ÎNELE ȘI CORPURI

Scurt istoric : Definiția, așa cum o știm / folosim azi, de inel îi este atribuită lui Fraenkel (1914) însă conceptul este mult mai vechi. Astfel:

- Gauss (1801) a definit mulțimea (inelul!) $\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\}$ și a arătat că în acest "inel" orice element nenul și neinversabil se poate scrie în mod unic ca un produs de elemente prime generalizând teorema fundamentală a aritmeticii.
- Dedekind (1871) a definit conceptul de ideal prim, generalizând numerele prime. Istoria îl creditează pe Dedekind ca fiind cel care a inventat conceptul de inel (el le numea "order"), deși la el inelele erau doar comutative. În mod cert Dedekind a definit conceptul de corp.
- B. Peirce (1881) a definit conceptul mai general de "algebră asociativă" și a demonstrat clasificarea acestor algebre (peste corpul $\mathbb{C}$) în dimensiune 2 și 3. Clasificarea completă a celor de dimensiune 3 a fost făcută de E. Study (1890). Aceste obiecte erau numite și "sisteme hipercomplexe" (Frobenius așa le numea).

- Emmy Noether (1920) a publicat o lucrare despre teoria idealelor și a definit o clasă de inele care azi îi poartă numele, anume "inele noetheriene".
- Hilbert (1893) a numit aceste obiecte matematice "inele" și a demonstrat faimoasa "teoremă a bazei" care marchează un punct de cotitură în istoria și evoluția matematicii, fiind prima teoremă în matematică "neconstructivistă", i.e. demonstrația ei nu "construiește" explicit rezultatul dorit.

Definiție (Fraenkel, 1914) Se numește inel un triplet (R, α, β), unde R e o mulțime nevidă, $\alpha, \beta : R \times R \longrightarrow R$ sunt două funcții a.î.:

1) (R, α) este grup abelian; notăm $\alpha((a,b)) \overset{not}{=} a+b$ $(\forall)\, a, b \in R$ și elementul neutru cu 0_R sau 0.
2) (R, β) este un monoid; notăm $\beta((a,b)) \overset{not}{=} ab$, $(\forall)\, a, b \in R$ și elementul neutru cu 1_R sau 1.
3) (distributivitatea) Au loc următoarele egalități:
$$a(b+c) = ab + ac$$
$$(a+b)c = ac + bc,$$
$(\forall)\, a, b, c \in R$.

În plus, R s.n. inel comutativ dacă $ab = ba$, $(\forall)\, a, b \in R$.

Exemple 1) $R = \{0\}$ este un inel, numit inelul nul.

Dacă într-un inel R, $1 = 0 \Rightarrow R = \{0\}$ inelul nul. (Exercițiu!) Din acest motiv, în inelele noastre $1 \neq 0$ (prin convenție).

2) $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sunt toate inele. Mai mult

$\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\}$ este un inel, cu adunarea și înmulțirea uzuală a numerelor complexe, numit inelul întregilor lui Gauss.

3) Fie $G = (G, +)$ un grup abelian și $R := \mathrm{End}(G) \overset{\text{def}}{:=} \{f : G \to G \mid f \text{ morfism de grupuri}\}$

Atunci, R este un inel, numit inelul de endomorfisme al lui G cu:

$$(f + g)(x) := f(x) + g(x)$$

$$(f \cdot g)(x) := f(g(x)), \text{ i.e. } f \cdot g = f \circ g$$

$(\forall)\ f, g \in R$, $x \in G$. (Exercițiu!)

4) Dacă R e un inel, atunci inelul opus R^{op} este definit astfel:

$(R^{op}, +) := (R, +)$ și înmulțirea

$a * b := ba$, $(\forall)\ a, b \in R^{op} = R$ (ca set)

Evident, R e inel comutativ $\Leftrightarrow R = R^{op}$ (ca inele).

5) (inelul/algebra de funcții pe o mulțime)

Fie X o mulțime și R un inel. Fie

$$R^X := \{ f : X \to R \mid f \text{ funcție} \}$$

Atunci R^X are o structură de inel cu:

$$(f+g)(x) := f(x) + g(x)$$
$$(f \cdot g)(x) := f(x) g(x)$$

$(\forall)$ $f, g \in R^X$, $x \in X$. (Exercițiu!)

Dacă $f \in R^X$ vom nota cu

$$\boxed{\mathrm{supp}(f)} \stackrel{def}{:=} \{ x \in X \mid f(x) \neq 0_R \}$$

și o numim suportul lui f. Vom spune că $f \in R^X$ are suport finit și vom nota asta cu $\mathrm{supp}(f) < \infty$ dacă $\mathrm{supp}(f)$ e o mulțime finită.

Inelul R^X s.n. inelul de funcții pe X și are un loc cheie în relație "algebră vs geometrie", mai precis în "algebrizarea problemelor din geometrie".

6) (inelul/algebra grupal) Fie G = grup și R = inel și definim

$$R[G] := \{ f : G \to R \mid f \text{ funcție}, \mathrm{supp}(f) < \infty \}$$

Atunci, $R[G]$ are o structură de inel cu:

$$(f+g)(x) := f(x) + g(x)$$

(1) $$(f * g)(x) := \sum_{\substack{y, z \in G \\ yz = x}} f(y)\, g(z) = \sum_{y \in G} f(y)\, g(y^{-1}x)$$

$(\forall)\ f, g \in R[G]$, $x \in G$, cu elementul unitate

$$1_{R[G]} : G \longrightarrow R,\quad 1_{R[G]}(g) := \delta_{1_G, g} := \begin{cases} 1_R, & g = 1_G \\ 0_R, & g \neq 1_G \end{cases}$$

(Exercițiu!) numit <u>inelul grupal</u> al lui R și G.

Multiplicarea definită prin (1) s.n. <u>produs de convoluție</u>

7) (<u>inelul de matrici</u>) Fie R = <u>inel</u> și $m, n \in \mathbb{N}^*$.

Fie $M_{m,n}(R) := \{ A : \{1, \dots m\} \times \{1, \dots n\} \longrightarrow R \mid A = \text{funcție} \}$

Vom nota $A((i,j)) \overset{not}{=} a_{ij}$, $(\forall)\ i = \overline{1,m}$, $j = \overline{1,n}$ și

$A \overset{not}{=} (a_{ij})_{\substack{1 \le i \le m \\ 1 \le j \le n}}$ și o numim <u>matrice cu m linii și n coloane</u>. A o putem reprezenta ca un tablou

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$$

Două matrici $A = (a_{ij})$, $B = (b_{ij}) \in M_{m,n}(R)$ sunt egale $\Longleftrightarrow$ sunt egale ca funcții; i.e.

$$A = B \Longleftrightarrow a_{ij} = b_{ij}, \ (\forall)\ i = \overline{1,m},\ j = \overline{1,n}.$$

Dacă $m = n$ vom nota $M_n(R) \stackrel{not}{=} M_{n,n}(R)$ și o numim mulțimea matricilor pătratice ale ordinului n.

$M_{m,n}(R)$ are o structură de grup abelian cu

$$(A + B)((i,j)) := A((i,j)) + B((i,j)), \quad (2)$$

$(\forall)\ A, B \in M_{m,n}(R)$, $i = \overline{1,m}$, $j = \overline{1,n}$.

Scrise sub formă de tablou adunarea matricilor se face "pe componente", i.e.

$$(a_{ij}) + (b_{ij}) = (a_{ij} + b_{ij}).$$

Elementul neutru în grupul abelian $(M_{m,n}(R), +)$ este matricea nulă notată cu $O_{m,n}$ și definită prin $O_{m,n}(i,j) := 0_R$, $(\forall)\ i,j$.

Dacă în plus, $m = n$, atunci $M_n(R)$ are o structură de inel cu înmulțirea definită prin:

(3) $\boxed{(AB)((i,j)) := \sum_{k=1}^{n} A((i,k))\, B((k,j))}$

$(\forall)\ A, B \in M_n(R)$, $i, j = \overline{1,n}$. Explicit, dacă $A = (a_{ij})$ şi $B = (b_{ij})$, atunci

$AB = (c_{ij})$, unde fiecare c_{ij} e dat de

(3') $$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}, \quad (\forall)\ i, j = \overline{1,n}$$

Formula (3) spune că atunci când înmulţim două matrici înmulţim "linii pe coloane".

