АЛГЕБРА ЗА ИНФОРМАТИЧАРЕ

ЗОРАН ПЕТРОВИЋ

Предавања за школску 2013/14 годину

Групе

Алгебарске операције и алгебарске структуре

На самом почетку овог курса пажњу ћемо посветити основним појмовима алгебре — појму алгебарске операције и алгебарске структуре. Дефинишимо најпре појам алгебарске операције.

Дефиниција 1 Нека је A непразан скуп и n природан број. Операција f дужине n на скупу A, или n-арна операција скупа A је функција $f\colon A^n \to A$.

Уколико је f n-арна операција, кажемо и да је f операција дужине n. То можемо записати и овако $\#(f) = n$, где са $\#(f)$ означавамо дужину операције f.

Истакнимо одмах да ће нам посебно значајни бити случајеви када је $n = 0$, $n = 1$ и $n = 2$.

- У случају да је $n = 0$, имамо нуларну операцију $f\colon A^0 \to A$.
- У случају да је $n = 1$, говоримо о унарној операцији $f\colon A \to A$.
- Ако је $n = 2$, у питању је бинарна операција $f\colon A^2 \to A$.

Појаснимо најпре појам нуларне операције. Скуп A^0 је заправо једночлан (поновите мало знање из математичке логике). Стога се нуларна операција своди на избор једног елемента из скупа A (елемент који је слика тог јединог елемента из A^0 је изабрани елемент). Из тог разлога, често се и не говори о нуларним операцијама, него о константама, тј. изабраним елементима датог скупа. Ми ћемо користити и један и други приступ, указујући на специфичности у појединим случајевима.

У случају бинарне операције, најчешће се не пише $f(a, b)$, него $(a\, f\, b)$. Уосталом, да ли збир два броја пишете као $+(a, b)$ или као $(a+b)$ (спољашње заграде морамо да пишемо због формирања сложенијих израза)? Бинарне операције обично ћемо означавати са $\cdot$, $*$, $\circ$ и слично управо због наведеног начина писања.

Наведимо неке примере.

1. Сабирање $(+)$ и множење $(\cdot)$ су примери бинарних операција у скуповима $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$.
2. Пресек $(\cap)$, односно унија $(\cup)$ су примери бинарних операција на партитивном скупу $\mathcal{P}(X)$ неког непразног скупа X.
3. На скупу позитивних целих бројева, тј. на скупу $\mathbb{N} \setminus \{0\}$, дефинишемо операције NZD (највећи заједнички делилац) и NZS (највећи заједнички садржалац). Ово нам је (добро) познато из

школске математике. Овде имамо редак случај да бинарну операцију не пишемо у инфиксном запису, тј. писаћемо $\mathrm{NZD}(m,n)$, а не $m\,\mathrm{NZD}\,n$.

4. (**посебно важан пример**) Нека је $n \geq 2$ природан број. Посматрајмо скуп $Z_n = \{0, 1, \ldots, n-1\}$. На овом скупу можемо дефинисати две веома важне бинарне операције — сабирање по модулу n, у ознаци $+_n$ и множење по модулу n, у ознаци $\cdot_n$ на следећи начин. Означимо са $\rho(m,n)$, где је m цео број, а $n \geq 2$ природан број, остатак при дељењу m са n (подсетимо се да се остатак при дељењу m са n дефинише као јединствени природан број r за који важи $m = qn + r, 0 \leq r < n$ за неки цео број q). Тада, за $a, b \in Z_n$:

$$a +_n b := \rho(a + b, n);$$

$$a \cdot_n b := \rho(a \cdot b, n).$$

5. Налажење супротног елемента у Z $(-)$ је пример једне унарне операције: $m \mapsto -m$.

6. Налажење супротног елемента у Z_n $(-_n)$ је пример једне унарне операције:
$$-_n m = \begin{cases} 0 & m = 0 \\ n - m & m \neq 0 \end{cases}$$

7. Комплемент подскупа $(\ ^c)$ је пример једне унарне операције у скупу $\mathcal{P}(X)$: $A \mapsto A^c$.

8. На скупу позитивних целих бројева $\mathbb{N} \setminus \{0\}$ можемо дефинисати и две n-арне операције (где је $n \geq 2$):

$$(m_1, \ldots, m_n) \mapsto \mathrm{NZD}(m_1, \ldots, m_n) \quad (m_1, \ldots, m_n) \mapsto \mathrm{NZS}(m_1, \ldots, m_n).$$

Дефинишимо сада и појам алгебарске структуре.

Дефиниција 2 Алгебарска структура је уређена $(n+1)$-торка

$$\mathbb{A} = (A, f_1, \ldots, f_n),$$

где је A непразан скуп, који се назива и носач структуре $\mathbb{A}$, а $f_1, \ldots, f_n$ су операције на скупу A при чему је $\#(f_i) \geq \#(f_{i+1})$ за све $i = \overline{1, n-1}$.

Приметимо да неке од ових операција могу бити и дужине 0, тј. као део алгебарске структуре могу се појавити и константе. Уобичајено је да се операције пишу у опадајућем поретку својих дужина (зато је то и стављено у оквиру дефиниције). На пример, уколико у структури имамо само бинарне, унарне и нуларне операције, то најпре пишемо бинарне операције, потом унарне и на крају константе. У вези са овим

је и појам сигнатуре дате структуре $\mathbb{A}$, у ознаци $\sigma(\mathbb{A})$, а која се дефинише са

$$\sigma(\mathbb{A}) := (\#(f_1), \ldots, \#(f_n)).$$

Јасно је да би две структуре биле једнаке, морају имати исту сигнатуру.

Наведимо и неке важне примере алгебарских структура.

1. $\mathbb{N} = (N, +, \cdot, 0, 1)$, $\sigma(\mathbb{N}) = (2, 2, 0, 0)$.
2. $\mathbb{Z} = (Z, +, \cdot, -, 0, 1)$, $\sigma(\mathbb{Z}) = (2, 2, 1, 0, 0)$.
3. $\mathbb{Z}_n = (Z_n, +_n, \cdot_n, -_n, 0, 1)$, $\sigma(\mathbb{Z}_n) = (2, 2, 1, 0, 0)$.
4. $\mathbb{P}(X) = (\mathcal{P}(X), \cup, \cap, ^c, \emptyset, X)$, $\sigma(\mathbb{P}(X)) = (2, 2, 1, 0, 0)$.

Појам групе и основна својства

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 3 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 4 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) јединствено 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 аксиома групе. Уведимо најпре једну помоћну ознаку. Производ $\prod_{i=1}^{n} x_i$ (где $x_i \in G$) дефинишемо рекурентном формулом

$$\prod_{i=1}^{n} x_i := e, \text{ ако је } n = 0,$$

$$\prod_{i=1}^{n+1} x_i := \prod_{i=1}^{n} x_i \cdot x_{n+1}, \text{ за } n \geq 0.$$

Посебно, ако је $x_1 = x_2 = \cdots = x_n = x$, уместо $\prod_{i=1}^{n} x$ пишемо x^n. Често ћемо уместо $\prod_{i=1}^{n} x_i$ писати $(x_1 \cdots x_n)$.

- 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 тешкоћа 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
$$ax = b \qquad (*)$$
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 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 правоугаоник, који није квадрат. Сем идентичне трансформације, он има још само три симетрије: две осне рефлексије (у односу на осе које су симетрале наспрамних страница) и једну централну рефлексију (у односу на центар правоугаоника). Јасно је да композиција те две осне рефлексије даје централну. Означимо ову групу и њене елементе са

$$V=\{\varepsilon,\sigma_1,\sigma_2,\rho\},$$

где је са ε означена идентична трансформација, σ_1 и σ_2 су осне рефлексије, а ρ централна рефлексија. Није тешко саставити таблицу множења у овој групи.

$\circ$	ε	σ_1	σ_2	ρ
ε	ε	σ_1	σ_2	ρ
σ_1	σ_1	ε	ρ	σ_2
σ_2	σ_2	ρ	ε	σ_1
ρ	ρ	σ_2	σ_1	ε

Приметимо да за сваки елемент x ове групе важи: $x^2=\varepsilon$ и да је група комутативна. Касније ћемо видети да из прве чињенице следи и друга. Група V зове се и Клајнова група.

Пређимо сада на сложеније примере.

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 $2n\pi/n$, 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). Приметиомо да 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, 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

Подгрупе

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

$$H \subseteq G \quad \text{и} \quad x * y = x \cdot y \text{ за све } x, y \in H.$$

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

Присетимо се да смо појам групе дефинисали на два еквивалентна начина — као структуру са само једном бинарном операцијом, односно као структуру са једном бинарном, једном унарном и једном нуларном операцијом. Уколико се присетимо појма подалгебре, знамо шта мора бити испуњено да би нека структура била подструктура друге. У нашем случају, изабрани елементи се морају поклапати, а такође и инверзи елемената из H морају бити једнаки инверзима тих елемената када се посматрају као елементи групе G. Дакле, ако је e неутрал у G, ε неутрал у H, x^{-1} инверз елемента $x \in G$, x' инверз елемента $x \in H$, онда мора бити:

- $e = \varepsilon$;
- за све $x \in H$: $x^{-1} = x'$.

Докажимо да је то заиста тако. Нека је $h \in H$ ма који елемент из H. Тада важи:

$$h * \varepsilon = h.$$

Но, тада је и

$$h \cdot \varepsilon = h,$$

пошто је $x \cdot y = x * y$ за све $x, y \in H$, а $h, \varepsilon \in H$. Множењем горње једнакости са h^{-1} добијамо

$$h^{-1} \cdot h \cdot \varepsilon = h^{-1} \cdot h,$$

а с обзиром да је $h^{-1} \cdot h = e$, следи

$$e \cdot \varepsilon = e,$$

те је заиста $\varepsilon = e$.

Да бисмо доказали да је за све $x \in H$ испуњено $x^{-1} = x'$, напишимо шта значи то да је x^{-1} инверз елемента x у G и да је x' инверз елемента x у H (елемент x припада H):

$$x \cdot x^{-1} = x^{-1} \cdot x = e, \tag{1}$$

$$x * x' = x' * x = \varepsilon. \tag{2}$$

Но, с обзиром да x, x' припадају H и да је $e = \varepsilon$, добијамо да је

$$x \cdot x' = x' \cdot x = e. \tag{3}$$

Из (1) и (3) на основу јединствености инверза у групи добијамо да мора бити $x' = x^{-1}$.

Наведимо сада један користан став.

Став 6 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 $x \in H$ 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 $xy = x(y^{-1})^{-1} \in H$. □

Став 7 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. Наиме, нека су H_i подгрупе од G, где $i \in I$. Како за све $i \in I$ неутрал e припада H_i, то је

$$\bigcap_{i \in I} H_i \neq \emptyset.$$

Нека $x, y \in \bigcap_{i \in I} H_i$. Тада за све $i \in I$: $x \in H_i$ и $y \in H_i$. Како су H_i подгрупе, то $xy^{-1} \in H_i$, за све $i \in I$, те заиста $xy^{-1} \in \bigcap_{i \in I} H_i$.

Стога има смисла следеће питање.

Питање: 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 наравно неутрал e). Наиме, ако су $a_1 \cdots a_n$ и $b_1 \cdots b_m$ производи елемената из $X \cup X^{-1}$, јасно је да је то и

$$a_1 \cdots a_n \cdot (b_1 \cdots b_m)^{-1} = a_1 \cdots a_n \cdot b_m^{-1} \cdots b_1^{-1}.$$

Стога скуп са десне стране горње једнакости заиста чини подгрупу у односу на рестрикцију операције, а јасно је да свака подгрупа H за коју је $X \subset H$ мора садржати тај скуп као свој подскуп. Према томе, заиста је то најмања подгрупа која садржи скуп X као свој подскуп.

Приметимо на крају да, мада се Став 7 може проширити у случају пресека на произвољну колекцију подскупова, то се не може урадити за уније. Једноставан пример нам даје Клајнова група V. Наиме, $H_1 = \{\varepsilon, \sigma_1\}$, $H_2 = \{\varepsilon, \sigma_2\}$ и $H_3 = \{\varepsilon, \rho\}$, су подгрупе од V и за њих важи:

$$V = H_1 \cup H_2 \cup H_3,$$

а ниједна од њих није садржана у некој другој од њих.

Циклične групе

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 8 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, али ће више речи о томе бити у наредним лекцијама.

Ред групе; ред елемента

Уводимо сада појам реда групе и реда елемента групе.

Дефиниција 9 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 10 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 $0 \leq r < n$. Тада је

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

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

Став 11 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 $d = \mathrm{NZD}(m, n)$. 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 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 $0 \leq r < n$. 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 $0 \leq r < n = \omega(a)$, 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 12 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 13 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 $a^r = a^k(a^s)^{-q}$. 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 већ доказаном 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 14 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 наравно није случајно.

Изоморфизми група

Пређимо сада на појам изоморфизма група.

Дефиниција 15 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 16 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 17 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 18 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 $f\colon \mathbb{Z}_n \to G$ 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.

Групе пермутација

У овој лекцији обрађујемо веома значајан пример групе — групу пермутација (групу симетрија).

Дефиниција 19 Нека је X непразан скуп. Посматрајмо скуп S_X задат са:

$$S_X = \{\pi\colon X \to X \mid \pi \text{ је бијекција } \}.$$

Тада је $\mathbb{S}_X = (S_X, \circ)$, где је са $\circ$ означена операција композиције функција, једна група и зовемо је групом пермутација скупа X.

Елементе групе $\mathbb{S}_X$ зовемо и пермутацијама скупа X. Ако постоји бијекција између X и Y, онда су одговарајуће групе пермутација изоморфне.

Став 20 Ако постоји бијекција између X и Y, онда је $\mathbb{S}_X \cong \mathbb{S}_Y$.

Доказ. Нека је $g\colon X \to Y$ бијекција. Дефинишимо $f\colon S_X \to S_Y$ са:

$$f(\pi) := g \circ \pi \circ g^{-1}.$$

Јасно је да је $g \circ \pi \circ g^{-1}$ једна пермутација скупа Y уколико је π пермутација скупа X. Осим тога, ако је $\sigma \in S_Y$, онда је $f(g^{-1} \circ \sigma \circ g) = \sigma$, те је f „на". Јасно је да је f и „1–1". Треба само проверити да је $f(\rho \circ \pi) = f(\rho) \circ f(\pi)$, уколико $\rho, \pi \in S_X$. Учинимо то:

$$f(\rho \circ \pi) = g \circ (\rho \circ \pi) \circ g^{-1} = (g \circ \rho \circ g^{-1}) \circ (g \circ \pi \circ g^{-1}) = f(\rho) \circ f(\pi).$$

Дакле, f заиста успоставља изоморфизам између $\mathbb{S}_X$ и $\mathbb{S}_Y$. □

Уколико је $X = \{1, 2, \ldots, n\}$, онда уместо $\mathbb{S}_{\{1,2,\ldots,n\}}$ пишемо краће $\mathbb{S}_n$. На основу претходног става, свака коначна група пермутација неког скупа изоморфна је једној од група $\mathbb{S}_n$. Стога се сада концентришемо на групу $\mathbb{S}_n$.

Почнимо једним примером. Нека је $n = 9$ и пермутација $\sigma \in \mathbb{S}_9$ задата са:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 5 & 3 & 8 & 2 & 7 & 1 & 6 & 9 \end{pmatrix}.$$

Можемо ли ову пермутацију некако једноставније записати? Елемент 1 слика се у 4, 4 у 8, 8 у 6, 6 у 7, а 7 у 1. Некако смо „затворили круг":

$$1 \mapsto 4 \mapsto 8 \mapsto 6 \mapsto 7 \mapsto 1.$$

Запишимо то овако: (14867). Прецизније, (14867) означава пермутацију скупа $\{1, 2, \ldots, 9\}$ у којој се 1 слика у 4, 4 у 8, 8 у 6, 6 у 7, а 7 у 1, док се остали елементи сликају сами у себе. Како се остали елементи не појављују у овом запису, а сликају се сами у себе, то се (14867) може видети и као елемент групе S_n за ма које $n \geq 8$. Оваква пермутација назива се циклус или цикл дужине 5. Пермутација у којој

$$a_1 \mapsto a_2 \mapsto \cdots \mapsto a_{k-1} \mapsto a_k \mapsto a_1,$$

при чему су елементи a_i различити, означава се са $(a_1 a_2 \ldots a_k)$, зове се циклус дужине k (или k-цикл).

Вратимо се пермутацији σ. Први елемент који нисмо „покупили" до сада је елемент 2. Видимо да

$$2 \mapsto 5 \mapsto 2.$$

Дакле, добијамо нови цикл (25), који је дужине 2. Цикли дужине 2 зову се и транспозиције (само два елемента замене своја места). Видимо да се преостали елементи 3 и 9 не померају при пермутацији σ: $3 \mapsto 3$, односно $9 \mapsto 9$. То се може записати и у облику циклуса дужине 1: (3), односно (9). Но, то су, по нашој дефиницији, заправо идентичне пермутације (3 се слика у 3, а остали такође сами у себе!), те их често и не пишемо. Проверимо да ли је

$$\sigma = (14867)(25).$$

Овде треба напоменути да знак за композицију $\circ$ најчешће нећемо писати. Осим тога, подсетимо читаоца да су ово функције, те ова ознака значи да прво делује (25), а потом (14867). Није тешко проверити да горња једнакост заиста важи. Овако смо нашу пермутацију приказали о облику производа дисјунктних циклуса (циклуси $(a_1a_2\dots a_k)$ и $(b_1b_2\dots b_l)$ су дисјунктни уколико су $\{a_1,a_2,\dots,a_k\}$ и $\{b_1,b_2,\dots,b_l\}$ дисјунктни скупови). Заправо важи следећа теорема.

Теорема 21 Свака пермутација из $\mathbb{S}_n$ може се на јединствен начин, до на редослед фактора, представити у облику производа дисјунктних циклуса.

Ову теорему нећемо доказивати. Приметимо да важи следеће. Уколико су циклуси ρ и π дисјунктни, онда је $\rho\pi=\pi\rho$. То није тешко директно проверити анализирајући где се сликају поједини елементи.

Уколико пак циклуси нису дисјунктни, они не морају да комутирају:

$$(12)(23)=(123),\quad (23)(12)=(132).$$

Приметимо да је

$$(a_1a_2\dots a_k)=(a_2\dots a_ka_1)=\dots=(a_k\dots a_1a_2\dots a_{k-1}).$$

У конкретном случају $k=4$:

$$(a_1a_2a_3a_4)=(a_2a_3a_4a_1)=(a_3a_4a_1a_2)=(a_4a_1a_2a_3).$$

У вези са овим, природно се поставља питање колико у S_n има различитих циклуса дужине k, где је $k\le n$. На то питање није тешко одговорити. Наиме, најпре је потребно из скупа од n елемената изабрати њих k. То се може извести на $\binom{n}{k}$ начина. Ти елементи се међусобно могу поређати у циклус дужине k на $k!$ начина. Но, видели смо да неке од тих пермутација заправо задају исти циклус. Прецизније, од датих k елемената може се формирати $\frac{k!}{k}=(k-1)!$ различитих циклуса. Дакле, различитих циклуса дужине k у S_n има $\binom{n}{k}(k-1)!=\frac{n(n-1)\cdots(n-k+1)}{k}$. Наравно, ово се може доказати и на друге начине. Размислите како.

Позабавимо се мало рачунањем са циклусима. Најпре, лако је проверити да је, ако су a,b,c међусобно различити, $(ab)(bc)=(abc)$. Општији резултат је следећи. Ако су $a_1,a_2,\dots,a_{k+l}$ међусобно различити онда је:

$$(a_1a_2\dots a_k)(a_ka_{k+1}\dots a_{k+l})=(a_1a_2\dots a_{k+l}),$$

за све $k\ge 2, l\ge 1$. Користећи овај резултат, лако се показује да је сваки циклус производ транспозиција:

$$(a_1a_2)(a_2a_3)\cdots(a_{k-1}a_k)=(a_1a_2\dots a_k).$$

Како је свака пермутација производ циклуса то закључујемо да важи следећи став.

Став 22 Свака пермутација из $\mathbb{S}_n$ може се представити у облику производа транспозиција.

Овде треба истаћи да представљање није јединствено. Нпр.

$$(12)(23)(34) = (14)(13)(12).$$

Оно што јесте јединствено је парност броја транспозиција које се појављују у факторизацији дате пермутације. Тај резултат такође нећемо доказивати. Укажимо само да пермутације које се могу представити у облику производа парног броја транспозиција зовемо парне пермутације, док се пермутације које се представљају у облику непарног броја транспозиција зову непарне пермутације. Скуп свих парних пермутација чини групу. Та група се означава са $\mathbb{A}_n$ и важи следећи став.

Став 23 За свако $n \geq 2$ је $\mathbb{A}_n \leq \mathbb{S}_n$ и $|\mathbb{A}_n| = \frac{n!}{2}$.

Доказ. Како је идентична пермутација очигледно парна (зашто?), то је $A_n \neq \emptyset$. Осим тога, ако су σ и π парне пермутације, то је и $\sigma\pi^{-1}$ парна пермутација. Наиме, ако је $\sigma = \tau_1\tau_2\cdots\tau_{2k}$, а $\pi = \phi_1\phi_2\cdots\phi_{2l}$, представљање ових пермутација у облику производа парног броја транспозиција то је $\sigma\pi^{-1} = \tau_1\tau_2\cdots\tau_{2k}\phi_{2l}\cdots\phi_2\phi_1$ представљање у облику производа парног броја транспозиција (појаснити ову последњу једнакост). Стога закључујемо да је $\mathbb{A}_n$ заиста подгрупа групе $\mathbb{S}_n$.

Да бисмо одредили ред подгрупе $\mathbb{A}_n$, изаберимо било коју транспозицију τ. Тада можемо дефинисати функцију $\Phi\colon A_n \to S_n \setminus A_n$ са: $\Phi(\pi) := \tau\pi$. Није тешко уверити се да је Φ бијекција. Резултат одавде следи (проверити да је Φ бијекција и објаснити како се добија тражени резултат). □

Ако је $\pi \in \mathbb{S}_n$ и $(a_1a_2\ldots a_k)$ један k-цикл тада је

$$\pi(a_1a_2\ldots a_k)\pi^{-1} = (\pi(a_1)\pi(a_2)\ldots\pi(a_k)).$$

Ово се лако може проверити. Споменимо узгред да је

$$(a_1a_2\ldots a_k)^{-1} = (a_ka_{k-1}\ldots a_1).$$

Видели смо да је група $\mathbb{S}_n$ генерисана транспозицијама. То је прилично велики генераторни скуп. Заправо се могу наћи знатно једноставнији скупови генератора за $\mathbb{S}_n$.

Став 24 Група $\mathbb{S}_n$ генерисана је:

1. транспозицијама $(12), (13), \ldots, (1n)$;
2. транспозицијама $(12), (23), (34), \ldots (n-1, n)$;
3. пермутацијама (12) и $(123\ldots n)$.

Доказ.
1. Лако се може проверити да је $(ab) = (1a)(1b)(1a)$. Дакле, све транспозиције се могу добити помоћу наведених.

2. Довољно је показати да можемо да добијемо све транспозиције облика $(1a)$ за $2 \leq a \leq n$. Наравно, (12) је већ на списку! Ево како добијамо (13):

$$(13) = (12)(23)(12).$$

Сада када имамо (13) није тешко добити и (14):

$$(14) = (13)(34)(13).$$

Уочавамо правилност:

$$(1, k+1) = (1k)(k, k+1)(1k).$$

На овај начин добијамо све транспозиције за које знамо да генеришу $\mathbb{S}_n$. Стога и почетне транспозиције генеришу $\mathbb{S}_n$.

3. Подсетимо се формуле: $\pi(a_1 \dots a_k)\pi^{-1} = (\pi(a_1) \dots \pi(a_k))$ (**веома** пажљив читалац је можда приметио да се ова формула крије и у идентитету $(13) = (12)(23)(12)$). Уколико је $\pi = (12 \dots n)$ добијамо

$$(12 \dots n)(12)(12 \dots n)^{-1} = (23).$$

Када смо добили (23), није нам тешко да добијемо и (34):

$$(12 \dots n)(23)(12 \dots n)^{-1} = (34).$$

Уочавамо правилност:

$$(12 \dots n)(k, k+1)(12 \dots n)^{-1} = (k+1, k+2),$$

за $1 \leq k \leq n-2$. Тако добијамо све транспозиције за које знамо да генеришу $\mathbb{S}_n$, па према томе закључујемо да и дате две пермутације такође генеришу $\mathbb{S}_n$. □

Приметимо да парност k-цикла зависи од k. Заправо је k-цикл парна пермутација ако и само ако је k непаран (погледајте како смо k-цикл представили у облику производа транспозиција). То посебно значи да је сваки цикл дужине три (трицикл!) једна парна пермутација. Важи следећи став.

Став 25 Ако је $n \geq 3$, онда је $\mathbb{A}_n$ генерисана циклусима дужине 3.

Доказ. Ово заправо није тешко доказати. Уколико је $n = 3$ и немамо шта да доказујемо. Наиме, $\mathbb{S}_3 = \{(1), (12), (13), (23), (123), (132)\}$ ((1) представља идентичну пермутацију). Дакле, овде је заправо $\mathbb{A}_3 = \{(1), (123), (132)\}$. Претпоставимо стога да је $n \geq 4$. Како је, према

претходном ставу, скуп $\{(12), (13), \ldots, (1n)\}$ један скуп генератора групе $\mathbb{S}_n$, то се и сваки елемент из $\mathbb{A}_n$ може представити у облику производа ових елемената. Но, како је у питању елемент из $\mathbb{A}_n$, он је представљен у облику производа парног броја таквих транспозиција. Групишући их две по две, добијамо да је довољно да покажемо да се пермутације облика $(1a)(1b)$, где је $a \neq b$ могу представити у облику производа циклуса дужине 3. Но, заправо је $(1a)(1b) = (a1)(1b) = (a1b)$! Дакле, то је већ циклус дужине 3. Овим је доказ завршен. □

Позабавимо се сада питањем одређивања реда елемената из $\mathbb{S}_n$. Директном провером се добија да је $\omega((a_1 \ldots a_k)) = k$. Како се свака пермутација може представити у облику производа дисјунктних циклуса, то би морало бити корисно за одређивање реда произвољне пермутације. Доказаћемо један општи став.

Став 26 Нека је G произвољна група и $a, b \in G$ такви да је:

1. $\omega(a) = m$, $\omega(b) = n$;
2. $ab = ba$;
3. $\langle a \rangle \cap \langle b \rangle = \{e\}$.

Тада је $\omega(ab) = \text{NZS}(m, n)$.

Доказ. Како је $ab = ba$, то је за сваки $k \in \mathbb{N}$: $(ab)^k = a^k b^k$. То се лако доказује индукцијом (докажите то за вежбу!). Ради краћег записа уведимо ознаке: $s = \omega(ab)$, $t = \text{NZS}(m, n)$. Осим тога, $t = mt_1 = nt_2$. Како је

$$(ab)^t = a^t b^t = a^{mt_1} b^{nt_2} = (a^m)^{t_1} (b^n)^{t_2} = e^{t_1} e^{t_2} = e,$$

то добијамо $s \mid t$.

С обзиром да је $s = \omega(ab)$,

$$e = (ab)^s = a^s b^s.$$

Добијамо да је $a^s = (b^s)^{-1}$. Но, $a^s \in \langle a \rangle$, а $(b^s)^{-1} \in \langle b \rangle$ те смо добили елемент из пресека $\langle a \rangle \cap \langle b \rangle$. Како је овај пресек тривијалан, мора бити $a^s = e$ и $(b^s)^{-1} = e$, тј. $b^s = e$. Но, с обзиром на то да је $m = \omega(a)$ и $n = \omega(b)$, следи да $m \mid s$ и $n \mid s$. Имајући у виду да је $t = \text{NZS}(m, n)$, добијамо да $t \mid s$. Закључујемо да је $s = t$. □

Из овог резултата можемо добити две последице.

Последица 27 Ако су σ и τ дисјунктни циклуси из $\mathbb{S}_n$, онда је $\omega(\sigma\tau) = \text{NZS}(\omega(\tau), \omega(\sigma))$.

Доказ. Да бисмо применили претходни став, довољно је показати да је $\langle \tau \rangle \cap \langle \sigma \rangle = \{(1)\}$. Претпоставимо да је $\pi \in \langle \tau \rangle \cap \langle \sigma \rangle$. Нека је $\sigma = (a_1 \ldots a_k)$, а $\tau = (b_1 \ldots b_l)$. Нека је $i \in \{1, \ldots, n\}$ произвољан елемент.

Ако $i \notin \{a_1, \ldots, a_k\}$, с обзиром да је $\pi = \sigma^s$, за неко s, мора бити $\pi(i) = i$. Ако пак $i \in \{a_1, \ldots, a_k\}$, онда $i \notin \{b_1, \ldots, b_l\}$, те с обзиром да је $\pi = \tau^t$, за неко t, мора бити $\pi(i) = i$. Закључујемо да је π идентична пермутација, те је пресек тривијалан. □

Следећи резултат је генерализација претходног.

Последица 28 Ако је $\pi = \sigma_1 \cdots \sigma_k$ представљање пермутације π у облику производа дисјункних циклуса, онда је $\omega(\pi) = \text{NZS}(\omega(\sigma_1), \ldots, \omega(\sigma_k))$.

Искористимо управо доказано на једном примеру.

Пример 29 а) Испитати да ли у $\mathbb{S}_7$ постоји елемент реда 12.
б) Испитати да ли у $\mathbb{S}_7$ постоји елемент реда 8.

а) Елемент $(1234)(567)$ је на основу претходних резултата реда 12.
б) Питање се своди на следеће. Да ли број 8 може бити најмањи заједнички садржалац бројева мањих од њега? Да то није могуће, може се установити једноставном анализом. Остављамо читаоцима да се у то уверe.

Ми смо се до сада бавили цикличним, диедарским и групама пермутација. Да ли се можда неке од ових група подударају? Није тешко видети да су групе $\mathbb{S}_2$ и $\mathbb{A}_3$ цикличне групе (реда 2 односно 3). Много је занимљивија следећа чињеница:

$$\mathbb{D}_3 \cong \mathbb{S}_3.$$

Наиме, група $\mathbb{D}_3$ је група симетрија једнакостраничног троугла. Означимо темена тог троугла бројевима 1, 2 и 3. Свака симетрија троугла индукује једну пермутацију скупа свих темена, а тиме и скупа $\{1, 2, 3\}$. Није тешко уверити се која пермутација одговара којој симетрији троугла. Препоручујемо читаоцима да нацртају цртеж и сами одреде наведене симетрије. Такође за вежбу остављамо да читаоци сами покажу да ниједна од група $\mathbb{S}_n$, $\mathbb{D}_n$, за $n \geq 3$, није циклична.

Размотримо два занимљива примера из геометрије.

Пример 30 Група ротационих симетрија правилног тетраедра изоморфна је групи $\mathbb{A}_4$.

И овде је добро темена тетраедра нумерисати бројевима од 1 до 4. Свака ротациона симетрија индукује пермутацију скупа темена. Тако добијамо функцију из групе симетрија тетраедра у групу $\mathbb{A}_4$ (уверите се да добијамо само парне пермутације). Но, та функција не само да је бијекција, него је и изоморфизам, пошто је у оба случаја операција у групи заправо композиција пресликавања. ♣

Пример 31 Група ротационих симетрија коцке изоморфна је групи $\mathbb{S}_4$.

Размотримо најпре колико има ротационих симетрија коцке. Како коцка има 6 страна, то за сваки пар страна постоје по три нетривијалне ротације коцке око оса које пролазе кроз центре наспрамних страна. Ротације су за $\pi/2$, π и $3\pi/2$. Тако добијамо 9 ротација.

Коцка има и 4 дијагонале и око сваке дијагонале постоје две нетривијалне ротације — за углове од $2\pi/3$ и $4\pi/3$. Дакле, добијамо још 8 ротација.

Коцка има и 12 ивица. Постоји 6 ротација за π око оса које пролазе кроз средишта наспрамних ивица коцке.

Укупно смо добили $9+8+6+1 = 24$ ротације (додали смо и идентичну трансформацију).

Свака од ротација пермутује дијагонале коцке. Тако се свака ротација може видети и као пермутација скупа од 4 елемента. Све оне су различите, а има их 24 колико и елемената групе $\mathbb{S}_4$. С обзиром да су у оба случаја групне операције композиција функција добијамо да је тражена група симетрија изоморфна групи $\mathbb{S}_4$. Препоручујемо читаоцима да детаљније проуче овај пример и провере које ротације одговарају којим елементима из $\mathbb{S}_4$. ♣

За крај ове лекције докажимо једну једноставну, али веома важну теорему, која показује зашто групе пермутација имају значајно место у теорији група.

