13.03.2021

Structuri algebrice II
Inele și corpuri

Def: $(A,+,\cdot)$ ("anneau") este **inel** dacă:

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

Exemple: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \boxed{\mathbb{Z}_n}, \mathcal{M}_n(A)$, A inel

$A^M = \{ f : M \to A \}$, $M \neq \emptyset$ mulțime, A inel

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

$\quad f\cdot g = x \mapsto f(x)\cdot g(x)$

Def: A inel,

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

Ex.: $U(\mathbb{Z}) = \{-1, +1\}$, $U(\mathbb{Q}) = \mathbb{Q} \setminus \{0\}$

$U(\mathbb{Z}_n) = \{ \hat{k} \mid (k,n) = 1 \}$, $U(\mathcal{M}_n(A)) = \{ X \in \mathcal{M}_n(A) \mid \det(X) \in U(A) \}$

Teoremă (Bézout): $a,b \in \mathbb{Z}$, $(a,b) = d \Rightarrow \exists\, \alpha, \beta \in \mathbb{Z}: \ \alpha a + \beta b = d$

E 1. Fie $\alpha \in \mathbb{Z} \setminus \{0\}$. Pe mulțimea $\mathbb{Z}$ definim operațiile:

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

Atunci:

$\boxed{A}$ 0 este elementul neutru al operației $\oplus$

$\boxed{B}$ operația $\odot$ este asociativă

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

$\boxed{D}$ $x \in \mathbb{Z}$ este inversabil față de legea $\odot$ dacă și numai dacă $x = 3$

R: $e \in \mathbb{Z}$ este element neutru pt. $\oplus$ dacă $\forall x \in \mathbb{Z}$:

$$x \oplus e = x$$

$x \oplus e = x \iff x + e + \alpha = x \iff e + \alpha = 0 \iff e = -\alpha$

$\Rightarrow$ $-\alpha$ este singurul element neutru al operației $\oplus$

$\alpha \neq 0 \Rightarrow \boxed{A}$ fals

$\odot$ este asociativă $\iff \forall x, y, z \in \mathbb{Z}$: $(x \odot y) \odot z = x \cdot (y \odot z)$

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

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

$\Rightarrow \forall x, y, z \in \mathbb{Z}$: $(x \odot y) \odot z = x \cdot (y \odot z) \Rightarrow \boxed{B}$ adevărată

$(\mathbb{Z}, \oplus, \odot)$ <u>inel</u> : $(\mathbb{Z}, \oplus)$ grup abelian ✓

$(\mathbb{Z}, \odot)$ monoid ? ✓

e element neutru pt $\odot$: $\forall x \in \mathbb{Z}: \ x \odot e = e \odot x = x$

$$x \odot e = x \iff (x-2)(e-2)+2 = x \iff (x-2)(e-2) = x-2 \iff$$
$$\iff (x-2)(e-2) - (x-2) = 0 \iff (x-2)(e-3) = 0$$

Această afirmație trebuie să fie adevărată pentru orice $x \in \mathbb{Z}$, deci elementul neutru pentru $\odot$ este $e = 3$.

Rămâne de studiat distributivitatea: $\forall x,y,z \in \mathbb{Z}: \ x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z)$

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

Pentru ca distributivitatea să funcționeze, trebuie să avem $\forall x,y,z \in \mathbb{Z}$:

$$(x-2)\cdot(y+z+\alpha-2)+2 = (x-2)(y-2)+2 + (x-2)(z-2)+2+\alpha$$
$$\iff (x-2)(y+z+\alpha-2-y+2-z+2) = \alpha+2 \iff$$
$$\iff (x-2)\cdot(\alpha+2) = \alpha+2 \iff$$
$$\iff (\alpha+2)(x-3) = 0$$

$\Rightarrow (\mathbb{Z}, \oplus, \odot)$ inel $\iff \alpha = -2 \Rightarrow \boxed{C}$ este falsă

$x \in \mathbb{Z}$ este inversabil față de $\odot \iff \exists x' \in \mathbb{Z}: x \odot x' = 3$

$$x \odot x' = 3 \iff (x-2)(x'-2)+2 = 3 \iff (x-2)(x'-2) = 1$$

Deci $x \in \mathbb{Z}$ este inversabil $\iff x-2 \in \{1,-1\} \iff x \in \{3,1\} \Rightarrow \boxed{D}$ falsă