<u>Exerciţiu</u> În contextul de mai sus arătaţi că $M_n(R)$ cu legile de compoziţie (2) şi (3) este un <u>inel</u> cu elementul unitate $1_{M_n(R)} \overset{not}{=} I_n$, matrice

$$I_n : \{1, \dots n\} \times \{1, \dots, n\} \to R, \quad I_n(i,j) := \delta_{ij}$$

$(\forall)\ i, j = \overline{1,n}$, i.e.

$$I_n = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & & & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix},$$ n.n. <u>matricea unitate</u> de ordin n

<u>Obs</u>: Dacă $n \geq 2$ atunci inelul $M_n(R)$ este <u>necomutativ</u> căci:

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \text{ şi } \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Exercițiu* Fie G un grup și R = inel. Atunci $R[G]$ este inel comutativ $\Longleftrightarrow$ G e grup abelian și R este inel comutativ.

Matricile $e_{ij} \in M_n(R)$ definite prin

$$e_{ij} := \begin{array}{cc} i \rightarrow & \begin{pmatrix} 0 & \cdots & 0 & \cdots & 0 \\ 0 & \cdots & \cdots & \cdots & 0 \\ \vdots & & 1 & & \vdots \\ \vdots & & \vdots & & \vdots \\ 0 & \cdots & \cdots & \cdots & 0 \end{pmatrix} \\ & \uparrow j \end{array}, \quad (\forall)\ i, j = \overline{1,n}$$

s.n. matrice elementare.

Exercițiu: Arătați că $\underbrace{e_{ij} e_{kl} = \delta_{jk} e_{il}}$, $(\forall)\ i, j, k, l = \overline{1,n}$, unde δ_{jk} este simbolul lui Kronecker $\delta_{jk} = \begin{cases} 0, & j \neq k \\ 1, & j = k. \end{cases}$

Definiție Fie R un inel și $a \in R$.

1) a s.n. divizor al lui zero la stânga (resp. la dreapta) dacă $(\exists)\ 0 \neq b \in R$ a.î. $ab = 0$ (resp. $\cancel{ba =}$ $ba = 0$).

a s.n. divizor al lui zero dacă e divizor al lui zero și la stânga și la dreapta.

Un inel R s.n. integru dacă 0_R este singurul divizor al lui zero.

Un inel comutativ și integru s.n. domeniu de integritate.

2) a s.n. inversabil la stânga (resp. la dreapta) dacă $(\exists)\ b \in R$ a.î. $ab = 1$ (resp. $ba = 1$).
a s.n. inversabil dacă este inversabil și la stânga și la dreapta.
R s.n. corp dacă orice element nenul al său este inversabil.

Notație: $U(R) := \{a \in R \mid a \text{ e inversabil}\}$ este grupul (cu înmulțirea din inelul R) elementelor inversabile din R.

Observații 1) (reguli de calcul într-un inel). Dacă R e un inel atunci:

- $a0 = 0a = 0$, $(\forall)\ a \in R$
- $a(-b) = (-a)b = -ab$, $(\forall)\ a, b \in R$
- Dacă $ab = ba$ și $n \in \mathbb{N}^*$ $\Rightarrow$

$$(a+b)^n = \sum_{k=0}^{n} C_n^k a^{n-k} b^k.$$ (Exercițiu!)

Notație dacă $m \in \mathbb{N}^*$ și $x \in R$ atunci

$$mx \overset{not}{:=} \underbrace{x + \dots + x}_{\text{de } m \text{ ori}}.$$

2) $\mathbb{Z}$, $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ sunt domenii de integritate.

3) $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{R})$ sunt divizori ai lui zero în $M_2(\mathbb{R})$.

4) $U(\mathbb{Z}) = \{\pm 1\}$, $U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$
(Exercițiu !)

5) $a \in R$ este inversabil $\iff$ $(\exists)\, b \in R$ a.î. $ab = ba = 1$. Un astfel de b, dacă există, este **unic** și se notează cu a^{-1}.

Dem „$\Leftarrow$" nimic de arătat. „$\Rightarrow$" Pp. că a e inversabil la stânga și la dreapta și fie $a', a'' \in R$ a.î. $aa' = 1$ și $a''a = 1$. Atunci:

$a'' = a''1 = a''(aa') = (a''a)a' = 1a' = a'$,

i.e. $a' = a'' \overset{\text{not}}{=} b$. ∎

6) $\boxed{U(\mathbb{Z}_n) = \{\hat{x} \in \mathbb{Z}_n \mid (x, n) = 1\}}$ (Exercițiu!)

$\Rightarrow$ inelul $\mathbb{Z}_n$ este corp dacă și numai dacă n este număr prim. ∎

Definiție Fie R = inel și $S \subseteq R$. S s.n. subinel al lui R dacă:

a) $1 \in S$

b) $x - y \in S$, $(\forall)\, x, y \in S$

c) $xy \in S$, $(\forall)\, x, y \in S$.

$\mathbb{Z}$ este subinel în corpul $\mathbb{Q}$ și $\mathbb{Z}$ e subinel în $\mathbb{Z}[i]$.

Dacă $(S_\lambda)_{\lambda\in\Lambda}$ e o familie de subinele în R

$\Rightarrow \bigcap_{\lambda\in\Lambda} S_\lambda$ este tot subinel în R.

Definiție Fie R = inel și $I \subseteq R$. I s.n. ideal stâng (resp. drept) al lui R și scriem asta $I \leq_s R$ (resp. $I \leq_d R$), dacă:

1) $I \leq (R,+)$, i.e. $x - y \in I$, $(\forall)\ x, y \in I$

2) $(\forall)\ r \in R$ și $(\forall)\ x \in I$ avem că $rx \in I$ (resp. $xr \in I$).

I s.n. ideal bilateral al lui R dacă este ideal stâng și drept al lui R. Notăm: $I \trianglelefteq R$.

Observații și exemple:

1) $\{0\}$ și R sunt ideale bilaterale în orice inel R.

2) Dacă R = inel comutativ, noțiunile de ideal stâng, drept, bilateral coincid. În acest caz ele s.n. (simplu) ideale.

3) I este ideal în $\mathbb{Z} \iff (\exists!)\ n \in \mathbb{N}$ a.î. $I = n\mathbb{Z} = \{nt \mid t \in \mathbb{Z}\}$.

4) O intersecție arbitrară de ideale stângi (drepte, bilaterale) este un ideal stâng (drept, bilateral). (Exercițiu!)

Propoziție Fie R = inel și $I \leq_s R$ (resp. $I \leq_{dl} R$).
Atunci, $I = R \iff I$ conține un element inversabil.

Dem "$\Rightarrow$" este OK căci $1_R \in R = I$ este element inversabil.

"$\Leftarrow$" Fie $u \in I \leq_s R$ și u = inversabil $\Rightarrow (\exists)$ $v \in R$ a.î. $uv = vu = 1$. Fie $x \in R$.

$\Rightarrow x = x1 = x(vu) = \underset{\substack{\uparrow \\ R}}{(xv)}\underbrace{u}_{\in I} \in I \Rightarrow$

$x \in I$ i.e. $R \subseteq I \subseteq R \Rightarrow I = R$. ▨

Analog pt. ideale drepte.

Corolar Fie R = inel comutativ. Atunci R este corp $\iff$ singurele sale ideale sunt $\{0\}$ și R.

Dem: "$\Rightarrow$" Fie $I \leq R$ ideal, $I \neq \{0\} \Rightarrow$
$(\exists)$ $x \in I$, $x \neq 0 \underset{R\text{ e corp}}{\Longrightarrow} x$ e inversabil $\overset{(P)}{\Longrightarrow} I = R$

"$\Leftarrow$" Fie $r \in R$, $r \neq 0$. Vreau: r e inversabil
$I = Rr = \{xr \mid x \in R\}$ este un ideal în R și $I \neq 0$, căci $r = 1r \in I$
$\Rightarrow I = R \Rightarrow 1 \in I \Rightarrow (\exists)$ $x \in R$ a.î. $1 = xr = rx$, i.e. r e inv. ▨

Def: Fie R = inel și $E \subseteq R$ o submulțime. Fie

$$(E| := \bigcap_{\substack{I \leq_s R \\ I \supseteq E}} I \ ; \ |E) := \bigcap_{\substack{I \leq_d R \\ I \supseteq E}} I \ ; \ (E) := \bigcap_{\substack{J \trianglelefteq R \\ J \supseteq E}} J .$$

Atunci $(E|$, $|E)$ și (E) s.n. idealul stâng / drept / bilateral generat de E.