Теорема 32 (Кејлијева теорема) Свака група G изоморфна је некој подгрупи групе $\mathbb{S}_G$.

Доказ. Ако је $g \in G$, са $L_g : G \to G$ означимо бијекцију дефинисану са:

$$L_g(x) := g \cdot x.$$

Јасно је да је L_g бијекција пошто је $L_g \circ L_{g^{-1}} = \mathrm{id}_G (= L_e)$. Дакле, $(L_g)^{-1} = L_{g^{-1}}$. Осим тога:

$$L_g \circ L_h = L_{g \cdot h}.$$

Дакле, видимо да је $G' = \{L_g : g \in G\}$ једна подгрупа групе $\mathbb{S}_G$.

Функција $f : G \to G'$ дефинисана са $f(g) = L_g$ остварује изоморфизам између G и G'. □

У случају да је група коначна добијамо следећу последицу.

Последица 33 Свака коначна група реда n изоморфна је некој подгрупи групе $\mathbb{S}_n$.

Директан производ група

Један од начина на који од већ постојећих група можемо формирати нове групе је *директан производ група*.

Дефиниција 34 Нека су $(G_1, *_1), (G_2, *_2), \ldots, (G_1, *_n)$ групе. Дефинишемо директан производ $(P, *)$ ових група са:

- $P := G_1 \times G_2 \times \cdots G_n$;
- $(g_1, g_2, \ldots, g_n) * (g_1', g_2', \ldots, g_n') := (g_1 *_1 g_1', g_2 *_2 g_2', \ldots, g_n *_n g_n')$.

Није тешко проверити да је $(P, *)$ заиста група. Наиме, асоцијативност се лако проверава, док је неутрални елемент $e \in P$ дат са:

$$e = (e_1, e_2, \ldots, e_n),$$

где је e_i неутрални елемент у групи G_i. Такође је јасно шта је инверзни елемент:

$$(x_1, x_2, \ldots, x_n)^{-1} = (x_1^{-1}, x_2^{-1}, \ldots, x_n^{-1}).$$

Погледајмо за почетак неке једноставне примере.

Пример 35 Група $\mathbb{Z}_2 \times \mathbb{Z}_3$ је циклична група.

Приметимо најпре да је скуп носач структуре $\mathbb{Z}_2 \times \mathbb{Z}_3$, скуп

$$\{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}.$$

Да бисмо показали да је група циклична, морамо наћи елемент, који је генерише, тј. елемент реда 6. Није тешко уверити се да је један такав елемент, елемент $(1,1)$:

$$\begin{aligned}
(1,1) + (1,1) &= (1 +_2 1, 1 +_3 1) = (0,2);\\
(1,1) + (1,1) + (1,1) &= (1 +_2 0, 1 +_3 2) = (1,0);\\
(1,1) + (1,1) + (1,1) + (1,1) &= (1 +_2 1, 1 +_3 0) = (0,1);\\
(1,1) + (1,1) + (1,1) + (1,1) + (1,1) &= (1 +_2 0, 1 +_3 1) = (1,2);\\
(1,1) + (1,1) + (1,1) + (1,1) + (1,1) + (1,1) &= (1 +_2 1, 1 +_3 2) = (0,0).
\end{aligned}$$

Остављамо читаоцима да провере да ли је још неки елемент генератор ове групе. ♣

Пример 36 Група $\mathbb{Z}_2 \times \mathbb{Z}_2$ није циклична група.

Скуп носач је скуп $\{(0,0), (0,1), (1,0), (1,1)\}$. Но, није тешко уверити се да је сваки елемент у овом скупу, осим неутрала, реда 2:

$$\begin{aligned}
(0,1) + (0,1) &= (0 +_2 0, 1 +_2 1) = (0,0);\\
(1,0) + (1,0) &= (1 +_2 1, 0 +_2 0) = (0,0);\\
(1,1) + (1,1) &= (1 +_2 1, 1 +_2 1) = (0,0).
\end{aligned}$$

♣

Природно се поставља питање: за које $m, n \geq 2$ је група $\mathbb{Z}_m \times \mathbb{Z}_n$ циклична група? Одговор на ово питање даје следећи став.

Став 37 Група $\mathbb{Z}_m \times \mathbb{Z}_n$ је циклична ако и само ако је $\mathrm{NZD}(m, n) = 1$.

Доказ.
$\Longrightarrow$: Претпоставимо да је $\mathrm{NZD}(m, n) = d > 1$. Покажимо да тада група $\mathbb{Z}_m \times \mathbb{Z}_n$ не може бити циклична. Нека је $r = \frac{mn}{d} < mn$. Покажимо да је

$$\underbrace{x + \cdots + x}_{r} = 0,$$

за све $x \in \mathbb{Z}_m \times \mathbb{Z}_n$. Нека је $x = (s, t)$, произвољан елемент групе $\mathbb{Z}_m \times \mathbb{Z}_n$. Дакле, знамо да је $s \in \{0, 1, \ldots, m-1\}$ и $t \in \{0, 1, \ldots, n-1\}$ и да важи:

$$\underbrace{s + \cdots + s}_{m} = 0, \quad \underbrace{t + \cdots + t}_{n} = 0.$$

Но, тада је

$$\underbrace{s + \cdots + s}_{r} = \underbrace{\underbrace{(s + \cdots + s)}_{m} + \cdots + \underbrace{(s + \cdots + s)}_{m}}_{\frac{n}{d}} = \underbrace{0 + \cdots + 0}_{\frac{n}{d}} = 0,$$

као и

$$\underbrace{t + \cdots + t}_{r} = \underbrace{\underbrace{(t + \cdots + t)}_{n} + \cdots + \underbrace{(t + \cdots + t)}_{n}}_{\frac{m}{d}} = \underbrace{0 + \cdots + 0}_{\frac{m}{d}} = 0.$$

Одавде следи да је

$$\underbrace{(s, t) + \cdots + (s, t)}_{r} = 0,$$

те је ред сваког елемента у групи $\mathbb{Z}_m \times \mathbb{Z}_n$ највише r, дакле мањи од mn, те група не може бити цикична.
$\Longleftarrow$: Претпоставимо да је $\mathrm{NZD}(m, n) = 1$. Докажимо да је елемент $(1, 1)$ генератор групе $\mathbb{Z}_m \times \mathbb{Z}_n$, тј. да је ред тог елемента једнак mn. Означимо са r ред елемента $(1, 1)$. Дакле,

$$\underbrace{(1, 1) + \cdots + (1, 1)}_{r} = (0, 0).$$

То значи да је

$$\underbrace{1 + \cdots + 1}_{r} = 0$$

у групи $\mathbb{Z}_m$, из чега следи да $m \mid r$, као и

$$\underbrace{1 + \cdots + 1}_{r} = 0$$

у групи $\mathbb{Z}_n$, из чега следи да $n \mid r$. Дакле, $\mathrm{NZS}(m,n) \mid r$. Но, како су m и n узајамно прости, то је $\mathrm{NZS}(m,n) = mn$ и закључујемо да $mn \mid r$. Дакле, ред елемента $(1,1)$ у групи $\mathbb{Z}_m \times \mathbb{Z}_n$ је бар mn, те мора бити и једнак mn. Закључујемо да је та група циклична. □

Напомена. У случају да је група G комутативна, тј. да за све $x, y \in G$ важи: $xy = yx$, уобичајено је за ознаку операције у групи користити ознаку $+$. У том случају ознака mx, где је $m \in \mathbb{Z}$ одговара ознаци x^m. Нпр.

$$6x = \underbrace{x + \cdots + x}_{6}.$$

Како је свака циклична група реда n изоморфна групи $\mathbb{Z}_n$, то закључујемо да је директан производ цикличне групе реда m и цикличне групе реда n циклична група (реда mn) ако и само ако су m и n узајамно прости. Приметимо да се у овом тврђењу имплицитно „крије" следећи резултат: ако је $G \cong G'$ и $H \cong H'$, онда је $G \times H \cong G' \times H'$. Размислите како бисте ово доказали.

Индукцијом није тешко показати да важи следећи резултат. Ако су $m_1, m_2, \ldots, m_n$ пар по пар узајамно прости, онда имамо изоморфизам група

$$\mathbb{Z}_{m_1 m_2 \cdots m_n} \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_n}.$$

Осим што се конструкција директног производа може искористити за добијање нових група од старих, она се може употребити и за испитивање структуре неке дате групе. Наиме, корисно је знати да је дата група изоморфна директном производу неких других група. У ту сврху користан је следећи став.

Став 38 Нека је G група, а H и K подгрупе групе G за које важи:

1. $G = H \cdot K$;
2. за све $x \in H$ и све $y \in K$: $xy = yx$;
3. $K \cap H = \{e\}$.

Тада је $G \cong H \times K$.

Доказ. Напоменимо најпре да је $H \cdot K = \{h \cdot k : h \in H, k \in K\}$.
Дефинишемо функцију $f : H \times K \to G$ са:

$$f(h,k) := hk.$$

Докажимо да је f изоморфизам група. Пре свега, како је $G = H \cdot K$, јасно је да је f „на". Да бисмо доказали да је хомоморфизам, морамо проверити да важи следеће:

$$\text{за све } h, h' \in H \text{ и све } k, k' \in K : f((h,k)\cdot(h',k')) = f(h,k)\cdot f(h',k'),$$

тј. да за све $h, h' \in H, k, k' \in K$:

$$hh'kk' = hkh'k'.$$

Но, како по претпоставци елементи из H и елементи из K међусобно комутирају, то наведена једнакост јесте испуњена.

Остаје да проверимо да је f „1–1". Претпоставимо да је

$$f(h,k) = f(h',k').$$

То значи да је

$$hk = h'k',$$

односно

$$(h')^{-1}h = k'k^{-1}.$$

Но, како $(h')^{-1}h$ припада подгрупи H, а $k'k^{-1}$ подгрупи K, то смо добили елемент из $H \cap K$, а та подгрупа је тривијална. Закључујемо да мора бити $(h')^{-1}h = e$ и $k'k^{-1} = e$, те следи да је $h = h'$ и $k = k'$, тј. $(h,k) = (h',k')$. □

Ради илустрације примене ове теореме, урадимо два примера.

Пример 39 $\mathbb{D}_6 \cong \mathbb{D}_3 \times \mathbb{Z}_2$.

Дакле, у групи $\mathbb{D}_6$ треба наћи једну подгрупу изоморфну са $\mathbb{D}_3$ и једну изоморфну са $\mathbb{Z}_2$ чији је пресек тривијалан, а елементи међусобно комутирају. Група $\mathbb{D}_6$ је група симетрија правилног шестоугла, док је групе $\mathbb{D}_3$ група симетрија једнакостраничног троугла. Где се у правилном шестоуглу „крије" једнакостранични троугао? Није тешко видети да, ако су темена правилног шестоугла A, B, C, D, E, F, дијагонале AC, CE, EA образују једнакостранични троугао. Ротација шестоугла за угао $2\pi/3$, тј. ротација ρ^2, јесте симетрија тог троугла. Ако за σ узмемо осну рефлексију око праве која садржи дијагоналу BE, онда се лако можемо уверити да је подгрупа $H = \{\varepsilon, \rho^2, \rho^4, \sigma, \sigma\rho^2, \sigma\rho^4\}$, изоморфна групи $\mathbb{D}_3$. Ако за групу K узмемо групу генерисану елементом ρ^3, тј. ако је $K = \{\varepsilon, \rho^3\}$, то лако проверавамо да је $H \cdot K = \mathbb{D}_6$. Осим тога, елемент ρ^3 комутира са свим елементима из H ($\sigma\rho^3 = \rho^{-3}\sigma = \rho^3\sigma$, па заправо ρ^3 комутира са свим елементима из $\mathbb{D}_6$). Како је $H \cap K = \{\varepsilon\}$, на основу претходног става закључујемо да је $\mathbb{D}_6 \cong H \times K$, тј. $\mathbb{D}_6 \cong \mathbb{D}_3 \times \mathbb{Z}_2$. ♣

Пример 40 Ако је G коначна група чији је сваки елемент сем неутрала реда 2, онда је G изоморфна директном производу цикличних група реда 2.

Докажимо најпре да је група у којој је сваки елемент реда 2 комутативна. Нека су a и b произвољни елементи из G. По претпоставци је $a^2 = e$, $b^2 = e$, $(ab)^2 = e$. Одавде следи да је

$$(ab)^2 = a^2b^2,$$

тј.

$$abab = aabb,$$

што, после скраћивања даје

$$ab = ba.$$

Нека је $x_1 \neq e$ произвољан елемент групе G, различит од неутрала. Посматрајмо подгрупу H_1 генерисану тим елементом. Она је реда 2 пошто је елемент реда x_1 реда 2. Уколико је $H_1 = G$, доказ је завршен. У супротном, изаберимо елемент $x_2 \in G \setminus H_1$ и нека је $K_2 = \langle x_2 \rangle$. Тада је $H_2 = H_1 \cdot K_2 = \{e, x_1, x_2, x_1x_2\}$ једна подгрупа групе G (проверите!). Подгрупе H_1 и K_2 испуњавају услове претходног става (зашто?), те добијамо да је $H_2 \cong H_1 \times K_2$. Уколико је $H_2 = G$, доказ је завршен. У супротном, бирамо елемент $x_3 \in G \setminus H_2$ и посматрамо подгрупу $K_3 = \langle x_3 \rangle$. Као и у претходном случају $H_3 = H_2 \cdot K_3$ је подгрупа групе G и $H_3 \cong H_2 \times K_3 \cong H_1 \times K_2 \times K_3$. Овакав поступак мора се завршити пошто је група G коначна, а $|H_k| = 2^k$. Стога добијамо да је за неко n испуњено $G \cong H_1 \times K_2 \times \cdots \times K_n$, а сви ови фактори су цикличне групе реда 2. ♣

Лагранжева и Кошијева теорема; примене

Подсетимо се да смо увели појам реда групе и реда елемента. У случају цикличне групе, ред саме групе једнак је реду елемента који генерише ту групу. Природно је поставити питање о вези између реда елемента и реда коначне групе и у случају да група није циклична. Још општије, каква је веза између реда коначне групе и реда неке њене подгрупе? Испоставља се да је одговор једноставан и сада ћемо се тиме позабавити.

Дефиниција 41 Ако је $H \leq G$ и $x \in G$, скуп

$$xH = \{x \cdot h : h \in H\},$$

назива се леви косет подгрупе H у групи G. Аналогно, скуп

$$Hx = \{h \cdot x : h \in H\},$$

назива се десни косет.

Како $e \in H$, косет xH (Hx) садржи елемент x. У општем случају $xH \neq Hx$. Нпр. ако је $G = \mathbb{D}_3$ и $H = \{\varepsilon, \sigma\}$, онда је

$$H\rho = \{\rho, \sigma\rho\} \neq \{\rho, \rho\sigma\} = \rho H,$$

пошто је $\rho\sigma = \sigma\rho^2$. Скуп свих левих косета подгрупе H у G означаваћемо са G/H, а свих десних косета са $H\backslash G$. Као што смо видели, леви косет, који садржи елемент x, не мора бити једнак десном косету који садржи тај елемент, па је у општем случају $G/H \neq H\backslash G$. У наредним лекцијама видећемо када су ови скупови једнаки, али то је друга прича. За сада само можемо да закључимо да постоји бијекција између њих која левом косету xH придружује десни косет Hx.

Став 42 Важи следеће:

1. $xH = yH$ ако и само ако је $x^{-1}y \in H$;
2. ако је $xH \neq yH$, онда је $xH \cap yH = \emptyset$.

Доказ.
1. $\Longrightarrow$: Претпоставимо да је $xH = yH$. То посебно значи да $y \in xH$, тј. постоји $h \in H$ за који је $y = xh$. Но, тада је $h = x^{-1}y$, па закључујемо да $x^{-1}y \in H$.

$\Longleftarrow$: Нека $x^{-1}y \in H$. Претпоставимо да $z \in xH$. Дакле, $z = xh$, за неко $h \in H$. Тада је $z = x(x^{-1}y)(x^{-1}y)^{-1}h = y((x^{-1}y)^{-1}h)$, но, како је H подгрупа од G и $x^{-1}y \in H$, то и $(x^{-1}y)^{-1}h \in H$, па закључујемо да $z \in yH$. Обратно, ако $z \in yH$, онда постоји $h' \in H$, такав да је $z = yh'$. Тада је $z = x((x^{-1}y)h')$, а како је $x^{-1}y \in H$ и како је H подгрупа од G, то $z \in xH$. Закључујемо да је $xH = yH$ уколико $x^{-1}y \in H$.

2. Претпоставимо да је $xH \cap yH \neq \emptyset$. То значи да за неке $h, h' \in H$ важи: $xh = yh'$. Одавде следи да је $x^{-1}y = h(h')^{-1}$, а како је $H \leq G$, то $h(h')^{-1} \in H$. На основу претходно доказаног, следи да је $xH = yH$. $\square$

Дакле, различити леви косети ма које подгрупе H су дисјунктни. Како сваки елемент x лежи у косету xH, то закључујемо да важи следећи став.

Став 43 Нека је G група и $H \leq G$. Тада је G дисјунктна унија различитих левих косета подгрупе H.

Дефиниција 44 Уколико је скуп левих косета G/H бесконачан, кажемо да је подгрупа H бесконачног индекса у групи G. Уколико је тај скуп коначан, онда се индекс подгрупе H у групи G, у ознаци $[G : H]$, дефинише као број елемената у G/H, тј. $[G : H]$ је број различитих левих косета подгрупе H у групи G.

Напомена. Како постоји бијекција између G/H и $H\backslash G$, то је $[G : H]$ такође и број различитих десних косета H у G. Осим тога, бесконачна група може садржати подгрупе коначног индекса. На пример, подгрупа од $\mathbb{Z}$ генерисана елементом 3 је индекса 3 (проверити ово).

Теорема 45 (Лагранжова теорема) Нека је G коначна група и $H \leq G$. Тада је

$$|G| = |H| \cdot [G : H].$$

Посебно, ред подгрупе H, дели ред групе G.

Доказ. Како је група G коначна, то је очигледно G коначна унија левих косета подгрупе H, тј. за неке $x_1, \ldots, x_k \in G$ важи:

$$G = x_1 H \sqcup x_2 H \sqcup \cdots \sqcup x_k H,$$

при чему је $k = [G : H]$. Но, $|xH| = |yH|$ за све $x, y \in G$. Наиме, функција $f : xH \to yH$ дефинисана са: $f(xh) = yh$ задаје бијекцију између ова два скупа (проверите ово). Стога је $|G| = |H| \cdot k = |H| \cdot [G : H]$. □

Наведимо неке последице Лагранжове теореме.

Последица 46 Ред сваког елемента коначне групе дели ред те групе.

Доказ. Нека је G коначна група и $x \in G$. Јасно је да ред елемента x мора бити коначан. Осим тога, $\omega(x) = |\langle x \rangle|$, а према Лагранжовој теореми $|\langle x \rangle| \mid |G|$. □

Последица 47 Свака група простог реда је циклична.

Доказ. Нека је $|G| = p$, где је p прост број. Ако је x било који елемент из G различит од неутрала, онда је $\omega(x) \neq 1$ и $\omega(x) \mid p$. Закључујемо да је $\omega(x) = p$, те је $\langle x \rangle = G$. □

Последица 48 Ако је G коначна група и $x \in G$, онда је $x^{|G|} = e$.

Доказ. Присетимо се да је $x^m = e$ ако и само ако $\omega(x) \mid n$. Како $\omega(x) \mid |G|$, резултат следи. □

У скупу $Z_n = \{0, 1, \ldots, n-1\}$, где је $n \geq 2$ можемо увести операцију $\cdot_n$ (множење по модулу n). Наравно, у односу на ову операцију Z_n не чини групу. Посматрајмо стога следећи скуп.

$$\Phi(n) := \{k : 1 \leq k < n, \mathrm{NZD}(k, n) = 1\}.$$

Важи следећи став.

Став 49 За све $n \geq 2$, $(\Phi(n), \cdot_n)$ је комутативна група.

Доказ. Најпре треба проверити да ли множење по модулу n заиста задаје бинарну операцију на скупу $\Phi(n)$, тј. да ли је испуњено следеће:

$$\text{ако } x, y \in \Phi(n) \text{ онда } x \cdot_n y \in \Phi(n).$$

Уколико је $\mathrm{NZD}(x,n) = 1 = \mathrm{NZD}(y,n)$, онда је и $\mathrm{NZD}(x \cdot y, n) = 1$. Наиме, добро нам је познато следеће:

$$\mathrm{NZD}(a,b) = 1 \textbf{ акко постоје } p, q \in \mathbb{Z} \text{ тако да је } ap + bq = 1.$$

Дакле, постоје $p, q \in \mathbb{Z}$ за које је $xp + nq = 1$, као и $p', q' \in \mathbb{Z}$ за које је $yp' + nq' = 1$. Множењем ове две релације, добијамо да је

$$xy(pp') + n(qyp' + xpq' + nqq') = 1,$$

те мора бити $\mathrm{NZD}(x \cdot y, n) = 1$. С обзиром да је

$$x \cdot y \equiv x \cdot_n y \pmod{n},$$

то је и $\mathrm{NZD}(x \cdot_n y, n) = 1$.

Познато нам је да је операција $\cdot_n$ асоцијативна и комутативна. Осим тога, $1 \in \Phi(n)$, па постоји и неутрални елемент за ову операцију. Но, сваки елемент из $\Phi(n)$ заиста има инверз. Наиме, ако $x \in \Phi(n)$, онда постоје $p, q \in \mathbb{Z}$ за које је $xp + nq = 1$. Ако са $\bar{p}$ означимо елемент из Z_n, који је конгруентан елементу p по модулу n, онда је $\bar{p} \in \Phi(n)$ и осим тога је $x \cdot_n \bar{p} = 1$. □

Ред групе $\Phi(n)$ означавамо са $\varphi(n)$. Ова функција φ зове се Ојлерова функција.

Последица 50 (Ојлерова теорема) Нека је $n \geq 2$ и x цео број, узајамно прост са n, онда је

$$x^{\varphi(n)} \equiv 1 \pmod{n}.$$

Доказ. Како је x узајамно прост са n, то је x конгруентан по модулу n неком броју $\bar{x} \in \Phi(n)$. Но, $|\Phi(n)| = \varphi(n)$ и на основу Последице 48 знамо да у групи $\Phi(n)$ важи једнакост $\bar{x}^{\varphi(n)} = 1$. То заправо значи да је $x^{\varphi(n)}$ конгруентно са 1 по модулу n. □

У случају да је p прост број, очигледно је да је $\varphi(p) = p - 1$. Стога добијамо још једну последицу Лагранжове теореме.

Последица 51 (Мала Фермаова теорема) Ако је p прост број, који не дели цео број x, онда је

$$x^{p-1} \equiv 1 \pmod{p}.$$

Како израчунати $\varphi(n)$ за произвољно $n \geq 2$? За функцију φ важи следеће:

1. уколико су m и n узајамно прости, онда је $\varphi(mn) = \varphi(m)\varphi(n)$;
2. за сваки прост број p и $m \geq 1$: $\varphi(p^m) = p^m - p^{m-1}$.

Прву особину доказаћемо када се будемо бавили комутативним прстенима са јединицом, док се друга лако доказује. Наиме, $x \in Z_{p^m} \setminus \{0\}$ није у $\Phi(p^m)$ ако и само ако $p \mid x$. Дакле, $x \in \{p, 2p, \ldots, (p^{m-1}-1)p\}$. Према томе,

$$\varphi(p^m) = |\Phi(p^m)| = (p^m - 1) - (p^{m-1} - 1) = p^m - p^{m-1}.$$

Коришћењем ова два својства, добијамо да важи следећи резултат. Ако је $n = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ факторизација броја n на просте факторе, онда је

$$\begin{aligned}
\varphi(n) &= \varphi(p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}) \\
&= \varphi(p_1^{m_1})\varphi(p_2^{m_2}) \cdots \varphi(p_k^{m_k}) \\
&= p_1^{m_1-1}(p_1-1)p_2^{m_2-1}(p_2-1)\cdots p_k^{m_k-1}(p_k-1) \\
&= p_1^{m_1}\left(1-\frac{1}{p_1}\right) p_2^{m_2}\left(1-\frac{1}{p_2}\right)\cdots p_k^{m_k}\left(1-\frac{1}{p_k}\right) \\
&= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right).
\end{aligned}$$

Лагранжова теорема нам показује да, на пример, група реда 20 не може да има подгрупу реда 12 и сл. Она нам не говори ништа о томе да ли, на пример, група реда 20 има подгрупу реда 10 (постојање такве подгрупе не би било у супротности са Лагранжовом теоремом). Оваква питања су знатно сложенија и ми се њима нећемо много бавити. Само ћемо навести једну теорему, која говори о постојању подгрупа одређеног реда и навести неке њене последице у облику примера.

Теорема 52 (Кошијева теорема) Ако је G коначна група и p прост број такав да $p \mid |G|$, онда у G постоји елемент реда p.

Дакле, уколико је p прост број, који дели ред групе G, у G постоји елемент реда p, а самим тим и подгрупа реда p.

Пример 53 Свака група реда 6 изоморфна је или групи $\mathbb{Z}_6$ или групи $\mathbb{D}_3$.

Нека је $|G| = 6$. Уколико у G постоји елемент реда 6, онда је $G \cong \mathbb{Z}_6$. Претпоставимо стога да у G не постоји елемент реда 6. На основу Кошијеве теореме у G постоји елемент x реда 3 и елемент y реда 2. Како је $\omega(x) = \omega(x^2)$, то $y \notin \langle x \rangle$. Стога је

$$G = \langle x \rangle \sqcup y\langle x \rangle = \{e, x, x^2, y, yx, yx^2\}.$$

Елемент xy је у G и једнак је неком од наведених елемената. Није тешко уверити се (уверите се!) да су једине могућности:

1. $xy = yx$;
2. $xy = yx^2$.

Но, ако је $xy = yx$, добијамо да је

$$G \cong \langle y \rangle \times \langle x \rangle \cong \mathbb{Z}_6$$

(зашто?), што противречи претпоставци да у G нема елемената реда 6. Преостаје могућност $xy = yx^2$ и у том случају је $G \cong \mathbb{D}_3$ (при изоморфизму који x слика у ρ, а y у σ). ♣

Завршићемо ову лекцију описом група реда 8. Да бисмо могли да је извршимо, биће нам потребан још један пример групе.

Добро нам је познато рачунање са комплексним бројевима. Сваки комплексан број се може написати у облику $a + bi$, где су a и b реални бројеви, а i је имагинарна јединица, тј. за i важи следеће: $i^2 = -1$. Хамилтон је у математику увео кватернионе. Сваки кватернион може се написати у облику $a + bi + cj + dk$, где су a, b, c, d реални бројеви, а i, j, k имагинарне јединице за које још важи: $ij = k = -ji, jk = i = -kj, ki = j = -ik$. Као што се може видети, множење кватерниона није комутативно, но многа друга својства, која важе за комплексне бројеве важе и за кватернионе. Наравно, и поред занимљивости кватерниона, ми се нећемо њима детаљно бавити. Но, означимо са Q_8 следећи скуп:

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}.$$

Није тешко уверити се да је $(Q_8, \cdot)$ група. Зовемо је кватернионска група. Наведимо таблицу ове групе.

$\cdot$	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

Приметимо да је Q_8 генерисана елементима i и j и да за ове елементе важи: $i^2 = j^2$ и $jij^{-1} = i^{-1}$.

Пример 54 Свака група реда 8 изоморфна је тачно једној од група:

$$\mathbb{Z}_8, \quad \mathbb{Z}_2 \times \mathbb{Z}_4, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \quad \mathbb{D}_4, \quad Q_8.$$

Нека је G група реда 8. Уколико у G постоји елемент реда 8, онда је $G \cong \mathbb{Z}_8$. Уколико је пак у G сваки елемент реда 2, према ранијем резултату следи да је $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. Претпоставимо у даљем да у G постоји елемент реда 4 и да не постоји елемент реда 8.

Нека је x реда 4 и нека $y \notin \langle x \rangle$. Тада је

$$G = \langle x \rangle \sqcup y\langle x \rangle = \{e, x, x^2, x^3, y, yx, yx^2, yx^3\}.$$

Одредимо који од ових елемената може бити једнак елементу xy. Пре свега, како $y \notin \langle x \rangle$ и како је $x \neq e$, то $xy \notin \{e, x, x^2, x^3, y\}$. Уколико је пак $xy = yx^2$, добијамо да је $x = yx^2y^{-1}$ из чега следи да је $x^2 = yx^4y^{-1} = yey^{-1} = e$, па би x био реда 2, што није. Закључујемо да $xy \in \{yx, yx^3\}$.

Одредимо још колико је y^2. Пре свега, како $y \notin \langle x \rangle$, то $y^2 \notin y\langle x \rangle$. Осим тога, како је $\omega(x) = \omega(x^3) = 4$, а у G нема елемената реда 8 то y^2 не може бити ни x ни x^3. Дакле, $y^2 \in \{e, x^2\}$.

Добили смо 4 случаја

1. $xy = yx$, $y^2 = e$;
2. $xy = yx$, $y^2 = x^2$;
3. $xy = yx^3$, $y^2 = e$;
4. $xy = yx^3$, $y^2 = x^2$.

Размотримо сваки посебно.

1. У овом случају је група G комутативна и функција $f\colon \mathbb{Z}_2 \times \mathbb{Z}_4 \to G$ дефинисана са $f(r, s) = y^r x^s$ је изоморфизам. Јасно је да је f бијекција. Само треба проверити слагање са операцијама.

$$f(r +_2 r', s +_4 s') = y^{r+_2 r'} x^{s+_4 s'}.$$

Како је y реда 2 и x реда 4, то је $y^{r+_2 r'} = y^r y^{r'}$ и $x^{s+_4 s'} = x^s x^{s'}$. Дакле,

$$f(r +_2 r', s +_4 s') = y^r y^{r'} x^s x^{s'}.$$

Како је $xy = yx$, то је

$$y^r y^{r'} x^s x^{s'} = y^r x^s y^{r'} x^{s'} = f(r, s) f(r', s').$$

Дакле, заиста је

$$f(r +_2 r', s +_4 s') = f(r, s) f(r', s').$$

2. У овом случају је такође група G комутативна. Приметимо да је сада елемент y реда 4, но елемент $y^3 x$ је реда 2:

$$(y^3 x)^2 = y^6 x^2 = x^6 x^2 = x^8 = e.$$

Стога је изоморфизам $f\colon \mathbb{Z}_2 \times \mathbb{Z}_4 \to G$ задат са: $f(r, s) = (y^3 x)^r x^s$. Проверите детаље!

3. У овом случају, ситуација је јасна. Изоморфизам $f\colon \mathbb{D}_4 \to G$ задат је са: $f(\sigma) = y$, $f(\rho) = x$.

4. И у овом случају није тешко видети како функција $f\colon Q_8 \to G$ задата са: $f(i) = x$, $f(j) = y$ задаје изоморфизам (важно је приметити да је $ij = k = ji^3$ и $i^2 = j^2$). ♣

Нормалне погрупе

У случају да је $H \leq G$ разматрали смо скуп G/H, скуп свих левих косета подгрупе H у групи G. Испоставља се да се у неким случајевима на овом скупу може задати структура групе.

Уведимо најпре следећу дефиницију.

Дефиниција 55 Нека је G група и $x, y \in G$. Елемент y је конјугован елементу x уколико постоји $g \in G$ за који је $y = gxg^{-1}$.

Није тешко уверити се да је на овај начин дефинисана једна релација еквиваленције. Наиме, сваки елемент је конјугован сам себи: $x = exe^{-1}$. Ако је y конјугован елементу x, тј. ако је $y = gxg^{-1}$, онда је и $x = (g^{-1})y(g^{-1})^{-1}$, па је x конјугован елементу y. Проверу транзитивности остављамо читаоцима. Класе еквиваленције при овој релацији називају се и класе конјугације.

Дефиниција 56 Подгрупа H групе G је нормална уколико је H унија неких класа конјугације. Ако је H нормална подгрупа од G онда пишемо:

$$H \triangleleft G.$$

Став 57 Нека је $H \leq G$. Следећи услови су еквивалентни:

1. $H \triangleleft G$;
2. за све $g \in G$: $gHg^{-1} \subseteq H$;
3. за све $g \in G$: $gH = Hg$.

Доказ.

$1 \implies 2$. Нека су $g \in G$ и $h \in H$ произвољни. Елемент ghg^{-1} је конјугат елемента $h \in H$. Како је H нормална подгрупа, она је унија класа конјугације, па самим тим мора да садржи целу класу конјугације елемента h. Стога је и $ghg^{-1} \in H$.

