АЛГЕБРА 1

Групе

Коначно генерисане Абелове групе

Зоран Петровић

11. и 18. децембар 2012.

Подсетимо се диедарске групе:

$$\mathbb{D}_n = \langle\ \sigma, \rho \mid \sigma^2 = \varepsilon, \rho^n = \varepsilon, \sigma\rho = \rho^{n-1}\sigma\ \rangle.$$

Њена абелизација задата је са:

$$\mathbb{D}_n^{\mathrm{Ab}} = \langle\ \sigma, \rho \mid 2\sigma = 0, n\rho = 0, \sigma + \rho = (n-1)\rho + \sigma\ \rangle.$$

Тако добијамо систем једначина

$$\begin{aligned} 2\sigma &= 0 \\ n\rho &= 0 \\ (n-2)\rho &= 0. \end{aligned}$$

Одузимањем последње једначине од претпоследње добијамо систем

$$\begin{aligned} 2\sigma &= 0 \\ 2\rho &= 0 \\ (n-2)\rho &= 0. \end{aligned}$$

Природно је разликовати два случаја.

$n = 2k + 1$. Добијамо систем

$$\begin{aligned} 2\sigma &= 0 \\ 2\rho &= 0 \\ (2k-1)\rho &= 0. \end{aligned}$$

Уколико од последње једначине одузмемо претпоследњу помножену са $k - 1$ добијамо

$$\begin{aligned} 2\sigma &= 0 \\ 2\rho &= 0 \\ \rho &= 0. \end{aligned}$$

Дакле, све се своди на

$$\begin{aligned} 2\sigma &= 0 \\ \rho &= 0. \end{aligned}$$

Према томе ради се о Абеловој групи генерисаној са два генератора σ и ρ, при чему је један од тих генератора (ρ) заправо једнак 0. Тај нам је генератор и непотребан и добијамо Абелову групу са једним генератором σ, који задовољава услов $2\sigma = 0$ и ниједан други (који није последица овог и аксиома групе). Јасно је да се ради о цикличној групи (пошто је у питању један генератор) реда два (пошто је ред тог генератора 2), те је $\mathbb{D}^{\mathrm{Ab}}_{2k+1} \cong \mathbb{Z}_2$.

$n = 2k$. Овде добијамо систем

$$\begin{aligned} 2\sigma &= 0 \\ 2\rho &= 0 \\ (2k-2)\rho &= 0. \end{aligned}$$

Одузимањем од последње једначине претпоследње помножене са $k-1$ добијамо

$$\begin{aligned} 2\sigma &= 0 \\ 2\rho &= 0 \\ 0 &= 0, \end{aligned}$$

тј. добијамо систем

$$\begin{aligned} 2\sigma &= 0 \\ 2\rho &= 0. \end{aligned}$$

Овде се ради о Абеловој групи генерисаној са два генератора σ и ρ који задовољавају само услове $2\sigma = 0$ и $2\rho = 0$ (и наравно њихове последице, које следе из аксиома групе). Дакле, једини елементи у овој групи су $0, \sigma, \rho, \sigma + \rho$, при чему међу овима нема једнаких и још је $2(\sigma + \rho) = 0$. Закључујемо да се ради о Клајновој групи и добијамо да је $\mathbb{D}^{\mathrm{Ab}}_{2k} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.

Приметимо да смо у овом разматрању користили, као што је уобичајено за Абелове (комутативне) групе адитивну нотацију, тј. операција у групи означена је са $+$, неутрал са 0, а n-ти степен елемента x означава се са nx.

Наш задатак је да покажемо да је *свака коначно генерисана Абелова група* изоморфна директном производу цикличних група. Важна је претпоставка да се ради о коначно генерисаној Абеловој групи, пошто група $(\mathbb{Q}, +)$ није изоморфна директном производу цикличних група, али она нема коначан скуп генератора (размислите како бисте показали

да она није изоморфна директном производу цикличних, можда ће вам наставак лекције помоћи у томе).

