АЛГЕБРА

Групе

Основни појмови и примери

Зоран Петровић

21. фебруар 2011.

Групе су један од централних објеката у овом курсу и неколико недеља ће бити посвећено управо њима. Појам групе се може увести на два еквивалентна начина.

Дефиниција 1 Група је алгебарска структура $(G, \cdot)$, где је G непразан скуп, а $\cdot$ бинарна операција на скупу G, за које важи:

1. за све $x, y, z \in G$: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$;
2. постоји $e \in G$ тако да је за сваки $x \in G$ испуњено: $x \cdot e = x = e \cdot x$;
3. за сваки $x \in G$ постоји $\bar{x} \in G$ тако да је $x \cdot \bar{x} = e = \bar{x} \cdot x$.

Дефиниција 2 Група је алгебарска структура $(G, \cdot, ', 1)$, где је G непразан скуп, $\cdot$ бинарна операција на скупу G, $'$ унарна операција на скупу G и 1 изабрани елемент из G, за које важи:

1. за све $x, y, z \in G$: $(x \cdot y) \cdot z = x \cdot (y \cdot z)$;
2. за све $x \in G$: $x \cdot 1 = x = 1 \cdot x$;
3. за све $x \in G$: $x \cdot x' = 1 = x' \cdot x$.

Покажимо да су ове дефиниције еквивалентне.

Ако је $(G, \cdot, ', 1)$ група у смислу друге дефиниције онда је тражени елемент e из прве дефиниције заправо 1, док је за $x \in G$ тражени елемент $\bar{x}$ заправо x'. Дакле, то је доста једноставно. Нешто је сложеније показати како се на основу структуре из прве дефиниције добија структура из друге.

Претпоставимо да је структура $(G, \cdot)$ група у смислу прве дефиниције. Приметимо да је елемент e (који се зове неутрал групе), из ове дефиниције, јединствено одређен. Наиме, претпоставимо да постоји

и елемент e' који задовољава исте услове као и e. Тада добијамо да је $e \cdot e' = e'$ пошто је e неутрал, али је и $e \cdot e' = e$ пошто је e' неутрал. Дакле, $e = e'$. За изабрани елемент, који нам треба у другој дефиницији узимамо елемент e.

Да бисмо имали дефинисану унарну операцију $'$ на скупу G, која задовољава услове из друге дефиниције, покажимо да је за дати елемент $x \in G$ елемент $\bar{x}$ (који се зове инверз елемента x) једиственo одређен. То се показује на сличан начин као и јединственост неутрала. Претпоставимо да, осим $\bar{x}$, постоји и елемент $\tilde{x}$, који задовољава исте услове. Тада је $\tilde{x}\cdot(x\cdot\bar{x}) = \tilde{x}\cdot e = \tilde{x}$, но такође је $\tilde{x}\cdot(x\cdot\bar{x}) = (\tilde{x}\cdot x)\cdot\bar{x} = e\cdot\bar{x} = \bar{x}$ и добијамо да је $\tilde{x} = \bar{x}$. Дакле са: $x' := \bar{x}$, при чему је $\bar{x}$ јединствени елемент из прве дефиниције, добијамо добро дефинисану унарну операцију, која задовољава својства из друге дефиниције.

Убудуће ћемо чешће користити прву дефиницију, при чему ћемо знак операције $\cdot$ често изостављати (дакле писаћемо xy, а не $x \cdot y$), а и уместо „дата је група $(G, \cdot)$“, писаћемо кратко „дата је група G“. Осим тога, инверз елемента x обично ћемо записивати овако: x^{-1}.

