

Monoid (M, \circ)

- parte stabilită: $x \in G, y \in G \Rightarrow x \circ y \in G$
- „ \circ ” asoc.: $(a \circ b) \circ c = a \circ (b \circ c)$
- „ \circ ” are elem. neutr: $\exists e \in M$ a.t. $e \circ x = x \circ e = x$

Ex: (\mathbb{Z}, \cdot) , $(M_{m,n}(K), \circ)$

Grup: (G, \circ)

- parte stabilită: $x \in G, y \in G \Rightarrow x \circ y \in G$
- „ \circ ” asoc.: $(a \circ b) \circ c = a \circ (b \circ c)$
- „ \circ ” are elem. neutr: $\exists e \in G$ a.t. $e \circ x = x \circ e = x$
- toate elem. simetrizabile: $\exists x' \in G$ a.t. $x \circ x' = x' \circ x = e$

Ex: sunt gr: $(\mathbb{Z}, +)$, (\mathbb{Q}^*, \cdot) , $(\mathbb{Z}_n, +)$

Nu sunt gr: $(\mathbb{N}, +)$, (\mathbb{Z}, \cdot) , $(M_{m,n}(K), \circ)$, (\mathbb{Z}^*, \cdot)

Notații

- $\mathcal{U}(M) = \{x \in M \mid x\text{-inversabil}\}$; $(\mathcal{U}(M), \circ)$ - grupul elem. inversabile din M

Ex. $(\mathcal{U}(\mathbb{Z}_n), \circ)$, $(\mathbb{Z}_{p^*}, \circ)$ grup
 $\hookrightarrow p$ prim

$$\mathcal{U}(M') = \{f: M \rightarrow M \mid f\text{-bij}\} = S_m$$

(S_m, \circ) gr. simetric asociat lui M / gr. permutărilor lui M

- $(GL_n(K), \circ)$ - grup general liniar de ordin n peste K
 \hookrightarrow gr. necomutativ

Ex. $(GL_n(\mathbb{Z}), \circ) = \{A \in M_n(\mathbb{Z}) \mid \det A = \pm 1\}$

! $\mathbb{Z}(G) = \{x \in G \mid xy = yx\} \rightarrow$ CENTRUL grupului !

- $\Delta_n = \{1, r, r^2, \dots r^{n-1}, s, sr, sr^2, \dots sr^{n-1}\}$
 \hookrightarrow gr. diedral

$$! r^n = s^2 = 1 ; r^k s = s r^{n-k} !$$

(Δ_n, \circ) gr. necomutativ

- $A_n = \{\Gamma \in S_n \mid \Gamma\text{-par}\}$ - gr. altern

Morfisme

Def: Fie (G, \cdot) , $(H, *)$ gr. O fct. $f: G \rightarrow H$ s.n. morfism dacă:

$$\forall x, y \in G : f(x \cdot y) = f(x) * f(y) \Leftrightarrow f \in \text{Hom}(G, H)$$

• morfism + bij. \Rightarrow izomorfism ($G \cong H$)

• $f: G \rightarrow G$ - endomorfism

• endomorfism + bij \Rightarrow automorfism

Ex: $f: (\mathbb{R}, +) \rightarrow (\mathbb{R}^*, \cdot)$, $f(x) = e^x$ morfism

$g: (\mathbb{R}, +) \rightarrow (\mathbb{R}_+^*, \cdot)$, $f(x) = e^x$ izomorfism

Ordinalul unui elem.

