I Скупови, функције, релације и операције

А) Скупови

Скуп се одређује као укупност неких елемената као целине, а за елементе није битан поредак. Скуп је основни математички појам који се не дефинише.

Пр. 1. $A = \{1, 2, 3\}$ $B = \{1, 2, \ldots, 100\}$

$C = \{2, 4, \ldots, 2k, \ldots\} = 2\mathbb{N}$ → набрајање

$C = \{2k \mid k \in \mathbb{N}\}$ → конструкција

Скупови се могу одредити аксиоматски.
Проширење појма скупа је **мултискуп**, где се евидентира понављање, а редослед није битан.

$\{9, 10, 9, 10\} \neq \{9, 10\}$ → једнакост важи у смислу скупова, али не и у смислу мулти-скупова

мултискуп оцена

колекција - други назив за мултискуп

Основне ознаке и примери:

Навођење: набрајање, конструкција, аксиоме
$\emptyset$, $\{\}$ - празан скуп
$\in$ - припадност
$\subset$ - подскуп

$\emptyset$ - празан скуп ($\{\}$)

$\mathbb{N} \subset \mathbb{N}_0 \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ → основни бројевни скупови

Полазна релација је **релација припадности** ($\in$) којом одређујемо да ли неки елемент припада скупу.

$\subset$ → релација бити подскуп између скупова

Пр. 2. $A = \{a, b, c, \{d\}, \{e, f\}\}$

$a \in A$, $b \in A$, $c \in A$, $d \notin A$, $\{d\} \in A$,

$\{a, b\} \notin A$

$a \not\subset A$, $\{a\} \subset A$, $\{\{a\}\} \not\subset A$, $\{a, b\} \subset A$, $\{a, \{d\}\} \subset A$

Подскуп B скупа A јесте скуп B чији сваки елемент припада скупу A.

Партитивни скуп скупа A ($P(A)$) је скуп свих подскупова скупа A.

партитивни скуп $|P(A)| = 2^n$
кардинални број скупа
уређени пар:
$(a,b) \overset{def.}{=} \{\{a\},\{a,b\}\}$

Пр. 3. $A = \{a, b\}$

$P(A) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$

Број елемената партитивног скупа од скупа $A = \{a_1, a_2, \dots, a_n\}$ са n елемената износи $|P(A)| = 2^n$.

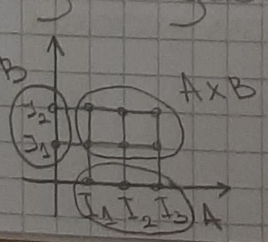
За коначан скуп X користимо ознаку броја елемената $|X|$ (**кардинални број скупа**).

Деф. **Уређени пар** (a,b) је скуп од два елемента уређена поретком, прецизно $(a,b) \overset{def.}{=} \{\{a\},\{a,b\}\}$.

основна особина: $(a,b) = (c,d) \Leftrightarrow a = c \wedge b = d$

Уређена n-торка $(a_1, \dots, a_n)$ је проширење појма уређеног пара.

Деф. **Декартов производ** скупова (**директан** производ скупова) је скуп $A \times B = \{(a,b) \mid a \in A \wedge b \in B\}$.



Пр. 4. $A \times B = \{(i_1, j_1), (i_1, j_2), (i_2, j_1), (i_2, j_2), (i_3, j_1), (i_3, j_2)\}$

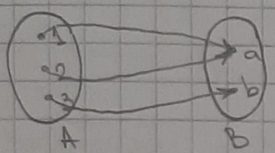
Специјално, ако $B=A$, добијамо $A^2 = A \times A = \{(a_1, a_2) \mid a_1 \in A \land a_2 \in A\}$.

$A^n = A^{n-1} \times A$; $A^1 = A$

Слично се разматра A^3 – скуп уређених тројки са елементима из скупа A, односно A^n – скуп уређених n-торки са елементима из скупа A.

Б) Функције

Пр. 5. Функције над дискретним скуповима



$f: A \to B$

елементарне ф-је над $\mathbb{R}$:

$y=x$, $y=x^2$, $y=ax^2+bx+c$ $(a\neq 0)$,
$y=kx+n$, $y=\sqrt{x}$, $y=x^\alpha$, $y=a^x$, $y=e^x$,
$y=\log_a x$, $y=\ln x$, $y=\sin x$, $y=\cos x$,
$y=tg\,x$, $y=ctg\,x$, ...

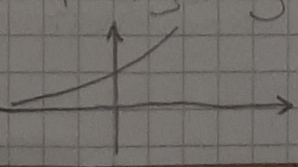
Деф. Функција $f: X \to Y$ скупа X у скуп Y јесте подскуп Декартовог производа $(f \subseteq X \times Y)$ са особинама да за сваки уређени пар $(x,y) \in f$ важи:

1. скуп првих компоненти x одређује домен као цео скуп X
2. ако важи $(x,y) \in f$ и $(x,z) \in f$ тада $y=z$.

Уобичајено је уместо $(x,y) \in f$ писати $y=f(x)$ тако да 1) и 2) можемо одредити и овако:

1. за свако $x \in X$ постоји слика $y=f(x)$
2. ако $y=f(x)$ и $z=f(x)$, онда $y=z$.

Пр. 6. $y=e^x: \mathbb{R} \to \mathbb{R}$



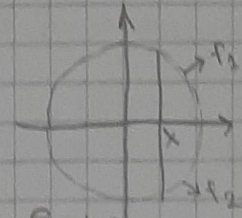
1. За свако x из домена постоји тачно једно $y=e^x$

2. За једно x постоји тачно једно y

Пр. 7. Да ли са овом везом $x^2+y^2=1$ јесте одређена функција $y=f(x)$ када слика $y=f(x):[-1,1]\to\mathbb{R}$?

$y=\pm\sqrt{1-x^2}$

$$f_{1,2}(x)=\begin{cases} f_1(x)=\sqrt{1-x^2} \\ f_2(x)=-\sqrt{1-x^2}\end{cases}$$



није функција него пресликавање

Деф. 3 За функцију $f: X\to Y$ користимо називе X - домен и Y - кодомен. Притом, $y=f(x)$ називамо правилом придруживања.

Т1 Функције $f_1: X_1\to Y_1$ и $f_2: X_2\to Y_2$ су једнаке ако и само ако (акко):

$X_1=X_2 \wedge Y_1=Y_2 \wedge (\forall x\in X_1)\ f_1(x)=f_2(x)$.

На овај начин функција се одређује као уређена тројка домена, кодомена и правила придруживања.

Пр. 8. $y=f_1(x)=\ln e^x:\mathbb{R}\to\mathbb{R}$ и $y=f_2(x)=x:\mathbb{R}\to\mathbb{R}$ су једнаке

функције $y=f_1(x)=e^{\ln x}:\mathbb{R}^+\to\mathbb{R}$ и $y=f_2(x)=x:\mathbb{R}\to\mathbb{R}$ нису једнаке

функције $y=f_1(x)=x\sqrt{x-1}:[1,+\infty)\to\mathbb{R}$ и $y=f_2(x)=x\sqrt{x-1}:\mathbb{R}\to\mathbb{C}$ нису једнаке

„1-1" и „на" функције

Деф. Функција $y=f(x): X\to Y$ је 1-1 (инјективна) ако се различитим оригиналима сликају у различчије слике.

1-1

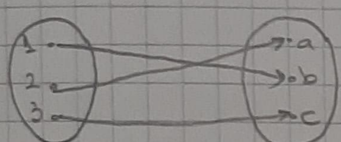
није 1-1

Деф. Функција је **на (сурјекција)** ако сваки елемент кодомена јесте слика неког оригинала.

