АЛГЕБРА
Коначно генерисане Абелове групе

Зоран Петровић

Осмо предавање

Абелове, или комутативне, групе су оне групе у којима свака два елемента комутирају, тј. за свака два елемента x и y Абелове групе G важи: $xy = yx$. Често се, а то ћемо и ми урадити, у случају да се разматрају Абелове групе, за операцију у групи користи ознака $+$, а за неутрал 0.

Као што се сећамо, диедарска група $\mathbb{D}_n$ може се задати са два генератора r и s између којих важе релације:

$$s^2 = e, \quad r^n = e, \quad sr = r^{n-1}s.$$

Знамо да та група има сложену и занимљиву структуру. Претпоставимо да сада разматрамо *Абелову групу* задату са два генератора r, и s и релацијама

$$2s = 0, \quad nr = 0, \quad s + r = (n-1)r + s.$$

Видимо да нам последња релација даје $(n-2)r = 0$, а из те релације и друге релације добијамо да је $2r = 0$. Сада разликујемо два случаја.

1. $\underline{n = 2k+1}$: Тада, из $2r = 0$ и $(2k+1)r = 0$, добијамо да је $r = 0$. Дакле, довољан је заправо само један генератор s и за њега важи $2s = 0$. Видимо да је дата група изоморфна групи $\mathbb{Z}_2$.

2. $\underline{n = 2k}$: Видимо да је тада релација $nr = 0$ последица релације $2r = 0$, те заправо имамо групу са два генератора r и s и две релације $2r = 0$ и $2s = 0$. Закључујемо да је група о којој се ради изоморфна групи $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Напомена: Заправо је група коју смо разматрали ништа друго до Абелизација диедарске групе, па смо добили резултат, који смо и очекивали.

Видимо да смо без већих проблема били у могућности да идентификујемо о којој се групи заправо ради само на основу генератора и релација међу њима. То је тако у случају произвољне Абелове групе са коначно много генератора. Испоставља се да је свака коначно генерисана Абелова група изоморфна директном производу цикличних група. Наравно да овако нешто ни приближно не важи за произвољне групе!

Уведимо још неку терминологију карактеристичну за Абелове групе. Ако су B, C подгрупе Абелове групе A, нека је

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

Заправо је $B + C$ најмања подгрупа групе A, која садржи као своје подгрупе и подгрупу B и подгрупу C. Природно је звати је сумом подгрупа B и C. Уколико за те подгрупе важи и $B \cap C = \{0\}$, говоримо о директној суми подгрупа, у ознаци $B \oplus C$. Као и код векторских простора, у случају директне суме сваки елемент те суме се на јединствен начин може приказати у облику збира једног елемента из B и једног елемента из C. Општије, уколико су $B_1, \ldots, B_n$ подгрупе Абелове групе A, онда се дефинише њихова сума $B_1 + \cdots + B_n$ са:

$$B_1 + \cdots + B_n := \{b_1 + \cdots + b_n : b_i \in B_i \text{ за све } i = \overline{1, n}\}.$$

Ова сума је директна уколико се сваки елемент из те суме на тачно један начин може представити у наведеном облику. Еквивалентно, сума је директна уколико за све $i = \overline{2, n}$ важи:

$$(B_1 + \cdots + B_{i-1}) \cap B_i = \{0\}.$$

Није тешко уверити се да је

$$B_1 \oplus B_2 \oplus \cdots \oplus B_n \cong B_1 \times B_2 \times \cdots \times B_n,$$

где наравно $B_1 \oplus B_2 \oplus \cdots \oplus B_n$ означава директну суму. Изоморфизам

$$f \colon B_1 \times B_2 \times \cdots \times B_n \to B_1 \oplus B_2 \oplus \cdots \oplus B_n$$

дат је са: $f(b_1, b_2, \ldots, b_n) = b_1 + b_2 + \cdots + b_n$.