Докажимо сада нека једноставна својства која следе из дефиниције. Уведимо најпре једну помоћну ознаку. Ако су $x_1, x_2, \ldots, x_n$ елементи групе G, где је $n \geq 1$, производ $x_1 \cdots x_n$ дефинишемо рекурентном формулом:

$$x_1 \cdots x_n := x_1, \text{ ако је } n = 1,$$
$$x_1 \cdots x_{n+1} := (x_1 \cdots x_n) \cdot x_{n+1}, \text{ за } n \geq 1.$$

Посебно, ако је $x_1 = x_2 = \cdots = x_n = x$, уместо $x \cdots x$ пишемо x^n.

- За свако $n \geq 2$ и свако r, за које је $1 \leq r < n$ важи:

  $$(x_1 \cdots x_r) \cdot (x_{r+1} \cdots x_n) = (x_1 \cdots x_n).$$

  Ово заправо значи да заграде можемо произвољно да постављамо, па их ми често нећемо ни писати. Резултат се без проблема доказује индукцијом по n. У случају да су сви x_i једнаки добијамо да је за све $m, n \in \mathbb{N}$: $x^m x^n = x^{m+n}$.

- За сваки $x \in G$:

  $$(x^{-1})^{-1} = x$$

  Овај резултат следи из јединствености инверза. Наиме, и елемент x и елемент $(x^{-1})^{-1}$ задовољавају услове за инверз елемента x^{-1}, па су стога једнаки.

- За све $x, y \in G$:

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

  Обратите пажњу на редослед фактора! Проверимо да ли је $y^{-1}x^{-1}$ инверз елемента xy:

  $$(y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}x)y = y^{-1}ey = y^{-1}y = e,$$
  $$(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xex^{-1} = xx^{-1} = e.$$

- Свака једначина облика
$$ax = b$$
има тачно једно решење у G. То је тачно и за једначину облика $xa = b$.

Није тешко проверити да је $a^{-1}b$ једно решење ове једначине:
$$a(a^{-1}b) = (aa^{-1})b = eb = b.$$
Решење је јединствено јер из $ax_1 = ax_2$ следи да је $a^{-1}ax_1 = aa^{-1}x_2$, тј. $ex_1 = ex_2$, па мора бити $x_1 = x_2$.

- За све $a, x \in G$ и $n \geq 1$:
$$(axa^{-1})^n = ax^n a^{-1}.$$
Доказ се изводи индукцијом по n.

Ако је $n = 1$, онда је тврђење тривијално тачно. Претпоставимо да је тврђење тачно за n и докажимо га за $n + 1$.

$$(axa^{-1})^{n+1} = \underbrace{(axa^{-1})^n(axa^{-1}) = ax^n a^{-1}axa^{-1}}_{\text{индуктивна хипотеза}} = ax^n xa^{-1} = ax^{n+1}a^{-1}.$$

Степен елемента x^m може се дефинисати и за негативне m:
$$x^{-n} := (x^{-1})^n, \text{ за } n \geq 1.$$

Наравно, ако је $n = 0$ узимамо $x^0 = e$. За вежбу доказати да важи:

- За свако $x \in G$ и свако $n \geq 1$: $x^{-n} = (x^n)^{-1}$.
- За свако $x \in G$ и све $m, n \in \mathbb{Z}$: $x^m x^n = x^{m+n}$.
- За свако $x \in G$ и све $m, n \in \mathbb{Z}$: $(x^m)^n = x^{mn}$.

Пређимо сада на примере група. Први и најједноставнији примери група су примери група које формирају бројеви. То су групе $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, а такође и $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{Q}^+, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{R}^+, \cdot)$, као и $(\mathbb{C} \setminus \{0\}, \cdot)$. Наравно, овде су $+$ и $\cdot$ уобичајене операције сабирања и множења бројева, док су са $\mathbb{Q}^+$ ($\mathbb{R}^+$) означени сви позитивни рационални (реални) бројеви. Но, наравно да појам групе није уведен због група које чине бројеви.

Посматрајмо неки правилни многоугао у равни и потрудимо се да нађемо које све он симетрије има. У ту сврху, за почетак, није лоше посматрати неки конктретан случај и ми ћемо се концентрисати на два примера. На правилни петоугао и правилни шестоугао.