на

није на

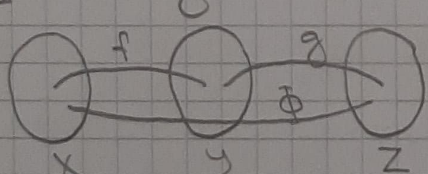
Деф. Функција је 1-1 и на **(бијекција)** уколико је и 1-1 и на функција ($1 \overset{на}{-} 1$).



$1 \overset{на}{-} 1$

Деф. За дате функције $f: X \to Y$ и $g: Y \to Z$, **композиција функција** f и g је функција $\Phi = g \circ f: X \to Z$ са правилом придруживања

$\Phi(x) = (g \circ f)(x) = g(f(x))$.



Т2 Нека су дате функције $f: X \to Y$, $g: Y \to Z$, $h: Z \to W$, тада важи закон асоцијативности $(h \circ g) \circ f = h \circ (g \circ f)$.

Пр. 9. $((\sin \circ \exp) \circ \cos)(x) = (\sin \circ (\exp \circ \cos))(x) =$

$= \sin(e^{\cos x})$ $\quad (\sin \exp)(\cos x) \quad$ $\sin(e^{\cos x})$

Деф. Функција $i: X \to X$ дефинисана са правилом придруживања $i(x) = x$ назива се **идентичка ф-ја**.

Деф. За функцију $f: X \to Y$ ако постоји функција $\varphi: Y \to X$ таква да $\varphi \circ f = i$, тада кажемо да $\varphi = f^{-1}$ **инверзна функција**

Т3 Ако је $f: X \xrightarrow[1-1]{на} Y$ бијекција, тада постоји инверзна функција $f^{-1}: Y \to X$.

В) Искази

Деф. У математици под исказом подразумевамо тврђење за које се зна тачно јединствено одређена истинитосна вредност.

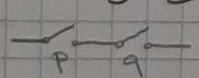
$J(I) = \top$ – тачно

$J(I) = \bot$ – нетачно

Искази се означавају $p, q, r, \dots$ Помоћу исказа формирамо нове исказе користећи таблице

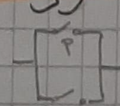
p	q	$p \wedge q$
$\top$	$\top$	$\top$
$\top$	$\bot$	$\bot$
$\bot$	$\top$	$\bot$
$\bot$	$\bot$	$\bot$

конјункција



p	q	$p \vee q$
$\top$	$\top$	$\top$
$\top$	$\bot$	$\top$
$\bot$	$\top$	$\top$
$\bot$	$\bot$	$\bot$

дисјункција



p	q	$p \Rightarrow q$
$\top$	$\top$	$\top$
$\top$	$\bot$	$\bot$
$\bot$	$\top$	$\top$
$\bot$	$\bot$	$\top$

импликација

p	q	$p \Leftrightarrow q$
$\top$	$\top$	$\top$
$\top$	$\bot$	$\bot$
$\bot$	$\top$	$\bot$
$\bot$	$\bot$	$\top$

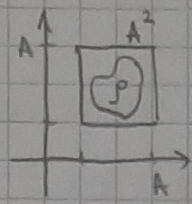
еквиваленција

p	$\neg p$
$\top$	$\bot$
$\bot$	$\top$

негација

Г) Бинарне релације

Деф. Бинарна релација ρ скупа A се одређује као подскуп $\rho \subseteq A^2$.



За уређени пар $(x,y) \in A^2$ уводимо ознаку $x\rho y$ или $(x,y) \in \rho$ ако $x\rho y = \top$. $\neg x\rho y$ ($(x,y) \notin \rho$) ако $x\rho y = \bot$.

Типови бинарних релација:

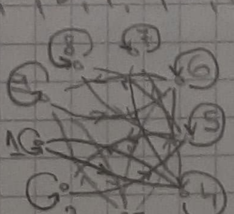
1. бинарна релација ρ скупа A је **рефлексивна** (R) ако важи $x\rho x$ за свако x из A
2. **симетрична** (S) ако важи $x\rho y \Rightarrow y\rho x$ за $(\forall x,y \in A)$
3. **антисиметрична** (AS) ако важи $x\rho y \wedge y\rho x \Rightarrow x=y$ $(\forall x,y \in A)$
4. **транзитивна** (T) ако важи $(\forall x,y,z \in A)$ $x\rho y \wedge y\rho z \Rightarrow x\rho z$.

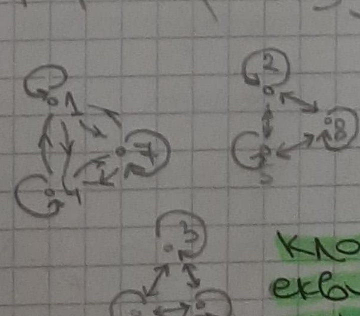
Деф. Релација **еквиваленције** релација ρ скупа A јесте ако је рефлексивна, симетрична и транзитивна.

Деф. Релација **поретка** ако је рефлексивна, антисиметрична и транзитивна.

Пр. 10. За скуп $A=\{1,2,3,4,5,6,7,8,9\}$ и релацију $x\rho y \Leftrightarrow x \equiv y \pmod 3$

$3 \mid y-x$





Класе еквиваленције

Увек је могуће релацију еквиваленције поделити на

класе еквиваленције
1. ако сваког чвора постоји петља
2. ако стрелица иде од x ка y мора и да се врати
3. други начин записивања антисиметричности
$x \rho y \land x \neq y \Rightarrow \neg y \rho x$ (нема пута повратка)

П) Квантификатори

Ако је $P(x)$ унарна релација скупа A, тада уводимо квантификаторе $\forall$ и $\exists$:
1. $(\forall x) P(x)$ - универзални квантификатор
   $J((\forall x) P(x)) = T$ акко за свако $x \in A$ важи $J(P(x)) = T$.
2. $(\exists x) P(x)$ - егзистенцијални квантификатор
   $J((\exists x) P(x)) = T$ акко за неко $x \in A$ важи $J(P(x)) = T$.

Пр. 1. За скуп $A = \mathbb{N}$ посматрајмо унарни предикат $P(x) = 2 | x$ (x је паран број). Тада важи $(\exists x) P(x)$ да важи (нпр. 2). Притом, није за свако x $P(x)$ (нису сви парни).

За скуп $A = \mathbb{R}$ посматрајмо унарни предикат $P(x) \to x^2 + 1 > 0$. Тада важи $(\forall x) P(x)$.

Написати све типове релација помоћу квантификатора:
ρ је R ако $(\forall x)\, x \rho x$
ρ је S ако $(\forall x)(\forall y)\, x \rho y \Rightarrow y \rho x$
ρ је AS ако $(\forall x)(\forall y)\, x \rho y \land y \rho x \Rightarrow x = y$

ρ је T ако $(\forall x)(\forall y)(\forall z)\ x\rho y \wedge y\rho z \Rightarrow x\rho z$.

Б) Алгебарске структуре са једном бинарном операцијом

Деф. Бинарна операција $\circ$ скупа A се одређује као ф-ја $\circ : A^2 \to A$. (уопштење: $A^n \to A$ - n-арна)

Пр. 12. За $A = \mathbb{R}$: $x+y : \mathbb{R}^2 \to \mathbb{R}$,
$x-y : \mathbb{R}^2 \to \mathbb{R}$,
$x \cdot y : \mathbb{R}^2 \to \mathbb{R}$.

