Inele și corpuri

Inel: $(R,+,\cdot)$ a.î. $(R,+)$ grup abelian $\begin{cases} \text{ass: } (x+y)+z = x+(y+z) & \forall x,y,z\in R \\ \text{com: } x+y = y+x \\ \exists\, 0\in R : x+0 = x = 0+x, \forall x\in R \\ \forall x\in R\ \exists -x\in R : x+(-x)=0=(-x)+x \end{cases}$

$(R,\cdot)$ monoid $\begin{cases} \text{asociativit. } (xy)z = x(yz) & \forall x,y,z\in R \\ \exists\, 1\in R : x\cdot 1 = x = 1\cdot x, \forall x\in R \end{cases}$

distribut. bilaterală: $\begin{aligned} x(y+z) &= xy+xz \\ (y+z)x &= yx+zx \end{aligned}$ $\forall x,y,z\in R$

Corp: $(K,+,\cdot)$ inel, $K\neq\{0\}$ & $\forall x\in K^* = K\setminus\{0\}\ \exists x^{-1}\in K : x\cdot x^{-1} = 1 = x^{-1}\cdot x$

(cu alte cuvinte $(K^*,\cdot)$ este grup)

Morfism de $f: R\to S$ $\quad f(x+y) = f(x)+f(y)$, $f(x\cdot y) = f(x)\cdot f(y)$ $\forall x,y\in R$.

Izomorfism = morfism bijectiv

1. $A = \mathbb{Z}$ sau $A = \mathbb{R}$, $a\in A$ (Temă: $A = \mathbb{Q}$)

$x\oplus y = x+y-a$

$x * y = xy - ax - ay + a^2 + a$ $\quad \forall x,y\in A$

Să se arate că $(\mathbb{Z},\oplus,*)$ este inel, $(\mathbb{R},\oplus,*)$ este corp și sunt izomorfe cu $(\mathbb{Z},+,\cdot)$ resp. $(\mathbb{R},+,\cdot)$.

Soluția $\quad x*y = xy - ax - ay + a^2 + a = x(y-a) - a(y-a) + a = (x-a)(y-a) + a$

$x,y,z\in A$

$(x\oplus y)\oplus z = (x+y-a)\oplus z = x+y-a+z-a = x+y+z-2a$

$x\oplus(y\oplus z) = x\oplus(y+z-a) = x+y+z-a-a = x+y+z-2a$

$x\oplus y = x+y-a = y+x-a = y\oplus x$

Caut. e a.i. $x \oplus e = x$, $\forall x \in A$

$x + e - a = x \Rightarrow e = a$

Caut $\bar{x} \in A$ a.i. $x \oplus \bar{x} = a$.

$x + \bar{x} - a = a$

$\bar{x} = 2a - x \in A$

$x * (y * z) = (x-a)\left[(y*z) - a\right] + a = (x-a)\left((y-a)(z-a) - a + a\right) + a = (x-a)(y-a)(z-a) + a$

$(x*y) * z = \left[(x-a)(y-a) + a\right] * z = \left[(x-a)(y-a) + a - a\right](z-a) + a = (x-a)(y-a)(z-a) + a$

$x * y = (x-a)(y-a) + a = y * x$

Caut. $e' \in A$ a.i. $x * e' = x$, $\forall x \in A$

$(x-a)(e'-a) + a = x$

$(x-a)(e'-a) = (x-a)$, $\forall x \in A$

$x = a \Rightarrow x - a = 0$ $\Rightarrow$ egalit. de mai sus este adev. pt. orice e'

$x \neq a \Rightarrow x - a \neq 0 \Rightarrow e' - a = 1 \Rightarrow e' = a + 1$

Verif. distribut.

$x * (y \oplus z) = (x-a)(y \oplus z - a) + a = (x-a)(y + z - 2a) + a = (x-a)y + (x-a)z - 2a(x-a) + a$

$(x*y) \oplus (x*z) = \left[(x-a)(y-a) + a\right] + \left[(x-a)(z-a) + a\right] - a = (x-a)(y-a) + a + (x-a)(z-a)$

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

Deci $(A, \oplus, *)$ inel comut. pt. $A = \mathbb{Z}$ sau $A = \mathbb{R}$.