$2 \implies 3$. Нека је $g \in G$ произвољан елемент. Докажимо да је $gH \subseteq Hg$. Посматрајмо елемент $h \in H$. На основу 2, $ghg^{-1} \in H$, па је $ghg^{-1} = h'$ за неко $h' \in H$. Но, тада је и $gh = h'g \in Hg$, па закључујемо да је $gH \subseteq Hg$. Обратно, уочимо елемент $hg \in Hg$. Елемент $g^{-1}h(g^{-1})^{-1}$ на основу 2 припада H, па је $g^{-1}h(g^{-1})^{-1} = h_1$ за неко $h_1 \in H$. Стога је $hg = gh_1 \in gH$, те је $Hg \subseteq gH$.

$3 \implies 1$. Претпоставимо да је C нека класа конјугације за коју је $C \cap H \neq \emptyset$. Треба доказати да је $C \subseteq H$. Узмимо елемент $h \in C \cap H$. Тада је сваки елемент из C облика ghg^{-1} за неки $g \in G$. Но, како је

по 3, $gH = Hg$, то је $gh = h'g$ за неко $h' \in H$, па је $ghg^{-1} = h'gg^{-1} = h'$. Закључујемо да $ghg^{-1} \in H$. Дакле, заиста је $C \subseteq H$. □

Приметимо да, у случају да је $H \triangleleft G$, важи једнакост $gHg^{-1} = H$.

Став 58 Свака подгрупа индекса 2 је нормална.

Доказ. Нека је $H \leq G$ и $[G : H] = 2$. То значи да је за сваки елемент $a \notin H$ из G испуњено:

$$G = H \sqcup aH.$$

Но, такође је и

$$G = H \sqcup Ha.$$

Како је $aH \cap H = \emptyset$, мора бити $aH \subseteq Ha$. Но, из истих разлога је $Ha \subseteq aH$. Закључујемо да је $aH = Ha$ за све $a \in G \setminus H$. Ако пак $a \in H$, онда је $aH = H$ (H је подгрупа, па је производ ма која два елемента из H у H; осим тога, ако је $h \in H$ произвољан елемент, онда је $h = a(a^{-1}h) \in aH$), а такође је и $Ha = H$. Дакле, и у овом случају важи једнакост $aH = Ha$, па је $H \triangleleft G$. □

Дефиниција 59 Нека је G група. Дефинишемо центар групе G, у ознаци $Z(G)$ са:

$$Z(G) := \{g \in G : (\forall x \in G)(xg = gx)\}.$$

Став 60 $Z(G)$ је подгрупа групе G.

Доказ. Како је $ex = xe$ за све $x \in G$, то $e \in Z(G)$. Претпоставимо да g припада центру. То значи да је $gx = xg$ за све $x \in G$. Но, тада следи да је и $g^{-1}x = xg^{-1}$ за све $x \in G$, те $g^{-1} \in Z(G)$. Коначно, ако $g, h \in Z(G)$ и $x \in G$, онда је

$$(gh)x = g(hx) = g(xh) = (gx)h = (xg)h = x(gh),$$

те $gh \in Z(G)$. □

Пример 61 Важи следеће:

1. за све $n \geq 2$: $A_n \triangleleft \mathbb{S}_n$;
2. за сваку групу G: $\{e\} \triangleleft G$;
3. за сваку групу G: $G \triangleleft G$;
4. за сваку групу G: $Z(G) \triangleleft G$;
5. за све $n \geq 3$: $\langle \rho \rangle \triangleleft \mathbb{D}_n$.

Количничке групе

У случају да су X и Y подскупови од G, дефинишемо $X \cdot Y$ са:

$$X \cdot Y := \{x \cdot y : x \in X, y \in Y\}.$$

Став 62 Скуп свих левих косета нормалне подгрупе H групе G чини једну групу у односу на управо дефинисано множење подскупова од G.

Доказ. Нека су aH и bH произвољни косети. Докажимо да је, при услову да је $H \triangleleft G$,

$$(aH) \cdot (bH) = (ab)H.$$

Ово није тешко доказати. Наиме, приметимо да је $HH = H$. Јасно је да је $HH \subseteq H$ (производ два елемента из H такође је у H пошто је H подгрупа од G). Осим тога, како $e \in H$, добијамо $H = eH \subseteq HH$. Добијамо:

$$(aH) \cdot (bH) = a(Hb)H = a(bH)H = (ab)(HH) = (ab)H.$$

Овде смо користили чињеницу да је $H \triangleleft G$ и асоцијативност множења.

Сада није тешко показати да је $(G/H, \cdot)$ група. Наиме,

$$((aH) \cdot (bH)) \cdot (cH) = ((ab)H) \cdot (cH) =$$

$$= ((ab)c)H = (a(bc))H = (aH) \cdot ((bc)H) = (aH) \cdot ((bH) \cdot (cH)).$$

Јасно је да је $H = eH$ неутрал:

$$(aH) \cdot H = (aH) \cdot (eH) = (ae)H = aH,$$

као и

$$H \cdot (aH) = (eH) \cdot (aH) = (ea)H = aH.$$

Инверз елемента aH је $a^{-1}H$:

$$(aH) \cdot (a^{-1}H) = (aa^{-1})H = eH = H;$$

$$(a^{-1}H) \cdot (aH) = (a^{-1}a)H = eH = H.$$

□

Овако добијена група зове се количничка група групе G по нормалној подгрупи H. Убудуће, када говоримо о групи G/H подразумевамо да је H нормална подгрупа од G и да је множење косета дефинисано на наведени начин. Наравно, често нећемо писати неке непотребне заграде и знак множења.

Дефиниција 63 Група G је проста уколико су њене једине нормалне подгрупе G и $\{e\}$.

Уколико група G није комутативна, то не мора бити ни њена количничка група. Ипак има случајева у којима количничка група јесте комутативна, а сама група то није.

Дефиниција 64 Ако су $x, y \in G$, дефинишемо комутатор елемената x и y, у ознаци $[x, y]$ са:

$$[x, y] := x^{-1}y^{-1}xy.$$

Приметимо да је $xy = yx$ акко $[x, y] = e$. Подгрупу групе G генерисану комутаторима означавамо са $[G, G]$ и зовемо комутаторска подгрупа од G.

Став 65 а) Комутаторска подгрупа је нормална подгрупа.
б) Ако је $H \triangleleft G$, онда је G/H комутативна ако и само ако је $[G, G] \subseteq H$.

Доказ. а) Производ два комутатора не мора бити комутатор, али инверз ма ког комутатора јесте комутатор:

$$[x, y]^{-1} = (x^{-1}y^{-1}xy)^{-1} = y^{-1}x^{-1}(y^{-1})^{-1}(x^{-1})^{-1} = y^{-1}x^{-1}yx = [y, x].$$

У сваком случају, ми посматрамо подгрупу генерисану комутаторима и треба да покажемо да је она нормална. Сваки елемент подгрупе генерисане неким скупом X је скуп свих могућих производа елемената из X и њихових инверза. Како је инверз комутатора и сам комутатор, то је сваки елемент из комутаторске групе производ комутатора. Стога, нека су $g, x_1, y_1, \ldots, x_n, y_n$ произвољни елементи групе G. Тада је

$$g[x_1, y_1][x_2, y_2] \cdots [x_n, y_n]g^{-1} = (g[x_1, y_1]g^{-1})(g[x_2, y_2]g^{-1}) \cdots (g[x_n, y_n]g^{-1})$$

Но,

$$g[x, y]g^{-1} = gx^{-1}y^{-1}xyg^{-1} = (gx^{-1}g^{-1})(gy^{-1}g^{-1})(gxg^{-1})(gyg^{-1}) =$$

$$= (gxg^{-1})^{-1}(gyg^{-1})^{-1}(gxg^{-1})(gyg^{-1}) = [gxg^{-1}, gyg^{-1}],$$

те добијамо

$$g[x_1, y_1] \cdots [x_n, y_n]g^{-1} = [gx_1g^{-1}, gy_1g^{-1}] \cdots [gx_ng^{-1}, gy_ng^{-1}] \in [G, G].$$

б) $\Rightarrow$: Претпоставимо да је група G/H комутативна. То значи да је за све $x, y \in G$ испуњено:

$$xH \cdot yH = yH \cdot xH.$$

Другим речима,

$$xyH = yxH,$$

па мора бити

$$(yx)^{-1}(yx) \in H,$$

те

$$[x, y] = x^{-1}y^{-1}xy \in H.$$

Дакле, комутатор ма која два елемента је у H, па закључујемо да је $[G, G] \subseteq H$.

$\Leftarrow$: Претпоставимо да је $[G, G] \subseteq H$. Треба показати да је група G/H комутативна. Нека су $x, y \in G$ произвољни елементи. По претпоставци $[x, y] \in H$, тј. $x^{-1}y^{-1}xy \in H$. То значи да је $(yx)^{-1}(xy) \in H$, па мора бити $(yx)H = (xy)H$, тј. $(yH) \cdot (xH) = (xH) \cdot (yH)$. Закључујемо да је G/H комутативна група. □

Група $G/[G, G]$ назива се Абелизација групе G и означава са G^{Ab} (комутативне групе се зову и Абелове групе). Понеки пут је погодно за испитивање да ли су две групе изоморфне прећи на њихове Абелизације, зато што важи следећи став.

Став 66 Ако је $G \cong H$ онда је и $G^{\mathrm{Ab}} \cong H^{\mathrm{Ab}}$.

Нека је $f\colon G \to H$ изоморфизам. Тада је $f([x, y]) = [f(x), f(y)]$, што се лако може установити. Одавде следи да

$$f\left[[G, G]\right] \subseteq [H, H]. \tag{1}$$

Дефинишимо функцију

$$\tilde{f}\colon G^{\mathrm{Ab}} \to H^{\mathrm{Ab}},$$

са:

$$\tilde{f}(x[G, G]) := f(x)[H, H].$$

Показаћемо да је $\tilde{f}$ добро дефинисана функција, која остварује изоморфизам између $G/[G, G]$ и $H/[H, H]$.

Добра дефинисаност: Нека је

$$x[G, G] = y[G, G].$$

Треба показати да је

$$f(x)[H, H] = f(y)[H, H].$$

Но, како је $x[G, G] = y[G, G]$, мора бити $x^{-1}y \in [G, G]$, па на основу (1) следи да $f(x)^{-1}f(y) = f(x^{-1}y) \in [H, H]$. Дакле, заиста је

$$f(x)[H, H] = f(y)[H, H].$$

$\tilde{f}$ је „на”: Нека је $z[H,H]$ произвољан елемент из H^{Ab}. Како је f „на”, то постоји $x \in G$ за који је $f(x) = z$. Но, тада је $\tilde{f}(x[G,G]) = f(x)[H,H] = z[H,H]$, па је $\tilde{f}$ заиста „на”.

$\tilde{f}$ је „1–1”: Ако је

$$\tilde{f}(x[G,G]) = \tilde{f}(y[G,G]),$$

то значи да је

$$f(x)[H,H] = f(y)[H,H],$$

па је

$$f(x^{-1}y) \in [H,H].$$

Другим речима, за неке $z_1, u_1, \ldots, z_n, u_n \in H$ је

$$f(x^{-1}y) = [z_1,u_1]\cdots[z_n,u_n].$$

Како је f „на”, то постоје $x_1, y_1, \ldots, x_n, y_n \in G$ такви да је

$$f(x_1) = z_1, \ldots, f(x_n) = z_n, \quad f(y_1) = u_1, \ldots, f(y_n) = u_n.$$

То значи да је

$$f(x^{-1}y) = [f(x_1),f(y_1)]\cdots[f(x_n),f(y_n)] = f([x_1,y_1]\cdots[x_n,y_n]).$$

Како је f „1–1”, мора бити

$$x^{-1}y = [x_1,y_1]\cdots[x_n,y_n].$$

Следи да $x^{-1}y \in [G,G]$, па је $x[G,G] = y[G,G]$ и закључујемо да је и функција $\tilde{f}$ „1–1”.

$\tilde{f}$ се слаже са операцијама:

$$\tilde{f}((x[G,G])\cdot(y[G,G])) = \tilde{f}((xy)[G,G]) = f(xy)[H,H] = (f(x)f(y))[H,H] =$$

$$= (f(x)[H,H])(f(y)[H,H]) = \tilde{f}(x[G,G])\tilde{f}(x[G,G]).$$

Закључујемо да је $\tilde{f}$ заиста изоморфизам. □

Пример 67 За све $n \geq 2$: $\mathbb{S}_n^{\mathrm{Ab}} \cong \mathbb{Z}_2$.

Показаћемо да је $[\mathbb{S}_n,\mathbb{S}_n] = A_n$ за све $n \geq 2$. Јасно је да је $\pi^{-1}\sigma^{-1}\pi\sigma$ парна пермутација за сваке две пермутације π и σ (зашто?). Према томе, $[\mathbb{S}_n,\mathbb{S}_n] \subseteq A_n$.

Случај $n = 2$ је тривијалан. Претпоставимо стога да је $n \geq 3$. Докажимо да сваки цикл дужине 3 припада $[\mathbb{S}_n,\mathbb{S}_n]$. Како ти цикли генеришу A_n, добићемо да је $[\mathbb{S}_n,\mathbb{S}_n] = A_n$. Но,

$$(abc) = (ab)(bc) = (ab)(ac)(ab)(ac) = (ab)^{-1}(ac)^{-1}(ab)(ac) = [(ab),(ac)].$$

Како је $[\mathbb{S}_n : A_n] = 2$, то је група $\mathbb{S}_n/A_n$ реда 2 и као таква је изоморфна групи $\mathbb{Z}_2$. ♣

Пример 68 За све $l \geq 2$:

1. $(\mathbb{D}_{2s})^{\mathrm{Ab}} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$;
2. $(\mathbb{D}_{2s-1})^{\mathrm{Ab}} \cong \mathbb{Z}_2$.

Показаћемо најпре да је $[\mathbb{D}_n, \mathbb{D}_n] = \langle \rho^2 \rangle$. Проверимо све случајеве:

1. $[\rho^k, \rho^l] = \varepsilon$;
2. $[\sigma\rho^k, \rho^l] = (\sigma\rho^k)^{-1}(\rho^l)^{-1}(\sigma\rho^k)\rho^l = \sigma\rho^k\rho^{-l}\sigma\rho^k\rho^l = \rho^{-k}\rho^l\rho^{k+l} = \rho^{2l}$;
3. $[\rho^k, \sigma\rho^l] = (\rho^k)^{-1}(\sigma\rho^l)^{-1}\rho^k(\sigma\rho^l) = \rho^{-k}\sigma\rho^l\rho^k\sigma\rho^l = \rho^{-k}\rho^{-l}\rho^{-k}\rho^l = \rho^{-2k}$;
4. $[\sigma\rho^k, \sigma\rho^l] = (\sigma\rho^k)^{-1}(\sigma\rho^l)^{-1}\sigma\rho^k\sigma\rho^l = \sigma\rho^k\sigma\rho^l\sigma\rho^k\sigma\rho^l = \rho^{-k}\rho^l\rho^{-k}\rho^l = \rho^{2l-2k}$.

Видимо да је заиста $[\mathbb{D}_n, \mathbb{D}_n] = \langle \rho^2 \rangle$. Сада се разликују случајеви када је n парно, односно непарно. Наиме, ако је $n = 2s-1$, ред елемента ρ^2 је n (зашто?), па је $\langle \rho^2 \rangle = \langle \rho \rangle$. Стога је $[\mathbb{D}_{2s-1}, \mathbb{D}_{2s-1}] = \langle \rho \rangle$ и заиста је $(\mathbb{D}_{2s-1})^{\mathrm{Ab}} \cong \mathbb{Z}_2$.

У случају $n = 2s$, ред елемента ρ^2 је s и

$$(\mathbb{D}_{2s})^{\mathrm{Ab}} = \{\langle \rho^2 \rangle, \sigma\langle \rho^2 \rangle, \rho\langle \rho^2 \rangle, \sigma\rho\langle \rho^2 \rangle\}.$$

Ово је група са 4 елемента у којој је сваки елемент реда 2 (проверити ово!), па на основу ранијих резултата (а може и директно), добијамо да је $(\mathbb{D}_{2s})^{\mathrm{Ab}} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. ♣

Докажимо на крају још један став, који нам даје карактеризацију група одређеног реда.

Став 69 Ако је p непаран прост број, онда је свака група реда $2p$ или циклична или је изоморфна групи $\mathbb{D}_p$.

Доказ. Нека је G група реда $2p$. На основу Кошијеве теореме, у групи G постоји елемент x реда p и елемент y реда 2. Како ред елемента дели ред групе, то $y \notin \langle x \rangle$. Стога је

$$G = \langle x \rangle \sqcup y\langle x \rangle = \{e, x, \ldots, x^{p-1}, y, yx, \ldots, yx^{p-1}\}.$$

Ред елемента yx може бити 2, p или $2p$ ($yx \neq e$). Уколико је $\omega(yx) = 2p$, група G је циклична.

Покажимо да $\omega(yx) \neq p$. Претпоставимо да је $\omega(yx) = p$. Тада добијамо (рачунамо у групи $G/\langle x \rangle$ — подгрупа $\langle x \rangle$ је нормална пошто је индекса 2):

$$\langle x \rangle = e\langle x \rangle = (yx)^p\langle x \rangle = (yx\langle x \rangle)^p = (y\langle x \rangle)^p = y^p\langle x \rangle.$$

Дакле, $y^p \in \langle x \rangle$. Како је p непаран број, а $\omega(y) = 2$, мора бити $y \in \langle x \rangle$, што није тачно. Добили смо контрадикцију, те можемо закључити да

$\omega(yx) \neq p$. Остаје случај $\omega(yx) = 2$. Тада добијамо да је $(yx)^2 = e$, па је $yxyx = e$ из чега следи да је $yx = x^{-1}y$. С обзиром да је $x^p = e$ и $y^2 = e$, видимо да се изоморфизам између G и $\mathbb{D}_p$ може остварити придруживањем $y \mapsto \sigma$, $x \mapsto \rho$. □

Хомоморфизми група

Већ смо упознати са појмом изоморфизма група. Општији појам је појам хомоморфизма.

Дефиниција 70 Нека су $(G, \cdot)$ и $(H, *)$ групе. Функција $f: G \to H$ је хомоморфизам уколико за све $x, y \in G$ важи:

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

Дакле, изоморфизам је онај хомоморфизам који је и бијекција. Приметимо да се лако показује, на исти начин као и у случају изоморфизма, да се при сваком хомоморфизму неутрал групе G слика у неутрал групе H, а инверз елемента из групе G у инверз његове слике у групи H (подсетите се тог доказа). Како хомоморфизам не мора бити бијекција, природно је испитати у којој мери дати хомоморфизам „одступа" од изоморфизма. Важан појам у вези са тим је и појам *језгра* хомоморфизма.

Дефиниција 71 Нека је $f: G \to H$ хомоморфизам група. Језгро хомоморфизма f, у ознаци $\mathrm{Ker}(f)$ дефинише се са:

$$\mathrm{Ker}(f) := \{g \in G : f(g) = e_H\},$$

где је са e_H означен неутрал у H.

Став 72 Језгро сваког хоморфизма $f: G \to H$ је нормална подгрупа групе G.

Доказ. Како је $f(e_G) = e_H$, то $e_G \in \mathrm{Ker}(f)$, па $\mathrm{Ker}(f) \neq \emptyset$. Претпоставимо да $x, y \in \mathrm{Ker}(f)$. Треба показати да $x^{-1}y \in \mathrm{Ker}(f)$. Но,

$$f(x^{-1}y) = f(x)^{-1} * f(y) = e_H^{-1} * e_H = e_H,$$

те заиста $x^{-1}y \in \mathrm{Ker}(f)$. Дакле, доказали смо да је $\mathrm{Ker}(f) \leq G$.

Да бисмо показали да је језгро нормална подгрупа, посматрајмо произвољне елементе $x \in \mathrm{Ker}(f)$ и $g \in G$. Тада је

$$f(gxg^{-1}) = f(g) * f(x) * f(g)^{-1} = f(g) * e_H * f(g)^{-1} = e_H,$$

те закључујемо да је $g\mathrm{Ker}(f)g^{-1} \subseteq \mathrm{Ker}(f)$, за све $g \in G$, те је заиста $\mathrm{Ker}(f) \triangleleft G$. □

Став 73 Хомоморфизам група $f: G \to H$ је „1–1" ако и само ако је

$$\mathrm{Ker}(f) = \{e_G\}.$$

Доказ.
$\Longrightarrow$: Претпоставимо да је f „1–1" и нека $x \in \mathrm{Ker}(f)$. То значи да је

$$f(x) = e_H = f(e_G).$$

Како је f „1–1", мора бити $x = e_G$. Закључујемо да је $\mathrm{Ker}(f) = \{e_G\}$.
$\Longleftarrow$: Нека је $\mathrm{Ker}(f) = \{e_G\}$. Претпоставимо да је $f(x) = f(y)$. То значи да је

$$f(x^{-1}y) = f(x^{-1}) * f(y) = f(x)^{-1} * f(y) = e_H^{-1} * e_H = e_H,$$

па је $x^{-1}y \in \mathrm{Ker}(f) = \{e_G\}$. Добијамо да је $x = y$, те закључујемо да је f „1–1". □

Уколико је $\mathrm{Ker}(f) = \{e_G\}$, кажемо и да је језгро тривијално. Ако је f „1–1" хомоморфизам, кажемо и да је f *мономорфизам*.

Дефиниција 74 Слика хомоморфизма $f: G \to H$, у ознаци $\mathrm{Im}(f)$, дефинише се са:

$$\mathrm{Im}(f) := \{y \in H : (\exists x \in G) y = f(x)\}.$$

Дакле, слика хоморфизма је заправо обична слика функције f.

Став 75 Ако је $f: G \to H$ хомоморфизам, онда је $\mathrm{Im}(f) \leq H$.

Доказ. Како је $e_H = f(e_G)$, то $\mathrm{Im}(f) \neq \emptyset$. Претпоставимо да $y_1, y_2 \in \mathrm{Im}(f)$. То значи да постоје x_1, x_2 такви да је $f(x_1) = y_1$ и $f(x_2) = y_2$. Но, тада је

$$y_1^{-1} * y_2 = f(x_1)^{-1} * f(x_2) = f(x_1^{-1}x_2) \in \mathrm{Im}(f).$$

□

Приметимо да слика хомоморфизма не мора бити нормална подгрупа од H. Наиме, ако је $H \leq G$ онда је слика од H при инклузији (која је хомоморфизам) сама подгрупа H и ако она није нормална, то нам даје тражени пример.

Теореме о изоморфизмима

Хомоморфизам, који је уједно и „на", зовемо *епиморфизам*. Основни пример епиморфизма је следећи. Нека је G група и H ма која њена нормална подгрупа. Тада је са $p(a) = aH$ задат један *епиморфизам* $p\colon G \to G/H$. Наравно, јасно је да је p „на". Осим тога

$$p(ab) = (ab)H = (aH)(bH) = p(a)p(b),$$

те је p и хомоморфизам.

Наведимо сада прву теорему о изоморфизмима за групе.

Теорема 76 Нека је $f\colon G \to H$ хомоморфизам група. Тада f индукује изоморфизам $\tilde{f}\colon G/\mathrm{Ker}(f) \to \mathrm{Im}(f)$ дефинисан са: $\tilde{f}(x\,\mathrm{Ker}(f)) := f(x)$.

Доказ. Покажимо најпре да је $\tilde{f}$ добро дефинисана функција. Наиме, нека је $x\,\mathrm{Ker}(f) = y\,\mathrm{Ker}(f)$. То значи да $x^{-1}y \in \mathrm{Ker}(f)$. Дакле, $f(x^{-1}y) = e_H$, па је $f(x) = f(y)$, те је $\tilde{f}(x\,\mathrm{Ker}(f)) = \tilde{f}(y\,\mathrm{Ker}(f))$. Функција $\tilde{f}$ је хомоморфизам:

$$\tilde{f}\left((x\,\mathrm{Ker}(f))(y\,\mathrm{Ker}(f))\right) = \tilde{f}((xy)\,\mathrm{Ker}(f)) = f(xy) = f(x) * f(y) =$$

$$= \tilde{f}(x\,\mathrm{Ker}(f)) * \tilde{f}(y\,\mathrm{Ker}(f)).$$

Из дефиниције хомоморфизма $\tilde{f}$, очигледно је да је $\mathrm{Im}(\tilde{f}) = \mathrm{Im}(f)$.

Остаје да се покаже да је $\tilde{f}$ „1–1". тј. да је $\mathrm{Ker}(\tilde{f})$ тривијално. Претпоставимо да $x\,\mathrm{Ker}(f) \in \mathrm{Ker}(\tilde{f})$. То значи да је $\tilde{f}(x\,\mathrm{Ker}(f)) = e_H$. Из дефиниције $\tilde{f}$, следи да $x \in \mathrm{Ker}(f)$, те је $x\,\mathrm{Ker}(f) = \mathrm{Ker}(f)$. □

Наведимо неке примере примене ове теореме.

Пример 77 Ако са $\rho(x, n)$ означимо остатак при дељењу целог броја x природним бројем $n \geq 2$, онда је са $f(x) = \rho(x, n)$ дефинисан хомоморфизам група $f\colon \mathbb{Z} \to \mathbb{Z}_n$, који индукује изоморфизам $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

Препоручујемо читаоцима да се сами увере у наведени резултат.

Пример 78 Ако са V означимо подгрупу групе S_4 дату са:

$$V = \{(1), (12)(34), (13)(24), (14)(23)\},$$

онда је $V \lhd S_4$ и $S_4/V \cong S_3$.

Већ нам је познато да је V нормална подгрупа (зашто то знамо?). Остаје да се нађе тражени изоморфизам. У ту сврху, ако је $X = \{(12)(34), (13)(24), (14)(23)\}$, дефинишимо хомоморфизам $f : S_4 \to S_X$ са:

$$f(\pi)(x) = \pi x \pi^{-1},$$

за $x \in X$. Како је $V \lhd S_4$, јасно је да је $\pi x \pi^{-1} \in V$, за све $x \in X \subset V$. Но, не може бити $\pi x \pi^{-1} = (1)$, јер би тада било $x = (1)$, што није тачно. Дакле, $f(\pi)$ заиста припада S_X. Проверимо да ли је f хомоморфизам:

$$f(\sigma\pi)(x) = (\sigma\pi)x(\sigma\pi)^{-1} = \sigma(\pi x \pi^{-1})\sigma^{-1} = f(\sigma)(\pi x \pi^{-1}) = f(\sigma)(f(\pi)(x)).$$

Добијамо да је $f(\sigma\pi) = f(\sigma) \circ f(\pi)$, те је f заиста хомоморфизам.

Одредимо језгро хомоморфизма f. Пре свега, како је V комутативна, то је $V \subseteq \mathrm{Ker}(f)$ (зашто?). Покажимо да важи и обратно, тј. да је заправо $\mathrm{Ker}(f) = V$. Претпоставимо да $\pi \in \mathrm{Ker}(f)$. То значи да је π пермутација из S_4 за коју важи:

$$\pi(12)(34)\pi^{-1} = (12)(34), \quad (2)$$
$$\pi(13)(24)\pi^{-1} = (13)(24), \quad (3)$$
$$\pi(14)(23)\pi^{-1} = (14)(23). \quad (4)$$

Претпоставимо да је $\pi(1) = 1$. Како је $\pi(12)(34)\pi^{-1} = (\pi(1)\pi(2))(\pi(3)\pi(4))$, из претпоставке да је $\pi(1) = 1$ и једнакости (2), следи да је

$$(1\pi(2))(\pi(3)\pi(4)) = (12)(34).$$

Видимо да мора бити $\pi(2) = 2$ и $\pi(3) \in \{3, 4\}$. Уколико је $\pi(3) = 3$, добијамо да је $\pi = (1) \in V$. Претпоставимо да је $\pi(3) = 4$. То значи да је заправо $\pi = (34)$. Но, то би значило да је

$$\pi(13)(24)\pi^{-1} = (\pi(1)\pi(3))(\pi(2)\pi(4)) = (14)(23),$$

што је у супротности са (3). Дакле, претпоставка да је $\pi(1) = 1$, доводи до закључка да је π идентична пермутација, те да π припада V. На исти начин се показује да, уколико је $\pi(k) = k$ за било које k, мора бити $\pi = (1)$.

Претпоставимо да π нема фиксну тачку . Сада можемо, без губитка општости, претпоставити да је $\pi(1) = 2$. Из (2) добијамо

$$(2\pi(2))(\pi(3)\pi(4)) = (12)(34).$$

Очигледно да мора бити $\pi(2) = 1$ и $\pi(3) \in \{3, 4\}$. Како π нема фиксну тачку, добијамо да је $\pi(3) = 4$ и $\pi(4) = 3$, тј. $\pi = (12)(34) \in V$.

На овај начин смо показали да је $\mathrm{Ker}(f) = V$. Прва теорема о изоморфизмима каже да је тада

$$S_4/\mathrm{Ker}(f) \cong \mathrm{Im}(f),$$

тј. да је количничка група S_4/V изоморфна једној подгрупи од S_X. Но, $|S_4/V| = 24/4 = 6 = |S_X|$. Закључујемо да мора бити $\mathrm{Im}(f) = S_X$ и добијамо изоморфизам $S_4/V \cong S_X \cong S_3$. ♣

Наведимо сада један став, који се доказује помоћу наведене теореме (мада га ми нећемо давати).

Став 79 Ако је H подгрупа групе G таква да је $[G : H] = p$, при чему је p најмањи прост број који дели ред групе G, онда је $H \triangleleft G$.

Напомена: Као и увек, врло је важно да се у тврђење не уноси нешто чега у њему нема! Дакле, уопште се не тврди да *за сваку групу* G уопште постоји подгрупа H индекса као у ставу. Но, *ако постоји*, онда је она нормална.

Пример 80 Свака група реда 15 је циклична.

На основу Кошијеве теореме постоји елемент x реда 3 и елемент y реда 5. Подгрупа $H = \langle y \rangle$ је стога индекса 3 и на основу претходног става она је нормална. Стога је

$$xyx^{-1} = y^r \tag{5}$$

за неко $r \in \{1, 2, 3, 4\}$. Уколико је $r = 1$, онда на стандардан начин добијамо да је $G \cong \langle x \rangle \times \langle y \rangle \cong \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_{15}$. Покажимо да остале могућности за r нису могуће. Ако (5) помножимо слева са x и здесна са x^{-1}, добијамо

$$x^2yx^{-2} = xy^rx^{-1} = (xyx^{-1})^r = (y^r)^r = y^{r^2}. \tag{6}$$

Множењем (6) слева са x и здесна са x^{-1} добијамо

$$x^3yx^{-3} = y^{r^3}. \tag{7}$$

Но, с обзиром да је $x^3 = e$ из (7) добијамо

$$y = y^{r^3}, \tag{8}$$

тј.

$$y^{r^3-1} = e. \tag{9}$$

Дакле, с обзиром да је $\omega(y) = 5$, мора бити $5 \mid r^3 - 1$. Но, лако се може проверити да 5 не дели ниједан од бројева $2^3 - 1$, $3^3 - 1$, $4^3 - 1$. ♣

Друга и трећа теорема о изоморфизмима укључују у своју формулацију две подгрупе дате групе G.

Теорема 81 (Друга теорема о изоморфизмима) Нека је G група, $H \leq G$ и $K \triangleleft G$. Тада је $HK \leq G$, $H \cap K \triangleleft H$ и

$$HK/K \cong H/H \cap K.$$

Доказ. Пре свега, треба показати да је $HK \leq G$. Како $e \in H \cap K$, то је $e = ee \in HK$, па $HK \neq \emptyset$. Претпоставимо да су x и y елементи из HK. Дакле, постоје елементи $h, h' \in H$ и $k, k' \in K$ такви да је $x = hk$, $y = h'k'$. Тада је

$$x^{-1}y = k^{-1}h^{-1}h'k' = k^{-1}((h')^{-1}h)^{-1}k' =$$

$$= \overbrace{((h')^{-1}h)^{-1}}^{\in H} \underbrace{\overbrace{\left(\underbrace{((h')^{-1}h)}_{\in H}\underbrace{k^{-1}}_{\in K}((h')^{-1}h)^{-1}\right)}^{\in K}}_{\in K} k' \in HK.$$

С обзиром да је $K \triangleleft G$, то је и $K \triangleleft HK$. Дефинишимо функцију $f: H \to HK/K$ са: $f(h) = hK$. С обзиром да је

$$f(hh') = (hh')K = (hK)(h'K) = f(h)f(h'),$$

f је хомоморфизам.

Докажимо да је f „на". Нека је xK произвољан елемент из HK/K. Дакле, за неко $h \in H$ и $k \in K$, $x = hk$. Тада је

$$xK = (hk)K = h(kK) = hK = f(h),$$

па је f заиста „на".