Деф. Уређени пар $(A,\circ)$ називамо групоид. Користимо и ознаку $\mathcal{A} = (A,\circ)$.

Пр. 13. Примери групоида

1) $(A,\circ)$ са коначним скупом $A = \{0,1,2,3\}$ при чему је операција дата Кејлијевом таблицом.

$\circ$	0	1	2	3
0	0	1	2	3
1	2	2	1	1
2	0	1	3	2
3	3	2	1	0

Битно је да су сви резултати у A.

→ пример коначног групоида

2) $(\mathbb{Z},+)$ је групоид са бесконачно много елемената ($A = \mathbb{Z}$).

Деф. Групоиди $(G,\circ)$ и $(H,\cdot)$ су изоморфни ако постоји бијекција $f : G \xrightarrow[\text{на}]{1-1} H$ таква да $(\forall x,y \in G)\ f(x\circ y) = f(x)\cdot f(y)$.

Пр. 14. Групоиди датих таблица су изоморфни

∘	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	a	b	c	d
a	a	b	c	d
b	b	d	a	c
c	c	a	d	b
d	d	c	b	a

$\leftrightarrow$

∘	0	1	3	2
0	0	1	3	2
1	1	2	0	3
3	3	0	2	1
2	2	3	1	0

пренумерација и замена места

доказ: $f\begin{pmatrix} 0 & 1 & 2 & 3 \\ a & b & c & d \end{pmatrix}$

$f: \{0,1,2,3\} \xrightarrow[\text{на}]{1-1} \{a,b,c,d\}$ и при том важи

$(\forall x,y)\ f(x\circ y) = f(x)\cdot f(y)$ провером свих могућности

$f(2\circ 3) \overset{?}{=} f(2)\cdot f(3)$

$f(1) \overset{?}{=} d\cdot c = b$ што важи у f

Два елемента групоида $(A,\circ)$ су пермутабилни елементи ако важи $x\circ y = y\circ x$.

Деф. Групоид $(A,\circ)$ је комутативан групоид ако су сви елементи пермутабилни.

Други начин деф. Групоид је комутативан ако важи закон комутативности: $(\forall x,y)\ x\circ y = y\circ x$.

Деф. Групоид $(A,\circ)$ одређује семигрупу (полугрупу) ако важи закон асоцијативности

$(\forall x,y,z)\ (x\circ y)\circ z = x\circ(y\circ z)$.

Комутативност и асоцијативност су два алгебарска закона који не зависе један од другог.

У семигрупи се уводи појам степеновања:

$a^m = a^{m-1}\circ a$ и притом $a^1 = a$, $a\in A$, $m\in \mathbb{N}$.

Приметимо да у семигрупи $(A,\circ)$ није битан редослед рачунања $(a^m = ((\ldots((a\circ a)\circ a)\ldots)\circ a))$, јер нам асоцијативност обезбеђује истоветност резултата.

Деф. Ако у групоиду $(A, \circ)$ постоји елемент $e_L \in A$ такав да $(\forall a \in A)\ e_L \circ a = a$ тада је e_L леви неутрални елемент.

Деф. Ако у групоиду $(A, \circ)$ постоји елемент $e_D \in A$ такав да $(\forall a \in A)\ a \circ e_D = a$ тада је e_D десни неутрални елемент.

Деф. Ако у групоиду $(A, \circ)$ постоји елемент $e \in A$ такав да $(\forall a \in A)\ e \circ a = a \circ e = a$, тада је e неутрални елемент.

Семигрупа $(A, \circ)$ са неутралним елементом се назива моноид.

Моноид је одређен са 3 ствари:

1) операција је унутрашња
2) операција је асоцијативна
3) постоји неутрални елемент.

(Т) Ако у семигрупи постоји леви и десни неутрал, они су једнаки.

Доказ: $e_L \circ e_D = e_D$ јер је e_L леви неутрал
$e_L \circ e_D = e_L$ јер је e_D десни неутрал $\Big|\ e_L = e_D$

(Т) Ако у групоиду постоји неутрални елемент, он је јединствен.

Доказ: $a \circ e_1 = e_1 \circ a = a$

$a \circ e_2 = e_2 \circ a = a$

$e_1 = e_2 \circ e_1 = e_1 \circ e_2 = e_2$

Пр. 15. $(\mathbb{N}, +)$ није моноид, а $(\mathbb{Z}, +)$ јесте.

У моноидима је дозвољена дефиниција **нултог степена**: $a^0 = e$.

Деф. Нека је $(A, \circ)$ моноид са неутралним елементом e. Ако за свако $a \in A$ постоји елемент $a'_L \in A$ тако да важи $a'_L \circ a = e$ тада је a'_L **леви инверзни елемент** за елемент a. Ако $(\forall a \in A)(\exists a'_D)\ a \circ a'_D = e$ тада је a'_D **десни инверзни елемент**. Ако у моноиду $(A, \circ)$ са неутралом e за сваки елемент $a \in A$ постоји $a' \in A$ тако да $a' \circ a = a \circ a' = e$, тада a' називамо **инверзни елемент**.

Т Ако постоје леви и десни инверзни елемент у моноиду, они су **једнаки**.

Доказ: Нека је e неутрал у моноиду $(A, \circ)$ и нека су a'_L и a'_D леви и десни инверз елемента a

$$a'_L \circ a = e$$

$$a \circ a'_D = e$$

$$a'_L = a'_L \circ e = a'_L \circ (a \circ a'_D) = (a'_L \circ a) \circ a'_D = e \circ a'_D = a'_D$$

Доказати да у моноиду ако постоји инверзни елемент да је он **јединствен**.

Доказ: ПНС: постоје два инверзна елемента a' и a''

$$a \circ a' = a' \circ a = e$$

$$a \circ a'' = a'' \circ a = e$$

$$a' = a' \circ e = a' \circ (a \circ a'') = (a' \circ a) \circ a'' = e \circ a'' = a'' \ \lightning$$

инверзни елемент је јединствен

Деф. Моноид $(A, \circ)$ у коме сваки елемент има инверзни елемент називамо **група**.

1) $\circ : A^2 \to A$
2) $a \circ (b \circ c) = (a \circ b) \circ c$
3) $(\exists e)(\forall a)\ a \circ e = e \circ a = a$
4) $(\forall a)(\exists a')\ a \circ a' = a' \circ a = e$.

Додатно, ако је операција комутативна, онда је $(A, \circ)$ **комутативна (Абелова) група**.

Уобичајено је за групе да a' означавамо са a^{-1}, па такво означавање нам допушта увођење **негативних степена** у групи $(A, \circ)$: $a^{-n} = (a^{-1})^n,\ n \in \mathbb{N}$.

Т У групи $(A, \circ)$ важи $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.

Доказ:

1) $(a \circ b) \circ (b^{-1} \circ a^{-1}) = \ldots = e$

$= (a \circ (b \circ b^{-1})) \circ a^{-1} = (a \circ e) \circ a^{-1} = a \circ a^{-1} = e$

2) и слично $(b^{-1} \circ a^{-1}) \circ (a \circ b) = e$

из 1) и 2) сагласно дефиницији инверзног елемента закључујемо да је $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.

