

Глава 2

Алгебарске структуре

Апстрактна алгебра проучава произвољне скупове и операције дефинисане на тим скуповима. При томе се природа скупова као и самих операција дефинисаних на тим скуповима могу знатно разликовати од скупова бројева и уобичајених операција са бројевима. Без обзира на то, показује се да разне операције у различитим скуповима могу имати низ заједничких својстава.

2.1 Декартов производ скупова

Дефиниција 2.1. *Пар елемената a и b код којег се зна која је компонента (координата) прва, а која друга, назива се уређен пар (двојка) и означава се (a, b) . Уређени парови (a, b) и (c, d) су једнаки ако и само ако је $a = c$ и $b = d$.*

Слично се дефинише уређена тројка (a, b, c) неких елемената a , b и c , као и уређена n -торка (a_1, a_2, \dots, a_n) елемената a_1, a_2, \dots, a_n .

Ако су дати скупови A и B , можемо посматрати уређене парове (a, b) , где је $a \in A$ и $b \in B$.

Дефиниција 2.2. *Скуп $A \times B$ дефинисан са*

$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

назива се Декартов, Картезијев или директан производ скупова A и B .

Слично се дефинише скуп $A \times B \times C$, као и скуп $A_1 \times A_2 \times \dots \times A_n$. Скуп $A \times A$ се означава и са A^2 , а скуп $\underbrace{A \times A \times \dots \times A}_n$ са A^n .

На пример, скуп \mathbb{R}^2 представља координате свих тачака координатне равни, док скуп \mathbb{R}^3 представља координате свих тачака у простору.

ПРИМЕР 2.1. Скуп $[a, b] \times [c, d]$ представља скуп свих уређених парова (x, y) , где је $x \in [a, b]$ и $y \in [c, d]$. Ако су x и y координате тачке у равни, тада скуп $[a, b] \times [c, d]$ одређује правоугаоник у координатној равни са теменима $A(a, c)$, $B(b, c)$, $C(b, d)$ и $D(a, d)$.

2.2 Бинарна операција

Дефиниција 2.3. Пресликавање $*$: $S^2 \rightarrow S$, где је S непразан скуп, је бинарна операција у скупу S .

Уместо $*(a, b) = c$ за $a, b, c \in S$, пише се $a * b = c$. Бинарном операцијом се, дакле, сваком уређеном пару елемената из скупа S додељује један елемент који је такође из S . На пример, на скупу \mathbb{N} су нам познате операције сабирања и множења, при чему се уместо $*$ за те операције користе ознаке $+$ и \cdot . Тако је $+(2, 3) = 2 + 3 = 5$ или $\cdot(2, 3) = 2 \cdot 3 = 6$.

Ако је S коначан скуп, бинарна операција може да се зада навођењем свих парова *оригинал - слика*, што се прегледно може приказати Кејлијевом таблицом.

ПРИМЕР 2.2. Кејлијевим таблицама дефинисане су операције \circ (у скупу $\{1, 2, 3, 4, 5\}$) и $*$ (у скупу $\{a, b, c, d, e\}$).

\circ	1	2	3	4	5
1	2	2	1	1	2
2	2	2	1	1	2
3	1	1	3	3	1
4	1	1	3	3	1
5	2	2	1	1	1

$*$	a	b	c	d	e
a	a	a	a	a	a
b	a	b	b	b	b
c	a	b	c	c	c
d	a	b	c	d	d
e	a	b	c	d	e

Поред бинарних, дефинишу се и n -арне операције као пресликавања $S^n \rightarrow S$. За $n = 1$ операција се зове *унарна*.

Бинарне операције могу да имају разна својства.

Дефиниција 2.4. Операција $*$ у скупу S је *комутативна* ако за свако $a, b \in S$ важи

$$a * b = b * a.$$

Дефиниција 2.5. Операција $*$ у скупу S је *асоцијативна* ако за свако $a, b, c \in S$ важи

$$a * (b * c) = (a * b) * c.$$

За асоцијативну операцију се може писати и $a * b * c$ јер поредак заграда (односно редослед извршавања операција) не утиче на резултат.

2.3 Алгебарске структуре са једном бинарном операцијом

Скуп са једном или више операција чини *алгебарску структуру*.

Дефиниција 2.6. *Ако је $*$ бинарна операција у скупу S , онда се уређен пар $(S, *)$ назива групоид.*

За групоид $(S, *)$ скуп S је његов *домен*. Комутативни групоид је онај групоид чија је операција комутативна. На пример, са доменом \mathbb{N} имамо комутативне групоиде $(\mathbb{N}, +)$, (\mathbb{N}, \cdot) , али и бесконачно много других, као што су: (\mathbb{N}, nzd) , (\mathbb{N}, nzs) , (\mathbb{N}, \max) , (\mathbb{N}, \min) (Ознаке nzd и nzs су уобичајене скраћенице за највећи заједнички делилац и најмањи заједнички садржалац).

Кардиналност групоида је кардиналност његовог домена. У том смислу постоје коначни и бесконачни групоиди.

Дефиниција 2.7. *Групоид са асоцијативном операцијом је асоцијативни групоид, полугрупа или семигрупа.*

На пример, групоид $(\mathbb{N}, +)$ је полугрупа. Групоид $(\mathcal{P}(A), \cup)$, где је $\mathcal{P}(A)$ партитивни скуп скупа A , је такође полугрупа. У полугрупи се дефинише n -ти степен елемента a :

$$a^1 = a, \quad a^n = a * a^{n-1}, \quad n = 2, 3, \dots$$

Због асоцијативности операције $*$ елемент a^n је једнозначно одређен.

У групоиду могу постојати и неки посебни елементи.

Дефиниција 2.8. *За $e \in S$ се каже да је неутрални или јединични елемент (јединица) групоида $(S, *)$ ако за свако $a \in S$ важи*

$$a * e = e * a = a.$$

Дакле, јединични елемент је комутативан са сваким елементом групоида.

