Direktni proizvod grupa

Definicija (Dekartov proizvod)

Dekartov proizvod skupova $S_1, S_2, \ldots, S_n$ je skup svih uređenih n-torki $(a_1, a_2, \ldots, a_n)$, gdje je $a_i \in S_i$ za $i = 1, 2, \ldots, n$.

Dekartov proizvod označavamo sa

$$S_1 \times S_2 \times \ldots \times S_n$$

ili sa

$$\prod_{i=1}^{n} S_i$$

(#) Neka su $(G_1, *)$ i $(G_2, \circ)$ dvije date grupe. Za (a_1, a_2) i (b_1, b_2) iz $G_1 \times G_2$ definirajmo operaciju množenja po komponentama

$$(a_1, a_2)(b_1, b_2) = (a_1 * b_1,\ a_2 \circ b_2)$$

Pokazati da je $G_1 \times G_2$ grupa u odnosu na datu operaciju množenja.

R.: ZATVORENOST

Neka su $a_i \in G_i$ i $b_i \in G_i$ $(i \in \{1,2\})$. Kako je G_1 grupa slijedi da je $a_1 * b_1 \in G_1$, a kako je G_2 grupa slijedi da $a_2 \circ b_2 \in G_2$. Time $(a_1, a_2), (b_1, b_2) \in G_1 \times G_2 \Rightarrow (a_1, a_2) \cdot (b_1, b_2) \in G_1 \times G_2$

$\Rightarrow$ dabo $\checkmark$ množenje je zatvorena binarna operacija.

MNOŽENJE JE ASOCIJATIVNO

$$(a_1, a_2) \cdot \left[(b_1, b_2)(c_1, c_2)\right] = (a_1, a_2)(b_1 * c_1,\ b_2 \circ c_2)$$

$$= (a_1 * (b_1 * c_1),\ a_2 \circ (b_2 \circ c_2)) = ((a_1 * b_1) * c_1,\ (a_2 \circ b_2) \circ c_2)$$

$$= (a_1 * b_1,\ a_2 \circ b_2)(c_1, c_2) = \left[(a_1, a_2)(b_1, b_2)\right](c_1, c_2)$$

POSTOJI IDENTITET

Ako je e_i identitet u G_i, tada je očigledno da je množenje po komponentama (e_1, e_2) identitet u $G_1 \times G_2$.

SVAKI ELEMENT IMA INVERZ

(a_1^{-1}, a_2^{-1}) je invert elementa (a_1, a_2)

Prema tome $G_1 \times G_2$ je grupa.

(#) Napisati sve elemente grupe $U(8)\times U(10)$. Izračunati $(3,7)\cdot(5,3)$ i $(3,7)\cdot(7,9)$.

Rj: $U(8)=\{1,3,5,7\}$

$U(10)=\{1,3,7,9\}$

$$U(8)\times U(10)=\{(1,1),(1,3),(1,7),(1,9),(3,1),(3,3),(3,7),(3,9),(5,1),(5,3),(5,7),(5,9),(7,1),(7,3),(7,7),(7,9)\}$$

$$(3,7)\cdot(5,3)=(7,1),\qquad (3,7)\cdot(7,9)=(5,3).$$

(#) Napisati sve elemente grupe $\mathbb{Z}_2\times\mathbb{Z}_3$. Pokazati da je $\mathbb{Z}_6$ ciklička grupa, te pokazati da je $\mathbb{Z}_2\times\mathbb{Z}_3\cong\mathbb{Z}_6$.

Rj: $\mathbb{Z}_2\times\mathbb{Z}_3=\{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2)\}$

$\mathbb{Z}_2\times\mathbb{Z}_3=\langle(1,2)\rangle$

	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Iz tabele vidimo $\mathbb{Z}_2\times\mathbb{Z}_3\cong\mathbb{Z}_6$

	(0,0)	(1,2)	(0,1)	(1,0)	(0,2)	(1,1)
(0,0)	(0,0)	(1,1)	(0,1)	(1,0)	(0,2)	(1,1)
(1,2)	(1,1)	(0,1)	(1,0)	(0,2)	(1,1)	(0,0)
(0,1)	(0,1)	(1,0)	(0,2)	(1,1)	(0,0)	(1,2)
(1,0)	(1,0)	(0,2)	(1,1)	(0,0)	(1,2)	(0,1)
(0,2)	(0,2)	(1,1)	(0,0)	(1,2)	(0,1)	(1,0)
(1,1)	(1,1)	(0,0)	(1,2)	(0,1)	(1,0)	(0,2)

(#) Klasifikovati grupe reda 4. Drugim riječima pokazati da je grupa reda 4 izomorfna sa $\mathbb{Z}_4$ ili sa $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Rj.

