14. Legi de compoziţie

$M =$ mulţime nevidă

„$*$": $M \times M \to M$; $(x, y) \to x * y$ se numeşte **lege de compoziţie internă.**

Exemple: „ + ": $\mathbb{R} \times \mathbb{R}\ (x, y) \to x + y$ adunarea pe $\mathbb{R}$;

„ $\cdot$ ": $\mathbb{R} \times \mathbb{R}\ (x, y) \to x \cdot y$ înmulţirea pe $\mathbb{R}$.

Proprietăţi:

1) Asociativitatea = (A) „$*$" este asociativă dacă

$(\forall) x, y, z \in M$: $(x * y) * z = x * (y * z)$

2) Comutativitatea = (C) „$*$" este comutativă dacă

$(\forall) x, y \in M$: $x * y = y * x$

3) Element neutru = (EN)

$(\exists) e \in M$, astfel încât $x * e = e * x = x$, $(\forall) x \in M$

4) Un element este simetrizabil = (E.S.)

$(\forall) x \in M$, $(\exists) x' \in M$, astfel încât $x * x' = x' * x = e$

Exemplu: „$\cdot$": $\mathbb{R} \times \mathbb{R} \to \mathbb{R}$

1) (A): $(x \cdot y) \cdot z = x \cdot (y \cdot z)$, $(\forall) x, y, z \in \mathbb{R}$;

2) (C): $x \cdot y = y \cdot x$, $(\forall) x, y \in \mathbb{R}$;

3) (E.N.): „$\cdot$" admite elementul neutru $1 \in \mathbb{R}$;

$(\exists) 1 \in \mathbb{R}$ astfel încât $x \cdot 1 = 1 \cdot x = x$, $(\forall) x \in \mathbb{R}$;

4) (E.S.): orice element real nenul este simetrizabil

$(\forall) x \in \mathbb{R}^*$, $(\exists) x' = \frac{1}{x} \in \mathbb{R}$ (inversul lui x), astfel încât $x \cdot \frac{1}{x} = \frac{1}{x} \cdot x = 1$.

Parte stabilă

$M \neq \varnothing$ mulţime: „$*$" : $M \times M \to M$ lege de compoziţie pe M

- $H \subset M$, $H \neq \varnothing$ este ***parte stabilă*** a lui M în raport cu „$*$" dacă:

$(\forall) x, y \in H$ am $x * y \in H$.

Exemplu: $(\mathbb{R}, +)$, $N \subset \mathbb{R}$, N parte stabilă a lui $\mathbb{R}$, în raport cu „+".

Monoizi

$M \neq \varnothing$ mulţime „$*$": $M \times M \to M$ lege de compoziţie pe M

- $(M, *)$ monoid: → „$*$" este (A); → „$*$" admite (E.N.)
- $(M, *)$ monoid: comutativ → $(M, *)$ monoid; → „$*$" este (C)

Exemple: $(\mathbb{N}, +)$; $(\mathbb{Z}, +)$; $(\mathbb{Q}, +)$; $(\mathbb{R}, +)$;
$(\mathbb{N}, \cdot)$; $(\mathbb{Z}, \cdot)$; $(\mathbb{Q}, \cdot)$; $(\mathbb{R}, \cdot)$
sunt monoizi comutativi.

Grupuri

$G \neq \varnothing$ mulţime: „$*$" : $G \times G \to G$ lege de compoziţie

$(G, *)$ se numeşte grup dacă: → „$*$" este (A); → „$*$" are (E.N.); → $(\forall) x \in G$ este (E.S.)

$(G, *)$ se numeşte grup comutativ sau grup abelian **dacă**: → $(G, *)$ grup; → „$*$" este (C)

Exemple: $(\mathbb{Z}, +)$ grupul comutativ al numerelor întregi;
$(\mathbb{Q}^*, \cdot)$ grupul abelian al numerelor raţionale nenule

Grupul claselor de resturi modulo *n*

$\mathbb{Z}_n = \left\{\hat{0}, \hat{1}, \hat{2}, ..., \widehat{n-1}\right\}$ „+": $\mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ $\left(\hat{x}, \hat{y}\right) \to \hat{x} + \hat{y}$; $(\mathbb{Z}_n, +)$ este grup abelian.

Subgrupuri

$(G, *)$ grup, $H \subset G$, $H \neq \varnothing$

- H subgrup al lui G dacă „$*$” induce pe H o lege de compoziţie astfel încât $(H, *)$ grup.

