
   Dovoljno je dokazati da iz $a\text{Ker}(f) = b\text{Ker}(f)$ sledi $f(a) = f(b)$
   Zaista, $a\text{Ker}(f) = b\text{Ker}(f)$ akko $a^{-1}b \in \text{Ker}(f)$ akko $f(a^{-1}b) = e$ akko $f(a) = f(b)$
2. $\tilde{f}$ je "na":
   po definiciji $\text{Im}(f)$.
3. $\tilde{f}$ je homomorfizam:
   Važi $\tilde{f}(a\text{Ker}(f) \cdot b\text{Ker}(f)) = \tilde{f}((ab)\text{Ker}(f)) = f(ab) = f(a)f(b) = \tilde{f}(a\text{Ker}(f))\tilde{f}(b\text{Ker}(f))$

4.7 Dejstva grupa

Definicija 4.39 *Neka je G grupa i X neprazan skup. Pod dejstvom grupe G na skupu X podrazumevamo svako preslikavanje $\theta : G \times X \longrightarrow X$ takvo da važi:*

1. $\theta(e, x) = x, \quad \forall x \in X$
2. $\theta(g, \theta(h, x)) = \theta(gh, x), \quad \forall g, h \in G, \forall x \in X$

Definicija 4.40 *Neka je G grupa i X neprazan skup. Pod dejstvom grupe G na skupu X podrazumevamo svaki homomorfizam $\varphi : G \longrightarrow \mathbb{S}_X$.*

Dokažimo da svako dejstvo iz prethodne definicije zadaje jedno dejstvo iz ove i obrnuto.

$\Rightarrow$ Neka je $\theta : G \times X \longrightarrow X$ dejstvo. Definišimo $\varphi : G \longrightarrow \mathbb{S}_X$ sa $\varphi(g)(x) = \theta(g, x)$ i dokažimo da je dejstvo od prethodne definicije.

(a) φ je dobro definisano tj. $\varphi(g)$ je bijekcija:

i. $\varphi(g)$ je "1-1":
Neka je $\varphi(g)(x) = \varphi(g)(y)$ tj $\theta(g, x) = \theta(g, y)$, Tada je $\theta(g^{-1}, \theta(g, x)) = \theta(g^{-1}, \theta(g, y))$, pa kako je $\theta(g^{-1}, \theta(g, x)) =^{2)}= \theta(g^{-1}gx) = \theta(e, x) =^{1)}= x$ i slično $\theta(g^{-1}, \theta(g, y)) = y$ to je $x = y$

ii. $\varphi(g)$ je "na":
Neka je $y \in X$. Tada je $\varphi(g)(\theta(g^{-1}, y)) = \theta(g, \theta(g^{-1}, y)) =^{2)}= \theta(gg^{-1}, y) = \theta(e, y) =^{1)}= y$

(b) φ je homomorfizam:
Važi $\varphi(gh)(x) = \theta(gh, x) =^{2)}= \theta(g, \theta(h, x)) = \varphi(g)(\theta(h, x)) = \varphi(g)(\varphi(h)(x)) = (\varphi(g) \circ \varphi(g))(x)$

¡=: Neka je $\varphi : G \longrightarrow \mathbb{S}_X$ homomorfizam. Definišimo $\theta : G \times X \longrightarrow X$ sa $\theta(g, x) := \varphi(g)(x)$ Dokažimo da θ zadovoljava 1), 2) iz definicije prethodne.

(a) $\theta(e, x) = \theta(e)(x) =^*= \mathrm{id}(x) = x$ $\quad (*) : \varphi$ je homomorfizam =¿ neutral se slika u neutral: $\varphi(e) = \mathrm{id}$

(b) $\theta(gh, x) = \varphi(gh)(x) = (\varphi(g) \circ \varphi(h))(x) = \varphi(g)(\varphi(h)(x)) = \varphi(g)(\theta(h, x)) = \theta(g, \theta(h, x))$

Komentar: Umesto $\theta(g, x)$ iz prethodne definicije skraćeno pišemo $g \cdot x$. Tada se 1) i 2) zapisuju:
1) $e \cdot x = x$
2) $g \cdot (h \cdot x) = (gh) \cdot x$
Primer: $X = \mathbb{C}$ i $G = \mathbb{C}_n = \{1, \epsilon, \epsilon^2, ..., \epsilon^{n-1}\}$ $\quad \epsilon = \cos\frac{2\pi}{n} + i \sin\frac{2pi}{n}$
Tada G dejstvuje na X sa: $g \cdot x = gx$
Primer: $X = \{1, 2, .., n\}, G = \mathbb{S}_n$ Tada G dejstvuje na X sa $\pi \cdot x = \pi(x)$
Primer: Neka je G grupa. Tada G dejstvuje na G sa: $g \cdot x = gxg^{-1}$ (konjugacija)
Ovo je zaista dejstvo, jer:
1) $e \cdot x = exe^{-1} = x$
2) $g \cdot (h \cdot x) = g \cdot (hxh^{-1}) = ghxh^{-1}g^{-1} = ghx(gh^{-1}) = (gh) \cdot x$

Definicija 4.41 *Neka grupa G dejstvuje na skupu X. Orbita elementa $x \in X$ u oznaci $\Omega(x)$ definiše se sa: $\Omega(x) = \{g \cdot x | g \in G\}$, a stabilizator u oznaci $\sum_x$, $\sum_x = \{g \in G | g \cdot x = x\}$.*

Komentar: $\Omega(x) \subseteq X$, $\quad \sum_x \subseteq G$. Takođe, $x \in \Omega(x)$, a $e \in \sum_x$.
Na X uvodimo relaciju $\sim$ sa $x \sim y$ akko $y = g \cdot x$ za neko $g \in G$. Dokažimo da je $\sim$ relacija ekvivalencije.

(R) $x \sim x$ jer je $x = e \cdot x$

(S) Neka je $x \sim y$. Tada postoji $g \in G$ td. $y = g \cdot x \quad g^{-1} \cdot \sqcup$. Sledi $g^{-1} \cdot y = g^{-1}(g \cdot x) =^{2)}= (g^{-1}g) \cdot x = e \cdot x =^{1)}= x$ pa je $y \sim x$

(T) Neka je $x \sim y$ i $y \sim z$. Tada postoje $g, h \in G$ td. $y = g \cdot x$, a $= h \cdot y$.Sledi $z = h \cdot y = h \cdot (g \cdot x) =^{2)}= (hg) \cdot x$, pa je $x \sim z$

Klasa ekvivalencije elementa x u odnosu na $\sim$ je: $\{y | x \sim y\} = \Omega(x)$ pa važi:
1) $x \in \Omega(x)$
2) za sve $x, y \in X$ je $\Omega(x) \cap \Omega(y) = \emptyset$ ili $\Omega(x) = \Omega(y)$
3) $\bigcup_{x \in X} \Omega(x) = X$

Stav 4.42 *Neka je X neprazan skup i G grupa koja dejstvuje na X. Tada za svako $x \in X$ važi $\sum_x \leq G$ i postoji bijekcija između $\Omega(x)$ i $G/\sum_x$*

Dokaz: Dokažimo prvo da je $\sum_x \leq G$. Kako je $e \in \sum_x$ to $\sum_x \neq \emptyset$, pa je dovoljno dokazati da za $g, h \in \sum_x$ važi $gh^{-1} \in \sum_x$. Važi $g \cdot x = x$ i $h \cdot x = x \quad / h^{-1}$. Tada je $h^{-1} \cdot x = h^{-1} \cdot (h \cdot x) =^{2)} = (h^{-1}h) \cdot x = e \cdot x =^{1)} = x$, pa je $(gh^{-1}) \cdot x =^{2)} = g \cdot (h^{-1} \cdot x) = g \cdot x = x$ pa je zaista $gh^{-1} \in \sum_x$ Dokažimo i drugi deo. Dovoljno je dokayati da je $F : G/\sum_x \longrightarrow \Omega(x)$ zadato sa $F(g\sum_x) = g \cdot x$ bjekcija.

1. F je dobro definisano.
   Važi $g\sum_x = h\sum_x$ akko $g^{-1}h \in \sum_x$ akko $(g^{-1}h) \cdot x = x \quad / g \cdot \sqcup \Rightarrow^* g \cdot x = g \cdot ((g^{-1}h) \cdot x) =^{2)} = (gg^{-1}h) \cdot x = h \cdot x$ akko $F(g\sum_x) = F(h\sum_x)$
2. F je bijekcija.
   (a) F je "na"
   po definiciji $\Omega(x)$
   (b) F je "1-1"
   Dovoljno je dokazati da na mestu * važi $\Leftarrow$ tj da iz $g \cdot x = h \cdot x \quad / g^{-1} \cdot \sqcup$ sledi $(g^{-1}h) \cdot x = x$. Zaista, važi $g^{-1}(g \cdot x) = g^{-1} \cdot (h \cdot x) =^{2)} = (g^{-1}h) \cdot x$
   $g^{-1}(g \cdot x) = (g^{-1}g) \cdot x = e \cdot x =^{1)} = x$

Teorema 4.43 ***(Posledica)*** *Ako konačna grupa G dejstvuje na skupu X, tada za svako $x \in X$ važi $|G| = |\Omega(x)| \cdot |\sum_x|$.*

Dokaz: Po prethodnom stavu je $|\Omega(x)| = |G/\sum_x| = [G : \sum_x] =$ Lagranž $= \frac{|G|}{|\sum_x|}$

Teorema 4.44 ***(Košijeva)*** *Neka je G konačna grupa i p prost broj koji deli $|G|$. Tada postoji element reda p.*