Одредимо језгро хомоморфизма f. Узмимо произвољни елемент $h \in H$. Тада $h \in \mathrm{Ker}(f)$ ако и само ако је $f(h) = K$ (K је неутрал у HK/K). С обзиром да је $f(h) = hK$, добијамо да је $h \in \mathrm{Ker}(f)$ ако и само ако $h \in K$, тј. $\mathrm{Ker}(f) = H \cap K$. Прва теорема о изоморфизмима даје: $H/\mathrm{Ker}(f) \cong \mathrm{Im}(f)$, тј. $H/H \cap K \cong HK/K$. Приметимо да $H \cap K \triangleleft H$ следи из чињенице да је $H \cap K$ језгро неког хомоморфизма. □

Пример 82 Нека су $m, n \geq 2$ природни бројеви. Применити другу теорему о изоморфизмима на групе $\mathbb{Z}$, $m\mathbb{Z}$ и $n\mathbb{Z}$.

Друга теорема о изоморфизмима даје

$$(m\mathbb{Z} + n\mathbb{Z})/n\mathbb{Z} \cong m\mathbb{Z}/(m\mathbb{Z} \cap n\mathbb{Z}).$$

Нека је $d = \mathrm{NZD}(m, n)$, а $s = \mathrm{NZS}(m, n)$, тада је

$$m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}, \quad m\mathbb{Z} \cap n\mathbb{Z} = s\mathbb{Z}.$$

Дакле,

$$d\mathbb{Z}/n\mathbb{Z} \cong m\mathbb{Z}/s\mathbb{Z}.$$

Група $d\mathbb{Z}$ изоморфна је групи $\mathbb{Z}$ при изоморфизму $f: \mathbb{Z} \to d\mathbb{Z}$ датом са $f(x) = dx$. Нека је $n = dn'$. При изоморфизму f, подгрупа $n'\mathbb{Z}$ слика се на подгрупу $n\mathbb{Z}$. Другим речима, имамо изоморфизам

$$d\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/n'\mathbb{Z}.$$

Знамо да је $sd = mn$, па је $n' = n/d = s/m$. Заправо је група $m\mathbb{Z}/s\mathbb{Z}$ изоморфна групи $\mathbb{Z}/n'\mathbb{Z}$. ♣

Теорема 83 (Трећа теорема о изоморфизмима) Нека су H и K нормалне подгрупе групе G за које је $H \subseteq K$. Тада је $K/H \triangleleft G/H$ и

$$(G/H)/(K/H) \cong G/K.$$

Доказ. Дефинишимо функцију $f: G/H \to G/K$ са $f(gH) = gK$. Ова функција јесте добро дефинисана пошто из претпоставке да је $gH = g'H$ следи да је $g^{-1}g' \in H$, а како је $H \subseteq K$, то из $g^{-1}g' \in H$ следи да $g^{-1}g' \in K$, па је $gK = g'K$. Очигледно је да је f један епиморфизам. Одредимо језгро од f.

$$gH \in \mathrm{Ker}(f) \text{ акко } gK = K \text{ акко } g \in K.$$

Видимо да је $\mathrm{Ker}(f) = K/H$. Резултат се сада добија применом прве теореме о изоморфизмима. □

Пример 84 Нека су природни бројеви $m, n \geq 2$ такви да $m \mid n$. Применити трећу теорему о изоморфизмима на: $\mathbb{Z}$, $m\mathbb{Z}$ и $n\mathbb{Z}$.

Наравно, $n\mathbb{Z}$ је подгрупа од $\mathbb{Z}$ генерисана елементом n. Како $m \mid n$, то је $n\mathbb{Z} \subseteq m\mathbb{Z}$. Дакле, на основу треће теореме о изоморфизмима, добијамо

$$(\mathbb{Z}/n\mathbb{Z})/(m\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/m\mathbb{Z}.$$

Као и у раније наведеном примеру,

$$m\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/d\mathbb{Z},$$

где је $d = n/m$. Ми знамо да је свака циклична група реда n изоморфна са $\mathbb{Z}_n$ и $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$. Осим тога, за сваки делилац реда цикличне групе, постоји тачно једна подгрупа те групе тог реда. Уколико је G циклична група реда n и $d \mid n$, онда постоји тачно једна подгрупа H групе G, која је реда d и тада је $G/H \cong \mathbb{Z}_m$, где је $m = n/d$. ♣

Дејства група

Започнимо ову лекцију следећом дефиницијом.

Дефиниција 85 Нека је G група и X непразан скуп. Под дејством групе G на скупу X подразумевамо хомоморфизам $\varphi: G \to \mathbb{S}_X$.

Дакле, овај појам и није непознат читаоцима. Већ смо у претходној лекцији користили овакве хомоморфизме у појединим примерима. Постоји други, еквивалентан начин, задавања дејства групе на скупу.

Дефиниција 86 Нека је G група и X непразан скуп. Под дејством групе G на скупу X подразумевамо функцију $\Theta: G \times X \to X$ за коју важи:

а) $\Theta(e, x) = x$, за све $x \in X$;

б) $\Theta(g, \Theta(h, x)) = \Theta(gh, x)$ за све $x \in X$ и $g, h \in G$.

Није тешко уверити се да су ове дефиниције еквивалентне. Наиме, ако је $\varphi: G \to \mathbb{S}_X$ задат хомоморфизам, функцију $\Theta: G \times X \to X$, која задовољава тражене услове задајемо са

$$\Theta(g, x) := \varphi(g)(x).$$

Како је φ хомоморфизам, то је $\varphi(e) = id_X$, па је

$$\Theta(e, x) = \varphi(e)(x) = id_X(x) = x.$$

Такође је

$$\Theta(gh, x) = \varphi(gh)(x) = (\varphi(g) \circ \varphi(h))(x) = \varphi(g)(\varphi(h)(x)) =$$

$$= \varphi(g)(\Theta(h, x)) = \Theta(g, \Theta(h, x)).$$

Обратно, ако је задата функција $\Theta: G \times X \to X$, која има наведена својства, хомоморфизам $\varphi: G \to \mathbb{S}_X$ дефинише се са

$$\varphi(g)(x) := \Theta(g, x).$$

Остављамо читаоцима да провере да је тако заиста добијен један хомоморфизам $\varphi: G \to \mathbb{S}_X$.

Уместо $\Theta(g, x)$ често ћемо писати $g \cdot x$. Својства функције Θ се тада записују овако:

а) $e \cdot x = x$, за све $x \in X$;

б) $(gh) \cdot x = g \cdot (h \cdot x)$, за све $g, h \in G$ и $x \in X$.

Наравно, не треба „мешати" ову ознаку са ознаком операције у групи G (операцију у групи често нећемо ни писати, као што смо и до сада радили у многим случајевима). У вези са дејством групе појављују се два значајна појма.

Дефиниција 87 Нека група G дејствује на непразном скупу X. Орбита елемента $x \in X$, у ознаци $\Omega(x)$, дефинише се са:

$$\Omega(x) := \{g \cdot x : g \in G\}.$$

Стабилизатор елемента $x \in X$, у ознаци Σ_x, дефинише се са:

$$\Sigma_x := \{g \in G : g \cdot x = x\}.$$

Наведимо неке примере дејства групе на скупу.

Пример 88 Нека је $X = \mathbb{R}^2$, а $G = \mathbb{Z}_2$. Тада је дејство групе G на скупу X задато са:

$$0 \cdot (x_1, x_2) = (x_1, x_2), \quad 1 \cdot (x_1, x_2) = (-x_1, -x_2).$$

Орбита елемента $(x_1, x_2) \in \mathbb{R}^2$ је

$$\Omega(((x_1, x_2)) = \{(x_1, x_2), (-x_1, -x_2)\}.$$

Приметимо да је једино орбита елемента $(0, 0)$ једночлана, док су све остале двочлане. ♣

Пример 89 Нека је $X = \mathbb{C}$, а $G = \mathbb{C}_n$ (где је $n \geq 2$). Тада је дејство групе G на X задато са:

$$g \cdot x := gx.$$

Подсетимо се да је $\mathbb{C}_n = \{z \in \mathbb{C} : z^n = 1\}$. Дакле, $\mathbb{C}_n \subseteq \mathbb{C}$ и наведено дејство заиста јесте дефинисано. Орбита сваког комплексног броја $z \neq 0$ је

$$\Omega(z) = \left\{ e^{\frac{2k\pi i}{n}} z : 0 \leq k < n \right\},$$

док је

$$\Omega(0) = \{0\}.$$

Дакле, свака орбита има или n елемената, или 1 елемент. ♣

Пример 90 Нека је G произвољна група и H нека њена подгрупа. Тада је задато дејство G на G/H са:

$$g \cdot (aH) := (ga)H.$$

У овом случају орбита ма ког елемента једнака је целом скупу X. За дејство које има само једну орбиту кажемо да је транзитивно. ♣

Пример 91 Нека је G произвољна група и H нека њена подгрупа. Дејство групе H на скупу G задато је са:

$$h \cdot x := hx.$$

Јасно је да је орбита елемента $x \in G$ једнака десном косету Hx. ♣

Пример 92 Нека је G било која група и $X = G$. Дејство G на G задато је са:

$$g \cdot x = gxg^{-1}.$$

Приметимо да се у овом случају орбите поклапају са класама конјугације, док се стабилизатори елемената из G поклапају са централизаторима тих елемената. ♣

Већ је из дефиниције, а посебно из ових примера, јасно да се природно може увести релација еквиваленције на скупу на коме дејствује нека група тако да се класе еквиваленције поклапају са орбитама. Између осталог добијамо да је X дисјунктна унија различитих орбита.

Следећи став повезује орбиту неког елемента и његов стабилизатор.

Став 93 Нека је X непразан скуп и нека група G дејствује на X. Тада је $\Sigma_x \leq G$ за свако $x \in X$. Осим тога, постоји бијекција између G/Σ_x и $\Omega(x)$.

Доказ. Како је $e \cdot x = x$, видимо да $e \in \Sigma_x$. Уколико $g \in \Sigma_x$, то је $g \cdot x = x$. Тада је и

$$g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = e \cdot x = x,$$

па закључујемо да и g^{-1} припада стабилизатору елемента x. Ако су $g, h \in \Sigma_x$, то је

$$(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = x,$$

па $gh \in \Sigma_x$. Тако смо показали да је $\Sigma_x \leq G$.

Бијекцију $f\colon G/\Sigma_x \to \Omega(x)$ задајемо са

$$f(g\,\Sigma_x) := g \cdot x.$$

Проверимо најпре добру дефинисаност функције f.

$$\begin{aligned} g\,\Sigma_x = h\,\Sigma_x &\implies h^{-1}g \in \Sigma_x \\ &\implies (h^{-1}g) \cdot x = x \\ &\implies h^{-1} \cdot (g \cdot x) = x \\ &\implies h \cdot (h^{-1} \cdot (g \cdot x)) = h \cdot x \\ &\implies (hh^{-1}) \cdot (g \cdot x) = h \cdot x \\ &\implies e \cdot (g \cdot x) = h \cdot x \\ &\implies g \cdot x = h \cdot x. \end{aligned}$$

Јасно је да је f „на". Остаје само да се провери да је f „1–1".

$$\begin{aligned} g \cdot x = h \cdot x &\implies h^{-1} \cdot (g \cdot x) = h^{-1} \cdot (h \cdot x) \\ &\implies (h^{-1}g) \cdot x = (h^{-1}h) \cdot x \\ &\implies (h^{-1}g) \cdot x = e \cdot x \\ &\implies (h^{-1}g) \cdot x = x \\ &\implies h^{-1}g \in \Sigma_x \\ &\implies g\,\Sigma_x = h\,\Sigma_x. \end{aligned}$$

□

Применом овог резултата у случају коначне групе, добијамо следећу последицу.

Последица 94 Уколико коначна група G дејствује на непразном скупу X, онда ред орбите ма ког елемента дели ред групе G. □

Пример 95 Наћи пример дејства групе $\mathbb{Z}_6$ за које постоје орбите свих могућих редова.

Посматраћемо дејство групе $\mathbb{Z}_6$ на $\mathbb{R}^6$ задато са:

$$n \cdot (x_0, \ldots, x_5) = (x_{n+_6 0}, \ldots, x_{n+_6 5}).$$

На пример, $2 \cdot (x_0, x_1, x_2, x_3, x_4, x_5) = (x_2, x_3, x_4, x_5, x_0, x_1)$. Тада

$$|\Omega((1,2,3,4,5,6))| = 6, \quad |\Omega((1,2,3,1,2,3))| = 3,$$

$$|\Omega((1,2,1,2,1,2))| = 2, \quad |\Omega((2,2,2,2,2,2))| = 1.$$

Проверите ово! ♣

Искористимо до сада добијене резултате за доказ Кошијеве теореме.

Доказ Кошијеве теореме. Дакле, нека је G коначна група и p прост број који дели ред групе G. Треба доказати да у G постоји елемент реда p. У ту сврху, нека је $H = \langle a \rangle$ нека циклична група реда p и

$$X = \{(x_1, x_2, \ldots, x_p) \in G^p : x_1 x_2 \cdots x_p = e\}.$$

Приметимо пре свега да је $|X| = |G|^{p-1}$. Наиме, $x_1, \ldots, x_{p-1}$ могу бити ма који елементи групе G, а тада је $x_p = (x_1 \cdots x_{p-1})^{-1}$. Стога $p \mid |X|$. Дејство групе H на X задато је са:

$$a \cdot (x_1, x_2, \ldots, x_p) := (x_2, \ldots, x_p, x_1).$$

Дакле, дејство одговара цикличном пермутовању дате p-торке. Приметимо да је довољно задати дејство генератора пошто је H циклична група (зашто?). Како ред орбите ма ког елемента дели ред групе H, закључујемо да је ред ма које орбите или 1 или p. Приметимо да је орбита елемента $(e, e, \ldots, e)$ једночлана. Како је X дисјунктна унија различитих орбита, тј.

$$X = \Omega_1 \sqcup \Omega_2 \sqcup \cdots \sqcup \Omega_k,$$

за неке орбите $\Omega_1, \ldots, \Omega_k$, и како постоји бар једна једночлана орбита закључујемо да мора постојати бар још једна таква. Наиме, уколико је нпр. Ω_1 једина једночлана орбита, добили бисмо једнакост

$$|G|^{p-1} = 1 + p(k-1).$$

Но, ово није могуће пошто $p \mid |G|$. Нека је $\Omega_2 = \{(x_1, x_2, \ldots, x_p)\}$ једночлана орбита различита од $\{(e, e, \ldots, e)\}$. Тада мора бити

$$a \cdot (x_1, x_2, \ldots, x_p) = (x_1, x_2, \ldots, x_p),$$

тј.

$$(x_2, \ldots, x_p, x_1) = (x_1, x_2, \ldots, x_p).$$

Добијамо да је $x_1 = x_2 = \cdots = x_p$. Означимо тај елемент са g. По претпоставци, $g \neq e$, а осим тога, како $(g, g, \ldots, g) \in X$, мора бити $g^p = e$. Закључујемо да је g тражени елемент реда p. □

Видели смо да је број елемената у орбити неког елемента једнак индексу стабилизатора. Да ли постоји веза између стабилизатора два елемента из исте орбите? Важи следећи став.

Став 96 Нека група G дејствује скупу X. Ако су елементи x и y из исте орбите, онда су њихови стабилизатори конјуговане подгрупе.

Доказ. По претпоставци постоји елемент $g \in G$ такав да је $y = g \cdot x$. Покажимо да је

$$\Sigma_y = g\,\Sigma_x\,g^{-1}.$$

$\subseteq$: Нека је $h \in \Sigma_y$. Како је $y = g \cdot x$, то је $x = g^{-1} \cdot y$. Добијамо

$$(g^{-1}hg) \cdot x = g^{-1} \cdot (h \cdot (g \cdot x)) = g^{-1} \cdot (h \cdot y) = g^{-1} \cdot y = x.$$

Дакле, $g^{-1}hg \in \Sigma_x$, па $h \in g\,\Sigma_x\,g^{-1}$.

$\supseteq$: Нека је $h \in \Sigma_x$. Тада је

$$(ghg^{-1}) \cdot y = g \cdot (h \cdot (g^{-1} \cdot y)) = g \cdot (h \cdot x) = g \cdot x = y.$$

Дакле, $g\,\Sigma_x\,g^{-1} \subseteq \Sigma_y$. □

Нека G дејствује на X и нека је g елемент из G. Скуп свих фиксних тачака елемента g, у ознаци X^g задаје се са:

$$X^g := \{x \in X : g \cdot x = x\}.$$

Приметимо да важи следеће:

$$x \in X^g \iff g \in \Sigma_x.$$

Став 97 Нека G дејствује на X. Ако су елементи g и h конјуговани, онда постоји бијекција између скупова X^g и X^h.

Доказ. Нека је $g = khk^{-1}$. Дефинишимо функцију $f\colon X \to X$ са $f(x) = k \cdot x$. Покажимо да f успоставља бијекцију између X^h и X^g.

$$x \in X^h \Rightarrow h \cdot x = x \Rightarrow g \cdot f(x) = g \cdot (k \cdot x) = k \cdot (h \cdot (k^{-1} \cdot (k \cdot x)))$$

$$= k \cdot (h \cdot ((k^{-1}k) \cdot x)) = k \cdot (h \cdot (e \cdot x)) = k \cdot (h \cdot x) = k \cdot x = f(x).$$

Дакле, $f\left[X^h\right] \subseteq X^g$. Но, ако $y \in X^g$, није тешко проверити да $k^{-1} \cdot y \in X^h$ (проверите!), док је очигледно $f(k^{-1} \cdot y) = y$. Стога добијамо да f заиста успоставља тражену бијекцију. □

Формула која одређује број различитих орбита је веома корисна у разним применама. Дајемо је у оквиру наредне теореме.

Теорема 98 Нека коначна група G дејствује на коначном скупу X. Тада је број различитих орбита једнак броју

$$\frac{1}{|G|}\sum_{g\in G}|X^g|\,.$$

Доказ. Означимо тражени број различитих орбита са k. Дакле,

$$X=\Omega_1\sqcup\cdots\sqcup\Omega_k,$$

где су Ω_i различите орбите. Посматрајмо скуп E задат са

$$E=\{(g,x)\in G\times X : g\cdot x=x\}.$$

„Пребројаћемо" елементе у E на два начина. Приметимо најпре да је

$$E=\bigsqcup_{g\in G}\{g\}\times X^g.$$

Дакле,

$$|E|=\sum_{g\in G}|X^g|\,. \tag{10}$$

С друге стране,

$$E=\bigsqcup_{x\in X}\Sigma_x\times\{x\}.$$

Према томе,

$$|E|=\sum_{x\in X}\Sigma_x=\sum_{i=1}^{k}\sum_{x\in\Omega_i}|\Sigma_x|.$$

Како елементи из исте орбите имају конјуговане стабилизаторе, то је $|\Sigma_x|=|\Sigma_y|$ уколико су x и y у истој орбити. Изаберимо по један елемент x_i из сваке од орбита Ω_i. Добијамо

$$|E|=\sum_{i=1}^{k}\sum_{x\in\Omega_i}|\Sigma_{x_i}|=\sum_{i=1}^{k}|\Omega_i||\Sigma_{x_i}|=\sum_{i=1}^{k}[G:\Sigma_{x_i}]|\Sigma_{x_i}|=\sum_{i=1}^{k}|G|=k|G|. \tag{11}$$

Из (10) и (11) тражени резултат следи. □

За крај наводимо један пример примене управо доказане формуле.

Пример 99 Темена, средишта ивица и тежишта страна правилног тетраедра треба обојити коришћењем три боје. Показати да има укупно 400707 начина на који се то може извести.

Ово заправо уопште није тешко показати, ма колико то у почетку изгледало. Размотримо најпре проблем мало пажљивије. Рецимо да желимо да темена тетраедра обојимо са две боје, нпр. плавом и црвеном,

али тако да је једно теме обојено плавом бојом, а остала црвеном. Јасно је да је то могуће урадити на само један начин. Наиме, треба имати у виду да темена немају никакве додатне ознаке. Према томе, било које од њих обележимо плавом бојом, а онда сва остала црвеном. Ако бисмо наш тетраедар заротирали, добили бисмо само другачији распоред темена, али то је тај исти тетраедар!

Ево како ћемо поступити при решавању задатка. Означимо сва темена бројевима $1, 2, 3$ и 4. Означимо ивицу чија су крајња темена a и b са $[a, b]$ (при чему је $a < b$). На крају, означимо страну на којој су темена a, b и c са $[a, b, c]$ (при чему је $a < b < c$). Дакле, укупно имамо $4+6+4$ тачке које желимо да обележимо са три боје. Нека је X скуп свих могућих обојених означених тетраедара (са овако означеним теменима, ивицама и странама) са три боје као у условима примера. Видимо да је $|X| = 3^{14}$. То наравно није тражени одговор. Наиме, многи од ових обојених тетраедара са означеним теменима, ивицама и странама, заправо представљају један те исти обојени тетраедар, само посматран из различитих углова (да се тако изразимо).

У нашем поједностављеном примеру бојења темена са две боје тако да је једно теме обојено плавом, а остала црвеном, добили бисмо 4 различита означена тетраедра (у зависности од тога које од означених темена смо обојили плавом бојом), а заправо постоји само једно бојење, пошто темена нису означена у поставци задатка. Сваки од овако обојених тетраедара се ротацијом може превести у било који други. Тако поступамо и при решавању постављеног задатка. Наиме, посматрамо дејство групе ротација тетраедра на скупу X и интересује нас број различитих орбита, пошто су тетраедри из исте орбите само различити положаји једног те истог обојеног тетраедра.

Група ротација правилног тетраедра је група A_4. По формули изведеној у претходној теореми, број различитих орбита је

$$\frac{1}{|A_4|} \sum_{\pi \in A_4} |X^\pi|.$$

Присетимо се да је $|X^g| = |X^h|$ уколико су елементи g и h конјуговани. Дакле, довољно је при примени горње формуле посматрати само по један елемент из сваке класе конјугације. Како су класе конјугације у групи A_4:

$$\{(123), (124), (134), (234)\};$$
$$\{(132), (142), (143), (243)\};$$
$$\{(12)(34), (13)(24), (14)(23)\};$$
$$\{(1)\},$$

то добијамо да је број различитих орбита једнак

$$\frac{1}{12}\left(|X^{(123)}| \cdot 4 + |X^{(132)}| \cdot 4 + |X^{(12)(34)}| \cdot 3 + |X^{(1)}| \cdot 1\right).$$

Одредимо $|X^{(123)}|$. Теме 4 може бити обојено било којом бојом. Ако је теме 1 обојено неком бојом, онда том бојом мора бити обојено и теме 2 и теме 3 пошто наведена ротација тетраедра преводи теме 1 у теме 2, теме 2 у теме 3, а теме 3 у теме 1, а ми посматрамо скуп фиксних тачака при дејству (123). Слично, ако је средиште ивице $[1,2]$ обојено неком бојом, онда том истом бојом мора бити обојено и средиште ивице $[2,3]$ и средиште ивице $[1,3]$. Исто то важи и за ивице $[1,4]$, $[2,4]$ и $[3,4]$. Тежиште стране $[1,2,3]$ може бити обојено ма којом бојом, али тежишта страна $[1,2,4]$, $[1,3,4]$ и $[2,3,4]$ морају бити обојена истом бојом. Добијамо да је

$$|X^{(123)}| = \underbrace{3}_{\text{теме } 4} \cdot \underbrace{3}_{\text{темена } 1,2,3} \cdot \underbrace{3}_{\text{ивице } [1,2],[1,3],[2,3]} \cdot \underbrace{3}_{\text{ивице } [1,4],[2,4],[3,4]} \cdot$$

$$\cdot \underbrace{3}_{\text{страна } [1,2,3]} \cdot \underbrace{3}_{\text{стране } [1,2,4],[1,3,4],[2,3,4]} = 3^6.$$

Потпуно аналогно добијамо да је $|X^{(132)}| = 3^6$. С обзиром да је $X^{(1)} = X$, одредимо још и $|X^{(12)(34)}|$. У овом случају, темена 1 и 2 морају бити обојена истом бојом, као и темена 3 и 4. Средиште ивице $[1,2]$, као и ивице $[3,4]$ може бити обојено ма којој бојом, док средишта ивица $[1,4]$ и $[2,3]$ морају бити обојена истом бојом, као и средишта ивица $[1,3]$ и $[2,4]$. Тежишта страна $[1,2,3]$ и $[1,2,4]$ морају бити обојена истом бојом, као и средишта страна $[1,3,4]$ и $[2,3,4]$. Добијамо да је

$$|X^{(12)(34)}| = \underbrace{3}_{\text{темена } 1,2} \cdot \underbrace{3}_{\text{темена } 3,4} \cdot \underbrace{3}_{\text{ивица } [1,2]} \cdot \underbrace{3}_{\text{ивица } [3,4]} \cdot$$

$$\cdot \underbrace{3}_{\text{ивице}[1,4],[2,3]} \cdot \underbrace{3}_{\text{ивице } [1,3],[2,4]} \cdot \underbrace{3}_{\text{стране } [1,2,3],[1,2,4]} \cdot \underbrace{3}_{\text{стране } [1,3,4],[2,3,4]} = 3^8.$$

Дакле, број различитих орбита (тј. обојених тетраедара) је

$$\frac{1}{12}\left(3^6 \cdot 4 + 3^6 \cdot 4 + 3^8 \cdot 3 + 3^{14} \cdot 1\right) = 400707.$$

♣

Коначно генерисане Абелове групе

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 100 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 101 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 $m_1 x_1 + \cdots + m_n x_n$, 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 102 Нека је F слободна Абелова група са системом слободних генератора $[x_1, \ldots, x_n]$ и F' слободна Абелова група са системом слободних генератора $[x'_1, \ldots, x'_n]$. 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 103 Група $\mathbb{Z}^n$ је слободна Абелова група са слободним системом генератора

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

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

$$f(m_1, m_2, \ldots, m_n) := m_1 a_1 + m_2 a_2 + \cdots + m_n a_n.$$

Није тешко проверити да је f заиста хомоморфизам. Осим тога

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

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

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 104 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

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

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

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

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

$$[x_1 + t_2x_2 + \cdots + t_nx_n, x_2, \ldots, x_n]$$

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

$$R = \langle d_1x_1\rangle \oplus \langle d_2x_2\rangle \oplus \cdots \oplus \langle d_nx_n\rangle,$$

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:

$$d_1 := \min\{m_1 > 0 : \text{ за неки систем слободних генератора}$$

$$[x_1, \ldots, x_n] \text{ и неке } m_2, \ldots, m_n \in \mathbb{Z}, m_1x_1 + \cdots + m_nx_n \in R\}.$$

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 $[y_1, \ldots, y_n]$ такав да $d_1y_1 \in R$.

На основу дефиниције d_1, постоји неки систем слободних генератора $[x_1, \ldots, x_n]$ и цели бројеви $m_2, \ldots, m_n$ 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 $[x_2, x_1 + qx_2, \ldots, x_n]$ 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 $[x_1 + t_2 x_2 + \cdots + t_n x_n, x_2, \ldots, x_n]$.

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

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

Најпре је

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

пошто су $y_1, y_2, \ldots, y_n$ 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 $[z_2, \ldots, z_2]$ 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 $[y_1, z_2, \ldots, z_n]$ 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 $d_2 = q d_1 + r$, 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

$$r z_2 + d_1(y_1 + q z_2) + \cdots + d_n z_n \in R,$$

а како је $0 < r < d_1$ и $[z_2, y_1 + qz_2, \ldots, z_n]$ 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. □

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

Теорема 107 Нека је A коначно генерисана Абелова група. Тада постоје позитивни цели бројеви $d_1, \ldots, d_k$ и природан број s такви да $d_i \mid d_{i+1}$ за све $i = \overline{1, k-1}$ и да је

$$A \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2} \times \cdots \times \mathbb{Z}_{d_k} \times \mathbb{Z}^s. \tag{12}$$

Доказ. Како је A коначно генерисана, то постоји коначно много елемената $a_1, \ldots, a_n \in A$ тако да је $A = \langle a_1, \ldots, a_n \rangle$. Нека је F слободна група са n генератора $x_1, \ldots, x_n$. 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 $y_1, y_2, \ldots, y_n$ 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. □

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 (12) 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 108 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

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

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.

Комутативни прстени са јединицом

У овој лекцији прелазимо на изучавање алгебарских структура са две бинарне операције, које обично зовемо сабирање и множење. Пређимо на дефиницију основног објекта, који ћемо овде проучавати.

Дефиниција 109 Комутативан прстен са јединицом је структура $(A, +, \cdot)$ за коју важи

- $(A, +)$ је Абелова група;
- $(A, \cdot)$ је комутативан моноид;
- За све $x, y, z \in A$ важи: $x \cdot (y + z) = x \cdot y + x \cdot z$.

Неутрал за сабирање (операцију $+$ у прстену) у комутативном прстену A означавамо са 0 (или понекад, због прецизности, са 0_A) и зовемо нулом прстена A, док неутрал за множење (операцију $\cdot$ у прстену) означавамо са 1 (или понекад, због прецизности, са 1_A) и зовемо јединицом прстена A.

Сви прстени, са којима у даљем будемо радили, биће комутативни прстени са јединицом и кратко ћемо их звати прстени. У сваком прстену A, за сваки елемент $a \in A$, важи: $a \cdot 0_A = 0_A$. Ево како то можемо показати:

$$a \cdot 0_A = a \cdot (0_A + 0_A) = a \cdot 0_A + a \cdot 0_A.$$

Коришћењем чињенице да је $(A, +)$ Абелова група, добијамо да је

$$0_A = a \cdot 0_A.$$

Уколико би у прстену A важило: $0_A = 1_A$ (приметимо да нигде нисмо захтевали да је нула прстена различита од његове јединице), добили бисмо да за свако $a \in A$ важи:

$$a = a \cdot 1_A = a \cdot 0_A = 0_A,$$

па би било $A = \{0_A\}$. Такав прстен називамо нула прстен. У даљем ћемо увек претпоставити да је $0_A \neq 1_A$.

Приметимо још да је у сваком прстену испуњено: $-a = (-1_A) \cdot a$. Наиме,

$$a + (-1_A) \cdot a = 1_A \cdot a + (-1_A) \cdot a = a \cdot 1_A + a \cdot (-1_A) = a \cdot (1_A + (-1_A)) = a \cdot 0_A = 0_A,$$

те следи да је заиста $(-1_A) \cdot a = -a$. На сличан начин се доказују и други идентитети попут, на пример, $(-a) \cdot b = -(a \cdot b)$, $(-a) \cdot (-b) = a \cdot b$ итд.

Структура $(A, \cdot)$ је моноид, па у њој неки елементи могу имати инверз. Јасно је да то не може бити 0, пошто је $0 \cdot a = 0 \neq 1$ за сваки елемент $a \in A$. Стога је природно посматрати све оне елементе из $A \setminus \{0\}$ који имају инверз у односу на множење. Скуп свих таквих елемената означаваћемо са $U(A)$. Јасно је да је $(U(A), \cdot)$ једна комутативна група и звaћемо је групом инвертибилних елемената прстена. Дакле, када кажемо да је неки елемент прстена инвертибилан, мислимо на инвертибилност у односу на операцију множења, пошто у односу на сабирање сваки елемент сигурно има свој супротни елемент. Уколико је $U(A) = A \setminus \{0\}$, прстен A је поље.

Наведимо неке примере комутативних прстена са јединицом:

- $\mathbb{Z}$;
- $\mathbb{Z}_n = (Z_n, +_n, \cdot_n)$;
- $\mathbb{R}$;
- $\mathbb{Q}$;
- $\mathbb{C}$.

Наравно да $+_n$ и $\cdot_n$ означавају операције сабирања и множења по модулу n. Приметимо да су последња три прстена заправо поља, док први то сигурно није, а други за неке n јесте, а за неке n није. Заправо важи следеће.

$$U(\mathbb{Z}_n) = \Phi(n) \text{ (погледајте раније предавања).}$$

Дакле,

$$\mathbb{Z}_n \text{ је поље ако и само ако је } n \text{ прост број.}$$

Важан пример прстена чини и прстен полинома са коефицијентима у неком комутативном прстену са јединицом A и неодређеном X, тј. прстен $A[X]$. Ми се нећемо детаљно бавити конструкцијом наведеног прстена, прихватићемо га као скуп свих формалних израза облика $a_0 + a_1X + \cdots + a_nX^n$, при чему $a_i \in A$, за све i, а сабирање и множење се изводи као што изводимо сабирање и множење полинома са којима смо радили у средњој школи. Дакле,

$$A[X] = \{a_0 + a_1X + \cdots + a_nX^n : n \in \mathbb{N}, a_i \in A\}.$$

Но, за разлику од полинома из средње школе, нека правила престају да важе. На пример, подсетимо се појма степена полинома. Уколико је $p = a_0 + a_1X + \cdots + a_nX^n$, при чему је $a_n \neq 0$, онда је степен полинома p баш n. Тај полином p је моничан уколико је ту $a_n = 1$. У средњој школи смо навикли да је степен производа два полинома једнак збиру њихових степена:

$$\deg(ab) = \deg a + \deg b,$$

где је са $\deg a$ означен степен полинома a. Но, посматрајмо пример два полинома из $\mathbb{Z}_6[X]$. Нека је $a = 2 + 3X$, а $b = 1 + 2X$. Тада је

$$a \cdot b = (2 + 3X) \cdot (1 + 2X) = 2 + X.$$

Приметимо да су операције у прстену $\mathbb{Z}_6$ сабирање и множење по модулу 6, те како је $2 \cdot_6 3 = 0$ и сл. добијамо наведени резултат. Феномен, који се овде појавио састоји се у томе да производ два ненулта елемента ипак може бити једнак 0.