У скупу $G = \{1, 2, 3, 4, 5\}$ дефинисана је бинарна операција

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

Да ли у групоиду $(A, \circ)$ постоји e? $e = 1$

За елемент 2 одреди леве и десне инверзне елементе

$2 \circ 3 = 1,\ 2 \circ 4 = 1 \to 3$ и 4 су десни инверзи за 2

$4 \circ 2 = 1,\ 5 \circ 2 = 1 \to 4$ и 5 су леви инверзи за 2

$\circ : G^2 \to G$ није асоцијативна: $5 \circ (2 \circ 3) \neq (5 \circ 2) \circ 3$.

$5 \circ 1 = 1 \circ 3 \Leftrightarrow 5 = 3$ ↯

Прстени и поља

Пр. 16. Испитати да ли је $(\mathbb{Z}, +)$ група.

1) $+ : \mathbb{Z}^2 \to \mathbb{Z}$ операција је унутрашња, тј. $(\mathbb{Z}, +)$ је групоид

2) $(a+b)+c = a+(b+c)$ ✓ $(\mathbb{Z}, +)$ је семигрупа

3) $(\exists e=0)(\forall a)\ a+0=0+a=a$ $(\mathbb{Z}, +)$ је моноид

4) $(\forall a)(\exists a')\ a+a'=a'+a=0$ $a'=-a$ адитивни запис инверза $(\mathbb{Z}, +)$ је група

5) важи и комутативност, па је група Абелова

Важи $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ су примери бесконачних Абелових група са адитивним записом

$(\mathbb{Z}_k, +_k)$ је адитивна група остатака по модулу k.
Конкретно $(\mathbb{Z}_4, +_k)$ $A=\{0,1,2,3\}$ - остаци при дељењу са 4.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

↗ свака колона има 1 нулу па смо сигурни да има инверз

→ пример коначне групе

$3' = 1$ јер $3+1=0$

$(\mathbb{Z}_p \setminus \{0\}, \cdot_p)$ је мултипликативна група остатака по модулу простог броја p

Конкретно $(\mathbb{Z}_5 \setminus \{0\}, \cdot_5)$ $A=\{1,2,3,4\} = \mathbb{Z}_5 \setminus \{0\}$

$\cdot_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$4' = 4^{-1} = 4$ јер $4 \cdot_5 4 = 1$

$(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{C} \setminus \{0\}, \cdot)$ су примери бесконачних група (комутативних) са мултипликативним записом

Деф. Нека је дата група $(G, \circ)$. Ако непразан подскуп $H \subseteq G$ образује групу у односу на бинарну операцију $\circ$ ($\circ : H^2 \to H$, $\circ$ је асоц., $\exists e$, $(\forall a \in H)(\exists a' \in H)$), тада сматрамо да је $(H, \circ)$ **подгрупа** полазне групе $(G, \circ)$.

Т Алгебарска структура $(H, \circ)$ је подгрупа групе $(G, \circ)$ ако важи:

1) $\emptyset \neq H \subseteq G$
2) за свако $a, b \in H$ важи $a \circ b \in H$
3) $(\forall a \in H)\ a' \in H$.

Пр. 17. За реалну мултипликативну групу $(\mathbb{R} \setminus \{0\}, \cdot)$ проверити да скуп $H = \{x + y\sqrt{5} \mid x^2 - 5y^2 = 1 \land x, y \in \mathbb{Q}\}$ образује подгрупу $(H, \cdot)$.

I начин: провером аксиома се доказује да је $(H, \cdot)$ група, а самим тим је по дефиницији и подгрупа

II начин: применом теореме 1)...

2) доказ исти као доказ затворености

3) $a^{-1} = x - y\sqrt{5} \in H$ ✓ јер $a \cdot a^{-1} = e = 1$

пошто важе 1, 2 и 3, у питању је подгрупа

Изоморфизам група

Нека су дате групе $(G, \circ)$ и $(H, *)$. Функција $f : G \to H$ која испуњава $(\forall a, b \in G)\ f(a \circ b) = f(a) * f(b)$ се назива **хомеоморфизам** група. Специјално, ако је још f бијекција, тада хомеоморфизам називамо **изоморфизам**.

Пр. 18. $(\mathbb{R}, +)$ и $(\mathbb{R}^+, \cdot)$ су изоморфне групе.

$f : \mathbb{R} \to \mathbb{R}^+$ дефинисана са $f(x) = 2^x$ испуњава:

1) f је бијекција (графици); 2) $f(x+y) = 2^{x+y} = 2^x \cdot 2^y = f(x) \cdot f(y)$

Деф. Алгебарска структура $(R,+,\cdot)$ за неки скуп $R \neq \emptyset$ се назива прстен уколико важи:

1) $(R,+)$ је Абелова група
2) $(R,\cdot)$ је семигрупа
3) важе дистрибутивности

$(\forall x,y,z)\ x\cdot(y+z) = xy + xz$

$(\forall x,y,z)\ (x+y)z = xz + yz.$

Код прстена је сабирање увек комутативно, а множење у општем случају не мора бити.

Ако важи комутативност множења, прстен је комутативан.

Ако множење има неутрал, онда је у питању прстен са јединицом, а е називамо јединицом прстена.

Пр. 19 Битни примери прстена:

1) $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ - примери бесконачних прстена (провером аксиома се доказује)
2) $(\mathbb{Z}_k, +_k, \cdot_k)$ прстен остатака по модулу природног броја k
3) $(R[x],+,\cdot)$ прстен полинома са коефицијентима из неког прстена R - пример небројеног прстена

$$R[x] = \{ \sum_{k=0}^{n} a_k x^k \mid a_k \in R,\ n \in \mathbb{N} \}$$

4) прстен квадратних матрица истог формата је пример некомутативног прстена са јединицом.

(Т) У прстену $(R,+,\cdot)$ важе алгебарски закони:

1) $0\cdot x = x \cdot 0 = 0$ за неутрал 0 за сабирање
2) $-(x\cdot y) = (-x)y = x(-y)$
3) $(-x)(-y) = xy$.

① Испитати природу алгебарске структуре $(R, \circ, *)$, где је $x \circ y = x + y + 1$, $x * y = x + y + xy$.

Потпрстен и изоморфизми

Деф. Нека је дат прстен $(R, +, \cdot)$. Ако непразан скуп $H \subseteq R$ сам за себе образује прстен у односу на бинарне операције $+$ и $\cdot$, тада кажемо да је $(H, +, \cdot)$ **потпрстен** полазног прстена $(R, +, \cdot)$.
Провера да ли $(H, +, \cdot)$ образује прстен се врши или провером аксиома или применом следеће теореме:

Т Алгебарска структура $(H, +, \cdot)$ образује потпрстен прстена $(R, +, \cdot)$ ако важи:

1. $\emptyset \neq H \subseteq R$
2. $(\forall a, b \in H)\ a - b \in H$
3. $(\forall a, b \in H)\ ab \in H$.

Деф. Функција $f: R_1 \to R_2$ назива се **хомоморфизам** прстена $(R_1, +_1, \cdot_1)$ и $(R_2, +_2, \cdot_2)$ ако важи:

$f(a +_1 b) = f(a) +_2 f(b)$

$f(a \cdot_1 b) = f(a) \cdot_2 f(b)$, $(\forall a, b \in R_1)$, и додатно

$f(1_{R_1}) = 1_{R_2}$ ако прстени имају јединице.

Хомоморфизам $f: R_1 \to R_2$ који је и бијекција назива се **изоморфизам** прстена.