Un ideal stâng I (resp. drept, bilateral) s.n. finit generat dacă există $F \subseteq R$ finită a.î. $I = (E|$ (resp. $I = |E)$, $I = (E)$).

Obs: 1) $(\phi| = |\phi) = (\phi) := \{0_R\}$

2) $(E|$ este "cel mai mic ideal" (în sensul relației de incluziune) al lui R ce conține E, i.e.: dacă $E \subseteq J \leq_s R \Rightarrow (E| \subseteq J$. În plus, $E \subseteq (E|$

Propoziție Fie R = inel și $E \subseteq R$ o submulțime nevidă. Atunci

1) $(E| = \left\{ \sum_{i=1}^{n} a_i x_i \mid n \in \mathbb{N}^*, a_i \in R, x_i \in E, (\forall) i = \overline{1,n} \right\}$

2) $|E) = \left\{ \sum_{i=1}^{n} x_i a_i \mid n \in \mathbb{N}^*, a_i \in R, x_i \in E, (\forall) i = \overline{1,n} \right\}$

3) $(E) = \left\{ \sum_{i=1}^{n} a_i x_i b_i \mid n \in \mathbb{N}^*, a_i, b_i \in R, x_i \in E, (\forall) i = \overline{1,n} \right\}$

Dem: Vom arăta doar 1) – restul se fac analog.

Fie $I := \left\{ \sum_{i=1}^{n} a_i \cdot x_i \mid n \in \mathbb{N}^*, a_i \in R, x_i \in E, (\forall) i = \overline{1,n} \right\}$

• <u>Afirm</u> : $I \leq_s R$ și $E \subseteq I$

În adevăr, dacă $\alpha = \sum_{i=1}^{n} a_i x_i$, $\beta = \sum_{j=1}^{m} b_j y_j$

$\Rightarrow \alpha - \beta \in I$, fiind o sumă de acelaşi tip

În plus, dacă $r \in R \Rightarrow r\alpha = \sum_{i=1}^{n} (r a_i) x_i \in I$

$\Rightarrow I \leq_R R$. În plus, dacă $\underline{x \in E} \Rightarrow$

$x = 1_R x \in I$ i.e. $E \subseteq I$.

$\Rightarrow E \subseteq I \leq_s R \Rightarrow \underline{(E| \subseteq I}$.

Arătăm că $I \subseteq (E|$. Fie $\underline{\alpha \in I} \Rightarrow$

$\alpha = a_1 x_1 + \dots + a_n x_n$, $a_i \in R$, $x_i \in E$ $(\forall)\, i = \overline{1,n}$

Cum $x_i \in E \subseteq (E| \Rightarrow a_i x_i \in (E|$, $(\forall)\, i = \overline{1,n}$

$\Rightarrow$ ($(E|$ e ideal stâng) $\sum_{i=1}^{n} a_i x_i = \underline{\alpha \in (E|}$

i.e. $(E| = I$ i.e. 1) e arătat. 2) și 3) Analog

$\boxtimes$

<u>Obs</u> : Dacă $E = \{a\}$, $a \in R \Rightarrow$

$(a| = \{ra \mid r \in R\} \overset{not}{=} \underline{Ra}$

$|a) = \{ar \mid r \in R\} \overset{not}{=} \underline{aR}$

$(a) = \left\{ \sum_{i=1}^{n} r_i a s_i \mid n \in \mathbb{N}^*, r_i, s_i \in R\ (\forall)\, i = \overline{1,n} \right\}$

$\overset{not}{=} \underline{RaR}$

Def: 1) Un ideal stâng (resp. drept, bilateral) I al unui inel R s.n. <u>principal</u> dacă $(\exists)\, a \in R$ a.î. $I = Ra$ (resp. $I = aR$, $I = RaR$).

2) Un inel R s.n. <u>inel principal</u> dacă este domeniu de integritate (i.e. comutativ și integru) și orice ideal al său este principal.

<u>Exemplu</u> $(\mathbb{Z}, +, \cdot)$ este un inel principal.

Orice corp comutativ K este inel principal, caci $\{0\} = K0$ și $K = K1$. $\boxtimes$

- <u>Suma și produs de ideale</u>

Fie R = inel și I, J două ideale stângi (resp. drepte, bilaterale). Mulțimea

$$IJ \overset{def}{:=} \left\{ \sum_{i=1}^{n} x_i y_i \;\middle|\; n \in \mathbb{N}^*,\ x_i \in I,\ y_i \in J,\ (\forall)\ i = \overline{1,n} \right\}$$

este un ideal stâng (resp. drept, bilateral) (Exercițiu!) numit <u>produsul idealelor</u> I și J. Similar și <u>recursiv</u> putem defini produsul unui număr <u>finit</u> de ideale. Dacă $I_1, \dots, I_n$ sunt ideale stângi atunci $I_1 I_2 \dots I_n := (I_1 I_2 \dots I_{n-1}) I_n$

Similar, dacă $(I_\lambda)_{\lambda \in \Lambda}$ este o familie nevidă de ideale stângi (resp. drepte, bilaterale) de inelul R atunci mulțimea

$$\boxed{\sum_{\lambda \in \Lambda} I_\lambda} := \left\{ \sum_{i=1}^{n} x_{\lambda_i} \;\middle|\; n \in \mathbb{N}^*,\ x_{\lambda_i} \in I_{\lambda_i},\ (\forall)\ i=\overline{1,n} \right\}$$

este un ideal stâng (drept, bilateral) (Exercițiu!) numit suma familiei de ideale $(I_\lambda)_{\lambda \in \Lambda}$.

În particular, dacă $I_1, \dots, I_n$ sunt ideale stângi în R, atunci

$$I_1 + \dots + I_n = \left\{ \sum_{k=1}^{n} x_k \;\middle|\; x_k \in I_k,\ (\forall)\ k=\overline{1,n} \right\}$$

Exercițiu: Fie $R = (\mathbb{Z}, +, \cdot)$, $m, n \in \mathbb{N}^*$. Atunci $m\mathbb{Z} + n\mathbb{Z} = (m,n)\mathbb{Z}$, $m\mathbb{Z} \cdot n\mathbb{Z} = mn\mathbb{Z}$ și $m\mathbb{Z} \cap n\mathbb{Z} = [m,n]\mathbb{Z}$. (temă!)

Definiție: Fie R = inel. Un element $x \in R$ s.n. nilpotent dacă $(\exists)\ n \in \mathbb{N}$ a.î. $x^n = 0$.

Notăm: $N(R) := \{ x \in R \mid x = \text{nilpotent} \}$.

Un element $e \in R$ s.n. idempotent dacă $e^2 = e$. Notăm: $\mathrm{Idem}(R) := \{ e \in R \mid e \text{ idempotent} \}$

Exerciții 1) Fie A = inel comutativ. Atunci:

a) Arătați că $N(A)$ este ideal în A.

b) Dacă $x \in N(A)$ și $u \in U(A) \Rightarrow u + x \in U(A)$;

c) Dacă $e, f \in \mathrm{Idem}(A) \Rightarrow$
$$e \oplus f := e + f - 2ef \in \mathrm{Idem}(A)$$
și $(\mathrm{Idem}(A), \oplus, \cdot)$ este un inel comutativ.

d)* Arătați că dacă $|\mathrm{Idem}(A)| < \infty \Rightarrow (\exists)\, t \in \mathbb{N}$ a.î. $|\mathrm{Idem}(A)| = 2^t$.

Exercițiu 2) Fie p = nr. prim. Arătați că
$$|\mathrm{Idem}(M_2(\mathbb{Z}_p))| = p(p+1) + 2$$

Definiție Fie R, S două inele. O funcție $f : R \to S$ s.n. morfism de inele dacă:
$$f(x+y) = f(x) + f(y), \quad f(xy) = f(x)f(y)$$
$(\forall)\, x, y \in R$ și $f(1_R) = 1_S$.