Уведимо још неке ознаке за Абелове групе. Уколико је A Абелова група, а B, C њене подгрупе, онда је

$$B + C := \{b + c : b \in B, c \in C\}.$$

Јасно је да је ово подгрупа групе A и то је заправо најмања подгрупа групе A, која садржи B и C као своје подгрупе (докажите то!). Наравно да је називамо *сума подгрупа B и C*. Уколико је $B \cap C = \{0\}$, онда је сума $B + C$ директна и пишемо $B \oplus C$ (присетите се суме векторских простора из линеарне алгебре). У случају директне суме, сваки елемент x из те суме може се *на јединствен начин* приказати у облику $x = b + c$, где b припада подгрупи B, а c подгрупи C. Наиме, како је у питању сума подгрупа, јасно је да је сваки елемент тог облика. Докажимо јединственост. Уколико је

$$x = b + c, \quad x = b_1 + c_1,$$

где $b, b_1 \in B$, $c, c_1 \in C$ онда је $b - b_1 = c_1 - c$, но овај елемент припада и подгрупи B и подгрупи C, а како је њихов пресек тривијалан то мора бити $b - b_1 = 0$ и $c_1 - c = 0$, тј. $b = b_1$ и $c = c_1$, те је приказ јединствен.

Сва ова дискусија о директној суми две подгрупе заправо показује да важи следећи изоморфизам

$$B \times C \cong B \oplus C.$$

Наиме, лако се провери да је са $f(b, c) = b + c$ задат један изоморфизам $f : B \times C \to B \oplus C$.

Као и у случају векторских простора и овде се може увести директна сума коначно много подгрупа Абелове групе (подсетите се услова) и показати да је $A_1 \times \cdots \times A_n \cong A_1 \oplus \cdots \oplus A_n$. Урадите то за вежбу.

Дакле, ми се у овој лекцији бавимо коначно генерисаним Абеловим групама. Абелова група A је коначно генерисана уколико постоји коначан подскуп $\{x_1, \ldots, x_s\} \subseteq A$ такав да важи:

$$A = \{m_1 x_1 + \cdots + m_s x_s\}$$

(подсетите се дефиниције подгрупе дефинисане неким скупом уз чињеницу да је група A Абелова). Другим речима,

$$A = \langle x_1 \rangle + \cdots + \langle x_s \rangle.$$

Према томе, свака коначно генерисана Абелова група је сума коначно много цикличних група. Наш задатак је у томе да докажемо да је свака коначно генерисана Абелова група заправо директна сума коначно много цикличних група (те је према претходним напоменама изоморфна директном производу цикличних група).

Уведимо неке неопходне појмове.

Ако је n најмањи број за који дата група A има систем од n генератора (систем од n генератора је уређена n-торка елемената групе који генеришу целу групу) и ако је $[x_1, \ldots, x_n]$ један такав систем генератора, онда за њега кажемо да је један минималан систем генератора. Важно је приметити да важи следеће.

> Ако је $[x_1, x_2, \ldots, x_n]$ минималан систем генератора и $q_2, \ldots, q_n$ ма који цели бројеви, онда је и $[x_1 + q_2x_2 + \cdots q_nx_n, x_2, \ldots, x_n]$ један минималан систем генератора.

У ову чињеницу, није се тешко уверити. Само треба показати да је и новодобијени систем такође систем генератора. За то је довољно да се покаже да се сваки од елемената $x_1, \ldots, x_n$ може добити приказати преко ових генератора, а једино што ту заиста треба проверити је да је x_1 такав. Но, то је јасно:

$$x_1 = (x_1 + q_2x_2 + \cdots q_nx_n) - q_2x_2 - \cdots - q_nx_n.$$

Дефиниција 1 Нека је $[x_1, \ldots, x_n]$ неки систем генератора. Формула облика

$$m_1x_1 + \cdots m_nx_n = 0,$$

где су $m_1, \ldots, m_n \in \mathbb{Z}$, зове се релација међу генераторима. Релација је нетривијална уколико је бар један од коефицијената m_i различит од нуле.

Наравно да би ова дефиниција требало да нас подсети на појам линеарне зависности међу векторима у векторском простору. Како радимо са Абеловим групама, овде имамо целобројне коефицијенте.

Дефиниција 2 Коначно генерисана Абелова група је слободна уколико она има систем генератора међу којима нема нетривијалних релација.

Став 3 Свака коначно генерисана слободна Абелова група изоморфна је тачно једној групи облика $\mathbb{Z}^n$ за неко $n \geqslant 1$.

Наравно, са $\mathbb{Z}^n$ означен је директан производ од n група $\mathbb{Z}$.