Поље

Деф. Алгебарска структура $(T, +, \cdot)$ са две бинарне операције назива се **тело** ако су испуњени услови (аксиоме): $+: T^2 \to T$, $\cdot: T^2 \to T$

1. $(T, +)$ је Абелова група

2. $(T\setminus\{0\},\cdot)$ је група

3. бинарна операција $\cdot$ је са обе стране дистрибутивна према $+$, тј. важи:

$x\cdot(y+z) = xy + xz$

$(x+y)z = xz + yz, \ (\forall x,y,z\in T)$

Прво се дефинише појам тела, па поље.

Деф. Комутативно тело се назива **поље**.

Поље се може дефинисати и као алгебарска структура где су $+$ и $\cdot$ бинарне операције за које важе услови (аксиоме):

1. $(F,+)$ Абелова група
2. $(F\setminus\{0\},\cdot)$ Абелова група
3. множење је дистрибутивно према сабирању

Пр. 20. 1) $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$ су бесконачна поља, а $(\mathbb{Z},+,\cdot)$ није поље

2) $(\mathbb{Z}_p,+_p,\cdot_p)$ поље остатака по модулу простог броја p – коначно поље

$(\mathbb{Z}_6,+_6,\cdot_6)$ није поље јер нпр. $3\cdot 2=0$, и $3,2\neq 0$

3) поља Галоа $(\mathcal{G},\oplus,\odot)$ са $|\mathcal{G}|=p^k$ елемената за $GF(p^k)$

Потпоља и изоморфизми поља

Деф. Ако је $(F,+,\cdot)$ поље, тада подскуп $P\subseteq F$ одређује потпоље уколико је алгебарска структура $(P,+,\cdot)$ сама за себе поље.

Т Алгебарска структура $(P,+,\cdot)$ је **потпоље** поља F уколико важи:

1. $\emptyset\neq P\subseteq F$

2. $(\forall a, b \in P)\ a-b \in P$

3. $(\forall a, b \in P)\ a \cdot b^{-1} \in P$

Деф. Функција $f: F_1 \to F_2$ назива се хомоморфизам поља $(F_1, +_1, \cdot_1)$ и $(F_2, +_2, \cdot_2)$ ако важи:

$f(a +_1 b) = f(a) +_2 f(b)$

$f(a \cdot_1 b) = f(a) \cdot_2 f(b)$, $(\forall a, b \in F_1)$ и

$f(1_{F_1}) = 1_{F_2}$.

Посебно, ако је f бијекција, онда је f изоморфизам поља.

Матрице

Нека је $(F,+,\cdot)$ поље. Тада **матрица** формата $m\times n$ над пољем F је правоугаона шема облика:

$$A=\begin{bmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & & a_{2n} \\ a_{31} & a_{32} & a_{33} & & a_{3n} \\ \dots & & & & \dots \\ a_{m1} & a_{m2} & a_{m3} & \dots & a_{mn} \end{bmatrix}$$

Елементи матрице a_{ij} су из поља.

Други приступ **дефиницији** матрице је да се она схвати као функција $A:\{1,2,\dots,m\}\times\{1,2,\dots,n\}\to F$ када се издвајају елементи a_{ij}.

Низ елемената $a_{i1}, a_{i2}, \dots, a_{in}$ одређује i-ту врсту, а низ елемената $a_{1j}, a_{2j}, \dots, a_{mj}$ одређује j-ту колону.

Матрица p-те врсте $A_{p\rightarrow}=[a_{p1}\ a_{p2} \dots a_{pn}]$

Матрица q-те колоне $A_{q\downarrow}=\begin{bmatrix} a_{1q} \\ a_{2q} \\ \dots \\ a_{nq}\end{bmatrix}$

Матрица A је формата 3×4 (3 врсте и 4 колоне).

$$A=\begin{bmatrix} 4 & 7 & -3 & 0 \\ 11 & -1 & 4 & 5 \\ 2 & 3 & -10 & 9 \end{bmatrix} \qquad A_{1\rightarrow}=[4\ 7\ -3\ 0] \qquad A_{1\downarrow}=\begin{bmatrix} 4 \\ 11 \\ 2 \end{bmatrix}$$

Скуп свих матрица $m\times n$ над пољем F означавамо $F^{m\times n}$. Посебно, ако $m=n$, матрице су **квадратне**, иначе су **неквадратне**. За квадратну матрицу формирамо два низа: **главну** дијагоналу као низ $a_{11}, a_{22}, \dots, a_{ii}, \dots a_{(n-1)(n-1)}, a_{nn}$, и **споредну дијагоналу** као низ $a_{1n}, a_{2(n-1)}, \dots, a_{i(n+1-i)}, \dots, a_{n1}$.

Ако $A\in F^{m\times n}$ тада је одређујемо сажетим записом елемената $A=[a_{ij}]_{m\times n}$, или $A=[a_{ij}]$.

*Из дефинисања матрице као ф-је важи за $A=[a_{ij}]_{m_1 \times n_1}$ и $B=[b_{ij}]_{m_2 \times n_2}$:

$$A=B \iff m_1=m_2 \land n_1=n_2 \land (\forall i,j)\ a_{ij}=b_{ij}.$$

За једнакост матрица „=" важи:

1. $A=A$ (Р)
2. $A=B \Rightarrow B=A$ (С)
3. $A=B \land B=C \Rightarrow A=C.$ (Т)

Операције над матрицама

1. Збир матрица

За $A=[a_{ij}]_{m\times n}$, $B=[b_{ij}]_{m\times n}$ дефинишемо $C=A+B=[c_{ij}]_{m\times n}$ ако је $(\forall i)(\forall j)\ c_{ij}=a_{ij}+b_{ij}$.

За матрицу $A=[a_{ij}]_{m\times n}$ супротна матрица је $-A=[-a_{ij}]_{m\times n}$, а разлика матрица $A=[a_{ij}]_{m\times n}$ и $B=[b_{ij}]_{m\times n}$ је збир матрица $D=A+(-B)=[d_{ij}]_{m\times n}$ ако је $(\forall i)(\forall j)\ d_{ij}=a_{ij}-b_{ij}$.

2. Производ скалара са матрицом

За скалар $\alpha \in \mathbb{F}$ и матрицу $A=[a_{ij}]_{m\times n}$ дефинишемо производ скалара и матрице множењем $C=\alpha A=[c_{ij}]_{m\times n}$, ако је $(\forall i)(\forall j)\ c_{ij}=\alpha a_{ij}$.

У скупу матрица $\mathbb{F}^{m\times n}$ се уводи нула матрица:

$$O=\begin{bmatrix} 0 & 0 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 0 \end{bmatrix}$$

Важна тврђење: Д3

Т 1) $(\mathbb{F}^{m\times n},+)$ је комутативна група

2) $(\forall \alpha \in F)(\forall A,B \in \mathbb{F}^{m\times n})\ \alpha(A+B)=\alpha A+\alpha B$

3) $(\forall \alpha,\beta \in F)(\forall A \in \mathbb{F}^{m\times n})\ (\alpha+\beta)A=\alpha A+\beta A$

4. $(\forall \alpha,\beta\in F)(\forall A\in \mathbb{F}^{m\times n})\ \alpha(\beta A)=(\alpha\beta)A$

5. за јединични скалар $1\in F$ важи $(\forall A\in\mathbb{F}^{m\times n})\ 1A=A$

3. производ матрица

Деф. Производ матрица $A=[a_{ij}]_{m\times n}$ и $B=[b_{ij}]_{n\times k}$ над пољем $\mathbb{F}$ је матрица $C=A\cdot B=[c_{ij}]_{m\times k}$ одређена елементима $c_{ij}=a_{i1}\cdot b_{1j}+a_{i2}b_{2j}+\dots+a_{in}b_{nj}$, редом за индексе $i\in\{1,2,\dots,m\}$ и $j\in\{1,2,\dots,k\}$.

