Structuri algebrice II

Inele și corpuri

Def: $(A,+,\cdot)$ este <u>inel</u> dacă:

- $(A,+)$ grup abelian: $-\ \forall x,y\in A: x+y\in A$
  $-\ \forall x,y,z\in A: (x+y)+z=x+(y+z)$
  $-\ \exists 0_A\in A: x+0_A=0_A+x=x,\ \forall x\in A$
  $-\ \forall x\in A,\ \exists x'\in A: x+x'=x'+x=0_A$
  $-\ \forall x,y\in A: x+y=y+x$
- $(A,\cdot)$ monoid: $-\ \forall x,y\in A: x\cdot y\in A$
  $-\ \forall x,y,z\in A: (x\cdot y)\cdot z=x\cdot(y\cdot z)$
  $-\ \exists 1_A\in A: x\cdot 1_A=1_A\cdot x=x,\ \forall x\in A$
- Distributivitatea: $-\ \forall x,y,z\in A: x\cdot(y+z)=x\cdot y+x\cdot z$
  $(y+z)\cdot x=y\cdot x+z\cdot x$

Exemple: $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{C},+,\cdot)$

$(\mathbb{Z}_n,+,\cdot)$, $(\mathcal{M}_n(A),+,\cdot)$
↳ inel

$A^M=\{f: M\to A\}$, $M\neq\varnothing$ multime
A - inel

$(A^M,+,\cdot)$ $\qquad (f+g)(x)=f(x)+g(x)$
$(f\cdot g)(x)=f(x)\cdot g(x)$

Def: A inel

$$U(A)=A^\times=\{x\in A\mid \exists x'\in A: x\cdot x'=x'\cdot x=1_A\}$$

Exemple: $U(\mathbb{Z},+,\cdot)=\{-1,1\}$

$U(\mathbb{Q},+,\cdot)=\mathbb{Q}\setminus\{0\}=\mathbb{Q}^*$

$U(\mathbb{R},+,\cdot)=\mathbb{R}^*$

$U(\mathbb{C},+,\cdot)=\mathbb{C}^*$

$U(\mathbb{Z}_n,+,\cdot)=\{\hat{k} \mid (k,n)=1\}$

$U(\mathcal{M}_n(A),+,\cdot)=\{B\in\mathcal{M}_n(A) \mid \det(B)\in U(A)\}$

↳ inel

Teorema (Bézout): $a,b\in\mathbb{Z}$ cu $(a,b)=d \Rightarrow \exists \alpha,\beta\in\mathbb{Z}$ a.î.

$$\boxed{\alpha\cdot a+\beta\cdot b=d}$$

Exercițiul 1: Fie $\alpha\in\mathbb{Z}^*$. Pe mulțimea $\mathbb{Z}$ definim operațiile:

$$x\oplus y=x+y+\alpha$$

$$x\odot y=(x-2)(y-2)+2$$

Atunci:

[A] 0 este elementul neutru al operației $\oplus$ (F)

[B] operația $\odot$ este asociativă (A)

[C] $(\mathbb{Z},\oplus,\odot)$ este inel dacă și numai dacă $\alpha=2$ (F)

[D] $x\in\mathbb{Z}$ este inversabil față de $\odot$ dacă și numai dacă $x=3$. (F)

Soluție: [A] $e\in\mathbb{Z}$ este elementul neutru pentru $\oplus$ dacă $\forall x\in\mathbb{Z}$:

$$x\oplus e=e\oplus x=x$$

$x\oplus e=x \Leftrightarrow x+e+\alpha=x \Leftrightarrow e+\alpha=0 \Leftrightarrow e=-\alpha \Rightarrow$

$\Rightarrow -\alpha$ este singurul element neutru al lui $\oplus$ cu $\alpha\in\mathbb{Z}^*$

[B] $\odot$ asociativă dacă $\forall x,y,z\in\mathbb{Z}: (x\odot y)\odot z=x\odot(y\odot z)$

R: $x \odot y = (x-2)(y-2)+2$

$(x \odot y) \odot z = [(x-2)(y-2)+2] \odot z = [(x-2)(y-2)+\alpha-2](z-2)+2 =$

$=\!\!=\!\!=$ $(x-2)(y-2)(z-2)+2$

$x \odot (y \odot z) = x \odot [(y-2)(z-2)+2] = (x-2)[(y-2)(z-2)+\alpha-2]+2 =$

$(x-2)(y-2)(z-2)+2$

C] $(\mathbb{Z}, \oplus, \odot)$ inel dacă: $(\mathbb{Z}, \oplus)$ grup abelian { - parte stab. - asoc. - elem. neutru: $-\alpha$ - elem. simet. - com. } ✓

