CURS 1

Grupuri, inele şi corpuri

Definiţia 1. Fie A o mulţime. O funcţie $\varphi : A \times A \to A$ se numeşte **operaţie binară** sau **lege de compoziţie** pe A.

Definiţiile 2. Fie $*$ o operaţie în A. Spunem că:
i) operaţia $*$ este **asociativă** dacă

$$(a_1 * a_2) * a_3 = a_1 * (a_2 * a_3),\ \forall a_1, a_2, a_3 \in A;$$

ii) operaţia $*$ este **comutativă** dacă

$$a_1 * a_2 = a_2 * a_1,\ \forall a_1, a_2 \in A.$$

iii) operaţia $*$ **admite element neutru** dacă există un element $e \in A$ astfel încât

$$a * e = e * a = a,\ \forall a \in A$$

(elementul $e \in A$ se numeşte **element neutru** al lui A relativ la $*$).
iv) Dacă $*$ este o operaţie pe A care are element neutru pe e, spunem că un **element** $a \in A$ este **simetrizabil** dacă există un element $a' \in A$ astfel încât

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

Elementul a' se numeşte **simetricul lui** a.

Terminologie şi notaţii. În notaţie additivă ($* = +$), elementul neutru este notat cu 0 şi numit **element nul (sau zero)**, iar simetricul unui element a (dacă există) este notat cu $-a$ şi este numit **opusul lui** a. În notaţie muliplicativă ($* = \cdot$), elementul neutru este notat cu 1 şi numit **element unitate**, iar simetricul unui element a (dacă există) este notat cu a^{-1} şi e numit **inversul lui** a.

Definiţiile 3. O pereche $(A, *)$ se numeşte **monoid** dacă $*$ este asociativă şi admite element neutru. Dacă, în plus, operaţia $*$ este comutativă spunem că $(A, *)$ este un **monoid comutativ**. Un monoid $(A, *)$ se numeşte **grup** dacă toate elementele sale sunt simetrizabile. Dacă, în plus, operaţia $*$ este comutativă spunem că $(A, *)$ este **grup comutativ** sau **grup abelian**.

Definiţia grupului poate fi rescrisă astfel: $(A, *)$ *se numeşte* ***grup*** *dacă au loc următoarele condiţii:*

(i) $(a_1 * a_2) * a_3 = a_1 * (a_2 * a_3),\ \forall a_1, a_2, a_3 \in A$ *(*$*$ *este asociativă);*

(ii) $\exists e \in A,\ \forall a \in A :\ a * e = e * a = a$ *(*$*$ *admite element neutru);*

(iii) $\forall a \in A,\ \exists a' \in A :\ a * a' = a' * a = e$ *(toate elementele lui* A *sunt simetrizabile).*

Atenţie!!! Câteva greşeli care apar frecvent în definiţia grupului:

1) Condiţia (iii) de mai sus nu vorbeşte depre ,,existenţa elementelor simetrizabile", ci despre faptul că toate elementele sunt simetrizabile. Elemente simetrizabile există şi în monoizi care nu sunt grupuri, de exemplu elementul neutru, dar acolo există şi elemente care nu sunt simetrizabile, iar în grupuri, nu.

2) Ordinea cuantificatorilor în scrierea formală a proprietăţilor (ii) şi (iii) este esenţială. În general, cuantificatorii $\exists$ şi $\forall$ nu comută, iar aici permutarea lor duce la condiţii mult diferite de cele din definiţia grupului.

Definiţiile 4. Fie φ o operaţie pe A şi $B \subseteq A$. Spunem că B este **parte stabilă** a lui A în raport cu φ (sau în (A, φ)) dacă:

$$b_1, b_2 \in B \Rightarrow \varphi(b_1, b_2) \in B.$$

Dacă B este stabilă, atunci se poate defini cu ajutorul lui φ o operaţie pe B astfel:

$$\varphi' : B \times B \to B,\ \varphi'(b_1, b_2) = \varphi(b_1, b_2).$$

Aceasta se numeşte **operaţia indusă** de φ în B şi se notează, de multe ori, tot cu φ.