Dokaz: Neka je $X = \{(g_0, g_1, ..., g_{p-1}) | g \in G, g_0 \cdot g_1 \cdot ... \cdot g_{p-1} = e\}$. Tada važi: $|X| = |G|^{p-1}$, jer je g_{p-1} jedinstveno određen izborom $g_0, ..., g_{p-2} \quad$ jer $g_{p-1} = (g_0 \cdot ... \cdot p_{p-2})^{-1}$. Specijalno p deli $|X|$. Primetimo da je $\omega(g) = p$ akko $g \neq e$ i $g^p = e \quad$ (jer tada $\omega(g)|p$ i $\omega(p) \neq 1$) akko $g \neq e$ i $(g, g, ..., g) \in X$. Definišimo dejstvo grupe $\mathbb{Z}_p$ na X sa: $n \cdot (g_0, ..., g_{p-1}) = (g_n, g_{(n+1)\%p}, ..., g_{(n+(p-1))\%p})$. Ovo jeste dejstvo jer je $(g_n, g_{n+1}, ..., g_{p-1}, g_0, .., g_{n-1}) \in X$ (iz $g_0...g_{n-1}g_n...g_{p-1} = e$ sledi $g_0...g_{n-1} = (g_n...g_{p-1})^{-1}$ pa je $g_n...g_{p-1}g_0...g_{n-1} = e$). Pravila 1) i 2) se lako proveravaju. Neka su $\Omega_1, ..., \Omega_k$ sve različite orbite pri ovom dejstvu. Tada važi: $|\Omega_1| + ... + |\Omega_k| = |X|$, a za svako Ω_i važi $|\Omega_i|$ deli $|\mathbb{Z}_p| = p$ pa $|\Omega_i| \in \{1, p\}$. Primetimo da je $\Omega(e, e, ..., e) = \{(e, e, ..., e)\}$ pa kako je $|X|$ deljiv sa p. to postoji barem p brojeva $1 \leq i \leq k$ takvih da $|\Omega_i| = 1$ i $\Omega_i \neq \{(e, e, , ..., e)\}$,, a tada je $\Omega_i = \{(g, g, ..., g)\}$ za neko $g \neq e$. Tada je i $\omega(g) = p$, čime je dokaz završen.

Neka je G grupa koja dejstvuje na x. Tada za $g \in G$ definišemo $x^g = \{x \in X | g \cdot x = x\}$ što je fiksni skup elemenata $g \in G$.

Teorema 4.45 *(**Bernsajdova lema**) Neka konačna grupa G dejstvuje na konačnom skupu X. Tada važi:*
$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|$ *gde je sa X/G označen skup orbita pri voom dejstvu.*

Dokaz: Posmatrajmo $S = \{(g,x) \in G \times X | g \cdot x = x\}$. Tada važi:
$S = \bigsqcup_{g \in G} \{g\} \times X^g = \bigsqcup_{x \in X} \sum_x \times \{x\}$, pa je $|S| = \sum_{g \in G} |X^g| = \sum_{x \in X} |\sum_x|$.
Neka su $\Omega_1, \Omega_2, ..., \Omega_k$ sve različito zadate pri ovom dejstvu. Tada je:
$\sum_{x \in X} |\sum_x| = \sum_{i=1}^{k} \sum_{x \in \Omega_i} |\sum_x| =^{*} = \sum_{i=1}^{k} \sum_{x \in \Omega_i} \frac{|G|}{\Omega(x)} =^{**} = \sum_{i=1}^{k} \sum_{x \in \Omega_i} \frac{|G|}{|\Omega_i|}$
$= \sum_{i=1}^{k} |\Omega_i| \frac{|G|}{|\Omega_i|} = \sum_{i=1}^{k} |G| = k|G| = |X/G| \cdot |G|$

* $|G| = |\Omega(x)| \cdot |\sum_x|$

** $x \in \Omega_i \Rightarrow \Omega_i = \Omega(x)$

Primer: Okrugla torta je podeljena na 4 jednaka parčeta. Na svako parče želimo da postavimo svećicu jedne od 3 boje. Na koliko različitih načina to možemo da uradimo?
$X-$ skup ukrašavanja "fiksirane"torte: $|X| = 3^4$. Na X dejstvuje grupa $\{\mathrm{id}, \rho, \rho^2, \rho^3\}$, gde je ρ rotacija za 90° oko centra. Ono što nas zanima jeste broj različitih orbita pri ovom dejstvu.
$|X^\rho| = 3 \quad |X^{\rho^2}| = 3^2 \quad |X^{\rho^3}| = 3 \quad |X^{\mathrm{id}}| = 3^4$

Stav 4.46 *Neka G dejstvuje na X. Ako su $g, h \in G$ konjugovani element, tada postoji bijekcija između X^g i X^h.*

4.8 Konačno generisane Abelove grupa

Podsetnik: G je generisana skupom S ako važi $G =< S >$, tj. $G =< S >= \{x_1 x_2 ... x_n | n \in \mathbb{N}, x \in S \cup S^{-1}\}$
Notacija: Kod Abelovih grupa operaciju označavamo sa $+$ (a ne sa $\cdot$). Tada n-ti stepen elementa a označavamo sa na (a ne sa a^n).
Inverz elementa a označavamo sa $-a$, a neutral sa 0.
*Neka je A Abelova grupa generisana konačnim skupom $S = \{a_1, a_2, ..., a_k\}$. Tada je:
$A =< S >= \{n_1 a_1 + n_2 a_2 + ... + n_k a_k | n_i \in \mathbb{Z}\}$. Primetimo da je $< a_i >= \{n_i a_i | n_i \in \mathbb{Z}\}$, pa je:
$A =< S >=< a_1 > + < a_2 > + ... + < a_k >$.
*Neka je A Abelova grupa i $A_1, A_2, ..., A_k \leq A$. Tada je A suma ovih podgrupa ako važi:
$A = A_1 + A_2 + ... + A_k$. Ova suma je direktna ako se svaki element $a \in A$ može zapisati na jedinstven način $a_1 + a_2 + ... + a_k = a$, gde je $a_i \in A_i$ za $1 \leq i \leq k$.

Stav 4.47 *Abelova grupa A je direktna suma svojih podgrupa $A_1, A_2, ..., A_K$ akko $(A_1 + ... + A_{i-1}) \cap A_i = \{0\}$ za $2 \leq i \leq k$.*

Dokaz:

$\Rightarrow$ Neka je $a \in (A_1 + ... + A_{i-1}) \cap A_i$. Tada je $a = a_1 + a_2 + ... + a_{i-1} + 0 + 0 + ... + 0 = 0 + 0 + ... + a_i + ... + 0 \quad a_t \in A_t$.
Zbog jedinstvenosti zapisa, važi:
$a_1 = 0, a_2 = 0, ..., a_{i-1} = 0, 0 = a_i$ pa je $a = 0$.

$\Leftarrow$ Neka za $a \in A$ važi: $a = a_1 + a_2 + ... + a_k = a_1' + ... + a_k'$ gde je $a_i, a_i' \in A_i$. Tada je:
$a_1 - a_1' + a_2 - a_2' + ... + a_{k-1} + a_{k-1}' = b$, pa je $b \in (A_1 + ... + A_{k-1}) \cap A_k$, te iz uslova sledi $b = 0$, tj. $a_k = a_k'$. Nastavljajući na isti način (indukcijom) dobijamo:
$a_{k-1} = a_{k-1}' \quad a_{k-2} = a_{k-2}' \quad ... \quad a_1 = a_1'$.

Vratimo se na slučaj $A =< S >$, gde je $S =< a_1, a_2, ..., a_k >$. Tada je $A =< a_1 > + < a_2 > + ... + < a_k >$, a ova suma je direktna suma iz $n_1a_1 + ... + n_ka_k = 0$ sledi $n_1a_1 = 0 \quad ... \quad n_ka_k = 0$.
Ako je A direktna suma svojih podgrupa $A_1, ..., A_k$ tada pišemo:
$A = A_1 \oplus ... \oplus A_k$.

Stav 4.48 *Neka je A Abelova grupa koja je direktna suma svojih podgrupa $A_1, ..., A_k$. Tada je: $A \cong A_1 \times ... \times A_k$.*

Dokaz: Dovoljno je dokazati da je $F = A_1 \times ... \times A_k \to A_1 \oplus ... \oplus A_k$, zadato sa $F(a_1, ..., a_k) = a_1 + ... + a_k$ izomorfizam.

1. F je izomorfizam:
   Važi
$$\begin{aligned} F((a_1, ..., a_k) + (a'_1, ..., a'_k)) &= F(a_1 + a'_1, ..., a_k + a'_k) \\ &= a_1 + a'_1 + ... + a_k + a'_k \\ &= a_1 + a_2 + ... + a_k + a'_1 + ... + a'_k \\ &= F(a_1, ..., a_k) + F(a'_1, ..., a'_k) \end{aligned}$$
2. F je bijekcija:
   (a) F je "na"po definiciji $A_1 + ... + A_k$
   (b) F je "1-1"važi $F(a_1, ..., a_k) = F(a'_1, ..., a'_k)$ akko $a_1 + ... + a_k = a'_1 + ... + a'_k = a$, pa iz jedinstvenosti zapisa a sledi $a_i = a'_i, 1 \leq i \leq k$.

Teorema 4.49 *Neka je A Abelova grupa i $x_1, x_2, ..., x_k \in A$. Tada je $< x_1, x_2, ..., x_k >=< x_1 + n_2x_2 + ... + n_kx_k, x_2, ..., x_k >$ za proizvoljne $n_2, ..., n_k \in \mathbb{Z}$.*

Dokaz: Označimo $B =< x_1, ..., x_k >$ i $C =< x_1 + n_2x_2 + ... + n_kx_k, x_2, ..., x_k >$. Kako je B (odnosno C) minimalna podgrupa od A koja sadrži skup $\{x_1, ..., x_k\}$ (odnosno $\{x_1 + n_2x_2 + ... + n_kx_k, x_2, ..., x_k\}$), pa je dovoljno dokazati da je $\{x_1, , ..., x_k\} \subseteq C$ i $\{x_1 + n_2x_2 + ... + n_kx_k, x_2, ..., x_k\} \subseteq B$, tj. $x_1 \in C$ i $x_1 + n_2x_2 + ... + n_kx_k \in B$. Drugo sledi direktno, a prvo iz $x_1 = 1 \cdot (x_1 + n_2x_2 + ... + n_kx_k) + (-n_2)x_2 + ... + (-n_k)x_k$.