Симетрије које постоје у равни су: транслације, ротације, осне рефлексије и клизајуће рефлексије. Ако читалац није чуо за клизајуће

рефлексије, то му ништа неће сметати. Наиме, клизајућа рефлексија је композиција једне транслације и једне осне рефлексије, па је довољно погледати шта се дешава са транслацијама и осним рефлексијама. Јасно је да транслације не долазе у обзир као симетрије неког многоугла. Слично се могу избацити и све ротације сем оне око центра многоугла. Наравно, не долазе у обзир ни све ротације око центра многоугла. У случају правилног n-тоугла, у „игри“ су само ротације за углове облика $2k\pi/n$. Тако добијамо n различитих ротација, односно симетрија правилног n-тоугла. Дакле, у случају правилног петоугла имамо 5 ротација, док у случају правилног шестоугла имамо 6 ротација (не заборавимо да је ротација за угао $2npi/n$, односно ротација за угао 2π заправо идентична трансформација). Што се тиче осних рефлексија, ту је добро разликовати случај петоугла и шестоугла. У случају петоугла, имамо пет осних рефлексија и то око правих које пролазе кроз једно теме и средиште наспрамне странице. У случају правилног шестоугла имамо три рефлексије у односу на праве које пролазе кроз наспрамна темене и још три у односу на праве које пролазе кроз средишта наспрамних страница. Наравно, препоручујемо читаоцу да нацрта одговарајуће цртеже.

Означимо са ρ ротацију за угао $2\pi/n$ у смеру супротном кретању казаљке на часовнику. Видимо да су тада све ротације облика ρ^k за неки k који може узимати вредности од 0 до $n-1$ (говоримо о правилном n-тоуглу). Ако са ε означимо идентичну симетрију, онда је $\rho^n = \varepsilon$. Са σ означимо било коју од наведених осних рефлексија. Није тешко проверити да је свака споменута рефлексија облика $\sigma\rho^k$ где је $0 \leq k < n$. Овде је добро разликовати случај парног и непарног n, односно једноставне случајеве правилног петоугла и правилног шестоугла. Приметимо да је $\sigma^2 = \varepsilon$. Посматрајмо скуп

$$\{\varepsilon, \rho, \ldots, \rho^{n-1}, \sigma, \sigma\rho, \ldots, \sigma\rho^{n-1}\}.$$

У односу на операцију композиције пресликавања, овај скуп представља групу. Та група има $2n$ елемената и назива се *диедарска* група и означава са $\mathbb{D}_n$.

Проверимо да је ово заиста група. Јасно је да је неутрал групе идентично пресликавање ε. Остаје нам да проверимо две ствари.

1) Да је композиција добро дефинисана на горенаведеном скупу.

2) Да сваки елемент из горенаведеног скупа има инверз.

Наиме, није јасно због чега нпр. елемент $\rho\sigma$ припада том скупу. А и за многе друге композиције то није јасно. Испоставља се да је довољно да се провери колико је $\rho\sigma$; из тог резултата ће све следити.

Директном провером добија се да је

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

Израчунајмо сада колико је $\rho^2\sigma$:

$$\rho^2\sigma = \rho\sigma\rho^{n-1} = \sigma\rho^{n-1}\rho^{n-1} = \sigma\rho^{2n-2} = \sigma\rho^{n-2}.$$

Није тешко добити и општи резултат:

$$\rho^k\sigma = \sigma\rho^{n-k}.$$

То се једноставно добија, нпр. индукцијом по k.