Дефиниција 110 За елемент $a \neq 0$, комутативног прстена са јединицом A, кажемо да је прави делитељ нуле у A уколико постоји $b \in A \setminus \{0\}$ такав да је $a \cdot b = 0$.

Став 111 У пољу нема правих делитеља нуле.

Доказ. Претпоставимо да у пољу F постоје прави делитељи нуле, тј. да постоје a и b такви да је $a \neq 0$ и $b \neq 0$, а да је $a \cdot b = 0$. Како је $a \neq 0$, а у пољу сваки елемент различит од нуле има инверз, постоји елемент a^{-1} за који важи $a^{-1} \cdot a = 1$. Тако добијамо да је

$$0 = a^{-1} \cdot 0 = a^{-1} \cdot (a \cdot b) = (a^{-1} \cdot a) \cdot b = 1 \cdot b = b,$$

што противречи претпоставци $b \neq 0$. □

Дефиниција 112 Комутативан прстен са јединицом у коме нема правих делитеља нуле зовемо област целих или домен.

Дакле, на основу претходног става, свако поље је домен, но има и домена који нису поља. На пример, $\mathbb{Z}$ је домен који није поље. Занимљив је следећи резултат.

Став 113 Сваки коначан домен је поље.

Доказ. Претпоставимо да је A коначан домен и да је $a \in A \setminus \{0\}$. Треба показати да a има инверз. У ту сврху, посматрајмо функцију $L_a \colon A \to A$ дефинисану са $L_a(x) = a \cdot x$, за $x \in A$. Ова функција је „1–1". Наиме, ако је $L_a(x) = L_a(y)$, онда је $a \cdot x = a \cdot y$, па је $a \cdot (x - y) = 0$. Како је A домен, а $a \in A \setminus \{0\}$, мора бити $x - y = 0$, тј. $x = y$. Но, свака „1–1" функција која слика коначан скуп у њега самог мора бити бијекција. Закључујемо да је L_a бијекција, па постоји a' тако да је $L_a(a') = 1$, тј. постоји $a' \in A$ за који је $a \cdot a' = 1$, те a има инверз. □

Дефиниција 114 Елемент $a \in A$ је регуларан уколико из $a \cdot x = a \cdot y$ следи да је $x = y$.

Дакле, регуларни елементи су они елементи „са којима можемо скратити" неке једнакости. Приметимо да су инвертибилни елементи обавезно и регуларни, али да регуларни елементи не морају бити инвертибилни. Наиме, јасно је да у $\mathbb{Z}$ сваки елемент различит од нуле регуларан, а да само 1 и -1 имају инверз у $\mathbb{Z}$. Но, став 113 није тешко уопштити.

Став 115 У сваком коначном прстену сваки регуларан елемент је инвертибилан.

Упутство: Погледајте доказ става 113. □

Дакле, сваки елемент у коначном прстену је или делитељ нуле или инвертибилан. Уколико скуп свих делитеља нуле у прстену A означимо са $Z(A)$, овај резултат можемо кратко записати и на следећи начин. Ако је A коначан комутативан прстен са јединицом онда је

$$A = Z(A) \sqcup U(A).$$

Као што у теорији група имамо појам подгрупе неке групе, тако и у теорији комутативних прстена са јединицом имамо појам потпрстена са јединицом.

Дефиниција 116 Нека су $(A, +, \cdot)$ и $(B, +', \cdot')$ комутативни прстени са јединицом при чему је $B \subseteq A$. Уколико је за све $x, y \in B$ испуњено:

$$x + y = x +' y, \quad x \cdot y = x \cdot' y$$

и $1_A = 1_B$, онда је B један потпрстен са јединицом прстена A.

Приметимо да такође важи и $0_A = 0_B$, но та се чињеница може извести из преосталих, што није тачно за једнакост $1_A = 1_B$. На пример, нека је $A = \{(0,0), (0,1), (1,0), (1,1)\}$ и $B = \{(0,0), (1,0)\}$, где су операције дефинисане по координатама, а на свакој координати су сабирање, односно множење по модулу 2. Тада B јесте комутативан прстен са јединицом, но јединица у B је елемент $(1,0)$, а јединица у A је $(1,1)$. Стога B није потпрстен са јединицом прстена A.

Важнији од појма потпрстена је појам идеала.

Дефиниција 117 Нека је A комутативан прстен са јединицом и I непразан подскуп од A. Тада је I идеал у A уколико

1. за све $x, y \in I$: $x + y \in I$;
2. за све $a \in A$ и $x \in I$: $a \cdot x \in I$.

Приметимо да $0 \in I$ за сваки идеал I. Наиме, како је I непразан, то постоји $x \in I$. Но, тада је и $0 = 0 \cdot x \in I$. Ознака $I \lhd A$ означава да је I идеал у A.

Са идеалима се могу вршити операције сабирања и множења као и са елементима.

Дефиниција 118 Нека су I и J идеали прстена A.

1. $I + J := \{x + y : x \in I, y \in J\}$;
2. $I \cdot J := \{x_1 y_1 + \cdots + x_n y_n : x_i \in I \text{ за све } i = \overline{1,n}, y_j \in J \text{ за све } j = \overline{1,n}, \text{ и све } n \geq 1\}$.

Директна провера показује да су $I+J$ и $I \cdot J$ заиста идеали у прстену A. Приметимо да је $I \cdot J$ заправо најмањи идеал који садржи све могуће производе елемената из I са елементима из J.

Као и у случају подгрупа, пресек два идеала $I \cap J$ јесте идеал, док је њихова унија $I \cup J$ идеал ако и само ако је један од тих идеала садржан у другом. Заправо, ако посматрамо само операцију сабирања, приметимо да су идеали подгрупе групе $(A, +)$, а знамо да из чињенице да је унија две подгрупе подгрупа, следи да је једна од њих садржана у другој. Други смер се лако проверава.

Наведимо неке примере.

Пример 119 Ако је A комутативан прстен са јединицом и $a \in A$ произвољан елемент, онда је

$$\langle a \rangle := \{r \cdot a : r \in A\},$$

идеал. Овај идеал назива се главни идеал генерисан елементом a.

Како је $r \cdot a + s \cdot a = (r + s) \cdot a$, као и $s \cdot (r \cdot a) = (sr) \cdot a$, видимо да је $\langle a \rangle$ заиста идеал у прстену A. ♣

Пример 120 Сваки идеал у $\mathbb{Z}$ је облика $\langle m \rangle$ за неки природан број m.

Нека је $I \lhd \mathbb{Z}$. Како је $(I, +)$ подгрупа групе $(\mathbb{Z}, +)$, то на основу претходног знања о подгрупама групе $\mathbb{Z}$, добијамо да је $I = \langle m \rangle$. ♣

Напомена: Идеал $\langle m \rangle$ означава се и са $m\mathbb{Z}$ (скуп свих целобројних умножака броја m).

Пример 121 Нека су m и n позитивни цели бројеви. Одредити:

$$\langle m \rangle \cdot \langle n \rangle, \quad \langle m \rangle + \langle n \rangle, \quad \langle m \rangle \cap \langle n \rangle.$$

Пре свега, $\langle a \rangle \cdot \langle b \rangle = \langle ab \rangle$ важи у сваком прстену и за све елементе a и b (проверите!). Стога је $\langle m \rangle \cdot \langle n \rangle = \langle mn \rangle$. На основу дефиниције:

$$\langle m \rangle + \langle n \rangle = \{mx + ny : x, y \in \mathbb{Z}\}.$$

Како ми знамо да је $\langle m \rangle + \langle n \rangle$ сигурно главни идеал, потребно је само одредити који је његов генератор. Но, није потребно много размишљати о томе. Из горње једнакости се просто намеће да је

$$\langle m \rangle + \langle n \rangle = \langle d \rangle,$$

где је $d = \text{NZD}(m, n)$. Пре свега, добро нам је познато да увек постоје $p, q \in \mathbb{Z}$ за које је $mp + nq = d$. Стога, $d \in \langle m \rangle + \langle n \rangle$, па мора бити и $\langle d \rangle \subseteq \langle m \rangle + \langle n \rangle$. Но, како $d \mid m$ и $d \mid n$, то постоје m_1 и n_1 такви да је $m = dm_1$ и $n = dn_1$. Уколико је $mx+ny$ произвољан елемент из $\langle m \rangle + \langle n \rangle$ добијамо:

$$mx + ny = dm_1x + dn_1y = d(m_1x + n_1y),$$

те закључујемо да $mx + ny \in \langle d \rangle$, те је заиста $\langle m \rangle + \langle n \rangle = \langle d \rangle$.

Одредимо још и $\langle m \rangle \cap \langle n \rangle$. Приметимо да $x \in \langle m \rangle \cap \langle n \rangle$ ако и само ако $m \mid x$ и $n \mid x$. Но, то управо значи да је $\langle m \rangle \cap \langle n \rangle = \langle \text{NZS}(m, n) \rangle$. ♣

Пример 122 У прстену $\mathbb{Z}[X]$ постоји идеал који није главни.

Посматрајмо идеал I генерисан са два елемента 2 и X, $I = \langle 2, X\rangle$ (ознака $\langle S\rangle$ означава најмањи идеал (који увек постоји јер је пресек ма које колекције идеала идеал) који садржи скуп S; у случају да је $S = \{x_1, \ldots, x_n\}$ пишемо $\langle x_1, \ldots, x_n\rangle$, уместо $\langle\{x_1, \ldots, x_n\}\rangle$). Овај идеал сигурно није главни. Наиме, претпоставимо да је

$$\langle 2, X\rangle = \langle a(X)\rangle,$$

за неки полином $a(X)$. Како је $2 \in \langle a(X)\rangle$, то мора бити $2 = a(X) \cdot b(X)$ за неки полином $b(X)$. То значи да је $a(X)$ константан полином. Но, из чињенице да $X \in \langle a(X)\rangle$, следи да $a(X) \mid X$, па мора бити $a(X) = 1$, или $a(X) = -1$. То би значило да је $1 = 2p(X) + Xq(X)$ за неке полиноме $p(X), q(X) \in \mathbb{Z}[X]$. Но, заменом 0 уместо X добијамо да је тада $1 = 2p(0)$, те би следило да $\frac{1}{2} \in \mathbb{Z}$. Закључујемо да наведени идеал није главни. ♣

Пример 123 Нека је K ма које поље. Тада је сваки идеал у прстену $K[X]$ главни.

У доказу ћемо користити чињеницу да за полиноме $a(X)$ и $b(X)$ из $K[X]$ за које је $b(X) \neq 0$ постоје и једнозначно су одређени полиноми, $q(X)$ и $r(X)$ такви да је

$$a(X) = q(X)b(X) + r(X), \quad r(X) = 0 \text{ или } \deg r(X) < \deg b(X).$$

Ово је познато еуклидско дељење полинома, или дељење са остатком, са којим смо упознати у средњој школи (додуше само за реалне, односно комплексне полиноме, али ћемо само такве случајеве у применама и разматрати).

Нека је $I \lhd K[X]$. Уколико је $I = \{0\}$, јасно је да је I главни идеал генерисан елементом 0. Претпоставимо стога да је $I \neq \{0\}$. Нека је μ моничан полином најмањег степена који се налази у I. Тај полином сигурно постоји пошто је I идеал. Докажимо да је $I = \langle\mu\rangle$. Посматрајмо произвољни елемент $a \in I$. На основу резултата наведеног горе, постоје полиноми q и r (читалац сигурно примећује да понекад полиноме означавамо са $a(X)$, а понекад и само са a, као и да производ два елемента у прстену понекад пишемо без ознаке операције множења) такви да је $a = q\mu + r$, при чему је степен полинома r мањи од степена полинома μ, или је $r = 0$. Како $a, \mu \in I$, добијамо да је $r = a - q\mu$ такође из I. Но, уколико је $r \neq 0$, множењем инверзом водећег коефицијента од r добили бисмо да се у I налази моничан полином степена мањег од степена полинома μ што противречи избору полинома μ. Закључујемо да мора бити $r = 0$, тј. да $\mu \mid a$, те да $a \in \langle\mu\rangle$, чиме је доказ завршен. ♣

Пример 124 Нека је K поље и $I \lhd K$. Тада је $I = \{0\}$, или је $I = K$.

Претпоставимо да је I идеал у K и да је $I \neq \{0\}$. То значи да идеал I садржи неки елемент $x \neq 0$. Уколико је a ма који елемент из K, добијамо да и a припада идеалу I. Наиме, како је I идеал, а $x \neq 0$, то постоји x^{-1} и елемент $(ax^{-1}) \cdot x$ мора припадати идеалу I, а јасно је да је тај елемент једнак елементу a. ♣

Пример 125 Нека је A ма који комутативан прстен са јединицом и $u \in U(A)$. Тада је $\langle u \rangle = A$.

Доказ се изводи на исти начин као у претходном примеру. ♣

Пређимо сада на појам хомоморфизма прстена.

Дефиниција 126 Нека су $(A, +, \cdot)$ и $(B, +', \cdot')$ два комутативна прстена са јединицом. Функција $f\colon A \to B$ је хомоморфизам прстена уколико је $f(1_A) = 1_B$ и уколико за све $x, y \in A$ важи:

$$f(x + y) = f(x) +' f(y) \quad \text{и} \quad f(x \cdot y) = f(x) \cdot' f(y).$$

Пример 127 Функција $\rho_n\colon \mathbb{Z} \to \mathbb{Z}_n$ задата са $\rho_n(x) := \rho(x, n)$, где је са $\rho(x, n)$ означен остатак при дељењу x са n, је један хомоморфизам прстена.

Овај хомоморфизам ћемо искористити да опишемо идеале у прстенима $\mathbb{Z}_n$, но пре тога ћемо навести неке опште резултате о хомоморфизмима.

Дефиниција 128 Нека је $f\colon A \to B$ хомоморфизам комутативних прстена са јединицом. Језгро хомоморфизма f, у ознаци $\mathrm{Ker}(f)$ дефинише се са:

$$\mathrm{Ker}(f) := \{x \in A : f(x) = 0_B\}.$$

Став 129 Нека је $f\colon A \to B$ хомоморфизам комутативних прстена са јединицом. Тада важи:

а) $\mathrm{Ker}(f) \lhd A$;

б) ако је $J \lhd B$ онда је $f^{-1}[J] \lhd A$;

в) ако је $I \lhd A$ и f „на", онда је $f[I] \lhd B$.

Доказ.

а) Нека $x, y \in \mathrm{Ker}(f)$. Тада је

$$f(x + y) = f(x) +' f(y) = 0_B +' 0_B = 0_B,$$

па $x + y \in \mathrm{Ker}(f)$.

Уколико је $x \in \mathrm{Ker}(f)$ и $a \in A$:

$$f(a \cdot x) = f(a) \cdot' f(x) = f(a) \cdot' 0_B = 0_B,$$

те $a \cdot x \in \mathrm{Ker}(f)$.

б) Нека је J идеал у B и $x, y \in f^{-1}[J]$. То значи да је $f(x) \in J$ и $f(y) \in J$. Како је J идеал, закључујемо да и $f(x+y) = f(x) +' f(y) \in J$. Дакле, $x + y \in f^{-1}[J]$.

Такође, уколико је $x \in f^{-1}[J]$ и $a \in A$, добијамо да је $f(a \cdot x) = f(a) \cdot' f(x) \in J$, пошто $f(x) \in J$, а J је идеал. Закључујемо да $a \cdot x \in f^{-1}[J]$.

в) Нека су $u, v \in f[I]$. То значи да је $u = f(x)$ и $v = f(y)$ за неке $x, y \in I$. Како је I идеал, то је $x + y \in I$, а како је $u +' v = f(x) +' f(y) = f(x+y)$, закључујемо да је $u +' v \in f[I]$.

Уколико је $u \in f[I]$, а $b \in B$, с обзиром да је по претпоставци f „на", добијамо да постоји $a \in A$ тако да је $b = f(a)$. Осим тога је $u = f(x)$ за неко $x \in I$. Како је I идеал, $a \cdot x$ припада I, па је $b \cdot' u = f(a) \cdot f(x) = f(a \cdot x)$ из $f[I]$. □

Приметимо да је, као и у случају хомоморфизма група, $\mathrm{Ker}(f) = \{0_A\}$ ако и само ако је хомоморфизам f инјективан.

У општем случају директна слика идеала не мора бити идеал. На пример, јасно је да функција $i\colon \mathbb{Z} \to \mathbb{Q}$ дефинисана са $i(x) = x$ за све $x \in \mathbb{Z}$, јесте хомоморфизам (то је инклузија прстена целих бројева у поље рационалних бројева). Но,

$$i[\langle 2 \rangle] = \{2m : m \in \mathbb{Z}\},$$

а то очигледно није идеал у $\mathbb{Q}$, пошто су, на основу раније доказаног, једини идеали у $\mathbb{Q}$: $\{0\}$ и $\mathbb{Q}$.

Пример 130 Нека је $n \geq 2$ цео број. Тада је сваки идеал у $\mathbb{Z}_n$ главни.

Искористићемо хомоморфизам $\rho_n\colon \mathbb{Z} \to \mathbb{Z}_n$, који је и „на". Нека је $J \lhd \mathbb{Z}_n$. Тада је $\rho_n^{-1}[J] \lhd \mathbb{Z}$. На основу структуре идеала прстена $\mathbb{Z}$, знамо да постоји $m \geq 0$ такав да је $\rho_n^{-1}[J] = \langle m \rangle$. Но, тада је

$$J = \rho_n[\rho_n^{-1}[J]] = \rho_n[\langle m \rangle] = \langle \rho_n(m) \rangle.$$

Приметимо да једнакост $J = \rho_n[\rho_n^{-1}[J]]$ следи из чињенице да је ρ_n „на", док је јасно да је $f[\langle a \rangle] = \langle f(a) \rangle$ за сваки епиморфизам (хомоморфизам који је „на") f и сваки елемент a (покажите да је ово тачно!). ♣

Напомена. Можда је читалац приметио да смо овај резултат могли да докажемо као и у случају прстена целих бројева. Наиме, сваки идеал у $\mathbb{Z}_n$ је и подгрупа цикличне групе, па је тиме и сама циклична. А знамо како изгледају цикличне подгрупе групе $\mathbb{Z}_n$. У овом доказу само треба обратити пажњу на чињеницу да је свака подгрупа од $\mathbb{Z}_n$ заиста идеал (у случају прстена $\mathbb{Z}$, то је тривијално испуњено, пошто се множење елементима из $\mathbb{Z}$ заправо своди на сабирање (уз евентуално множење са -1 које одговара тражењу супротног елемента)). Чињеница да је то испуњено и за $\mathbb{Z}_n$ захтева мали доказ. Размислите мало о томе.

Пример 131 Навести пример комутативног прстена са јединицом и подгрупе адитивне групе тог прстена, која није идеал.

Посматрамо прстен $A = \mathbb{Z}_2 \times \mathbb{Z}_2$. Овде су операције дефинисане по координатама и заправо је A директан производ прстена $\mathbb{Z}_2$ и $\mathbb{Z}_2$ (поновите појам директног производа алгебри). Скуп $\{(0,0),(1,1)\}$ је подгрупа адитивне групе тог прстена, али није идеал пошто елемент $(1,0)\cdot(1,1) = (1,0)$ не припада том скупу, а $(1,1)$ му припада. ♣

Пример 132 Наћи све идеале у прстену $\mathbb{Z}_{12}$.

Знамо да су сви идеали у овом прстену главни. Такође знамо да је сваки елемент у $\mathbb{Z}_{12}$ или делитељ нуле или инвертибилан. Како сваки инвертибилан елемент генерише, према једном од раније наведених примера, цео прстен, остаје да се види које идеале генеришу делитељи нуле. Приметимо да је $m \in Z_{12}$ делитељ нуле ако и само ако $2 \mid m$ или $3 \mid m$ (зашто?). Стога је

$$Z(\mathbb{Z}_{12}) = \{0,2,3,4,6,8,9,10\}.$$

Приметимо да, пошто је $5 \in U(\mathbb{Z}_{12})$ и $10 = 5 \cdot_{12} 2$ имамо да је $\langle 10\rangle = \langle 2\rangle$ (размислите како се ово може генерализовати). Такође је $9 = -3 = (-1)\cdot 3$, па је и $\langle 9\rangle = \langle 3\rangle$. Добијамо да је и $\langle 8\rangle = \langle 4\rangle$.

С друге стране, $\langle 2\rangle \neq \langle 4\rangle$. Наиме, претпоставимо да $2 \in \langle 4\rangle$. Тада би постојао $m \in Z_{12}$ такав да је $2 = 4 \cdot_{12} m$. То би значило да постоји цео број q такав да је $2 = 4m + 12q$. Дељењем са 2 добили бисмо да је $1 = 2m + 6q$ за неке целе бројеве m и q што свакако није могуће. Како је очигледно $4 \in \langle 2\rangle$, то добијамо да је $\langle 4\rangle \subset \langle 2\rangle$ (идеал генерисан са 4 је прави подскуп идеала генерисаног са 2). На сличан начин се добија да је $\langle 6\rangle \subset \langle 3\rangle$. Читаоцима остављамо да се увере да су сви различити идеали прстена $\mathbb{Z}_{12}$ следећи:

$$\langle 0\rangle, \langle 2\rangle, \langle 3\rangle, \langle 4\rangle, \langle 6\rangle, \mathbb{Z}_{12}$$

У даљем ћемо претпоставити да су сви идеали са којима радимо прави, тј. да нису једнаки целом прстену.

Дефиниција 133 Нека је $I \triangleleft A$. На A дефинишемо релацију конгруенције по модулу I са:

$$a \equiv b \pmod{I} \quad \textbf{акко} \quad a - b \in I.$$

Проверимо да је ова релација заиста конгруенција.

Рефлексивност. Како је $a - a = 0 \in I$, то је заиста $a \equiv a \pmod{I}$ за све $a \in A$.

Симетричност. Нека је $a \equiv b \pmod{I}$. То значи да $a - b \in I$, но, множењем са (-1) добијамо да $b - a = (-1)(a - b)$ припада I, па је $b \equiv a \pmod{I}$.

Транзитивност. Нека је $a \equiv b \pmod{I}$ и $b \equiv c \pmod{I}$. Дакле, $a - b \in I$ и $b - c \in I$. Но, тада је и

$$a - c = (a - b) + (b - c) \in I,$$

те је $a \equiv c \pmod{I}$.

Слагање са $+$. Нека је $a \equiv a' \pmod{I}$ и $b \equiv b' \pmod{I}$. Дакле, $a - a' \in I$ и $b - b' \in I$. Добијамо да је

$$(a + b) - (a' + b') = (a - a') + (b - b') \in I.$$

Слагање са $\cdot$. Нека је $a \equiv a' \pmod{I}$ и $b \equiv b' \pmod{I}$. Дакле, $a - a' \in I$ и $b - b' \in I$. Добијамо да је

$$a \cdot b - a' \cdot b' = (a \cdot b - a' \cdot b) + (a' \cdot b - a' \cdot b') = (a - a') \cdot b + a' \cdot (b - b') \in I.$$

Приметимо да је класа еквиваленције елемента a заправо скуп

$$a + I = \{a + x : x \in I\}.$$

Скуп класа еквиваленције означавамо са A/I. На основу претходног добијамо да је структура $(A/I, +, \cdot)$ један комутативан прстен са јединицом где су операције $+$ и $\cdot$ дефинисане са:

$$(a + I) + (b + I) := (a + b) + I, \quad (a + I) \cdot (b + I) := (a \cdot b) + I.$$

Наравно да неке од ових заграда нећемо увек записивати.

Као и у случају група, важе и теореме о изоморфизмима за прстене. Навешћемо само прву.

Теорема 134 *(*Теорема о изоморфизмима за прстене*)* Нека је $f\colon A \to B$ хомоморфизам комутативних прстена са јединицом. Тада је $\tilde{f}\colon A/\mathrm{Ker}(f) \to \mathrm{Im}(f)$ задато са:

$$\tilde{f}(a + \mathrm{Ker}(f)) := f(a)$$

изоморфизам комутативних прстена са јединицом.

Доказ. Проверимо најпре да је $\tilde{f}$ добро дефинисано. У ту сврху, нека је $a + \mathrm{Ker}(f) = b + \mathrm{Ker}(f)$. То значи да $a - b \in \mathrm{Ker}(f)$, тј. да је $f(a) = f(b)$. Закључујемо да је $\tilde{f}$ заиста добро дефинисано.

Проверимо да је $\tilde{f}$ хомоморфизам.

$$\tilde{f}((a + \mathrm{Ker}(f)) + (b + \mathrm{Ker}(f))) = \tilde{f}((a + b) + \mathrm{Ker}(f)) = f(a + b) =$$

$$= f(a) + f(b) = \tilde{f}(a + \mathrm{Ker}(f)) + \tilde{f}(b + \mathrm{Ker}(f)).$$

$$\tilde{f}((a + \mathrm{Ker}(f)) \cdot (b + \mathrm{Ker}(f))) = \tilde{f}((a \cdot b) + \mathrm{Ker}(f)) = f(a \cdot b) =$$

$$= f(a) \cdot f(b) = \tilde{f}(a + \mathrm{Ker}(f)) \cdot \tilde{f}(b + \mathrm{Ker}(f)).$$

Јасно је да је $\tilde{f}$ „на". Остаје да се провери да је $\tilde{f}$ „1–1".

$$\begin{aligned}\tilde{f}(a+\mathrm{Ker}(f)) = \tilde{f}(b+\mathrm{Ker}(f)) &\implies f(a)=f(b)\\ &\implies f(a-b)=0\\ &\implies a-b\in\mathrm{Ker}(f)\\ &\implies a+\mathrm{Ker}(f)=b+\mathrm{Ker}(f).\end{aligned}$$

Проверимо још и да $\tilde{f}$ слика јединицу прстена у јединицу прстена:

$$\tilde{f}(1_A+\mathrm{Ker}(f)=f(1_A)=1_B.$$

Закључујемо да је $\tilde{f}$ заиста један изоморфизам комутативних прстена са јединицом. □

Пример 135 Нека је $I \lhd A$. Тада је $p\colon A\to A/I$ један епиморфизам. ♣

Пример 136 За све $n\geq 1$ важи: $\mathbb{Z}/n\mathbb{Z}\cong\mathbb{Z}_n$.

Хомоморфизам $\rho_n\colon\mathbb{Z}\to\mathbb{Z}_n$, дат раније, је „на", а осим тога $\mathrm{Ker}(\rho_n)=n\mathbb{Z}$, те резултат следи. ♣

Већ смо у претходној лекцији навели појам директног производа два прстена, а и познат нам је општи појам директног производа алгебри, но ипак дајмо и ту дефиницију.

Дефиниција 137 Нека су $(A_1,+^1,\cdot^1),\dots(A_n,+^n,\cdot^n)$ комутативни прстени са јединицом. На Декартовом производу

$$A=A_1\times\cdots\times A_n,$$

задајемо структуру комутативног прстена са јединицом са:

$$(a_1,\dots,a_n)+(b_1,\dots,b_n):=(a_1+^1 b_1,\dots,a_n+^n b_n)$$

$$(a_1,\dots,a_n)\cdot(b_1,\dots,b_n):=(a_1\cdot^1 b_1,\dots,a_n\cdot^n b_n)$$

Приметимо да је $0_A=(0_{A_1},\dots,0_{A_n})$ и $1_A=(1_{A_1},\dots,1_{A_n})$.

Став 138 Нека су $m_1,\dots,m_n$ позитивни цели бројеви за које је: $\mathrm{NZD}(m_i,m_j)=1$ за све $i\neq j$. Тада је

$$\mathbb{Z}/(m_1\cdots m_n)\mathbb{Z}\cong(\mathbb{Z}/m_1\mathbb{Z})\times\cdots\times(\mathbb{Z}/m_n\mathbb{Z}).$$

Доказ. Дефинишимо хомоморфизам

$$f\colon\mathbb{Z}\to(\mathbb{Z}/m_1\mathbb{Z})\times\cdots\times(\mathbb{Z}/m_n\mathbb{Z})$$

са:

$$f(x)=(x+m_1\mathbb{Z},\dots,x+m_n\mathbb{Z}).$$

Остављамо читаоцима да провере да је f заиста хомоморфизам. Одредимо језгро овог хомоморфизма. Нека је $x \in \mathrm{Ker}(f)$. То значи да је $f(x) = (m_1\mathbb{Z}, \ldots, m_n\mathbb{Z})$, тј. то значи да $x \in m_1\mathbb{Z}$, $\ldots$, $x \in m_n\mathbb{Z}$. Дакле, у језгру се налазе они цели бројеви, који су дељиви свим бројевима $m_1, \ldots, m_n$. Како су m_i узајамно прости то језгро чине умношци од $m_1 \cdots m_n$, тј.

$$\mathrm{Ker}(f) = (m_1 \cdots m_n)\mathbb{Z}.$$

Добијамо да је

$$\mathbb{Z}/(m_1 \cdots m_n)\mathbb{Z} \cong \mathrm{Im}(f).$$

Но, како је $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}_m$, то је

$$|\mathbb{Z}/(m_1 \cdots m_n)\mathbb{Z}| = m_1 \cdots m_n = |(\mathbb{Z}/m_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_n\mathbb{Z})|.$$

Закључујемо да f мора бити „на". Тиме смо добили тражени изоморфизам. □

Последица 139 *(*Кинеска теорема о остацима*)* Нека су $m_1, \ldots, m_n$ позитивни цели бројеви који су пар по пар узајамно прости и $x_1, \ldots, x_n$ произвољни цели бројеви. Тада постоји цео број x такав да је

$$\begin{aligned} x &\equiv x_1 \pmod{m_1} \\ x &\equiv x_2 \pmod{m_2} \\ &\cdots\cdots\cdots\cdots \\ x &\equiv x_n \pmod{m_n} \end{aligned}$$

Ако је x' неки други цео број који задовољава наведени систем конгруенција, онда је

$$x \equiv x' \pmod{m_1 \cdots m_n}.$$

Доказ. Посматрајмо елемент

$$(x_1 + m_1\mathbb{Z}, \ldots, x_n + m_n\mathbb{Z}) \in (\mathbb{Z}/m_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_n\mathbb{Z}).$$

Како је хомоморфизам f, из доказа претходне теореме, „на", то постоји $x \in \mathbb{Z}$ који се слика у наведени елемент, тј. постоји $x \in \mathbb{Z}$ за који је

$$x + m_1\mathbb{Z} = x_1 + m_1\mathbb{Z}, \quad \ldots \quad , x + m_n\mathbb{Z} = x_n + m_n\mathbb{Z},$$

но, то управо значи да је

$$x \equiv x_1 \pmod{m_1}, \quad \ldots \quad , x \equiv x_n \pmod{m_n}.$$

Уколико је x' други цео број који задовољава наведене конгруенције, то значи да је $f(x) = f(x')$, тј.

$$x - x' \in \mathrm{Ker}(f) = (m_1 \cdots m_n)\mathbb{Z},$$

као што је и тврђено. □

Став 140 Ако су прстени A и B изоморфни, онда је $(U(A),\cdot) \cong (U(B),\cdot)$

Доказ. Јасно је да се инвертибилни елементи при сваком хомоморфизму сликају у инвертибилне елементе. Наиме, ако је $a \in U(A)$, то значи да постоји a' такав да је $a \cdot a' = 1_A$. Но, тада је $f(a) \cdot f(a') = f(a \cdot a') = f(1_A) = 1_B$, па и $f(a)$ има инверз.

Према томе, $f[U(A)] \subseteq U(B)$ за сваки хомоморфизам $f\colon A \to B$. Уколико је f изоморфизам и $b \in U(B)$, то постоји $a \in A$ такав да је $f(a) = b$. Но, елемент b има инверз, па је $b \cdot b' = 1_B$ за неки $b' \in B$. Елемент b' је слика неког елемента a': $f(a') = b'$. Но, тада је $f(a \cdot a') = f(a) \cdot f(a') = b \cdot b' = 1_B$, те како је f „1–1", мора бити $a \cdot a' = 1_A$ те a има инверз. Закључујемо да f успоставља бијекцију између $U(A)$ и $U(B)$. Како је f хомоморфизам, добијамо тражени изоморфизам. □

Став 141 Важи једнакост: $U(A_1 \times \cdots \times A_n) = U(A_1) \times \cdots \times U(A_n)$.