Теорема 2.1. *Ако у групоиду постоји јединични елемент, он је јединствен.*

Доказ. Ако претпоставимо да постоје бар два јединична елемента, e_1 и e_2 , тада је $e_1 * e_2 = e_2$ и $e_2 * e_1 = e_1$. Како је $e_1 * e_2 = e_2 * e_1$ (јединични елемент је комутативан са сваким другим елементом), то је $e_1 = e_2$. ■

Дефиниција 2.9. *Ако у групоиду $(S, *)$ постоји неутрални елемент e и ако за елемент $a \in S$ постоји елемент $a^{-1} \in S$, такав да је*

$$a^{-1} * a = a * a^{-1} = e,$$

тада за a^{-1} кажемо да је супротни или инверзни елемент елемента a .

Теорема 2.2. *Ако у полугрупи $(S, *)$ за $a \in S$ постоји инверзни елемент, он је јединствен.*

Доказ. Ако претпоставимо да за a постоје два инверзна елемента, a_1^{-1} и a_2^{-1} , тада је

$$a_1^{-1} = a_1^{-1} * e = a_1^{-1} * (a * a_2^{-1}) = (a_1^{-1} * a) * a_2^{-1} = e * a_2^{-1} = a_2^{-1}. \blacksquare$$

Дефиниција 2.10. *Полугрупа $(S, *)$ је група ако у њој постоји јединични елемент и ако сваки елемент из S има свој инверзни елемент.*

Ако скуп S има n елемената, кажемо да је $(S, *)$ група реда n . Група $(S, *)$ је комутативна или Абелова ако је операција $*$ комутативна.

2.4 Примери група

Постоји велики број разних примера група. Најпознатије су оне које се односе на скупове бројева.

Групе бројева

Алгебарска структура $(\mathbb{Z}, +)$ је група. Заиста, збир било која два цела броја је цео број. Асоцијативност сабирања важи у \mathbb{R} , па и у његовом подскупу \mathbb{Z} . Неутрални елемент је $e = 0$, док је $-a$ супротан (инверзан) елемент елемента $a \in \mathbb{Z}$. Ова група је Абелова.

Уобичајено је да се за групе са операцијом сабирања каже да су адитивне. Примери адитивних група су и: $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$.

За групе са операцијом множења кажемо да су мултипликативне. Примери таквих група су: (\mathbb{Q}^+, \cdot) , (\mathbb{R}^+, \cdot) , $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{C} \setminus \{0\}, \cdot)$.

Групе пермутација

Пермутација скупа $\{1, 2, \dots, n\}$ је бијективно пресликавање тог скупа у самог себе. На пример, пермутација $(3, 2, 5, 1, 4)$ скупа $\{1, 2, 3, 4, 5\}$ је пресликавање p које симболички може да се запише у облику

$$p = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix}.$$

Скуп S_n свих пермутација скупа $\{1, 2, \dots, n\}$ чини групу у односу на композицију пресликавања (пермутација). Неутрални елемент те групе је пермутација у којој се сваки елемент пресликава у самог себе. Дакле, ако је \circ композиција пермутација, тада је (S_n, \circ) група са неутралним

елементом $\begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}$. Датој пермутацији p је инверзна пермутација која је одређена инверзним пресликавањем p^{-1} . На пример, пермутацији $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix}$ групе (S_5, \circ) инверзна пермутација је $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 5 & 3 \end{pmatrix}$.

За формирање Кејлијевих таблица погодно је користити запис пермутације у такозваној цикличној нотацији. На пример, пермутација $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$ се записује као $(13)(45)$, што значи да се 1 пресликава у 3 и 3 у 1, 4 у 5 и 5 у 4, док се 2 пресликава у 2. У овој нотацији је

$$S_3 = \{e, (12), (13), (23), (123), (132)\},$$

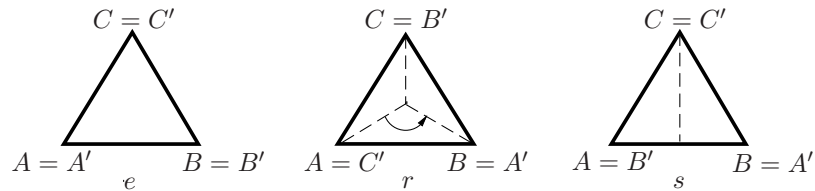
где је e неутрални елемент групе (S_3, \circ) и где (123) означава пермутацију у којој се 1 пресликава у 2, 2 у 3 и 3 у 1. Из Кејлијеве таблице групе (S_3, \circ)

\circ	e	(12)	(13)	(23)	(123)	(132)
e	e	(12)	(13)	(23)	(123)	(132)
(12)	(12)	e	(132)	(123)	(23)	(13)
(13)	(13)	(123)	e	(132)	(12)	(23)
(23)	(23)	(132)	(123)	e	(13)	(12)
(123)	(123)	(13)	(23)	(12)	(132)	e
(132)	(132)	(23)	(12)	(13)	e	(123)

видимо да група није Абелова. Ред ове групе је 6, а у општем случају ред групе (S_n, \circ) је $n!$.

Групе симетрија

Пресликавање геометријске фигуре које чува растојање између тачака назива се *изометријска трансформација* или *изометрија*. Изометрија фигуре у саму себе назива се *симетрија*.

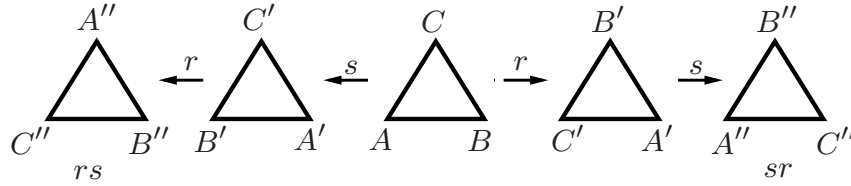


Слика 2.1. Пресликавања e , r и s

За дато $n \geq 3$, групу D_n (групу симетрија) чине све симетрије правилног n -тоугла. Група D_n има $2n$ елемената: $e, r, r^2, \dots, r^{n-1}, s, sr, \dots, sr^{n-1}$, где је e идентичка трансформација, r је ротација око

центра многоугла за $2\pi/n$, док је s осна симетрија. Оса симетрије је било која права одређена центром и неким теменом многоугла ако је n паран број, односно центром и средиштем било које странице многоугла ако је n непаран број. За $n = 3$ група симетрија једнакостраничног троугла ABC има 6 елемената дефинисаних помоћу пресликавања e , r и s (Слика 2.1).

Група D_3 није Абелова јер је, на пример $rs \neq sr$ (Слика 2.2).