Пре него што пређемо на општи случај, позабавићемо се најпре појмом *слободне Абелове групе* (са коначно много генератора).

Дефиниција 1 Нека је F Абелова група и $x_1, \ldots, x_n \in F$. Тада је F слободна Абелова група са системом слободних генератора $[x_1, \ldots, x_n]$ уколико за сваку Абелову групу A и елементе $a_1, \ldots, a_n \in A$ постоји тачно један хомоморфизам $f \colon F \to A$ за који је $f(x_i) = a_i$ за све $i = \overline{1, n}$.

Ово би требало да нас подсети на став о одређености линеарног пресликавања из предмета Линеарна алгебра (линеарно пресликавање је у потпуности задато када је задато на базним векторима).

Приметимо најпре да међу слободним генераторима не сме бити никаквих релација. Другим речима, важи следећи став.

Став 2 Ако је F слободна Абелова група са системом слободних генератора $[x_1, \ldots, x_n]$ и ако је

$$m_1 x_1 + \cdots + m_n x_n = 0,$$

за неке $m_i \in \mathbb{Z}$, онда мора бити $m_1 = \cdots = m_n = 0$.

Доказ. Претпоставимо да бар један од m_i није једнак нули. Нека је то нпр. m_2. Уочимо Абелову групу $\mathbb{Z}$ и елемент $1 \in \mathbb{Z}$. По дефиницији слободне Абелове групе, постоји тачно један хомоморфизам $f\colon F \to \mathbb{Z}$ такав да је $f(x_2) = 1$ и $f(x_i) = 0$ за све $i \neq 2$. Но, то значи да се елемент $m_1x_1 + \cdots + m_nx_n$, који је по претпоставци једнак 0 у F, слика у елемент $m_2 \neq 0$ у $\mathbb{Z}$. Ова контрадикција нам показује да су сви m_i једнаки нули. □

Наведени став појашњава терминологију—група је слободна зато што има генераторе међу којима не постоје везе (као у песми: „Остаћу слободан, нећу се везати, важно је само ...").

Испоставља се да су две слободне Абелове групе са истим бројем слободних генератора изоморфне.

Став 3 Нека је F слободна Абелова група са системом слободних генератора $[x_1, \dots, x_n]$ и F' слободна Абелова група са системом слободних генератора $[x'_1, \dots, x'_n]$. Тада је $F \cong F'$.

Доказ. На основу дефиниције слободне Абелове групе, постоји тачно један хомоморфизам $f\colon F \to F'$ и тачно један хоморфизам $g\colon F' \to F$ за које је $f(x_i) = x'_i$ и $g(x'_i) = x_i$ за све $i = \overline{1,n}$. Но, тада је за све $i = \overline{1,n}$, $(g \circ f)(x_i) = x_i$ и $(f \circ g)(x'_i) = x'_i$. Како и идентични хомоморфизми id_F, односно $\mathrm{id}_{F'}$ имају иста својства, то, на основу јединствености, закључујемо да је

$$g \circ f = \mathrm{id}_F, \quad f \circ g = \mathrm{id}_{F'}.$$

Одавде следи да је $F \cong F'$. □

Став 4 Група $\mathbb{Z}^n$ је слободна Абелова група са слободним системом генератора

$$[(1,0,\dots,0),(0,1,\dots,0),\dots,(0,0,\dots,1)].$$

Доказ. Треба показати да су испуњени наведени услови из дефиниције. У ту сврху, нека је A произвољна Абелова група и $a_1, \dots, a_n \in A$. Тада је хомоморфизам $f\colon \mathbb{Z}^n \to A$ задат са:

$$f(m_1, m_2, \dots, m_n) := m_1a_1 + m_2a_2 + \cdots + m_na_n.$$

Није тешко проверити да је f заиста хомоморфизам. Осим тога

$$f(1,0,\dots,0) = m_1, \quad f(0,1,\dots,0) = m_2, \quad \cdots \quad , f(0,0,\dots,1) = m_n.$$

Наравно, јасно је и да је ово једини начин да се зада тражени хомоморфизам. □

Дакле, свака слободна Абелова група са коначним системом генератора изоморфна је једној од група $\mathbb{Z}^n$ за неко $n \geq 1$. Важи и више од тога.

