Algebra

2.2. Inele și corpuri

Definiție 2.2.1.

Un inel este un triplet $(R, +, \cdot)$ care constă dintr-o mulțime R împreună cu două operații $+, \cdot : R \times R \to R$, a.î.

(a) $(R, +)$ este un grup abelian

(b) $\cdot$ este asociativă

(c) $\cdot$ este distributivă bilateral în raport cu $+$, adică pentru orice $x, y, z \in \mathbb{R}$ avem:

$$x \cdot (y+z) = xy + xz \quad \text{și} \quad (y+z) \cdot x = yx + zx$$

Inelul R se zice comutativ sau unitar, după cum operația $\cdot$ este și comutativă respectiv are unitate (are element neutru).

Observație 2.2.2.

Într-un inel R se notează cu 0 elementul neutru pentru $+$ și cu 1 elementul neutru pentru $\cdot$ (dacă acesta din urmă) există. Ordinea operațiilor este cea obișnuită, mai precis mai întâi acționează înmulțirea și pe urmă adunarea.

Exemple 2.2.3.

(a) $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sunt inele comutative și unitare deoarece $\cdot$ este comutativă $(x \cdot y = y \cdot x)$ și are element unitar $(e = 1)$

(b) Dacă R este un element comutativ, atunci $(M_{n \times n}(R), +, \cdot)$ este de asemenea inel; totuși $(M_{n \times n}(R), +, \cdot)$ nu este în mod necesar comutativ. Dacă R este unitar atunci așa este și $(M_{n \times n}(R), +, \cdot)$, iar elementul neutru pentru înmulțirea matricilor este așa numita matrice unitate de rank n:

$$I_n = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

(c) Dacă $(R, +)$ este un grup abelian și $(R, +, \cdot)$ este un inel unde $xy = 0 \ \forall \ x, y \in R$ atunci inelul se numește pătrat nul. În particular $R = \{0\}$, acest inel se numește inelul nul și este notat $R = 0$

(d) Dacă $(R, +, \cdot)$ este un inel atunci definim inelul opus $(R^0, +, *)$, unde $R = R^0$ și $x * y = yx \ \forall\ x, y \in R$

Definiție 2.2.5.

Un corp este un inel unitar $(K, +, \cdot)$ cu proprietatea că oricare $x \in K^*$ este inversabil (în raport cu $\cdot$), adică $(K, +)$ și $(K^*, \cdot)$ sunt grupuri abeliene și înmulțirea este distributivă față de adunare $(a \cdot (b+c) = ab + ac \ \forall\ a, b, c \in K)$

Observație 2.2.6.

Un inel K este un corp atunci când $(K^*, \cdot)$ este un grup.

Exemple 2.2.7.

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

(b) $(\mathbb{Z}, +, \cdot)$ nu este un corp pentru că $(\mathbb{Z}^*, \cdot)$ nu are invers.

Subinele și subcorpuri

Definiție 2.2.8.

Fie $(R, +, \cdot)$ un inel. Un subinel a lui R este o submulțime

$S \subseteq R$, cu proprietatea că operațiile $+$ și $\cdot$ din R induc operații bine definite pe S, adică $x, y \in S \Rightarrow$ $\Rightarrow x + y, xy \in S$, se mai spune că S este o parte stabilă în raport cu $+$ și $\cdot$, iar operațiile induse îl fac pe S un inel. Se scrie $S \leq R$. Dacă $1 = R$ atunci se zice unitar un subinel $S \leq R$ cu proprietatea $1 \in S$.

Exemplu 2.2.9.

(1) $\mathbb{Z} \leq \mathbb{Q}$

(2) $2\mathbb{Z} \leq \mathbb{Z}$ și $1 \notin 2\mathbb{Z}$

(3) $\forall$ inel R are subinelele triviale, adică $\{0\}$ și R.

Propoziție 2.2.10.

Fie $(R, +, \cdot)$ un inel și fie $S \subseteq R$ o submulțime.
Următoarele afirmații sunt echivalente:

(i) $S \leq R$

(ii) (a) $0 \in S$

(b) $x, y \in S \Rightarrow x + y \in S$

(c) $x \in S \Rightarrow -x \in S$

(d) $x, y \in S \Rightarrow xy \in S$

(iii) (a) $0 \in S$

(b) $x, y \in H \Rightarrow x - y \in H$

(c) $x, y \in S \Rightarrow xy \in S$

Propoziție 2.2.11.

Fie $(R, +, \cdot)$ un inel. Dacă $S_i \leq R$, $i \in I$ atunci avem

$\bigcap_{i \in I} S_i \leq R$

Observație 2.2.12.

Reuniunea a două sau mai multe subinele nu este cu necesitate subinel

Definiție 2.2.13.

Fie $(K, +, \cdot)$ un corp. Un subcorp a lui K este o submulțime $L \subseteq K$ cu proprietatea că operațiile + și $\cdot$ din R induc operații bine definite pe L, iar cu operațiile induse L formează un corp. Se scrie $L \leq K$.

Observație 2.2.14.

Un subcorp este un subinel comutativ unitar care are inversă.

<u>Propoziție</u> 2.2.15

Fie $(K, +, \cdot)$ un corp și fie $L \subseteq K$ o submulțime.
Următoarele afirmații sunt echivalente:

(i) $L \leq K$

(ii) (a) $0, 1 \in L$

(b) $x, y \in L \Rightarrow x + y \in L$

(c) $x \in L \Rightarrow -x \in L$

(d) $x, y \in L \Rightarrow xy \in L$

(e) $x \in L^* \Rightarrow x^{-1} \in L$

(iii) (a) $0, 1 \in L$

(b) $x, y \in L \Rightarrow x - y \in L$

(c) $x, y \in L^* \Rightarrow xy^{-1} \in L$

Homomorfisme

Definiție 2.2.17.

Un homomorfism de inele (respectiv corpuri) este o funcție $f: R \to S$ ($f: K \to L$), unde R și S (K și L) sunt două inele (corpuri), a.î. $f(x+y) = f(x) + f(y)$ și $f(x \cdot y) = f(x) \cdot f(y)$ pentru $\forall\ x, y \in R$ ($x, y \in K$). Dacă inelele R și S sunt unitare, atunci un homomorfism $f: R \to S$ se zice unitar dacă $f(1_R) = 1_S$. Un homomorfism de inele (corpuri) se numește izomorfism dacă el este și bijectiv. În acest caz, inelele (corpurile) se zic izomorfe și notăm $R \cong S$ ($K \cong L$).

Exemplu 2.2.18.

Pentru două inele (corpuri) R și S funcțiile 1_R și $0: G \to H$, $0(x) = 0$ sunt un izomorfism, respectiv un homomorfism.

Lemă 2.2.19.

Un homomorfism de corpuri este sau unitar sau nul.

Lamă 2.2.20.

Compunerea a două homomorfisme de inele (corpuri) este de asemenea un homomorfism. Funcția inversă a unui izomorfism de inele (corpuri) este de asemenea un izomorfism.