Слика 2.2. Пресликавања rs и sr

2.5 Алгебарске структуре са две бинарне операције

Нека је S скуп у којем су дефинисане две бинарне операције: $*$ и \circ .

Дефиниција 2.11. Бинарна операција \circ је дистрибутивна у односу на бинарну операцију $*$ ако је

$$\begin{aligned} a \circ (b * c) &= (a \circ b) * (a \circ c), \\ (a * b) \circ c &= (a \circ c) * (b \circ c) \end{aligned}$$

за свако $a, b, c \in S$.

На пример, операција множења у \mathbb{R} је дистрибутивна у односу на операцију сабирања, док операција сабирања није дистрибутивна у односу на операцију множења?

Дефиниција 2.12. Структура $(S, *, \circ)$ је прстен ако је:

1. $(S, *)$ Абелова група,
2. (S, \circ) је полугрупа,
3. Операција \circ дистрибутивна у односу на операцију $*$.

На пример, $(\mathbb{Z}, +, \cdot)$ је прстен. Често се операције $*$ и \circ у прстену називају 'сабирање' и 'множење', па чак и означавају са $+$ и \cdot . Исто тако, ако за те операције постоје неутрални елементи, они се називају 'нултим' (за операцију $*$) и 'јединичним' (за операцију \circ). Уколико су структуре $(S, *)$ и (S, \circ) групе, онда се оне често називају 'адитивна' и 'мултипликативна' група структуре $(S, *, \circ)$, односно $(S, +, \cdot)$.

Нека је 0 неутрални елемент у односу на операцију $+$ и нека је $-a$ елемент који је инверзан елементу $a \in S$ у односу на исту операцију.

Теорема 2.3. У прстену $(S, +, \cdot)$ важе следећа тврђења.

1. За свако $x \in S$ је $x \cdot 0 = 0 \cdot x = 0$.
2. За свако $x \in S$ и свако $y \in S$ је

$$-(x \cdot y) = (-x) \cdot y = x \cdot (-y).$$

Доказ. 1. На основу својства неутралног елемента 0 и дистрибутивности имамо

$$x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0.$$

Ако левој и десној страни додамо елемент који је супротан елементу $x \cdot 0$, добијамо прву једнакост. На сличан начин се доказује да је и $0 \cdot x = 0$.

2. На основу 1. и дистрибутивности имамо да је

$$0 = 0 \cdot y = (x + (-x)) \cdot y = x \cdot y + (-x) \cdot y.$$

Према томе, елемент $(-x) \cdot y$ је супротан елементу $x \cdot y$. Како је и елемент $-(x \cdot y)$ супротан елементу $x \cdot y$, то значи да важи прва једнакост. Слично се доказује да је и $-(x \cdot y) = x \cdot (-y)$. ■

Прстен $(S, +, \cdot)$ у коме је операција \cdot комутативна назива се *комутативни прстен*. Ако у односу на операцију \cdot постоји неутрални (јединични) елемент, онда је то *прстен са јединицом*. На пример, структура $(\mathbb{Z}, +, \cdot)$ је комутативан прстен са јединицом.

ПРИМЕР 2.3. Нека је \mathcal{P} скуп свих полинома (по x) са реалним коефицијентима и нека је $+$ операција сабирања, а \cdot операција множења полинома. Структура $(\mathcal{P}, +)$ је Абелова група у којој је неутрални (нулти) елемент број (полином) 0. Осим тога, структура (\mathcal{P}, \cdot) је комутативна полугрупа у којој је неутрални (јединични) елемент број (полином) 1. Како је и операција \cdot дистрибутивна у односу на операцију $+$, структура $(\mathcal{P}, +, \cdot)$ је комутативни прстен са јединицом.

Полазећи од алгебарске структуре прстен, можемо дефинисати још неке структуре са две бинарне операције. Нека је структура $(S, *, \circ)$ прстен и нека је e неутрални елемент за операцију $*$.

Дефиниција 2.13. Ако је $(S \setminus \{e\}, \circ)$ група, за прстен $(S, *, \circ)$ кажемо да је тело.

Дефиниција 2.14. Ако је $(S \setminus \{e\}, \circ)$ Абелова група, за прстен $(S, *, \circ)$ кажемо да је поље.

Према Дефиницији 2.13, тело је прстен са јединицом у коме сви елементи осим елемента e имају инверзни елемент у односу на операцију \circ . Ако је у телу операција \circ комутативна, онда је та структура поље. Структуре $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ и $(\mathbb{C}, +, \cdot)$ су примери поља.

Као и код прстена, за операције $*$ и \circ често се користе симболи $+$ и \cdot . Уместо ознаке e за неутрални елемент операције $+$ користи се ознака 0 , док се ознака 1 користи за јединични елемент операције \cdot . Ако је структура $(S, +, \cdot)$ поље и ако је S коначан скуп, тада се та структура назива *коначно поље* или *поље Галоа* (E. Galois је француски математичар - видети 2.7).

2.6 Питања и задаци

Појмови. У овој глави су дефинисани појмови: *уређен пар, Декартов производ, бинарна операција, Кејлијева таблица, комутативна операција, асоцијативна операција, групоид, комутативан групоид, полугрупа, неутрални елемент, инверзни елемент, група, Абелова група, дистрибутивност, прстен, тело, поље*. Неопходно је знати дефиниције свих ових појмова, као и примере у којима се они појављују.

1. Нека скуп S има n елемената. Колико различитих 1) операција; 2) комутативних операција; 3) асоцијативних операција може да се дефинише у скупу S ?

Групоид. У 2.3 видели смо да скуп S са једном бинарном операцијом чини групоид. Проверити да ли је $(S, *)$ групоид значи утврдити да ли $x, y \in S$ за све елементе $x * y \in S$. Групоид са асоцијативном операцијом је полугрупа.

2. Нека је $A = \mathbb{Q} \setminus \{-1\}$ и нека је операција $*$ дефинисана са

$$a * b = a + b + ab$$

за $a, b \in S$. Доказати да је $(A, *)$ групоид који има јединични елемент.

3. Нека је $\mathcal{P}(S)$ партитивни скуп датог скупа $S \neq \emptyset$. Који од групоида $(\mathcal{P}(S), \cup)$, $(\mathcal{P}(S), \cap)$ и $(\mathcal{P}(S), \setminus)$ су комутативни?