Teoremă: $H \subset G$ subgrup al grupului $(G, *)$ dacă şi numai dacă sunt îndeplinite:

$(\forall)x, y \in H \Rightarrow x * y \in H$;

$(\forall)x \in H \Rightarrow x' \in H$ (unde x' este simetricul lui x în raport cu legea „$*$”).

Exemple: $(\mathbb{Z}, +)$ subgrup al lui $(\mathbb{Q}, +)$ $\quad$ $(\mathbb{Q}, +)$ subgrup al lui $(\mathbb{R}, +)$

$(\mathbb{Z}^*, \cdot)$ subgrup al lui $(\mathbb{Q}^*, \cdot)$ $\quad$ $(\mathbb{Q}^*, \cdot)$ subgrup al lui $(\mathbb{R}^*, \cdot)$

- Fie $(G, *)$ grup. $(H, *)$ subgrup al lui $(G, *)$. Avem:

- Elementul neutru al lui H coincide cu elementul neutru al lui G;

$(\forall)x \in H \Rightarrow x' \in H$;

- Sunt echivalente afirmaţiile:

- H subgrup al lui G;

$(\forall)x, y \in H \Rightarrow xy' \in H$;

$(\forall)x, y \in H \Rightarrow xy \in H$ şi $x' \in H$.

Ordinul unui element: $(G, *)$ grup cu elementul neutru e, $x \in G$.

- Cel mai mic număr natural $n \in \mathbb{N}^*$, cu proprietatea $x^n = e$, se numeşte ordinul elementului x, în grupul G.

Exemple: $(\mathbb{Z}_4, +)$, $e = \hat{0}$: $\hat{1}+\hat{1}+\hat{1}+\hat{1}=\hat{0}$ ord $(\hat{1}) = 4$; $\hat{2}+\hat{2}=\hat{0}$ ord $(\hat{2}) = 2$.

$(\mathbb{Z}_5, \cdot)$, $e = \hat{1}$: $\hat{2}^4 = \hat{1} \Rightarrow$ ord $(\hat{2}) = 4$;

$\hat{3}^4 = \hat{1} \Rightarrow$ ord $(\hat{3}) = 4$;

$\hat{4}^2 = \hat{1} \Rightarrow$ ord $(\hat{4}) = 2$.

Morfisme şi izomorfisme de grupuri

Fie $(G_1,*)$ şi $(G_2,\circ)$ grupuri.

- $f: G_1 \to G_2$ se numeşte **morfism** de grupuri dacă $f(x*y)=f(x)\circ f(y)$.
- Dacă $G_1 = G_2$, atunci f se numeşte **endomorfism.**
- $f: G_1 \to G_2$ morfism de grupuri, e_1, e_2 sunt elemente neutre din grupurile G_1 şi G_2. Atunci:

1) $f(e_1) = e_2$;

2) $f(x') = \left(f(x)\right)'$, $(\forall) x \in G_1$;

3) $f\left(x^n\right)=\left(f(x)\right)^n$, $(\forall) x \in G_1$; $(\forall) n \in \mathbb{Z}$

- $(G_1,*)$ şi $(G_2,\circ)$ grupuri. $f: G_1 \to G_2$ se numeşte **izomorfism** de grupuri dacă:

1) f este bijectivă;

2) f este morfism de grupuri.

- Dacă $G_1 = G_2$, $f: G_1 \to G_1$ îndeplineşte condiţiile de mai sus, se numeşte **automorfism** al lui G_1.
- $f: G_1 \to G_2$ izomorfism de grupuri, atunci $f^{-1}: G_2 \to G_1$ izomorfism de grupuri.

Inele

Fie $I \neq \varnothing$.

$(I,*,\circ)$ se numeşte inel dacă:

→ $(I,*)$ grup abelian

→ $(I,\circ)$ monoid

→ „$\circ$” distributivă faţă de „$*$” →

→ adică: $\begin{cases} x\circ(y*z)=x\circ y * x\circ z \\ (y*z)\circ x = y\circ x * z\circ x \end{cases} (\forall) x,y,z \in I$

Observaţii: Dacă $(I,\circ)$ monoid comutativ, atunci I se numeşte inel comutativ.

Exemplu: $(\mathbb{Z}, +, \cdot)$ inel comutativ; $(\mathbb{R}, +, \cdot)$ inel comutativ.

Fie e_1 elementul neutru al legii „$*$” (al primei legi) şi e_2 elementul neutru al legii „$\circ$” (al celei de-a doua legi).