$\begin{cases} \rightarrow \text{cel mai mic } n \in \mathbb{N}^* \text{ pt. care } a^n = 1 \\ \rightarrow \text{dacă } a^n \neq 1 \Rightarrow \text{ord}(a) = \infty \end{cases}$

• $\text{ord}(x) = n \Leftrightarrow \begin{cases} i) x^n = 1 \\ ii) m \in \mathbb{Z}, x^m = 1 \Rightarrow n | m \end{cases}$

• $\text{ord}(x) < \infty, \text{ord}(y) < \infty, xy = yx \Rightarrow$

$\Rightarrow \text{ord}(xy) | [\text{ord}(x), \text{ord}(y)]$

$\Rightarrow \text{ord}(x^k) = \frac{\text{ord } x}{(k, \text{ord}(x))}$

$\Rightarrow \text{ord}(xy) = \text{ord}(yx).$

$\rightarrow f: G \rightarrow H$ morfism și $x \in G$:

• $\text{ord}(x) = n \in \mathbb{N}^* \Rightarrow \text{ord}(f(x)) \in \mathbb{N}^*$ și $\text{ord}(f(x)) | \text{ord}(x)$

• $\text{ord}(f(x)) = \infty \Rightarrow \text{ord}(x) = \infty$

• f izomorfism $\Rightarrow \text{ord}(x) = \text{ord}(f(x))$

! 2 gr. sunt izomorfe \Rightarrow au același nr. de elem. de un anumit ordin

T. Lagrange: G - finit, $x \in G \Rightarrow \text{ord}(x) < \infty$ și $\text{ord}(x) | |G|$

Subgrupuri

Def. Fie (G, \cdot) grup și $H \subseteq G$. Sp. că $H \leq G$ dacă:

i) $\forall x, y \in H \Rightarrow x \cdot y \in H$

ii) (H, \cdot) grup

T $H \leq G \Leftrightarrow$ i) $H \neq \emptyset$ (el. neutru $e \in H$)

ii) $\forall x, y \in H \Rightarrow x \cdot y \in H$

iii) $\forall x \in H \Rightarrow x^{-1} \in H$

Ex: $\mathbb{Z} \leq \mathbb{Q}$; $\mathbb{N} \not\leq \mathbb{Q}$ pt. $(\mathbb{Q}, +)$; $2 \mathbb{Z} + 1 \not\leq \mathbb{Z}$

• $\{1\}$ și G - subgr. triviale

• $k\mathbb{Z} = \{kx \mid x \in \mathbb{Z}\} \leq (\mathbb{Z}, +)$

$f: G \rightarrow H$ morfism:

- dacă $H \subseteq G \Rightarrow f(H) \subseteq K$
- dacă $L \subseteq K \Rightarrow f^{-1}(L) = \{g \in G \mid f(g) \in L\} \subseteq G$
- $K_r(f) = \{x \in G \mid f(x) = 1_H\} \subseteq G$
- $f(G) \subseteq H$

T. Cayley: Pf. V gr. G , există inj. de gr: $t: G \rightarrow S_G$

Subgrupuri generate

Def. Fie (G, \cdot) gr. și $X \subseteq G$. At. subgr:

$$\langle X \rangle = \bigcap_{\substack{H \subseteq G \\ X \subseteq H}} H \text{ s.n. subgr. generat de } X$$

- $X \subseteq \langle X \rangle$
- $K \subseteq G$ și $X \subseteq K \Rightarrow \langle X \rangle \subseteq K$

\bigcap unei familii de subgrupuri e subgr.

\bigcup subgr., în general, NU e subgr.

Grupuri ciclice

Gr. (G, \cdot) e ciclic dacă:

$$\exists x \in G \text{ a.t. } G = \langle x \rangle$$

\hookdownarrow G e generat de x
 \hookdownarrow x generator pt. G

$$\Rightarrow G = \{x^n \mid n \in \mathbb{Z}\}$$

$$\begin{aligned} \text{Ex. } &-(\mathbb{Z}, +) \text{ e generat de } \langle 1 \rangle = \{n \cdot 1 \mid n \in \mathbb{Z}\} \\ &\langle -1 \rangle = \{-1 \cdot n \mid n \in \mathbb{Z}\}. \end{aligned}$$

$$\bullet (\mathbb{Z}_n, +) \text{ ciclic } \mathbb{Z}_n = \langle a \rangle \Leftrightarrow (a, n) = 1$$

$$\bullet (\mathbb{Z}_p^*, \cdot) \text{ ciclic } (p-\text{prim})$$

$$\bullet O_n = \{z \in \mathbb{C} \mid z^n = 1\}, (O_n, \cdot) \text{ ciclic}$$

$$\bullet \text{Gr. Klein } K = \{1, a, b, c\} \text{ nu e ciclic}$$

P Fie $G = \langle x \rangle$ ciclic

- dacă $|G| = n \in \mathbb{N}^* \Leftrightarrow \text{ord } x = n$
- G e inf. $\Leftrightarrow \text{ord } x = \infty$