Доказ. Нека је A коначно генерисана слободна Абелова група и $[x_1, \ldots, x_n]$ један систем генератора међу којима нема нетривијалних релација. Дефинишимо функцију $f\colon \mathbb{Z}^n \to A$ са:

$$f(m_1, \ldots, m_n) = m_1x_1 + \cdots + m_nx_n.$$

Није тешко уверити се да је f један изоморфизам. Пре свега, јасно је да је f „на", пошто је $[x_1, \ldots, x_n]$ систем генератора, те је заиста сваки елемент у групи траженог облика. Осим тога, f је и „1–1". Наиме, ако је $f(m_1, \ldots, m_n) = f(p_1, \ldots, p_n)$ то значи да је

$$m_1x_1 + \cdots + m_nx_n = p_1x_1 + \cdots + p_nx_n.$$

Следи да је

$$(m_1 - p_1)x_1 + \cdots + (m_n - p_n)x_n = 0.$$

Како међу генераторима $x_1, \ldots, x_n$, по претпоставци, нема нетривијалних релација, закључујемо да је $m_1 - p_1 = \cdots = m_n - p_n = 0$, те је f заиста „1–1". Оставља се за (врло лаку) вежбу доказ чињенице да се f слаже са операцијама.

Дакле, доказали смо да је свака коначно генерисана слободна Абелова група изоморфна некој од група $\mathbb{Z}^n$. Остаје да докажемо јединственост, тј. да из $\mathbb{Z}^m \cong \mathbb{Z}^n$ следи да је $m = n$.

Претпоставимо, стога, да је $\mathbb{Z}^m \cong \mathbb{Z}^n$ и да је $m \leqslant n$. Искористићемо знање линеарне алгебре. Наиме, у групи $\mathbb{Z}^n$ налазе се канонски генератори

$$\begin{array}{rcl} e_1 & = & (1, 0, \ldots, 0) \\ e_2 & = & (0, 1, \ldots, 0) \\ \vdots & \vdots & \vdots \quad \vdots \quad \vdots \quad \vdots \\ e_n & = & (0, 0, \ldots, 1) \end{array}$$

n-димензионалног векторског простора $\mathbb{R}^n$. Нека је $h\colon \mathbb{Z}^m \to \mathbb{Z}^n$ један изоморфизам. Генератори групе $\mathbb{Z}^m$ су наравно

$$\begin{array}{rcl} e'_1 & = & (1, 0, \ldots, 0) \\ e'_2 & = & (0, 1, \ldots, 0) \\ \vdots & \vdots & \vdots \quad \vdots \quad \vdots \quad \vdots \\ e'_m & = & (0, 0, \ldots, 1) \end{array}$$

и има их m. За сваки генератор e_i групе $\mathbb{Z}^n$ постоје цели бројеви $a_{i1}, \ldots, a_{im}$ такви да је

$$e_i = h(a_{i1}e'_1 + \cdots + a_{im}e'_m) = a_{i1}h(e'_1) + \cdots + a_{im}h(e'_m).$$

Из овога следи, ако сада посматрамо реални векторски простор $\mathbb{R}^n$, да је сваки од вектора базе тог простора добијен као линерна комбинација m вектора: $h(e'_1), \ldots, h(e'_m)$. Но, ми знамо да n-димензионални векторски простор не може бити генерисан са мање од n вектора. Другим речима, мора бити $m \geqslant n$, те закључујемо да је $m = n$ што и завршава тражени доказ. □

Докажимо најпре два става, који су од општег значаја, а користићемо их у даљем.

Став 4 Нека су G_1, G_2 групе и $H_1 \triangleleft G_1$, $H_2 \triangleleft G_2$. Тада је $H_1 \times H_2 \triangleleft G_1 \times G_2$ и

$$G_1 \times G_2 / H_1 \times H_2 \cong G_1/H_1 \times G_2/H_2.$$

Доказ. Јасно је да $H_1 \times H_2 \neq \emptyset$, јер $(e_1, e_2) \in H_1 \times H_2$ (наравно, са e_i означен је неутрал у групи G_i). Ако $(h_1, h_2), (h_1', h_2') \in H_1 \times H_2$, онда је и $(h_1, h_2)^{-1}(h_1', h_2') = (h_1^{-1}, h_2^{-1})(h_1', h_2') = (h_1^{-1}h_1', h_2^{-1}h_2') \in H_1 \times H_2$, те је, заиста, $H_1 \times H_2$ подгрупа од $G_1 \times G_2$. Ова подгрупа је и нормална, јер из $(h_1, h_2) \in H_1 \times H_2$ и $(g_1, g_2) \in G_1 \times G_2$ следи да је

$$(g_1, g_2)(h_1, h_2)(g_1, g_2)^{-1} = (g_1, g_2)(h_1, h_2)(g_1^{-1}, g_2^{-1}) = (g_1 h_1 g_1^{-1}, g_2 h_2 g_2^{-1}),$$