Observaţiile 5. a) Fie φ o operaţie pe A, $B \subseteq A$ o parte stabilă în (A, φ) şi φ' operaţia indusă de φ în B. Dacă φ este asociativă (comutativă), atunci φ' este asociativă (comutativă).
b) Fie φ_1 şi φ_2 două operaţii definite pe A şi $B \subseteq A$ stabilă în raport cu φ_1 şi φ_2, iar φ_1' şi φ_2' operaţiile induse de φ_1 şi φ_2 în B. Dacă φ_1 este distributivă în raport cu φ_2, adică

$$\varphi_1(a_1, \varphi_2(a_2, a_3)) = \varphi_2(\varphi_1(a_1, a_2), \varphi_1(a_1, a_3))$$

pentru orice $a_1, a_2, a_3 \in A$, atunci φ_1' este distributivă în raport cu φ_2'.
c) Existenţa elementului neutru este o proprietate care, în general, nu ,,se moşteneşte" de la o operaţie la o operaţie indusă. De exemplu, $\mathbb{N}^*$ este o parte stabilă în $(\mathbb{N}, +)$, dar $(\mathbb{N}^*, +)$ nu are element neutru.

Definiţia 6. Fie $(G, \cdot)$ un grup. O submulţime $H \subseteq G$ se numeşte **subgrup** al lui $(G, \cdot)$ dacă verifică condiţiile:
i) H este stabilă în $(G, \cdot)$, adică

$$h_1, h_2 \in H \Rightarrow h_1 h_2 \in H;$$

ii) H este grup în raport cu operaţia indusă de operaţia din $(G, \cdot)$.

Exemplele 7. a) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ sunt subgrupuri în $(\mathbb{C}, +)$, $\mathbb{Z}$, $\mathbb{Q}$ sunt subgrupuri în $(\mathbb{R}, +)$ şi $\mathbb{Z}$ este subgrup în $(\mathbb{Q}, +)$.
b) $\mathbb{Q}^*$, $\mathbb{R}^*$ sunt subgrupuri în $(\mathbb{C}^*, \cdot)$ şi $\mathbb{Q}^*$ este subgrup în $(\mathbb{R}^*, \cdot)$.
c) $\mathbb{N}$ nu este un subgrup al lui $(\mathbb{Z}, +)$.

Definiţia 8. Fie $(G, *)$, $(G', \perp)$ grupuri. O funcţie $f : G \to G'$ se numeşte **morfism** dacă

$$f(x_1 * x_2) = f(x_1) \perp f(x_2),\ \forall\ x_1, x_2 \in G.$$

Un morfism bijectiv se numeşte **izomorfism**. Un morfism al lui $(G, *)$ în el însuşi se numeşte **endomorfism** al lui $(G, *)$. Un izomorfism al lui $(G, *)$ pe el însuşi se numeşte **automorfism** al lui $(G, *)$. Dacă există un izomorfism $f : G \to G$, atunci vom spune că grupurile $(G, *)$ şi $(G', \perp)$ sunt izomorfe şi vom scrie $G \simeq G'$ sau $(G, *) \simeq (G', \perp)$.

Pentru simplificarea scrierii, revenim la notaţia multiplicativă a operaţiilor.

Teorema 9. Fie $(G, \cdot)$ şi $(G', \cdot)$ grupuri, iar 1, respectiv $1'$ elementul neutru al lui $(G, \cdot)$, respectiv $(G', \cdot)$. Dacă $f : G \to G'$ este morfism, atunci:
(a) $f(1) = 1'$;
(b) $f(x^{-1}) = [f(x)]^{-1},\ \forall\ x \in G$.

Demonstraţie.