Ako je G ciklička grupa npr. $G = \{e, a, a^2, a^3\}$ tada je $G \cong \mathbb{Z}_4$

	e	a	a^2	a^3
e	e	a	a^2	a^3
a	a	a^2	a^3	e
a^2	a^2	a^3	e	a
a^3	a^3	e	a	a^2

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$f: G \to \mathbb{Z}_4$

$a^i \to i$ je izomorfizam

Ako G nije ciklička, neka je $G = \{e, a, b, ab\}$. Prema Lagranžovoj teoremi tada je $|a| = |b| = |ab| = 2$ (a time $a^2 = e$, $b^2 = e$, $(ab)^2 = e$).

	e	a	b	ab
e	e	a	b	ab
a	a	e	ab	b
b	b	ab	e	a
ab	ab	b	a	e

	(0,0)	(1,0)	(0,1)	(1,1)
(0,0)	(0,0)	(1,0)	(0,1)	(1,1)
(1,0)	(1,0)	(0,0)	(1,1)	(0,1)
(0,1)	(0,1)	(1,1)	(0,0)	(1,0)
(1,1)	(1,1)	(0,1)	(1,0)	(0,0)

$(ab)^2 = e$

$abab = e$ /.b sa desne

$aba = b$ /.a sa desne

$ab = ba$

$abab = e$

$\Downarrow$

$aba = b$

i $bab = a$

Preslikavanje

$e \to (0,0)$

$a \to (1,0)$

$b \to (0,1)$

$ab \to (1,1)$ je

izomorfizam sa G na $\mathbb{Z}_2 \times \mathbb{Z}_2$

Teorem (red elementa u direktnom proizvodu)
Red elementa u direktnom proizvodu konačnog broja konačnih grupa je najmanji zajednički sadržalac redova komponenata elementa. Simbolima

$$|(g_1, g_2, \dots, g_n)| = NZS(|g_1|, |g_2|, \dots, |g_n|)$$

(#) Dokazati teorem iznad.

Rj.:
Identitet grupe G_i označimo sa e_i. Neka su

$$s = NZS(|g_1|, |g_2|, \dots, |g_n|)$$
$$t = |(g_1, g_2, \dots, g_n)|$$

Kako je s sadržalac svakog $|g_i|$ imamo da

$$(g_1, g_2, \dots, g_n)^s = (g_1^s, g_2^s, \dots, g_n^s) = (e_1, e_2, \dots, e_n)$$

iz čega slijedi $t \leq s$.

S druge strane, iz $(g_1^t, g_2^t, \dots, g_n^t) = (g_1, g_2, \dots, g_n)^t = (e_1, e_2, \dots, e_n)$ vidimo da je t zajednički sadržalac od $|g_1|, |g_2|, \dots, |g_n|$. Time $s \leq t$.

(#) Pronaći redove svih elemenata grupe $\mathbb{Z}_2 \times \mathbb{Z}_6$.

tj.

$$\mathbb{Z}_2 \times \mathbb{Z}_6 = \{(0,0), (0,1), (0,2), (0,3), (0,4), (0,5), (1,0), (1,1), (1,2), (1,3), (1,4), (1,5)\}$$

$|(0,0)| = NZS(|0|,|0|) = NZS(1,1) = 1$

$|(0,1)| = NZS(|0|,|1|) = NZS(1,6) = 6$

$|(0,2)| = NZS(1,3) = 3$

$|(0,3)| = NZS(1,2) = 2$

$|(0,4)| = NZS(1,3) = 3$

$|(0,5)| = NZS(1,6) = 6$

$|(1,0)| = NZS(|1|,|0|) = NZS(2,1) = 2$

$|(1,1)| = NZS(2,6) = 6$

$|(1,2)| = NZS(2,3) = 6$

$|(1,3)| = NZS(2,2) = 2$

$|(1,4)| = NZS(2,3) = 6$

$|(1,5)| = NZS(2,6) = 6$

(#) Odredite sve homomorfizme iz grupe $\mathbb{Z}_2 \times \mathbb{Z}_2$ u grupu $\mathbb{Z}_4$.

R.:

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

Primjetimo da je $\mathbb{Z}_2 \times \mathbb{Z}_2 = \langle (0,1), (1,0) \rangle$.

	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)
(0,1)	(0,1)	(0,0)	(1,1)	(1,0)
(1,0)	(1,0)	(1,1)	(0,0)	(0,1)
(1,1)	(1,1)	(1,0)	(0,1)	(0,0)

Red elementa (0,0) je 1

Red elementa (0,1), (1,0) i (1,1) je 2

$\mathbb{Z}_4 = \{0,1,2,3\}$

Red elementa 0 je 1

Red elementa 1 je 4

Red elementa 3 je 4

Red elementa 2 je 2

Kako je $\mathbb{Z}_2 \times \mathbb{Z}_2$ generisan sa elementima (0,1) i (1,0), dovoljno je da pronađemo slike samo za ova dva elementa. Postoje četiri mogućnosti:

(i) $\phi(0,1) = 0$, $\phi(1,0) = 0$

(ii) $\phi(0,1) = 2$, $\phi(1,0) = 0$

(iii) $\phi(0,1) = 0$, $\phi(1,0) = 2$

(iv) $\phi(0,1) = 2$, $\phi(1,0) = 2$.

