Def.: Fie $\sigma \in S_n$. O pereche (i, j) cu $1 \le i < j \le n$ s.n. **inversiune** a lui σ dacă $\sigma(i) > \sigma(j)$.
Numărul inversiunilor lui σ = $\mathrm{Inv}(\sigma)$.

Exemple:

1) $\sigma = e \qquad \mathrm{Inv}(e) = 0$

2) $\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ n & n-1 & \dots & 1 \end{pmatrix}$

$\mathrm{Inv}(\sigma) = C_n^2 = \dfrac{n(n-1)}{2}$

3) $\sigma = (i \ \ j)$ cu $i < j$

$$\sigma = \begin{pmatrix} 1 & \dots & i-1 & i & i+1 & \dots & j & j+1 & \dots & n \\ 1 & \dots & i-1 & j & i+1 & \dots & i & j+1 & \dots & n \end{pmatrix}$$

Inversiuni: $(i, i+1), \dots, (i, j)$,
$(i+1, j), \dots, (j-1, j)$

$j - i + (j-1-i)$
$= 2(j-i) - 1$
(impar)

↑ Numărul de inversiuni

Definim pentru $\sigma \in S_n$:

$$\varepsilon(\sigma) \overset{def}{=} \prod_{1 \le i < j \le n} \frac{\sigma(j) - \sigma(i)}{j - i}$$ **signatura lui σ**

Teoremă: $\varepsilon(\sigma) = (-1)^{\mathrm{Inv}(\sigma)}$, deci

- $\varepsilon(\sigma) = 1$, dacă $\mathrm{Inv}(\sigma)$ par
  $\to \sigma$ s.n. **permutare pară**
- $\varepsilon(\sigma) = -1$, dacă $\mathrm{Inv}(\sigma)$ impar
  $\to \sigma$ s.n. **permutare impară**

Dem.:

Funcția φ, $\varphi : \{(i,j) \mid 1 \leq i < j \leq n\} \to \{A \mid A \subset \{1,\dots,n\} \text{ cu } |A| = 2\}$

$\varphi((i,j)) = \{\sigma(i), \sigma(j)\}$ este bijectivă.

φ surjectivă: Fie $A = \{a, b\}$, $a \neq b$

σ bij. $\Rightarrow (\exists)\ \underset{p \neq q}{p, q}\quad \sigma(p) = a,\ \sigma(q) = b$

Dacă $p < q$, avem $\varphi((p,q)) = \{a, b\} = A$

Dacă $p > q$, avem $\varphi((q,p)) = \{b, a\} = A$

$|\text{Domeniul lui } \varphi| = C_n^2 = |\text{Codomeniul lui } \varphi|$

$\Downarrow$

φ bijectivă

Atunci $\left| \prod_{1 \leq i < j \leq n} \sigma(j) - \sigma(i) \right| = \prod_{1 \leq i < j \leq n} |\sigma(j) - \sigma(i)|$

$\overset{\varphi \text{ bij.}}{=\!=} \prod_{1 \leq i < j \leq n} (j - i)$

$\Rightarrow |\varepsilon(\sigma)| = 1 \Rightarrow \varepsilon(\sigma) \in \{-1; 1\}$

Numărul factorilor < 0 de la numărător în $\varepsilon(\sigma)$ este $\text{Inv}(\sigma)$.

$\Rightarrow \varepsilon(\sigma) = (-1)^{\text{Inv}(\sigma)}$

Teoremă: Pentru orice $\sigma, \tau \in S_n$ avem
$$\varepsilon(\sigma\tau) = \varepsilon(\sigma)\,\varepsilon(\tau)$$
[**reformulat** $\varepsilon : S_n \to \{1,-1\} = U_2$ morfism de grupuri]

Dem.:

$$\varepsilon(\sigma\tau) = \prod_{1\le i<j\le n} \frac{\sigma(\tau(j))-\sigma(\tau(i))}{j-i}$$
$$= \prod_{1\le i<j\le n}\left[\frac{\sigma(\tau(j))-\sigma(\tau(i))}{\tau(j)-\tau(i)}\cdot\frac{\tau(j)-\tau(i)}{j-i}\right]$$
$$=\underbrace{\left[\prod_{1\le i<j\le n}\frac{\sigma(\tau(j))-\sigma(\tau(i))}{\tau(j)-\tau(i)}\right]}_{\varepsilon(\sigma)}\cdot\underbrace{\left[\prod_{1\le i<j\le n}\frac{\tau(j)-\tau(i)}{j-i}\right]}_{\varepsilon(\tau)}$$

$$\left(\frac{\sigma(a)-\sigma(b)}{a-b}=\frac{\sigma(b)-\sigma(a)}{b-a}\right)$$

Corolar: Fie $n\ge 2$. Fie $A_n = \{\sigma\in S_n \mid \sigma \text{ pară}\}$. Atunci A_n este subgrup normal al lui S_n și $S_n/A_n \simeq U_2$, deci $|A_n| = \frac{n!}{2}$