4. Нека је $A = \{(a, b, c) \mid a^2 + b^2 + c^2 \neq 0\} \subset \mathbb{R}^3$ и нека је операција $*$ дефинисана са

$$(a, b, c) * (x, y, z) = (ax + bz + cy, az + by + cx, ay + bx + cz).$$

Испитати да ли је $(A, *)$ групоид.

5. Нека је $(A, *)$ комутативни групоид у коме важи

$$(x * y) * z = (z * x) * y.$$

Доказати да је $(A, *)$ полугрупа.

6. У скупу \mathbb{R} дефинисана је операција $*$ са

$$x * y = xy - ax + by$$

где су a и b реални бројеви. Одредити све вредности a, b за које је $(\mathbb{R}, *)$ полугрупа.

Група. Према Дефиницији 2.10 у 2.3 полугрупа $(S, *)$ је *група* ако има јединични елемент и ако сваки елемент из S има инверзни елемент. Ако S има n елемената, кажемо да је група реда n . Група је *комутативна* или *Абелова* ако је операција $*$ комутативна.

7. Нека је $S = \{M, NL, ND, NLK\}$ скуп стројевих наредби са значењима: M - мирно, NL - налево (ротација у леву страну за 90°), ND - надесно (ротација у десну страну за 90°) и NLK - на-лево-круг (ротација у леву страну за 180°) и нека је \circ операција извршавања две узастопне наредбе. Проверити тачност дате Кејлијеве таблице

\circ	M	NL	ND	NLK
M	M	NL	ND	NLK
NL	NL	NLK	M	ND
ND	ND	M	NLK	NL
NLK	NLK	ND	NL	M

а затим испитати да ли је (S, \circ) група.

8. Нека је $2^{\mathbb{Z}} = \{2^m \mid m \in \mathbb{Z}\}$. Доказати да је $(2^{\mathbb{Z}}, \cdot)$ група.

9. Нека је $G = \{x \in \mathbb{R} \mid x \neq 1\}$ и $x * y = xy - x - y + 2$. Доказати да је $(G, *)$ група.

10. Милан, Милица, Зоран и Зорица крећу аутом на пут и при томе се смењују на позицији возача. Доказати да скуп свих пермутација седења у којима су Милан и Милица, односно Зоран и Зорица увек једно поред другог, образује групу. Да ли је та група Абелова?

11. Одредити све групе симетрија 1) квадрата; 2) правилног петоугла; 3) правилног шестоугла.

12. Нека је $S = \{f_1, f_2, f_3, f_4, f_5, f_6\}$, где је

$$f_1(x) = x, \quad f_2(x) = \frac{1}{x}, \quad f_3(x) = 1 - x,$$

$$f_4(x) = \frac{1}{1-x}, \quad f_5(x) = \frac{x-1}{x}, \quad f_6(x) = \frac{x}{x-1}$$

и нека је \circ операција на S дефинисана са $(f \circ g)(x) = f(g(x))$ за $f, g \in S$. Доказати да је (S, \circ) група.

13. На скупу \mathbb{R}^2 дефинисана је операција $*$ са

$$(x, y) * (u, v) = (x + ue^{-y}, y + v)$$

за $(x, y) \in \mathbb{R}^2$ и $(u, v) \in \mathbb{R}^2$. Испитати да ли је $(\mathbb{R}^2, *)$ група.

14. Нека је $A = (-\pi/2, \pi/2)$. На скупу A дефинисана је операција $*$ са

$$a * b = \arctan(\tan a + \tan b), \quad a, b \in A.$$

Доказати да је $(A, *)$ група.

15. Испитати да ли је (A, \star) група ако је

$$A = \{x + y\sqrt{2}; x, y \in \mathbb{Q}, x^2 - 2y^2 = 1\}$$

и $a \star b = ab$ за $a, b \in A$.

16. Нека је $(A, *)$ група. Доказати да за свако $x, y \in A$ важи

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

17. У групи $(A, *)$ за свако $x \in A$ важи $x * x = e$, где је e јединични елемент те групе. Доказати да је $(A, *)$ Абелова група.

18. Нека је $(S, *)$ коначна група. Доказати да за свако $x \in S$ постоји природан број n такав да је $x^n = e$, где је e јединични елемент те групе.

Прстен. У 2.5 видели смо да је прстен алгебарска структура са две бинарне операције (једна је 'сабирање', а друга 'множење') за које важе одређени услови. Из тврђења Теореме 2.3 закључујемо да операције у прстену имају нека својства која су слична својствима сабирања и множења бројева.

19. Нека је $m \in \mathbb{Z}$ и $m\mathbb{Z} = \{ma \mid a \in \mathbb{Z}\}$. Доказати да је $(m\mathbb{Z}, +, \cdot)$ прстен.

20. Нека је $\mathcal{P}(A)$ партитивни скуп скупа A и нека су Δ и \cap редом операције симетричне разлике и пресека скупова. Доказати да је структура $(\mathcal{P}(A), \Delta, \cap)$ комутативни прстен са јединицом (*Булов прстен*).

21. У скупу \mathbb{Z} дефинисане су операције $*$ и \bullet са

$$a * b = a + b + 1, \quad a \bullet b = ab + a + b.$$

Доказати да је $(\mathbb{Z}, *, \bullet)$ прстен.

22. У скупу \mathbb{Z} дефинисане су операције $*$ и \bullet са

$$a * b = a + b - 4, \quad a \bullet b = ab - 4a - 4b + 20.$$

Доказати да је $(\mathbb{Z}, *, \bullet)$ прстен.

23. У скупу \mathbb{Z}^2 дефинисане су операције $*$ и \circ са

$$(a, b) * (c, d) = (a + c, b + d), \quad (a, b) \circ (c, d) = (ac - bd, ad + bc).$$

Испитати да ли је $(\mathbb{Z}^2, *, \circ)$ прстен.

Поље. Из Дефиниције 2.14 следи да је поље структура $(S, *, \circ)$ у којој су $(S, *)$ и $(S \setminus \{e\}, \circ)$ Абелове групе и у којој је операција \circ дистрибутивна у односу на операцију $*$.

24. Нека је $A = \{x + y\sqrt{2} \mid x, y \in \mathbb{Q}\}$. Доказати да је $(A, +, \cdot)$ поље.