(i) $\Rightarrow$ $\phi(0,0) = 0$, $\phi(1,1) = 0$;

(ii) $\Rightarrow$ $\phi(0,0) = 0$, $\phi(1,1) = 2$;

(iii) $\Rightarrow$ $\phi(0,0) = 0$, $\phi(1,1) = 2$;

(iv) $\Rightarrow$ $\phi(0,0) = 0$, $\phi(1,1) = 0$;

(#) Odrediti broj elemenata reda 5 u grupi $\mathbb{Z}_{25} \times \mathbb{Z}_5$.

Rj:

Prema prethodnoj Teoremi možemo prebrojati broj elemenata $(a,b) \in \mathbb{Z}_{25} \times \mathbb{Z}_5$ sa osobinom

$$5 = |(a,b)| = NZS(|a|, |b|)$$

Da bi vrijedila ova jednakost moguća su tri slučaja

1° $|a|=5$, $|b|=1$, 2° $|a|=5$, $|b|=5$,

3° $|a|=1$, $|b|=5$.

Pa posmatrajmo svaki od ovih slučajeva

1° $|a|=5$, $|b|=1$

$\Rightarrow a \in \{5, 10, 15, 20\}$, $b \in \{0\}$

$\forall x \in \{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24\}$, $|x| = 25$

U 1° imamo 4 elemenata

2° $|a|=5$, $|b|=5$ $\Rightarrow a \in \{5, 10, 15, 20\}$, $b \in \{1, 2, 3, 4\}$

U drugom slučaju imamo 16 elemenata

$|a|=1$, $|b|=1 \Rightarrow NZS(1,1)=1$

U ovom slučaju imamo jedan element reda 1

3° $|a|=1$, $|b|=5$ $\Rightarrow a \in \{0\}$, $b \in \{1, 2, 3, 4\}$ $\Rightarrow$ 4 elementa

Prema tome $\mathbb{Z}_{25} \times \mathbb{Z}_5$ ima 24 elemenata reda 5.

Prisjetimo se Fundamentalne teoreme za ciklične grupe:

Teorema (Fundamentalna teorema za ciklične grupe)
Svaka podgrupa cikličke grupe je ciklička. Štaviše, ako je $|\langle a\rangle| = n$, tada je red bilo koje podgrupe grupe $\langle a\rangle$ djelilac broja n; i za svaki pozitivni djelilac k broja n, grupa $\langle a\rangle$ ima tačno jednu podgrupu reda k - naime $\langle a^{\frac{n}{k}}\rangle$.

(#) Dokazati teoremu iznad.

Rj.

Prisjetimo se važne f-je iz teorije brojeva koja se zove Euler-ova fi f-ja. Neka je $\phi(1)=1$, i za svaki cijeli $n>1$, označimo sa $\phi(n)$ broj pozitivnih cijelih koji su manji od n i koji su relativno prosti sa n. Primjetimo da iz definicije grupe $U(n)$ imamo da $|U(n)|=\phi(n)$. Prvih 12 vrijednosti od $\phi(n)$ su dati u sljedećoj tabeli.

n	1	2	3	4	5	6	7	8	9	10	11	12
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

Teorema (broj elemenata bilo kojeg reda u cikličkoj grupi).
Ako je d pozitivan cijeli koji dijeli n, tada je broj elemenata reda d u cikličkoj grupi reda n $\phi(d)$.

(#) Dokazati teoremu iznad.

Rj: U dokazu ćemo iskoristiti sljedeću teoremu

Teorema (Fundamentalna teorema za ciklične grupe)
Svaka podgrupa cikličke grupe je ciklička. Štaviše, ako je $|\langle a\rangle|=n$, tada je red bilo koje podgrupe od $\langle a\rangle$ djelilac od n; i za svaki pozitivan djelilac k broja n, grupa $\langle a\rangle$ ima tačno jednu podgrupu reda k - naime $\langle a^{\frac{n}{k}}\rangle$.

Prema Fundamentalnoj teoremi za ciklične grupe da ter grupa ima točno jednu podgrupu reda d - nazovimo je $\langle a \rangle$. Tada svaki element reda d također generira podgrupu $\langle a \rangle$.