Dem.:

$\varepsilon : S_n \to U_2$ morfism surjectiv de grupuri

$i \ne j$ $\quad (i\ j) \rightsquigarrow$ impară (Inv(σ) impar)

$\operatorname{Ker} \varepsilon = A_n$ subgrup normal

Teorema fundamentală de izomorfism $\Rightarrow$

$$\Rightarrow S_n / A_n \simeq \operatorname{Im} \varepsilon = U_2$$

$$|S_n / A_n| = |U_2| = 2$$

$$[S_n : A_n] = \frac{|S_n|}{|A_n|} = \frac{n!}{|A_n|}$$

Consecință: Un ciclu de lungime n este permutare $\Rightarrow$ produs de $n-1$ transpoziții

impară, dacă n par

pară, dacă n impar

$$\varepsilon(\tau) = (-1)^{n-1}$$

$$\sigma = \tau_1 \dots \tau_r$$

cicluri

Exercițiu: Dacă $\sigma = \tau_1 \dots \tau_r$ produs de cicluri disjuncte.

lung. n_1 $\quad$ n_r

$$o(\sigma) = [n_1, \dots, n_r]$$

Inele și corpuri

Def.: S.m. inel: $(R, +, \cdot)$

$(R,+)$ abelian

$(R,\cdot)$ monoid

$$\begin{cases} a(b+c)=ab+ac \\ (b+c)a=ba+ca \end{cases} \quad (\forall)\ a,b,c\in R$$

$a\cdot b = ab$

→ 0 el. neutru, $-a$ simetricul lui a

→ 1 el. neutru

Dacă, în plus, $ab=ba$, $(\forall)\ a,b$, R s.m.
inel comutativ.

Observație! $a\cdot 0 = 0\cdot a = 0$

$$a\cdot 0 = a\cdot(0+0) = a\cdot 0 + a\cdot 0$$
$$\Downarrow\ (-(a\cdot 0))$$
$$0 = a\cdot 0$$

$$(-a)b = a\cdot(-b) = -(ab)$$
$$(-a)\cdot(-b) = ab$$

Dacă $1=0 \Rightarrow (\forall)\ a\in R$, $a = a\cdot 1 = a\cdot 0 = 0$

$\Rightarrow R=\{0\}$ inel trivial

Vom presupune mereu că $1\neq 0$.

Exemple de inele:

1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ inele comutative

2) $\mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2} \mid a,b\in\mathbb{Z}\}$ inel comutativ

cu $+$ și $\cdot$ desemnate

3) $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ inel comutativ

4) X mulțime $\neq \emptyset$

$(\mathrm{Func}(X, \mathbb{R}), +, \cdot)$ inel comutativ

$f, g : X \to \mathbb{R}$ $\quad +$ $\quad f+g : X \to \mathbb{R}$ $\quad (f+g)(x) = f(x) + g(x)$, $(\forall)\, x \in X$

$\cdot$ $\quad f \cdot g : X \to \mathbb{R}$ $\quad (fg)(x) = f(x) \cdot g(x)$, $(\forall)\, x \in X$

5) Inele de matrice

R inel, $n \in \mathbb{N}^*$

O matrice $n \times n$ cu elemente din R.

$\parallel$

O funcție $A : \{1, \dots, n\} \times \{1, \dots, n\} \to R$

notăm $A((i,j)) = a_{ij}$, $(\forall)\, i, j$

Identificăm $A \sim \begin{pmatrix} a_{11} & \dots & a_{1n} \\ - - - & - - - & - - - \\ a_{n1} & \dots & a_{nn} \end{pmatrix} \overset{\text{not.}}{=} (a_{ij})_{1 \leq i, j \leq n}$

$M_n(R)$ = mulțimea tuturor acestor matrice

$+$ $\quad (a_{ij})_{i,j} + (b_{ij})_{i,j} \overset{\text{def.}}{=} (a_{ij} + b_{ij})_{i,j}$