а овај елемент припада $H_1 \times H_2$, јер су подгрупе H_1 и H_2 нормалне.

Дефинишимо $f: G_1/H_1 \times G_2/H_2 \to G_1 \times G_2/H_1 \times H_2$ са:

$$f(g_1H_1, g_2H_2) = (g_1, g_2)H_1 \times H_2.$$

Проверимо најпре добру дефинисаност f.

$$\begin{aligned}
& (g_1H_1, g_2H_2) = (g_1'H_1, g_2'H_2) \\
\Rightarrow\ & g_1H_1 = g_1'H_1, g_2H_2 = g_2'H_2 \\
\Rightarrow\ & g_1^{-1}g_1' \in H_1, g_2^{-1}g_2' \in H_2 \\
\Rightarrow\ & (g_1^{-1}g_1', g_2^{-1}g_2') \in H_1 \times H_2 \\
\Rightarrow\ & (g_1, g_2)^{-1}(g_1', g_2') \in H_1 \times H_2 \\
\Rightarrow\ & (g_1, g_2)H_1 \times H_2 = (g_1', g_2')H_1 \times H_2.
\end{aligned}$$

На сличан начин се проверава да је f „1–1”.

$$\begin{aligned}
& f(g_1H_1, g_2H_2) = f(g_1'H_1, g_2'H_2) \\
\Rightarrow\ & (g_1, g_2)H_1 \times H_2 = (g_1', g_2')H_1 \times H_2 \\
\Rightarrow\ & (g_1, g_2)^{-1}(g_1', g_2') \in H_1 \times H_2 \\
\Rightarrow\ & (g_1^{-1}g_1', g_2^{-1}g_2') \in H_1 \times H_2 \\
\Rightarrow\ & g_1^{-1}g_1' \in H_1, g_2^{-1}g_2' \in H_2 \\
\Rightarrow\ & g_1H_1 = g_1'H_1, g_2H_2 = g_2'H_2.
\end{aligned}$$

Како је f очигледно „на” (зашто је f „на”?), то остаје да се провери да се f слаже са операцијама.

$$\begin{aligned}
f((g_1H_1, g_2H_2)(g_1'H_1, g_2'H_2) &= f((g_1g_1')H_1, (g_2g_2')H_2) \\
&= (g_1g_1', g_2g_2')H_1 \times H_2 \\
&= ((g_1, g_2)(g_1', g_2'))H_1 \times H_2 \\
&= (g_1, g_2)H_1 \times H_2 \cdot (g_1', g_2')H_1 \times H_2 \\
&= f(g_1H_1, g_2H_2)f(g_1'H_1', g_2'H_2).
\end{aligned}$$

□

Дефинишимо једну важну подгрупу сваке Абелове групе. То је торзиона подгрупа.

Дефиниција 5 Нека је A Абелова група. Са $T(A)$ означавамо скуп свих елемената из A који су коначног реда.

Покажимо да је $T(A)$ заиста подгрупа од A (у односу на рестрикцију операције са A). Наиме, $0 \in T(A)$. Осим тога, ако $x, y \in T(A)$, то жачи да постоје $m, n > 0$ за које је $mx = 0$ и $ny = 0$. Но, тада је $mn(x-y) = mnx - mny = nmx - mny = n0 - m0 = 0$, те је и елемент $x-y$ коначог реда.

Став 6 Нека су A и B изоморфне Абелове групе. Тада је и $T(A) \cong T(B)$ и $A/T(A) \cong B/T(B)$.