- I este inel **fără divizori ai lui zero** dacă $x \neq e_1$ şi $y \neq e_1 \Rightarrow x \circ y \neq e_1$;
- I este inel comutativ cu cel puţin două elemente şi fără divizori ai lui zero, atunci I se numeşte **domeniu de integritate**.

Reguli de calcul într-un inel

$(I, *, \circ)$ inel.

1) $(\forall) x \in I, e_1 \circ x = x \circ e_1 = e_1$;

2) $e_1 \neq e_2$ (e_1 elementul neutru al primei legi; e_2 elementul neutru al celei de-a doua legi)

3) Regula semnelor:

$(\forall)$ $x, y \in I$; $(-x) \circ y = x \circ (-y) = -x \circ y$;

$(-x) \circ (-y) = x \circ y$, unde $(-x)$ este elementul simetrizabil al lui x în raport cu prima lege „$*$”

4) $(\forall) x, y, z \in I, x \circ (y - z) = x \circ y - x \circ z$;

$(y - z) \circ x = y \circ x - z \circ x$.

5) I inel fără divizori ai lui zero, $(\forall) x, y, z \in I$; $x \neq e_1$; $x \circ y = x \circ z$ sau $y \circ x = z \circ x$, atunci $y = z$.

Subinele

$(I, *, \circ)$ inel. $M \subset I, M \neq \varnothing$ se numeşte subinel al inelului I, dacă $(M, *, \circ)$ inel.

Exemple: $(\mathbb{Z}^*, +, \cdot)$ subinel al inelului $(\mathbb{C}^*, +, \cdot)$;

$(\mathbb{Q}, +, \cdot)$ subinel al inelului $(\mathbb{R}, +, \cdot)$

Morfisme şi izomorfisme de inele

$(I_1, \perp, \Delta)$ şi $(I_2, *, \circ)$ două inele.

- $f\colon I_1 \to I_2$ este morfism de inele dacă:
  - $f(x \perp y) = f(x) * f(y)$, $(\forall)\, x, y \in I_1$;
  - $f(x \,\Delta\, y) = f(x) \circ f(y)$, $(\forall)\, x, y \in I_1$;
- $f\colon I_1 \to I_1$ morfism de inele se numeşte **endomorfism** al inelului I_1;
- $f\colon I_1 \to I_2$ surjectivă, atunci f se numeşte **morfism unitar** de inele;
- $f\colon I_1 \to I_2$ morfism bijectiv, atunci f se numeşte **izomorfism** de inele;
- $f\colon I_1 \to I_1$ izomorfism, atunci f se numeşte **automorfism**.

Exemplu: $1_{\mathbb{R}} : \mathbb{R} \to \mathbb{R}$ funcţia identică pe A; 1_A este automorfism între $(\mathbb{R}, +, \cdot)$ şi $(\mathbb{R}, +, \cdot)$.

Corpuri

Fie K mulţime nevidă care conține cel puţin două elemente.

$(K, *, \circ)$ corp dacă:
- $(K, *)$ grup abelian
- $(K, \circ)$ grup
- „$\circ$" distributivă faţă de „$*$"

Obs.: $(K, \circ)$ grup abelian $\Rightarrow$ $(K, *, \circ)$ se numeşte ***corp comutativ.***

Exemple: $(\mathbb{Q}^*, +, \cdot)$ corp comutativ;

$(\mathbb{R}^*, +, \cdot)$ corp comutativ;

Proprietăţi:

1) Un corp nu are divizori ai lui zero (este ***domeniu de integritate***);

2) Orice domeniu de integritate finit este corp.

Morfisme şi izomorfisme de corpuri

$(K_1, \perp, \Delta)$ şi $(K_2, *, \circ)$ corpuri.

- $f: K_1 \to K_2$ este morfism de corpuri dacă:
  - $f(x \perp y) = f(x) * f(y), \quad (\forall x, y \in K_1)$;
  - $f(x \Delta y) = f(x) \circ f(y), \quad (\forall x, y \in K_1)$
- $f: K_1 \to K_2$ morfism bijectiv de corpuri, atunci f este **izomorfism** de corpuri;
- $f: K_1 \to K_1$ morfism, se numeşte **endomorfism** al corpului K_1;
- $f: K_1 \to K_1$ izomorfism, se numeşte **automorfism** al corpului K_1.

Teoremă: Orice morfism de corpuri este injectiv.