Доказ. Нека је $a = (a_1, \ldots, a_n) \in A_1 \times \cdots \times A_n$. Тада

$$\begin{aligned} a \in U(A_1 \times \cdots \times A_n) &\iff \text{постоји } b \in A : a \cdot b = 1 \\ &\iff \text{постоје } b_i \in A_i \text{ т. д. } a_i \cdot b_i = 1 \text{ за све } i \\ &\iff a_1 \in U(A_1), \ldots, a_n \in U(A_n) \\ &\iff a \in U(A_1) \times \cdots \times U(A_n). \end{aligned}$$

□

Теорема 142 Ако су $m_1, \ldots, m_n$ пар по пар узајамно прости позитивни цели бројеви, онда је

$$\mathbb{Z}_{m_1 \cdots m_n} \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n}$$

и

$$\varphi(m_1 \cdots m_n) = \varphi(m_1) \cdots \varphi(m_n),$$

где је φ Ојлерова функција.

Доказ. Како је $\mathbb{Z}_m \cong \mathbb{Z}/m\mathbb{Z}$, то први резултат следи из става 6. Осим тога, $\varphi(m) = |U(\mathbb{Z}_m)|$, те резултат за Ојлерову функцију следи из става 8 и става 9. □

Групе $U(\mathbb{Z}_n)$ имају занимљиву структуру, но ми се њима нећемо детаљно бавити. Но, ипак ћемо, због примена, доказати да је за сваки прост број p група $U(\mathbb{Z}_p)$ циклична. Заправо, доказаћемо општији резултат, али пре тога морамо да докажемо нешто у вези Абелових група.

Став 143 Нека је A Абелова група реда m и нека за свако d, које дели m, постоји највише d елемената $a \in A$ за које је $da = 0$. Тада је група A циклична.

Доказ. Докажимо најпре следећи резултат, који је и сам по себи занимљив:

$$\sum_{d|m} \varphi(d) = m.$$

Посматрајмо цикличну групу G реда m. Као што знамо, она има тачно једну подгрупу реда d за сваки d који је делилац броја m. Осим тога, циклична група реда d има тачно $\varphi(d)$ генератора. Следи да у цикличној групи реда m има тачно $\varphi(d)$ елемената реда d (сваки елемент реда d генеришу исту подгрупу групе G) за свако d које дели m. Стога једнакост следи.

Вратимо се нашој групи A. Означимо са $\psi_A(d)$ број елемената реда d у A. Сваки елемент $x \in A$ је неког реда d, где $d \mid m$. То значи да је

$$\sum_{d|m} \psi_A(d) = m.$$

С друге стране, ако је $\psi_A(d) > 0$, онда у групи A постоји елемент a, који је реда d. Посматрајмо подгрупу A' генерисану тим елементом. У њој има d елемената и за свако $z \in A'$ важи $dz = 0$. То значи да су сви елементи $x \in A$ за које је $dx = 0$ садржани у подгрупи A'. Дакле, сваки елемент реда d у A је садржан у цикличној подгрупи A', која је реда d. Но, ми знамо да у цикличној групи реда d има тачно $\varphi(d)$ генератора, тј. елемената реда d. Закључујемо да важи следеће: ако је за неко d, које дели m, $\psi_A(d) > 0$, онда је за то d: $\psi_A(d) = \varphi(d)$. С обзиром да је

$$\sum_{d|m} \varphi(d) = m = \sum_{d|m} \psi_A(d),$$

закључујемо да је за све d, који деле m испуњено $\psi_A(d) = \varphi(d)$. То посебно значи да је и $\psi_A(m) = \varphi(m) > 0$, па у A има елемената реда m, те је група A заиста циклична. □

Теорема 144 Нека је F поље и G коначна подгрупа групе $(F \setminus \{0\}, \cdot)$. Тада је G циклична група.

Доказ. Покажимо најпре да сваки полином $p(X)$ из $F[X]$ степена n има највише n нула у пољу F. Доказ се изводи индукцијом по степену полинома $p(X)$.

За $n = 1$ нема шта да се доказује, јасно је да полином има тачно једну нулу у F.

Претпоставимо да је $n > 1$ и да је тврђење тачно за све полиноме степена мањег од n. Ако полином $p(X)$ нема ниједну нулу у пољу F, онда је тврђење испуњено. Претпоставимо да $p(X)$ има неку нулу $a \in F$. Еуклидско дељење полинома $p(X)$ полиномом $X - a$ даје:

$$p(X) = (X - a)q(X) + r,$$

где је $r = 0$, или је то константан не-нула полином. Но, с обзиром да је $p(a) = 0$, добијамо да је $r = 0$. Стога је $p(X) = (X - a)q(X)$. Полином $q(X)$ је степена $n-1$ и по индукцијској хипотези има највише $n-1$ нулу у F. Како је свака нула полинома $p(X)$ или једнака a или је нека нула полинома $q(X)$ закључујемо да $p(X)$ има највише n нула у F.

Пређимо сада на доказ наше теореме. Теорему ћемо доказати тако што ћемо се уверити да група G испуњава услове претходног става (јасно је да је G комутативна група). С обзиром да овде користимо мултипликативну нотацију, треба да покажемо да за сваки d који дели ред групе G, у групи G има највише d елемената a за које је $a^d = 1$. Но, $G \subset F$ и елемент $a \in G$ за који је $a^d = 1$ у G(тј. у F) је заправо нула полинома $X^d - 1$ из $F[X]$. Ово је полином степена d и према претходно доказаном, он има највише d нула у F. Закључујемо да су услови за примену претходног става испуњени те добијамо да је G циклична група. □

Дакле, доказали смо да је свака коначна подгрупа мултипликативне групе поља циклична. Истакнимо још једном да се ради о коначним подгрупама. Наравно да мултипликативна група произвољног поља F, тј. група $(F \setminus \{0\}, \cdot)$ не мора бити циклична! Нпр. $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{C} \setminus \{0\}, \cdot)$ сигурно нису цикличне (ти скупови су непребројиви!).

Погледајмо како можемо искористити чињеницу да је $(\mathbb{Z}_p \setminus \{0\}, \cdot_p)$ циклична група. Пре свега, уведимо терминологију.

Дефиниција 145 Ма који генератор групе $(\mathbb{Z}_p \setminus \{0\}, \cdot_p)$ зове се примитивни корен модуло p.

Став 146 Нека је r ма који примитивни корен модуло p. Тада је са:

$$\mathrm{ind}_r(a) = x \text{ **акко** } r^x = a,$$

дефинисан изоморфизам $\mathrm{ind}_r \colon (\mathbb{Z}_p \setminus \{0\}, \cdot_p) \to (\mathbb{Z}_{p-1}, +_{p-1})$.

Доказ. Овај став је заправо само преформулација и прецизирање тврђења да је група $(\mathbb{Z}_p \setminus \{0\}, \cdot_p)$ циклична.

Како је r примитивни корен модуло p, то за свако $a \in \mathbb{Z}_p \setminus \{0\}$ постоји тачно једно $x \in \mathbb{Z}_{p-1}$ за које је $r^x = a$. Наиме, r је генератор наведене групе, па је сваки елемент у тој групи неки степен од r. Како та група има $p-1$ елемената, то $x \in \mathbb{Z}_{p-1}$. Ми треба да проверимо да ли је ind_r хомоморфизам, тј. да ли је

$$\mathrm{ind}_r(a \cdot_p b) = \mathrm{ind}_r(a) +_{p-1} \mathrm{ind}_r(b),$$

за све $a, b \in \mathbb{Z}_p \setminus \{0\}$. Нека је $x = \mathrm{ind}_r(a)$ и $y = \mathrm{ind}_r(b)$. Дакле, $r^x = a$ и $r^y = b$. Тада је

$$a \cdot_p b = r^x \cdot_p r^y = r^{x+y}.$$

С обзиром на чињеницу да је $\omega(r) = p - 1$, то је

$$r^{x+y} = r^{x +_{p-1} y},$$

па добијамо да је

$$a \cdot_p b = r^{x +_{p-1} y},$$

те је

$$\mathrm{ind}_r(a \cdot_p b) = x +_{p-1} y = \mathrm{ind}_r(a) +_{p-1} \mathrm{ind}_r(b).$$

Дакле, ind_r је заиста хомоморфизам, а да је бијекција следи из чињенице да је $\omega(r) = p - 1$. □

Пример 147 Наћи све примитивне корене модуло 13.

За почетак потражимо бар један примитивни корен. Почнимо од 2:

$$2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 8, \quad 2^4 = 3, \quad 2^5 = 6, \quad 2^6 = 12, \quad 2^7 = 11, \quad 2^8 = 9$$

$$2^9 = 5, \quad 2^{10} = 10, \quad 2^{11} = 7,$$

док је, наравно, $2^0 = 1$. Дакле, заиста је $\langle 2 \rangle = \mathbb{Z}_{13} \setminus \{0\}$. Да бисмо нашли све примитивне корене модуло 13, направимо таблицу за ind_2.

a	1	2	3	4	5	6	7	8	9	10	11	12
$\mathrm{ind}_2(a)$	0	1	4	2	9	5	11	3	8	10	7	6

С обзиром да је $2^{\mathrm{ind}_2(a)} = a$, није тешко извршити проверу.

Ова таблица нам омогућава да нађемо и све остале примитивне корене модуло 13. Наиме, подсетимо се да важи следеће:

Ако је $\omega(r) = n$ онда је $\omega(r^m) = n$ ако и само ако је $\mathrm{NZD}(n, m) = 1$.

Пошто је у нашем случају $\omega(2) = 12$, то је $\omega(2^m) = 12$ ако и само ако је $\mathrm{NZD}(m, 12) = 1$, тј. ако и само ако је $m \in \{1, 5, 7, 11\}$. Дакле, остали примитивни корени по модулу 13 су: $6 (= 2^5)$, $11 (= 2^7)$ и $7 (= 2^{11})$. ♣

Пример 148 Решити конгруенцију

$$x^5 \equiv 7 \pmod{13}.$$

Већ знамо да је 2 примитивни корен по модулу 13. Применом ind_2 на дату конгруенцију добијамо да је

$$5y \equiv 11 \pmod{12},$$

где смо са y означили $\mathrm{ind}_2(x) \in \mathbb{Z}_{12}$. Тако смо применом ind_2 једну конгруенцију петог степена свели на линеарну, која се лако може решити. С обзиром да је $5 \cdot_{12} 5 = 1$, добијамо да је

$$y \equiv 7 \pmod{12}.$$

Дакле, како је $y = \mathrm{ind}_2(x)$, добијамо да је

$$x \equiv 11 \pmod{13}.$$

♣

Поља

Започнимо ову лекцију једним примером.

Пример 149 Проверити да је са:

$$f(p(X)) = p(i),$$

где је i имагинарна јединица, дефинисан један хомоморфизам $f\colon \mathbb{R}[X] \to \mathbb{C}$ и применити на тај хомоморфизам теорему о изоморфизмима прстена.

Није тешко проверити да је f заиста хомоморфизам прстена. Нека су $a(X), b(X) \in \mathbb{R}[X]$ и нека је $c(X) = a(X) \cdot b(X)$. Тада је

$$f(a(X)) = a(i) = a_0 + a_1 i + a_2 i^2 + \cdots + a_m i^m,$$

$$f(b(X)) = b(i) = b_0 + b_1 i + b_2 i^2 + \cdots + b_n i^n$$

и

$$f(c(X)) = c(i) = c_0 + c_1 i + c_2 i^2 + \cdots + c_{m+n} i^{m+n},$$

при чему смо претпоставили да је степен полинома $a(X)$ једнак m, а степен полинома $b(X)$ једнак n. Но, знамо како се множе полиноми, па је за $k = \overline{0, m+n}$:

$$c_k = a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0,$$

при чему је наравно $a_i = 0$ за $i > m$, односно $b_j = 0$, за $j > n$. Но, тада је јасно да је заиста

$$c(i) = a(i) \cdot b(i),$$

те је

$$f(a(X) \cdot b(X)) = f(a(X)) \cdot f(b(X)).$$

Још лакше се проверава да је $f(a(X)+b(X)) = f(a(X))+f(b(X))$, а јасно је и да је $f(1) = 1$ (константан полином има константну вредност).

Теорема о изоморфизмима за прстене даје следећи изоморфизам:

$$\mathbb{R}[X]/\mathrm{Ker}(f) \cong \mathrm{Im}(f).$$

Идентификујмо слику и језгро хомоморфизма f.

Уколико је $a+bi$ произвољни елемент из $\mathbb{C}$, јасно је да је $f(a+bX) = a + bi$, па је f „на". Претпоставимо да $a(X) \in \mathrm{Ker}(f)$. То значи да је $a(i) = 0$. Дакле, $a(X)$ је полином са реалним коефицијентима чија је једна нула комплексан број i. Из средње школе нам је познато да је тада и $-i$ обавезно нула тог полинома. Но, α је нула полинома $a(X)$ ако и само ако $X - \alpha$ дели $a(X)$ (ово смо већ имали прилике да користимо). Добијамо да и $X - i$ дели $a(X)$, али да и $X + i = X - (-i))$ такође дели $a(X)$. Полиноми $X - i$ и $X + i$ су узајамно прости, па

закључујемо да полином $X^2+1=(X-i)(X+i)$ дели $a(X)$. Према томе, ако $a(X)\in \mathrm{Ker}(f)$, онда $(X^2+1)\mid a(X)$. То се може записати и овако:

$$a(X)\in \mathrm{Ker}(f)\Longrightarrow a(X)\in\langle X^2+1\rangle,$$

где наравно $\langle X^2+1\rangle$ означава главни идеал генерисан полиномом X^2+1. Јасно је да важи и обратно. Наиме, ако $a(X)\in\langle X^2+1\rangle$, то значи да је $a(X)=q(X)(X^2+1)$ за неки полином $q(X)$, но тада је

$$f(a(X))=f(q(X)(X^2+1))=f(q(X))f(X^2+1)=q(i)(i^2+1)=0,$$

па $a(X)\in\mathrm{Ker}(f)$. Закључујемо да је $\mathrm{Ker}(f)=\langle X^2+1\rangle$, те важи изоморфизам

$$\mathbb{R}[X]/\langle X^2+1\rangle\cong\mathbb{C}.$$

♣

Урадимо још један пример.

Пример 150 Доказати да је $\mathbb{Q}(\sqrt{2}):=\{a+b\sqrt{2}:a,b\in\mathbb{Q}\}$ једно потпоље поља $\mathbb{C}$. Применити теорему о изоморфизмима за прстене на хомоморфизам $f\colon\mathbb{Q}[X]\to Q(\sqrt{2})$ дефинисан са $f(a(X))=a(\sqrt{2})$.

Јасно је да је разлика два елемента из $Q(\sqrt{2})$ такође у $Q(\sqrt{2})$. Проверимо то за производ.

$$(a+b\sqrt{2})(c+d\sqrt{2})=(ac+2bd)+(ad+bc)\sqrt{2},$$

а како су $ac+2bd$ и $ad+bc$ рационални бројеви ако су то a,b,c,d, закључујемо да $(a+b\sqrt{2})(c+d\sqrt{2})\in\mathbb{Q}(\sqrt{2})$. Да бисмо показали да је $\mathbb{Q}(\sqrt{2})$ потпоље поља комплексних бројева, треба још само да проверимо да је инверз сваког не-нула елемента из $\mathbb{Q}(\sqrt{2})$ такође у $\mathbb{Q}(\sqrt{2})$. Приметимо да је $a+b\sqrt{2}=0$ ако и само ако је $a=b=0$. Наиме, уколико претпоставимо да је $b\neq 0$, а $a+b\sqrt{2}=0$, добијамо да је $\sqrt{2}=-\frac{a}{b}$, па би $\sqrt{2}$ био рационалан број, а знамо још из средње школе да то није случај. Дакле, уколико је $a+b\sqrt{2}\neq 0$, то је (наравно да је и $a-b\sqrt{2}\neq 0$ за $a,b\in\mathbb{Q}$):

$$\frac{1}{a+b\sqrt{2}}=\frac{1}{a+b\sqrt{2}}\cdot\frac{a-b\sqrt{2}}{a-b\sqrt{2}}=\frac{a-b\sqrt{2}}{a^2-2b^2}=\frac{a}{a^2-2b^2}+\frac{-b}{a^2-2b^2}\sqrt{2}\in\mathbb{Q}(\sqrt{2}).$$

На исти начин као и у претходном примеру, проверава се да је f хомоморфизам. Осим тога, како је $f(a+bX)=a+b\sqrt{2}$, видимо да је f „на". Покажимо да је $\mathrm{Ker}(f)=\langle X^2-2\rangle$.

Уколико $a(X)\in\langle X^2-2\rangle$, то је $a(X)=q(X)(X^2-2)$ за неки полином $q(X)\in\mathbb{Q}[X]$, па је

$$f(a(X))=f(q(X)(X^2-2))=f(q(X))f(X^2-2)=q(\sqrt{2})((\sqrt{2})^2-2)=0.$$

Дакле, $\langle X^2-2\rangle \subseteq \mathrm{Ker}(f)$. Покажимо да важи обратна импликација. Нека $a(X) \in \mathrm{Ker}(f)$. То значи да је $a(\sqrt{2})=0$, па $(X-\sqrt{2}) \mid a(X)$. Да бисмо показали да $(X^2-2) \mid a(X)$, потребно нам је, а и довољно, да покажемо да и $(X+\sqrt{2}) \mid a(X)$, тј. да је $a(-\sqrt{2})=0$. Нека је

$$a(X)=a_0+a_1X+a_2X^2+\cdots+a_nX^n.$$

Како је $a(\sqrt{2})=0$, то је

$$a_0+a_1\sqrt{2}+a_2\cdot 2+a_3\cdot 2\sqrt{2}+\cdots+a_n(\sqrt{2})^n=0.$$

Природно је дакле раздвојити парне степене од X и непарне степене од X. Претпоставимо, због једноставности ознака, да је $n=2k$ (ако је n непаран број, то додајемо још један коефицијент који је једнак нули — то не мења ништа у полиному, само у запису). Дакле,

$$a(X)=\sum_{i=0}^{k} a_{2i}X^{2i}+\sum_{i=0}^{k-1} a_{2i+1}X^{2i+1}.$$

Добијамо да је

$$\sum_{i=0}^{k} a_{2i}2^i+\left(\sum_{i=0}^{k-1} a_{2i+1}2^i\right)\sqrt{2}=0.$$

Како су $a_s \in \mathbb{Q}$, то мора бити

$$\sum_{i=0}^{k} a_{2i}2^i \quad \text{и} \quad \sum_{i=0}^{k-1} a_{2i+1}2^i=0.$$

Но, одавде добијамо да је и

$$\sum_{i=0}^{k} a_{2i}2^i-\left(\sum_{i=0}^{k-1} a_{2i+1}2^i\right)\sqrt{2}=0,$$

а то управо значи да је $a(-\sqrt{2})=0$ ($(-\sqrt{2})^{2i}=2^i$, а $(-\sqrt{2})^{2i+1}=-2^i\sqrt{2}$). Овим је завршен доказ да је $\mathrm{Ker}(f)=\langle X^2-2\rangle$, те добијамо изоморфизам

$$\mathbb{Q}[X]/\langle X^2-2\rangle \cong \mathbb{Q}(\sqrt{2}).$$

♣

Напомена 151 Могли смо и краће доказати да је $\mathrm{Ker}(f) \subseteq \langle X^2-2\rangle$. Наиме, ако је $a(X) \in \mathrm{Ker}(f)$, поделимо $a(X)$ са X^2-2. Добијамо да је $a(X)=q(X)(X^2-2)+r+sX$, за неки полином $q(X) \in \mathbb{Q}[X]$ и рационалне бројеве r,s. Како је $a(\sqrt{2})=0$, добијамо да је $r+s\sqrt{2}=0$, а како су $r,s \in \mathbb{Q}$, то је $r=s=0$, тј. $a(X) \in \langle X^2-2\rangle$. Но, није лоше видети и онај дужи доказ, па је зато и презентиран.

Изанализирајмо мало шта смо добили у претходним примерима. Посматрајмо, да се тако изразимо, „леву" страну у добијеним изоморфизмима. Видимо да се у оба случаја ради о количничким прстену прстена полинома по идеалу који је генерисан једним нерастављивим (над пољем $\mathbb{Q}$) полиномом другог степена. Оставимо за сада по страни чињеницу да је полином другог степена и концентришимо се на то да је он нерастављив. Количнички прстен је у оба случаја заправо поље. То, наравно не може бити случајно. Доказаћемо следећу важну теорему.

Теорема 152 Нека је F поље и $a(X) \in F[X] \setminus \{0\}$ нерастављив полином.

а) $E = F[X]/\langle a(X)\rangle$ је поље.

б) Поље E садржи потпоље изоморфно пољу F.

в) Полином $a(X)$ има бар једну нулу у пољу E.

г) На основу а) можемо сматрати да је $F \subset E$. Тада се E може видети и као векторски простор над пољем F и димензија тог простора једнака је степену полинома $a(X)$.

Доказ. а) Знамо да је E комутативни прстен са јединицом. Треба да докажемо да је E поље, тј. да сваки елемент из E који није нула има инверз у односу на множење. Означимо идеал $\langle a(X)\rangle$ са I. Дакле, $E = F[X]/I$ и нула у том прстену је заправо $0 + I = I$. Претпоставимо да је $c(X) + I \neq I$, тј. да $c(X)$ не припада идеалу I. То значи да $a(X)$ не дели $c(X)$. Како је $a(X)$ нерастављив полином, закључујемо да је највећи заједнички делилац полинома $a(X)$ и $c(X)$ једнак 1. Стога постоје полиноми $p(X)$ и $q(X)$ за које је

$$a(X)p(X) + c(X)q(X) = 1.$$

Преласком на количнички прстен добијамо једнакост

$$(a(X) + I)(p(X) + I) + (c(X) + I)(q(X) + I) = 1 + I.$$

С обзиром на чињеницу да је $a(X) \in I$ добијамо да је

$$(c(X) + I)(q(X) + I) = 1 + I,$$

те елемент $c(X) + I$ заиста има инверз у E. Закључујемо да је E поље.

б) Дефинишимо хомоморфизам $f\colon F \to E$ са $f(\alpha) = \alpha + I$ за све $\alpha \in F$. Како су једини идеали у ма ком пољу $\{0\}$ и цело поље, то закључујемо да је $\mathrm{Ker}(f) = \{0\}$ (језгро је увек идеал, али не може бити једнако целом пољу пошто се при хомоморфизму јединица слика у јединицу, а не у нулу). Дакле, хомоморфизам f успоставља изоморфизам између F и слике од f, која је потпоље од E.

в) Уочимо елемент $X+I$ у E. Означимо га са $\widetilde{X}$. Означимо и елемент $a+I$ са $\widetilde{a}$, за $a \in F$. Уколико је $a(X) = a_0 + a_1X + \cdots a_nX^n$, добијамо да је

$$a(\widetilde{X}) = \widetilde{a}_0 + \widetilde{a}_1\widetilde{X} + \widetilde{a}_2\widetilde{X}^2 + \cdots + \widetilde{a}_n\widetilde{X}^n$$

$$= (a_0+I) + (a_1+I)(X+I) + (a_2+I)(X+I)^2 + \cdots + (a_n+I)(X+I)^n,$$

$$= (a_0 + a_1X + a_2X^2 + \cdots + a_nX^n) + I = a(X) + I = I,$$

те добијамо да $\widetilde{X}$ заиста анулира полином $a(X)$.

г) Како E садржи потпоље F' изоморфно са F, заиста са алгебарске тачке можемо сматрати да је $F \subset E$. У овом случају кажемо и да је поље E једно проширење поља F. Наравно да елементе поља E можемо сабирати, али, с обзиром да је $F \subset E$, можемо их и множити елементима из F. На основу својстава операција у пољу E добијамо да је E заиста векторски простор над F. Димензију тог простора зовемо и степен проширења поља E над F и означавамо са $[E:F]$. Наш задатак је да докажемо да је $[E:F] = \deg a(X)$. Доказаћемо заправо да је

$$[1+I, X+I, \ldots, X^{n-1}+I]$$

једна база простора E уколико је полином $a(X)$ степена n.

$\{1+I, X+I, \ldots, X^{n-1}+I\}$ је генератриса: Уочимо ма који елемент $p(X)+I \in E$. Тада је

$$p(X) = q(X)a(X) + r(X),$$

где је $r(X) = 0$, или је $\deg r(X) < \deg a(X) = n$. Дакле,

$$r(X) = r_0 + r_1X + \cdots + r_{n-1}X^{n-1},$$

где наравно неки, па и сви, коефицијенти $r_i \in F$ могу бити једнаки 0. Но, тада је

$$p(X) + I = (q(X)+I)(a(X)+I) + (r(X)+I),$$

те је

$$p(X) + I = r_0(1+I) + r_1(X+I) + \cdots + r_{n-1}(X^{n-1}+I).$$

Закључујемо да $1+I, \ldots, X^{n-1}+I$ заиста генеришу E.

Линеарна независност: Нека је

$$c_0(1+I) + c_1(X+I) + \cdots + c_{n-1}(X^{n-1}+I) = 0 + I,$$

за неке $c_i \in F$. Тада је

$$(c_0 + c_1X + \cdots + c_{n-1}X^{n-1}) + I = I,$$

те

$$c_0 + c_1X + \cdots + c_{n-1}X^{n-1} \in I = \langle a(X)\rangle.$$

Но, полином $a(X)$ је степена n и он може да дели полином $c_0+c_1X+\cdots+c_{n-1}X^{n-1}$ једино ако је $c_0+c_1X+\cdots+c_{n-1}X^{n-1}=0$. Но, то управо значи да је $c_0 = c_1 = \cdots = c_{n-1} = 0$, те закључујемо да су $1+I, \ldots, X^{n-1}+I$ заиста линеарно независни. □

Искористимо управо доказану теорему да конструишемо поље од 4 елемента. Приметимо да $\mathbb{Z}_4$ јесте комутативан прстен, али наравно да да није поље пошто у $\mathbb{Z}_4$ важи: $2 \cdot 2 = 0$, а $2 \neq 0$.

Пример 153 Конструисати поље, које има тачно 4 елемента.

Како ово извести? Пре свега, ми знамо да је $\mathbb{Z}_2$ поље и да има 2 елемента. Претходна теорема нам каже да ако нађемо нерастављив полином $a(X) \in \mathbb{Z}_2[X]$, који је степена n онда ће $\mathbb{Z}_2[X]/\langle a(X)\rangle$ бити поље, које је истовремено векторски простор над $\mathbb{Z}_2$ димензије n. Дакле, то поље је као векторски простор над $\mathbb{Z}_2$ изоморфно $\mathbb{Z}_2^n$, те има 2^n елемената. Нама је потребно поље са 4 елемента, тј. потребан нам је нерастављив полином из $\mathbb{Z}_2[X]$ степена 2. Такав полином наравно није тешко наћи. То је полином $a(X) = 1 + X + X^2$. Како је то полином другог степена, он је нерастављив ако и само ако нема ниједну нулу у $\mathbb{Z}_2$, а како је $a(0) = 1$ и $a(1) + 1$, то је заиста испуњено. Дакле, наше поље F_4 је дато са

$$F_4 = \mathbb{Z}_2[X]/\langle X^2 + X + 1\rangle.$$

Означимо са η елемент $X + \langle X^2 + X + 1\rangle$ у овом пољу. Добијамо да је

$$F_4 = \{0, 1, \eta, 1 + \eta\}.$$

Како у пољу F_4 важи: $\eta^2 = 1 + \eta$ (зашто?), можемо написати и таблице сабирања и множења у том пољу.

$+$	0	1	η	$1+\eta$
0	0	1	η	$1+\eta$
1	1	0	$1+\eta$	η
η	η	$1+\eta$	0	1
$1+\eta$	$1+\eta$	η	1	0

$\cdot$	0	1	η	$1+\eta$
0	0	0	0	0
1	0	1	η	$1+\eta$
η	0	η	$1+\eta$	1
$1+\eta$	0	$1+\eta$	1	η

♣

Вратимо се поново на теорему. Претпоставимо да нам је дат неки полином $a(X) \in F[X]$ где је F неко поље. Тај полином наравно не мора имати линеарну факторизацију над пољем F. Поставља се питање: да ли постоји неко поље E које садржи поље F и у коме се полином $a(X)$ факторише на линеарне факторе? То заиста јесте тачно и претходна теорема нам показује и пут доказа.

Последица 154 Нека је F поље и $a(X) \in F[X]$. Тада постоји раширење E поља F у коме се полином $a(X)$ факторише на линеарне факторе.

Доказ. Јасно је да можемо да претпоставимо да је полином $a(X)$ нерастављив, пошто бисмо у супротном његову факторизацију добили тако што бисмо нашли раширење у коме сви његови фактори имају линеарну факторизацију.

На основу доказане теореме, постоји поље E', које је раширење поља F, а у коме полином $a(X)$ има бар једну нулу, назовимо је α. То значи да у $E'[X]$ важи факторизација

$$a(X) = (X - \alpha)b(X),$$

где је $b(X) \in E'[X]$ и $\deg b(X) = n - 1$. Уколико сада $b(X)$ раставимо на нерастављиве факторе у $E'[X]$, на њих можемо применити претходно закључивање. Тако процес настављамо све док не дођемо до линеарне факторизације. Јасно је да се процес мора завршити пошто у сваком кораку добијамо бар једну нову нулу почетног полинома, а он ни у једном пољу не може имати више од n нула. □

Сва поља, која ћемо у даљем разматрати ће бити такозвана бројевна поља, тј. потпоља од $\mathbb{C}$. Приметимо да свако такво поље обавезно садржи као своје потпоље поље $\mathbb{Q}$. Најмање раширење поља F у коме се дати полином из $F[X]$ факторише на линеарне факторе назива се коренско поље тог полинома.

Позабавимо се сада „десном" страном у изоморфизму доказаном у другом примеру. Појављује се следећа ознака: $\mathbb{Q}(\sqrt{2})$. Посматрајмо ствари мало општије.

Нека је B комутативни прстен са јединицом, A његов потпрстен (са јединицом наравно) и $b \in B \setminus A$. Како одредити најмањи потпрстен од B који садржи и A (као подскуп) и b као елемент? Очигледно је да такав прстен мора да садржи и све степене од b, као и све елементе облика $a_0 + a_1 b + a_2 b^2 + \cdots + a_n b^n$ где $a_i \in A$. Дакле, мора да садржи све елементе облика $p(b)$, где $p(X) \in A[X]$. Но, то је заправо и довољно, тј. тражени најмањи потпрстен је

$$A[b] := \{p(b) : p(X) \in A[X]\}.$$

Наиме, $A[b]$, овако дефинисан, је заиста потпрстен од B (очигледно је да је $A \subset A[b]$ и $b \in A[b]$):

$$\begin{aligned} p(b), q(b) \in A[b] &\implies p(b) - q(b) = (p - q)(b) \in A[b]; \\ p(b), q(b) \in A[b] &\implies p(b)q(b) = (pq)(b) \in A[b]. \end{aligned}$$

Уколико је F поље и $\alpha \in \mathbb{C} \setminus F$, онда са $F[\alpha]$ означавамо најмањи потпрстен који садржи F и α, а са $F(\alpha)$ најмање потпоље које садржи (као своје потпоље) F и α (као свој елемент). Поставља се природно питање: када је $F[\alpha] = F(\alpha)$? Другим речима, интересује нас у ком је случају прстен $F[\alpha]$ поље. Није тешко наћи један потребан услов за то. Претпоставимо да је $F[\alpha]$ поље. Како је

$$F[\alpha] = \{p(\alpha) : p(X) \in F[X]\},$$

а сваки елемент поља, који је различит од нуле има инверз, то и елемент $\alpha \in F[\alpha]$ има инверз у $F[\alpha]$, тј. постоји $a(\alpha) \in F[X]$ такав да је $\alpha \cdot a(\alpha) = 1$. Ако је $a(X) = a_0 + a_1 X + \cdots + a_n X^n$, то добијамо да је

$$a_n \alpha^{n+1} + \cdots + a_1 \alpha^2 + a_0 \alpha - 1 = 0,$$

тј. постоји полином $p(X) \in F[X]$ такав да је $p(\alpha) = 0$.

Дефиниција 155 Нека је F потпоље од $\mathbb{C}$ и $\alpha \in \mathbb{C}$. Тада је α алгебарски над F уколико постоји полином $p(X) \in F[X]$ за који је $p(\alpha) = 0$.

Дакле, видели смо да је потребан услов да прстен $F[\alpha]$ буде поље да је α алгебарски над F. Но, то је и довољан услов.