□

Definiţiile 10. Un triplet $(R, +, \cdot)$ în care R este o mulţime, iar $+$ şi $\cdot$ sunt operaţii pe R se numeşte **inel** dacă verifică următoarele axiome:
i) $(R, +)$ este grup abelian;
ii) Operaţia $\cdot$ este asociativă;
iii) Operaţia $\cdot$ este distributivă faţă de $+$, adică

$$a(b+c) = ab + ac \text{ şi } (b+c)a = ba + ca,\ \forall a, b, c \in \mathbb{R}.$$

Inelul $(R, +, \cdot)$ se numeşte **comutativ**, respectiv **cu unitate** dacă operaţia $\cdot$ este comutativă, respectiv dacă are element unitate (notat cu 1). Dacă $(R, +, \cdot)$ este un inel cu unitate, atunci un element $a \in R$ se numeşte **inversabil** dacă

$$\exists\ a^{-1} \in R :\ a^{-1}a = 1 = aa^{-1}.$$

Uneori inelul $(R, +, \cdot)$ va fi notat cu R.

Observaţiile 11. a) În liceu se foloseşte denumirea de inel pentru ceea ce am numit mai sus inel cu unitate.
b) Dacă $(R, +, \cdot)$ este inel atunci, întrucât $(R, +)$ este grup, rezultă că mulţimea R este nevidă. Conform convenţiilor de termiologie amintite anterior, elementul neutru al grupului $(R, +)$ va fi notat cu 0 şi îl vom numi zero. Vom nota pe $R \setminus \{0\}$ cu R^*. Dacă $a \in R$, atunci opusul (simetricul faţă de $+$) al lui a va fi notat cu $-a$. Întrucât $(R, +)$ este grup abelian, avem

$$-(a+b) = -a - b,\ \forall a, b \in R.$$

Definiţia 12. Un inel cu unitate $(K, +, \cdot)$ se numeşte **corp** dacă:
i) K conţine cel puţin două elemente, adică $|K| \geq 2$.
ii) Orice $a \in K^*$ este inversabil.

Observaţia 13. Un triplet $(K, +, \cdot)$ este corp dacă şi numai dacă:
1) $(K, +)$ este grup abelian.
2) K^* este stabilă în $(K, \cdot)$ şi $(K^*, \cdot)$ este grup.
3) Operaţia $\cdot$ este distributivă în raport cu $+$.

Teorema 14. Dacă $(R, +, \cdot)$ este un inel, atunci pentru orice $a \in R$, funcţiile

$$t_a, t'_a : R \to R,\ t_a(x) = ax,\ t'_a(x) = xa$$

sunt endomorfisme ale grupului $(R, +)$.

Demonstraţie.

□

Corolarul 15. (Reguli de calcul într-un inel) Fie $(R, +, \cdot)$ un inel.
a) Pentru orice $a, b \in R$ au loc egalităţile:

$$a0 = 0 = 0a,\ a(-b) = -ab = (-a)b,\ (-a)(-b) = ab. \tag{1}$$

Primele două (şiruri de) egalităţi din (1) rezultă din teorema de mai sus şi din Teorema 9.

Ultima egalitate se obţine astfel:

$$(-a)(-b) = -((-a)b) = -(-ab) = ab.$$

b) Dacă R este inel asociativ, $a \in R$ şi $n \in \mathbb{N}^*$, atunci

$$(-a)^n = \begin{cases} a^n & \text{dacă } n \text{ este par} \\ -a^n & \text{dacă } n \text{ este impar} \end{cases}$$

c) Dacă $a, b, c \in R$ atunci

$$a(b-c) = ab - ac \text{ şi } (b-c)a = ba - ca.$$

Observaţiile 16. 1) Dacă $(R, +, \cdot)$ este un inel cu unitate, atunci

$$R \neq \{0\} \Leftrightarrow |R| \geq 2 \Leftrightarrow 0 \neq 1.$$

Cum implicaţiile din şirul

$$R \neq \{0\} \Leftarrow |R| \geq 2 \Leftarrow 0 \neq 1$$

sunt evidente, rămâne de demonstrat că $R \neq \{0\}$ implică $0 \neq 1$, adică

$$0 = 1 \Rightarrow R = \{0\}.$$

Într-adevăr,

2) Dacă R este inel cu unitate şi $R \neq \{0\}$, atunci 0 nu este inversabil.