4.9 Normalna forma konačno generisane Abelove grupe

Teorema 4.50 *Neka je A konačno generisana Abelova grupa. Tada postoje $k, l \geq 0$ i $d_1, d_2, ..., d_k \geq 2$ td. $d_1|d_2, d_2|d_3, ..., d_{k-1}|d_k$ i $A \cong \mathbb{Z}_{d_1} \times ... \times \mathbb{Z}_{d_k} \times \mathbb{Z}_{d_k}$. Uz to, takvi k, l i d_i su jedinstveni.*

Komentar: Ako je $k = 0$, tada je $A \cong \mathbb{Z}_l$, a ako je $l = 0$, tada je $A \cong \mathbb{Z}_{d_1} \times ... \times \mathbb{Z}_{d_k}$.
Primer:

1. $\mathbb{Z}_8 \times \mathbb{Z}_{20} = \mathbb{Z}_8 \times \mathbb{Z}_{4\cdot 5} \cong \mathbb{Z}_8 \times \mathbb{Z}_4 \times \mathbb{Z}_5 \cong \mathbb{Z}_4 \times \mathbb{Z}_8 \times \mathbb{Z}_5 \cong \mathbb{Z}_4 \times \mathbb{Z}_{40}$
2. $\mathbb{Z}_{20} \times \mathbb{Z}_{30} \times \mathbb{Z}_{50} = \mathbb{Z}_{2^2\cdot 5} \times \mathbb{Z}_{2\cdot 5\cdot 3} \times \mathbb{Z}_{2\cdot 5^2} \cong \mathbb{Z}_{2^2} \times \mathbb{Z}_5 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_2 \times \mathbb{Z}_{5^2} \cong \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_{2^2} \times \mathbb{Z}_3 \times \mathbb{Z}_{5^2} \cong \mathbb{Z}_{10} \times \mathbb{Z}_{10} \times \mathbb{Z}_{300}$

4.10 Generatori i relacije

Primeri:

1. $\mathbb{D}_n =< \rho, \sigma >$, a relacije su $\rho^n = \mathrm{id}, \quad \sigma^2 = \mathrm{id}, \quad \rho\sigma = \sigma\rho^{n-1}$

2. $\mathbb{Z} =< 1 >$, nema relacije (slobodna grupa - ne moćemo dobiti 0 sabiranjem jedinica)

3. $\mathbb{Z}_n =< 1 >$, a relacija je $n1 = 0$

Neka je A Abelova grupa generisana skupom $\{x_1, ..., x_k\}$ koji zadovoljava sistem relacija:
$a_{11}x_1 + a_{12}x_2 + ... + a_{1k}x_k = 0$
$a_{21}x_1 + a_{22}x_2 + ... + a_{2k}x_k = 0$
$\vdots$
$a_{m1}x_1 + a_{m2}x_2 + ... + a_{mk}x_k = 0$, gde su $a_{ij} \in \mathbb{Z}$ (*)
Primer: Preslikavanje $\rho_n : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ zadato sa $\rho_n(k) =$ ostatak pri deljenju k sa n je homomorfizam, pa po teoremi o izomorfizmu važi: $\mathbb{Z}/\text{Ker}\rho_n \cong \text{Im}\rho_n$. Kako je $\text{Im}\rho_n = \mathbb{Z}_n$, a $\text{Ker}\rho_n = n\mathbb{Z} =< n >$, to je $\mathbb{Z}/ < n > \cong \mathbb{Z}_n$
*Grupa razmatrana na početku poglavlja zadata generatorima i relacijama je izomorfna sa $\mathbb{Z}^k/ < (a_{11}, ..., a_{1k}), ..., (a_{m1}, .., a_{mk}) >$.
Generatoru x_i odgovara $(0, 0, ...0, 1, 0, ..., 0) + < (a_{11}, ..., a_{1k}), ..., (a_{m1}, .., a_{mk}) >$. Jedinica je na i-tom poziciji.
*Sistem relacija * pridružujemo matrici:

$$\begin{bmatrix} a_{11} & a_{12} & ... & a_{1k} \\ a_{21} & a_{22} & ... & a_{2k} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & ... & a_{mk} \end{bmatrix} = M_{m,k}(\mathbb{Z})$$

Naravno, u svakoj matrici iz $M_{m,k}(\mathbb{Z})$ mozemo pridruziti jedan sistem relacija.
Primetimo da ako na matricu primenimo sledece operacije, odgovarajuca grupa se ne menja:

1. $V_i \longleftrightarrow V_j$ (zamena mesta i-te i j-te)

2. $V_i \longrightarrow -V_i$

3. $V_i \longrightarrow V_i + \alpha V_j, \quad i \neq j, \quad \alpha \in \mathbb{Z}$

Slicno, grupa se ne menja ni kada iste operacije primenimo na kolone (tacnije, dobijamo grupu izomorfnu polaznoj).

1. $K_i \longleftrightarrow K_j$ (zamena mesta i-te i j-te kolone -zamena x_i i x_j - koordinate)

2. $K_i \longrightarrow -K_i$ zamena generatora x_i sa $-x_i$.

3. $K_i \longrightarrow K_i + \alpha K_j$ za $i \neq j, \alpha \in \mathbb{Z}$ - dobijamo sledeći sistem relacija:
   $a_{11}x_1 + \cdots + (a_{1i} + \alpha a_{1j})x_i + \cdots + a_{1j}(x_j - \alpha x_i) + \cdots + a_{1k}x_k = 0$
   $\cdots$
   $a_{m1}x_1 + \cdots + (a_{mi} + \alpha a_{mj})x_i + \cdots + a_{mj}(x_j - \alpha x_i) + \cdots + a_{mk}x_k = 0$
   Grupa se ne menja jer je dovoljno generator x_j zameniti generatorom $x_j - \alpha x_i$ (što ne menja grupu po *)

Abelova grupa generisana sa $\{x_1, \ldots, x_k\}$ i sistemom relacija:
$d_1x_1 = 0$
$\ldots d_lx_l = 0$ za $l \leq k$
Tada je $A \cong \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_l} \times \mathbb{Z}^{k-l}$

Teorema 4.51 *Nea je $M \subset \mathbb{M}_{m,k}(\mathbb{Z})$. Tada se matrica M pomoću operacija nad kolonama i vrstama koje smo prethodno naveli može svesti na matricu oblika:*

$$\begin{bmatrix} d_1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & d_2 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & d_l & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{bmatrix}$$

za neko $l \leq k$ i $d_1, \dots, d_l \in \mathbb{N}$ tj $d_1 | d_2, d_2 | d_3, \dots, d_{l-1} | d_l$

Primer: $k = 3, l = 4$

$$\begin{bmatrix} 6 & 4 & -8 \\ 4 & -12 & 6 \\ 10 & 6 & -8 \\ -8 & 12 & 14 \end{bmatrix} \sim \begin{bmatrix} 2 & 0 & 0 \\ 0 & 4 & 10 \\ 0 & 26 & 12 \\ 0 & 60 & -34 \end{bmatrix} \sim \dots$$

5 Komutativni prteni sa jedinicom

Definicija 5.1 *Algebarska struktura $(A, +, \cdot)$ je komutativi prsten sa jedinicom ako su $+$ i $\cdot$ binarne operacije za koje važi:*

1. *$(A, +)$ je Abelova grupa*
2. *$\cdot$ je asocijativna i komutativna*
3. *postoji neutral za $\cdot$*
4. *$(\forall x, y, z \in A) x \cdot (y + z) = (x \cdot y) + (x \cdot z)$*

Notacija: Neutral za $\cdot$ oznacavamo sa 1 (ili 1_A ako postoji mogućnost zabune), a neutrali za $+$ sa 0 (ili 0_A). Inverz u odnosu na sabiranje elementa a označavamo sa $-a$ i pišemo $a - b$ umesto $a + (-b)$. Da bismo pojednostavili zapis, uzimamo da $\cdot$ ima prednost u odnosu na $+$ pa umesto $(x \cdot y) + (x \cdot z)$ pišemo $x \cdot z + x \cdot z$

Primeri:

1. $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$ kpj
2. $(\mathbb{Z}, +, \cdot)$ kpj
3. $(\mathbb{Z}, +_n, \cdot_n)$ kpj
4. $(\mathbb{M}_n(\mathbb{R}), +, \cdot)$ je prsten sa jedinicom

Tvrdjenje 5.2 *Neka je A kpj i $a \in A$. Tada važi:*

1. $0 \cdot a = 0$
2. $-a = (-1) \cdot a$
3. $(-a) \cdot b = -(a \cdot b) \quad (b \in A)$

Dokaz:

1. Važi: $0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a \quad / -(0 \cdot a)$, pa sledi da je $0 = 0 \cdot a$
2. Sledi iz 3)
3. Važi: $0 =^{1)} = 0 \cdot b = (a + (-a)) \cdot b = a \cdot b + (-a) \cdot b$ pa iz jedinstvenosti inverza za $+$ sledi da je $-(a \cdot b) = (-a) \cdot b$

Komentar: Pod inverzom ćemo uvek podrazumevati inverz u odnosu na $\cdot$

Definicija 5.3 *Neka je A kpj. Tada skup svih elemenata z A koji imaju inverz označavamo sa:* $\bigcup(A) = \{a \in A | (\exists b \in A) a \cdot b = 1\}$

Inverz elementa (ako postoji) x označavamo sa x^{-1}

Tvrdjenje 5.4 *Neka je A kpj. Tada je $(\bigcup(A), \cdot)$ grupa.*

Dokaz: Kako je $1 \in \bigcup(A)$ (jer $1 \cdot 1 = 1$) to $\bigcup(A) \neq \emptyset$ pa je dovoljno dokazati da za $x, y \in \bigcup(A)$ važi $xy^{-1} \in \bigcup(A)$.
Iz $x, y \in \bigcup(A)$ sledi da postoje $z, t \in A$ td. $xz = 1$ i $yt = 1$. Tada je $t = y^{-1}$, pa važi:
$xy^{-1}yz = xtyz = xz = 1$ tj $xy^{-1} \in \bigcup(A)$

Primeri:

1. $\bigcup(\mathbb{Q}) = \mathbb{Q}\backslash\{0\} \quad \bigcup(\mathbb{R}) = \mathbb{R}\backslash\{0\} \quad \bigcup(\mathbb{C}) = \mathbb{C}\backslash\{0\}$
2. $\bigcup(\mathbb{Z}) = \{1, -1\}$
3. $\bigcup(\mathbb{Z}_n) = \Phi(n)$

Definicija 5.5 *KPJ A je polje ako važi* $\bigcup(A) = A\backslash\{0\}$

Primeri: $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$ su polja, a $(\mathbb{Z}, +, \cdot)$ nije polje.
$(\mathbb{Z}_n, +_n, \cdot_n)$ je polje akko je n prost broj.
Primer: Neka je A kpj. Tada je $A[x]$ (prsten polinoma sa koeficijentim u A): $(A[x], +, \cdot)$ kpj.
Za $p \in A[x]$ sa deg(p) označavamo stepen polinoma p. Tada: $deg(pg) \leq deg(p) + deg(q)$.
U $\mathbb{Z}_6[x]$ ne mora da važi jednakost, jer je npr $(2x+1)(3x+1) = 5x + 1$.