Teorema ($\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ i $|a^k| = \frac{n}{\gcd(n,k)}$)

Neka je a element grupe reda n i neka je k pozitivan cijeli. Tada $\langle a^k \rangle = \langle a^{\gcd(n,k)} \rangle$ i $|a^k| = \frac{n}{\gcd(n,k)}$.

Corolar 1 (red elementa u konačnoj cikličkoj grupi)

U konačnoj cikličkoj grupi, red elementa dijeli red grupe.

Corolar 2 (kriterij za $\langle a^i \rangle = \langle a^j \rangle$ i $|a^i| = |a^j|$)

Neka je $|a| = n$. Tada $\langle a^i \rangle = \langle a^j \rangle$ ako i samo ako $\gcd(n,i) = \gcd(n,j)$, i $|a^i| = |a^j|$ ako i samo ako $\gcd(n,i) = \gcd(n,j)$.

Corolar 3 (generatori konačnih cikličkih grupa)

Neka je $|a| = n$. Tada $\langle a \rangle = \langle a^j \rangle$ ako i samo ako $\gcd(n,j) = 1$ i $|a| = |\langle a^j \rangle|$ ako i samo ako $\gcd(n,j) = 1$.

Corolar 4 (generatori od $\mathbb{Z}_n$)

Cijeli broj $k \in \mathbb{Z}_n$ je generator grupe $\mathbb{Z}_n$ ako i samo ako $\gcd(n,k) = 1$.

Kako svaki element reda d generira podgrupu $\langle a \rangle$ prema Corolaru 3 iznad, a^k generira $\langle a \rangle$ ako i samo ako $\gcd(k,d) = 1$. Broj takvih elemenata je točno $\phi(d)$.

(#) Odrediti broj cikličkih podgrupa reda 10 u grupi $\mathbb{Z}_{100} \times \mathbb{Z}_{25}$.

Rj. U rješenju ovog zadatka ćemo upotrebiti sljedeću teoremu:

Teorem

Ako je d pozitivan cijeli broj koji dijeli n, tada broj elemenata reda d u cikličnoj grupi reda n je jednak broju i iznosi $\phi(d)$.

Prebrojmo prvo broj elemenata (a,b) reda 10.

$$\left.\begin{array}{l} |(a,b)| = 10 \\ |(a,b)| = NZS(|a|,|b|) \end{array}\right\} \Rightarrow NZS(|a|,|b|) = 10$$

gdje $|a|$ dijeli 100, a $|b|$ dijeli 25.

Moguća su sljedeća tri slučaja:

1° $|a|=10$, $|b|=1$; 2° $|a|=10$, $|b|=5$

Prema Fundamentalnoj teoremi za cikličke grupe ako je $|\langle a\rangle| = n$ i k je djelilac broja n tada grupa $\langle a\rangle$ ima točno jednu podgrupu reda k – naime podgrupu $\langle a^{\frac{n}{k}}\rangle$.

Kako 10 dijeli 100 postoji samo jedna ciklička podgrupa reda 10.

Prema izpisanoj teoremi iznad, kako je 10 pozitivan cijeli broj koji dijeli 100, broj elemenata reda 10 u cikličkoj grupi $\mathbb{Z}_{100}$ iznosi $\phi(10) = 4$ tj. postoje četri generatora.

Ako je $|b|=1$ postoji samo jedan izbor za b. Ako je $|b|=5$ postoje

četri izbora za b.
Time u ova dva slučaja imamo ukupno 20 mogućnosti.

3° $|a|=2$, $|b|=5$.

Prema Fundamentalnoj teoremi za cikličke grupe svaka konačna ciklička grupa parnog reda ima jedinstvenu podgrupu reda 2, pa imamo samo jednu mogućnost za a. Očigledno je da postoje četri mogućnosti za b. Pa ovaj slučaj proizvodi 4 mogućnosti za (a, b).

Time grupa $\mathbb{Z}_{100} \times \mathbb{Z}_{25}$ ima 24 elemenata reda 10.

Kako svaka ciklička podgrupa reda 10 ima 4 elementa reda 10; kako ni jedne dvije cikličke podgrupe ne mogu imati zajednički element reda 10, moramo imati

$$\frac{24}{4} = 6$$

cikličkih podgrupa reda 10.

(Ova metoda je slična određivanju broja ovaca u toru brojeći noge i djeljeći sa 4.)

Teorem (kriterij da $G \times H$ bude ciklička)

Neka su G i H konačne cikličke grupe. Tada je $G \times H$ ciklička ako i samo ako su $|G|$ i $|H|$ relativno prosti.

(#) Dokazati teoremu iznad.

