АЛГЕБРА 1

Групе

Цикличне групе; изоморфизми група

Зоран Петровић

2. новембар 2011.

Видели смо да је $\{\varepsilon, \rho, \rho^2, \rho^3, \rho^4, \rho^5\}$ једна подгрупа групе $\mathbb{D}_6$. Приметимо да је у овој групи сваки елемент облика ρ^k за неки цео број k. Групе са овим својством називају се цикличне групе.

Дефиниција 1 Група G је *циклична* група уколико постоји елемент $x \in G$ такав да је сваки елемент из G облика x^m за неки цео број m, односно

$$G = \{x^m : m \in \mathbb{Z}\}.$$

Такав елемент зовемо генератор цикличне групе.

У складу са дефиницијом групе генерисане неким подскупом, циклична група је она група која је генерисана једночланим подскупом, тј. једним елементом. Уколико желимо да истакнемо да је G циклична група чији је генератор a, онда то пишемо овако: $G = \langle a \rangle$.

Група ротација правилног n-тоугла, је такође циклична група и она је генерисана ротацијом за угао $2\pi/n$. Наведимо још неке примере цикличних група.

- $\mathbb{Z}_n = (Z_n, +_n)$ је циклична група генерисана елементом 1. Овде је $+_n$ сабирање по модулу n, а $Z_n = \{0, 1, \ldots, n-1\}$, где је $n \geq 2$.
- $\mathbb{C}_n = \{z \in \mathbb{C} : z^n = 1\}$ је такође циклична група у односу на множење комплексних бројева. То је група свих n-тих корена из јединице и генерисана је елементом $e^{2i\pi/n} (= \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n})$. Генератор те групе се зове и *примитивни* n-ти корен из јединице.
- $(\mathbb{Z}, +)$ је циклична група генерисана елементом 1.

Приметимо да постоје и цикличне групе са коначно много елемената, као и цикличне групе са бесконачно много елемената. Заправо за сваки природан број $n \geq 1$ постоји циклична група са n елемената

(у случају да је $n = 1$ добијамо тривијалну групу чији је једини елемент неутрал). Природно се поставља питање: да ли су две цикличне групе са истим бројем елемената суштински различите? Испоставља се да је одговор негативан — сваке две цикличне групе са истим бројем елемената су изоморфне, али ће више речи о томе бити у наредним лекцијама.

Уводимо сада појам реда групе и реда елемента групе.

Дефиниција 2 Ако је група G коначна онда број њених елемената зовемо ред групе и означавамо са $|G|$. У случају да је група бесконачна, кажемо да је она бесконачног реда.

Нека је a елемент неке групе. Уколико не постоји природан број $n \geq 1$ за који је $a^n = e$, кажемо да је елемент a бесконачног реда. Уколико такав елемент постоји, онда је ред елемента a, у ознаци $\omega(a)$ задат са:

$$\omega(a) := \min\{m \geq 1 : a^m = e\}.$$

Став 3 Ред ма ког елемента неке групе једнак је реду подгрупе генерисане тим елементом.

Доказ. Уколико је елемент a бесконачног реда, онда је $a^k \neq a^l$ за све $k \neq l$. Наиме, ако је $a^k = a^l$ за неке k и l при чему је $k > l$, онда је $a^{k-l} = e$, а $k - l \geq 1$, што противречи претпоставци да је a бесконачног реда. Но, из чињенице да је $a^k \neq a^l$ за $k \neq l$ следи да је подгрупа $\langle a \rangle$ бесконачна.

Дакле, елемент бесконачног реда генерише бесконачну подгрупу. Обратно, ако је подгрупа генерисана елементом a бесконачна онда елемент a мора бити бесконачног реда. Претпоставимо да је $\omega(a) = n \geq 1$. Тврдимо да је тада

$$\langle a \rangle = \{e, \ldots, a^{n-1}\}$$

и да су сви ови елементи различити. Наиме, сваки елемент из $\langle a \rangle$ је облика a^m за неки цео број m. Поделимо са остатком m са n. Добијамо да је $m = qn + r$, где је $0 \leqslant r < n$. Тада је

$$a^m = (a^n)^q a^r = e^q a^r = a^r \in \{e, \ldots, a^{n-1}\}.$$

Закључујемо да је $\langle a \rangle = \{e, \ldots, a^{n-1}\}$. Уколико би било $a_r = a^s$ за неке $0 \leqslant r < s < n$, онда би важило и $a^{s-r} = e$, а то није могуће, јер је $0 < s - r < n$, а $n = \omega(n)$. Закључујемо да су сви ови елементи различити, те је ред те подгрупе заиста n, а то је и ред елемента a.□