Definicija 5.6 *Neka je A kpj. Za element $a \in A\backslash\{0\}$ kažemo da je pravi delitelj nule ako postoji $b \in A\backslash\{0\}$ td $a \cdot b = 0$.*
Skup svih delitelja nula označavamo sa $Z(A)$ (to su pravi delitelji nule u 0)

Definicija 5.7 *Neka je A kpj. Za element $a \in A$ kažemo da je regularan ako za sve $x, y \in A$ važi: $ax = ay \Rightarrow x = y$. SKup svih regularnih elemenata označavamo sa $R(A)$.*

Primeri:

1. $Z(\mathbb{Q}) = \{0\}, \quad R(\mathbb{Q}) = \mathbb{Q}\backslash\{0\}, \quad \bigcup(\mathbb{Q}) = \mathbb{Q}\backslash\{0\}$ i slično za $\mathbb{R}$ i $\mathbb{C}$.
2. $Z(\mathbb{Z}) = \{0\}, \quad R(\mathbb{Z}) = \mathbb{Z}\backslash\{0\}, \quad \bigcup(\mathbb{Z}) = \{1, -1\}$
3. $Z(\mathbb{Z}_n) = \mathbb{Z}_n\backslash\Phi(n), \quad R(\mathbb{Z}_n) = \Phi(n), \quad \bigcup(\mathbb{Z}_n) = \Phi(n)$

Tvrdjenje 5.8 *Neka je A kpj. Tada je $\bigcup(A) \subseteq R(A)$.*

Dokaz: Neka je $a \in \bigcup(a)$. Tada postoji $b \in A$. Zato važi:
$ax = ay \Rightarrow bax = bay \Rightarrow x = y$, pa je $a \in R(A)$.

Tvrdjenje 5.9 *Neka je A kpj. Tada je element $a \in A$ regularan akko nije delitelj nule.*

Dokaz:

$(\Rightarrow)$: Neka je $a \cdot b = 0$. Dvooljno je dokazati da mora biti $b = 0$.
Kako je $a \cdot b = 0 = a \cdot 0$, iz $a \in R(A)$ sledi $b = 0$.

$(\Leftarrow)$: Neka je $ax = ay$. Sledi $ax - ay = a(x - y) = 0$, pa kako a nije delitelj nule to je $x - y = 0$, tj. $x = y$. Sledi $a \in R(A)$.

Stav 5.10 *Neka je A konačan kpj. Tada važi: $\bigcup(A) = R(A)$*

Dokaz: Neka je $a \in R(A)$.Dovoljno je dokazati da je $a \in \bigcup(A)$ tj da postoji $b \in A$ td. $a \cdot b = 1$.
Posmatrajmo skup $\{a \cdot b | b \in R(A)\}$. Kako je $a \in R(A)$, to su elementi $a \cdot b$ različiti, pa važi $|\{a \cdot b | b \in R(A)\}| = |R(A)|$.
Zato je dovoljno dokazati da $\{a \cdot b | b \in R(A)\} \subseteq R(A)$, jer tada $1 \in R(A) = \{a \cdot b | b \in R(A)\}$.
Drugim rečima, dovoljno je dokazati da za $a, b \in R(A)$ važi $a \cdot b \in R(A)$.
Zaista za $x, y \in A$ važi $abx = aby \Rightarrow bx = by \Rightarrow x = y$.

Definicija 5.11 *Neka je A kpj. Tada je A oblast celih (ili domen) ako važi: $R(A) = A\backslash\{0\}$.*

A polje $\Rightarrow$ A domen.
A konačan i domen $\Rightarrow$ A polje.

5.1 Potprsten i ideali

Definicija 5.12 *Neka su $(A, +, \cdot)$ i $(B, +', \cdot')$ kpj. Tada je $(B, +, \cdot)$ potprsten od $(A, +, \cdot)$ ako važi $B \subseteq A$, $1_B = 1_A$ i za sve $x, y \in B$ važi $x + y = x +' y$ i $x \cdot y = x \cdot' y$.*

Primer: $(\mathbb{Z}, +, \cdot)$ je potprsten od $(\mathbb{Q}, +, \cdot)$ a $(\mathbb{Q}, +, \cdot)$ je potprsten od $(\mathbb{C}, +, \cdot)$.

Definicija 5.13 *Neka je A kpj. Za $I \subseteq A$, $I \neq \emptyset$, kažemo da je ideal u A ako važi:*

1. $(\forall x, y \in I) \quad x + y \in I$
2. $(\forall a \in A)(\forall x \in I) \quad a \cdot x \in I$

Pišemo $I \lhd A$.

Primer: Neka je A kpj i $x \in A$. Tada je glavni ideal generisan sa x. $\quad < x >:= \{ax | a \in A\}$.

Tvrdjenje 5.14 $< x > \lhd A$.

Dokaz: izvodimo po definiciji

1. Neka su $u, v \in < x >$. Tada je $u = ax, v = bx$, pa je $u + v = ax + bx = (a + b)x \in < x >$
2. Neka je $a \in A$ i $u \in < x >$. Tada je $u = bx$, pa je $au = abx \in < x >$

Komentar: Neka je $I \lhd A$, Tada za I važi $0 \cdot x + 0 \in I$, kao i $(-1) \cdot x = -x \in I$, pa je $(I, +) \leq (A, +)$

Stav 5.15 *Svaki ideal u* $\mathbb{Z}$ *je glavni.*

Dokaz: Neka je $I \lhd \mathbb{Z}$. Tada je $(I, +) \leq (\mathbb{Z}, +)$ pa kako je $(\mathbb{Z}, +)$ ciklična, to je i $(I, +)$ ciklična, pa je $I =< n >$
Slično važi za $(\mathbb{Z}, +_n, \cdot_n)$ uz isti dokaz.

Stav 5.16 *Neka je K polje i* $I \lhd K$. *Tada je* $I = \{0\}$ *ili* $I = K$ *(trivijalni ideali)*

Dokaz: Dovoljno je pokazati ako postoji $a \in I \backslash \{0\}$ da je tada $I = K$. Neka je $x \in K$. Tada kako je $a \in K \backslash \{0\}$ postoji $a^{-1} \in K$ a samim tim $xa^{-1}a = x \in I$

Definicija 5.17 *Neka je A kpj i* $I, J \lhd A$. *Tada definišemo:*

1. $I + J = \{x + y | x \in I, y \in J\}$
2. $I \cdot J = \{x_1 y_1 + \cdots + x_n y_n | n \in \mathbb{N}, x_i \in I, y_i \in J\}$

Stav 5.18 *Neka je A kpj i* $I, J \lhd A$. *Tada su* $I \cap J, I + J, I \cdot J$ *ideali u A.*

Dokaz:

1. Neka su $x, y \in I \cap J$. Tada je $x, y \in I$ i $x, y \in J$, pa je $x + y \in I, x + y \in J$ (jer $I, J \lhd A$) tj. $x + y \in I \cap J$.
   Neka je $x \in A$ i $x \in A \cap J$. Tada je $x \in I, x \in J$ pa je $ax \in I$ i $ax \in J$ (jer $I, J \lhd A$) tj $ax \in I \cap J$.
2. Neka su $x, y \in I + J$. Tada je $x = u_1 + v_1, \quad y = u_2 + v_2$, za neke $u_1, u_2 \in I, \quad v_1, v_2 \in J$. Sledi
   $x + y = u_1 + v_1 + u_2 + v_2 = u_1 + u_2 + v_1 + v_2$ Kako je $u_1 + u_2 \in I, \quad v_1 + v_2 \in J$ sledi da je $u_1 + u_2 + v_1 + v_2 \in I + J$.
   Neka je $a \in A, x \in I + J$. Tada je $x = u + v$ za neke $u \in I, v \in J$, pa je $ax = a(u + v) = au + av \in I + J$ jer je $au \in I$ i $av \in J$.
3. Neka su $x, y \in I \cdot J$. Tada je $x = u_1 v_1 + \cdots + u_n v_n \quad y = w_1 t_1 + \cdots + w_m t_m$ za neke $u_i \in I, v_i \in J, w_j \in I, t_j \in J$
   Sledi $x + y = x = u_1 v_1 + \cdots + u_n v_n + w_1 t_1 + \cdots + w_m t_m \in I \cdot J$
   Neka je $a \in A$ i $x \in I \cdot J$. Tadaje $x = u_1 v_1 + \cdots + u_n v_n$ za neke $u_i \in I$, $v_i \in J$.
   Sledi: $ax = au_1 v_1 + \cdots + au_n v_n \in I \cdot J$.