Exemple: 1) $\mathrm{Id}_R : R \to R$, $\mathrm{Id}_R(r) := r$, $(\forall)\, r \in R$ e morfism de inele. Mai general, dacă $S \subseteq R$ e subinel $\Rightarrow$ incluziunea canonică
$$i : S \hookrightarrow R, \quad i(s) := s, \quad (\forall)\, s \in S$$
e morfism de inele.

2) $f : R \to M_n(R)$, $f(r) := rI_n$, $(\forall)\, r \in R$ este morfism de inele.

Def: Un morfism de inele $f : R \to S$ s.n. izomorfism dacă $(\exists)\ g : S \to R$ morfism de inele a.î. $f \circ g = Id_S$ și $g \circ f = Id_R$.

Un izomorfism de inele $f : R \to R$ s.n. automorfism al lui R.

Exemple / Exerciții

1) Nu există un morfism de inele $\mathbb{Q} \to \mathbb{Z}$ (singurul morfism de grupuri $(\mathbb{Q},+) \to (\mathbb{Z},+)$ este cel nul!)

2) Dacă $n \geq 2 \Rightarrow$ nu există un morfism de inele de $M_n(\mathbb{Q}) \longrightarrow \mathbb{Q}$. (Exercițiu!)

3) Compunerea a două morfisme de inele e tot morfism de inele.

Dacă $f : R \to S$ e morfism de inele și $u \in U(R) \Rightarrow f(u) \in U(S)$ și

$$f(u)^{-1} = f(u^{-1}).$$

Propoziție Fie $f : R \to S$ un morfism de inele. Atunci f este izomorfism $\Leftrightarrow$ f e bijectivă.

Dem „$\Rightarrow$" O.K. din definiție.

„$\Leftarrow$" Fie $f : R \to S$ morfism de inele, bijectiv. Suficient să arăt că f^{-1} e tot morfism de inele

• $f^{-1}(a+b) = f^{-1}(a) + f^{-1}(b)$, $(\forall)\ a, b \in S$ (88)

este OK de la grupuri!

• $f^{-1}(ab) \overset{?}{=} f^{-1}(a) f^{-1}(b)$, $(\forall)\ a, b \in S$

$\Longleftrightarrow$ (f e bijectivă) $f(f^{-1}(ab)) = f(f^{-1}(a) f^{-1}(b))$

$\Longleftrightarrow$ (f e morfism) $(f \circ f^{-1})(ab) = (f \circ f^{-1})(a) (f \circ f^{-1})(b)$

$\Longleftrightarrow$ $ab = ab$, și O.K. $\boxtimes$

Propoziție Fie $f : R \to S$ morfism de inele. Atunci:

1) Dacă $R' \subseteq R$ e subinel în $R \Longrightarrow f(R')$ e subinel în S. În particular, $\mathrm{Im}(f) \subseteq S$ e subinel

2) Dacă $S' \subseteq S$ este subinel în $S \Longrightarrow f^{-1}(S')$ este subinel în R.

3) Dacă $J \leq_s S$ (resp. drept, bilateral) $\Longrightarrow$ $f^{-1}(J) \leq_s R$ (resp. drept, bilateral).

În particular, $\mathrm{Ker}(f) = f^{-1}(0_S) = \{r \in R \mid f(r) = 0_S\}$ este ideal bilateral în R.

4) Dacă f este surjectiv și $I \leq_s R$ (resp. drept, bilateral). $\Longrightarrow f(I) \leq_s S$ (resp. drept, bilateral).

Dem: 1) $1_R \in R' \Longrightarrow 1_S = f(1_R) \in f(R')$

- $f(R') \leq (S,+)$ ok, de la grupuri.
- Fie $\alpha, \beta \in f(R') \Rightarrow (\exists)\ a, b \in R'$

a.î. $\alpha = f(a)$, $\beta = f(b) \Rightarrow$

$$\underline{\alpha b} = f(a)f(b) = f(\underbrace{ab}_{\in R'}) \in \underline{f(R')}$$

$\Rightarrow f(R')$ este subinel.

2) $1_R \in f^{-1}(S')$, căci $f(1_R) = 1_S \in S'$.

- $f^{-1}(S') \leq (R,+)$ ok, de la grupuri.
- Fie $\alpha, \beta \in f^{-1}(S') \overset{?}{\Rightarrow} \alpha\beta \in f^{-1}(S')$

$$f(\alpha\beta) = \underbrace{f(\alpha)}_{\in S'}\underbrace{f(\beta)}_{\in S'} \in S', \text{ căci } S' \text{ e subinel}$$

3) $f^{-1}(J) \leq (R,+)$ e ok, de la grupuri.

Fie $r \in R$ și $a \in f^{-1}(J)$. <u>Vrem</u>: $ra \overset{?}{\in} f^{-1}(J)$

$$f(ra) = f(r)\underbrace{f(a)}_{\in J} \in J, \text{ căci } J \text{ e ideal stâng.}$$

$\Rightarrow f^{-1}(J) \leq_R R$. Analog, pt. drept / bilateral.

4) $f(I) \leq (S,+)$, ok de la grupuri. Fie

$\underline{s \in S}$ și $\underline{y \in f(I)} \Rightarrow$ (f e <u>surjectiv</u>)

$(\exists)\ r \in R$ a.î. $s = f(r)$, $y = f(a)$, $a \in I$

$$\Rightarrow \underline{sy} = f(r)f(a) = f(\underbrace{ra}_{\in I \leq_s R}) \in \underline{f(I)}, \text{ ok.}$$

$\boxed{/\!/}$

Teoremă (teorema de corespondență pentru ideale)

Fie $f : R \to S$ un morfism **surjectiv** de inel...

Atunci funcția

$$F : \{ I \mid I \leq_s R,\ I \supseteq \mathrm{Ker}(f) \} \xrightarrow{\sim} \{ J \mid J \leq_s S \}$$

$$F(I) := f(I),\ (\forall) I \ldots$$

este **bijectivă** cu inversa $F^{-1}(J) := f^{-1}(J), (\forall) J \ldots$

(similar pentru ideale drepte / bilaterale).

Dem: Din teorema de corespondență de la prepuneri știm că funcția:

$$\mathcal{F} : \underbrace{\{ I \mid I \leq (R,+),\ I \supseteq \mathrm{Ker}(f) \}}_{\overset{not}{=} \mathcal{A}'} \to \underbrace{\{ J \mid J \leq (S,+) \}}_{\overset{not}{=} \mathcal{B}'}$$

$$\mathcal{F}(I) := f(I),\ (\forall) I \ldots$$

e bijectivă cu inversa $J \longmapsto f^{-1}(J)$.

Dar:

$$\mathcal{A} := \{ I \mid I \leq_s R,\ I \supseteq \mathrm{Ker}(f) \} \subseteq \mathcal{A}'$$

$$\mathcal{B} := \{ J \mid J \leq_s S \} \subseteq \{ J \mid J \leq (S,+) \} \overset{not}{=} \mathcal{B}'$$

și $F = \mathcal{F}|_{\mathcal{A}} : \mathcal{A} \to \mathcal{B}$. Propoziția precedentă spune că F e corect definită și e bijectivă, fiind restricție unei bijecții. ∎

• Caracteristica unui inel

Fie R = inel și $(R,+)$ grupul abelian subiacent inelului. În acest grup putem calcula $\sigma(1)$, ordinul elementului 1. Numărul natural definit prin:

$$car(A) \stackrel{def}{=} \begin{cases} \sigma(1), & \text{dacă } \sigma(1) \text{ este finit} \\ 0, & \text{dacă } \sigma(1) = \infty \end{cases}$$

s.n. caracteristica inelului R.

obs: 1) $car(R) = 0 \iff \underbrace{1+1+\dots+1}_{de\ n\ ori} \neq 0,\ (\forall)\ n \in \mathbb{N}^*$

Dacă $car(R) = n > 0 \Rightarrow n$ este cel mai mic număr natural nenul a.î. $n1_R = \underbrace{1_R + \dots + 1_R}_{de\ n\ ori} = 0$.

$car(\mathbb{Z}) = 0$, $car(\mathbb{Z}_n) = n$, $(\forall)\ n \geq 2$.

2) Dacă $car(R) = 0 \Rightarrow R$ conține un subinel $R' := \{n1_R \mid n \in \mathbb{Z}\} \subseteq R$, izomorf cu $\mathbb{Z}$.