$(\mathbb{Z}, \odot)$ monoid { - parte stab. ✓ }

Distributivitatea { - asoc. ✓ - elem. id. ? ✓ }

$e \in \mathbb{Z}$ elementul identitate pentru $\odot$ dacă $\forall x \in \mathbb{Z}$:

$e \odot x = x \odot e = x$

$x \odot e = x \Leftrightarrow (x-2)(e-2)+2 = x \Leftrightarrow (x-2)(e-2)+2-x = 0 \Leftrightarrow$

$\Leftrightarrow (x-2)(e-2)-(x-2) = 0 \Leftrightarrow (x-2)(e-2-1) = 0 \Leftrightarrow e-2-1 = 0 \Leftrightarrow$

$\Leftrightarrow e-3 = 0 \Leftrightarrow e = 3 \in \mathbb{Z}$

Distributivitatea: $x \odot (y \oplus z) = x \odot y \oplus x \odot z$

$(y \oplus z) \odot x = y \odot x \oplus z \odot x$, $\forall x, y, z \in \mathbb{Z}$

$x \odot (y \oplus z) = x \odot [y+z+\alpha] = (x-2)(y+z+\alpha-2)+2$

$(x \odot y) \oplus (x \odot z) = [(x-2)(y-2)+2] \oplus [(x-2)(z-2)+2]$

$= (x-2)(y-2)+2+(x-2)(z-2)+2+\alpha$

$(x-2)(y+z+\alpha-2)+2 = (x-2)(y-2)+2+(x-2)(z-2)+2+\alpha$

$\Leftrightarrow (x-2)(y+z+\alpha-2)-(x-2)(y-2)-(x-2)(z-2)+2-2 = \alpha+2$

$\Leftrightarrow (x-2)[y+z+\alpha-2-(y-2)-(z-2)] = \alpha+2$

$\Leftrightarrow (x-2)(y+z+\alpha-2-y+2-z+2) = \alpha+2$

$\Leftrightarrow (x-2)(\alpha+2) = \alpha+2 \Leftrightarrow (x-2)(\alpha+2) - (\alpha+2) = 0$

$\Leftrightarrow (\alpha+2)(x-2-1) = 0 \Leftrightarrow (\alpha+2)(x-3) = 0. \Leftrightarrow \alpha+2 = 0 \Rightarrow \alpha = -2$

Dacă $\alpha = -2 \Rightarrow (\mathbb{Z}, \oplus, \odot)$ inel

D $x \in \mathbb{Z}$ inversabil față de $\odot$ dacă $\exists\, x' \in \mathbb{Z}$: $x \odot x' = x' \odot x = 3$

$x \odot x' = 3 \Leftrightarrow (x-2)(x'-2)+2 = 3 \Leftrightarrow \underbrace{(x-2)}_{\in \mathbb{Z}}\underbrace{(x'-2)}_{\in \mathbb{Z}} = 1$

$(x-2) \in \{1, -1\} \Leftrightarrow x \in \{3, 1\}$

Dacă $x \in \{3, 1\} \Rightarrow x$ este inversabil.

Exercițiul 2: Considerăm ecuația: $\hat{3}\cdot x + \hat{2} = \hat{7}$ în inelul $\mathbb{Z}_8$.

Atunci:

A ecuația are soluție unică (A)

B $x \in \{\hat{3}, -\hat{3}\}$ (F)

C ecuația inițială are aceleași soluții ca: $\hat{2}\cdot x + \hat{3} = \hat{7}$ (F)

D elementul $\hat{7}$ este inversabil în $\mathbb{Z}_8$ (A)

Soluție: $\mathbb{Z}_8 = \{\hat{0}, \hat{1}, \hat{2}, \dots, \hat{7}\}$

A $\hat{3}\cdot x + \hat{2} = \hat{7} \Leftrightarrow \hat{3}\cdot x = \hat{5}$

R: $U(\mathbb{Z}_n, +, \cdot) = \{\hat{k} \mid (k, n) = 1\}$

$(3, 8) = 1$ (A) $\Rightarrow \exists\, \hat{3}^{-1} \in \mathbb{Z}_8$, unde $\hat{3}^{-1} = \hat{3}$ ($\hat{3}\cdot\hat{3} = \hat{9} \equiv \hat{1}$ ← elem. id.)