Din (1) rezultă că (într-un inel) dacă într-un produs unul dintre factori este zero, atunci produsul este zero. Inversa acestei afirmaţii nu este, în general, adevărată. Inelele în care această inversă este adevărată constituie o clasă specială de inele.

Definiţia 17. Fie R un inel. Un element $a \in R$, $a \neq 0$ se numeşte **divizor al lui zero** dacă există $b \in R$, $b \neq 0$ astfel încât $ab = 0$ sau $ba = 0$. Un inel $R \neq \{0\}$ comutativ, cu unitate şi care nu conţine divizori ai lui zero (diferiţi de zero) se numeşte **domeniu de integritate**.

Observaţia 18. a) Un inel R nu are divizori ai lui zero dacă şi numai dacă R^* este o parte stabilă în $(R, \cdot)$, adică

$$a, b \in R,\ a \neq 0 \text{ şi } b \neq 0 \Rightarrow ab \neq 0.$$

Menţionăm că implicaţia de mai sus este echivalentă cu

$$a, b \in R,\ ab = 0 \Rightarrow a = 0 \text{ sau } b = 0.$$

b) Corpurile nu au divizori ai lui zero, prin urmare corpurile comutative sunt domenii de integritate.
Într-adevăr, pentru un corp K şi $a, b \in K$,

$$ab = 0 \text{ şi } a \neq 0 \Rightarrow b = 1 \cdot b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0 = 0.$$

Exemplele 19. a) $(\mathbb{Z}, +, \cdot)$ este domeniu de integritate, dar nu este corp, pentru că singurele elemente inversabile din $(\mathbb{Z}, +, \cdot)$ sunt -1 şi 1.
b) $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sunt corpuri comutative.
c) Pe o mulţime formată dintr-un singur element există o singură operaţie. Dacă luăm în calitate de $+$ şi de $\cdot$ această operaţie, atunci se obţine un inel asociativ, comutativ şi cu element unitate. Acesta se numeşte **inelul nul**. În acest inel avem $0 = 1$. Din Observaţia 16 1) rezultă că inelul nul este caracterizat de această egalitate.
d) Fie $n \in \mathbb{N}$, $n \geq 2$. Reamintim **teorema împărţirii cu rest în** $\mathbb{Z}$: *Oricare ar fi numerele întregi a şi b, cu $b \neq 0$, există o singură pereche de numerele întregi $(q, r) \in \mathbb{Z} \times \mathbb{Z}$ astfel încât*

$$a = b \cdot q + r \text{ şi } 0 \leq r < |b|$$

Aceasta permite partiţionarea mulţimii $\mathbb{Z}$ în clase determinate de resturile ce pot fi obţinute prin împărţire la n : $\{n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\}$, unde $r + n\mathbb{Z} = \{r + nk \mid k \in \mathbb{Z}\}$ $(r \in \mathbb{Z})$. Folosim următoarele notaţii

$$\widehat{r} = r + n\mathbb{Z} \ (r \in \mathbb{Z}) \text{ şi } \mathbb{Z}_n = \{n\mathbb{Z}, 1 + n\mathbb{Z}, \ldots, (n-1) + n\mathbb{Z}\} = \{\widehat{0}, \widehat{1}, \ldots, \widehat{n-1}\}.$$

Să observăm că pentru $a, r \in \mathbb{Z}$,

$$\widehat{a} = \widehat{r} \Leftrightarrow a + n\mathbb{Z} = r + n\mathbb{Z} \Leftrightarrow a - r \in n\mathbb{Z} \Leftrightarrow n|a - r.$$

Operaţiile

$$\widehat{a} + \widehat{b} = \widehat{a+b}, \quad \widehat{a}\,\widehat{b} = \widehat{ab}$$

sunt bine definite, adică, dacă se consideră alţi reprezentanţi a' şi b' pentru două clase $\widehat{a}$, respectiv $\widehat{b}$ rezultatele operaţiilor rămân aceleaşi. Într-adevăr, din $a' \in \widehat{a}$ şi $b' \in \widehat{b}$ rezultă

$$n|a' - a,\ n|b' - b \Rightarrow n|a' - a + b' - b \Rightarrow n|(a' + b') - (a + b) \Rightarrow \widehat{a' + b'} = \widehat{a + b}$$