Став 4 Ако је елемент a бесконачног реда и $m \neq 0$, онда је и a^m бесконачног реда. Уколико је $\omega(a) = n$ и $m \neq 0$ онда је

$$\omega(a^m) = \frac{n}{\mathrm{NZD}(m, n)}.$$

Доказ. Први део тврђења се лако доказује. Наиме, ако је $(a^m)^r = e$, онда је и $a^{mr} = e$, па би и a био коначног реда. Доказ другог дела је тежи.

Нека је $d = \text{NZD}(m, n)$. Тада је $m = m_1 d$ и $n = n_1 d$, при чему су m_1 и n_1 узајамно прости. Ми треба да докажемо да је $\omega(a^m) = n_1$.

$$(a^m)^{n_1} = a^{mn_1} = a^{m_1 d n_1} = a^{m_1 n} = (a^n)^{m_1} = e^{m_1} = e.$$

Претпоставимо да је $k > 0$ такав да је $(a^m)^k = e$. Треба да покажемо да је $n_1 \leqslant k$. Дакле, $a^{mk} = e$ и $a^n = e$ (пошто је $n = \omega(a)$). Постоје цели бројеви q и r такви да је $mk = qn + r$, где је $0 \leqslant r < n$. Добијамо да је $a^{mk} = (a^n)^q a^r$, те следи да је $a^r = e$. Но, $n = \omega(a)$ и $0 \leqslant r < n$, па мора бити $r = 0$. Дакле, $n \mid mk$. Добијамо $dn_1 \mid dm_1 k$, па $n_1 \mid m_1 k$. Како су m_1 и n_1 узајамно прости добијамо да $n_1 \mid k$, па мора бити $n_1 \leqslant k$, што се и тражило. □

Напомена. Приметимо да се у овом доказу „крије" и доказ следећег резултата: ако је n ред елемента a, онда за сваки $l \in \mathbb{Z}$ важи

$$a^l = e \text{ ако и само ако } n \mid l.$$

Како је овај резултат од посебног значаја, даћемо и његов комплетан доказ.

- Претпоставимо да је $n = \omega(a)$ и да је $a^l = e$. Поделимо l са n. Добијамо да је $l = qn + r$, где је $0 \leqslant r < n$. Но, тада је

  $$e = a^l = a^{qn+r} = (a^n)^q \cdot a^r = e^q \cdot a^r,$$

  те добијамо да је $a^r = e$. Како је $0 \leqslant r < n = \omega(a)$, то је могуће једино ако је $r = 0$. Дакле, $n \mid l$.

- Нека $n \mid l$. Тада је $l = qn$, за неки цео број q и добијамо

  $$a^l = a^{qn} = (a^n)^q = e^q = e.$$

Пример 5 Одредити ред елемента 18 у групи $\mathbb{Z}_{120}$.

Решење. Како је 1 генератор групе $\mathbb{Z}_{120}$,

$$18 = \underbrace{1 + \cdots + 1}_{18}$$

и $\text{NZD}(18, 120) = 6$, то је ред елемента 18 једнак $\frac{120}{6} = 20$. ♣

Докажимо сада теорему о подгрупама цикличне групе.

Теорема 6 1) Свака подгрупа цикличне групе и сама је циклична.
2) Ако је G циклична група коначног реда n и ако $k \mid n$, онда постоји тачно једна подгрупа H групе G, која је реда k.

Доказ. 1) Нека је $G = \langle a \rangle$ и $H \leqslant G$. Ако је $H = \{e\}$, немамо шта да доказујемо. У супротном нека је $s = \min\{n > 0 : a^n \in H\}$. Показаћемо да је $H = \langle a^s \rangle$. Како је $a^s \in H$, то је и $(a^s)^m \in H$ за све $m \in \mathbb{Z}$, па је $\langle a \rangle \subseteq H$.