$\hat{3} \mid \hat{3}\cdot x = \hat{5} \Rightarrow x = \hat{3}\cdot\hat{5} = \hat{15} \equiv \hat{7}$

C) $\hat{2}\cdot x+\hat{3}=\hat{7} \Leftrightarrow \hat{2}\cdot x=\hat{4} \Rightarrow x\in\{\hat{2},\hat{6}\}$

$\hat{2}\cdot\hat{2}=\hat{4}$

$\hat{2}\cdot\hat{6}=\hat{12}=\hat{4}$

D) $(7,8)=1$ (A) $\Rightarrow \hat{7}$ - inversabil în $\mathbb{Z}_8$

Teoremă (Euler): $n\in\mathbb{N}^*$, $a\in U(\mathbb{Z}_n)$:

$$\boxed{a^{\varphi(n)}=\hat{1}} \text{ în } \mathbb{Z}_n, \text{ unde}$$

$$\varphi(n)=|\{k<n \mid (k,n)=1\}|=|U(\mathbb{Z}_n)|$$

↳ numărul elementelor inversabile din $\mathbb{Z}_n$.

Obs: Dacă $n=p$ - nr. prim, atunci $\varphi(p)=p-1$ și $a^{\varphi(p)}=\hat{1}$ în $\mathbb{Z}_p$.

Obs: $n=p_1^{\alpha_1}\cdot p_2^{\alpha_2}\cdot\ldots\cdot p_k^{\alpha_k} \Rightarrow \varphi(n)=n\cdot\left(1-\frac{1}{p_1}\right)\cdot\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_k}\right)$

Exercițiul 3: Fie elementul $\hat{8}$ în $\mathbb{Z}_{15}$.

A) $\hat{8}^2+\hat{8}-\hat{1}=\hat{11}$ (A)

B) $\hat{8}^{10}=\hat{1}$ (F)

C) $\hat{8}^{2021}=\hat{8}$ (A)

D) $\hat{8}^{576}+\hat{8}^{236}=\hat{3}$ (A)

Soluție: A) $\hat{8}^2+\hat{8}-\hat{1}=\hat{64}+\hat{8}-\hat{1}=\hat{71}\equiv\hat{11}$

B) $(8,15)=1 \Rightarrow \hat{8}$ - inversabil în $\mathbb{Z}_{15}$.

$\hat{8}^{\varphi(15)}=\hat{1} \Rightarrow \hat{8}^8=\hat{1}$

$15=3\cdot5 \Rightarrow \varphi(15)=15\cdot\left(1-\frac{1}{3}\right)\cdot\left(1-\frac{1}{5}\right)=15\cdot\frac{2}{3}\cdot\frac{4}{5}=8$

$\hat{8}^{16} = \underbrace{\hat{8}^{8}}_{\hat{1}} \cdot \hat{8}^{2} = \hat{8}^{2} = \hat{64} = \hat{4}$

$2021 : 8 = 252 \quad r = 5$

C $\hat{8}^{2021} = \underbrace{\left(\hat{8}^{8}\right)^{252}}_{\hat{1}} \cdot \hat{8}^{5} = \hat{8}^{5} = \underbrace{\hat{8}^{2}}_{\hat{4}} \cdot \underbrace{\hat{8}^{2}}_{\hat{4}} \cdot \hat{8} = \underbrace{\hat{16}}_{\hat{1}} \cdot \hat{8} = \hat{8}$

D $\underbrace{\hat{8}^{567}}_{\left(\hat{8}^{8}\right)^{70}\cdot\hat{8}^{7}} + \underbrace{\hat{8}^{236}}_{\left(\hat{8}^{8}\right)^{29}\cdot\hat{8}^{4}} = \left(\hat{8}^{8}\right)^{70} \cdot \hat{8}^{7} + \left(\hat{8}^{8}\right)^{29} \cdot \hat{8}^{4}$

$= \hat{8}^{7} + \hat{8}^{4} = \hat{8}^{5} \cdot \hat{8}^{2} + \hat{8}^{2} \cdot \hat{8}^{2}$

$= \hat{8} \cdot \hat{4} + \hat{4} \cdot \hat{4}$

$= \hat{32} + \hat{16}$

$= \hat{2} + \hat{1} = \hat{3}.$