Rj:

Neka je $|G| = m$ i $|H| = n$ tako da je $|G \times H| = mn$. Da dokažemo prvu polovinu teoreme, pretpostavimo da je $G \times H$ ciklička grupa i pokažimo da su m i n relativno prosti. Pretpostavimo da je $\gcd(m,n) = d$, i da je (g,h) generator grupe $G \times H$. Kako je

$$(g,h)^{\frac{mn}{d}} = \left((g^m)^{\frac{n}{d}}, (h^n)^{\frac{m}{d}} \right) = (e,e)$$

imamo da je $mn = |(g,h)| \leq \frac{mn}{d}$. Prema tome $d = 1$.

Da bi pokazali drugu polovicu teoreme, neka je $G = \langle g \rangle$ i $H = \langle h \rangle$ i pretpostavimo da je $\gcd(m,n) = 1$. Tada

$$|(g,h)| = NZS(m,n) = mn = |G \times H|$$

a time je (g,h) generator grupe $G \times H$.

Korolar 1 (kriterij da $G_1 \times G_2 \times \dots \times G_n$ bude ciklička)

Vanjski direktni proizvod $G_1 \times G_2 \times \dots \times G_n$ konačnog broja konačnih cikličkih grupa je ciklička grupa ako i samo ako su $|G_i|$ i $|G_j|$ relativno prosti kada je $i \neq j$.

Korolar 2 (kriterij da $\mathbb{Z}_{n_1, n_2, \dots, n_k} \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \times \mathbb{Z}_{n_k}$)

Neka je $m = n_1 n_2 \dots n_k$. Tada je $\mathbb{Z}_m$ izomorfno sa $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \dots \times \mathbb{Z}_{n_k}$ ako i samo ako su n_i i n_j relativno prosti kada je $i \neq j$.

(#) (a) Odrediti $\langle (12), (123) \rangle$.

(b) Odrediti generatore grupe $\mathbb{Z} \times \mathbb{Z}_n$.

Rj.:

(a) $\langle (12), (123) \rangle = S_3$

(b) $\mathbb{Z} \times \mathbb{Z}_n = \langle (1,0), (0,1) \rangle$

Teorema

Neka je H podgrupa grupe G koja je generisana skupom $\{g_i \in G \mid i \in I\}$. Tada je $h \in H$ tačno onda kada je proizvod oblika

$$h = g_{i_1}^{\alpha_1} g_{i_2}^{\alpha_2} \dots g_{i_n}^{\alpha_n}$$

gdje g_{i_k}-ovi ne moraju biti različiti.

(#) Dokazati teoremu iznad.

Rj. Neka je K skup svih proizvoda oblika $g_{i_1}^{\alpha_1} \dots g_{i_n}^{\alpha_n}$ gdje g_{i_k}-ovi nisu neophodno različiti. Jasno je da je tad K podskup od H. Ono što treba da pokažemo je, da je K podgrupa grupe G. U tom slučaju imaćemo da je $K = H$, s obzirom da je H najmanja podgrupa koja sadrži sve g_i-jeve.

Očigledno K je zatvoren u odnosu na operaciju grupe.

Kako je $g_i^0 = 1$ identitet je u K. Ostalo je da pokažemo da invert elementa $g = g_{i_1}^{k_1} g_{i_2}^{k_2} \dots g_{i_n}^{k_n}$ u grupi K mora također biti u K. U svakom slučaju,

$$g^{-1} = \left(g_{i_1}^{k_1} \dots g_{i_n}^{k_n} \right)^{-1} = \left(g_{i_n}^{-k_n} g_{i_{n-1}}^{-k_{n-1}} \dots g_{i_1}^{-k_1} \right).$$

Definicija (p-grupa)

Neka je p prost broj. Grupu G definiziramo kao p-grupa ako svaki element grupe G ima red jednak stepenu broja p.

Na primjer $\mathbb{Z}_2 \times \mathbb{Z}_2$ i $\mathbb{Z}_4$ su 2-grupe, dok je $\mathbb{Z}_{27}$ 3-grupa.

Teorema

Svaka konačna abelova grupa je unutrašnji direktni proizvod p-grupa.

Teorema (Fundamentalna teorema konačnih Abelovih grupa)

Svaka konačna Abelova grupa G je izomorfna direktnom proizvodu cikličkih grupa oblika

$$\mathbb{Z}_{p_1^{d_1}} \times \mathbb{Z}_{p_2^{d_2}} \times \dots \times \mathbb{Z}_{p_n^{d_n}}$$

gdje su p_i-jevi prosti brojevi (koji ne moraju biti različiti)

(#) Klasifikovati sve Abelove grupe reda 36.

Rj.

(#) Pronaći sve Abelove grupe reda 80.

R.j.

Faktorizacija broja 80 je

$$80 = 5 \cdot 16 = 5 \cdot 2 \cdot 8 = 5 \cdot 2^4$$

Kako je G Abelova grupa reda 80, prema fundamentalnoj teoremi konačnih Abelovih grupa, G je proizvod faktora oblika $\mathbb{Z}_5, \mathbb{Z}_2, \mathbb{Z}_4, \mathbb{Z}_8$ i $\mathbb{Z}_{16}$.