Primer: Neka su $m, n \in \mathbb{Z}$.

$$< n > \cap < m > =< \text{NZS}(n, m) >$$

$$< n > + < m > = \{kn + lm | k, l \in \mathbb{Z}\} =< \text{NZD}(n, m) >$$

$$< n > \cdot < m > =< nm >$$

Stav 5.19 *Neka je K polje. Tada je svaki ideal u $K[x]$ glavni.*

Slika dokaza:
U prstenu $K[x]$ važi lema o količniku i ostatku, tj za sve $f, g \in K[x], g \neq 0$ postoje $q, r \in K[x]$ td. $f = qg + r$ i deg $r <$ deg g. Dokaz u zadatku I. Neka je sada $I \lhd K[x]$, $I \neq \{0\}$. Uzmimo $g \in I \backslash \{0\}$ td je deg g najmanje moguće. Želimo da dokažemo da je $I =< g >$. Za ovo je dovoljno dokazati da za svako $f \in I$ važi $g|f$. Neka je $f \in I$. Tadda je $f = gq + r$ za neke $q, r \in K[x]$ td deg $r <$ deg g. Važi $r + f - gq < inI$ pa je $r + 0$ tj $g|f$.

Komentar: U $\mathbb{Z}[x]$ ne važi lema o količniku i ostatku; npr za $f = x^2, g = 2x$:
$x^2 = 2x \cdot \square + \square$ Ne može!

Stav 5.20 *U $\mathbb{Z}[x]$ postoje ideali koji nisu glavni.*

Dokaz: Dokažimo da ideal $I =< 2 > + < x >$ nije glavni. Važi: $I = \{a_n x^n + \cdots + a_1 x + 2a_0 | a_0, a_1, \ldots, a_n \in \mathbb{Z}\}$.
Dokažimo da I nije glavni. PP: $I =< f >$.
Kako je $2 \in I$ to $f|2$ pa je $f \in \{-1, 1, -2, 2\}$. Važi $f \notin \{-1, 1\}$ jer je u suprotnom $< f >= \mathbb{Z}[x] \neq I$. ledi $f \in \{2, -2\}$. Međutim $x \in I$, a $2 \nmid z$.

5.2 Homomorfizmi KPJ

Definicija 5.21 *Neka su $(A, +, \cdot)$ i $(B, +', \cdot')$ kpj. Funkcija $f : A \longrightarrow B$ je homomorfizam kpj ako za sve $x, y \in A$ važi:*

1. $f(x + y) = f(x) +' f(y)$
2. $f(x \cdot y) = f(x) \cdot' f(y)$
3. $f(1_A) = 1_B$

Primer: Neka je $\rho_n : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ zadato sa $\rho_n(k) =$ ostatak pri deljenju k sa n. Tada je ρ_n homomorfizam kpj.

Definicija 5.22 *Neka je $f : A \longrightarrow B$ homomorfizam kpj. Jezgro ovog homomorfizma je $Ker(f) = \{a \in A | f(a) = 0_B\}$, a lika je $Im(f) = \{f(a) | a \in A\}$*

Stav 5.23 *Neka je $f : A \longrightarrow B$ homomorfizam kpj. Tada važi:*

1. *$Ker(f) \lhd A$*
2. *ako je $J \lhd B$, tada je $f^{-1}[J] \lhd A$*
3. *ako je $I \lhd A$ i f je "na", tada je $f[I] \lhd B$*

Podsetnik: $f^1[S] = \{x \in A | f(x) \in S\}$
Dokaz: Važi Ker$(f) = f^{-1}[\{0\}]$ pa kako je $\{0_B\} \lhd B$ to 1 sledi iz 2

2: Neka su $x, y \in f^{-1}[J]$. Tada je $f(x), f(y) \in J$, $f(x) + f(y) \in J$ jer je $J \lhd B$ pa je $f(x) + f(y) = f(x + y)$ tj $x + y \in f^{-1}[J]$.
Neka je $a \in A$ i $x \in f^{-1}[J]$. Tada je $f(ax) = f(a) \cdot f(x) \in J$ (jer je $J \lhd B$), pe je $ax \in f^{-1}[J]$.

3: Neka su $x, y \in f(I)$. Tada je $x = f(a_1), y = f(a_2)$ za neke $a_1, a_2 \in I$.
Sledi: $x + y = f(a_1) + f(a_2) = f(a_2 + a_2) \in f(I)$.
Neka je $b \in B$ i $x \in f(I)$. Tada je $x = f(a)$ za neko $a \in I$, kao i $b = f(a')$ za neko $a' \in A$ (jer je f "na"), pa je $bx = f(a') \cdot f(a) = f(a'a) \in f(I)$.

5.3 Količnički prsten

Definicija 5.24 *Neka je A kpj i $I \lhd A$. Tada na A uvodimo relaciju $\equiv (mod\ I)$ sa $a \equiv b (mod\ I)$ akko $a - b \in I$*

Komentar: U $\mathbb{Z}$ je $I =< n >$. Tada $a \equiv b (\text{mod } < n >)$ akko $a - b \in < n >$ akko n deli $a - b$.

Stav 5.25 *$\equiv (mod\ I)$ je relacija ekvivalencije*

Dokaz:

(R): $a \equiv a (\text{mod } I)$ jer je $a - a = 0 \in I$

(S): Neka je $a \equiv b (\text{mod } I)$. Tada je $a - b \in I$ pa je $(-1)(a - b) = b - a \in I$ i sledi $b \equiv a (\text{mod } I)$

(T): Neka je $a \equiv b (\text{mod } I)$, $b \equiv (\text{mod } I)$. Tada je $a - b, b - c \in I$ pa je $a - b + b - c = a - c \in I$ i sledi $a \equiv c (\text{mod } I)$.

Tvrdjenje 5.26 *$\equiv (mod\ I)$ se slaže sa $+$ i $\cdot$*

Dokaz:

+: Dokazujemo da iz $a_1 \equiv b_1 (\text{mod } I)$ i $a_2 \equiv b_2 (\text{mod } I)$ sledi $a_1 + a_2 \equiv b_1 + b_2 (\text{mod } I)$.
Zaista iz ova dva sledi $a_1 - b_1 \in I$ i $a_2 - b_2 \in I$ pa $a_1 - b_1 + a_2 - b_2 = (a_1 + a_2) - (b_1 + b_2)$ tj $a_1 + a_2 \equiv b_1 + b_2 (\text{mod } I)$

$\cdot$: Ako je $a_1 \equiv b_1 (\text{mod } I)$ i $a_2 \equiv b_2 (\text{mod } I)$ tada je $a_1 - b_1, a_2 - b_2 \in I$ pa je $a_1 a_2 - b_1 b_2 = a_2(a_1 - b_1) + b_1(a_2 - b_2) \in I$ i sledi $a_1 a_2 \equiv b_1 b_2 (\text{mod } I)$

* Klase ekvivalencije u odnosu na $\equiv (\text{mod } I)$ su $\{b | b \equiv a (\text{mod } I)\} = \{b | b - a \in I\} = a + I$ što je tačno levi koset podgrupe I u A

* Količnički skup je $A/I = \{a + I | a \in A\}$. Na A/I možemo uvesti operacije $+$ i $\cdot$ sa:

$$(a + I) + (b + I) := (a + b) + I$$

$$(a+I)\cdot(b+I) := (ab)+I$$

Ove operacije su dobro definisane, jer ako je $a+I=a'+I$ i $b+I=b'+I$, tada je $a\equiv a'(\text{mod } I)$ i $b\equiv b'(\text{mod } I)$ pa je $a+b\equiv a'+b'(\text{mod } I)$ i $ab\equiv a'b'(\text{mod } I)$ i sledi $(a+b)+I=(a'+b')+I$ i $(ab)+I=(a'b')+I$.

Tvrdjenje 5.27 *$(A/I,+,\cdot)$ je kpj. (dokaz sami, jedinica 1+I)*

Teorema 5.28 ***(o izomorfizmu za KPJ:*** *Neka je $f: A\longrightarrow B$ homomorfizam KPJ. Tada je $\tilde{f}: A/Ker(f)\longrightarrow Im(f)$, zadato sa $\tilde{f}(a+Ker(f))=f(a)$ izomorfizam KPJ. Specijalno, $A/Ker(f)\cong Im(f)$.*

Dokaz:
$\tilde{f}$ je dobro definisano i "1-1"
Važi:

$$\begin{array}{lllll} & \text{akko} & a\equiv b(\text{mod Ker}(f)) & \text{akko} & f(a)-f(b)=0 \\ a+\text{Ker}(f)=b+\text{Ker}(f) & \text{akko} & f(a-b)=0 & \text{akko} & f(a)-f(b)=0 \\ & \text{akko} & f(a)=f(b) & \text{akko} & \tilde{f}(a+\text{Ker}(f))=\tilde{f}(b+\text{Ker}(f)) \end{array}$$

$\tilde{f}$ je "na"
Po definiciji $\text{Im}(f)$ **$\tilde{f}$ je homomorfizam**
Važi:

$$\tilde{f}((a+\text{Ker}(f))\cdot(b+\text{Ker}(f))=\tilde{f}(ab+\text{Ker}(f))=f(ab)=f(a)\cdot f(b) \quad (1)$$
$$=\tilde{f}(a+\text{Ker}(f))\cdot\tilde{f}(b+\text{Ker}(f)) \quad (2)$$

Takođe: $\tilde{f}(1+\text{Ker}(f))=f(1)=1$

Primer: Za $\rho_n:\mathbb{Z}\longrightarrow\mathbb{Z}_n:\quad \text{Ker}\rho_n=n\mathbb{Z},\quad \text{Im}\rho_n=\mathbb{Z}_n$, pa je $\mathbb{Z}/n\mathbb{Z}\cong\mathbb{Z}_n$