şi

$$a' = a + nk,\ b' = b + nl\ (k, l \in \mathbb{Z}) \Rightarrow a'b' = ab + n(al + bk + nkl) \in ab + n\mathbb{Z} \Rightarrow \widehat{a'b'} = \widehat{ab}.$$

Se verifică uşor că operaţiile $+$ şi $\cdot$ sunt asociative şi comutative, $+$ admite element neutru pe $\widehat{0}$, pentru orice clasă $\widehat{a}$ există un element opus în $(\mathbb{Z}_n, +)$,

$$-\widehat{a} = \widehat{-a} = \widehat{n - a},$$

operaţia $\cdot$ admite element neutru pe $\widehat{1}$ şi este distributivă faţă de $+$. Prin urmare, $(\mathbb{Z}_n, +, \cdot)$ este un inel cu unitate.

Luând, de exemplu $n = 4$, inelul obţinut $(\mathbb{Z}_4, +, \cdot)$ are divizori ai lui zero:

$$\widehat{2} \in \mathbb{Z}_4 \setminus \{\widehat{0}\} = \{\widehat{1}, \widehat{2}, \widehat{3}\} \text{ şi } \widehat{2} \cdot \widehat{2} = \widehat{0}.$$

Prin urmare, inelul $(\mathbb{Z}_n, +, \cdot)$ nu este, în general, un corp. De fapt, $\widehat{a} \in \mathbb{Z}_n$ *este inversabil dacă şi numai dacă* $(a, n) = 1$ (exerciţiu pentru seminar). Rezultă că *inelul* $(\mathbb{Z}_n, +, \cdot)$ *este corp dacă şi numai dacă n este număr prim.*

Definiţia 20. Fie $(R,+,\cdot)$ un inel. O submulţime $A \subseteq R$ se numeşte **subinel** al lui $(R,+,\cdot)$ dacă
i) A este stabilă în raport cu $+$ şi $\cdot$, adică

$$a_1, a_2 \in A \Rightarrow a_1 + a_2 \in A \text{ şi } a_1 a_2 \in A.$$

ii) A este un inel în raport cu operaţiile induse de $+$ şi $\cdot$ din R.

Observaţiile 21. a) Dacă $(R,+,\cdot)$ este inel şi $A \subseteq R$, atunci A este subinel al lui R dacă şi numai dacă A este subgrup al grupului $(R,+)$ şi A este stabilă în $(R,\cdot)$.

Afirmaţia rezultă din definiţiile subinelului şi subgrupului şi din Observaţia 5 b).
b) Dacă A e un subinel al inelului R, atunci elementul nul din $(A,+)$ coincide cu elementul nul din $(R,+)$, iar opusul unui element $a \in A$ în $(A,+)$ coincide cu opusul lui a în $(R,+)$.
c) Orice subinel al unui inel R conţine elementul nul din R.
d) Un subinel A al unui inel cu unitate R, în general, nu conţine unitatea lui R. De exemplu, $(\mathbb{Z},+,\cdot)$ este inel cu unitate şi $2\mathbb{Z}$ este subinel al acestuia, dar $1 \notin 2\mathbb{Z}$.

Exemplele 22. a) Dacă R este un inel, atunci $\{0\}$ şi R sunt subinele ale lui R. Un subinel al lui R diferit de $\{0\}$ şi R se numeşte **propriu**.
b) Fiecare din inelele $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ şi $\mathbb{C}$ este subinel în următoarele.

Definiţia 23. Fie $(K,+,\cdot)$ un corp. O submulţime $A \subseteq K$ se numeşte **subcorp** al lui $(K,+,\cdot)$ dacă
i) A este stabilă în raport cu $+$ şi $\cdot$, adică

$$a_1, a_2 \in A \Rightarrow a_1 + a_2 \in A \text{ şi } a_1 a_2 \in A.$$

ii) A este corp în raport cu operaţiile induse de $+$ şi $\cdot$ din K.