Acum $A = \mathbb{R}$; fie $x \in \mathbb{R} \setminus \{a\}$. Caut $x' \in \mathbb{R}$ a.i.

$x * x' = a + 1$

$(x-a)(x'-a) + a = a + 1$

$x \neq a \Rightarrow x - a \neq 0 \Rightarrow \exists (x-a)^{-1} = \frac{1}{x-a} \in \mathbb{R}$

$x' - a = \frac{1}{x-a} \Rightarrow x' = \frac{1}{x-a} + a \in \mathbb{R}$

Deci $(\mathbb{R}, \oplus, *)$ corp.

Obs. $x * a = (x-a)(a-a) + a = a$, $\forall x \in A$

$(A,+,\cdot) = \{\ldots -1, 0, 1, 2, \ldots\}$

$(A,\oplus,*) = \{\ldots\ldots a, a+1, \ldots\}$

$f: A \to A, \quad f(x) = x+a \qquad f: (A,+,\cdot) \to (A,\oplus,*)$

$f(x+y) = x+y+a$

$f(x)\oplus f(y) = f(x)+f(y)-a = x+a+y+a-a = x+y+a$ $\Big\} \Rightarrow f(x+y) = f(x)\oplus f(y)$

$f(xy) = xy+a$

$f(x)*f(y) = (f(x)-a)(f(y)-a)+a = (x+a-a)(y+a-a)+a = x\cdot y+a$ $\Big\} \Rightarrow$

$f(xy) = f(x)*f(y)$

$g: A \to A \qquad g(x) = x-a$

$f\circ g: A \to A \qquad (f\circ g)(x) = f(g(x)) = f(x-a) = x-a+a = x = 1_A(x)$

$g\circ f: A \to A \qquad (g\circ f)(x) = g(f(x)) = g(x+a) = x+a-a = x = 1_A(x)$

$f\circ g = 1_A = g\circ f \Rightarrow g = f^{-1}$ deci f este bij. (izomorfism)

2. $n \in \mathbb{N}$, $n \geq 2 \rightsquigarrow \mathbb{Z}_n = \{\hat{0}, \hat{1}, \ldots, \hat{n-1}\}$ $(\mathbb{Z}_n, +, \cdot)$ inel

a) n prim $\Leftrightarrow$ $(\mathbb{Z}_n, +, \cdot)$ nu are divizori ai lui zero

b) Să se rezolve ec.

$\hat{x}^2 - \hat{4}\hat{x} + \hat{3} = \hat{0}$ în $\mathbb{Z}_{11}$ și $\mathbb{Z}_{15}$

$\hat{3}\hat{x}^2 - \hat{4}\hat{x} + \hat{1} = \hat{0}$ în $\mathbb{Z}_5$ și $\mathbb{Z}_9$

Soluție. $(R,+,\cdot)$ inel. Spunem că R nu are divizori ai lui zero dacă

$x, y \in R \quad x\cdot y = 0 \Rightarrow x = 0$ sau $y = 0$

a) $\Leftarrow$ n nu este prim deci $\exists\, m, q \in \mathbb{Z}$ $1 < m, q < n$ a.î.

$n = m\cdot q \Rightarrow \hat{n} = \widehat{m\cdot q} = \hat{m}\cdot\hat{q}$ în $\mathbb{Z}_n$

Dar $\hat{n}=\hat{0}$ și $\hat{m}\neq\hat{0}$, $\hat{q}\neq\hat{0}$ $\Rightarrow$ $\hat{0}=\hat{m}\cdot\hat{q}$ $\Rightarrow \mathbb{Z}_n$ are divizori ai lui zero

(Ex: $\hat{4}\cdot\hat{3}=\hat{0}$ în $\mathbb{Z}_{12}$)

„$\Rightarrow$" Fie $x,y\in\mathbb{Z}$ a.î. $\hat{x}\cdot\hat{y}=\hat{0}$ în $\mathbb{Z}_n \Rightarrow \hat{xy}=\hat{0}$ în $\mathbb{Z}_n$

$\Rightarrow n \mid xy$

Știm n este prim $\Rightarrow n\mid x$ sau $n\mid y \Rightarrow \hat{x}=\hat{0}$ sau $\hat{y}=\hat{0}$ în $\mathbb{Z}_n$

b) $x^2-\hat{4}x+\hat{3} = x^2-\hat{3}x-\hat{1}x+\hat{3} = x(x-\hat{3})-(x-\hat{3}) = (x-\hat{3})(x-\hat{1})$