Доказ. Нека је $f\colon A \to B$ изоморфизам. Покажимо да је $f[T(A)] = T(B)$, из чега ће следити да рестрикција f на $T(A)$ успоставља први тражени изоморфизам. Но, како је f изоморфизам, то за сваки елемент $x \in A$ важи: $\omega(x) = \omega(f(x))$ ово показује да се елемент коначног реда слика у елемент коначног реда, тј. да је $f[T(A)] \subseteq T(B)$. Нека је $y \in T(B)$. Како је f „на", то постоји $x \in A$ за који је $f(x) = y$. Но, како је $\omega(y) = \omega(f(x)) = \omega(x)$, то је и x коначног реда, тј. $x \in T(A)$. Закључујемо да је заиста $f[T(A)] = T(B)$.

Докажимо да је и $A/T(A) \cong B/T(B)$. Дефинишемо $\tilde{f}\colon A/T(A) \to B/T(B)$ са: $\tilde{f}(a + T(A)) := f(a) + T(B)$. Функција $\tilde{f}$ јесте добро дефинисана. Наиме, ако је $a + T(A) = a' + T(A)$, то жачи да је $a - a' \in T(A)$. Но, тада је и $f(a) - f(a') = f(a - a') \in f[T(A)] = T(B)$, те је $f(a) + T(B) = f(a') + T(B)$.

Покажимо да је $\tilde{f}$ „1–1". Нека је $\tilde{f}(a+T(A)) = \tilde{f}(a'+T(A))$. То жачи да је $f(a) + T(B) = f(a') + T(B)$, те је $f(a - a') = f(a) - f(a') \in T(B)$, те је и елемент $a - a'$ коначног реда, тј. $a - a' \in T(A)$, па следи да је $a + T(A) = a' + T(A)$.

Нека је $b + T(B)$ произвољан елемент из $B/T(B)$. Како је f „на", то постоји $a \in A$ тако да је $b = f(a)$. Но, тада је $b + T(B) = f(a) + T(B) = \tilde{f}(a + T(A))$. Закључујемо да је $\tilde{f}$ и „на".

Остаје да се покаже да се $\tilde{f}$ слаже са операцијама.

$$\begin{aligned}
\tilde{f}((a + T(A)) + (a' + T(A))) &= \tilde{f}((a + a') + T(A)) \\
&= f(a + a') + T(B) \\
&= (f(a) + f(a')) + T(B) \\
&= (f(a) + T(B)) + (f(a') + T(B)) \\
&= \tilde{f}(a + T(A)) + \tilde{f}(a' + T(A)).
\end{aligned}$$

□

Следећи једноставан став је веома користан.

Став 7 Нека је $q \in \mathbb{Z} \setminus \{0\}$ и $n \geq 2$. Тада је број решења једначине $qx = 0$ у групи $\mathbb{Z}_n$ једнак $\mathrm{NZD}(q, n)$.

Доказ. Нека је $x \in Z_n = \{0, 1, \ldots, n-1\}$. Тада је

$$qx = 0 \text{ у групи } \mathbb{Z}_n \textbf{ акко } n \mid qx \text{ у } \mathbb{Z}.$$

Нека је $d = \text{NZD}(q, n)$. То значи да је $q = dq_1$ и $n = dn_1$, при чему је $\text{NZD}(q_1, n_1) = 1$. Како $n \mid qx$, то $dn_1 \mid dq_1x$, па $n_1 \mid q_1x$. Како су n_1 и q_1 узајамно прости, добијамо да $n_1 \mid x$. Дакле, за $x \in \{0, 1, \ldots, n-1\}$ важи: $qx = 0$ у групи $\mathbb{Z}_n$ ако и само ако је $x \in \{0, n_1, 2n_1, \ldots, (d-1)n_1\}$. Закључујемо да једначина $qx = 0$ у групи $\mathbb{Z}_n$ заиста има $d = \text{NZD}(q, n)$ решења. □

Последица 8 Број решења једначине $qx = 0$ у групи $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$ једнак је $\text{NZD}(q, n_1)\text{NZD}(q, n_2) \cdots \text{NZD}(q, n_k)$.

Доказ. Овај резултат непосредно следи из претходног става. Наиме, ако је $x = (x_1, x_2, \ldots, x_k) \in Z_{n_1} \times Z_{n_2} \times \cdots Z_{n_k}$, то је $qx = 0$ ако и само ако је за све $i = \overline{1,k}$: $qx_i = 0$. С обзиром да је, према претходном ставу, број решења једначине $qx_i = 0$ у групи $\mathbb{Z}_{n_i}$ једнак $\text{NZD}(q, n_i)$, то тражени резултат следи. □

Урадимо један пример примене претходно доказаног.

