

CURS 1

Inele și corpuri

Definiția 1. Fie A o mulțime. O funcție $\varphi : A \times A \rightarrow A$ se numește **operație binară** sau **lege de compoziție** pe A .

Definițiile 2. Fie $*$ o operație în A . Spunem că:

i) operația $*$ 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) operația $*$ este **comutativă** dacă

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

iii) operația $*$ **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 numește **element neutru** al lui A relativ la $*$).

iv) Dacă $*$ este o operație 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 numește **simetricul lui** a .

Terminologie și notații. În notație aditivă ($*$ = +), elementul neutru este notat cu 0 și numit **element nul (sau zero)**, iar simetricul unui element a (dacă există) este notat cu $-a$ și este numit **opusul lui** a . În notație multiplicativă ($*$ = \cdot), elementul neutru este notat cu 1 și numit **element unitate**, iar simetricul unui element a (dacă există) este notat cu a^{-1} și e numit **inversul lui** a .

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

Definiția grupului poate fi rescrisă astfel: $(A, *)$ se numește **grup** dacă au loc următoarele condiții:

- (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).

Atenție!!! Câteva greșeli care apar frecvent în definiția grupului:

1) Condiția (iii) de mai sus nu vorbește despre „existența elementelor simetrizabile”, ci despre faptul că toate elementele sunt simetrizabile. Elemente simetrizabile există și în monoizi care nu sunt grupuri, de exemplu elementul neutru, dar acolo există și elemente care nu sunt simetrizabile, iar în grupuri, nu.

2) Ordinea cuantificatorilor în scrierea formală a proprietăților (ii) și (iii) este esențială. În general, cuantificatorii \exists și \forall nu comută, iar aici permutarea lor duce la condiții mult diferite de cele din definiția grupului.

Definițiile 4. Fie φ o operație pe A și $B \subseteq A$. 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 operație pe B astfel:

$$\varphi' : B^2 \rightarrow B, \varphi'(b_1, b_2) = \varphi(b_1, b_2).$$

Aceasta se numește **operația indusă** de φ în B și se notează, de multe ori, tot cu φ .

Observațiile 5. a) Fie φ o operație pe A , $B \subseteq A$ o parte stabilă în (A, φ) și φ' operația indusă de φ în B . Dacă φ este asociativă (comutativă), atunci φ' este asociativă (comutativă).

b) Fie φ_1 și φ_2 două operații definite pe A și $B \subseteq A$ stabilă în raport cu φ_1 și φ_2 , iar φ'_1 și φ'_2 operațiile induse de φ_1 și 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) Existența elementului neutru este o proprietate care, în general, nu „se moștenește” de la o operație la o operație indusă. De exemplu, \mathbb{N}^* este o parte stabilă în $(\mathbb{N}, +)$, dar $(\mathbb{N}^*, +)$ nu are element neutru.

Definiția 6. Fie (G, \cdot) un grup. O submulțime $H \subseteq G$ se numește **subgrup** al lui (G, \cdot) dacă verifică condițiile:

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 operația indusă de operația din (G, \cdot) .

Exemplele 7. a) \mathbb{Z} , \mathbb{Q} , \mathbb{R} sunt subgrupuri în $(\mathbb{C}, +)$, \mathbb{Z} , \mathbb{Q} sunt subgrupuri în $(\mathbb{R}, +)$ și \mathbb{Z} este subgrup în $(\mathbb{Q}, +)$.

b) \mathbb{Q}^* , \mathbb{R}^* sunt subgrupuri în (\mathbb{C}^*, \cdot) și \mathbb{Q}^* este subgrup în (\mathbb{R}^*, \cdot) .

c) \mathbb{N} nu este un subgrup al lui $(\mathbb{Z}, +)$.

Definiția 8. Fie $(G, *)$, (G', \perp) grupuri. O funcție $f : G \rightarrow G'$ se numește **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 numește **izomorfism**. Un morfism al lui $(G, *)$ în el însuși se numește **endomorfism** al lui $(G, *)$. Un izomorfism al lui $(G, *)$ pe el însuși se numește **automorfism** al lui $(G, *)$. Dacă există un izomorfism $f : G \rightarrow G'$, atunci vom spune că grupurile $(G, *)$ și (G', \perp) sunt izomorfe și vom scrie $G \simeq G'$ sau $(G, *) \simeq (G', \perp)$.

Pentru simplificarea scrierii, revenim la notația multiplicativă a operațiilor.

Teorema 9. Fie (G, \cdot) și (G', \cdot) grupuri, iar 1 , respectiv $1'$ elementul neutru al lui (G, \cdot) , respectiv (G', \cdot) . Dacă $f : G \rightarrow G'$ este morfism, atunci:

(a) $f(1) = 1'$;

(b) $f(x^{-1}) = [f(x)]^{-1}, \forall x \in G$.