Став 5 Ако је $\mathbb{Z}^r \cong \mathbb{Z}^s$, онда је $r = s$.

Доказ. Претпоставимо да је $r \leq s$. У доказу ћемо користити знање Линеарне алгебре. Наиме, приметимо да се у групи $\mathbb{Z}^s$ налазе и елементи канонске базе векторског простора $\mathbb{R}^s$, тј. вектори

$$e_1 = (1, 0, \dots,), \quad e_2 = (0, 1, \dots, 0), \quad \dots \quad , e_s = (0, 0, \dots 1).$$

То значи да су сви наведени базни вектори целобројне линеарне комбинације од r вектора

$$f(1, 0, \dots, 0), f(0, 1, \dots, 0), \dots, f(0, 0, \dots, 1),$$

где је f изоморфизам који постоји по претпоставци. То значи да тих r вектора чини генератрису простора $\mathbb{R}^s$ који је димензије s. Но, знамо да не може мање од s вектора генерисати векторски простор димензије s. Стога мора бити $r \geq s$. Како смо претпоставили да је $r \leq s$, добијамо да је $r = s$. □

Да резимирамо. Свака слободна Абелова група са коначно много генератора изоморфна је тачно једној од група $\mathbb{Z}^n$ за неко $n \geq 1$. Посебно, две слободне Абелове групе са коначно много генератора су изоморфне ако и само ако имају исти број генератора.

Позабавимо се сада подгрупама слободних Абелових група. У случају групе са једним генератором, тј. бесконачне цикличне групе, одговор нам је добро познат. Свака подгрупа слободне групе са једним слободним генератором x је генерисана елементом nx за неко $n \geq 0$. Случај у коме имамо више генератора је знатно сложенији.

Пошто ћемо у доказима који следе често прелазити са једног система генератора на други, корисно је издвојити следећу лему.

Лема 6 Ако је $[x_1, x_2, \dots, x_n]$ систем слободних генератора и $t_2, \dots, t_n \in \mathbb{Z}$, онда је и

$$[x_1 + t_2 x_2 + \dots + t_n x_n, x_2, \dots, x_n]$$

систем слободних генератора.

Доказ. Како је јасно да се генератори из првог система на јединствен начин могу изразити преко генератора из другог система, то резултат непосредно следи. □

Пређимо на главни резултат о подгрупама слободних Абелових група са коначно много генератора.

Теорема 7 Нека је F слободна Абелова група са n слободних генератора и R подгрупа од F. Тада постоји систем слободних генератора $[x_1, x_2, \dots, x_n]$ групе F и ненегативни цели бројеви $d_1, d_2, \dots, d_n$ за које је

$$R = \langle d_1 x_1 \rangle \oplus \langle d_2 x_2 \rangle \oplus \dots \oplus \langle d_n x_n \rangle,$$

при чему $d_i \mid d_{i+1}$ за све $i = \overline{1, n-1}$.

Напомена. Пре доказа ове теореме, потребно је истаћи да је могуће да неки од бројева d_i буду једнаки 0. Но, ту се подразумева да ако је неки d_k једнак 0, то су и сви d_i за $i \geq k$ (пошто $d_i \mid d_{i+1}$ — још можемо да „поднесемо” да напишемо да $0 \mid 0$, али да 0 дели неки број различит од 0 заиста нема никаквог смисла!).

Доказ теореме. Доказ изводимо по броју n, тј. по броју слободних генератора групе.

$n = 1$. У овом случају је све јасно као што смо већ напоменули.