Приметимо да је заправо $\rho^{n-1} = \rho^{-1}$. То нам омогућава да горње идентитете напишемо на једноставнији начин:

$$\rho\sigma = \sigma\rho^{-1}; \quad \rho^k\sigma = \sigma\rho^{-k},$$

а имамо и

$$\sigma\rho^k = \rho^{-k}\sigma.$$

Сада се може проверити да је горњи скуп затворен у односу на композицију пресликавања.

$$\sigma\rho^k\rho^l = \begin{cases} \sigma\rho^{k+l}, & \text{ако је } k+l < n \\ \sigma\rho^{k+l-n}, & \text{ако је } k+l \geq n. \end{cases}$$

$$\sigma\rho^k\sigma\rho^l = \begin{cases} \rho^{-k+l}, & \text{ако је } k \leq l \\ \rho^{n-k+l}, & \text{ако је } k > l. \end{cases}$$

$$\rho^k\sigma\rho^l = \begin{cases} \sigma\rho^{-k+l}, & \text{ако је } k \leq l \\ \sigma\rho^{n-k+l}, & \text{ако је } k > l. \end{cases}$$

Наравно да је

$$\rho^k\rho^l = \begin{cases} \rho^{k+l}, & \text{ако је } k+l < n \\ \rho^{k+l-n}, & \text{ако је } k+l \geq n. \end{cases}$$

Занимљиво је написати целу таблицу множења за групу $\mathbb{D}_6$:

$\circ$	ε	ρ	ρ^2	ρ^3	ρ^4	ρ^5	σ	$\sigma\rho$	$\sigma\rho^2$	$\sigma\rho^3$	$\sigma\rho^4$	$\sigma\rho^5$
ε	ε	ρ	ρ^2	ρ^3	ρ^4	ρ^5	σ	$\sigma\rho$	$\sigma\rho^2$	$\sigma\rho^3$	$\sigma\rho^4$	$\sigma\rho^5$
ρ	ρ	ρ^2	ρ^3	ρ^4	ρ^5	ε	$\sigma\rho^5$	σ	$\sigma\rho$	$\sigma\rho^2$	$\sigma\rho^3$	$\sigma\rho^4$
ρ^2	ρ^2	ρ^3	ρ^4	ρ^5	ε	ρ	$\sigma\rho^4$	$\sigma\rho^5$	σ	$\sigma\rho$	$\sigma\rho^2$	$\sigma\rho^3$
ρ^3	ρ^3	ρ^4	ρ^5	ε	ρ	ρ^2	$\sigma\rho^3$	$\sigma\rho^4$	$\sigma\rho^5$	σ	$\sigma\rho$	$\sigma\rho^2$
ρ^4	ρ^4	ρ^5	ε	ρ	ρ^2	ρ^3	$\sigma\rho^2$	$\sigma\rho^3$	$\sigma\rho^4$	$\sigma\rho^5$	σ	$\sigma\rho$
ρ^5	ρ^5	ε	ρ	ρ^2	ρ^3	ρ^4	$\sigma\rho$	$\sigma\rho^2$	$\sigma\rho^3$	$\sigma\rho^4$	$\sigma\rho^5$	σ
σ	σ	$\sigma\rho$	$\sigma\rho^2$	$\sigma\rho^3$	$\sigma\rho^4$	$\sigma\rho^5$	ε	ρ	ρ^2	ρ^3	ρ^4	ρ^5
$\sigma\rho$	$\sigma\rho$	$\sigma\rho^2$	$\sigma\rho^3$	$\sigma\rho^4$	$\sigma\rho^5$	σ	ρ^5	ε	ρ	ρ^2	ρ^3	ρ^4
$\sigma\rho^2$	$\sigma\rho^2$	$\sigma\rho^3$	$\sigma\rho^4$	$\sigma\rho^5$	σ	$\sigma\rho$	ρ^4	ρ^5	ε	ρ	ρ^2	ρ^3
$\sigma\rho^3$	$\sigma\rho^3$	$\sigma\rho^4$	$\sigma\rho^5$	σ	$\sigma\rho$	$\sigma\rho^2$	ρ^3	ρ^4	ρ^5	ε	ρ	ρ^2
$\sigma\rho^4$	$\sigma\rho^4$	$\sigma\rho^5$	σ	$\sigma\rho$	$\sigma\rho^2$	$\sigma\rho^3$	ρ^2	ρ^3	ρ^4	ρ^5	ε	ρ
$\sigma\rho^5$	$\sigma\rho^5$	$\sigma\varepsilon$	$\sigma\rho$	$\sigma\rho^2$	$\sigma\rho^3$	$\sigma\rho^4$	ρ	ρ^2	ρ^3	ρ^4	ρ^5	ε