Demonstrație. Pentru orice $x \in G$ avem

$$f(1)f(x) = f(1 \cdot x) = f(x) = 1' \cdot f(x),$$

adică $f(1)f(x) = 1' \cdot f(x)$, de unde rezultă (a). Folosind pe (a) avem:

$$x^{-1}x = 1 = xx^{-1} \Rightarrow f(x^{-1})f(x) = 1' = f(x)f(x^{-1}),$$

de unde urmează (b). □

Definițiile 10. Un triplet $(R, +, \cdot)$ în care R este o mulțime, iar $+$ și \cdot sunt operații pe R se numește **inel** dacă verifică următoarele axiome:

- i) $(R, +)$ este grup abelian;
- ii) Operația \cdot este asociativă;
- iii) Operația \cdot este distributivă față de $+$, adică

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

Inelul $(R, +, \cdot)$ se numește **comutativ**, respectiv **cu unitate** dacă operația \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 numește **inversabil** dacă

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

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

Observațiile 11. a) În liceu se folosește 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 mulțimea R este nevidă. Conform convențiilor de terminologie amintite anterior, elementul neutru al grupului $(R, +)$ va fi notat cu 0 și îl vom numi zero. Vom nota pe $R \setminus \{0\}$ cu R^* . Dacă $a \in R$, atunci opusul (simetricul față de $+$) al lui a va fi notat cu $-a$. Întrucât $(R, +)$ este grup abelian, avem

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

Definiția 12. Un inel cu unitate $(K, +, \cdot)$ se numește **corp** dacă:

- i) K conține cel puțin două elemente, adică $|K| \geq 2$.
- ii) Orice $a \in K^*$ este inversabil.

Observația 13. Un triplet $(K, +, \cdot)$ este corp dacă și numai dacă:

- 1) $(K, +)$ este grup abelian.
- 2) K^* este stabilă în (K, \cdot) și (K^*, \cdot) este grup.
- 3) Operația \cdot este distributivă în raport cu $+$.

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

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

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

Demonstrație. Pentru orice $x, y \in R$ avem:

$$t_a(x + y) = a(x + y) = ax + ay = t_a(x) + t_a(y),$$

adică t_a este endomorfism al grupului $(R, +)$. Analog se arată că t'_a este endomorfism. \square

Corolarul 15. (Reguli de calcul într-un inel) Fie $(R, +, \cdot)$ un inel.

a) Pentru orice $a, b \in R$ au loc egalitățile:

$$a0 = 0 = 0a, \quad a(-b) = -ab = (-a)b, \quad (-a)(-b) = ab. \quad (1)$$

Primele două (șiruri de) egalități din (1) rezultă din teorema de mai sus și din Teorema 9. Ultima egalitate se obține astfel:

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

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

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

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

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

Cum implicațiile din șirul

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

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

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

Într-adevăr, dacă $0 = 1$, pentru orice $a \in R$,

$$a = a \cdot 1 = a \cdot 0 = 0.$$

2) Dacă R este inel cu unitate și $R \neq \{0\}$, 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 afirmații nu este, în general, adevărată. Inelele în care această inversă este adevărată constituie o clasă specială de inele.

Definiția 17. Fie R un inel. Un element $a \in R$, $a \neq 0$ se numește **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 și care nu conține divizori ai lui zero (diferiți de zero) se numește **domeniu de integritate**.

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

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

Menționăm că implicația 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 și $a, b \in K$,

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

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 și 1 .

b) $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sunt corpuri comutative.

c) Pe o mulțime formată dintr-un singur element există o singură operație. Dacă luăm în calitate de $+$ și de \cdot această operație, atunci se obține un inel asociativ, comutativ și cu element unitate. Acesta se numește **inelul nul**. În acest inel avem $0 = 1$. Din Observația 16 1) rezultă că inelul nul este caracterizat de această egalitate.

d) Fie $n \in \mathbb{N}$, $n \geq 2$. Reamintim **teorema împărțirii cu rest în \mathbb{Z}** : Oricare ar fi numerele întregi a și b , cu $b \neq 0$, există o singură pereche de numere întregi $(q, r) \in \mathbb{Z} \times \mathbb{Z}$ astfel încât

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

Aceasta permite partiționarea mulțimii \mathbb{Z} în clase determinate de resturile ce pot fi obținute prin împărțire la n : $\{n\mathbb{Z}, 1 + n\mathbb{Z}, \dots, (n-1) + n\mathbb{Z}\}$, unde $r + n\mathbb{Z} = \{r + nk \mid k \in \mathbb{Z}\}$ ($r \in \mathbb{Z}$). Folosim următoarele notații