T $\forall 2$ grupuri ciclice cu același cardinal sunt izomorfe

- G ciclic și $|G| = n \Rightarrow G \cong \mathbb{Z}_n$
- G ciclic și $|G| = \infty \Rightarrow G \cong \mathbb{Z}$

Subgrupuri ciclice

T (G, \cdot) gr. ciclic. Dacă $H \subseteq G$, avem:

- $H \subseteq G \Leftrightarrow \exists d \in \mathbb{N}$ a.î. $H = \langle x^d \rangle$
- G infinit $\rightarrow \forall d, l \in \mathbb{N}, d \neq l, \langle x^d \rangle \neq \langle x^l \rangle$
- $|G| = n, H \subseteq G \Leftrightarrow \exists d \in \mathbb{N}$ a.î. $H = \langle x^d \rangle$, unde $d | n$

Relații de echivalență (subgrup)

(G, \cdot) grup, $H \subseteq G$. Pe G definim:

$$x \rho_H y \Leftrightarrow x^{-1} \cdot y \in H \quad (\times H)$$

$$x \rho'_H y \Leftrightarrow y \cdot x^{-1} \in H \quad (Hx)$$

↓

rel. de echiv. reflexivă: $x \rho x$

transitivă: $(x \rho y) \wedge (y \rho z) \Rightarrow x \rho z$

simetrică: $x \rho y \Rightarrow y \rho x$

! G mult. $\left| \begin{array}{l} \rho \text{ rel. de echiv.} \\ \Rightarrow G/\rho = \{ \rho \langle x \rangle \mid x \in G \} \end{array} \right. \stackrel{\text{not.}}{=} \text{mult. factor}$

clasa de echiv. a lui x $\{ y \in G \mid x \rho y \}$

T

(G, \cdot) grup, $H \subseteq G$

1. $|G/\rho_H| = |G/\rho'_H| \stackrel{\text{not.}}{=} |G:H| (G/\rho_H \neq G/\rho'_H)$

2. G finit $\Rightarrow |G| = |H| \cdot |G:H|$ (T. Lagrange)

$$\frac{|H|}{\sim} / |G| \stackrel{\text{subgrupuri}}{\sim} \text{ord}(g) / |G|$$

Subgrupuri normale

$H \leq G$, φ_H, φ_H' rel. echiv. pe G

$\forall x \in G, \varphi_H \langle x \rangle = xH$

$$\varphi_H' \langle x \rangle = Hx \quad (G/\varphi_H \neq G)$$

Def. Subgr. $H \leq G$ este normal ($N \trianglelefteq G$) dacă:

$\forall x \in G, xN = Nx$

sau

$x^{-1}n x \in N, \forall n \in N$

Exemplu: • G abelian, $N \leq G \Rightarrow N$ normal

- $\{1\}, G$
↳ elem. neutru
- Δ_4 nu este normal

Teorema I de izomorfism

$f: G \rightarrow H$ morfism. At:

$$\text{Ker } f = \{g \in G \mid f(g) = 1_H\} \trianglelefteq G$$

$\bar{f}: G^*/\text{ker } f \rightarrow f(G)$ e izomorfism ($\bar{f}(x \text{ker } f) = f(x)$)

↳ descompunerea canonica

$$\begin{array}{ccc} G & \xrightarrow{\delta} & H \\ \downarrow \text{ker } f & & \downarrow i \\ G/\text{ker } f & \xrightarrow{\bar{f}} & f(G) \end{array}$$