Претпоставимо да је $n > 1$ и да је тврђење тачно за слободне групе са мање од n генератора. Наравно, уколико $R = \{0\}$, немамо шта да доказујемо, тада су сви d_i једнаки нули, а и систем слободних генератора је ма који. Претпоставимо стога да је R нетривијална подгрупа. Број d_1 задајемо са:

$$d_1 := \min\{m_1 > 0 : \text{ за неки систем слободних генератора}$$
$$[x_1, \dots, x_n] \text{ и неке } m_2, \dots, m_n \in \mathbb{Z}, m_1x_1 + \cdots + m_nx_n \in R\}.$$

Да појаснимо мало како смо задали d_1. Посматрамо све могуће системе слободних генератора (обратите пажњу на чињеницу да разматрамо *систем*, дакле уређену n-торку, а не скуп — као и у Линеарној алгебри база је уређена n-торка вектора, а не само скуп вектора) и све линеарне комбинације елемената тог система, које припадају подгрупи R. Како је подгрупа нетривијална, то за сваки систем постоји бар једна нетривијална линеарна комбинација у тој подгрупи. Осим тога, како је R подгрупа, са сваким својим елементом садржи и његов супротан елемент те стога има линеарних комбинација са позитивним коефицијентима. Такође, пермутовањем чланова система постижемо да је баш први коефицијент позитиван. У сваком случају, d_1 јесте добро дефинисан позитиван цео број.

Покажимо најпре да постоји бар један систем слободних генератора $[y_1, \dots, y_n]$ такав да $d_1y_1 \in R$.

На основу дефиниције d_1, постоји неки систем слободних генератора $[x_1, \dots, x_n]$ и цели бројеви $m_2, \dots, m_n$ тако да

$$d_1x_1 + m_2x_2 + \cdots + m_nx_n \in R.$$

Докажимо да тада $d_1 \mid m_i$ за све $i = \overline{2, n}$. Претпоставимо да то није тачно и нека нпр. d_1 не дели m_2. То значи да постоје цели бројеви q и r за које важи:

$$m_2 = d_1q + r, \quad 0 < r < d_1.$$

Тада је

$$\begin{aligned} d_1x_1 + m_2x_2 + \cdots + m_nx_n &= d_1x_1 + (d_1q + r)x_2 + \cdots + m_nx_n \\ &= d_1(x_1 + qx_2) + rx_2 + \cdots + m_nx_n \\ &= rx_2 + d_1(x_1 + qx_2) + \cdots + m_nx_n. \end{aligned}$$

На основу Леме 6, систем $[x_2, x_1 + qx_2, \dots, x_n]$ је такође систем слободних генератора (зашто?), а први коефицијент у приказу једног елемента из R у том систему је мањи од d_1, који је по претпоставци најмањи такав. Закључујемо да $d_1 \mid m_i$ за све $i = \overline{2,n}$. То значи да је $m_i = d_1 t_i$ за све $i = \overline{2,n}$ и неке $t_i \in \mathbb{Z}$. Дакле,

$$d_1(x_1 + t_2 x_2 + \cdots + t_n x_n) \in R.$$

Тражени систем је $[x_1 + t_2 x_2 + \cdots + t_n x_n, x_2, \dots, x_n]$.

Дакле, показали смо да за бар један слободан систем генератора $[y_1, y_2, \dots, y_n]$ елемент $d_1 y_1$ припада R. Нека је $R_1 = \langle y_2, \dots, y_n \rangle \cap R$, где је са $\langle y_2, \dots, y_n \rangle$ наравно означена подгрупа од F коју генеришу $y_2, \dots, y_n$. Тврдимо да је тада

$$R = \langle d_1 y_1 \rangle \oplus R_2.$$

Најпре је

$$\langle d_1 y_1 \rangle \cap R_2 \subseteq \langle y_1 \rangle \cap \langle y_2, \dots, y_n \rangle = \{0\},$$