25. У скупу рационалних бројева су дефинисане операције $*$ и \circ са

$$a * b = a + b + 1, \quad a \circ b = a + b + ab.$$

Доказати да је $(\mathbb{Q}, *, \circ)$ поље.

26. У скупу реалних бројева дефинисане су операције $*$ и \circ са

$$x * y = x + y - 1, \quad x \circ y = 2xy - 2x - 2y + 3.$$

Доказати да је $(\mathbb{R}, *, \circ)$ поље.

27. Нека је A скуп уређених парова реалних бројева, а $*$ и \circ операције на скупу A дефинисане са

$$(a, b) * (c, d) = (a + c, b + d), \quad (a, b) \circ (c, d) = (ac - 2bd, ad + bc).$$

Доказати да је $(A, *, \circ)$ поље.

28. На скупу \mathbb{R} дефинисане су операције $*$ и \circ са

$$x * y = ax + by - 2, \quad x \circ y = xy - 2x - 2y + 6,$$

где су a и b реални бројеви. Одредити све вредности a, b за које је $(\mathbb{R}, *, \circ)$ поље.

2.7 Додатак

Хомоморфизам и изоморфизам група

Нека је $\mathbb{Z}_n = \{m \mid 1 \leq m \leq n-1, \text{nzd}(m, n) = 1\}$. Тада је $(\mathbb{Z}_n, \cdot_{\text{mod}(n)})$, где је $\cdot_{\text{mod}(n)}$ множење по модулу n , мултипликативна група. Из Кејлијевих таблица за групе $(\mathbb{Z}_8, \cdot_{\text{mod}(8)})$ и $(\mathbb{Z}_{12}, \cdot_{\text{mod}(12)})$

$\cdot_{\text{mod}(8)}$	1	3	5	7	$\cdot_{\text{mod}(12)}$	1	5	7	11
1	1	3	5	7	1	1	5	7	11
3	3	1	7	5	5	5	1	11	7
5	5	7	1	3	7	7	11	1	5
7	7	5	3	1	11	11	7	5	1

видимо да између тих група нема суштинске разлике.

Дефиниција 2.15. Нека су $(A, *)$ и (B, \circ) две групе. Ако постоји пресликавање $f : A \rightarrow B$ такво да је

$$f(x * y) = f(x) \circ f(y)$$

за свако $x, y \in A$, каже се да је f хомоморфизам групе $(A, *)$ на групу (B, \circ) .

ПРИМЕР 2.4. Функција $f : \mathbb{Z} \rightarrow \{-1, 1\}$ дефинисана са

$$f(2a) = 1, \quad f(2a + 1) = -1, \quad (a \in \mathbb{Z})$$

је хомоморфизам групе $(\mathbb{Z}, +)$ на групу $(\{-1, 1\}, \cdot)$.

Дефиниција 2.16. Нека је f хомоморфизам групе $(A, *)$ на групу (B, \circ) . Ако постоји бијекција између скупова A и B , тада се за f каже да је изоморфизам групе $(A, *)$ на групу (B, \circ) .

Обзиром на бијекцију између скупова A и B , у овом случају каже се такође да су групе $(A, *)$ и (B, \circ) изоморфне. За изоморфне групе може постојати више различитих изоморфизама.

ПРИМЕР 2.5. Пресликавање $f : \mathbb{R}^+ \rightarrow \mathbb{R}$ дефинисано са $f(x) = \ln x$ је изоморфизам групе (\mathbb{R}^+, \cdot) на групу $(\mathbb{R}, +)$ јер је

$$f(xy) = \ln(xy) = \ln x + \ln y = f(x) + f(y)$$

за свако $x, y \in \mathbb{R}^+$.

ПРИМЕР 2.6. Групе $(\mathbb{Z}, +)$ и $(2\mathbb{Z}, \cdot)$ (видети задатак 8) су изоморфне.

Важи и следеће тврђење [24].

Теорема 2.4. Сва коначна поља са истим бројем елемената су међусобно изоморфна.

Изоморфизам групе $(A, *)$ на саму себе назива се аутоморфизам те групе. На пример, функција $f : x \mapsto 2x$ је аутоморфизам групе $(\mathbb{R}, +)$.

Историјске напомене

1. Дуго година су се под појмом групе подразумевале групе пермутација. Увођење аксиома групе значило је и потрагу за новим примерима група. Међутим, то није довело до открића суштински нових група јер је свака коначна група изоморфна некој групи пермутација. То је познато као *Кејлијева теорема*.



2. Галоа (Evariste Galois, 1811-1832) је француски математичар који је рођен у малом месту крај Париза и који је већ са 15 година читао Лежандрову књигу *Елементи геометрије* (Eléments de géométrie). Са 17 година Галоа је почео озбиљно да се бави алгебарским једначинама и свој први рад у којем је дошао и до теорије група предао је Кошију. Међутим, није имао среће јер је Коши тај рад изгубио. Са 19

година пише још три рада који стицајем несрећних околности не стижу до рецензената. Своје генијалне идеје Галоа је оставио у тестаменту написаном ноћ уочи двобоја у којем је изгубио живот у 21. години.

3. Абел (Niels Henrik Abel, 1802-1829) је норвешки математичар, познат по томе што је доказао да једначина петог степена није алгебарски решива (не може да се реши помоћу радикала или корена). Међутим, као ни Галоа, тако ни Абел није имао среће са својим резултатима. На пример, Гаус није хтео ни да погледа рад који му је Абел послао. Од последица туберкулозе Абел је умро у 27. години, а његови резултати су касније постали познати. Данас се његово име спомиње у многим теоремама из *теорије редова, интеграла и елиптичких функција*.



Глава 3

Матрице и детерминанте

У многим проблемима и теоријске и примењене математике појављују се величине које могу да се опишу правоугаоном шемом бројева или елемената неког скупа. Теорија матрица омогућава једноставан рад и анализу таквих података, а детерминанте представљају једну специјалну функцију свих података из квадратне шеме.

3.1 Матрице - појам и основне операције

Матрице спадају међу кључне појмове у линеарној алгебри. У општем случају користе се за запис података који зависе од више параметара. Један од таквих примера је запис система линеарних једначина. Сви програмски језици подржавају рад са матрицама. Софтверски пакет за симболичка и нумеричка израчунавања MATLAB је концепцијски заснован на матрицама као базичним објектима.