Пр. $A=\begin{bmatrix}1&2&0\\5&4&5\end{bmatrix}_{2\times3}$ и $B=\begin{bmatrix}3&2&0&1\\-2&4&-1&3\\1&5&11&-7\end{bmatrix}_{3\times4}$

Матрице се могу множити само ако су им формати сагласни.

$$C=A\cdot B=\begin{bmatrix}(1\cdot3+2\cdot(-2)+0\cdot1) & (1\cdot2+2\cdot4+0\cdot5) & \cdots\\ (5\cdot3+4(-2)+5\cdot1) & (5\cdot2+4\cdot4+5\cdot5) & \cdots\end{bmatrix}=$$

$$=\begin{bmatrix}-1&10&-2&7\\12&51&51&-18\end{bmatrix}_{2\times4}$$

Матрице се множе врста пута колона.

4 Нека матрице $A=[a_1\ a_2\ a_3]$, $B=\begin{bmatrix}b_{11}&b_{12}&b_{13}\\b_{21}&b_{22}&b_{23}\\b_{31}&b_{32}&b_{33}\end{bmatrix}$ и $C=\begin{bmatrix}c_1\\c_2\\c_3\end{bmatrix}$ одређују скуп $M=\{A,B,C\}$. Одредити колико има смислених производа претходних матрица, уколико у производу учествује:

1) 2 матрице из M — AB, AC, BB, BC, CA
2) 3 -||- — 8
3) 4 -||- — 13 прод.
4) n -||-, $n\in\mathbb{N}$, $n\geq2$. *

$$C=A\cdot B=[a_{is}]_{m\times n}[b_{sj}]_{n\times k}=\left[\sum_{s=1}^{n}a_{is}b_{sj}\right]_{m\times k}$$

Јединична матрица I (I_n) је матрица (квадратна) која на главној дијагонали има јединице, а све остало нуле.

$$I = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ 0 & 0 & 1 \dots & 0 \\ 0 & 0 & 0 \dots & 1 \end{bmatrix}$$

За матрицу $A \in \mathbb{F}^{m \times n}$ и јединичне матрице I_n, I_m важи

$$A \cdot I_n = I_m \cdot A = A.$$

Елементи јединичне матрице одређују се Кронекеровим симболом $\delta_{ij} = \begin{cases} 1, & i=j \\ 0, & i \neq j \end{cases}$

Дијагонална матрица $D_n = D_n(d_1, d_2, \dots, d_n)$ је матрица која на главној дијагонали има елементе $d_1, d_2, \dots, d_n$, а остало нуле.

Доња троугаона матрица где за $a_{ij} = 0$ ако $j > i$, а горња троугаона $a_{ij} = 0$ за $i > j$.

$$\begin{bmatrix} a_{11} & 0 & \dots & 0 \\ a_{21} & a_{22} & & \vdots \\ \dots & & \dots & 0 \\ a_{n1} & \dots & & a_{nn} \end{bmatrix} \qquad \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ 0 & a_{2n} & \dots & a_{2n} \\ \vdots & & \ddots & \vdots \\ 0 & \dots & 0 & a_{nn} \end{bmatrix}$$

доња троугаона   горња троугаона

Скаларна матрица $D_n = D_n(d, d, \dots, d) = dI_n$.

Особине производа матрица

1. асоцијативност $(A \cdot B) \cdot C = A \cdot (B \cdot C)$ уколико су сагласни формати ($A \in \mathbb{F}^{m \times n}$, $B \in \mathbb{F}^{n \times k}$, $C \in \mathbb{F}^{k \times q}$)
2. дистрибутивност $A(B+C) = AB + AC$ ако постоје производи и $(A+B)C = AC + BC$
3. $(\alpha A)B = A(\alpha B) = \alpha(AB)$ ако постоје производи

(T) Алгебарска структура $(\mathbb{F}^{n \times n}, +, \cdot)$ јесте прстен са јединицом I_n.

$\mathbb{F}^{n \times n}$ – квадратне матрице формата $n \times n$ (реда n)

У општем случају овај производ није комутативан ($AB \neq BA$).

Степеновање квадратне матрице

Деф. За квадратну матрицу $A \in \mathbb{F}^{n\times n}$ одређујемо $A^1 = A$ и за $m \in \{2, 3, \dots\}$ одређујемо m-ти степен матрице са $A^m = A^{m-1} \cdot A$ и ако $A \neq 0$, онда $A^0 = I$.

Пр. индукцијом $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ $A^m = \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix}$, $m \in \mathbb{N}$.

Транспонована матрица

Деф. За матрицу $A = [a_{ij}] \in \mathbb{F}^{m\times n}$ транспонована матрица је матрица $A^T = [\alpha_{pq}] \in \mathbb{F}^{m\times n}$ таква да важи $\alpha_{pq} = a_{qp}$ редом за индексе $p \in \{1, \dots, n\}$ и $q \in \{1, \dots, m\}$

Пр. $A = \begin{bmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{bmatrix}$ $A^T = \begin{bmatrix} 1 & 4 \\ 2 & 5 \\ 3 & 6 \end{bmatrix}$

Т 1) $(\forall A \in \mathbb{F}^{m\times n})\ (A^T)^T = A$

2) $(A+B)^T = A^T + B^T$

3) $(\alpha A)^T = \alpha (A^T)$

4) $(AB)^T = B^T A^T$

У односу на транспоновање матрице могу бити:

- симетричне ако $A^T = A$
- косо симетричне ако $A^T = -A$
- ортогоналне ако $A^T \cdot A = I$.

Детерминанте

О пермутацијама скупа $\{1,2,\dots,n\}$

Деф. Пермутација p скупа $\{1,2,\dots,n\}$ је било које бијективно пресликавање $p:\{1,2,\dots,n\}\to\{1,2,\dots,n\}$.

$p(k)=j_k$, $p=\begin{pmatrix}1 & 2 & \dots & n\\ j_1 & j_2 & \dots & j_n\end{pmatrix}$ или $p=(j_1\, j_2 \dots j_n)$

Пр. $p=\{1,2,3\}$

$p_1=\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}$, $p_2=\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}$, $p_3=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$, $p_4=\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}$, $p_5=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$, $p_6=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}$

$\circ$	p_1	p_2	p_3	p_4	p_5	p_6
p_1	p_1	p_2	p_3	p_4	p_5	p_6
p_2	p_2	p_1	p_5	p_6	p_3	p_4
p_3	p_3	p_4	p_1	p_2	p_6	p_5
p_4	p_4	p_3	p_6	p_5	p_1	p_2
p_5	p_5	p_6	p_2	p_1	p_4	p_3
p_6	p_6	p_5	p_4	p_3	p_2	p_1

→ Кејлијева таблица

$(\{p_1,\dots,p_6\},\circ)$ – група

1. затвореност композиције
2. асоцијативна је композиција у општем случају
3. $e=p_1$
4. ако се попуни таблица до краја, лако се нађу инверзи

комутативност не важи

Елементи j_s и j_k образују инверзију у пермутацији $p=(j_1,j_2,\dots,j_n)$ ако важи $j_s>j_k$ за $s<k$. Са $I(j_1,\dots,j_k)$ одређујемо број инверзија.