$\cdot$ $\quad (a_{ij})_{i,j} \cdot (b_{ij})_{i,j} \overset{\text{def.}}{=} (c_{ij})_{i,j}$, unde

$$c_{ij} = \sum_{k=\overline{1,m}} a_{ik} \cdot b_{kj}$$

$(M_m(R), +, \cdot)$ inel [exercițiu]

1 la: $I_m = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & \ddots & & \vdots \\ 0 & \dots & & 1 \end{pmatrix}$

6) $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \in \mathbb{C}$
- inelul întregilor lui Gauss

7) R, S inele

$R \times S = \{(r, s) \mid r \in R, s \in S\}$ inel

$(r, s) + (r', s') \overset{\text{def.}}{=} (r + r', s + s')$ produsul

$(r, s) \cdot (r', s') \overset{\text{def.}}{=} (rr', ss')$ direct al

inelelor R, S

Def.: Fie R inel. Un element $a \in R$ s.m. inversabil dacă $(\exists)\ b \in R$ cu $ab = ba = 1$.

- b este unic determinat (dacă există)

$b = a^{-1}$ inversul lui a

$U(R) = \{a \mid a \text{ inversabil}\}$

$(U(R), \cdot)$ grup

Def. Un inel R s.m. corp dacă orice $a \in R \setminus \{0\}$ este inversabil [adică $U(R) = R \setminus \{0\}$].

Dacă R este și comutativ, R s.m. corp comutativ.

Exemple:

1) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ corpuri comutative

2) $\mathbb{Q}[\sqrt{2}]$ corp comutativ [exercițiu]

3) $\mathbb{Q}[\sqrt[3]{2}] \overset{def.}{=} \{a+b\sqrt[3]{2}+c\sqrt[3]{4} \mid a,b,c \in \mathbb{Q}\}$ corp comutativ

Def.: Fie R, S inele. O funcție $f: R \to S$ s.n.

• **morfism de inele**, dacă $\begin{cases} f(x+y)=f(x)+f(y) \\ f(xy)=f(x)f(y) \\ f(1_R)=f(1_S) \end{cases}$, $(\forall)\ x,y \in R$

• **izomorfism de inele**, dacă este morfism bijectiv de inele (în acest caz, spunem că inelele R și S sunt izomorfe, scriem $R \simeq S$)

Dacă R și S sunt corpuri,
$f: R \to S$ s.n. **(izo)morfism de corpuri** dacă este (izo)morfism de inele

Exerciții:

• $R \xrightarrow{Id_R} R$ izomorfism de inele

• $R \xrightarrow{f} S \xrightarrow{g} T$

f, g morfisme de inele $\Rightarrow g \circ f$ morfism de inele

• $f: R \to S$ izomorfism de inele $\Rightarrow$
$\Rightarrow f^{-1}: S \to R$ izomorfism de inele

· $f: R \to S$ morfism de corpuri $\Rightarrow$

- f injectiv
- $x \neq 0 \Rightarrow f(x) \neq 0$ și $f(x)^{-1} = f(x^{-1})$

Def.: 1) Fie R inel.

$\emptyset \neq A \subset R$ s.m. **subinel** dacă

$$\begin{cases} x, y \in A \Rightarrow x - y \in A \text{ și } xy \in A \\ 1 \in A \end{cases}$$

[consecință: $(A, +, \cdot)$ inel]

2) Fie R corp și $A \subset R$.

A s.m. **subcorp** dacă A este subinel și pentru orice $x \in A \setminus \{0\}$ avem $x^{-1} \in A$.

[consecință: $(A, +, \cdot)$ corp]

Exerciții:

$$A = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\} \text{ corp cu } +, \cdot \text{ matricelor}$$

$\mathbb{C} \xrightarrow{f} A$

$A \subset M_2(\mathbb{R})$

$\downarrow$

inel

$$f(a+bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \text{ morfism de inele}$$

$f(1) = I_2$

Exercițiu: $n \geq 2$, R inel
$\downarrow$
$M_n(R)$ nu este comutativ

Ideale și inele factor

Vom lucra doar cu inele comutative.