Пример 9 У групи $\mathbb{Z}_5 \times \mathbb{Z}_{10} \times \mathbb{Z}_{60}$ одредити број елемената реда 3, 6 и 12.

Означимо нашу групу са A. Тада је број елемената реда 3 у A за један мањи од броја решења једначине $3x = 0$ у A (пошто је 0 такође једно решење ове једначине, а то је неутрал, те није елемент реда 3). Дакле, број елемената реда 3 у овој групи једнак је:

$$\text{NZD}(3,5)\text{NZD}(3,10)\text{NZD}(3,60) - 1 = 1 \cdot 1 \cdot 3 - 1 = 2.$$

Нешто је сложеније одређивање елемената реда 6. Наиме сваки елемент реда 6 јесте решење једначине $6x = 0$ у A, али су и елементи реда 2 и реда 3 такође решења ове једначине. Заправо:

$$\{x \in A : \omega(x) = 6\} = \{x \in A : 6x = 0, 2x \neq 0, 3x \neq 0\}.$$

Дакле, треба одредити број елемената у скупу

$$\{x \in A : 6x = 0\} \setminus (\underbrace{\{x \in A : 2x = 0\}}_{B} \cup \underbrace{\{x \in A : 3x = 0\}}_{C}).$$

По добро познатој формули: $|B \cup C| = |B| + |C| - |B \cap C|$. Но,

$$x \in B \cap C \text{ акко } 2x = 0 \text{ и } 3x = 0.$$

Закључујемо да је $B \cap C = \{0\}$. Број елемената у B је, према претходној последици, једнак $\text{NZD}(2,5)\text{NZD}(2,10)\text{NZD}(2,60) = 1 \cdot 2 \cdot 2 = 4$. На исти начин се добије да је $|C| = 1 \cdot 1 \cdot 3 = 3$, док је $|\{x \in A : 6x = 0\}| = 1 \cdot 2 \cdot 6 = 12$. Добијамо да је број елемената реда 6 у групи A једнак $12 - (4 + 3 - 1) = 6$.

Најсложеније је одређивање броја елемената реда 12. Наиме,

$$\{x \in A : \omega(x) = 12\} = \{x \in A : 12x = 0, dx \neq 0, \text{ за све } d \text{ за које је } 1 \leqslant d < 12\}.$$

Није тешко уверити се да се ово може поједноставити, тј. да је

$$\{x \in A : (\exists d)(1 \leqslant d < 12 \wedge dx = 0)\} = \underbrace{\{x \in A : 4x = 0\}}_{D} \cup \underbrace{\{x \in A : 6x = 0\}}_{E}.$$

Приметимо да је $D \cap E = \{x \in A : 6x = 0, 4x = 0\} = \{x \in A : 2x = 0\}$. Како је

$$\begin{aligned}
|\{x \in A : 12x = 0\}| &= \mathrm{NZD}(12,5)\mathrm{NZD}(12,10)\mathrm{NZD}(12,60) = 1 \cdot 2 \cdot 12 = 24 \\
|\{x \in A : 4x = 0\}| &= \mathrm{NZD}(4,5)\mathrm{NZD}(4,10)\mathrm{NZD}(4,60) = 1 \cdot 2 \cdot 4 = 8 \\
|\{x \in A : 6x = 0\}| &= \mathrm{NZD}(6,5)\mathrm{NZD}(6,10)\mathrm{NZD}(6,60) = 1 \cdot 2 \cdot 6 = 12 \\
|\{x \in A : 2x = 0\}| &= \mathrm{NZD}(2,5)\mathrm{NZD}(2,10)\mathrm{NZD}(2,60) = 1 \cdot 2 \cdot 2 = 4,
\end{aligned}$$

то је број елемената реда 12 у групи A једнак: $24 - (8 + 12 - 4) = 8$. ♣

Користећи до сада урађено, можемо доказати следећи став.

Став 10 Нека су $k, l, s, t \geq 0$ и $d_1, \ldots, d_k, r_1, \ldots, r_l$ природни бројеви такви да је $d_1 > 1$, $r_1 > 1$, $d_i \mid d_{i+1}$, за $i = \overline{1, k-1}$ и $r_j \mid r_{j+1}$, за $j = \overline{1, l-1}$. Тада из

$$\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_k} \times \mathbb{Z}^s \cong \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \times \cdots \times \mathbb{Z}_{r_l} \times \mathbb{Z}^t$$

следи: $s = t$, $k = l$ и $d_i = r_i$ за све $i = \overline{1, k}$.