Појам матрице

Нека је K неко поље (на пример, \mathbb{R} или \mathbb{C}) и нека $a_{ij} \in K$ за $i = 1, \dots, m$ и $j = 1, \dots, n$.

Дефиниција 3.1. *Правоугаона шема (таблица) A од $m \cdot n$ елемената a_{ij} распоређених у облику*

$$\begin{array}{cccc} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{array}$$

је матрица типа $m \times n$ над пољем K . Ако је $K = \mathbb{R}$ матрица је реална, а ако је $K = \mathbb{C}$, матрица је комплексна. За a_{ij} кажемо да су елементи матрице. Пише се и $a_{ij} = (A)_{ij}$.

Матрице се означавају заградама (обичним или угластим) или вертикалним цртама,

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix}$$

или

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

или

$$A = \left\| \begin{array}{cccc} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{array} \right\|.$$

Краће ознаке за матрице су

$$A = (a_{ij})_{m \times n}, \quad A = [a_{ij}]_{m \times n}, \quad A = \|a_{ij}\|_{m \times n}.$$

Елементи $a_{i1}, a_{i2}, \dots, a_{in}$ чине i -ту врсту (ред), а елементи $a_{1j}, a_{2j}, \dots, a_{nj}$ чине j -ту колону (стубац) матрице A . Матрица типа $m \times n$ има m врста и n колона.

ПРИМЕР 3.1. Цена транспорта јединице производа из било које од три фабрике F_1, F_2 и F_3 до било ког од четири складишта S_1, S_2, S_3 и S_4 може прегледно да се представи матрицом типа 3×4 . На пример,

$$\begin{array}{c} S_1 \quad S_2 \quad S_3 \quad S_4 \\ \begin{pmatrix} F_1 & 13 & 12 & 16 & 15 \\ F_2 & 22 & 26 & 12 & 19 \\ F_3 & 17 & 16 & 15 & 11 \end{pmatrix} \end{array}.$$

Специјални случајеви матрица имају посебна имена. Матрица чији су сви елементи једнаки нули назива се *нула матрица* и означава се $O_{m \times n}$ или само са O ако је јасно које су димензије те матрице. Матрица типа $1 \times n$ назива се *матрица врста*, а матрица типа $m \times 1$ назива се *матрица колона* или вектор. Ако је $m = n$, тј.

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix},$$

матрица A је *квадратна матрица* реда n и краће се означава са $A = (a_{ij})_n$. Елементи $a_{11}, a_{22}, \dots, a_{nn}$ чине *главну дијагоналу*, а елементи $a_{1n}, a_{2,n-1}, \dots, a_{n1}$ *споредну дијагоналу* квадратне матрице A . Елементи главне дијагонале називају се *дијагоналним*. Њихов збир зове се *траг матрице* и означава се са $\text{tr} A$. Дакле,

$$\text{tr} A = \sum_{i=1}^n a_{ii}.$$

Дијагоналну матрицу формирану од елемената дијагонале матрице A означавамо са $\text{diag } A$. Квадратна матрица чији су сви елементи ван главне дијагонале једнаки нули, а бар један дијагонални је различит од нуле, назива се *дијагонална матрица*. Дијагонална матрица чији су сви дијагонални елементи међусобно једнаки зове се *скаларна матрица*. Од посебног интереса је скаларна матрица чији су сви дијагонални елементи једнаки јединици у пољу K . Таква матрица се назива *јединична матрица* и означава са I_n или E_n или само са I , односно E ако је јасно ког је реда. У општем случају пише се

$$E = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}.$$

Ако је δ_{ij} Кронекеров симбол, дефинисан са

$$\delta_{ij} = \begin{cases} 1, & i = j, \\ 0, & i \neq j, \end{cases} \quad (3.1)$$

тада је $E_n = I_n = [\delta_{ij}]_n$.

Постоје и друге врсте квадратних матрица као што су *горња троугаона* код које су сви елементи испод главне дијагонале једнаки нули и *доња троугаона* чији су сви елементи изнад главне дијагонале једнаки нули. Дакле, ако је

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & a_{nn} \end{bmatrix} \quad \text{и} \quad B = \begin{bmatrix} a_{11} & 0 & \dots & 0 \\ a_{21} & a_{22} & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix},$$

тада је A горња, а B доња троугаона матрица.

За елемент a_{ij} матрице A кажемо да је на месту (i, j) . За матрице истог типа елементи су *одговарајући* ако су на истом месту.

Дефиниција 3.2. Две матрице су једнаке ако су истог типа и ако су им одговарајући елементи једнаки.

Дефиниција 3.3. Подматрица или субматрица матрице A је матрица која се добија изостављањем неких врста и/или неких колона матрице A .

Матрица типа $m \times n$ има $\binom{m}{p} \cdot \binom{n}{q}$ подматрица типа $p \times q$ за $p \leq m$ и $q \leq n$.

Сабирање и одузимање матрица

Операције сабирања и одузимања матрица дефинишу се за матрице истог типа.

Дефиниција 3.4. Нека је $A = (a_{ij})_{m \times n}$ и $B = (b_{ij})_{m \times n}$. Збир матрица A и B је матрица $C = (c_{ij})_{m \times n}$, где је

$$c_{ij} = a_{ij} + b_{ij}$$

за $i = 1, \dots, m$ и $j = 1, \dots, n$.

ПРИМЕР 3.2. Количине продатих артикала A_1, A_2 и A_3 на продајним местима P_1, P_2, P_3 и P_4 у једном дану дате су матрицом A , а у наредном дану матрицом B :

$$A = \begin{matrix} & \begin{matrix} P_1 & P_2 & P_3 & P_4 \end{matrix} \\ \begin{matrix} A_1 \\ A_2 \\ A_3 \end{matrix} & \begin{pmatrix} 25 & 14 & 13 & 17 \\ 20 & 12 & 15 & 11 \\ 18 & 14 & 16 & 13 \end{pmatrix} \end{matrix}, \quad B = \begin{matrix} & \begin{matrix} P_1 & P_2 & P_3 & P_4 \end{matrix} \\ \begin{matrix} A_1 \\ A_2 \\ A_3 \end{matrix} & \begin{pmatrix} 21 & 17 & 14 & 16 \\ 19 & 16 & 14 & 12 \\ 23 & 18 & 10 & 15 \end{pmatrix} \end{matrix}.$$

Количина продатих артикала у оба дана одговара матрици

$$C = A + B = \begin{pmatrix} 46 & 31 & 27 & 33 \\ 39 & 28 & 29 & 23 \\ 41 & 32 & 26 & 28 \end{pmatrix}.$$

Из дефиниције сабирања матрица директно следи да у скупу S свих матрица типа $m \times n$ важе следећа својства:

1. $A + B = B + A$ (комутативност),
2. $(A + B) + C = A + (B + C)$ (асоцијативност),
3. $A + O = O + A = A$,
4. $A + (-A) = (-A) + A = O$, где је $-A = (-a_{ij})$.