Def.: Fie R inel comutativ. O submulțime $\emptyset \neq I \subset R$ s.n. **ideal** dacă

$$\begin{cases} x, y \in I \Rightarrow x - y \in I \longrightarrow (I \leq (R,+)) \\ a \in R,\ x \in I \Rightarrow ax \in I \end{cases}$$

Observație!
- $\left.\begin{array}{l} I \text{ ideal} \\ 1 \in I \end{array}\right| \Rightarrow I = R$
- Dacă $(\exists)\ x \in I$ inv. $\Rightarrow I = R$

$$\underset{\substack{\cap \\ R}}{(ax^{-1})}\, x = a$$

Exemple:

1) R, $\{0\}$ ideale
2) $\mathbb{Z}$ idealele sunt $n\mathbb{Z}$, $n \in \mathbb{N}$
3) R corp comutativ $\Rightarrow$ Idealele sunt R și $\{0\}$
4) R, S inele comutative. Atunci $R \times \{0\}$ și $\{0\} \times S$ sunt ideale în $R \times S$.
5) $f: R \to S$ morfism de inele $\Rightarrow \operatorname{Ker} f$ este ideal în R

$\operatorname{Ker} f \leq (R,+)$ – știm

$a \in R,\ x \in \mathrm{Ker}\, f \Rightarrow f(ax) = f(a)\underbrace{f(x)}_{\underset{0}{\|}} = 0 \Rightarrow$

$\Rightarrow ax \in \mathrm{Ker}\, f$

6) [exercițiu]

Dacă I, J ideale în R, atunci $I \cap J$ și $I + J \overset{\text{def.}}{=}$ $= \{x + y \mid x \in I, y \in J\}$ sunt ideale în R

7) [exercițiu]

Dacă $n, m \in \mathbb{N}$, atunci

$$\begin{cases} n\mathbb{Z} \cap m\mathbb{Z} = [n,m]\mathbb{Z} \\ n\mathbb{Z} + m\mathbb{Z} = (n,m)\mathbb{Z} \end{cases}$$

Exerciții:

R inel comutativ

(1) Intersecția unei familii nevide de ideale este ideală

(2) Dacă $\emptyset \neq X \subset R$, atunci

$$\bigcap_{\substack{I \text{ ideal} \\ X \subset I}} I = \text{cel mai mic ideal care îl include pe } X$$

$\|$

idealul generat de mulțimea X și se notează (X)

(3) $\cdot\ X = \{a\} \Rightarrow (X) = \{ra \mid r \in R\} \overset{\text{not.}}{=} Ra$

$\| \text{not.}$

(a)

• $X=\{a_1,\dots,a_n\} \Rightarrow (X) = \{x_1a_1+\dots+x_na_n \mid x_1,\dots,x_n\in R\}$

$(X) = (a_1,\dots,a_n)$

$(X) = Ra_1+\dots+Ra_n$

Idealul I s.n. **principal** dacă $(\exists)\, a\in R$ cu $I=(a)$.

finit generat dacă $(\exists)\, X$ finită cu $I=(X)$

Inelul factor

Fie R inel comutativ și I ideal, $I\neq R$.

$I \leq (R,+)$

$\downarrow$ normal, $\downarrow$ abelian

$(R/I, +)$ grup abelian

$R/I=\{\hat{x} \mid x\in R\}$

$\hat{x}=\hat{y} \Leftrightarrow x-y\in I$

$\hat{x}+\hat{y}=\widehat{x+y}$

Definesc pe R/I o înmulțire:

$\hat{x}\cdot\hat{y} \overset{def.}{=} \widehat{xy}$, $(\forall)\, x,y\in R$

Definiția este corectă.

$$\left.\begin{aligned}\hat{x}&=\hat{x}'\\ \hat{y}&=\hat{y}'\end{aligned}\right| \overset{?}{\Rightarrow} \widehat{xy} \overset{?}{=} \widehat{x'y'}$$

$\Updownarrow$

$x-x'\in I$

$y-y'\in I$

$$rs - r's' = rs - r's + r's - r's'$$
$$= \underbrace{\underbrace{(r-r')}_{\in I} s}_{\in I} + \underbrace{\underbrace{(s-s')}_{\in I} r'}_{\in I} \in I$$

Propoziție: $(R/I, +, \cdot)$ inel comutativ cu el. neutru $= \hat{1}$

$\pi : R \to R/I$ morfism surjectiv de inele

$\pi(r) = \hat{r}$ (cu $\ker \pi = I$)

Exemplu:

$R = \mathbb{Z}$, $m \in \mathbb{N}$, $m \geq 2$

$I = m\mathbb{Z}$ ideal în $\mathbb{Z}$

$\mathbb{Z}/_{m\mathbb{Z}}$ = inel $= \mathbb{Z}_m$ inelul claselor de resturi modulo m

$\hat{i} + \hat{j} = \widehat{i+j}$

$\hat{i}\hat{j} = \widehat{ij}$