$x^2-\hat{4}x+\hat{3}=\hat{0} \Leftrightarrow$

$(x-\hat{3})(x-\hat{1})=\hat{0}$

În $\mathbb{Z}_{11}$ (11 este nr. prim) nu există div. ai lui zero, deci

$x-\hat{3}=\hat{0}$ sau $x-\hat{1}=0 \Rightarrow x=\hat{3}$ sau $x=\hat{1}$.

În $\mathbb{Z}_{15}$ $(15=3\cdot 5)$ avem mai multe cazuri

I. $x-\hat{3}=\hat{0} \Rightarrow x=\hat{3}$ ✓

II. $x-\hat{1}=\hat{0} \Rightarrow x=\hat{1}$ ✓

III $x-\hat{3}=\hat{3}$ și $x-\hat{1}=\hat{5} \Rightarrow x=\hat{6}$ ✓

IV $x-\hat{3}=\hat{5} \Rightarrow x=\hat{8}$, $x-\hat{1}=\hat{7}$ nu obținem nr.

$\hat{3}\cdot\hat{10}=\hat{30}=\hat{0}$ în $\mathbb{Z}_{15}$

$\hat{5}\cdot\hat{9}=\hat{45}=\hat{0}$

IV. $x-\hat{1}=\hat{12} \Rightarrow x=\hat{13}$.

x	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{3}$	$\hat{4}$	$\hat{5}$	$\hat{6}$	$\hat{7}$	$\hat{8}$	$\hat{9}$	$\hat{10}$	$\hat{11}$	$\hat{12}$	$\hat{15}$	$\hat{14}$
$x-\hat{1}$	-1	0	1	$?$	3	4	5	6	7	8	9	10	11	12	13
$x-\hat{3}$	-3	$?$	-1	0	1	2	3	4	5	6	7	8	9	10	11
$(x-\hat{1})(x-\hat{3})$	3	0	-1	0	3	6	0	9	5	Nu	Nu	Nu	Nu	0	Nu

3. a) Să se rezolve ec. $x^3+\hat{1}=\hat{0}$ în $\mathbb{Z}_3$

b) Generalizare: Să se rezolve $x^p+\hat{1}=\hat{0}$ în $\mathbb{Z}_p$ (p nr. prim).

Soluție. a) $(x+\hat{1})^3 = x^3+\overset{\hat{0}}{\hat{3}}x^2+\overset{\hat{0}}{\hat{3}}x+\hat{1} = x^3+\hat{1}$

$(x+\hat{1})^3 = \hat{0}$

$x+\hat{1} = 0$

$x = -\hat{1} = \hat{2}$ în $\mathbb{Z}_3$.

b) $(x+\hat{1})^p = \sum_{i=0}^{p} C_p^i x^{p-i} = x^p + \sum_{i=1}^{p-1} C_p^i x^{p-i} + \hat{1}$

$C_p^i = \frac{p!}{(p-i)!\, i!} = \frac{1\cdot 2 \cdots i \cdot (i+1) \cdots p}{1\cdot 2 \cdots (p-i) \cdot 1\cdot 2 \cdots i} = \frac{(i+1)\cdots(p-1)\,p}{1\cdot 2\cdots(p-i)} = p \cdot \underbrace{\frac{(i+1)\cdots(p-1)}{1\cdot 2\cdots(p-i)}}_{\in \mathbb{Z}}$

$2 \nmid p,\ 3 \nmid p, \dots, (p-1) \nmid p$ pt. $i \in \{1, \dots, p-2\}$

pt. $i = p-1 \rightsquigarrow p-i = 1$

$p \mid C_p^i \Rightarrow \hat{C}_p^i = \hat{0} \Rightarrow (x+\hat{1})^p = x^p + \hat{1}$ în $\mathbb{Z}_p$

Ec. devine $(x+\hat{1})^p = \hat{0}$

$x+\hat{1} = \hat{0}$

$x = -\hat{1} = \hat{p-1}$ în $\mathbb{Z}_p$. ☒.