Dacă $car(R) = n > 0 \Rightarrow R$ conține un subinel, anume $R' := \{k1_R \mid 0 \leq k \leq n-1\} \simeq \mathbb{Z}_n$ izomorf cu $\mathbb{Z}_n$.

Exercițiu (morfismul Frobenius) Fie R = inel comutativ a.î. $car(R) = p > 0$, p = nr. prim. Atunci $F: R \to R$, $F(x) := x^p$, $(\forall)\ x \in R$ este un morfism de inele numit morfismul Frobenius.

$\Rightarrow$ are loc "formula școlarului leneș"

$$(x+y)^p = x^p + y^p,\ (\forall)\ x, y \in R.$$

• Produse directe de inele

• produsul a două inele: Fie R şi S două inele.

Atunci $R\times S$ este un inel cu:

$$(r,s)+(r',s'):=(r+r',s+s')$$

$$(r,s)\cdot(r',s'):=(rr',ss')$$

$(\forall)\ r,r'\in R$, $s,s'\in S$ (Exerciţiu!) numit $R\times S$ produsul direct al lui R şi S. In inelul

$$0_{R\times S}=(0_R,0_S),\quad 1_{R\times S}=(1_R,1_S).$$

$R\times S$ este exemplu tipic de inel care nu este integru căci $(0,1)\cdot(1,0)=(0,0)$.

$$\underset{0}{\not\parallel}\qquad\underset{0}{\not\parallel}$$

• produsul unei familii arbitrare de inele.

Fie $(R_\lambda)_{\lambda\in\Lambda}$ o familie nevidă $(\Lambda\neq\emptyset)$ de inele şi

$$\prod_{\lambda\in\Lambda}R_\lambda:=\left\{x:\Lambda\longrightarrow\bigcup_{\lambda\in\Lambda}R_\lambda \;\middle|\; x(\lambda)\in R_\lambda,\ (\forall)\,\lambda\in\Lambda\right\}$$

La fel ca la mulţimi notăm $x(\lambda)\overset{not}{=}x_\lambda\in R_\lambda$ şi $x\overset{not}{=}(x_\lambda)_{\lambda\in\Lambda}$. De la grupuri ştim că $\left(\prod_{\lambda\in\Lambda}R_\lambda,+\right)$ este un grup (chiar abelian – Exerciţiu!) cu:

$$(x_\lambda)_{\lambda\in\Lambda}+(y_\lambda)_{\lambda\in\Lambda}:=(x_\lambda+y_\lambda)_{\lambda\in\Lambda}$$

$(\forall)\ (x_\lambda)_{\lambda\in\Lambda},(y_\lambda)_{\lambda\in\Lambda}\in\prod_{\lambda\in\Lambda}R_\lambda$.

Mai mult, $\left(\prod_{\lambda\in\Lambda} R_\lambda, +, \cdot\right)$ este un inel, unde:

$$(x_\lambda)_{\lambda\in\Lambda} \cdot (y_\lambda)_{\lambda\in\Lambda} := (x_\lambda y_\lambda)_{\lambda\in\Lambda}$$

(în scrierea ca funcții $(x\cdot y)(\lambda) := x(\lambda)\, y(\lambda)$, $(\forall)\, x \in \prod_{\lambda\in\Lambda} R_\lambda$, $\lambda\in\Lambda$), cu elementul unitate $1 = (1_{R_\lambda})_{\lambda\in\Lambda}$. (Exercițiu!)

Observații 1) Dacă $\Lambda = \{1, 2, \dots n\}$, atunci notăm $\prod_{i=1}^{n} R_i = R_1 \times \dots \times R_n$. Dacă $R_1 = \dots = R_n \overset{not}{=} R$ atunci $\underbrace{R\times \dots \times R}_{\text{de n ori}} \overset{not}{=} R^n$, care este un inel care nu e integru $(\forall)\, n \geq 2$.

2) Dacă $R_\lambda := R$, $(\forall)\, \lambda \in \Lambda$ atunci $\prod_{\lambda\in\Lambda} R_\lambda = R^\Lambda$, inelul de funcții pe mulțimea Λ (vezi Exemplu 5) pag. 80).

3) Fie $\prod_{\lambda\in\Lambda} R_\lambda$ un produs direct de inele. Atunci $(\forall)\, \lambda\in\Lambda$ funcția:

$$p_\lambda : \prod_{\lambda\in\Lambda} R_\lambda \longrightarrow R_\lambda,\quad p_\lambda\left((x_\lambda)_{\lambda\in\Lambda}\right) := x_\lambda$$

este un morfism surjectiv de inele (Exercițiu!) numit proiecție canonică pe componenta λ.

• Pentru surjectivitate avem nevoie de .... axioma alegerii

Propoziție Fie $(R_\lambda)_{\lambda\in\Lambda}$ o familie de inele. Atunci

$$U\left(\prod_{\lambda\in\Lambda} R_\lambda\right) = \prod_{\lambda\in\Lambda} U(R_\lambda)$$

Dem. Fie $x = (x_\lambda)_{\lambda\in\Lambda} \in \prod_{\lambda\in\Lambda} R_\lambda$. Atunci:

x este inversabil în inelul $\prod_{\lambda\in\Lambda} R_\lambda \iff$

$(\exists)\ y = (y_\lambda)_{\lambda\in\Lambda}$ a.î. $xy = yx = 1 \iff$

$(\exists)\ y = (y_\lambda)_{\lambda\in\Lambda}$ a.î. $x_\lambda y_\lambda = y_\lambda x_\lambda = 1_{R_\lambda}$, $(\forall)\ \lambda\in\Lambda$

$\iff x_\lambda \in U(R_\lambda)$, $(\forall)\ \lambda\in\Lambda \iff x \in \prod_{\lambda\in\Lambda} U(R_\lambda)$

☑

Teorema facultativă (proprietatea de universalitate a produsului direct de inele). Fie $(R_\lambda)_{\lambda\in\Lambda}$ o familie de inele. Atunci:

$$\begin{tikzcd} & R \arrow[dl, dashed, "(\exists!)\ \overline{f}"'] \arrow[d, "(\forall) f_\lambda"] \\ \prod_{\lambda\in\Lambda} R_\lambda \arrow[r, "p_\lambda"'] \arrow[ur, phantom, "="] & R_\lambda \end{tikzcd}$$

$(\forall)\ R =$ inel, $(\forall)\ f_\lambda : R \to R_\lambda$ o familie de morfisme de inele $(\lambda\in\Lambda)$, $(\exists!)\ \overline{f} : R \longrightarrow \prod_{\lambda\in\Lambda} R_\lambda$ un morfism de inele a.î. $p_\lambda \circ \overline{f} = f_\lambda$, $(\forall)\ \lambda\in\Lambda$

Dem: • unicitatea lui $\overline{f}$.

Fie $\overline{f} : R \longrightarrow \prod_{\lambda\in\Lambda} R_\lambda$ un morfism de inele a.î. $p_\lambda \circ \overline{f} = f_\lambda$, $(\forall)\ \lambda\in\Lambda \implies$

$\Longrightarrow p_\lambda(\overline{f}(r)) = f_\lambda(r)$, $(\forall)\, r \in R, \lambda \in \Lambda$

$\Longrightarrow$ (definiţia lui p_λ) $\overline{f}(r)(\lambda) = f_\lambda(r)$,

$(\forall)\, r \in R$ şi $(\forall)\, \lambda \in \Lambda \Longrightarrow$

$$\overline{f}(r) = (f_\lambda(r))_{\lambda \in \Lambda}, \quad (\forall)\, r \in R$$

i.e. $\overline{f}$ este implementat în mod unic de familia de morfisme $(f_\lambda)_{\lambda \in \Lambda}$.