Različite mogućnosti su

$$G \cong \mathbb{Z}_5 \times \mathbb{Z}_{16}$$

$$G \cong \mathbb{Z}_5 \times \mathbb{Z}_8 \times \mathbb{Z}_2$$

$$G \cong \mathbb{Z}_5 \times \mathbb{Z}_4 \times \mathbb{Z}_4$$

$$G \cong \mathbb{Z}_5 \times \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

$$G \cong \mathbb{Z}_5 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

(#) Klasificirati sve abelove grupe reda 540.

Rj: $540 = 2 \cdot 270 = 2^2 \cdot 135 = 2^2 \cdot 5 \cdot 27 = 2^2 \cdot 3^3 \cdot 5$

Odredimo G, $|G| = 540$.

Prema fundamentalnoj teoremi konačnih Abelovih grupa, G je produkt faktora oblika $\mathbb{Z}_2$, $\mathbb{Z}_4$, $\mathbb{Z}_3$, $\mathbb{Z}_9$, $\mathbb{Z}_{27}$ i $\mathbb{Z}_5$.

Imamo sljedećih šest mogućnosti

$G \cong \mathbb{Z}_4 \times \mathbb{Z}_{27} \times \mathbb{Z}_5$

$G \cong \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_5$

$G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{27} \times \mathbb{Z}_5$

$G \cong \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

$G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_5$

$G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

V glavnem izreku 5.6 zaključne naloge nastopajo kar tri različne grupe, zato smo zaradi lažjega razločevanja abelovo grupo označili kar z A.

Obstajajo tudi grupe, ki niso abelove. Imenujemo jih **neabelove grupe**. Najmanjša neabelova grupa, ki je reda 6, je *diedrska grupa* $D_{2\cdot 3}$ oziroma njej izomorfna grupa, tako imenovana *simetrična grupa* S_3.

V nadaljevanju bomo uporabili kartezični produkt in direktni produkt, zato ju sedaj oba definirajmo.

Definicija 2.7. ***Kartezični produkt*** *množic* $S_1, S_2, ..., S_n$ *je množica vseh urejenih* n*=teric* $(a_1, a_2, ..., a_n)$, *kjer je* $a_i \in S_i$ *za* $i = 1, 2, ..., n$. *Kartezični produkt pišemo kot:*

$$S_1 \times S_2 \times \cdots \times S_n$$

ali

$$\prod_{i=1}^{n} S_i.$$

Sedaj, naj bodo $G_1, G_2, ..., G_n$ grupe in uporabimo multiplikativno notacijo za vse grupne operacije, kakor je to storil Fraleigh. Gledano na G_i kot množice lahko formiramo $\prod_{i=1}^{n} G_i$. Pokažimo, da lahko naredimo $\prod_{i=1}^{n} G_i$ v grupo z binarno operacijo množenja po komponentah.

Izrek 2.8. *Naj bodo* $G_1, G_2, ..., G_n$ *grupe. Za* $(a_1, a_2, ..., a_n)$ *in* $(b_1, b_2, ..., b_n)$ *v* $\prod_{i=1}^{n} G_i$, *definirajmo operacijo množenja po komponentah:*

$$(a_1, a_2, ..., a_n)(b_1, b_2, ..., b_n) = (a_1b_1, a_2b_2, ..., a_nb_n).$$

Potem je $\prod_{i=1}^{n} G_i$ *skupaj s to operacijo grupa, ki jo imenujemo* ***direktni produkt*** *grup* G_i.

Dokaz. Naj bo $a_i \in G_i$ in $b_i \in G_i$. Ker je G_i grupa, sledi da je $a_ib_i \in G_i$. Po definirani binarni operaciji na $\prod_{i=1}^{n} G_i$ v izreku, sledi, da je $\prod_{i=1}^{n} G_i$ zaprt za dano binarno operacijo. Zakon asociativnosti v $\prod_{i=1}^{n} G_i$ velja. To dokažemo tako, da uporabimo asociativnost po komponentah:

$$\begin{aligned}
(a_1, a_2, ..., a_n)[(b_1, b_2, ..., b_n)(c_1, c_2, ..., c_n)] &= (a_1, a_2, ..., a_n)(b_1c_1, b_2c_2, ..., b_nc_n) \\
&= (a_1(b_1c_1), a_2(b_2c_2), ..., a_n(b_nc_n)) \\
&= ((a_1b_1)c_1, (a_2b_2)c_2, ..., (a_nb_n)c_n) \\
&= (a_1b_1, a_2b_2, ..., a_nb_n)(c_1, c_2, ..., c_n) \\
&= [(a_1, a_2, ..., a_n)(b_1, b_2, ..., b_n)](c_1, c_2, ..., c_n).
\end{aligned}$$