пошто су $y_1, y_2, \dots, y_n$ слободни генератори и међу њима нема нетривијалних веза. Стога је сума $\langle d_1 y_1 \rangle + R_1$ заиста директна. Да бисмо показали да је та сума једнака R, узмимо ма који елемент $x \in R$. То значи да је за неке $m_i \in \mathbb{Z}$:

$$x = m_1 y_1 + m_2 y_2 + \ldots + m_n y_n.$$

Уколико m_1 није дељив са d_1, постоје q_1 и r_1 такви да је $m_1 = d_1 q_1 + r_1$, при чему је $0 < r_1 < d_1$. Но, тада

$$r_1 y_1 + m_2 y_2 + \ldots + m_n y_n = x - q d_1 y_1 \in R,$$

а како је $0 < r_1 < m_1$, то противречи избору d_1. Дакле, заиста $d_1 \mid m_1$, те је $m_1 = q_1 d_1$. Добијамо да је

$$x = q_1(d_1 y_1) + (m_2 y_2 + \cdots + m_n y_n) \in \langle d_1 y_1 \rangle + R_1.$$

Како је R_1 подгрупа слободне Абелове групе са мање од n генератора, по индуктивној хипотези следи да за неки слободан систем генератора $[z_2, \dots, z_2]$ те слободне групе и неке $d_i \geq 0$ такве да $d_i \mid d_{i+1}$ за $i = \overline{2, n-1}$ важи

$$R_1 = \langle d_2 z_2 \rangle \oplus \cdots \oplus \langle d_n z_n \rangle.$$

Дакле, заиста је

$$R = \langle d_1 y_1 \rangle \oplus \langle d_2 z_2 \rangle \oplus \cdots \oplus \langle d_n z_n \rangle$$

за неки слободан систем генератора $[y_1, z_2, \dots, z_n]$ слободне групе F. Остаје само да се покаже да је $d_1 \mid d_2$. Но, поступамо као и раније.

Уколико d_1 не дели d_2, запишемо d_2 у облику $d_2 = qd_1 + r$, где је $0 < r < d_1$. Како је

$$d_1 y_1 + d_2 z_2 + \cdots + d_n z_n \in R,$$

то добијамо

$$rz_2 + d_1(y_1 + qz_2) + \cdots + d_n z_n \in R,$$

а како је $0 < r < d_1$ и $[z_2, y_1 + qz_2, \dots, z_n]$ један систем слободних генератора, то смо добили контрадикцију с обзиром на избор броја d_1. Дакле, заиста $d_1 \mid d_2$ и доказ је завршен. $\square$

Искористићемо претходно добијену теорему о подгрупама слободне групе за доказ чињенице да је свака коначно генерисана Абелова група изоморфна директном производу цикличних група.

Теорема 8 Нека је A коначно генерисана Абелова група. Тада постоје позитивни цели бројеви $d_1, \dots, d_k$ и природан број s такви да $d_i \mid d_{i+1}$ за све $i = \overline{1, k-1}$ и да је

$$A \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_k} \times \mathbb{Z}^s. \tag{1}$$

Доказ. Како је A коначно генерисана, то постоји коначно много елемената $a_1, \dots, a_n \in A$ тако да је $A = \langle a_1, \dots, a_n \rangle$. Нека је F слободна група са n генератора $x_1, \dots, x_n$. На основу дефиниције слободне групе и чињенице да су a_i генератори групе A, добијамо да постоји епиморфизам $f\colon F \to A$ задат са $f(x_i) = a_i$ за $i = \overline{1, n}$ (подсетимо се да је епиморфизам заправо хомоморфизам који је „на”). На основу прве теореме о изоморфизму група следи да је $F/R \cong A$, где је $R = \mathrm{Ker}(f)$. На основу теореме о подгрупама слободне групе, следи да постоје слободни генератори $y_1, y_2, \dots, y_n$ групе F и ненегативни цели бројеви d_i такви да је $R = \langle d_1 y_1 \rangle \oplus \langle d_2 y_2 \rangle \oplus \cdots \oplus \langle d_n y_n \rangle$. Како је $F = \langle y_1 \rangle \oplus \langle y_2 \rangle \oplus \cdots \oplus \langle y_n \rangle$ (зашто?) то добијамо