- <u>Existenţa</u> Definim $\overline{f} : R \longrightarrow \prod_{\lambda \in \Lambda} R_\lambda$,

$$\overline{f}(r) := (f_\lambda(r))_{\lambda \in \Lambda}, \quad (\forall)\, r \in R.$$

Atunci $\overline{f}$ este un morfism de inele ce închide toate diagramele comutativ, i.e.

$$p_\lambda \circ \overline{f} = f_\lambda, \quad (\forall)\, \lambda \in \Lambda \quad \text{(Exerciţiu!)}$$ ▨

<u>Obs</u>: Ca la mulţimi/grupuri P.U.P.D. de inele spune că funcţia:

$$\boxed{\begin{aligned} \chi : \mathrm{Hom}_{\underline{Rings}}\Big(R, \prod_{\lambda \in \Lambda} R_\lambda\Big) &\xrightarrow{\sim} \prod_{\lambda \in \Lambda} \mathrm{Hom}_{\underline{Rings}}(R, R_\lambda) \\ \chi(u) &:= (p_\lambda \circ u)_{\lambda \in \Lambda}, \quad (\forall)\, u \in \ldots \end{aligned}}$$

este <u>bijectivă</u>, unde $\mathrm{Hom}_{\underline{Rings}}(\cdot,\cdot)$ este mulţimea morfismelor între două inele.

• Inele factor. Proprietatea de universalitate a inelelor factor

Fie R un inel și $I \trianglelefteq R$ un ideal bilateral în R.

Cum $I \leq (R,+)$ este subgrup în grupul abelian $(R,+)$ $\Rightarrow$ $(R/_I,+)$ are o structură de grup abelian (grupul factor!) cu:

(1) $\boxed{\hat{a} + \hat{b} := \widehat{a+b}}$, $(\forall)\, \hat{a}, \hat{b} \in R/_I$

Reamintim, de la construcția grupului factor:

$a \equiv b \pmod I \overset{def}{\Longleftrightarrow} a-b \in I$. Pentru $a \in R$

$\underline{\hat{a}} = \{x \in R \mid x \equiv a \pmod I\} =$

$= \{x \in R \mid x-a \in I\} = \{a+y \mid y \in I\}$

$\overset{not}{=} \underline{a+I}$

În plus, pe grupul abelian $(R/_I,+)$ definim o înmulțire astfel:

(2) $\boxed{\hat{a} \cdot \hat{b} := \widehat{ab}}$, $(\forall)\, \hat{a}, \hat{b} \in R/_I$.

• înmulțirea definită de (2) este corect definită?

Fie $\hat{a} = \hat{\alpha}$ și $\hat{b} = \hat{\beta} \overset{?}{\Longrightarrow} \hat{a}\cdot\hat{b} = \hat{\alpha}\cdot\hat{\beta}$

Știm că: $a-\alpha \in I$ și $b-\beta \in I$ și vrem să arătăm că $\underline{ab-\alpha\beta \overset{?}{\in} I}$

Avem:

$$ab - \alpha\beta = ab - \alpha b + \alpha b - \alpha\beta$$
$$= \underbrace{(a-\alpha)}_{\in I} b + \alpha \underbrace{(b-\beta)}_{\in I} \in I, \text{ căci}$$

I este ideal bilateral (şi stâng şi drept) în R

i.e. $\widehat{ab} = \widehat{\alpha\beta}$ şi deci (2) e corect definită.

Propoziție - Definiție Fie R = inel şi $I \trianglelefteq R$ un ideal bilateral al lui R. Atunci $(R/_I, +, \cdot)$ cu adunarea şi înmulţirea definite de (1) şi (2) este un inel cu

$$0_{R/I} = \hat{0} = I \text{ şi } 1_{R/I} = \hat{1} = \{1+y \mid y \in I\}$$

numit inelul factor al lui R prin I. În plus,

$$\pi : R \longrightarrow R/_I, \quad \pi(r) := \hat{r}, \ (\forall) r \in R$$

este morfism surjectiv de inele numită proiecţie canonică a lui R pe $R/_I$.

Dem: • $(R/_I, +)$ e grup abelian o.k., de la grupuri factor.

• $(R/_I, \cdot)$ e monoid cu $1_{R/I} = \hat{1}$. În adevăr, pentru $a, b, c \in R$ avem:

$\hat{a}(\hat{b}\hat{c}) = (\hat{a}\hat{b})\hat{c}$, căci $\widehat{a(bc)} = \widehat{(ab)c}$, (înmulţirea din R e asociativă) şi $\hat{1}$ e unitate în mod banal.

• distributivitatea: Pentru $a, b, c \in R$ avem:

$$\hat{a}(\hat{b}+\hat{c}) = \hat{a}(\widehat{b+c}) = \widehat{a(b+c)} =$$

$$= (R \text{ e inel}) = \widehat{ab+ac} = \widehat{ab} + \widehat{ac}$$

$$= \hat{a}\hat{b} + \hat{a}\hat{c}$$ și analog la dreapta.

Restul detaliilor sunt triviale. ☒

obs: Dacă $I \trianglelefteq R$, atunci $Ker(\pi) = I$, unde $\pi : R \longrightarrow R/_I$, $\pi(r) = \hat{r}$, $(\forall) r \in R$.

Reciproc, Dacă $f : R \longrightarrow S$ e morfism de inele $\Longrightarrow$ $Ker(f) \trianglelefteq R$ este un ideal bilateral în R. În concluzie, o submulțime $I \subseteq R$ este un ideal bilateral în R $\Longleftrightarrow$ I este nucleul unui morfism de inele $f : R \to S$.

Cu alte cuvinte, idealele bilaterale sunt, la nivel de inele, contrapartea subgrupurilor normale de la grupuri.

Exemplu Fie $R = (\mathbb{Z}, +, \cdot)$. Atunci, $I \leq R = \mathbb{Z}$ $\Longleftrightarrow$ $(\exists!)\, n \in \mathbb{N}$ a.î. $I = n\mathbb{Z}$. În acest caz,

inelul factor

$$\mathbb{Z}/_{n\mathbb{Z}} \overset{not}{=} \mathbb{Z}_n = \{\hat{0}, \hat{1}, \dots \widehat{n-1}\}$$ s.n.

inelul claselor de resturi modulo n.

Teoremă (proprietatea de universalitate a inelelor factor)

Fie R = inel, $I \trianglelefteq R$ ideal bilateral în R şi $\pi : R \longrightarrow R/_I$ proiecţia canonică, $\pi(r) = \hat{r}$.

$$\begin{tikzcd} R \arrow[r, "\pi"] \arrow[d, "(\forall) f"'] & R/_I \arrow[dl, dashed, "(\exists!) \overline{f}"] \\ S & \end{tikzcd}$$

Atunci: $(\forall)$ S un inel şi $(\forall)$ $f : R \longrightarrow S$ morfism de inele cu $\operatorname{Ker}(f) \supseteq I$, $(\exists!)$ $\overline{f} : R/_I \longrightarrow S$ morfism de inele a.î. $\overline{f} \circ \pi = f$.

În plus,

a) $\overline{f}$ este surjectiv $\Longleftrightarrow$ f este surjectiv.

b) $\overline{f}$ este injectiv $\Longleftrightarrow$ $\operatorname{Ker}(f) = I$.

Dem • **unicitatea** lui $\overline{f}$. Fie $\overline{f} : R/_I \longrightarrow R$ un morfism de inele cu $\overline{f} \circ \pi = f$ $\Longrightarrow$

$\Longrightarrow (\overline{f} \circ \pi)(r) = f(r)$, $(\forall)$ $r \in R$, i.e.

$\overline{f}(\hat{r}) = f(r)$, $(\forall)$ $r \in R$,

$\overline{f}$ este **unic determinat** de f.

• **existenţa**. Definim:

$\overline{f} : R/_I \longrightarrow S$, $\overline{f}(\hat{r}) := f(r)$, $(\forall)$ $\hat{r} \in R/_I$

Arătăm că $\overline{f}$ este **corect definită**!

În adevăr, dacă $\widehat{r} = \widehat{r'} \Longrightarrow$

$r - r' \in \underline{I \subseteq \mathrm{Ker}(f)} \Longrightarrow f(r - r') = 0$

$\Longrightarrow f(r) = f(r')$, i.e. $\overline{f}(\widehat{r}) = \overline{f}(\widehat{r'})$,

i.e. $\overline{f}$ e corect definită.

Arătăm acum că $\overline{f}$ e morfism de inele. Fie $\widehat{r_1}, \widehat{r_2} \in R/_I$. Atunci:

$\overline{f}(\widehat{r_1} + \widehat{r_2}) = \overline{f}(\widehat{r_1 + r_2}) = f(r_1 + r_2) =$ (f e morfism)

$= f(r_1) + f(r_2) = \overline{f}(\widehat{r_1}) + \overline{f}(\widehat{r_2})$ și

$\overline{f}(\widehat{r_1}\widehat{r_2}) = \overline{f}(\widehat{r_1 r_2}) = f(r_1 r_2) \overset{f \text{ morfism}}{=} f(r_1) f(r_2) = \overline{f}(\widehat{r_1})\overline{f}(\widehat{r_2})$

și în plus, $\overline{f}(\widehat{1_R}) = f(1_R) = 1_S$, i.e. $\overline{f}$ e morfism.