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

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

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

Operațiile

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

sunt bine definite, adică, dacă se consideră alți reprezentanți a' și b' pentru două clase \widehat{a} , respectiv \widehat{b} rezultatele operațiilor rămân aceleași. Într-adevăr, din $a' \in \widehat{a}$ și $b' \in \widehat{b}$ rezultă

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

și

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

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

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

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

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

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

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

Definiția 20. Fie $(R, +, \cdot)$ un inel. O submulțime $A \subseteq R$ se numește **subinel** al lui $(R, +, \cdot)$ dacă i) A este stabilă în raport cu $+$ și \cdot , adică

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

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

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

Afirmația rezultă din definițiile subinelului și subgrupului și din Observația 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 conține elementul nul din R .

d) Un subinel A al unui inel cu unitate R , în general, nu conține unitatea lui R . De exemplu, $(\mathbb{Z}, +, \cdot)$ este inel cu unitate și $2\mathbb{Z}$ este subinel al acestuia, dar $1 \notin 2\mathbb{Z}$.

Exemplele 22. a) Dacă R este un inel, atunci $\{0\}$ și R sunt subinele ale lui R . Un subinel al lui R diferit de $\{0\}$ și R se numește **propriu**.

b) Fiecare din inelele $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ și \mathbb{C} este subinel în următoarele.

Definiția 23. Fie $(K, +, \cdot)$ un corp. O submulțime $A \subseteq K$ se numește **subcorp** al lui $(K, +, \cdot)$ dacă

i) A este stabilă în raport cu $+$ și \cdot , adică

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

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

Observațiile 24. a) Din ii) rezultă că dacă A este subcorp, atunci avem $|A| \geq 2$.

b) Dacă $(K, +, \cdot)$ este corp și $A \subseteq K$, atunci A este subcorp dacă și numai dacă A este subgrup în $(K, +)$ și 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 și $A \subseteq K$, atunci A este subcorp dacă și numai dacă A este subinel în $(K, +, \cdot)$, $|A| \geq 2$ și pentru orice $a \in A^*$, $a^{-1} \in A$.

Exemplele 25. a) \mathbb{Q} este subcorp în \mathbb{R} și 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 .

Definiția 26. Fie $(R, +, \cdot)$ și $(R', +, \cdot)$ două inele. O funcție $f : R \rightarrow R'$ se numește **morfism** (sau **omomorfism**) **de inele** dacă pentru orice $x_1, x_2 \in R$,

$$f(x_1 + x_2) = f(x_1) + f(x_2) \text{ și } f(x_1 x_2) = f(x_1) f(x_2). \quad (2)$$

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

Fie $(R, +, \cdot)$ și $(R', +, \cdot)$ inele cu unitate (1 și $1'$ fiind, respectiv, unitățile lor). Un **morfism** $f : R \rightarrow R'$ se numește **unital** dacă

$$f(1) = 1' \quad (3)$$

Observația 27. Prima condiție din (2) arată că dacă $f : R \rightarrow R'$ este un morfism între inelele $(R, +, \cdot)$ și $(R', +, \cdot)$, atunci f este morfism al grupului $(R, +)$ în $(R', +)$.

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

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

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

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

Demonstrație. Din (1) rezultă că f este un morfism al grupului $(R, +)$ în $(R', +)$ de unde, conform Teoremei 9, rezultă (4). Din

$$xx^{-1} = 1 = x^{-1}x$$

și din (3) urmează

$$f(x)f(x^{-1}) = 1' = f(x^{-1})f(x)$$

ceea ce demonstrează pe (5). □

Exemplele 29. a) Dacă $(R, +, \cdot)$ și $(R', +, \cdot)$ sunt inele, atunci funcția $\theta : R \rightarrow R'$, $\theta(x) = 0$ este un morfism numit **morfismul nul** sau **zero**. Dacă R și R' sunt cu unitate și $|R'| \geq 2$, atunci morfismul θ nu este unital.

b) Fie $f : \mathbb{C} \rightarrow \mathbb{C}$, $f(z) = \bar{z}$ (unde \bar{z} este conjugatul lui z). Din

$$\overline{z_1 + z_2} = \bar{z}_1 + \bar{z}_2, \quad \overline{z_1 z_2} = \bar{z}_1 \bar{z}_2 \text{ și } \bar{\bar{z}} = z$$

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

Observația 30. Orice morfism nenul dintre două corpuri este unital.

Într-adevăr, dacă $(K, +, \cdot)$ și $(K', +, \cdot)$ sunt corpuri, iar $f : K \rightarrow K'$ este un morfism nenul, atunci există $x_0 \in K$ astfel încât $f(x_0) \neq 0$. Cum

$$1 \cdot x_0 = x_0 \Rightarrow f(1)f(x_0) = f(x_0) = 1'f(x_0),$$

înmulțind la dreapta ambii membri cu inversul lui $f(x_0)$, obținem $f(1) = 1'$.