5.4 Direktan proizvod prstena

Definicija 5.29 *Neka su $(A_1,+^1,\cdot^1),\ldots,(A_n,+^n,\cdot^n)$ kpj. Tada je njihov direktan proizvod kpj $(A,+,\cdot)$, gde je $A=A_1\times\cdots\times A_n$, a operacije $+$ i $\cdot$ definišemo sa:*

$$(a_1,\ldots,a_n)+(b_1,b_2,\ldots,b_n)=(a_1+^1b_1,\ldots,a_n+^nb_n)$$
$$(a_1,\ldots,a_n)\cdot(b_1,b_2,\ldots,b_n)=(a_1\cdot^1b_1,\ldots,a_n\cdot^nb_n)$$

Dokaz: dokazujemo da je $(A,+,\cdot)$ KPJ. (veci deo za vezbu) Nula:$(0,\ldots,0)$ Jedinica: $(1,\ldots,1)$ Proverimo distributivnost. Neka su $x,y,z\in A$. Tada je $x=(a_1,\ldots,a_n), y=(b_1,\ldots,b_n), z=(c_1,\ldots,c_n)$ za neke $a_i,b_i,c_i\in A_i$ i važi:

$$\begin{aligned} x\cdot(y+z)&=(a_1,\ldots,a_n)\cdot((b_1,\ldots,b_n)+(c_1,\ldots,c_n)) \\ &=(a_1,\ldots,a_n)\cdot(b_1+^1c_1,\ldots,b_n+^nc_n) \\ &=(a_1\cdot^1(b_1+^1c_1),\ldots,a_n\cdot^n(b_n+^nc_n) \\ &\text{distributivnost u } A_1,\ldots,A_n \\ &=(a_1\cdot^1b_1+^1a_1\cdot^1c_1,\ldots,a_n\cdot^nb_n+^na_n\cdot^nc_n) \\ &=(a_1\cdot^1b_1,\ldots,a_n\cdot^nb_n)+(a_1\cdot^1c_1,\ldots,a_n\cdot^nc_n) \\ &=x\cdot y+x\cdot z \end{aligned}$$

Stav 5.30 *(KTO) Neka su $m_1, \ldots, m_n$ u parovima uzajamno prosti prirodni brojevi. Tada važi:* $\mathbb{Z}/(m_1 \cdot m_2 \cdot \ldots \cdot m_n)\mathbb{Z} \cong \mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_n\mathbb{Z}$

Dokaz: Koristimo teoremu o izomorfizmu za KPJ. Posmatrajmo preslikavanje $f : \mathbb{Z} \longrightarrow \mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_n\mathbb{Z}$, zadato sa $f(k) = (k + m_1\mathbb{Z}, \ldots, k + m_n\mathbb{Z})$. Tada je f homomorfizam. Zaista $f(k+l) = (k+l+m_1\mathbb{Z}, \ldots, k+l+m_n\mathbb{Z}) = (k+m_1\mathbb{Z}+l+m_1\mathbb{Z}, \ldots, k+m_n\mathbb{Z}+l+m_n\mathbb{Z}) = (k + m_1\mathbb{Z}, \ldots, k + m_n\mathbb{Z}) + (l + m_1\mathbb{Z}, \ldots, l + m_n\mathbb{Z}) = f(k) + f(l)$
Slično za $\cdot$. Dalje, $\mathrm{Ker}(f) = \{k \in \mathbb{Z} | f(k) = 0\} = \{k \in \mathbb{Z} | (k+m_1\mathbb{Z}, \ldots, k+m_n\mathbb{Z}) = (0+m_1\mathbb{Z}, \ldots, 0+m_n\mathbb{Z})\} = \{k \in \mathbb{Z} | k \in m_1\mathbb{Z}, \ldots, k \in m_n\mathbb{Z}\} = \{k \in \mathbb{Z} | m_1, \ldots, m_n delek\} = (m_1 \cdot \ldots \cdot m_n)\mathbb{Z}$
Dakle $\mathbb{Z}/(m_1 \cdot m_n)\mathbb{Z} = \mathbb{Z}/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$. Kako je $\mathbb{Z}/(m_1 \cdot \ldots \cdot m_n)\mathbb{Z} \cong \mathbb{Z}_{m_1 \cdot \ldots \cdot m_n}$ to je $|\mathbb{Z}/(m_1 \cdot \ldots \cdot m_n)\mathbb{Z}| = m_1 \cdot \ldots \cdot m_n$ pa i $|\mathrm{Im}(f)| = m_1 \cdot \ldots \cdot m_n$. Sa druge strane, $|\mathbb{Z}/m_1\mathbb{Z} \times \ldots \times \mathbb{Z}/m_n\mathbb{Z}| = m_1 \cdot \ldots \cdot m_n$, pa je f "na"tj. $\mathrm{Im}(f) = \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_n\mathbb{Z}$.

Komentar: Ovo je u vezi sa $\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m$ akko $\mathrm{NZD}(m, n) = 1$ za grupe.

Teorema 5.31 *(KTO) Neka su $m_1, \ldots, m_n$ uzajamno prosti brojevi u parovima i $x_1, \ldots, x_n \in \mathbb{Z}$. Tada postoji ceo broj x td. $x \equiv x_1 (mod\ m_1), \ldots, x \equiv x_n (mod\ m_n)$. Uz to ako i $x' \in \mathbb{Z}$ zadovoljava ove kongruencije, važi:*
$x \equiv x' (mod m_1 \cdot \ldots \cdot m_n)$.

Dokaz: Primetimo da je $x \equiv x_1 (\mathrm{mod}\ m_i)$ ekvivalentno sa $x + m_i\mathbb{Z} = x_1 + m_i\mathbb{Z}$ pa je sistem kongruencija ekvivalentan sa $f(x) = (x_1 + m_1\mathbb{Z}, \ldots, x_n + m_n\mathbb{Z})$ gde je f iz prethodnog stava. Ovakvo x postoji jer je f "na". Takođe ako i x' zadovoljava ove kongruencije važi $f(x) = f(x')$ tj $f(x - x') = 0$ Dakle tada $x - x' \in \mathrm{Ker}\ f = (m_1 \cdot \ldots \cdot m_n)\mathbb{Z}$ t $x \equiv x' (\mathrm{mod}\ m_1 \cdot \ldots \cdot m_n)$.

Tvrdjenje 5.32 *$\varphi(mn) = \varpi(m) \cdot \varphi(n)$ za $NZD(m, n) = 1$*

Tvrdjenje 5.33 *Neka su A, A', B, B' kpj tj. $A \cong A'$ i $B \cong B'$. Tada je $A \times B \cong A' \times B'$.*

Skica dokaza: Neka su $f : A \longrightarrow A'$ i $g : B \longrightarrow B'$ izomorfizmi kpj. Tada je $F : A \times B \longrightarrow A' \times B'$ zadato sa $F(a, b) = (f(a), g(b))$ izomorfizam. Za vezbu - po koordinatama.

Stav 5.34 *Ako su kpj A i B izomorfni, tada su i grupe $\cup(A)$ i $\cup(B)$ izomorfne.*

Dokaz: Neka je $f : A \longrightarrow B$ izomorfizam kpj. Dovoljno je dokazati da je $g : \cup(A) \longrightarrow \cup(B)$ zadato sa $g(x) := f(x)$ izomorfizam.

g je dobro definisano:
Dovoljno je proveriti da za $x \in \cup(A)$ važi $f(x) \in \cup(B)$.
Ovo sledi iz $f(x^{-1}) = f(x)^{-1}$, pa je $f(x) \in \cup(B)$.

g je homomorfizam:
Ovo važi jer je $g(x \cdot y) = f(x \cdot y) = f(x) \cdot f(y) = g(x) \cdot g(y)$

g je bijekcija:

g je "1-1":
jer je f 1-1

g je "na":
Neka je $y \in \cup(B)$. Kako je f "na"to postoji $x \in A$ td $f(x) = y$. Dovoljno je dokazati da je $x \in \cup(A)$ jer je tada $f(x) = g(x) = y$. Posmatrajmo y^{-1}. Tada postoji $x' \in A$ td $f(x') = y^{-1}$ i važi $1 = yy^{-1} = f(x) \cdot f(x') = f(xx')$, a takođe $1 = f(1)$ pa je $1 = xx'$ tj $x' = x^{-1}$ (jer je f "1-1")

Stav 5.35 *Neka su $A_1, A_2, \ldots, A_n$ kpj. Tada važi:* $\cup(A_1 \times ... \times A_n) = \cup(A_1) \times ... \times \cup(A_n)$.

Dokaz: Važi $(a_1, a_2, ..., a_n) \in \cup(A_1 \times ... \times A_n)$ akko postoji $(b_1, ..., b_n) \in A_1 \times ... \times A_n$ td. $(a_1, ..., a_n) \cdot (b_1, ..., b_n) = (1, ..., 1)$ akko postoje $b_i \in A_i$ td. $a_i \cdot b_i = 1$ za $1 \leq i \leq n$ akko $a_i \in \cup(A_i)$ za $1 \leq i \leq n$ akko $(a_1, ..., a_n) \in \cup(A_1) \times ... \times \cup(A_n)$.

Teorema 5.36 *Neka su $m_1, ..., m_n$ u parovima uzajamno prosti prirodni brojevi. Tada važi:* $\mathbb{Z}_{m_1 \cdot ... \cdot m_n} \cong \mathbb{Z}_{m_1} \times ... \times \mathbb{Z}_{m_n}$, *kao i* $\Phi(m_1 \cdot ... \cdot m_n) \cong \Phi(m_1) \times ... \times \Phi(m_n)$
Specijalno $\varphi(m_1 \cdot ... \cdot m_n) = \varphi(m_1) \cdot ... \cdot \varphi(m_n)$.