Доказ. У доказу ћемо користити став 6. У ту сврху, одредимо торзионе подгрупе наведених група. Важи следеће:

$$T(\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_k} \times \mathbb{Z}^s) = \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_k} \times \{0\}^s.$$

Наиме, нека је $x = (x_1, \ldots, x_k, y_1, \ldots, y_s) \in \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_k} \times \mathbb{Z}^s$. Уколико је за бар једно j_0: $y_{j_0} \neq 0$, онда за ма које $n \geq 1$ важи: $n(x_1, \ldots, x_k, y_1, \ldots, y_s) = (nx_1, \ldots, nx_k, ny_1, \ldots, ny_s) \neq (0, \ldots, 0, 0, \ldots, 0)$, јер $ny_{j_0} \neq 0$. Дакле, такав елемент не може бити коначног реда. С друге стране, јасно је да је $d_k(x_1, \ldots, x_k, 0, \ldots, 0) = (0, \ldots, 0, 0, \ldots, 0)$ те закључујемо да је торзиона група заиста горенаведена подгрупа. Из става 6 следи да су за дате групе изоморфне њихове торзионе подгрупе и одговарајуће количничке групе, што, уз примену става 4 (како се тачно тај став примењује?) следи да је

$$\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_k} \cong \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \times \cdots \times \mathbb{Z}_{r_l} \text{ и } \mathbb{Z}^s \cong \mathbb{Z}^t.$$

На основу става 3 добијамо да је $s = t$. Концентришимо се сада на изоморфизам

$$\mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_k} \cong \mathbb{Z}_{r_1} \times \mathbb{Z}_{r_2} \times \cdots \times \mathbb{Z}_{r_l}.$$

Претпоставимо, на пример, да је $k \geqslant l$. Ако са L означимо групу са леве стране, а са D групу са десне стране, посматрајмо број решења једначине $d_1 x = 0$ у овим групама. Како су оне изоморфне, то постоји

и бијекција између скупа решења ових једначина (уверите се у то!). Но, број решења ове једначине у групи L једнак је

$$\mathrm{NZD}(d_1, d_1)\mathrm{NZD}(d_1, d_2)\cdots\mathrm{NZD}(d_1, d_k) = d_1 \cdot d_1 \cdots d_1 = d_1^k,$$

с обзиром на чињеницу да $d_1 \mid d_i$ за све $i \geqslant 1$. У групи D, број решења ове једначине једнак је

$$\mathrm{NZD}(d_1, r_1)\mathrm{NZD}(d_1, r_2)\cdots\mathrm{NZD}(d_1, r_l),$$

при чему је сваки од фактора у производу не већи од d_1. С обзиром да је овај производ једнак d_1^k и да је $k \geqslant l$, мора бити $k = l$ и морају сви фактори у овом производу бити једнаки d_1. Одавде следи да $d_1 \mid r_1$. Уколико бисмо сада посматрали број решења једначине $r_1 x = 0$ у овим групама, на исти начин бисмо добили да $r_1 \mid d_1$. Закључујемо да смо добили да је $k = l$ и $d_1 = r_1$.

Посматрајмо сада број решења једначине $d_2 x = 0$ у овим групама. Број решења ове једначине у групи L је $d_1 d_2^{k-1}$, док је у групи D тај број $d_1 s_2 \ldots s_k$ при чему је $s_i \leqslant d_i$ за све $i \geqslant 2$. Добијамо да је $d_1 d_2^{k-1} = d_1 s_2 \ldots s_k$. Скраћивањем са d_1 и коришћењем чињенице да је $s_i \leq d_i$, добијамо да мора бити $s_i = d_i$ за све $i \geqslant 2$. То посебно значи да $d_2 \mid r_2$. На исти начин као и пре, посматрањем броја решења једначине $r_2 x = 0$ у овим групама, добијамо да $r_2 \mid d_2$, па мора бити $d_2 = r_2$. Настављањем овог поступка добијамо да је за све $i = \overline{1, k}$: $d_i = r_i$, што је и требало доказати. □