$$\begin{aligned} A \cong F/R &\cong (\langle y_1 \rangle \oplus \langle y_2 \rangle \oplus \cdots \oplus \langle y_n \rangle)/(\langle d_1 y_1 \rangle \oplus \langle d_2 y_2 \rangle \oplus \cdots \oplus \langle d_n y_n \rangle) \\ &\cong (\langle y_1 \rangle \times \langle y_2 \rangle \times \cdots \times \langle y_n \rangle)/(\langle d_1 y_1 \rangle \times \langle d_2 y_2 \rangle \times \cdots \times \langle d_n y_n \rangle) \\ &\cong \langle y_1 \rangle/\langle d_1 y_1 \rangle \times \langle y_2 \rangle/\langle d_2 y_2 \rangle \times \cdots \times \langle y_n \rangle/\langle d_n y_n \rangle \end{aligned}$$

Како је $\langle y_i \rangle \cong \mathbb{Z}$ за све $i = \overline{1, n}$, то добијамо да је

$$\langle y_i \rangle/\langle d_i y_i \rangle \cong \begin{cases} \mathbb{Z}, & d_i = 0 \\ \{0\}, & d_i = 1 \\ \mathbb{Z}_{d_i}, & d_i \geq 2 \end{cases}$$

Тражени резултат следи. $\square$

Напомена. У случају да је $d_i = 1$, група $\mathbb{Z}_{d_i}$ је заправо тривијална група и те групе и не пишемо у факторизацији тако да је природно захтевати да је $d_i \geq 2$ у формули (1) за све i.

Претходна теорема установљава да се свака коначно генерисана Абелова група може представити у облику производа цикличних. У којој мери је тај приказ јединствен? На то питање нам одговор даје следећа теорема.

Теорема 9 Претпоставимо да је

$$\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_k} \times \mathbb{Z}^r \cong \mathbb{Z}_{e_1} \times \cdots \times \mathbb{Z}_{e_l} \times \mathbb{Z}^s,$$

при чему је $d_i \geq 2$, $e_j \geq 2$ за све i, j; $d_i \mid d_{i+1}$, као и $e_j \mid e_{j+1}$ за све i, j. Тада је $k = l$, $d_i = e_i$ за све i и $r = s$.

Доказ ове теореме нећемо давати. Напоменимо само да се бројеви d_i називају и *инваријантни делитељи*, а приказ у облику производа нормална форма.

Вратимо се на сам почетак ове лекције. Видели смо како смо без већих проблема, на основу скупа генератора и релација које међу њима важе, успели у том једноставном примеру да идентификујемо о којој се Абеловој групи ради, односно успели смо да је прикажемо у облику директног производа цикличних група. Опишимо укратко поступак у општем случају.

Претпоставимо да је Абелова група A задата генераторима $x_1, \ldots, x_n$ и релацијама

$$\begin{gathered} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = 0 \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = 0 \end{gathered}$$

Шта ово заправо значи? Ништа друго до да је A задато као количник слободне групе F са n слободних генератора и њене подгрупе R генерисане елементима $\sum_j a_{ij}x_j$, за $i = \overline{1, m}$. Наравно да се природно појављује матрица

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{11} & a_{12} & \cdots & a_{1n} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

Теорема коју смо доказали заправо каже да се ова матрица елементарним трансформацијама на врстама и колонама може свести на матрицу $[d_{ij}]$ тако да је $d_{ij} = 0$ за све $i \neq j$ и да $d_{ii} \mid d_{i+1,i+1}$ за све i. Дозвољене трансформације су:

- Множење врсте или колоне са -1

- Додавање врсти (колони) друге врсте (колоне) помножене неким целим бројем

Рад са врстама мења релације међу генераторима, док рад са колонама мења генераторе.