Став 156 Нека је F потпоље од $\mathbb{C}$ и $\alpha \in \mathbb{C}$. Тада је $F[\alpha]$ поље ако и само ако је α алгебарски над F.

Доказ. Један смер смо већ доказали. Остало је да се покаже да из чињенице да је α алгебарски над F следи да је $F[\alpha]$ поље. Како је α алгебарски над F, посматрајмо идеал $I \lhd F[X]$ дефинисан са:

$$I = \{a(X) \in F[X] : a(\alpha) = 0\}.$$

Није тешко проверити да је I заиста идеал. Како је сваки идеал у $F[X]$ главни, то постоји моничан полином $\mu_\alpha(X)$ за који је $I = \langle \mu_\alpha \rangle$.

Приметимо да је полином $\mu_\alpha(X)$ нерастављив. У супротном, нека је $\mu_\alpha(X) = a(X)b(X)$ за неке неконстантне полиноме $a(X), b(X)$ из $F[X]$. Но, тада је $a(\alpha)b(\alpha) = \mu_\alpha(\alpha) = 0$, па следи да је $a(\alpha) = 0$ или $b(\alpha) = 0$. Уколико је, на пример, $a(\alpha) = 0$, добили бисмо да $a(X) \in I$, па $\mu_\alpha(X) \mid a(X)$, што није могуће јер је $a(X)$ полином степена мањег од степена полинома $\mu_\alpha(X)$. Слично се добија и у случају да је $b(\alpha) = 0$.

Сада, као и у наведеним примерима, посматрамо хомоморфизам

$$f \colon F[X] \to F[\alpha]$$

дефинисан са $f(p(X)) = p(\alpha)$. Хомоморфизам f је очигледно „на", а $\mathrm{Ker}(f) = I$. Стога добијамо да је

$$F[X]/I \cong F[\alpha].$$

Но, како је $\mu_\alpha(X)$ нерастављив полином, $F[X]/I$ је поље, па је и $F[\alpha]$ такође поље. □

Приметимо да смо у оквиру доказа овог става добили и да је

$$[F(\alpha) : F] = \deg \mu_\alpha(X).$$

Полином $\mu_\alpha(X)$ из овог става зове се и минимални полином елемента α. Базу за $F(\alpha)$ над F чине елементи $1, \alpha, \ldots, \alpha^{n-1}$ уколико је $n = \deg \mu_\alpha(X)$.

Пример 157 Нека је $\alpha = \sqrt{2} + \sqrt{3}$.

а) Показати да је α алгебарски над $\mathbb{Q}$.

б) Наћи минимални полином за α над $\mathbb{Q}$.

в) Одредити $\frac{1}{\alpha+3}$ у облику $p(\alpha)$ за неки полином $p(X) \in \mathbb{Q}[X]$.

а) Нађимо полином који елемент α анулира. Како је $\alpha - \sqrt{2} = \sqrt{3}$, то је

$$\begin{aligned}(\alpha - \sqrt{2})^2 &= 3\\ \alpha^2 - 2\alpha\sqrt{2} + 2 &= 3\\ \alpha^2 - 1 &= 2\alpha\sqrt{2}\\ (\alpha^2 - 1)^2 &= (2\alpha\sqrt{2})^2\\ \alpha^4 - 2\alpha^2 + 1 &= 8\alpha^2\\ \alpha^4 - 10\alpha^2 + 1 &= 0.\end{aligned}$$

б) Покажимо да је минимални полином елемента α заиста полином $X^4 - 10X^2 + 1$. Означимо га са $\mu(X)$. Једино треба доказати је овај полином нерастављив над $\mathbb{Q}$. Како се ради о полиному четвртог степена, уколико је он растављив, он се раставља или на производ полинома првог степена и полинома трећег степена, или на производ два полинома другог степена.

$\mu(X)$ је производ полинома првог степена и полинома трећег степена над пољем $\mathbb{Q}$. То значи да $\mu_(X)$ има нулу у $\mathbb{Q}$. Но, ако полином

$$a_n X^n + \cdots + a_1 X + a_0$$

има рационалну нулу r/s (где је r/s нескратив разломак) онда $r \mid a_0$ и $s \mid a_n$. Како је у нашем случају $a_n = a_4 = 1$, то је $s = 1$, а како је $a_0 = 1$, то r може бити само 1 или -1. Но, ни 1 ни -1 нису нуле полинома $\mu(X)$.

$\mu(X)$ је производ два полинома другог степена. Дакле,

$$\mu(X) = (X^2 + aX + b)(X^2 + cX + d)$$

(како је $\mu(X)$ моничан, можемо претпоставити да су и ти полиноми монични). Добијамо (изједначавањем одговарајућих коефицијената)

$$\begin{aligned}a + c &= 0 &(13)\\ b + ac + d &= -10 &(14)\\ ad + bc &= 0 &(15)\\ bd &= 1 &(16)\end{aligned}$$

Из (13) добијамо да је $c = -a$. Тада из (15) следи да је $a(d - b) = 0$. Размотримо два случаја.

$a = 0$. Тада је и $c = 0$ и добијамо да се систем своди на две једначине

$$\begin{aligned} b + d &= -10 \quad (17) \\ bd &= 1 \quad (18) \end{aligned}$$

Из (18) следи да је $d = 1/b$ (сигурно ни b ни d нису једнаки нули). Заменом у (17) и сређивањем добијамо квадратну једначину

$$b^2 + 10b + 1 = 0.$$

Решења ове једначине су дата са:

$$b_{1,2} = \frac{-10 + \sqrt{96}}{2}$$

По претпоставци $b \in \mathbb{Q}$. Како је $\sqrt{96} = 4\sqrt{6}$, добили бисмо да је $\sqrt{6} \in \mathbb{Q}$. Остављамо читаоцима да покажу да ово није могуће.

$a \neq 0$. У овом случају је $b = d$. Из једначине (16) добијамо да је $b \in \{1, -1\}$. Заменом у (15) (узимајући у обзир да је $c = -a$) добијамо да је $a^2 = 12$ или $a^2 = 8$. По претпоставци је $a \in \mathbb{Q}$ па би из $a^2 = 12$ следило да $\sqrt{3} \in \mathbb{Q}$, а из $a^2 = 8$ да је $\sqrt{2} \in \mathbb{Q}$. Како ни једно ни друго није тачно закључујемо да је $\mu(X)$ нерастављив.

в) За налажење $\frac{1}{\alpha+3}$ можемо користити метод неодређених коефицијената. Наиме, знамо да постоје a, b, c, d такви да је

$$\frac{1}{\alpha + 3} = a + b\alpha + c\alpha^2 + d\alpha^3. \quad (19)$$

Потребно је одредити коефицијенте a, b, c, d. Из (19), множењем обе стране са $\alpha + 3$, добијамо

$$1 = (\alpha + 3)(a + b\alpha + c\alpha^2 + d\alpha^3). \quad (20)$$

Узимајући у обзир да је $\alpha^4 = 10\alpha^2 - 1$ и да су $1, \alpha, \alpha^2, \alpha^3$ линеарно независни над $\mathbb{Q}$, добијамо

$$\begin{array}{cccccc} 3a & & & -d & = & 1 \\ a & +3b & & & = & 0 \\ & b & +3c & +10d & = & 0 \\ & & c & +3d & = & 0 \end{array}$$

Препуштамо читаоцима да реше овај систем једначина. ♣

Дакле, видели смо да су од посебног значаја за теорију раширења поља они елементи који су алгебарски над датим пољем.

Дефиниција 158 За раширење E поља F кажемо да је алгебарско раширење ако је сваки елемент из E алгебарски над F.

За раширење E поља F кажемо да је коначно раширење уколико је E коначно димензионални простор над F.

Став 159 Свако коначно раширење је алгебарско.

Доказ. Нека је $[E : F] = n$. То значи да је E n-димензионални простор над пољем F. Узмимо произвољни елемент $\alpha \in E$ и покажимо да је он алгебарски над F. Како је димензија простора једнака n, то је скуп од $n+1$ вектора $\{1, \alpha, \ldots, \alpha^n\}$ сигурно линеарно зависан скуп вектора, тј. постоје $a_0, \ldots, a_n \in E$ такви да је

$$a_0 1 + a_1\alpha + \cdots + a_n\alpha^n = 0,$$

но, то управо значи да је $p(\alpha) = 0$, где је $p(X) = a_0 + a_1X + \cdots + a_nX^n \in F[X]$. Дакле, елемент α је алгебарски над F. □

Већ смо се упознали са проширењима облика $F(\alpha)$. Но, ако $\beta \notin F(\alpha)$, може се формирати и раширење $F(\alpha)(\beta)$, које се краће означава са $F(\alpha, \beta)$. Општије, имамо и раширења $F(\alpha_1, \ldots, \alpha_n)$. Но, веома је занимљив следећи резултат који нам каже да у случају алгебарских раширења поља $\mathbb{Q}$ ситуација није толико компликована колико изгледа.

Теорема 160 (Теорема о примитивном елементу) Свако коначно раширење E поља $\mathbb{Q}$ је облика $\mathbb{Q}(\alpha)$, за неко $\alpha \in E$.

Елемент α је тај примитивни елемент раширења E. Ову теорему нећемо доказивати.

Још два примера за крај.

Пример 161 Наћи примитивни елемент коренског поља полинома $X^4 - X^2 - 2 \in \mathbb{Q}[X]$.

Другим речима, треба наћи коренско поље K датог полинома и елемент $\alpha \in K$ за који је $K = \mathbb{Q}(\alpha)$. Факторишимо наш полином над $\mathbb{Q}$ методом комплетирања квадрата:

$$X^4 - X^2 - 2 = \left(X^2 - \frac{1}{2}\right)^2 - \frac{1}{4} - 2 = \left(X^2 - \frac{1}{2}\right)^2 - \left(\frac{3}{2}\right)^2 =$$

$$= \left(X^2 - \frac{1}{2} - \frac{3}{2}\right)\left(X^2 - \frac{1}{2} + \frac{3}{2}\right) = \left(X^2 - 2\right)\left(X^2 + 1\right) =$$

$$= (X - \sqrt{2})(X + \sqrt{2})(X - i)(X + i),$$

где је i наравно имагинарна јединица. Дакле, коренско поље K је поље $K = \mathbb{Q}(\sqrt{2}, i)$. Ми треба да нађемо α за које је $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(\alpha)$. Покушајмо да докажемо да се за α може узети елемент $\alpha = \sqrt{2} + i$. Јасно је да је $\mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{2}, i)$. Обратна инклузија је нетривијална.

Наравно, довољно је да докажемо да нпр. $\sqrt{2} \in \mathbb{Q}(\alpha)$, пошто из тога непосредно следи да и $i \in \mathbb{Q}(\alpha)$, а тиме и тражено. Једнакост

$$\alpha = \sqrt{2} + i,$$

„подигнимо" на трећи степен. Добијамо

$$\alpha^3 = 2\sqrt{2} + 6i - 3\sqrt{2} - i = -\sqrt{2} + 5i = 5(\sqrt{2} + i) - 6\sqrt{2}.$$

Дакле,

$$\alpha^3 - 5\alpha = 6\sqrt{2},$$

па је

$$\sqrt{2} = \frac{1}{6}(\alpha^3 - 5\alpha) \in \mathbb{Q}(\alpha).$$

♣

Пример 162 Нека је K коренско поље полинома $X^4 - 24X^2 + 4 \in \mathbb{Q}[X]$.
а) Показати да је $K = \mathbb{Q}(\sqrt{5}, \sqrt{7})$.
б) Одредити $\alpha \in \mathbb{C}$ тако да је $K = \mathbb{Q}(\alpha)$.

Поступимо као у претходном примеру.

$$\begin{aligned} X^4 - 24X^2 + 4 &= (X^2 - 12)^2 - 144 + 4 \\ &= (X^2 - 12)^2 - 140 \\ &= (X^2 - 12)^2 - (2\sqrt{35})^2 \\ &= (X^2 - 12 - 2\sqrt{35})(X^2 - 12 + 2\sqrt{35}) \\ &= (X^2 - (12 + 2\sqrt{35})(X^2 - (12 - 2\sqrt{35}), \end{aligned}$$

те добијамо $X^4 - 24X^2 + 4 = (X - \sqrt{12 + 2\sqrt{35}})(X + \sqrt{12 + 2\sqrt{35}})(X - \sqrt{12 - 2\sqrt{35}})(X + \sqrt{12 - 2\sqrt{35}})$. Према томе, добијамо да је

$$K = \mathbb{Q}\left(\sqrt{12 + 2\sqrt{35}}, \sqrt{12 - 2\sqrt{35}}\right).$$

Један савет: увек када добијете овакав резултат, није лоше помножити ова два корена и видети шта се добија. Применимо тај савет у овом случају.

$$\sqrt{12 + 2\sqrt{35}} \cdot \sqrt{12 - 2\sqrt{35}} = \sqrt{144 - 140} = \sqrt{4} = 2.$$

Дакле, можемо да закључимо да, ако је $\alpha = \sqrt{12 + 2\sqrt{35}}$, а $\beta = \sqrt{12 - 2\sqrt{35}}$, онда је $\alpha \cdot \beta = 2$, па је $\beta = \frac{2}{\alpha} \in \mathbb{Q}(\alpha)$. Закључујемо да је $K = \mathbb{Q}(\alpha)$. Тако смо нашли примитивни елемент и урадили пример под б)!

Други савет: када имате корен попут овога: $\sqrt{12 + 2\sqrt{35}}$, проверите да можда не можете да га „препознате". Шта то значи? У овом

случају, појављује се корен из броја облика $p + q\sqrt{s}$ где су p, q, s цели бројеви. Да ли је можда тај корен збир (или разлика) два корена из неких целих бројева? Како је $35 = 5 \cdot 7$, намеће се да израчунамо колико је $(\sqrt{5} + \sqrt{7})^2$. Добијамо

$$(\sqrt{5} + \sqrt{7})^2 = 5 + 2\sqrt{35} + 7 = 12 + 2\sqrt{35},$$

тј. баш оно што имамо. Дакле, $\alpha = \sqrt{5} + \sqrt{7}$ (приметимо да је $\beta = \sqrt{7} - \sqrt{5}$), те је $K = \mathbb{Q}\left(\sqrt{5} + \sqrt{7}\right)$. Ми треба да покажемо да је $K = \mathbb{Q}\left(\sqrt{5}, \sqrt{7}\right)$. То није тешко, поступићемо као у претходном примеру.

$$\begin{aligned}
\alpha &= \sqrt{5} + \sqrt{7} \\
\alpha^3 &= 5\sqrt{5} + 15\sqrt{7} + 21\sqrt{5} + 7\sqrt{7} \\
\alpha^3 &= 26\sqrt{5} + 22\sqrt{7} \\
22\alpha &= 22\sqrt{5} + 22\sqrt{7} \\
\alpha^3 - 22\alpha &= 4\sqrt{5} \\
\sqrt{5} &= \frac{\alpha^3 - 22\alpha}{4} \in \mathbb{Q}(\alpha) \\
\sqrt{7} &= \alpha - \sqrt{5} \\
\sqrt{7} &= \frac{26\alpha - \alpha^3}{4} \in \mathbb{Q}(\alpha).
\end{aligned}$$

Наравно, могли смо то да урадимо и другачије. Пошто смо већ препознали да је $\beta = \sqrt{7} - \sqrt{5}$, онда само треба показати да је

$$\mathbb{Q}\left(\sqrt{5} + \sqrt{7}, \sqrt{7} - \sqrt{5}\right) = \mathbb{Q}\left(\sqrt{5}, \sqrt{7}\right),$$

а то је наравно врло једноставно. ♣

Елементи опште алгебре

На самом почетку курса навели смо уистину основне појмове — појам алгебарске операције и алгебарске структуре. Потом смо се бавили конкретним структурама и ту су централну улогу имале групе, Абелове групе, комутативни прстени и поља. У овом завршном делу позабавићемо се општим алгебарским структурама и како се у општем случају уводе појмове, које смо обрађивали у случају конкретних структура које смо обрађивали.

Да бисмо радили са алгебарским структурама, тј. да бисмо испитали који закони важе у њима, морамо најпре увести појам алгебарског закона, а за то нам је потребан и појам алгебарског израза.

Појам алгебарског израза нам јесте познат из школске математике (појављује се чак и у укрштеним речима — једночлани алгебарски израз познат нам је као моном), али вероватно не баш у прецизној формулацији. У сваком случају, знамо да су алгебарски изрази неки записи у којима се појављују константе, променљиве и знаци алгебарских операција. Дакле, сам израз није неки број, него неки запис. Сваки запис је записан на неком језику, те нам је стога погодно да уведемо појам алгебарског језика.

Дефиниција 163 Алгебарски језик је произвољан непразан скуп чије елементе називамо функцијски (операцијски) симболи. Осим тога, сваком симболу је придружен један природан број, који представља његову дужину.

Обично користимо L као ознаку за алгебарски језик. Уколико $F \in L$, онда дужину симбола F означавамо са $\#(F)$. На пример, уколико желимо да записујемо изразе у којима се појављује само сабирање, довољно је узети да је $L = \{+\}$, где је овде $+$ симбол за сабирање (а не сама операција!). Уколико је ситуација сложенија, па разматрамо и сабирање и множење, а и нулу и јединицу, онда радимо са алгебарским језиком $L = \{+, \cdot, 0, 1\}$, где су овде $+$ и $\cdot$ операцијски симболи дужине 2, а 0 и 1 операцијски симболи дужине 0, који се називају и симболи константи (писали смо већ да су константе заправо нуларне операције, тј. операције дужине 0). Наравно, да бисмо записивали алгебарске изразе биће нам неопходни и зарези, као и заграде. Но, како су они увек потребни, не стављају се као део самог алгебарског језика (можда је ово добро место да поновите неке основне појмове логике првог реда, које сте обрадили у оквиру увода у математичку логику).

Као што нам је познато из школске математике, у оквиру израза се, поред заграда, знакова алгебарских операција и константи, такође појављују и променљиве. Дакле, потребан нам је и један скуп променљивих $\mathcal{V}ar = \{x_0, x_1, \ldots\}$. Овде је наведен скуп од пребројиво много променљивих, али наравно да ћемо ми у пракси најчешће користити и

ознаке x, y, z и слично за променљиве (просто је једноставније у формулама користити ове ознаке).

Сада можемо дефинисати и појам алгебарског израза (или само израза).

Дефиниција 164 Нека је L неки алгебарски језик. Алгебарски изрази језика L дефинишу се са:

- Променљиве и симболи константи су алгебарски изрази.
- Ако су $t_1, \ldots, t_n$ алгебарски изрази и $F(\in L)$ операцијски симбол језика L дужине n $(n \geq 1)$, онда је и $F(t_1, \ldots, t_n)$ алгебарски израз.
- Алгебарски изрази се могу добити једино коначном применом претходна два правила.

Дакле, последње својство нам говори о коначности записа алгебарских израза. Нпр. ако је $L = \{+, \cdot, 0, 1\}$ где су $+$ и $\cdot$ операцијски симболи дужине 2, а 0 и 1 симболи константи, онда

$$(x + 0), ((1 + 1) \cdot (x + (1 \cdot y))), (1 \cdot (0 \cdot 1))$$

јесу алгебарски изрази, док

$$1 + 1 + \cdots$$

то није.

Као што знамо, алгебарске изразе можемо да израчунавамо, тј. можемо наћи вредност алгебарског израза чим знамо вредности свих променљивих које се у њему појављују. Наравно, морамо да будемо мало опрезнији. На пример, на шта прво помислите када угледате запис

$$A + B$$

на табли? Вероватно је прва асоцијација да је неко сабирао две матрице. Или можда два линеарна оператора. Али, зашто би то било тако? Можда је реч о сабирању два полинома, или чак два реална броја. Наравно да бројеве најчешће пишемо малим словима, али то што је најчешће, не значи и да је увек. Још је више нејасно о чему се ради ако угледате

$$A * B$$

на табли или у нечијој свесци. Шта је сад ово? Јасно је да морамо да знамо више да бисмо могли да израчунамо неки израз. Најпре, морамо да знамо у ком скупу радимо, затим морамо да знамо о којим се операцијама ради (дакле, морамо да знамо интерпретацију операцијских симбола који се ту појављују, нпр. којој операцији одговара симбол звездице из горњег израза). Наравно, симболу дужине n одговара n-арна операција. Посебно, константном симболу (симболу дужине 0) одговара неки елемент из A. Напокон, морамо да знамо вредности променљивих које се појављују у изразу (придруживање $\alpha: \mathcal{V}ar \to A$ обично се назива валуација (увод у математичку логику...)).

Дефиниција 165 Вредност алгебарског израза t језика L при датој валуацији $\alpha: \mathcal{V} \to A$, у ознаци $t^{\mathbb{A}}[\alpha]$, где је $\mathbb{A}$ алгебарска структура језика L са скупом носачем A, дефинише се на следећи начин.

- Вредност симбола константе c је онај елемент $c^{\mathbb{A}}$ скупа A који је интерпретација константе c.
- Вредност промењиве x_i је $\alpha(x_i)$.
- Ако је $t = F(t_1, \ldots, t_n)$ где су $t_1, \ldots, t_n$ изрази и $F(\in L)$ операцијски симбол дужине n, онда је $t^{\mathbb{A}}[\alpha] = F^{\mathbb{A}}(t_1^{\mathbb{A}}[\alpha], \ldots, t_n^{\mathbb{A}}[\alpha])$, при чему је $F^{\mathbb{A}}$ интерпретација операцијског симбола F (дакле операција дужине n, која одговара симболу F).

Ово можда делује компликовано, али заправо није. Урадимо два примера.

Пример 166 Нека је $L = \{+, \cdot, 1\}$, где су $+$ и $\cdot$ операцијски симболи дужине 2, а 1 симбол константе. Ако је $\mathbb{A} = (M_2(\mathbb{R}), +, \cdot, E)$ алгебарска структура коју чине матрице реда 2 и у којима је $+$ операција сабирања матрица, $\cdot$ операција множења матрица, а E јединична матрица, израчунати вредност израза $((x+1)\cdot(x+1))$ уколико је валуација α таква да је

$$\alpha(x) = \begin{bmatrix} 2 & 3 \\ 1 & -2 \end{bmatrix},$$

док се $+$ интепретира као сабирање матрица, $\cdot$ као множење матрица, а 1 као јединична матрица.

Решење: Вредност датог израза је заправо једнака матрици

$$(\alpha(x) + E) \cdot (\alpha(x) + E),$$

односно матрици

$$\left(\begin{bmatrix} 2 & 3 \\ 1 & -2 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right) \cdot \left(\begin{bmatrix} 2 & 3 \\ 1 & -2 \end{bmatrix} + \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right),$$

чију ће вредност читаоци лако израчунати. ♣

Приметимо да је знак $+$ овде и операцијски симбол, а и сама операција! Уобичајен је случај да се користи иста ознака подразумевајући да се води рачуна о контексту у коме се дати симболи појављују. Уколико постоји могућност грешке, користе се различите ознаке.

Пример 167 Нека је $L = \{*, \circ, n, j\}$, где су $*$ и $\circ$ операцијски симболи дужине 2, а n и j симболи константи. Дат је израз

$$((x_1 * j) \circ ((j * (j * n)) * j)).$$

Израчунати вредност овог израза ако знамо да је алгебарска структура о којој се ради структура $\mathbb{Z}_3 = (Z_3, +_3, \cdot_3, 0, 1)$ при валуацији $\alpha : \mathcal{V}ar \to Z_3$, где је $\alpha(x_1) = 1$, док се $*$ интерпретира као сабирање, а $\circ$ као множење по модулу 3 и интерпретација константног симбола n је 0, а j је 1.

Решење: Урадимо ово детално. Како се $*$ интерпретира са $+_3$, а $\circ$ са $\cdot_3$, док је интепретација за n елемент 0, а за j елемент 1, добијамо:

$$\begin{aligned}
&((x_1 * j) \circ ((j * (j * n)) * j))^{\mathbb{Z}_3}[\alpha] \\
&= (x_1 * j)^{\mathbb{Z}_3}[\alpha] \cdot_3 ((j * (j * n)) * j)^{\mathbb{Z}_3}[\alpha] \\
&= (x_1^{\mathbb{Z}_3}[\alpha] +_3 j^{\mathbb{Z}_3}[\alpha]) \cdot_3 ((j * (j * n))^{\mathbb{Z}_3}[\alpha] +_3 j^{\mathbb{Z}_3}[\alpha]) \\
&= (\alpha(x_1) +_3 1) \cdot_3 ((j^{\mathbb{Z}_3}[\alpha] +_3 (j * n)^{\mathbb{Z}_3}[\alpha]) +_3 1) \\
&= (1 +_3 1) \cdot_3 ((1 +_3 (j^{\mathbb{Z}_3}[\alpha] +_3 n^{\mathbb{Z}_3}[\alpha])) +_3 1) \\
&= 2 \cdot_3 ((1 +_3 (1 +_3 0)) +_3 1) \\
&= 2 \cdot_3 ((1 +_3 1) +_3 1) \\
&= 2 \cdot_3 (2 +_3 1) \\
&= 2 \cdot_3 0 \\
&= 0.
\end{aligned}$$

♣

Позабавимо се сада појмом алгебарског закона и појмом алгебарске теорије.

Дефиниција 168 Нека је L неки алгебарски језик. Алгебарски закон језика L је формула облика $t_1 = t_2$, где су t_1 и t_2 алгебарски изрази језика L.

Дефиниција 169 Уколико је $\mathbb{A}$ алгебарска структура језика L и $t_1 = t_2$ неки алгебарски закон истог језика онда тај закон важи у алгебри $\mathbb{A}$, или да је $\mathbb{A}$ модел за тај закон, у ознаци

$$\mathbb{A} \models t_1 = t_2,$$

уколико за сваку валуацију $\alpha\colon \mathcal{V}ar \to A$ важи:

$$t_1^{\mathbb{A}}[\alpha] = t_2^{\mathbb{A}}[\alpha].$$

Другим речима, закон $t_1 = t_2$ важи у алгебри $\mathbb{A}$, уколико се вредности ових израза поклапају за све могуће вредности променљивих из скупа носача A.

Дефиниција 170 Скуп алгебарских закона назива се алгебарска теорија, а елементи тог скупа називају се аксиоме те теорије.

Дефиниција 171 Уколико је T нека алгебарска теорија, онда се са $\mathfrak{M}(T)$ означава класа свих алгебри у којима важе сви закони из T.

Класа $\mathfrak{M}(T)$ зове се и варијетет теорије T. Нека класа $\mathfrak{M}$ алгебри истог језика је варијетет (или једнакосна класа) уколико постоји алгебарска теорија T таква да је $\mathfrak{M} = \mathfrak{M}(T)$.

Овде је важно истаћи неколико чињеница. Најпре, ма каква била теорија T, увек постоји алгебра у којој су тачни сви закони из T.

Наиме, ма која једночлана алгебра $\mathbb{A} = \{a\}$, где је a произвољно је пример такве алгебре. Јасно је да су све операције у овој алгебри тривијалне и да сви алгебарски закони ту важе. Осим тога, $\mathfrak{M}(T)$ је заиста класа, а не скуп. Ово је већ опажање које је базирано на резултатима теорије скупова. Наиме, добро је познато да не постоји скуп чији су елементи сви скупови. Но, не постоји ни скуп који садржи све једночлане скупове (ово је питање из теорије скупова и тиме се нећемо бавити — читалац може консултовати неки основни уџбеник у коме се ово разматра). Како све једночлане алгебре (прецизније говорећи алгебре са једночланим базним скупом) припадају класи $\mathfrak{M}(T)$, то је та класа заиста сувише обимна да би представљала скуп.

Пример 172 Нека језик L садржи операцијски знак $\cdot$ дужине 2. тада је

$$((x \cdot y) \cdot z) = (x \cdot (y \cdot z)),$$

где су x, y, z ма које променљиве један алгебарски закон и наравно да нам је он познат као закон асоцијативности. Уколико се у L налази и операцијски знак $+$ дужине 2, онда је закон

$$(x \cdot (y + z)) = ((x \cdot y) + (x \cdot z)),$$

добро познат као закон дистрибутивности.

Наравно, у пракси ћемо избегавати писање непотребних заграда, па ћемо закон асоцијативности записивати у облику

$$(x \cdot y) \cdot z = x \cdot (y \cdot z),$$

а закон дистрибутивности у облику

$$x \cdot (y + z) = x \cdot y + x \cdot z.$$

Наведимо сада, у облику табеле, примере неких алгебарских теорија.

Теорија	**Језик**	**Аксиоме**
групоида (G)	$L_G = \{\cdot\}$	нема
полугрупа (S)	$L_S = L_G$	$(x \cdot y) \cdot z = x \cdot (y \cdot z)$
моноида (M)	$L_M = L_S \cup \{1\}$	$(x \cdot y) \cdot z = x \cdot (y \cdot z)$, $x \cdot 1 = x$, $1 \cdot x = x$
група (Grp)	$L_{Grp} = L_M \cup \{'\}$	$(x \cdot y) \cdot z = x \cdot (y \cdot z)$, $x \cdot 1 = x$, $1 \cdot x = x$, $x \cdot x' = 1$, $x' \cdot x = 1$
Абелових група (Ab)	$L_{Ab} = \{+, -, 0\}$	$(x + y) + z = x + (y + z)$, $x + 0 = x$, $0 + x = x$, $x + (-x) = 0$, $(-x) + x = 0$, $x + y = y + x$
прстена (Rng)	$L_{Rng} = L_{Ab} \cup L_S$	$(x + y) + z = x + (y + z)$, $x + 0 = x$, $0 + x = x$, $x + (-x) = 0$, $(-x) + x = 0$, $x + y = y + x$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, $x \cdot (y + z) = x \cdot y + x \cdot z$, $(y + z) \cdot x = y \cdot x + z \cdot z$
прстена са јединицом ($Ring$)	$L_{Ring} = L_{Ab} \cup L_M$	$(x + y) + z = x + (y + z)$, $x + 0 = x$, $0 + x = x$, $x + (-x) = 0$, $(-x) + x = 0$, $x + y = y + x$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, $x \cdot (y + z) = x \cdot y + x \cdot z$, $(y + z) \cdot x = y \cdot x + z \cdot x$, $x \cdot 1 = x$, $1 \cdot x = x$
комутативних прстена ($ComRng$)	$L_{ComRng} = L_{Rng}$	$(x + y) + z = x + (y + z)$, $x + 0 = x$, $0 + x = x$, $x + (-x) = 0$, $(-x) + x = 0$, $x + y = y + x$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, $x \cdot (y + z) = x \cdot y + x \cdot z$, $x \cdot y = y \cdot x$
комутативних прстена са јединицом ($ComRing$)	$L_{ComRing} = L_{Ring}$	$(x + y) + z = x + (y + z)$, $x + 0 = x$, $0 + x = x$, $x + (-x) = 0$, $(-x) + x = 0$, $x + y = y + x$, $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, $x \cdot (y + z) = x \cdot y + x \cdot z$, $x \cdot y = y \cdot x$, $x \cdot 1 = x$, $1 \cdot x = x$

Саме алгебарске теорије о којима је реч (подсетимо се да је алгебарска теорија скуп алгебарских закона) могу се краће и овако изразити:

- $G = \emptyset$;
- $S = G \cup \{(x \cdot y) \cdot z = x \cdot (y \cdot z)\}$;
- $M = S \cup \{x \cdot 1 = x, 1 \cdot x = x\}$;
- $Grp = M \cup \{x \cdot x' = 1, x' \cdot x = 1\}$
- $Ab = \{(x + y) + z = x + (y + z), x + 0 = x, 0 + x = x, x + (-x) = 0, (-x) + x = 0, x + y = y + x\}$;
- $Rng = Ab \cup S \cup \{x \cdot (y + z) = x \cdot y + x \cdot z, (y + z) \cdot x = y \cdot x + z \cdot x\}$;
- $Ring = Rng \cup M$;
- $ComRng = Rng \cup \{x \cdot y = y \cdot x\}$;

- $ComRing = ComRng \cup M$.

На пример, $\mathfrak{M}(Grp)$ означава класу свих група, док $\mathfrak{M}(ComRing)$ означава класу свих комутативних прстена са јединицом.

Хомоморфизми, директни производи и конгруенције

Нека су $\mathbb{A}$, $\mathbb{B}$ и $\mathbb{C}$ алгебре исте сигнатуре:

$$\begin{aligned} \mathbb{A} &= (A, \phi_1, \ldots, \phi_r, a_1, \ldots, a_s), \\ \mathbb{B} &= (B, \psi_1, \ldots, \psi_r, b_1, \ldots, b_s), \\ \mathbb{C} &= (C, \theta_1, \ldots, \theta_r, c_1, \ldots, c_s). \end{aligned}$$

Овде су a_i, b_j, c_k изабрани елементи (константе), док су остало операције ненулте дужине. Наравно, $\#(\phi_i) = \#(\psi_i) = \#(\theta_i)(= n_i)$.