Punctele a) și b) sunt ok de la grupuri. ▨

Teoremă (teorema fundamentală de izomorfism pt. inele)

Fie R, S două inele și $f : R \longrightarrow S$ un morfism de inele. Atunci există un izomorfism de inele $\boxed{R/_{\mathrm{Ker}(f)} \simeq \mathrm{Im}(f)}$.

Dem. Aplicăm P.U.I.F. pentru diagrama

$$\begin{tikzcd}
R \arrow[r, "\pi"] \arrow[d, "h"] & R/_{\mathrm{Ker}(f)} \arrow[dl, dashed, "(\exists!)\,\overline{f}"] \\
\mathrm{Im}(f) &
\end{tikzcd}$$

, unde $h(r) := f(r)$, $(\forall) r \in R$

h este morfism surjectiv de inele și
$\text{Ker}(h) = \text{Ker}(f)$, idealul prin care factorizez
pe R

$\overset{\text{P.U.I.F.}}{\Longrightarrow} (\exists!)\ \overline{f} : R/_{\text{Ker}(f)} \xrightarrow{\sim} \text{Im}(f)$ un
izomorfism de inele a.î. $\overline{f}(\hat{r}) = f(r)$,
$(\forall)\ \hat{r} \in R/_{\text{Ker}(f)}$. ▨

COROLAR (lema chinezească a resturilor) Fie
A = inel comutativ, I și $J \leq A$ ideale în A
a.î. $I + J = A$. Atunci există un
izomorfism de inele

$$A/_{I \cap J} \simeq A/_I \times A/_J .$$

Dem: Fie $f : A \longrightarrow A/_I \times A/_J$,
$$f(x) := (\hat{x}, \hat{\hat{x}}),\ (\forall)\ x \in R$$

Atunci, f e un morfism de inele (Exercițiu!)
și $\text{Ker}(f) = I \cap J$. În adevăr,

$x \in \text{Ker}(f) \Longleftrightarrow f(x) = (\hat{0}, \hat{\hat{0}}) \Longleftrightarrow$
$(\hat{x}, \hat{\hat{x}}) = (\hat{0}, \hat{\hat{0}}) \Longleftrightarrow \hat{x} = \hat{0}$ și $\hat{\hat{x}} = \hat{\hat{0}}$

$\iff x \in I$ și $x \in J \iff \underline{x \in I \cap J}$

• f este <u>surjectiv</u> ?

Fie $(\hat{x}, \hat{\hat{y}}) \in A/_I \times A/_J$. <u>Vreau</u> :

$(\exists)\ a \in A$ a.î. $f(a) = (\hat{x}, \hat{\hat{y}})$, i.e

$\hat{a} = \hat{x}$ și $\hat{\hat{a}} = \hat{\hat{y}}$.

Cum $I + J = A \implies (\exists)\ i \in I$ și $j \in J$ a.î.

$\underline{i + j = 1_R}$. Fie $\underline{a := jx + iy}$. Atunci

$\underline{\hat{a}} = \widehat{jx+iy} = \hat{j}\,\hat{x} + \underset{\overset{\|}{\hat{0}}}{\hat{i}} \cdot \hat{y} = \hat{j}\,\hat{x}$ $\quad i \in I \Rightarrow \hat{i} = \hat{0}$ în $A/_I$

$= \widehat{(1-i)}\,\hat{x} = \hat{x} - \hat{i}\,\hat{x} = \underline{\hat{x}}$

și analog,

$\hat{\hat{a}} = \widehat{\widehat{jx+iy}} = \underset{\overset{\|}{0}}{\underbrace{\hat{\hat{j}}}}\,\hat{\hat{x}} + \hat{\hat{i}}\,\hat{\hat{y}} = \hat{\hat{i}} \cdot \hat{\hat{y}} =$

$= \widehat{\widehat{(1-j)}}\,\hat{\hat{y}} = \hat{\hat{y}}$, i.e.

$f(jx + iy) = (\hat{x}, \hat{\hat{y}})$, i.e. f e <u>surjectiv</u>.

Aplicând <u>T.F.I.</u> $\implies$

$\bar{f} : A/_{I \cap J} \xrightarrow{\sim} A/_I \times A/_J$, $\bar{f}(\tilde{x}) := (\hat{x}, \hat{\hat{x}})$
$(\forall)\ \tilde{x} \in A/_{I \cap J}$

este <u>izomorfism</u> de inele. ▨

Corolar Fie $m, n \in \mathbb{N}$, $m, n \geq 2$, și prime între ele, i.e. $(m, n) = 1$. Atunci

$$f : \mathbb{Z}_{mn} \xrightarrow{\sim} \mathbb{Z}_m \times \mathbb{Z}_n,$$

$$f(\tilde{a}) := (\hat{a}, \hat{\hat{a}}), \ (\forall)\ \tilde{a} \in \mathbb{Z}_{mn}$$

este izomorfism de inele.

Dem: Aplicăm corolarul precedent pentru

$A := \mathbb{Z}$, $I := m\mathbb{Z}$, $J := n\mathbb{Z}$.

Cum $(m, n) = 1 \Rightarrow (\exists)\ h, k \in \mathbb{Z}$ a.î.

$hm + kn = 1 \Rightarrow m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$

și în plus, $m\mathbb{Z} \cap n\mathbb{Z} = mn\mathbb{Z}$. ∎

Scurt istoric: Lema chineză îi este atribuită lui Sun-Tsu un matematician chinez (nu se știe exact când a trăit, unde în secolul 3 sau 4 d.H) deși se pare că era era cunoscută și de indieni și din lumea arabă. Sun-Tsu a formulat-o într-un caz special (nu existau inele atunci!), în limbaj de congruențe. Mai precis, el a rezolvat sistemul

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

cu soluția $x = 23 + 105K$, $K \in \mathbb{Z}$

Sun-Tsu <u>nu</u> a dat soluție completă și nici un algoritm. <u>Demonstrație completă</u> a fost dată abia în <u>1247</u> de un chinez într-un tratat scris de matematică. Noțiunea de congruență a fost introdusă de <u>Gauss în 1801</u> și tot el a ilustrat folosirea lemei chineze într-o problemă privind calendarul!

<u>Aplicații ale lemei chineze. Exerciții Seminar</u>

1) Fie $m_1, \dots m_k \in \mathbb{N} \setminus \{0,1\}$ și $(m_i, m_j) = 1$, $(\forall) i \neq j$

$\Longrightarrow (\exists)$ un izo de inele

$$\mathbb{Z}_{m_1 m_2 \dots m_k} \simeq \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_k}$$

2) $\hat{x} \in U(\mathbb{Z}_n) \Longleftrightarrow (x, n) = 1$.

$\Longrightarrow |U(\mathbb{Z}_n)| = \varphi(n)$, indicatorul lui Euler.

3) $\varphi(m_1 m_2 \dots m_k) = \varphi(m_1) \dots \varphi(m_k)$,

$(\forall) m_1, \dots m_k \in \mathbb{N}^*$, cu $(m_i, m_j) = 1$, $(\forall)\ i \neq j$

4) Fie $n \in \mathbb{N}^*$, $n \geq 2$ și $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, descompunerea în factori primi. Atunci

$$\varphi(n) = n \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right)$$

5) $|U(\mathbb{Z}_{360})| = 96$.