Теорема 3.1. *Ако је S скуп свих матрица истог типа, тада је структура $(S, +)$ Абелова група.*

Доказ. Збир две матрице је матрица истог типа, сабирање је асоцијативно и комутативно, нула матрица је неутрални елемент, а за матрицу $A \in S$ инверзни елемент је *супротна матрица* $-A$. Према томе, испуњени су сви услови за Абелову групу. ■

Егзистенција супотног елемента у односу на сабирање омогућава увођење операције одузимања матрица у скупу S .

Дефиниција 3.5. *Нека је $A = (a_{ij})_{m \times n}$ и $B = (b_{ij})_{m \times n}$. Разлика матрица A и B , у ознаци $A - B$, је матрица C дата са*

$$C = A + (-B).$$

Множење матрице скаларом

Елементе λ, μ, \dots поља K зовео *скалари*.

Дефиниција 3.6. *Производ матрице $A = (a_{ij})_{m \times n}$ и скалара λ је матрица $B = (b_{ij})_{m \times n}$, где је $b_{ij} = \lambda a_{ij}$ за $i = 1, \dots, m$ и $j = 1, \dots, n$.*

За производ скалара λ и матрице A користимо ознаку $\lambda \cdot A$ или λA . Очигледно да је $0 \cdot A = O$ и $(-1) \cdot A = -A$.

Теорема 3.2. *Ако су A и B матрице истог типа, а λ и μ скалари, тада важи:*

1. $1 \cdot A = A$,
2. $(\lambda\mu)A = \lambda(\mu A)$,
3. $(\lambda + \mu)A = \lambda A + \mu A$,
4. $\lambda(A + B) = \lambda A + \lambda B$.

Доказ. Све наведене особине непосредно произилазе из одговарајућих особина операција сабирања и множења у пољу K . ■

Множење матрица

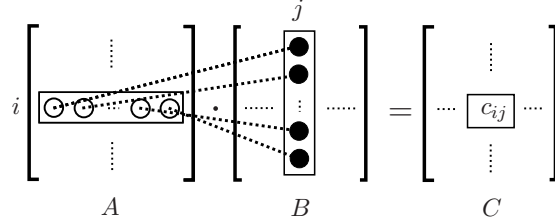
Производ матрица A и B дефинише се само ако су оне *сагласне*, односно ако је број колона матрице A једнак броју врста матрице B .

Дефиниција 3.7. *За сагласне матрице $A = (a_{ij})_{l \times m}$ и $B = (b_{ij})_{m \times n}$ производ $A \cdot B$ је матрица $C = (c_{ij})_{l \times n}$, где је*

$$c_{ij} = \sum_{k=1}^m a_{ik} b_{kj}$$

за $i = 1, \dots, l$ и $j = 1, \dots, n$.

Елемент c_{ij} је збир производа елемената i -те врсте матрице A и одговарајућих елемената j -те колоне матрице B . Због тога се каже да је он добијен множењем i -те врсте матрице A са j -том колоном матрице B . На Слици 3.1 приказана је шема рачунања елемента c_{ij} .



Слика 3.1. $c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \dots + a_{im}b_{mj}$

ПРИМЕР 3.3.

$$\begin{bmatrix} 2 & -1 & 3 & 0 \\ 1 & -2 & 4 & 1 \\ 0 & 3 & 5 & -1 \end{bmatrix} \cdot \begin{bmatrix} 4 & -3 \\ 1 & 2 \\ 0 & 3 \\ -1 & 1 \end{bmatrix} = \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \\ c_{31} & c_{32} \end{bmatrix},$$

где је

$$\begin{aligned} c_{11} &= 2 \cdot 4 + (-1) \cdot 1 + 3 \cdot 0 + 0 \cdot (-1) = 7 \\ c_{12} &= 2 \cdot (-3) + (-1) \cdot 2 + 3 \cdot 3 + 0 \cdot 1 = 1 \\ c_{21} &= 1 \cdot 4 + (-2) \cdot 1 + 4 \cdot 0 + 1 \cdot (-1) = 1 \\ c_{22} &= 1 \cdot (-3) + (-2) \cdot 2 + 4 \cdot 3 + 1 \cdot 1 = 6 \\ c_{31} &= 0 \cdot 4 + 3 \cdot 1 + 5 \cdot 0 + (-1) \cdot (-1) = 4 \\ c_{32} &= 0 \cdot (-3) + 3 \cdot 2 + 5 \cdot 3 + (-1) \cdot 1 = 20. \end{aligned}$$

ПРИМЕР 3.4. У складишту S_1 налази се 10 комада артикла A_1 , 7 комада артикла A_2 и 5 комада артикла A_3 , док складишта S_2 и S_3 садрже редом 6, 8 и 10, односно 4, 7 и 9 комада тих артикала. Ако је цена првог артикла 120 динара, другог 80, а трећег 180, колика је укупна вредност ускладиштених артикала у односу на свако складиште појединачно?

Решење. Стање залиха можемо приказати матрицом A , а цене артикала матрицом B , где је

$$A = \begin{bmatrix} 10 & 7 & 5 \\ 6 & 8 & 10 \\ 4 & 7 & 9 \end{bmatrix}, \quad B = \begin{bmatrix} 120 \\ 80 \\ 180 \end{bmatrix}.$$

Укупна вредност ускладиштених производа по складиштима S_1 , S_2 и S_3 одређена је елементима матрице

$$C = AB = \begin{bmatrix} 10 & 7 & 5 \\ 6 & 8 & 10 \\ 4 & 7 & 9 \end{bmatrix} \cdot \begin{bmatrix} 120 \\ 80 \\ 180 \end{bmatrix} = \begin{bmatrix} 2660 \\ 3160 \\ 2660 \end{bmatrix}.$$

Матрицу A типа $m \times n$ је могуће помножити матрицом B са леве и са десне стране само ако је B матрица типа $n \times m$. У том случају дефинисани су производи AB и BA . Ови производи су увек дефинисани за квадратне матрице истог типа.