Če je e_i identiteta v G_i, je potem očitno, da je z množenjem po komponentah $(e_1, e_2, ..., e_n)$ identiteta v $\prod_{i=1}^{n} G_i$. Nazadnje, $(a_1^{-1}, a_2^{-1}, ..., a_n^{-1})$ je inverz elementa $(a_1, a_2, ..., a_n)$. Torej je $\prod_{i=1}^{n} G_i$ grupa. □

~~Avtomorfizmi grupe $\mathbb{Z}_5$:~~

~~Grupa $\mathbb{Z}_5$ je ciklična, zato je vsak homomorfizem $\phi : \mathbb{Z}_5 \to \mathbb{Z}_5$ določen s sliko generatorja. Če označimo $\phi(1) = n$, bo ϕ bijektivna preslikava natanko takrat, ko bo~~

$$n \in \{1, 2, 3, 4\}.$$

~~Torej je~~

$$\mathrm{Aut}(\mathbb{Z}_5) \cong \mathbb{Z}_5^*.$$

~~Avtomorfizmi grupe $\mathbb{Z}_{10}$:~~

~~Tudi grupa $\mathbb{Z}_{10}$ je ciklična, zato velja podoben sklep kot zgoraj. Če označimo $\phi(1) = n$, bo tokrat ϕ bijektivna preslikava za~~

$$n \in \{1, 3, 7, 9\},$$

~~kar pomeni, da je~~

$$\mathrm{Aut}(\mathbb{Z}_{10}) \cong \mathbb{Z}_{10}^*.$$

~~Opomba: V splošnem so avtomorfizmi grupe $\mathbb{Z}_n$ v bijektivni korespondenci z elementi $\mathbb{Z}_n^*$. Elementu $m \in \mathbb{Z}_n^*$ pripada preslikava množenja z m po modulu n.~~ □

(7) Ugotovi, ali sta dani grupi izomorfni in poišči eksplicitni izomorfizem, če sta:

(a) $\mathbb{Z}_6$ in $\mathbb{Z}_2 \times \mathbb{Z}_3$,

(b) $\mathbb{Z}_4$ in $\mathbb{Z}_2 \times \mathbb{Z}_2$,

(c) $\mathbb{Z}_{30}$ in $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$.

Rešitev: (a) Imamo Abelovi grupi reda 6:

$$\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\},$$
$$\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}.$$

Grupa $\mathbb{Z}_6$ je ciklična z generatorjem 1, medtem ko pri grupi $\mathbb{Z}_2 \times \mathbb{Z}_3$ ni na prvi pogled jasno, ali je generirana z enim elementom. Hitro pa lahko preverimo, da jo generira element $(1, 1)$, kar pomeni, da lahko definiramo izomorfizem $\phi : \mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3$ s predpisi:

$$\phi(1) = (1, 1),$$
$$\phi(2) = (0, 2),$$
$$\phi(3) = (1, 0),$$
$$\phi(4) = (0, 1),$$
$$\phi(5) = (1, 2),$$
$$\phi(0) = (0, 0).$$

(b) Sedaj imamo dve Abelovi grupi reda 4:

$$\mathbb{Z}_4 = \{0, 1, 2, 3\},$$
$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1)\}.$$

Grupa $\mathbb{Z}_4$ je spet ciklična z generatorjem 1, medtem ko grupa $\mathbb{Z}_2 \times \mathbb{Z}_2$ tokrat ni ciklična. Če bi namreč bila, bi obstajal element reda 4. Preverimo pa lahko, da so vsi elementi, razen enote, reda 2, kar pomeni, da grupi $\mathbb{Z}_4$ in $\mathbb{Z}_2 \times \mathbb{Z}_2$ nista izomorfni.

(c) Grupi $\mathbb{Z}_{30}$ in $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ sta reda 30. Ker so $2, 3$ in 5 paroma tuja števila, ima element $(1, 1, 1) \in \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ red 30, zato lahko definiramo izomorfizem $\phi : \mathbb{Z}_{30} \to \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$ s predpisom:

$$\phi(k) = (k \mod (2), k \mod (3), k \mod (5)).$$

Opomba: Grupi $\mathbb{Z}_{mn}$ in $\mathbb{Z}_m \times \mathbb{Z}_n$ sta izomorfni natanko takrat, ko sta števili m in n tuji. V tem primeru je izomorfizem $\phi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ dan s predpisom

$$\phi(k) = (k \mod (m), k \mod (n)).$$

Od tod med drugim sledi, da za vsako končno Abelovo grupo G obstaja izomorfizem

$$G \cong \mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}},$$

kjer so p_i praštevila, ki delijo red grupe G. Isto praštevilo se lahko ponovi večkrat, kot smo videli v primeru $G = \mathbb{Z}_2 \times \mathbb{Z}_2$. □

(8) Poišči vse Abelove grupe reda 80.