Било би добро да читаоци испишу таблице множења за групе $\mathbb{D}_3$, $\mathbb{D}_4$ и $\mathbb{D}_5$. Ако погледамо „горњи леви угао“ наведене таблице, можемо да приметимо да се ту налази таблица множења у скупу $\{\varepsilon, \rho, \rho^2, \rho^3, \rho^4, \rho^5\}$. Заправо је то једна *подгрупа* групе $\mathbb{D}_6$.

Дефиниција 3 Ако су $(G, \cdot)$ и $(H, *)$ две групе, онда је група $(H, *)$ подгрупа групе $(G, \cdot)$ уколико је:

- $H \subseteq G$,
- $x * y = x \cdot y$ за све $x, y \in H$ и
- неутрал групе $(G, \cdot)$ је уједно и неутрал групе $(H, *)$.

Наведимо сада један користан став.

Став 4 Непразан скуп H групе G је подгрупа групе G у односу на рестрикцију операције из G ако и само ако је $xy^{-1} \in H$ за све $x, y \in H$.

Доказ. Јасно је да свака подгрупа задовољава наведено својство. Наиме, ако су $x, y \in H$, како је H подгрупа, то и $y^{-1} \in H$. Осим тога, операција у H је заправо рестрикција операције у G, па мора бити $xy^{-1} \in H$, пошто $x \in H$ и $y^{-1} \in H$.

Претпоставимо да је H непразан скуп и да задовољава тражени услов. Како је $H \neq \emptyset$, то постоји $h \in H$. Тада по претпоставци и $e = hh^{-1} \in H$. Ако је $x \imath H$ произвољан, из претпоставке и чињенице да $e \in H$, следи да и $x^{-1} = ex^{-1}$ такође припада H. Коначно, ако су $x, y \in H$, онда по већ доказаном, $y^{-1} \in H$, па је и $xy = x(y^{-1})^{-1} \in H$. □

Дакле, $\{\varepsilon, \rho, \rho^2, \rho^3, \rho^4, \rho^5\}$ је 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 5 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.

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.

Пре него што размотримо подгрупе цикличне групе, докажимо неке резултате за подгрупе.

Став 6 Ако су H и K подгрупе групе G, онда је $H \cap K$ подгрупа групе G, док је $H \cup K$ подгрупа групе G ако и само ако је $H \subseteq K$ или $K \subseteq H$.

Доказ. Докажимо најпре да је пресек две подгрупе такође подгрупа. Како и H и K морају садржати неутрал, то је $H \cap K \neq \emptyset$. Претпоставимо да $x, y \in H \cap K$. То значи да $x, y \in H$ и $x, y \in K$. На основу раније доказаног, $xy^{-1} \in H$ и $xy^{-1} \in K$, па $xy^{-1} \in H \cap K$. Закључујемо да је $H \cap K$ подгрупа групе G.