Dokaz: Koristimo da je $\mathbb{Z}/k\mathbb{Z} \cong \mathbb{Z}_k$, za $k \in \mathbb{N}$. Po stavu 3.34 iz knjige važi: $\mathbb{Z}/(m_1 \cdot ... \cdot m_n)\mathbb{Z} \cong \mathbb{Z}/m_1\mathbb{Z} \times ... \times \mathbb{Z}/m_n\mathbb{Z}$ pa prvi izomorfizam sledi iz pretposlednjeg tvrđenja. Za drugi izomorfizam, koristimo da je $Phi(k) = \cup(\mathbb{Z}_k)$ za $k \in \mathbb{Z}$, pa on sledi iz stava 3.36, 3.37 iz knjige. Konačno, poslednja jednakost sledi upoređivanjem broja elemenata.

5.5 Konačne podgrupe multiplikativne grupe polja

Neka je F polje. Tada je $\cup(F) = F\backslash\{0\}$.
Primer: $F = \mathbb{Z}_p : (\cup(\mathbb{Z}_p), \cdot_p) = (\mathbb{Z}_p, \backslash\{0\}, \cdot_p)$ $\quad p$ prost

Tvrdjenje 5.37 *Neka je F polje i $f \in F[x]\backslash\{0\}$ stepena n. Tada f ma najviše n nula u F.*

Dokaz: Indukcijom po n

Baza: n = 1 Tada je $f = ax + b$, pa je njegova jedina nula $x = -ba^{-1}$.

IK: Neka je f stepena n i neka je $\alpha \in F$ nula od f. Po lemi o količniku i ostatku, postoji $q \in F[x]$ i $c \in F : f = (x - \alpha)q + c$. Zamenom α dobijamo:
$0 = f(\alpha) = (\alpha - \alpha)q(\alpha) + c$ pa je $c = 0$ tj. $f = (x - \alpha)q$. Sledi da je q stepena n-1, pa po IH najviše ima n-1 nula. Primetimo da ako je $\beta \neq \alpha$ nula od f, tada važi:
$0 = f(\beta) = (\beta - \alpha)q(\beta)$, pa je β nula od q. Odavde sledi tvrđenje.

Teorema 5.38 *Neka je G konačna podgrupa multiplikativne grupe $(\cup(F), \cdot)$ polja F. Tada je G ciklična grupa.*

Kako je G konačna i Abelova, možemo primeniti teoremu o normalnoj formi. Dakle, $G \cong \mathbb{Z}_{d_1} \times ... \times \mathbb{Z}_{d_k}$ za neke $d_1|d_2, d_2|d_3, .., d_{k-1}|d_k, \quad d_1 \geq 2$. Iz ovoga sledi da za svako $a \in G$ važi $a^{d_k} = 1$. Specijalno svaki element grupe G je nula polinoma $x^{d_k} - 1$ pa po prethodnom tvrđenju sledi $d_k \geq |G| = d_1 \cdot ... \cdot d_k$. Sledi $k = 1$ tj $G \cong \mathbb{Z}_{d_1}$.

Primer: $F = \mathbb{Z}_p$, p prost i $G = \cup(\mathbb{Z}_p) = \mathbb{Z}_p\backslash\{0\} = \{1, 2, ..., p - 1\}$. Naravno $(G, \cdot_p)$ je grupa i po prethodnom, ona je ciklična tj. postoji $g \in \mathbb{Z}_p\backslash\{0\}$ td. $g \in \mathbb{Z}_p\backslash\{0\}$ td. $\mathbb{Z}_p\backslash\{0\} =< g >= \{1, g, g^2, ..., g^{p-2}\}$
Specijalno, neka je $p = 7$.
Za $g = 2$: $\begin{matrix} 1 & 2 & 4 & 8 \\ 1 & 2 & 4 & 1 \end{matrix}$ $\omega(2) = 3 \neq p - 1$ pa 2 nije primitivni koren.
Za $g = 3$: $\begin{matrix} 1 & 3 & 3^2 & 3^3 & 3^4 & 3^5 \\ 1 & 3 & 2 & 6 & 4 & 5 \end{matrix}$, pa je 3 primitivan koren po modulu 7.

Tvrdjenje 5.39 *Neka je g primitivni koren po modulu p. Tada za $a, b \in \mathbb{Z}_p\backslash\{0\}$ postoje i $u, v \in \{0, 1, ..., p - 2\}$ td. $a = g^u, \quad b = g^v$ i sledi $a \cdot_p b = g^u \cdot_p g^v = g^{u +_{p-1} v}$*

5.6 Raširenja polja

$x^2 = 2 \quad \pm\sqrt{2}$
$x^2 = -1 \quad \pm\sqrt{-1}$

Definicija 5.40 *Za polinom $f \in F[x]\backslash\{0\}$, gde je F polje, kažemo da je nerastavljiv u $F[x]$ ako ne postoje nekonstantni polinomi $g, h \in F[x]$ td. $f = gh$.*

Primer:

$$x^2 - 2 \quad \text{nerastavljiv u } \mathbb{Q}[x]$$
$$\text{rastavljiv u } \mathbb{R}[x] \quad (x - \sqrt{2})(x + \sqrt{2})$$

Teorema 5.41 ***(Kronikerova konstrukcija)**: Neka je F polje i $f \in F[x]\backslash\{0\}$ nerastavljiv polinom. Tada važi:*

1. *$E := F[x]\backslash < f >$ je polje.*
2. *Polje E sadrži potpolje izomorfno polju F (drugim rečima, E je raširenje polja F)*
3. *Polinom f ima nulu u E.*
4. *$[E : F] = deg\ f$ (biće definisano kasnije)*

Dokaz:

1. E je kpj, pa je dovoljno dokazati da svaki nenula element E ima inverz. Neka je $g+ < f >\neq 0+ < f >$ (gde je $g \in F[x]$). Tada $g \notin < f >$, tj. $f \nmid g$. Kako u $F[x]$ važi lema o količniku i ostatku, to za svaka dva polinoma možemo konstruisati Euklidov algoritam koji daje NZD tih polinoma. Kako NZD(f, g) deli i f i g, a $f \nmid g$, to je NZD$(f, g) = c \in F$. Opet, iz Euklidovog algoritma, sledi da postoje $u, v \in F[x]$ td. $fu + gv =$NZD$(f, g) = c$, pa je $fc^{-1}u + gc^{-1}v = 1$. Sledi:
   $(g+ < f >)(c^{-1}v+ < f >) = gc^{-1}v+ < f >= 1+ < f >$, jer je $1 - gc^{-1}v = fc^{-1}u \in < f >$
   Dakle, $g+ < f >$ je invertibilan.
2. Neka je $F' = \{c+ < f > | c \in F\}$. Tada je $\varphi : F \longrightarrow F'$, zadato sa $\varphi(c) = c+ < f >$, izomorfizam (za vezbu)
3. Neka je $f = a_n x^n + ... + a_1 x + a_0$. Označimo $\tilde{x} = x+ < f > \in E$ i dokažimo da je $\tilde{x}$ nula polinoma f. Zaista:
   $f(\tilde{x}) = a_n\tilde{x}^n + ... + a_1\tilde{x} + a_0 * (1+ < f >)$
   $= a_n(x+ < f >)^n + ... + a_1(x+ < f >) + a_0+ < f >$
   $= a_n x^n+ < f > +... + a_1 x+ < f > +a_0+ < f >$
   $= f+ < f >= 0+ < f >$ (po definiciji ideala) $a + I = b + I$ akko $a - b \in I$.
4. Na sledecem casu

Primer: $F = \mathbb{R}, \quad f = x^2 + 1$
$E = \mathbb{R}[x]/ < x^2 + 1 > \cong \mathbb{C}$
$g \in \mathbb{R}[x] : g = (x^2 + 1)q + ax + b$
$g+ < x^2 + 1 >= ax + b+ < x^2 + 1 > \quad a, b \in \mathbb{R}$
$ax + b+ < x^2 + 1 >= a(x+ < x^2 + 1 >) + b(1+ < x^2 + 1 >)$

$$\begin{aligned} i^2 &= (x+ < x^2 + 1 >)^2 \\ &= x^2+ < x^2 + 1 > \\ &= -1+ < x^2 + 1 > \end{aligned}$$

$\sqrt{2}$ konstruišemo sa $\mathbb{Q}[x]/ < x^2 - 2 >, x+ < x^2 - 2 >$

Definicija 5.42 *Neka je E raširenje polja F. Tada E možemo posmatrati kao vektorski prostor nad F. Ako je E konačne dimenzije nad F, tada sa $[E : F]$ označavamo dimenziju od E nad F i kažemo da je ona stepen raširenja E nad F.*

Primer: $[\mathbb{C} : \mathbb{R}] = 2$
$[1, i]$ je baza za $\mathbb{C}$ nad $\mathbb{R}$
$x \cdot 1 + y \cdot i, \quad x, y \in \mathbb{R}$

4. $[E : F] = \deg f$ - stepen raširenja
   Dovoljno je dokazati da je $[1+ < f >, x+ < f >, ..., x^{n-1}+ < f >]$ baza za E nad F (gde je $n = \deg f$).

   (a) B je generatrisa
   $E = F[x]/ < f >$. Izaberimo $g+ < f > \in E$. Dovoljno je pokazati da $\exists c_0, c_1, .., c_{n-1} \in F$ takvi da je $(*) \quad g+ < f >= c_0(1+ < f >) + c_1(x+ < f >) + ... + c_{n-1}(x^{n-1}+ < f >)$.
   Napomena: U $c_i(x^i+ < f >)$ pod c_i podrazumevamo $c_i+ < f >$.
   Po lemi o količniku i ostatku, postoje $q, r \in F[x]$ takvi da je $g = fq + r, \quad \deg r < \deg f$.
   Tada je $g - r = fq \in < f >$, pa je $g+ < f >= r+ < f >$. Kako je $\deg r < n$, to postoje $c_0, c_1, ..., c_{n-1} \in F$ takvi da je $r = c_0 + c_1x + ... + c_{n-1}x^{n-1}$, pa važi $(*)$

   (b) B je linearno nezavisan
   Dovoljno je pokazati da iz $c_0(1+ < f >) + c_1(x+ < f >) + ... + c_{n-1}(x^{n-1}+ < f >) = 0+ < f >$ sledi $c_0 = c_1 = ... = c_{n-1} = 0$
   Zaista, iz $c_0(1+ < f >) + ... + c_{n-1}(x^{n-1}+ < f >) = c_0 + c_1x + ... + c_{n-1}x^{n-1}+ < f >= 0+ < f >$ sledi
   $c_0 + c_1x + ... + c_{n-1}x^{n-1} \in < f >$ tj. $f | c_0 + c_1x + ... + c_{n-1}x^{n-1}$.
   Međutim polinom sa desne strane je stepena manjeg od n, pa je on nula polinom tj. $c_0 = c_1 = ... = c_{n-1} = 0$.

