II.4 Inele. Corpuri

II.4.1 Definiţie. Exemple

Definiţia II.4.1.1. *Un inel R este o mulţime, împreună cu două operaţii binare, notate $+ : R \times R \longrightarrow R$, $\cdot : R \times R \longrightarrow R$, astfel încât:*

(R1) $(R, +)$ *este grup abelian.*

(R2) *$(R,\cdot)$ este monoid.*

(R3) *(Distributivitate)* $x \cdot (y + z) = x \cdot y + x \cdot z, (\forall)x, y, z \in \mathbb{R}$, $(x + y) \cdot z = x \cdot z + y \cdot z, (\forall)x, y, z \in \mathbb{R}$

Proprietaţi suplimentare

(i) Inel comutativ: $x \cdot y = y \cdot x, (\forall)x, y \in R$.

(ii) Inel boolean: $x \cdot x = x, (\forall)x \in R$.

(iii) Inel integru: $(\forall)x, y \in R \setminus \{0\},\ x \cdot y \neq 0$ (avem voie să simplificăm la dreapta sau la stânga).

(iv) Corp: $(\forall)x \in R \setminus \{0\}$, x este inversabil în raport cu operaţia $\cdot$.

Exemplul II.4.1.2. *(i)* $(\mathbb{Z}, +, \cdot)$ *este un inel comutativ integru.*

(ii) $(\mathcal{M}_n(\mathbb{R}), +, \cdot)$ *este un inel necomutativ şi cu divizori ai lui zero.*

(iii) $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}_p, +, \cdot)$ *(p prim) sunt corpuri comutative.*

(iv) Există şi corpuri necomutative: corpul cuaternionilor $\mathbb{H}$ (după numele matematicianului W.R. Hamilton), având drept elemente tupluri de forma $q = (a, b, c, d)$ cu $a, b, c, d \in \mathbb{R}$, cu operaţia aditivă - adunarea pe componente. Pentru operaţia multiplicativă, notăm $1 = (1, 0, 0, 0)$, $i = (0, 1, 0, 0)$, $j = (0, 0, 1, 0)$, $k = (0, 0, 0, 1)$. Atunci orice $q \in \mathbb{H}$, $q = (a, b, c, d)$ se mai scrie $q = a \cdot 1 + b \cdot i + c \cdot j + d \cdot k$. Definim operaţia multiplicativă prin:

$$
\begin{aligned}
1 \cdot 1 &= 1 \\
1 \cdot i = i \cdot 1 &= i \\
1 \cdot j = j \cdot 1 &= j \\
1 \cdot k = k \cdot 1 &= k \\
i^2 = j^2 = k^2 &= -1 \\
i \cdot j = -j \cdot i &= k \\
j \cdot k = -k \cdot j &= i \\
k \cdot i = -i \cdot k &= j
\end{aligned}
$$

şi extindem prin liniaritate la toate elementele lui $\mathbb{H}$. Se obţine astfel pe $\mathbb{H}$ o structură de inel necomutativ, în care orice element $q \in \mathbb{H} \setminus \{0\}$ este inversabil, cu inversul: $q^{-1} = \frac{1}{a^2+b^2+c^2+d^2}(a \cdot 1 - b \cdot i - c \cdot j - d \cdot k)$, deci un corp necomutativ.

Teorema II.4.1.3. *Orice corp finit $\mathbb{k}$ este comutativ şi există $p, n \in \mathbb{N}$ cu p prim astfel încât $|\mathbb{k}| = p^n$. Mai mult, oricare două corpuri finite cu acelaşi număr de elemente sunt izomorfe (izomorfism de corpuri: bijecţie care păstrează cele două operaţii, elementele simetrizabile şi inversabilitatea în raport cu operaţiile).*

Un corp finit cu p^n elemente se mai numeste şi corp Galois şi se notează $GF(p^n)$ sau $\mathbb{F}_{p^n}$.

Construcţia unui corp Galois cu p^n elemente: fie $P \in \mathbb{Z}_p[X]$ un polinom ireductibil de grad n; atunci mulţimea resturilor la împărţirea cu P formează corpul dorit în raport cu adunarea şi înmulţirea polinoamelor modulo P.