Teorema II de izomorfism

(G, \cdot) grup, $N \trianglelefteq G$. Dacă $H \leq G$, atunci:

$$\begin{cases} HN = \{h \cdot n \mid h \in H, n \in N\} \leq G \\ N \trianglelefteq HN \text{ și } H \cap N \trianglelefteq H \\ H/HN \cong HN/N \end{cases}$$

Teorema III de izomorfism

(G, \cdot) -grup, $H, N \leq G, N \trianglelefteq H$

$$\begin{cases} H/N \trianglelefteq G/N \\ \hookrightarrow \{h \cdot N \mid h \in H\} \end{cases}$$

$$G/N/H/N \cong G/H$$

Grupuri factor (cât)

Def. (G, \cdot) grup, $N \leq G$. Pe G/N definim:

- $G/N \times G/N \rightarrow G/N \leftarrow$ gr. factor (G/N)
- $(xN)(yN) = (xy)N$
- $(xN)^{-1} = x^{-1}N$

Ex. $D_4/N \cong$ Klein

Grupuri finite

$$C(x) = \{g \in G \mid gx = xg\}$$

\hookrightarrow comutatorul lui x

$$Z(G) = \{x \in G \mid \forall g \in G, gx = xg\}$$

\hookrightarrow centrul lui x

$$\rightarrow x \sim y \Leftrightarrow \exists g \in G \text{ a.s.t. } g^{-1}xg = y$$

\hookrightarrow rel. de conjugare

[P]

$$\begin{cases} C(x) \leq G \\ Z(G) \trianglelefteq G \\ Cl(x) = \{g^{-1}xg \mid g \in G\} \end{cases}$$

Ecuatia claselor, p-grupuri

$$\hookrightarrow |G| = |Z(G)| + \sum_{i=1}^k |G : C(x_i)|$$

• G este un p-grup dacă: $\exists k \in \mathbb{N}$ a.s.t. $|G| = p^k$

T. Cauchy

G -finit, p -prim

dacă $p \mid |G|$, at. $\exists g \in G$ cu $\text{ord}(g) = p$

T. Sylow

G -finit, p -prim a.s.t. $p^n \mid |G|$; $n < 2$

at. G are un subgrup de ordin p^n .

Def. (G, \cdot) -finit, p -prim. Dacă $p^n \mid |G|$ și $p^{n+1} \nmid |G| \Rightarrow$
 \Rightarrow \exists subgr. din G de ord. p^n s.n. p subgr. Sylow al lui G

Inele

$(R, +, \cdot)$ form. inel dacă:

- $(R, +)$ gr. ab
- (R, \cdot) semigrup
- „ \cdot ” e distrib. față de „ $+$ ”: $a(b+c) = ab+ac$
 $(a+b)c = ac + bc$

* (R, \cdot) - monoid \Rightarrow inel cu unit.

* (R^*, \cdot) - grup \Rightarrow CORP

R e fără div. ai lui zero dacă:

$$\nexists x, y \in R, x, y \neq 0 \Rightarrow xy \neq 0$$

inelul R s.n. domeniu de integritate dacă:

R are unitate, com. și fără div. ai lui zero

inel cu unitate, finit + fără div. ai lui zero \Rightarrow CORP

Ex. $(\mathbb{Z}, +, \cdot)$ - dom. de int., dar NU e corp

$(\mathbb{Z}_p, +, \cdot)$ - corp com, dar nu e dom. de int., p - PRIM

Subcorpuri

$(K, +, \cdot)$ corp, $S \subseteq K$ urm. afirm. sunt echiv.:

1) L e parte stabilă față de $+$

$(L, +, \cdot)$ - corp

2) S subcorp în K

$$\{0, 1 \in S \Leftrightarrow |S| \geq 2\}$$

$$\nexists x, y \in S, x-y \in S$$

$$\nexists x, y \in S, y \neq 0, xy^{-1} \in S$$

cel mai mic subcorp al lui $K = P(K)$ s.n. subcorp prim al lui K

$$P(K) = \{(m \cdot 1_K)(n \cdot 1_K)^{-1} / m, n \in \mathbb{Z}, n \cdot 1_K \neq 0\}$$

$$P(K) \cong Q \text{ dacă } \text{char}(K) = \infty$$

$$\cong \mathbb{Z}_p \text{ dacă } \text{char}(K) = p.$$

Subinel

$(R, +, \cdot)$ inel, $S \subseteq R$. U.a.s.e:

1) S subinel în R

2) $0 \in S \Leftrightarrow S \neq \emptyset$

$$\nexists x, y \in S, x-y \in S \quad \Leftrightarrow S \subseteq (R, +)$$

$$\nexists x, y \in S, xy \in S$$

înăl ideal

Def. $(R, +, \cdot)$ înăl $i \subseteq R$

i ideal (bilateral) al lui R dacă:

1) i subinăl în R

2) $\forall x \in R, \forall r \in R, rx \in i \wedge x \in i \Rightarrow r \in i$

Ex. $\{0\}$, R ideale

P R înăl cu unitate, i ideal dacă $\exists n \in i$ inversabil $\Rightarrow i = R$

P $(R, +, \cdot)$ înăl, $i \subseteq R$. U.a.s.e:

1) i ideal

2) $0 \in i$

$x - y \in i$ (sau $x + y \in i$)

$rx \in i, x \in i, \forall r \in R, \forall x, y \in i$

Def. R înăl

1) $\langle x \rangle = \bigcap_{x \in S} S$ s.n. subinăl generat de x

2) $(x) = \bigcap_{x \in i} i$ s.n. ideal generat de x

3) $(r) = (\{r\})$ s.n. idealul principal generat de r .

4) $(r) = rR = \{rx / x \in R\}$ - idealul generat de r

Domeniu de ideal principal

\hookrightarrow dom. de int. în care fiecare ideal e principal

• T. de caract. a corporilor prin absența idealurilor

$(R, +, \cdot)$ înăl com. cu unitate, $i \subseteq R$

* dacă i ideal $\Rightarrow i = \{0\}$ sau R (inele triviale)

• R esențial: $(R, +, \cdot)$ înăl necom. cu unit. cu propr. *

T. I de izomorfism (inele)

$f: R \rightarrow S$ morfism înăl

1) $\text{Ker } f = \{r \in R / f(r) = 0\}$ ideal

2) $f(R) = \{f(r) / r \in R\}$ subinăl

3) $\bar{f}(r + \text{Ker } f) = f(r)$ izomorfism înăl

T. II de izomorfism (inele)

R -inăl, S subinăl, i ideal

1) $S+i = \{s+x / s \in S, x \in i\}$ subinăl

2) i ideal în $S+i$, $i \cap S$ ideal în S

3) $\frac{S+i}{i} \cong \frac{i}{i \cap S}$

Cörper

$(R, +, \cdot)$ inel cu unitate $\Rightarrow \text{ord}_{(R,+)}(1)$ s. n. $\text{char}(R)$
(caract. inel R)

Ex: $\mathbb{Z}/6 \Rightarrow \text{char}(\mathbb{Z}/6) = 6$

$\mathbb{Z} \Rightarrow \text{char}(\mathbb{Z}) = \infty = \text{char}(0)$

K -corp $\Rightarrow \text{char}(K) = \infty$ / nr. prim

T. Wedderburn: \nexists corp finit e comutativ

T. p -prim, $f \in \mathbb{Z}_p[x]$, grad $f = n > 0$

$\Rightarrow \mathbb{Z}_p[x]/\langle f \rangle$ are p^n elem.

P F -corp finit $\Rightarrow (F^*, \cdot)$ gr. ciclic

p -prim $\Rightarrow (\mathbb{Z}_p^*, \cdot)$ ciclic

T F -corp cu p^n elem.:

a) dacă $K \leq F \Rightarrow \exists d | n$ a.t. $|K| = p^d$

b) $\nexists d | n$, \exists ! K subcorp în F cu p^d elem.