Пр. $p_3=(2,1,3)=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}$

$\underset{j_1}{2}$ и $\underset{j_2}{1}$ јесу у инверзији, број инверзија p_3 је 1

$p_5=(3,1,2)=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$

3 и 1 су у инверзији и 3 и 2 су у инверзији; број је 2

Лема За скуп $\{1,2,\dots,n\}$ пермутације p и p^{-1} имају исти број инверзија.

Деф. Нека се свакој квадратној матрици $A=[a_{ij}]_{n\times n}$ над пољем $\mathbb{F}$ придружује скалар $|A| \stackrel{def}{=} \sum\limits_{(j_1,\dots,j_n)\in P} (-1)^{I(j_1,\dots,j_n)} a_{1j_1}\cdots a_{nj_n}$. Овај скалар назива се детерминанта квадратне матрице. Сумирање се врши по свим могућим пермутацијама. Користи се и ознака $\det A$.

Пр. $n=3$ $\quad |A| = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = (-1)^{\overbrace{I(1,2,3)}^{=0}} a_{11}a_{22}a_{33} + (-1)^{\overbrace{I(1,3,2)}^{=1}} a_{11}a_{23}a_{32}$

$+ (-1)^{\overbrace{I(2,1,3)}^{=1}} a_{12}a_{21}a_{33} + (-1)^{\overbrace{I(2,3,1)}^{=2}} a_{12}a_{23}a_{31} + (-1)^{\overbrace{I(3,1,2)}^{=2}} a_{13}a_{21}a_{32}$

$+ (-1)^{\overbrace{I(3,2,1)}^{=3}} a_{13}a_{22}a_{31} =$

$= a_{11}a_{22}a_{33} - a_{11}a_{23}a_{32} - a_{12}a_{21}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31}$

$$|A| = \begin{array}{|ccc|cc} + & + & + & & \\ a_{11} & a_{12} & a_{13} & a_{11} & a_{12} \\ a_{21} & a_{22} & a_{23} & a_{21} & a_{22} \\ a_{31} & a_{32} & a_{33} & a_{31} & a_{32} \\ - & - & - & & \end{array}$$

Сарусово правило – подудара се са дефиницијом

Основне особине детерминанти

(T) Детерминанта матрице $A=[a_{ij}]_{n\times n}$ $\det(A)$ једнака је детерминанти A^T. $\det A = \det A^T$

(T) Ако се замене две врсте (колоне), детерминанта мења знак.

(T) Ако се сви елементи једне врсте (колоне) матрице A помноже са скаларом λ добија се матрица B са особином $\det B = \lambda \det A$. Ако се све врсте помноже са λ добија се матрица B_2, где $\det B_2 = \lambda^n \det A$.

(T) Уколико у детерминанти сви елементи једне врсте се приказују као збирови одговарајућих елемената, тада се детерминанта раставља на збир две детерминанте, тако да се у првој задрже први сабирци, а у другој други.

$$|A| = \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ b_{i1}+c_{i1} & \cdots & b_{in}+c_{in} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ b_{i1} & \cdots & b_{in} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix} + \begin{vmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ c_{i1} & \cdots & c_{in} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{vmatrix}$$

Т Детерминанта матрице А једнака је нули ако:

1) сви елементи једне врсте (колоне) једнаки нули
2) матрица А има две једнаке врсте (колоне)
3) матрица А има две пропорционалне врсте (колоне)
4) једна врста (колона) матрице А је линеарна комбинација осталих врста (колона) матрице А
(α пута прва врста + β · друга)

Пр. $$\Delta = \begin{vmatrix} \sin^2\alpha & 1 & \cos^2\alpha \\ \sin^2\beta & 1 & \cos^2\beta \\ \sin^2\gamma & 1 & \cos^2\gamma \end{vmatrix} = \begin{vmatrix} \sin^2\alpha & \sin^2\alpha+\cos^2\alpha & \cos^2\alpha \\ \sin^2\beta & \sin^2\beta+\cos^2\beta & \cos^2\beta \\ \sin^2\gamma & \sin^2\gamma+\cos^2\gamma & \cos^2\gamma \end{vmatrix} = 0$$

Т Ако се елементи једне врсте (колоне) додају елементима друге врсте (колоне), вредност $|A|$ се не мења.

Развој детерминанте по некој врсти или колони

Нека је дата квадратна матрица $A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & & \vdots \\ a_{n1} & \cdots & a_{nn} \end{bmatrix}$. Нека је M_{pq} матрица која се добија из A изостављањем p-те врсте и q-те колоне. Детерминанту $|M_{pq}|$ називамо минор елемента a_{pq}. Скалар $A_{pq} = (-1)^{p+q} \det M_{pq}$ називамо кофактор (алгебарски комплемент) елемента a_{pq}.

Пр. $$A = \begin{bmatrix} 1 & -1 & 3 & -4 \\ -1 & 2 & 0 & 4 \\ 3 & 0 & 4 & 0 \\ -4 & 5 & -2 & -8 \end{bmatrix} \quad a_{12} = -1 \rightarrow |M_{12}| = \begin{vmatrix} -1 & 0 & 4 \\ 3 & 4 & 0 \\ -4 & -2 & -8 \end{vmatrix}$$

$$A_{12} = (-1)^{1+2} \det M_{12} = (-1) \cdot 72 = -72$$

Лапласов развој детерминанте

Т Нека је $A=[a_{ij}]_{n\times n}$ $(n\geq 2)$.

1) За свако $s=1,2,\dots,n$ важи

$$\det A = a_{s1}A_{s1}+a_{s2}A_{s2}+\dots+a_{sn}A_{sn}=\sum_{j=1}^{n} a_{sj}A_{sj}$$

2) За свако $k=1,2,\dots,n$ важи

$$\det A = a_{1k}A_{1k}+a_{2k}A_{2k}+\dots+a_{nk}A_{nk}=\sum_{i=1}^{n} a_{ik}A_{ik}.$$

Пр. $A=\begin{bmatrix} a & b & c\\ d & e & f\\ g & h & l\end{bmatrix}$ 1) по 3. врсти $|A|=\begin{vmatrix} a & b & c\\ d & e & f\\ g & h & l\end{vmatrix}=$

$$= g(-1)^{3+1}\begin{vmatrix} b & c\\ e & f\end{vmatrix}+h(-1)^{3+2}\begin{vmatrix} a & c\\ d & f\end{vmatrix}+l(-1)^{3+3}\begin{vmatrix} a & b\\ d & e\end{vmatrix}=$$

$$= g(bf-ec)-h(af-dc)+l(ae-bd)$$

Т За квадратну матрицу $A=[a_{ij}]_{n\times n}$ и $p,q\in\{1,\dots,n\}$ важи:

1) $\sum_{j=1}^{n} a_{pj}\cdot a_{qj}=\delta_{pq}\cdot|A|$

2) $\sum_{i=1}^{n} a_{ip}\, a_{iq}=\delta_{pq}|A|$, где је $\delta_{pq}=\begin{cases}1, & p=q\\ 0, & p\neq q\end{cases}$ и зове се Кронекеров симбол.

Троугаона детерминанта

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n}\\ 0 & a_{22} & & & \vdots\\ 0 & 0 & a_{33} & & \vdots\\ \vdots & & & \ddots & \\ 0 & \dots & & & a_{nn}\end{vmatrix}=a_{11}\cdot a_{22}\cdot\ldots\cdot a_{nn}$$

исто важи и за доњу троугаону детерминанту

Инверзна матрица

Деф. Нека је дата квадратна матрица A реда n над пољем F. Ако постоји квадратна матрица X истог реда као и матрица A, таква да важи $A\cdot X=X\cdot A=I_n$, тада је X инверзна матрица за матрицу A, и кориатимо ознаку A^{-1}.