ПРИМЕР 3.5. Ако је $A = \begin{bmatrix} 3 & 2 \\ 1 & 4 \end{bmatrix}$ и $B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, тада је

$$AB = \begin{bmatrix} 3 & 2 \\ 1 & 4 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 3 & 5 \\ 1 & 5 \end{bmatrix},$$

$$BA = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 3 & 2 \\ 1 & 4 \end{bmatrix} = \begin{bmatrix} 4 & 6 \\ 1 & 4 \end{bmatrix}.$$

Претходни пример указује да операција множења матрица није комутативна. Уколико за неке матрице A и B важи $AB = BA$, тада кажемо да оне *комутирају*, односно да су *комутативне*.

Својства операције множења матрица дата су у наредној теореме.

Теорема 3.3. Ако је A матрица типа $m \times n$, тада уз претпоставку сагласности матрица важи:

1. $(A \cdot B) \cdot C = A \cdot (B \cdot C)$ (асоцијативност),
2. $A \cdot (B + C) = A \cdot B + A \cdot C$ (дистрибутивност),
3. $A \cdot E_n = E_m \cdot A = A$.

Доказ. Доказ особине 1. дат је у Додатку, особина 2. једноставно следи из дистрибутивности множења у односу на сабирање реалних бројева, док особина 3. следи директно из дефиниције множења матрица. ■

Из ове теореме и својстава сабирања матрица следи тврђење.

Теорема 3.4. Скуп свих квадратних матрица истог реда са операцијама сабирања и множења матрица је прстен са јединицом.

Степен матрице

У скупу квадратних матрица дефинише се и степен матрице.

Дефиниција 3.8. Ако је A квадратна матрица, тада је

$$A^0 = E, \quad A^1 = A, \quad A^n = A^{n-1} \cdot A$$

за $n = 2, 3, \dots$

Теорема 3.5. *Ако је A квадратна матрица, а m и n природни бројеви, тада је*

1. $A^m \cdot A^n = A^{m+n}$,
2. $(A^m)^n = A^{mn}$.

Доказ. Доказ својства 1. се изводи методом математичке индукције по, на пример, n . Из дефиниције степена следи да је

$$A^m \cdot A^1 = A^m \cdot A = A^{m+1},$$

па тврђење важи за $n = 1$. Из претпоставке да тврђење важи за n , односно да је

$$A^m \cdot A^n = A^{m+n}$$

следи да је

$$\begin{aligned} A^m \cdot A^{n+1} &= A^m \cdot (A^n \cdot A) \\ &= (A^m \cdot A^n) \cdot A \\ &= A^{m+n} \cdot A \\ &= A^{m+n+1}, \end{aligned}$$

па тврђење важи и за $n + 1$. Слично се доказује и својство 2. ■

ПРИМЕР 3.6. *За матрицу $A = \begin{bmatrix} 2 & -4 \\ 1 & -2 \end{bmatrix}$ је $A^2 = O$, иако је $A \neq O$. Наравно, аналоган пример не постоји у скупу \mathbb{R} .*

ПРИМЕР 3.7. *Доказати да је $\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}^n = \begin{bmatrix} 1 & na \\ 0 & 1 \end{bmatrix}$, где је a реалан број, а n природан број.*

Решење. *За $n = 1$ тврђење је очигледно тачно. Из претпоставке да је тврђење тачно за неко $n \in \mathbb{N}$ следи*

$$\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}^{n+1} = \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix}^n \cdot \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & na \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & (n+1)a \\ 0 & 1 \end{bmatrix},$$

што значи да је тачно и за $n + 1$. На основу принципа математичке индукције тврђење је тачно за свако $n \in \mathbb{N}$.

Транспоноване матрице

Операција транспонованја је пример унарне операције у скупу матрица.

Дефиниција 3.9. Матрицу A^T добијену из матрице A заменом врста одговарајућим колонама називамо транспонованом матрицом дате матрице A .

За $A = (a_{ij})_{m \times n}$ имамо да је $A^T = (a_{ji})_{n \times m}$.

Теорема 3.6. Операција транспонованја матрица има следећа својства:

1. $(A^T)^T = A$;
2. $(\lambda A)^T = \lambda A^T$;
3. $(A + B)^T = A^T + B^T$;
4. $(AB)^T = B^T A^T$.

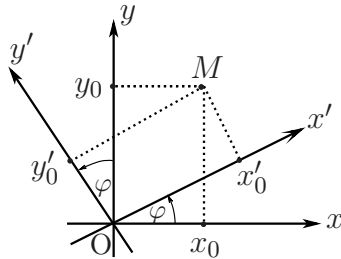
Доказ. Сва тврђења теореме следе из дефиниције транспоноване матрице и својстава одговарајућих операција. ■

У разним применама матричног рачуна сусрећу се квадратне матрице које имају посебна својства у односу на степеновање и транспоноване.

Дефиниција 3.10. Квадратна матрица A је симетрична ако је $A^T = A$, косиметрична ако је $A^T = -A$, ортогонална ако је $A^T A = E$, нилпотентна ако је $A^m = O$ за неко $m \in \mathbb{N}$, идемпотентна ако је $A^2 = A$, а инволутивна ако је $A^2 = E$.

ПРИМЕР 3.8. Матрица $A = \begin{bmatrix} \cos \varphi & \sin \varphi \\ -\sin \varphi & \cos \varphi \end{bmatrix}$ је ортогонална јер је $A^T A = E$.

Нека су x_0 и y_0 координате тачке M у правоуглом координатном систему xOy , а x'_0 и y'_0 координате те исте тачке у координатном систему $x'Oy'$ који је добијен ротацијом координатног система xOy за угао φ (Слика 3.2). Може се доказати да је $\begin{bmatrix} x'_0 \\ y'_0 \end{bmatrix} = A \cdot \begin{bmatrix} x_0 \\ y_0 \end{bmatrix}$.



Слика 3.2. Ротација координатног система