E2. Considerăm ecuația $\hat{3} \cdot x + \hat{2} = \hat{7}$ în inelul $\mathbb{Z}_8$

Atunci:

$\boxed{A}$. ecuația are soluție unică

$\boxed{B}$. $x \in \{\hat{3}, \widehat{-3}\}$

$\boxed{C}$. ecuația are aceleași soluții ca:

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

$\boxed{D}$ elementul $\hat{7}$ este inversabil în $\mathbb{Z}_8$

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

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

$$(3, 8) = 1 \Rightarrow \exists\ \hat{3}^{-1} \in \mathbb{Z}_8 \text{ și } \hat{3} = \hat{3}^{-1}$$

$$\Rightarrow \hat{3}^{-1} \cdot \hat{3} \cdot x = \hat{5} \Rightarrow x = \hat{3} \cdot \hat{5} = \widehat{15} = -\hat{1} = \hat{7}$$

$\Rightarrow \boxed{A}$ adev., $\boxed{B}$ falsă

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

$$(\Leftrightarrow 2x - 4 \equiv 0 \pmod 8))$$

$\Rightarrow \boxed{C}$ falsă

$\boxed{D}$ adevărată, pt. că $(7, 8) = 1$

Teoremă (Euler): $n \in \mathbb{N}^*$, $a \in U(\mathbb{Z}_n)$: $a^{\varphi(n)} = \hat{1}$ în $\mathbb{Z}_n$

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

În particular, dacă $n = p$ prim: $\varphi(p) = p-1$, $a^{\varphi(p)} = 1$ în $\mathbb{Z}_p$

<u>Obs.</u>: $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, $\boxed{\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right)}$

$$\downarrow$$

$$\varphi(n) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right) \cdots \left(p_k^{\alpha_k} - p_k^{\alpha_k - 1}\right)$$

wiki: Euler's totient function

E3. Fie elementul $\hat{8} \in \mathbb{Z}_{15}$.

$\boxed{A}$ $\hat{8}^2 + \hat{8} - \hat{1} = \widehat{11}$

$\boxed{B}$ $\hat{8}^{10} = \hat{1}$

$\boxed{C}$ $\hat{8}^{2021} = \hat{8}$

$\boxed{D}$ $\hat{8}^{567} + \hat{8}^{236} = \hat{3}$

R: $\hat{8}^2 + \hat{8} - \hat{1} = \widehat{64} + \hat{8} - \hat{1} = \widehat{71} = \widehat{11} \Rightarrow \boxed{A}$ adevărată

Din t. lui Euler $\varphi(15) = 15\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 15 \cdot \frac{2}{3} \cdot \frac{4}{5} = 8$

$\Rightarrow$ În $\mathbb{Z}_{15}$ avem: $a^8 = 1$, $\forall a \in U(\mathbb{Z}_{15})$

$\hat{8}^{10} = \underbrace{\hat{8}^8}_{\hat{1}} \cdot \hat{8}^2 = \hat{8}^2 = \widehat{64} = \hat{4} \neq \hat{1} \Rightarrow \boxed{B}$ falsă

$\hat{8}^{2021} = (\underbrace{\hat{8}^8}_{= \hat{1}})^{252} \cdot \hat{8}^5 = \hat{8}^5 = \hat{2}^{15} = \widehat{1024} \cdot \widehat{32} = \hat{4} \cdot \hat{2} = \hat{8} \Rightarrow \boxed{C}$ adevărată

$\hat{8}^{567} + \hat{8}^{236} = \left(\hat{8}^8\right)^{70} \cdot \hat{8}^7 + \left(\hat{8}^8\right)^{29} \cdot \hat{8}^4 = \hat{8}^7 + \hat{8}^4 = \hat{8} \cdot \hat{8}^6 + \widehat{64}^2 =$

$= \hat{8} \cdot \widehat{64}^3 + \widehat{64}^2 = \hat{8} \cdot \hat{4}^3 + \hat{4}^2 = \widehat{512} + \widehat{16} = \widehat{528} = \hat{3}$

$\Rightarrow \boxed{D}$ adevărată