Rešitev: Razcep števila 80 se glasi

$$80 = 5 \cdot 2^4.$$

Če je G Abelova grupa reda 80, je torej produkt faktorjev oblike $\mathbb{Z}_5, \mathbb{Z}_2, \mathbb{Z}_4, \mathbb{Z}_8$ in $\mathbb{Z}_{16}$. Različne možnosti so:

$$\begin{aligned}
G &\cong \mathbb{Z}_5 \times \mathbb{Z}_{16}, \\
G &\cong \mathbb{Z}_5 \times \mathbb{Z}_8 \times \mathbb{Z}_2, \\
G &\cong \mathbb{Z}_5 \times \mathbb{Z}_4 \times \mathbb{Z}_4, \\
G &\cong \mathbb{Z}_5 \times \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \\
G &\cong \mathbb{Z}_5 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.
\end{aligned}$$

□

~~(9) Zapiši grupno tabelo za operacijo v grupi $\mathbb{Z}_{10}^*$. Kateri grupi je izomorfna grupa $\mathbb{Z}_{10}^*$?~~

~~*Rešitev:* Z oznako $\mathbb{Z}_n^*$ označimo grupo (za množenje) obrnljivih elementov v kolobarju $\mathbb{Z}_n$. Ta grupa ima $\phi(n)$ elementov, njena enota pa je element 1.~~

~~V našem primeru je~~

$$\mathbb{Z}_{10}^* = \{1, 3, 7, 9\},$$

~~grupna tabela pa se glasi~~

$\circ$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

(4) Bijekciji $f, g : \mathbb{Z}_{17} \to \mathbb{Z}_{17}$ sta dani s predpisoma:

$$f(x) = 2x,$$
$$g(x) = x^3.$$

Poišči reda bijekcij f in g, če ju smatramo kot elementa simetrične grupe S_{17}.

Rešitev: Bijekcija f ima red 8, bijekcija g pa red 4.

(5) Kolikšen je maksimalen red, ki ga lahko ima element grupe S_{12}?

Rešitev: Maksimalen možni red je 60. Takšen red ima na primer permutacija

$$(1\,2\,3\,4\,5)(6\,7\,8\,9)(10\,11\,12).$$

(6) Poišči vse homomorfizme grup:

(a) $\mathbb{Z}_8 \to S_3$,

(b) $\mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_4$,

(c) $\mathbb{Z}_4 \to \mathbb{Z}_3$.

Rešitev:

(a) Vsak homomorfizem $\phi : \mathbb{Z}_8 \to S_3$ je določen z vrednostjo $\phi(1)$. Ker mora red elementa $\phi(1)$ deliti 8, dobimo štiri možnosti:

$$\phi(1) = (1)(2)(3),$$
$$\phi(1) = (1\,2)(3),$$
$$\phi(1) = (1\,3)(2),$$
$$\phi(1) = (1)(2\,3).$$

(b) Homomorfizem $\phi : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_4$ je določen s slikama elementov $(1, 0)$ in $(0, 1)$, ki morata imeti red 1 ali 2. Tako dobimo naslednje možnosti:

$$\phi(1,0) = 0,\ \phi(0,1) = 0,$$
$$\phi(1,0) = 2,\ \phi(0,1) = 0,$$
$$\phi(1,0) = 0,\ \phi(0,1) = 2,$$
$$\phi(1,0) = 2,\ \phi(0,1) = 2.$$

(c) Edini možni homomorfizem $\phi : \mathbb{Z}_4 \to \mathbb{Z}_3$ je ničelni homomorfizem.

(7) Poišči vse Abelove grupe reda 36.

Rešitev: Do izomorfizma natanko so to grupe:

$$G \cong \mathbb{Z}_{36},$$
$$G \cong \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3,$$
$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9,$$
$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3.$$

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

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

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

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

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

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

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

in tako je $k \leq v$.

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

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

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

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

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

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

. □

$$\varphi : G \longrightarrow D_{2n}$$

$$\varphi : a^i b^j \longmapsto \rho^i \tau^j$$

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

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

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

2.7 Direktni produkt grup

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

Naj bosta G in H grupi. **Direktni produkt** grup G in H je množica urejenih parov

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

skupaj z operacijo

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

pri čemer sta $\circ_G$ in $\circ_H$ oznaki operacij grup G in H.

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

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

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

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

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

□

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

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

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

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

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

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

DOKAZ: Dokaz prepuščamo bralcu. □

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

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

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

s predpisom

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

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

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

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

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

zato je φ homomorfizem grup.

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

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

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

2.8 ~~Center grupe~~

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

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

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