Pentru $p = 2$, asociind fiecărui polinom $a_0 + a_1X + \ldots + a_{n-1}X^{n-1} \in \mathbb{Z}_2[X]$ secvenţa coeficienţilor săi $(a_0, a_1, \ldots, a_{n-1}) \in (\mathbb{Z}_2)^n$, obţinem o structură de corp pe mulţimea stringurilor binare de lungime n.

Exemplul II.4.1.4. *Corpul $GF(2^3)$ (realizat pe mulţimea $(\mathbb{Z}_2)^3$).*

Căutăm un polinom de grad 3 ireductibil din $\mathbb{Z}_2[X]$; din cele 8 polinoame existente, se verifică uşor că doar X^3+X+1 şi X^3+X^2+1 sunt ireductibile. Alegem de exemplu $P = X^3 + X + 1$. Atunci resturile la împărţirea cu P sunt:

0	000
1	001
X	010
$X+1$	011
X^2	100
X^2+1	101
X^2+X	110
X^2+X+1	111

Pentru adunarea şi multiplicarea modulo P, avem de exemplu

$$\begin{aligned} (X^2+1)+(X^2+X+1) &= 2X^2+X+2 \\ &= X(mod\ P) \end{aligned}$$

şi

$$\begin{aligned} (X^2+1)(X^2+X+1) &= X^4+X^3+X^2+X^2+X+1 \\ &= X^4+2X^2 \\ &= X^4 \\ &= X^2+X(mod\ P) \end{aligned}$$

Exerciţiul II.4.1.5. *Scrieţi tabla înmulţirii în* $(\mathbb{Z}_2)^3$ *folosind corespondenţa de mai sus şi verificaţi că orice string diferit de* 000 *este inversabil.*

Fie acum $\mathbb{k}$ un corp şi $\mathbb{k}[X] = \{a_0 + a_1X + \ldots + a_nX^n \mid a_0, a_1, a_n \in \mathbb{k}, n \in \mathbb{N}\}$ inelul polinoamelor cu coeficienţi în $\mathbb{k}$.
Proprietăţi:

(i) $\mathbb{k}[X]$ inel integru.

(ii) (Teorema împărţirii cu rest) $(\forall)P, Q \in \mathbb{k}[X], Q \neq 0$, există în mod unic două polinoame $C, R \in \mathbb{k}[X]$, astfel încât $gradR < gradQ$ şi $P = Q \cdot C + R$.

(iii) (Teorema lui Bezout) Fie $P \in \mathbb{k}[X]$, $a \in \mathbb{k}$. Atunci $P(a) = 0 \Leftrightarrow X - a \mid P$.

(iv) $P \in \mathbb{k}[X]$, $gradP = n \Longrightarrow P$ are cel mult n rădăcini.

Consecinţa II.4.1.6. *Orice funcţie* $f : \mathbb{k} \longrightarrow \mathbb{k}$, *unde* $\mathbb{k}$ *este un corp finit, este polinomială (soluţie: polinomul de interpolare Lagrange).*

II.4.2 Aplicaţie în criptografie. Secret Sharing

Este metoda de a distribui un secret la un grup de participanţi, fiecărui participant fiindu-i atribuită câte o parte a secretului[1]. Secretul poate fi reconstituit doar prin combinarea a cel puţin un număr fixat de participanţi. Ideea: aşa cum două puncte din plan determină în mod unic o dreaptă(deci o funcţie de gradul I), 3 puncte determină o parabolă(o funcţie de gradul II), etc., k puncte în plan vor determina în mod unic un polinom de grad $k-1$. Fie n numărul participanţilor, $k < n$ şi S mesajul secret(un element dintr-un corp finit $\mathbb{k}$). Alegem la întâmplare $k-1$ elemente $a_1, a_2, a_3, ..., a_{k-1} \in \mathbb{k}$ şi luăm $a_0 = S$. Construim polinomul

$$P(X) = a_0 + a_1X + \ldots + a_{k-1}X^{k-1}$$

şi calculăm $(i, P(i))$ pentru $i = \overline{1, n}$ (deci corpul $\mathbb{k}$ va avea mai mult de n elemente). Fiecărui participant i se atribuie o pereche $(i, P(i))$ de elemente din corpul $\mathbb{k}$ (cunoscut de toţi). Fiind dat orice grup de k participanţi se poate reconstitui polinomul şi afla mesajul secret $S = a_0$.