Primer: Konstruisati polje od 8 elemenata. (sva polja imaju p^n elemenata, gde je p prost.)
Rešenje: Ovo polje tražimo u obliku $F[x]/ < f >$, gde je f nerastavljiv polinom. Zato bramo $F = \mathbb{Z}_2$ (u opštem slučaju $\mathbb{Z}_p$), a za f neki nerastavljiv polinom stepena 3 (u opštem slučaju n). Polinom stepena 3 je nerastavljiv u $\mathbb{Z}_2$ akko nema nula u $\mathbb{Z}_2$.
Dakle za f možemo uzeti npr. $f = x^3 + x + 1$ tj $\mathbb{Z}_2[x]/ < x^3 + x + 1 >$ je polje sa 8 elemenata.
? Kako računamo u ovom polju ?
Svaki element je oblika $ax^2 + bx + c+ < x^3 + x + 1 >$, gde su $a, b, c \in \mathbb{Z}_2$. Sabiranje je lako i vrši se po koordinatama.
$ax^2+bx+c+ < x^3+x+1 > +a'x^2+b'x+c'+ < x^3+x+1 >= (a+a')x^2+(b+b')x+(c+c')+ < x^3+x+1 >$
Množenje je komplikovanije. Važi:
$x^3 + x + 1+ < x^3 + x + 1 >= 0+ < x^3 + x + 1 >$, pa je $x^3+ < x^3 + x + 1 >= x + 1+ < x^3 + x + 1 >$ i sledi $x^4+ < x^3 + x + 1 >= x^2 + x+ < x^3 + x + 1 >$ Sada je:

$$
\begin{aligned}
&(ax^2 + bx + c+ < x^3 + x + 1 >)(a'x^2 + b'x + c'+ < x^3 + x + 1 >) = \\
&= aa'x^4 + (ba' + b'a)x^3 + (ac' + c'a + bb')x^2 + (bc' + c'b)x + cc'+ < x^3 + x + 1 >= \\
&= (ac' + ca' + bb' + aa')x^3 + (bc' + c'b + aa' + ba' + b'a)x + cc' + ba' + b'a+ < x^3 + x + 1 >
\end{aligned}
$$

Teorema 5.43 ***(Posledica)*** *Neka je F polje i $f \in F[x]$. Tada postoji raširenje E polja F u kome f faktoriše na linearne faktore (tj. ima sve nule).*

Definicija 5.44 *Neka je $f \in F[x]\backslash\{0\}$, gde je F polje. Korensko polje polinoma f je najmanje raširenje polja F u kome f ima linearnu faktorizaciju.*

6 Algebarski elementi

*Neka je F potpolje polja $\mathbb{C}$. Za $\alpha \in \mathbb{C}$ definišemo $F[\alpha] = \{c_0 + c_1\alpha + ... + c_n\alpha^n | n \in \mathbb{N}, c_i \in F\}$. Tada $F[\alpha]$ sadrži $F \cup \{\alpha\}$ i $(F[\alpha], +, \cdot)$ je KPJ. Uz to, $F[\alpha]$ je najmanji KPJ koji sadrži $F \cup \{\alpha\}$.
*Neka je $F(\alpha)$ najmanje potpolje koje sadrži $F \cup \{\alpha\}$. Jasno, $F[\alpha] \subseteq F(\alpha)$

Definicija 6.1 *Neka je F potpolje od $\mathbb{C}$ i $\alpha \in \mathbb{C}$. Tada je $\alpha \in \mathbb{C}$ algebarski nad F ako postoji $f \in F[x]\backslash\{0\}$ takvo da je $f(\alpha) = 0$*

Primer: $\sqrt{2}$ je algebarski nad $\mathbb{Q}$, dok π nije algebarski nad $\mathbb{Q}$. Oba jesu algebarska nad $\mathbb{R}$. Za $\alpha = \sqrt{2} \to x^2 - 2$.

Definicija 6.2 *Za moničan polinom koji je minimalnog stepena da zadovoljava gornju definiciju kažemo da je minimalni polinom za α nad F, u oznaci μ_α. (Moničan = vodeći koeficijent je 1).*
Osobine:

1. *μ_α je jedinstven.*
2. *μ_α je nerastavljiv u $F[x]$.*
3. *$p(\alpha) = 0$ akko $\mu_\alpha | p$ (za $p \in F[x]$)*

Dokaz:

1. Neka je μ'_α minimalni polinom. tada je $\mu_\alpha(\alpha) = 0$ i $\deg \mu_\alpha = \deg \mu'_\alpha$.
   Polinom $\mu_\alpha - \mu'_\alpha$ je nižeg stepena od μ_α i μ'_α i važi $(\mu_\alpha - \mu'_\alpha)(\alpha) = 0$, pa mora biti $\mu_\alpha - \mu'_\alpha = 0$, pa je $\mu_\alpha = \mu'_\alpha$
2. PPS $\mu_\alpha = f \cdot g$, gde su $f, g \in F[x]$ stepena barem 1. Tada je $0 = \mu_\alpha(\alpha) = f(\alpha)g(\alpha)$, pa je $f(\alpha) = 0$ ili $g(\alpha) = 0$ što nije moguće jer je $\deg f, \deg g < \deg \mu_\alpha$
3. Po lemi o količniku i ostatku, postoje $q, r \in F[x]$ takvi da je $p = q \cdot \mu_\alpha + r, \deg r < \deg \mu_\alpha$, pa je $p(\alpha) = q(\alpha)\mu_\alpha(\alpha) + r(\alpha)$, tj. $p(\alpha) = r(\alpha)$. Dakle
   $p(\alpha) = 0$ akko $r(\alpha) = 0$(jer je $\deg r < \deg \mu_\alpha$)
   akko $r = 0$
   akko $\mu_\alpha | p$

Stav 6.3 *Neka je F potpolje polja $\mathbb{C}$ i $\alpha \in \mathbb{C}$. Tada je $F[\alpha] = F(\alpha)$ akko je α algebarski nad F.*

Dokaz:

$\Rightarrow$ Iz $F[\alpha] = F(\alpha)$ sledi daje $F[\alpha]$ polje. Samim tim, inverz od α (što je $\frac{1}{\alpha}$) se nalazi u $F[\alpha]$ pa je $\frac{1}{\alpha} = p(\alpha)$ za neko $p \in F[\alpha]$. Sledi $\alpha p(\alpha) - 1 = 0$, pa je $f(\alpha) = 0$ za $f = x \cdot p - 1$, pa je α algebarski nad F.

$\Leftarrow$ Dovoljno je dokazati da je $F[\alpha]$ polje. Koristimo teoremu o izomorfizmu za KPJ. Posmatramo preslikavanje $\Phi : F[x] \longrightarrow F[\alpha]$ zadato sa $\Phi(p) = p(\alpha)$. Ovo preslikavanje (tzv. evaluacija polinoma) je homomorfizam KPJ ($\Phi(pq) = (pq)(\alpha) = p(\alpha)q(\alpha) = \Phi(p) \cdot \Phi(q)$). Sledi: $F[x]/\text{Ker } \Phi$ polje. Kako je Ker $\Phi \lhd F[x]$, to je Ker Φ glavni, tj. Ker $\Phi =< f >$, i uz to možemo izabrati da je f moničan. U Ker Φ se nalaze svi p takvi da je $p(\alpha) = 0$, pa kako je $f|p$, to je f najnižeg stepena, tako da je $f(\alpha) = 0$ (a $f \neq 0$), pa je $f = \mu_\alpha$.
Kako je μ_α nerastavljiv, to je po Kronekerovoj konstrukciji $F[x]/\text{Ker } \Phi = F[x]/ < \mu_\alpha >$ polje.

*Kada je α algebarski nad F, važi: $F[x]/ < \mu_\alpha > \cong F(\alpha) = F[\alpha]$ sledi $[F(\alpha) : F] = \deg \mu_\alpha$.
Primer: $F = \mathbb{Q}, \alpha = \sqrt{2}$
$\mu_{\sqrt{2}} = x^2 - 2, \quad \mathbb{Q}[x]/ < x^2 - 2 > \cong \mathbb{Q}(\sqrt{2})$ i ovo je minimalno polje koje sadrži $\mathbb{Q} \cup \{\sqrt{2}\}$
Primer: $\alpha = \sqrt{2} + \sqrt{3}, \quad$ Odrediti $\frac{1}{\alpha}$ u obliku $p(\alpha)$ za neki polinom $p(x) \in \mathbb{Q}[x]$.
$\frac{1}{\alpha} = p(\alpha) \Leftrightarrow \alpha p(\alpha) - 1 = 0 \quad$ Znamo $\mu_\alpha(\alpha) = 0$, pa ako je c slobodan član u μ_α važi:
$\mu_\alpha = xq + c$. Sledi $\alpha q(\alpha) + c = 0$, pa je $\frac{1}{\alpha} = \frac{-q(\alpha)}{c}$.

Definicija 6.4 *Neka su E i F potpolja od $\mathbb{C}$ takva da je E raširenje polja F. Tada kažemo da je E konačno raširenje od F ako je E konačnodimenzionalni prostor nad F.*

Teorema 6.5 ***(O primitivnom elementu)*** *Svako konačno raširenje E polja $\mathbb{Q}$ je oblika $E = \mathbb{Q}(\alpha)$ za neko $\alpha \in E$. Element α je primitivni element raširenja E.*