Observaţiile 24. a) Din ii) rezultă că dacă A este subcorp, atunci avem $|A| \geq 2$.
b) Dacă $(K,+,\cdot)$ este corp şi $A \subseteq K$, atunci A este subcorp dacă şi numai dacă A este subgrup în $(K,+)$ şi A^* este subgrup în $(K^*,\cdot)$.
c) Dacă A este subcorp în $(K,+,\cdot)$, atunci $0, 1 \in A$.
d) Dacă $(K,+,\cdot)$ este corp şi $A \subseteq K$, atunci A este subcorp dacă şi numai dacă A este subinel în $(K,+,\cdot)$, $|A| \geq 2$ şi pentru orice $a \in A^*$, $a^{-1} \in A$.

Exemplele 25. a) $\mathbb{Q}$ este subcorp în $\mathbb{R}$ şi în $\mathbb{C}$, iar $\mathbb{R}$ este subcorp în $\mathbb{C}$.
b) Dacă K este corp atunci $\{0\}$ este subinel al lui K, dar nu este subcorp, iar K este un subcorp al lui K.

Definiţia 26. Fie $(R,+,\cdot)$ şi $(R',+,\cdot)$ două inele. O funcţie $f : R \to R'$ se numeşte **morfism (**sau **omomorfism) de inele** dacă pentru orice $x_1, x_2 \in R$,

$$f(x_1 + x_2) = f(x_1) + f(x_2) \text{ şi } f(x_1 x_2) = f(x_1) f(x_2). \tag{2}$$

Un morfism bijectiv de inele se numeşte **izomorfism (de inele)**. Un morfism al lui $(R,+,\cdot)$ în el însuşi se numeşte **endomorfism al inelului** $(R,+,\cdot)$. Un izomorfism al lui $(R,+,\cdot)$ pe el însuşi se numeşte **automorfism al inelului** $(R,+,\cdot)$. Dacă există un izomorfism $f : R \to R'$, atunci se spune că inelele $(R,+,\cdot)$ şi $(R',+,\cdot)$ sunt **izomorfe** şi vom scrie $R \simeq R'$ sau $(R,+,\cdot) \simeq (R',+,\cdot)$.

Fie $(R,+,\cdot)$ şi $(R',+,\cdot)$ inele cu unitate (1 şi $1'$ fiind, respectiv, unităţile lor). Un **morfism** $f : R \to R'$ se numeşte **unital** dacă

$$f(1) = 1' \tag{3}$$

Exemplele 27. a) Dacă $(R,+,\cdot)$ şi $(R',+,\cdot)$ sunt inele, atunci funcţia $\theta : R \to R'$, $\theta(x) = 0$ este un morfism numit **morfismul nul** sau **zero**. Dacă R şi R' sunt cu unitate şi $|R'| \geq 2$, atunci morfismul θ nu este unital.
b) Fie $f : \mathbb{C} \to \mathbb{C}$, $f(z) = \overline{z}$ (unde $\overline{z}$ este conjugatul lui z). Din

$$\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2},\ \overline{z_1 z_2} = \overline{z_1}\,\overline{z_2} \text{ şi } \overline{\overline{z}} = z$$

rezultă că f este un automorfism al corpului $(\mathbb{C},+,\cdot)$ şi $f^{-1} = f$.

Prima condiţie din (2) arată că dacă $f : R \to R'$ este un morfism între inelele $(R,+,\cdot)$ şi $(R',+,\cdot)$, atunci f este morfism al grupului $(R,+)$ în $(R',+)$ prin urmare, avem:

Teorema 28. Fie $(R,+,\cdot)$, $(R',+,\cdot)$ inele şi $f : R \to R'$ un morfism. Atunci

$$f(0) = 0 \text{ şi } f(-x) = -f(x),\ \forall\ x \in R. \tag{4}$$

Dacă R şi R' sunt inele cu unitate, f este morfism unital şi $x \in R$ e inversabil, atunci

$$f(x^{-1}) = [f(x)]^{-1}. \tag{5}$$

Demonstraţie.

□

Observaţia 29. Orice morfism nenul dintre două corpuri este unital.
Într-adevăr,