Exemplul II.4.2.1. *Fie* $n = 5$, $k = 3$, $P = \hat{2}X^2 + \hat{7}X + \hat{10} \in \mathbb{k} = \mathbb{Z}_{11}$. *Secretul este* $S = \hat{10}$. *Mesajele participanţilor sunt:* $P(\hat{1}) = \hat{8}$, $P(\hat{2}) = \hat{10}$,

[1] A. Shamir, 1979.

$P(\hat{3}) = \hat{5}$, $f(\hat{4}) = \hat{4}$, $P(\hat{7}) = \hat{7}$. Alegem grupul de participanţi $(1, 2, 4)$. *Atunci polinomul reconstruit este:*

$$P(X) = \hat{8} \cdot \frac{(X-\hat{2})(X-\hat{4})}{(\hat{1}-\hat{2})(\hat{1}-\hat{4})} + \hat{10} \cdot \frac{(X-\hat{1})(X-\hat{4})}{(\hat{2}-\hat{1})(\hat{2}-\hat{4})} + \hat{4} \cdot \frac{(X-\hat{1})(X-\hat{2})}{(\hat{4}-\hat{1})(\hat{4}-\hat{1})}$$

şi

$$\begin{aligned} S &= P(0) \\ &= \hat{8} \cdot \hat{2} \cdot \hat{4} \cdot \hat{10}^{-1} \cdot \hat{8}^{-1} + \hat{10} \cdot \hat{1} \cdot \hat{4} \cdot \hat{1}^{-1} \cdot \hat{9}^{-1} + \hat{4} \cdot \hat{1} \cdot \hat{2} \cdot \hat{3}^{-1} \cdot \hat{2}^{-1} \\ &= \hat{8} \cdot \hat{2} \cdot \hat{4} \cdot \hat{10} \cdot \hat{7} + \hat{10} \cdot \hat{1} \cdot \hat{4} \cdot \hat{1} \cdot \hat{5} + \hat{4} \cdot \hat{1} \cdot \hat{2} \cdot \hat{4} \cdot \hat{6} \\ &= \hat{3} + \hat{2} + \hat{5} \\ &= \hat{10} \end{aligned}$$

Aplicatii Corpuri Galois

$P = X^3 + X + 1$

$X^4 \bmod P = X\ X^3 \bmod P = X(X^3 + X + 1 - X - 1) \bmod P = [X(X^3 + X + 1) + X(- X - 1)] \bmod P = X(X+1) \bmod P = X^2 + X$

$X(X^3 + X + 1) \bmod P = 0$

In CG(2^4) = GF(2^4)

$P = X^4 + X + 1$

Adunarea

$(X^3 + X^2 + X) + (X^3 + X^2) = 2X^3 + 2X^2 + X = X \bmod P = X$

$(X^3 + X) + (X^2 + X + 1) = X^3 + X^2 + X + X + 1 = (X^3 + X^2 + 1) \bmod P$

Inmultirea

$(X^3 + X^2 + X)(X^2 + 1) = (X^5 + X^4 + X^3 + X^3 + X^2 + X) \bmod P =$

$(X^5 + X^4 + X^2 + X) \bmod P = [X^5 + X^2 + (X^4 + X + 1) - 1] \bmod P =$

$(X^5 + X^2 + 1) \bmod P = (X\ X^4 + X^2 + 1) \bmod P = [X(X^4 + X + 1 - X - 1) + X^2 + 1] \bmod P = [X(X^4 + X + 1) + X(X+1) + X^2 + 1] \bmod P = [X^2 + X^2 + X + 1] \bmod P = (X + 1) \bmod P$

Deci $(X^3 + X^2 + X)(X^2 + 1) \bmod P = (X + 1) \bmod P$

In CG(3^2)

$P = X^2 + 1$

$(2X + 1)(X+2) \bmod P = (2X^2 + 5X + 2) \bmod P = (2X^2 + 2) \bmod P + 2X \bmod P = 2X \bmod P$

$P1 = X^2 + 2X + 2$

$(2X + 1)(X+2) \bmod P1 = (2X^2 + 5X + 2) \bmod P1 = (2X^2 + 2X + 2) \bmod P1 =$

$(X^2 + 2X + 2) \bmod P1 + X^2 \bmod P1 = X^2 \bmod P1 = (X^2 + 2X + 2 - 2X - 2) \bmod P1 =$

$(X^2 + 2X + 2) \bmod P1 + (-2X - 2) \bmod P1 = (X + 1) \bmod P1$