Претпоставимо да $x \in H$. Како је G циклична група, то је $x = a^k$ за неки цео број k. Тада постоје цели бројеви q и r за које је $k = qs + r$, при чему је $0 \leqslant r < s$. Дакле, $r = k - qs$ и добијамо $a^r = a^k(a^s)^{-k}$. Како је $a^k = x \in H$ и $a^s \in H$, то следи да $a^r \in H$. Но, $0 \leqslant r < s$ и по избору броја s мора бити $r = 0$. Дакле, $x = a^k = (a^s)^q \in \langle a^s \rangle$.

2) Како је $\omega(a) = n$ и $k \mid n$, то је према претходном ставу $\omega(a^{n/k}) = k$ и подгрупа H, генерисана елементом $a^{n/k}$ је реда k. Претпоставимо да постоји још једна подгрупа H_1 истог реда k. Како је према већдоказаном подгрупа H_1 циклична, онда је $H_1 = \langle a^l \rangle$. Како је $\omega(a^l) = |H_1| = k$, то је $(a^l)^k = e$. Дакле, $a^{kl} = e$, а $\omega(a) = n$, па добијамо да $n \mid kl$. Како $k \mid n$, добијамо да $\frac{n}{k} \mid l$, те је $l = \frac{n}{k} l_1$ за неко l_1. Но, тада је $a^l = (a^{n/k})^{l_1} \in H$ и $H_1 \subseteq H$. Како је $|H_1| = k = |H|$, то је $H_1 = H$ и тражена подгрупа је заиста јединствена. □

Пример 7 Одредити јединствену подгрупу H реда 6 у групи $\mathbb{Z}_{18}$.

Решење. Како је $18/6 = 3$, то је тражена подгрупа H генерисана елементом 3 и $H = \{0, 3, 6, 9, 12, 15\}$. Напишимо и таблицу сабирања у тој подгрупи.

$+_{18}$	0	3	6	9	12	15
0	0	3	6	9	12	15
3	3	6	9	12	15	0
6	6	9	12	15	0	3
9	9	12	15	0	3	6
12	12	15	0	3	6	9
15	15	0	3	6	9	12

♣

Упоредите ову таблицу са таблицом сабирања у групи $\mathbb{Z}_6$.

$+_6$	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

Евидентно је да ове таблице врло слично изгледају. То није случајно.

Пређимо сада на појам изоморфизма група.

Дефиниција 8 Нека су $(G, \cdot)$ и $(H, *)$ групе. Кажемо да су ове групе изоморфне уколико постоји бијекција $f: G \to H$ таква да је за све $x, y \in G$:

$$f(x \cdot y) = f(x) * f(y).$$

Бијекција из ове дефиниције зове се изоморфизам група G и H. Чињеницу да је група G изоморфна групи H записујемо овако: $G \cong H$.

Уколико је e неутрал у G, а ε неутрал у H и $f: G \to H$ изоморфизам, важи следеће:

- $f(e) = \varepsilon$;
- $f(x^{-1}) = f(x)^{-1}$.

Наиме, $f(e) = f(e \cdot e) = f(e) * f(e)$, те следи да је $f(e) = \varepsilon$. Слично, $\varepsilon = f(e) = f(x \cdot x^{-1}) = f(x) * f(x^{-1})$, па закључујемо да је $f(x^{-1}) = f(x)^{-1}$.

Став 9 Ако је $f: G \to H$ изоморфизам група, онда је и $f^{-1}: H \to G$, такође изоморфизам.

Доказ. Јасно је да $f^{-1} : H \to G$ постоји, пошто је f бијекција. Треба показати да је $f^{-1}(u * v) = f^{-1}(u) \cdot f^{-1}(v)$ за све $u, v \in H$. Како је f „на“, то постоје x и y тако да је $u = f(x)$ и $v = f(y)$. Но, тада је

$$f^{-1}(u * v) = f^{-1}(f(x) * f(y)) = f^{-1}(f(x \cdot y)) =$$

$$= (f^{-1} \circ f)(x \cdot y) = \mathrm{id}_G(x \cdot y) = x \cdot y = f^{-1}(u) \cdot f^{-1}(v).$$

□

Изоморфизам чува ред елемента у групи.