Дефиниција 173 Функција $h\colon A \to B$ је хомоморфизам алгебре $\mathbb{A}$ у алгебру $\mathbb{B}$ уколико важи:

- за све $j = \overline{1,s}$: $h(a_j) = b_j$.
- за све $i = \overline{1,r}$ и све $u_1, \ldots, u_{n_i} \in A$:
  $h(\phi_i(u_1, \ldots, u_{n_i})) = \psi_i(h(u_1), \ldots, h(u_{n_i}))$.

Дакле, хомоморфизам је она функција једног скупа носача у други, која константе слика у одговарајуће константе, а „комутира" са свим (одговарајућим) операцијама. Када желимо да истакнемо да је $h\colon A \to B$ хомоморфизам алгебри, писаћемо: $h\colon \mathbb{A} \to \mathbb{B}$ је хомоморфизам.

Дефиниција 174 Нека је $h\colon \mathbb{A} \to \mathbb{B}$ хомоморфизам.

- Уколико је h „1–1", кажемо да је h мономорфизам.
- Уколико је h „на", кажемо да је h епиморфизам.
- Уколико је h „1–1" и „на", кажемо да је h изоморфизам.
- Уколико је $\mathbb{A} = \mathbb{B}$, кажемо да је h ендоморфизам.
- Уколико је h изоморфизам и ендоморфизам, кажемо да је h аутоморфизам.

Став 175 Нека су $h\colon \mathbb{A} \to \mathbb{B}$ и $g\colon \mathbb{B} \to \mathbb{C}$ хомоморфизми. Тада:

а) $g \circ h$ је хомоморфизам.

б) Ако је су g и h мономорфизми, онда је то и $g \circ h$.

в) Ако је су g и h епиморфизми, онда је то и $g \circ h$.

г) Ако је су g и h изоморфизми, онда је то и $g \circ h$.

д) Ако је h изоморфизам, онда је h^{-1} изоморфизам.

Доказ. Доказаћемо само тврђења а) и д) (јасно је да остали резултати следе из основних чињеница о функцијама).

Доказ за а)

$$\begin{aligned}(g \circ h)(a_i) &= g(h(a_i)) \\ &= g(b_i) \quad (\text{пошто је } h \text{ хомоморфизам}) \\ &= c_i \qquad (\text{пошто је } g \text{ хомоморфизам}).\end{aligned}$$

$$\begin{aligned}(g \circ h)(\phi_i(u_1, \ldots, u_{n_i}) &= g(h(\phi_i(u_1, \ldots, u_{n_i})) \\ &= g(\psi_i(h(u_1), \ldots, h(u_{n_i})) \quad (\ h \text{ је хомоморфизам}) \\ &= \theta_i(g(h(u_1)), \ldots, g(h(u_{n_i}))) \quad (g \text{ је хомоморфизам}) \\ &= \theta_i((g \circ h)(u_1), \ldots, (g \circ h)(u_{n_i})).\end{aligned}$$

Доказ за д) Знамо да h^{-1} постоји и да $h^{-1}\colon B \to A$. Треба показати да је h^{-1} хомоморфизам.

Како је $h(a_i) = b_i$, то је и $h^{-1}(b_i) = a_i$.

Нека су $v_1, \ldots, v_{n_i}$ произвољни елементи из B. Како је h „на", то постоје u_j из A такви да је $h(u_j) = v_j$ за све $j = \overline{1, n_i}$. Добијамо

$$\begin{aligned}h^{-1}(\psi_i(v_1, \ldots, v_{n_i})) &= h^{-1}(\psi_i(h(u_1), \ldots, h(u_{n_i})) \\ &= h^{-1}(h(\phi_i(u_1, \ldots, u_{n_i}))(h \text{ је хомоморфизам}) \\ &= \phi_i(u_1, \ldots, u_{n_i}) \\ &= \phi_i(h^{-1}(v_1), \ldots, h^{-1}(v_{n_i})).\end{aligned}$$

□

Наведимо неке примере.

Пример 176 Са $\mathbf{R}^+$ означимо скуп позитивних реалних бројева. Тада је функција $\ln\colon \mathbf{R}^+ \to \mathbf{R}$ хомоморфизам групе $(\mathbf{R}^+, \cdot, ^{-1}, 1)$ у групу $(\mathbf{R}, +, -, 0)$ (добро нам је познато да је $\ln(x \cdot y) = \ln x + \ln y$, $\ln(x^{-1}) = -\ln x$ и $\ln 1 = 0$).

Пример 177 Конјуговање, тј. функција $g\colon \mathbf{C} \to \mathbf{C}$, задата са $g(z) = \overline{z}$, представља аутоморфизам алгебре $\mathbb{C} = (\mathbf{C}, +, \cdot, 0, 1)$ (са $\mathbf{C}$ је наравно означен скуп свих комплексних бројева).

Пример 178 Ако је $\rho_n: Z \to Z_n$ функција која целом броју придружује његов остатак по модулу n (где је $n \geq 2$), онда је тако задата хомоморфизам комутативног прстена са јединицом $\mathbb{Z} = (Z, +, \cdot, -, 0, 1)$ у комутативан прстен са јединицом $\mathbb{Z}_n = (Z_n, +_n, \cdot_n, -_n, 0, 1)$

Покажимо да је ρ_n заиста хомоморфизам. Пре свега, јасно је да је $\rho_n(0) = 0$ и $\rho_n(1) = 1$. Проверимо да важи и

$$\rho_n(s + t) = \rho_n(s) +_n \rho_n(t), \rho_n(s \cdot t) = \rho_n(s) \cdot_n \rho_n(t), \rho_n(-s) = -_n \rho(s).$$

Пре свега,

$$s = q \cdot n + \rho_n(s), \quad t = q' \cdot n + \rho_n(t),$$

за јединствено одређене целе бројеве q и q' (дељење са остатком). Добијамо да је

$$s + t = (q + q') \cdot n + (\rho_n(s) + \rho_n(t)).$$

Подсетимо се операције сабирања по модулу n. Добијамо да је

$$\rho_n(s) + \rho_n(t) = q'' \cdot n + (\rho_n(s) +_n \rho_n(t)),$$

за јединствено одређен цео број q'' (наравно да је тај број у овом случају или 0 или 1). Заменом у претходну једначину добијамо да је

$$s + t = (q + q' + q'') \cdot n + (\rho_n(s) +_n \rho_n(t)).$$

Како је $0 \leq \rho_n(s) +_n \rho_n(t) < n$, то на основу јединствености дељења са остатком можемо да закључимо да је $\rho_n(s) +_n \rho_n(t)$ заиста остатак при дељењу броја $s + t$ са n, тј. да важи

$$\rho_n(s + t) = \rho_n(s) +_n \rho_n(t),$$

а то је и требало доказати. На врло сличан начин се показује да је и

$$\rho_n(s \cdot t) = \rho_n(s) \cdot_n \rho_n(t),$$

Покажимо за крај да је $\rho(-s) = -_n s$ за све целе бројеве s. Пре свега,

$$s = q \cdot n + \rho_n(s),$$

за јединствено одређен цео број q. Тада је

$$-s = (-q) \cdot n + (-\rho_n(s)).$$

Уколико је $\rho_n(s) = 0$, то добијамо да је и $\rho_n(-s) = 0$, те је заиста $\rho_n(-s) = -_n \rho_n(s)$ (поновите дефиницију унарне операције $-_n$). У супротном је $0 < n - \rho_n(s) < n$. Добијамо да је

$$-s = (-q - 1) \cdot n + (n - \rho_n(s)),$$

где је $-q-1$ цео број, а $0 < n-\rho_n(s) < n$. Дакле, $n-\rho_n(s)$ је остатак при дељењу $-s$ са n, тј. заиста је $\rho_n(-s) = -_n s$. ♣

Позабавимо се сада нечим другим. Нека за наше алгебре $\mathbb{A}$ и $\mathbb{B}$ важи да је $A \subseteq B$. Природно је тада размотрити инклузију скупа A у скуп B, тј. функцију $i\colon A \to B$ такву да је $i(u) = u$ за све $u \in A$. Природно се поставља питање: да ли је i хомоморфизам? Анализирајмо мало ту ситуацију. Уколико је i заиста хомоморфизам, онда мора бити $i(a_k) = b_k$ за све $k = \overline{1,s}$ а како је $i(a_k) = a_k$, закључујемо да мора бити $a_k = b_k$ за све $k = \overline{1,s}$. Слично, мора бити испуњено и

$$\phi_k(u_1,\ldots,u_{n_k}) = i(\phi_k(u_1,\ldots,u_{n_k})) = \psi_k(i(u_1),\ldots,i(u_{n_k})) = \psi_k(u_1,\ldots,u_{n_k}),$$

за све $u_j \in A$. Дакле, операције ϕ_k и ψ_k морају давати исти резултат уколико су им аргументи из A. Често се краће каже да је операција ϕ_k рестрикција операције ψ_k.

Дефиниција 179 Нека је $\mathbb{A}$ и $\mathbb{B}$ алгебре за које важи: $A \subseteq B$. Тада је $\mathbb{A}$ подалгебра алгебре $\mathbb{B}$ уколико је за све $k = \overline{1,s}$ испуњено $a_k = b_k$ и уколико за све $u_j \in A$ и све $i = \overline{1,r}$ важи: $\phi_i(u_1,\ldots,u_{n_i}) = \psi_i(u_1,\ldots,u_{n_i})$

Уколико је $\mathbb{A}$ подалгебра од $\mathbb{B}$, то ћемо краће записивати са:

$$\mathbb{A} \leq \mathbb{B}.$$

Приметимо да из претходне дискусије следи да је $\mathbb{A} \leq \mathbb{B}$ ако и само ако је инклузија $i\colon A \to B$ хомоморфизам.

Примере није тешко наћи:

$$\mathbb{Z}(=(Z,+,\cdot,0,1)) \leq \mathbb{Q}(=(Q,+,\cdot,0,1)) \leq \mathbb{R}(=(R,+,\cdot,0,1)) \leq \mathbb{C}(=(C,+,\cdot,0,1)),$$

но приметимо да

$$\mathbb{Z}_n \not\leq \mathbb{Z},$$

јер се операције не поклапају на мањем скупу.

Један важан пример подалгебре појављује се на следећи начин. Нека је $h\colon\colon \mathbb{A} \to \mathbb{B}$ хомоморфизам алгебри. Посматрајмо слику хомоморфизма h:

$$\mathrm{Im}(h) = h[A] = \{h(u) : u \in A\}.$$

Како је $h(a_i) = b_i$ (подсетите се конвенције са почетка ове лекције), то сви изабрани елементи $b_1,\ldots,b_s$ припадају $\mathrm{Im}(h)$. Осим тога, нека су $v_1,\ldots,v_{n_i}$ произвољни елементи из $\mathrm{Im}(h)$. Тада постоје $u_1,\ldots,u_{n_i}$, такви да је $h(u_1) = v_1,\ldots,h(u_{n_i}) = v_{n_i}$. Стога добијамо:

$$\psi_i(v_1,\ldots,v_{n_i}) = \psi_i(h(u_1),\ldots,h(u_{n_i})) = h(\phi_i(v_1,\ldots,v_{n_i})) \in \mathrm{Im}(h).$$

Дакле, рестрикције операција $\psi_1,\ldots,\psi_r$ задају операције на $\mathrm{Im}(h)$, а како и $b_1,\ldots,b_s \in \mathrm{Im}(h)$, то је природно задата структура алгебре на $\mathrm{Im}(h)$, која је чини подалгебром алгебре $\mathbb{B}$. Користимо ознаку $h[\mathbb{A}]$ да означимо ту подалгебру.

Пређимо сада на појам директног производа алгебри.

Дефиниција 180 Нека су

$$\mathbb{A} = (A, \phi_1, \ldots, \phi_r, a_1, \ldots, a_s)$$

и

$$\mathbb{B} = (B, \psi_1, \ldots, \psi_r, b_1, \ldots, b_s)$$

две алгебре исте сигнатуре $\sigma(\mathbb{A}) = \sigma(\mathbb{B}) = (n_1, \ldots, n_r, \underbrace{0, \ldots, 0}_{s})$. Директан производ ових алгебри је алгебра

$$\mathbb{P} = (P, \zeta_1, \ldots, \zeta_r, p_1, \ldots, p_s),$$

где је $P = A \times B$, $p_j = (a_j, b_j)$, а операције ζ_i задате са:

$$\zeta_i((u_1, v_1), \ldots, (u_{n_i}, v_{n_i})) := (\phi_i(u_1, \ldots, u_{n_i}), \psi(v_1, \ldots, v_{n_i})).$$

Дакле, операције ζ_i су задате „по координатама".

Јасно је да је сигнатура алгебре $\mathbb{P}$ једнака сигнатури алгебра $\mathbb{A}$ и $\mathbb{B}$. Ми ћемо се касније бавити производима конкретних алгебарских структура, нпр. производима група, Абелових група, комутативних прстена са јединицом и сл. и тада ћемо се детаљније бавити овим појмом. Урадимо за сада само један једноставан пример.

Пример 181 Посматрајмо производ Абелових група $\mathbb{Z}_3$ и $\mathbb{Z}_4$. Скуп носач P је скуп

$$Z_3 \times Z_4 = \{0, 1, 2\} \times \{0, 1, 2, 3\}.$$

Операција на P је задата са:

$$(m_1, n_1) + (m_2, n_2) = (m_1 +_3 m_2, n_1 +_4 n_2),$$

где $m_i \in Z_3$, а $n_j \in Z_4$. На пример,

$$(2, 3) + (1, 2) = (0, 1).$$

Касније ћемо видети да постоји изоморфизам овог производа и групе $\mathbb{Z}_{12}$.

Може се дефинисати и производ алгебри $\mathbb{A}_1, \ldots, \mathbb{A}_n$ (за ма које n):

$$\mathbb{A}_1 \times \cdots \times \mathbb{A}_n.$$

где се операције изводе „по координатама", но алтернативно се тај производ може добити и поновљеним производима две алгебре (тј. тако ће се добити изоморфне алгебре). Нпр. алгебра $\mathbb{A}_1 \times \mathbb{A}_2 \times \mathbb{A}_3$ изоморфна је алгебри $(\mathbb{A}_1 \times \mathbb{A}_2) \times \mathbb{A}_3$ (а такође и алгебри $\mathbb{A}_1 \times (\mathbb{A}_2 \times \mathbb{A}_3)$), но више о томе ће бити речи касније, за конкретне алгебарске структуре. Произвољан директан производ (можда и бесконачно много алгебри)

$$\prod_{i \in I} \mathbb{A}_i,$$

такође није тешко дефинисати, али га ми нећемо разматрати.

У случају директног производа алгебри $\mathbb{A} \times \mathbb{B}$, природно се појављују два епиморфизма, пројекције на прву, односно другу координату:

$$\pi_A : \mathbb{A} \times \mathbb{B} \to \mathbb{A}, \quad \pi_A(u, v) = u,$$

$$\pi_B : \mathbb{A} \times \mathbb{B} \to \mathbb{B}, \quad \pi_A(u, v) = v.$$

Није тешко проверити да су то заиста хомоморфизми одговарајућих алгебри који су очигледно „на". Оно што је занимљиво у вези ових хомоморфизама је следећа чињеница. За сваку алгебру $\mathbb{C}$ исте сигнатуре, као и $\mathbb{A}$ и $\mathbb{B}$ и све хомоморфизме $h: \mathbb{C} \to \mathbb{A}$ и $g: \mathbb{C} \to B$ постоји јединствено одређени хомоморфизам $f: \mathbb{C} \to \mathbb{A} \times \mathbb{B}$ за који важи:

$$\pi_A \circ f = g, \text{ и } \pi_B \circ f = h.$$

Наравно да се хомоморфизам f задаје са: $f(w) = (g(w), h(w))$ за $w \in C$. Није тешко проверити да се тако добија један хомоморфизам. Суштина овог резултата је у томе да је задавање хомоморфизма у производ еквивалентно задавању хомоморфизма у сваку компоненту. Видећемо касније како то изгледа на конкретним примерима група и хомоморфизама.

Дефиниција 182 Нека је $\mathfrak{M}$ нека класа алгебри. Та класа је

а) затворена у односу на подалгебре уколико важи:

ако $\mathbb{A} \in \mathfrak{M}$ и $\mathbb{B} \leq A$ онда и $\mathbb{B} \in \mathfrak{M}$;

б) затворена у односу на хомоморфне слике уколико важи:

ако је $h: \mathbb{A} \to \mathbb{B}$ хомоморфизам и $\mathbb{A} \in \mathfrak{M}$ онда и $h[\mathbb{A}] \in \mathfrak{M}$;

в) затворена у односу на директне производе уколико важи:

ако за све $i \in I$ $A_i \in \mathfrak{M}$ онда и $\prod_{i \in I} \mathbb{A}_i \in \mathfrak{M}$,

Наведимо сада једну теорему, коју нећемо доказивати, а која карактерише једнакосне класе алгебри (варијетете).

Теорема 183 Нека је $\mathfrak{M}$ нека класа алгебри. Та класа је варијетет ако и само ако је затворена у односу на подалгебре, хомоморфне слике и директне производе.

Пажљив читалац није пропустио да примети да у примеру варијетета нисмо навели класу свих поља. То наравно није случајно, јер

класа свих поља не чини варијетет — директан производ два поља није поље. Наиме, ако су E и F, ма која поља онда у производу $E \times F$ важи:

$$(1_E, 0_F) \cdot (0_E, 1_F) = (0_E, 0_F),$$

те у том производу постоје прави делитељи нуле, а њих нема у пољима. Вратићемо се на ово касније када будемо проучавали прстене и поља.

Пређимо сада на појам *конгруенције*.

Дефиниција 184 Нека је

$$\mathbb{A} = (A, \phi_1, \ldots, \phi_r, a_1, \ldots, a_s)$$

нека алгебра и $\sim$ релација еквиваленције на скупу носачу A. Та релација је конгруенција уколико за све $i = \overline{1,r}$ и све $u_j, v_k \in A$:

$$\text{ако је } u_1 \sim v_1, \ldots u_{n_i}, \sim v_{n_i} \text{ онда је и } \phi_i(u_1, \ldots, u_{n_i}) \sim \phi_i(v_1, \ldots, v_{n_i}).$$

Другим речима, ако при ма којој операцији аргументе заменимо еквивалентним елементима, добијамо резултат еквивалентан почетном. Наведимо неке примере.

Пример 185 Основни пример конгруенције је пример конгруенције по модулу неког природног броја n ($n \geq 2$):

$$a \equiv b \pmod{n} \text{ ако и само ако } n \mid (a - b).$$

Конгруенцију по модулу n често ћемо означавати и са $\equiv_n$, због краткоће записа.

Није тешко проверити да је $\equiv_n$ заиста конгруенција (у горе наведеном смислу) алгебре $\mathbb{Z} = (\mathbf{Z}, +, \cdot)$. Наиме, лако се провери да је то релација еквиваленције. Проверимо да се „слаже са операцијама".

Уколико је $a \equiv_n b$ и $a_1 \equiv_n b_1$, онда $n \mid (a - b)$ и $n \mid (a_1 - b_1)$, тј.

$$a - b = nq \quad \text{и} \quad a_1 - b_1 = nq_1,$$

за неке целе бројеве q, q_1. Тада је

$$(a + a_1) - (b + b_1) = (a - b) + (a_1 - b_1) = nq + nq_1 = n(q + q_1),$$

па је заиста $(a + a_1) \equiv_n (b + b_1)$.

Такође,

$$aa_1 - bb_1 = aa_1 - ba_1 + ba_1 - bb_1 = (a-b)a_1 + b(a_1 - b_1) = nqa_1 + bnq_1 = n(qa_1 + bq_1),$$

те је $ab \equiv_n a_1 b_1$.

Пример 186 Дефинишимо релацију $\sim$ на скупу свих природних бројева са: $a \sim b$ ако и само ако се цифре на месту десетица у декадном запису ових бројева подударају.

На пример, $134 \sim 1235$, јер је 3 на месту десетица и код једног и код другог броја, док $3 \not\sim 13$ пошто у првом броју имамо 0 на месту десетица (која се наравно на пише у случају једноцифрених бројева), а у другом 3. Но, $100 \sim 3$, пошто оба броја имају 0 на месту десетица. Јасно је да је ово једна релација еквиваленције. Но, она није конгруенција структуре $(\mathbf{N}, +, \cdot)$. На пример, $13 \sim 411$ и $258 \sim 52$, али $13 + 258 = 271$, а $411 + 52 = 463$, па $(13 + 258) \not\sim (411 + 52)$.

Као што нам функције које сликају скуп носач једне структуре у скуп носач друге структуре нису посебно интересантне уколико нису и хомоморфизми (јер не поштују структуру), тако нам и произвољне релације еквиваленције на скупу носачу неке алгебре нису нарочито интересантне (јер не поштују структуру). Није неочекивано да постоји важна веза између хомоморфизама и конгруенција. Ево једног веома важног примера конгруенције.

Дефиниција 187 Нека су

$$\mathbb{A} = (A, \phi_1, \ldots, \phi_r, a_1, \ldots, a_s) \quad \text{и} \quad \mathbb{B} = (B, \psi_1, \ldots, \psi_r, b_1, \ldots, b_s)$$

две алгебре исте сигнатуре и $h\colon \mathbb{A} \to \mathbb{B}$ хомоморфизам. Језгро овог хомоморфизма, у ознаци $\mathrm{Ker}(h)$, је конгруенција алгебре $\mathbb{A}$, која се дефинише на следећи начин:

$$(u, v) \in \mathrm{Ker}(h) \overset{\text{def}}{\iff} h(u) = h(v).$$

Ако се присетимо се да се бинарна релација дефинише као скуп уређених парова, онда нам ова дефиниција неће изгледати необично (не би било баш лепо писати $u \,\mathrm{Ker}(h)\, v$, зар не?). Није тешко проверити да је ово заиста конгруенција. Проверу да је ово релација еквиваленције могу читаоци сами лако да изведу (а пошто је лако и могу, онда и треба!), ми ћемо овде проверити слагање са операцијама.

Дакле, нека су $u_j, v_k \in A$ за које важи

$$(u_1, v_1) \in \mathrm{Ker}(h), \ldots, (u_{n_i}, v_{n_i}) \in \mathrm{Ker}(h).$$

Треба показати да

$$(\phi_i(u_1, \ldots, u_{n_i}), \phi_i(v_1, \ldots, v_{n_i})) \in \mathrm{Ker}(h),$$

тј. да је

$$h(\phi_i(u_1, \ldots, u_{n_i})) = h(\phi_i(v_1, \ldots, v_{n_i})).$$

Проверимо то:

$$\begin{aligned} h(\phi_i(u_1, \ldots, u_{n_i})) &= \psi_i(h(u_1), \ldots, h(u_{n_i})) \text{ (јер је } h \text{ хомоморфизам)} \\ &= \psi_i(h(v_1), \ldots, h(u_{v_i})) \text{ (јер } (u_j, v_j) \in \mathrm{Ker}(h) \text{ за све } j) \\ &= h(\phi_i(v_1, \ldots, v_{n_i})) \text{ (јер је } h \text{ хомоморфизам).} \end{aligned}$$

Свака конгруенција на датој алгебри омогућава конструкцију количничке алгебре. Упознајмо се са том важном конструкцијом.

Дефиниција 188 Нека је

$$\mathbb{A} = (A, \phi_1, \ldots, \phi_r, a_1, \ldots, a_s),$$

дата алгебра и $\sim$ конгруенција те алгебре. Ако са $A/_\sim$ означимо скуп свих класа еквиваленције, а са $[u]$ класу класу еквиваленције елемента $u \in A$, онда количничку алгебру ове алгебре по конгруенцији $\sim$, у ознаци $\mathbb{A}/_\sim$, задајемо са:

$$\mathbb{A}/_\sim = (A/_\sim, \Phi_1, \ldots, \Phi_r, [a_1], \ldots, [a_s]),$$

где су операције Φ_i дефинисане са:

$$\Phi_i([u_1], \ldots, [u_{n_i}]) := [\phi_i(u_1, \ldots, u_{n_i})].$$

Морамо проверити добру дефинисаност ових операција. Наиме, морамо проверити следеће:

ако је $[u_1] = [v_1], \ldots, [u_{n_i}] = [v_{n_i}]$ да ли је $[\phi_i(u_1, \ldots, u_{n_i})] = [\phi_i(v_1, \ldots, v_{n_i})]$?

То није тешко проверити и у провери се користи чињеница да је $\sim$ конгруенција. Наиме, ако је $[u_1] = [v_1], \ldots, [u_{n_i}] = [v_{n_i}]$, то заправо значи да је $u_1 \sim v_1, \ldots, u_{n_i} \sim v_{n_i}$. Како је $\sim$ конгруенција, следи да мора бити $\phi_i(u_1, \ldots, u_{n_i}) \sim \phi_i(v_1, \ldots, v_{n_i})$, а то управо значи да је $[\phi_i(u_1, \ldots, u_{n_i})] = [\phi_i(v_1, \ldots, v_{n_i})]$.

Пример 189 На алгебарској структури $\mathbb{Z} = (Z, +, \cdot, 0, 1)$, задата је конгруенција $\equiv_n$, где је $n \geq 2$ природан број. Добијамо количничку структуру $\mathbb{Z}/_{\equiv_n} = (Z/_{\equiv_n}, +, \cdot, [0], [1])$. Овде смо користили исте ознаке за операције на количничкој структури као и на почетној алгебри (а то ћемо често, због једноставности записа, радити и касније). Операције на количничкој структури задате су са:

$$[a] + [b] := [a + b], \quad [a] \cdot [b] := [a \cdot b].$$

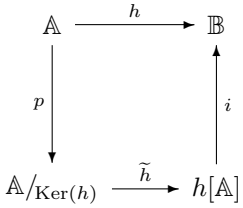
Приметимо да постоји тачно n различитих класа еквиваленције. Наиме, сваки цео број m конгруентан је по модулу n тачно једном од бројева из скупа $\{0, 1, \ldots, n-1\}$. То је јасно из чињенице да се он може записати у облику $m = qn + r$, где су бројеви q и r јединствено задати под условом да је $0 \leq r < n$. Дакле, $\mathbb{Z}/_{\equiv_n} = \{[0], [1], \ldots, [n-1]\}$. Како се сабирају и множе ове класе? Јасно је о чему се ради. Уколико $[s], [t] \in \{[0], [1], \ldots, [n-1]\}$, онда је $[s] + [t]$ она класа из тог скупа, која је једнака класи $[s + t]$. Јасно је да то мора бити класа $[s +_n t]$, јер се збир $s +_n t$ и дефинише као остатак при дељењу $s + t$ са n. Слично

је и $[s] \cdot [t] = [s \cdot_n t]$. Видимо да заправо функција $h\colon Z_n \to \mathbb{Z}/_{\equiv_n}$ задата са: $h(s) := [s]$ остварује изоморфизам структура $\mathbb{Z}_n$ и $\mathbb{Z}/_{\equiv_n}$. Тако смо установили да се све алгебарске структуре $\mathbb{Z}_n$ могу добити (до на изоморфизам) као количничке структуре (при различитим конгруенцијама) алгебарске структуре $\mathbb{Z}$. ♣

Ако је $\mathbb{A}$ нека алгебра и $\sim$ конгруенција те алгебре, на природан начин се дефинише хомоморфизам $p\colon \mathbb{A} \to \mathbb{A}/_\sim$ са: $p(u) := [u]$, где је $u \in A$. Читаоцу остављамо да провери да је p заиста хомоморфизам. С обзиром да је p и „на", зовемо га и канонским епиморфизмом алгебре $\mathbb{A}$ на своју количничку алгебру $\mathbb{A}/_\sim$.

За крај ове лекције наводимо теорему о разлагању (декомпозицији) хомоморфизма.

Теорема 190 Нека су $\mathbb{A}$ и $\mathbb{B}$ алгебре исте сигнатуре и $h\colon \mathbb{A} \to \mathbb{B}$ хомоморфизам алгебри. Тада се хомоморфизам h може разложити у облику следеће композиције: $h = i \circ \widetilde{h} \circ p$, где је i инклузија подалгебре $h[\mathbb{A}]$ у алгебру $\mathbb{B}$, p канонски епиморфизам алгебре $\mathbb{A}$ на своју количничку алгебру $\mathbb{A}/_{\mathrm{Ker}(h)}$, а $\widetilde{h}$ изоморфизам $\widetilde{h}\colon \mathbb{A}/_{\mathrm{Ker}(h)} \to h[\mathbb{A}]$ задат са: $\widetilde{h}([u]) := h(u)$. Дакле, следећи дијаграм комутира.



Доказ. Морамо проверити да ли је $\widetilde{h}$ добро дефинисан и да ли је изоморфизам. Пре свега, нека је $[u] = [v]$. Треба проверити да ли је $\widetilde{h}([u]) = \widetilde{h}([v])$, тј. да ли је $h(u) = h(v)$, но чињеница да је $[u] = [v]$ нам управо даје да $(u, v) \in \mathrm{Ker}(h)$, тј. $h(u) = h(v)$ што се заправо и тражило. Дакле, $\widetilde{h}$ јесте добро дефинисана функција. Јасно је да је $\widetilde{h}$ „на". Проверимо да ли је и „1-1". Претпоставимо да је $\widetilde{h}([u]) = \widetilde{h}([v])$. То значи да је $h(u) = h(v)$, те $(u, v) \in \mathrm{Ker}(h)$, па је заиста $[u] = [v]$. Остаје да проверимо да ли је $\widetilde{h}$ хомоморфизам.

$$\begin{aligned}
\widetilde{h}(\Phi_i([u_1], \ldots, [u_{n_i}]) &= \widetilde{h}([\phi_i(u_1, \ldots, u_{n_i})]) \text{ по дефиницији операције } \Phi_i \\
&= h(\phi_i(u_1, \ldots, u_{n_i})) \text{ по дефиницији функције } \widetilde{h} \\
&= \psi_i(h(u_1), \ldots, h(u_{n_i})) \text{ јер је } h \text{ хомоморфизам} \\
&= \psi_i(\widetilde{h}([u_1]), \ldots, \widetilde{h}([u_{n_i}])) \text{ по дефиницији } \widetilde{h}.
\end{aligned}$$

Дакле, $\widetilde{h}$ је заиста изоморфизам. Покажимо још да дијаграм комутира.

$$(i \circ \widetilde{h} \circ p)(u) = i(\widetilde{h}(p(u)))$$

$$
\begin{aligned}
&= i(\widetilde{h}([u])\\
&= i(h(u))\\
&= h(u).
\end{aligned}
$$

Овде смо наравно користили да је $p(u) = [u]$ и да је $i(v) = v$ за све $v \in h[\mathbb{A}]$, пошто је i инклузија. Овим је доказ завршен. □

Пример 191 Уочимо хомоморфизам $\rho_n\colon \mathbb{Z} \to \mathbb{Z}_n$, где је $\rho_n(m)$ остатак при дељењу m са n. Применити на њега теорему о разлагању хомоморфизма.

Јасно је да је хомоморфизам „на". Из теореме о разлагању хомоморфизма следи да је $\mathbb{Z}/_{\mathrm{Ker}(\rho_n)} \cong \mathbb{Z}_n$. Одредимо $\mathrm{Ker}(\rho_n)$. На основу дефиниције језгра хомоморфизма добијамо да је $(r, s) \in \mathrm{Ker}(\rho_n)$ ако и само ако је $\rho_n(r) = \rho_n(s)$. Другим речима, $(r, s) \in \mathrm{Ker}(\rho_n)$ ако и само ако r и s имају исти остатак при дељењу са n. Покажимо да је то еквивалентно са $r \equiv_n s$.

Пре свега, ако је $r = qn + \rho_n(r)$ и $s = q'n + \rho_n(s)$ и ако је $\rho_n(r) = \rho_n(s)$, онда је $r - s = n(q - q')$ и заиста је $r \equiv_n s$. Обратно, нека је $r \equiv_n s$. Како је јасно да је $r \equiv_n \rho_n(r)$ (зашто?), добијамо, с обзиром да је $\equiv_n$ релација еквиваленције, да је $\rho_n(r) \equiv_n \rho_n(s)$. Но и $\rho_n(r)$ и $\rho_n(s)$ су бројеви из скупа $\{0, \ldots, n-1\}$. Уколико претпоставимо да је нпр. $\rho_n(r) \leq \rho_n(s)$ добићемо да је $0 \leq \rho_n(s) - \rho_n(r) < n$ и да $n \mid (\rho_n(s) - \rho_n(r))$. То је могуће једино ако је $\rho_n(r) = \rho_n(s)$. Дакле, заиста се конгруенција $\mathrm{Ker}(\rho_n)$ поклапа са $\equiv_n$ и из теореме о разлагању хомоморфизма следи да је $\mathbb{Z}/_{\equiv_n} \cong \mathbb{Z}_n$, као што смо већ раније показали. ♣