Позабавимо се унијом две подгрупе. Јасно је да ако је једна од њих подскуп друге, њихова унија се поклапа са једном од њих, те јесте подгрупа групе G. Претпоставимо да је $H \cup K$ подгрупа групе G и нека $H \not\subseteq K$. Доказаћемо да је $K \subseteq H$. Како $H \not\subseteq K$, то постоји елемент h који јесте у H, а није у K. Узмимо произвољни елемент $k \in K$. Доказаћемо да је он у H и тиме показати да је $K \subseteq H$. Посматрајмо елемент $k \cdot h$. Како су и k и h из $K \cup H$, а $K \cup H$ је подгрупа групе G, то сигурно $k \cdot h \in K \cup H$. Но, ако $k \cdot h \in K$, користећи чињеницу да k припада K, добијамо да је и $h = k^{-1}kh$ из K, а то није могуће. Дакле, $k \cdot h$ мора бити у H, па како је $h \in H$ и $k = kh \cdot h^{-1}$, то $k \in H$. □

На сличан начин се може показати да је пресек произвољне фамилије подгрупа неке групе такође подгрупа те групе. Стога има смисла разматрати следећи проблем.

Проблем: Ако је G група и X подскуп те групе, да ли постоји најмања подгрупа групе G, која садржи X (као свој подскуп).

Одговор је потврдан—то је пресек свих подгрупа које садрже X. Наиме, сигурно постоји бар једна подгрупа групе G, која садрхи X (сама група G!), па има смисла говорити о пресеку. Најмања подгрупа која садржи X означава се са $\langle X \rangle$ и зове се *подгрупа генерисана са* X. Скуп X је скуп генератора те групе. Уколико је $X = \emptyset$, онда је $\langle X \rangle = \{e\}$. Уколико је $X = \{a\}$, онда је $\langle X \rangle$ циклична подгрупа генерисана елементом a и означавамо је са $\langle a \rangle$.

Вратимо се диедарској групи $\mathbb{D}_n$. Ако је $X = \{\rho, \sigma\}$, шта је $\langle X \rangle$? Јасно је да је заправо $\langle X \rangle = \mathbb{D}_n$. Дакле, група $\mathbb{D}_n$ је генерисана са два генератора.

Ако са X^{-1} означимо скуп свих инверза елемената из X,

$$X^{-1} = \{x^{-1} : x \in X\},$$

онда није тешко показати да је

$$\langle X \rangle = \{a_1 \cdots a_n : n \in \mathbb{N}, a_i \in X \cup X^{-1}\}.$$

У случају да је $n = 0$, производ $a_1 \cdots a_n$ је неутрал e.

Уколико је H подгрупа групе G, то записујемо овако: $H \leq G$.

Уводимо још појам реда елемента и реда групе.

Дефиниција 7 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 8 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 $x^k \neq x^l$ за $k \neq l$ следи да је подгрупа $\langle a \rangle$ бесконачна.

Претпоставимо да је $\omega(a) = n \geq 1$. Тврдимо да је тада

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

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 $0 \leq r < n$. Тада је

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

Закључујемо да је $\langle a \rangle = \{e, \ldots, a^{n-1}\}$, те је ред те подгрупе n, а то је ред елемента a. □

Став 9 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 $n_1 \leq k$. 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 $0 \leq r < n$. Добијамо да је $a^{mk} = (a^n)^q a^r$, те следи да је $a^r = e$. Но, $n = \omega(a)$ и $0 \leq r < n$, 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 $n_1 \leq k$, што се и тражило. □

Напомена: Приметимо да смо доказали и следећи резултат: Ако је n ред елемента a, онда за сваки $l \in \mathbb{Z}$ важи

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

Докажимо најзад и теорему о подгрупама цикличне групе.

Теорема 10 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 $H \leq G$. 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 $0 \leq r < s$. 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, $0 \leq r < s$ 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. □

Циклична група може имати више генератора. Заправо једино циклична група реда 2 има само један генератор. Бесконачна циклична

група $\langle a \rangle$ има два генератора: a и $-a$. Читаоци би могли да провере колико генератора има циклична група реда 10, а колико циклична група реда 9, а и да се увере да за $n \geq 3$ циклична група реда n има више од једног генератора.

За вежбу се такође препоручује да читаоци нађу све подгрупе група $\mathbb{D}_n$ за $n \in \{3, 4, 5, 6\}$.