Алгебарска структура $(F^{n\times n}, \cdot)$ је (некомутативна) семигрупа са јединицом I – јединична матрица реда n. Не постоји увек инверз (нпр. О матрица). Одређујемо услове под којим постоји инверзна матрица.

Прво дефинишемо адјунговану матрицу као матрицу која се састоји од кофактора транспоновано записаних $\mathrm{Adj}\,A = [A_{ij}]^T$.

Ⓣ $A \cdot \mathrm{Adj}A = \mathrm{Adj}A \cdot A = |A| \cdot I$ (1)

Ⓣ $|\mathrm{Adj}A| = |A|^{n-1}$

Ⓣ следи из (1): За квадратну матрицу $A = [a_{ij}]_{n\times n}$ постоји A^{-1} акко $|A| \neq 0$ и у том случају је:

$$A^{-1} = \frac{1}{|A|} \cdot \mathrm{adj}\,A.$$

Пр. $A = \begin{bmatrix} 1 & 1 & 2 \\ 1 & 3 & 1 \\ 4 & 1 & 1 \end{bmatrix} = 3 + 4 + 2 - 24 - 1 - 1 = -17 \neq 0$

$A_{11} = (-1)^{1+1} \begin{vmatrix} 3 & 1 \\ 1 & 1 \end{vmatrix} = 2$

$A_{12} = (-1)^{1+2} \begin{vmatrix} 1 & 1 \\ 4 & 1 \end{vmatrix} = 3$

$A_{13} = (-1)^{1+3} \begin{vmatrix} 1 & 3 \\ 4 & 1 \end{vmatrix} = -11$

$A_{21} = (-1)^{2+1} \begin{vmatrix} 1 & 2 \\ 1 & 1 \end{vmatrix} = 1$

$A_{22} = (-1)^{2+2} \begin{vmatrix} 1 & 2 \\ 4 & 1 \end{vmatrix} = -7$

$A_{23} = (-1)^{2+3} \begin{vmatrix} 1 & 1 \\ 4 & 1 \end{vmatrix} = 3$

$A_{31} = (-1)^{3+1} \begin{vmatrix} 1 & 2 \\ 3 & 1 \end{vmatrix} = -5$

$A_{32} = (-1)^{3+2} \begin{vmatrix} 1 & 2 \\ 1 & 1 \end{vmatrix} = 1$

$A_{33} = (-1)^{3+3} \begin{vmatrix} 1 & 1 \\ 1 & 3 \end{vmatrix} = 2$

$$\mathrm{adj}\,A = \begin{bmatrix} 2 & 1 & -5 \\ 3 & -7 & 1 \\ -11 & 3 & 2 \end{bmatrix}$$

$$A^{-1} = -\frac{1}{17} \begin{bmatrix} 2 & 1 & -5 \\ 3 & -7 & 1 \\ -11 & 3 & 2 \end{bmatrix}$$

Ⓣ $|A^{-1}| = \frac{1}{|A|}$, ако A је регуларна. Матрица је регуларна ако постоји A^{-1}, иначе је сингуларна.

Ⓣ Скуп свих регуларних квадратних матрица реда n образују (некомутативну) групу.
За регуларне матрице важи: $A^p \cdot A^q = A^{p+q}$, $(A^p)^q = A^{pq}$ за $p, q \in \mathbb{Z}$.

Ⓣ За детерминанте важи Коши-Бинеово својство: за две квадратне матрице истог реда n важи $|A \cdot B| = |A| \cdot |B|$.
Ово је особина детерминанти. Одатле $(\mathcal{M}, \cdot)$ - група, за $\mathcal{M}$ - скуп регуларних квадратних матрица реда n.
$A, B \in \mathcal{M} \ (\leftrightarrow |A|, |B| \neq 0) \rightarrow A \cdot B \in \mathcal{M} \ (\leftrightarrow |A \cdot B| = |A| \cdot |B| \neq 0)$

Системи линеарних једначина и Крамерове формуле

Деф. Систем линеарних једначина по $x_1, \dots, x_n$ је конјункција једначина:

$$a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = b_1$$
$$a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = b_2$$
$$\dots$$
$$a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = b_m$$

Ако $m=n$, ради се о квадратном систему, иначе је неквадратан.
Ако важи $b_1 = \dots = b_m = 0$, систем је хомоген. У супротном, ако постоји $b_i \neq 0$ систем је нехомоген.
Решење система је уређена n-торка $(\alpha_1, \dots, \alpha_n)$ која испуњава све једначине система, тј. систем као конјункција је тачан. По опстанку решења, систем може да буде сагласан (могућ) и несагласан. Сагласан је ако има бар 1 решење, несагласан ако нема ниједно. Ако има тачно 1 решење назива се одређен систем, а ако има више решења, онда је неодређен.

Поступци решавања линеарних система

Крамерове формуле - примењују се на квадратне системе (K).

$a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = b_1$

$\dots$

$a_{n1}x_1 + a_{n2}x_2 + \dots + a_{nn}x_n = b_n$

може се записати у матричном запису као $A \cdot X = b$, где је A матрица система, X матрица непознатих и b матрица слободних чланова.

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix} \quad X = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix} \quad b = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{bmatrix}$$

Напомена о решавању матрично задатих система:

$Ax = b$ у случају регуларне матрице A може се директно решити уз помоћ инверзне матрице $X = A^{-1} \cdot b$.

$A^{-1} / Ax = b \quad A^{-1} \cdot A \cdot X = A^{-1} \cdot b \quad IX = A^{-1} b \quad X = A^{-1} \cdot b$

Поред оваквих матричних система постоје и $\underset{m\times n}{X}\,\underset{n\times n}{A} = \underset{m\times n}{B}$

$X = B \cdot A^{-1}$, $|A| \neq 0$

$\underset{m\times m}{A} \cdot \underset{m\times n}{X} \cdot \underset{n\times n}{B} = \underset{m\times n}{C}$ $\quad |A| \neq 0, |B| \neq 0 \quad X = A^{-1} C B^{-1}$

За регуларне матрице важи $(A \cdot B)^{-1} = B^{-1} \cdot A^{-1}$.
(често формула)

(Т) (Крамерове формуле) Квадратни систем линеарних једначина (K) има јединствено решење акко $\det A \neq 0$ (систем је одређен). У том случају решење је дато Крамеровим формулама:

$$x_1 = \frac{\det(A_1)}{\det A}, \quad x_2 = \frac{\det(A_2)}{\det A}, \dots, x_n = \frac{\det(A_n)}{\det},$$

где је $\det(A_i)$ детерминанта која се добија од детерминанте det(A) тако што се i-та колона замени колоном слободних чланова тј. колоном из матрице b.

Често се разматра и $x_1 \cdot |A| = |A_1|, \ldots, x_n \cdot |A| = |A_n|$

Ако $|A| = 0$ и постоји $|A_i| \neq 0$, онда је систем несагласан.

$$\underbrace{x_i \cdot |A|}_{=0} = \underbrace{|A_i|}_{\neq 0}$$

Ако $|A| = 0$ и $(\forall i) |A_i| = 0$, онда систем није решив довољно брзо преко Гаусовог алгоритма.

① Квадратни систем решити матричном методом и Крамеровим формулама:

$$2x_1 + x_2 + x_3 = 1$$

$$x_1 + 2x_2 + x_3 = 2$$

$$x_1 + x_2 + 2x_3 = -3.$$

$$Ax = B$$