Став 10 Ако је $f: G \to H$ изоморфизам и $x \in G$, онда је $\omega(f(x)) = \omega(x)$.

Доказ. Размотримо најпре случај када је x бесконачног реда. Покажимо да је и $f(x)$ такође бесконачног реда. У супротном, је $(f(x))^n = \varepsilon$ за неко $n > 0$. Но, тада је $f(x^n) = f(e)$, а како је f „1–1“ закључујемо да је $x^n = e$, што противречи претпоставци да је x бесконачног реда. Закључујемо да да је и $f(x)$ бесконачног реда.

Нека је $n = \omega(x)$. Тада је $f(x)^n = f(x^n) = f(e) = \varepsilon$, па добијамо да је и $f(x)$ коначног реда m и да $m \mid n$. Но, $x^m = (f^{-1}(f(x)))^m = f^{-1}(f(x)^m) = f^{-1}(\varepsilon) = e$, па $n \mid m$. Дакле, $m = n$. □

Напомена. Овде смо искористили раније доказани резултат да је за елемент z неке групе испуњено: $z^m = e$ ако и само ако $\omega(z) \mid m$.

Заправо, две изоморфне групе су потпуно идентичне по својим алгебарским својствима; једино се могу разликовати по природи својих елемената.

У претходној лекцији доста пажње посвећено је цикличним групама. Испоставља се да важи следећа теорема.

Теорема 11 Свака циклична група изоморфна је или групи $\mathbb{Z}$ или групи $\mathbb{Z}_n$ за неко $n \geq 1$.

Доказ. Претпоставимо најпре да је G бесконачна циклична група. То значи да постоји елемент $a \in G$ такав да је

$$G = \{a^m : m \in \mathbb{Z}\}.$$

Осим тога, $x^k \neq x^l$ уколико је $k \neq l$. У овом случају дефинишимо $f: \mathbb{Z} \to G$ са: $f(m) = a^m$. Јасно је да је f бијекција (зашто?). Треба само проверити да је $f(m+n) = f(m) \cdot f(n)$ за све $m, n \in \mathbb{Z}$. Но, то је заправо раније наведено својство: $a^{m+n} = a^m \cdot a^n$. Закључујемо да је у овом случају $G \cong \mathbb{Z}$.

Претпоставимо да је G коначна циклична група, тј. да је за неки елемент $a \in G$

$$G = \{e, a, \ldots, a^{n-1}\},$$

за неки природан број $n \geq 2$ (случај $n = 1$ је једноставан, ту добијамо само тривијалну групу $\{e\}$). Доказаћемо да је у овом случају $G \cong \mathbb{Z}_n$. Дефинишемо функцију $f: \mathbb{Z}_n \to G$ са: $f(k) := a^k$. Као и у претходном случају, јасно је да је f бијекција. Треба само показати да је

$$f(k +_n l) = f(k) \cdot f(l).$$

Подсетимо се да је, за $k, l \in \{0, 1, \ldots, n-1\}$:

$$k +_n l = \begin{cases} k + l, & k + l < n \\ k + l - n, & k + l \geq n. \end{cases}$$

Уколико је $k + l < n$, добијамо да је

$$f(k) \cdot f(l) = a^k \cdot a^l = a^{k+l} = f(k+l) = f(k +_n l).$$

У случају да је $k + l \geq n$,

$$f(k) \cdot f(l) = a^k \cdot a^l = a^{k+l} = a^{(k+_n l)+n} = a^{k+_n l} \cdot a^n = a^{k+_n l} \cdot e = a^{k+_n l} = f(k +_n l).$$

Дакле, f је заиста изоморфизам и закључујемо да је $\mathbb{Z}_n \cong G$. □

Сада знамо да је јединствена подгрупа реда 6 у групи $\mathbb{Z}_{18}$, чију смо таблицу сабирања раније записали, изоморфна групи $\mathbb{Z}_6$, што објашњава сличност њихових таблица сабирања.