Facultativ: Teoremele de izomorfism pentru inele

Teorema (Teorema I de izomorfism pentru inele)

Fie $f : R \to S$ un morfism surjectiv de inele și $I \trianglelefteq R$ un ideal bilateral, $I \supseteq \mathrm{Ker}(f)$.
Atunci, $f(I) \trianglelefteq S$ e ideal bilateral în S
și există un izomorfism de inele:

$$R/_{I} \simeq S/_{f(I)}$$

Dem: Știm deja că $f(I) \trianglelefteq S$ (pg. 88) și din funcț teorema I de izomorfism pentru grupuri că

$$\overline{f} : R/_{I} \xrightarrow{\sim} S/_{f(I)}, \quad \overline{f}(\hat{r}) := \widehat{\widehat{f(r)}}$$

este izomorfism de grupuri abeliene. În plus,

$(\forall)\ \hat{r}_1, \hat{r}_2 \in R/_{I}$ avem:

$$\overline{f}(\hat{r}_1 \hat{r}_2) = \overline{f}(\widehat{r_1 r_2}) = \widehat{\widehat{f(r_1 r_2)}} = \widehat{\widehat{f(r_1)}} \cdot \widehat{\widehat{f(r_2)}}$$

$$= \overline{f}(\hat{r}_1)\overline{f}(\hat{r}_2) \text{ și } \overline{f}(\hat{1}) = \hat{\hat{1}}$$

i.e. $\overline{f}$ este și morfism de monoizi, i.e. $\overline{f}$ este izomorfism de inele $\boxtimes$

Obs Fie $I \trianglelefteq R$ ideal bilateral in R și $\pi : R \longrightarrow R/_I$, $\pi(r) = \hat{r}$, proiecția canonică.
Fie $J \trianglelefteq R$ ideal bilateral, $J \supseteq I$ și notăm $\pi(J) \overset{not}{=} J/_I$. Atunci Th I $\Rightarrow$ există un izomorfism de inele

$$\boxed{R/_J \simeq \frac{R/I}{R/J}} \quad (*)$$

Formula $(*)$ este utilă când calculăm inelele factor ale lui $\mathbb{Z}_n = \mathbb{Z}/_{n\mathbb{Z}}$ ☐

Teoremă (Teorema II de izomorfism pentru inele)
Fie R un inel, $S \subseteq R$ un subinel în R și $I \trianglelefteq R$ un ideal bilateral în R. **Atunci**:
$S + I := \{s + i \mid s \in S, i \in I\} \subseteq R$ este un subinel în R.
$I \trianglelefteq (S+I)$ e ideal bilateral în $S+I$, $I \cap S \trianglelefteq S$ și există un izomorfism de inele:

$$(S+I)/_I \simeq S/_{S \cap I}$$

Dem • $S + I \subseteq R$ e subinel în R.
$1_R = 1_R + 0 \in S + I$, căci $1_R \in S$ = subinel, $0 \in I$ = ideal.
i.e. $1_R \in S + I$. Pentru $s_1, s_2 \in S$ și $i_1, i_2 \in I$ avem:

$$s_1 + i_1 - (s_2 + i_2) = \underbrace{s_1 - s_2}_{\in S} + \underbrace{i_1 - i_2}_{\in I} \in S + I$$

și

$$(s_1 + i_1)(s_2 + i_2) = \underbrace{s_1 s_2}_{\in S} + \underbrace{s_1 i_2 + i_1 s_2 + i_1 i_2}_{\in I \text{ căci } I \trianglelefteq R} \in S + I$$

i.e. $S + I$ e subinel în R.

- $I \trianglelefteq S + I$, banal!: $i = 0 + i \in S + I$, $(\forall) i \in I$

Fie acum $f : S \longrightarrow (S+I)/_I$, $f(s) := \widehat{s}$, $(\forall) s \in S$.

Atunci f e morfism de inele (Ex!) și e surjectiv căci, dacă $\widehat{s+i} \in (S+I)/_I \Longrightarrow$

$f(s) = \widehat{s} = \widehat{s+i}$, căci $s + i - s = i \in I$.

$\mathrm{Ker}(f) \overset{?}{=} S \cap I$. Fie $s \in S$. Atunci

$s \in \mathrm{Ker}(f) \Longleftrightarrow \widehat{s} = \widehat{0} \Longleftrightarrow s \in I$ i.e.

$\mathrm{Ker}(f) = S \cap I$. Aplicând T.F.I. $\Longrightarrow$

$\tilde{f} : S/_{S \cap I} \xrightarrow{\sim} (S+I)/_I$, $\tilde{f}(\overline{s}) := \widehat{s}$,

este izomorfism de inele. $\boxtimes$

• CORPURI

Definiție Un inel K s.n. corp dacă orice element nenul al său este inversabil, i.e. $U(K) = K \setminus \{0\}$.
K s.n. corp comutativ dacă $ab = ba$, $(\forall)\ a, b \in K$.

Exemple 1) $\mathbb{Q}$, $\mathbb{R}$ și $\mathbb{C}$ sunt corpuri. Reamintim construcția lui $\mathbb{C}$ din $\mathbb{R}$. Fie

$$\mathbb{C} :\overset{def}{=} \mathbb{R} \times \mathbb{R} = \{(a, b) \mid a, b \in \mathbb{R}\}$$ și

definim legile de compoziție:

$$(a, b) + (\alpha, \beta) := (a + \alpha,\ b + \beta)$$
$$(a, b) \cdot (\alpha, \beta) := (a\alpha - b\beta,\ a\beta + b\alpha)$$

$(\forall)\ (a, b), (\alpha, \beta) \in \mathbb{R} \times \mathbb{R}$. Atunci, cu aceste două operații, $(\mathbb{C}, +, \cdot)$ este un corp comutativ (Exercițiu!) cu $0_{\mathbb{C}} = (0, 0)$, $1_{\mathbb{C}} = (1, 0)$; dacă $(a, b) \neq (0, 0) \Rightarrow$ inversul său este:

$$(a, b)^{-1} = \left(\frac{a}{a^2 + b^2},\ -\frac{b}{a^2 + b^2}\right).$$

Notație Fie $\boxed{i :\overset{def}{=} (0, 1) \in \mathbb{C}}$ Atunci:

$$i^2 = i \cdot i = (0, 1)(0, 1) = (-1, 0) = -(1, 0) = -1_{\mathbb{C}}$$

i.e. în corpul $\mathbb{C}$, $\boxed{i^2 = -1}$ i.e. i este rădăcina ecuației $x^2 + 1 = 0$.

Dacă $z=(a,b)\in\mathbb{C}$, atunci

$z=(a,b)=(a,0)+(0,b)=a(1,0)+(b,0)(0,1)=a(1,0)+b(1,0)(0,1)$

$=a1_{\mathbb{C}}+b1_{\mathbb{C}}i \overset{not}{=} \underline{a+bi}$, căci

$\varphi:\mathbb{R}\longrightarrow\mathbb{C}$, $\varphi(a):=(a,0)$ este un morfism injectiv de corpuri și pot identifica $(a,0)$ cu a, $\mathbb{R}\simeq \mathrm{Im}(\varphi)=\{(a,0)\mid a\in\mathbb{C}\}\subseteq\mathbb{C}$

$\Longrightarrow (\forall)\ z\in\mathbb{C}\ (\exists!)\ a,b\in\mathbb{R}$ a.î. $z=a+bi$, cu $i^2=-1$.

2) $\mathbb{Q}(i):=\{a+bi\mid a,b\in\mathbb{Q}\}\subseteq\mathbb{C}$

$\mathbb{Q}(\sqrt{2}):=\{a+b\sqrt{2}\mid a,b\in\mathbb{Q}\}\subseteq\mathbb{R}$

sunt și ele corpuri cu adunarea și înmulțirea uzuale (Exercițiu!).

3) Inelul claselor de resturi modulo n $(n\geq 2)$ $\mathbb{Z}_n$ este $\underline{\text{corp}} \Longleftrightarrow n$ este $\underline{\text{număr prim}}$. (Exercițiu!). În particular, $\mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_5, \mathbb{Z}_7, \ldots$ sunt $\underline{\text{corpuri finite}}$.

<ins>Exercițiu</ins> $\mathbb{Z}_2[X]/(X^2+X+\hat{1})$ este un <ins>corp</ins> cu 4 elemente!

Def. Fie K un corp și $F \subseteq K$ o submulțime. F s.n. subcorp al lui K (sau K este o extindere a lui F) dacă:

a) $(\forall)\ x, y \in F \Rightarrow x - y \in F$

b) $1 \in F$

c) $(\forall)\ x, y \in F,\ y \neq 0 \Rightarrow x y^{-1} \in F$.

Obs: Dacă $F \neq \{0\}$ atunci condiția b) se obține din c) cu $x = y \neq 0 \Rightarrow 1 = x x^{-1} \in F$. ▨

Exemple a) $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ fiecare este subcorp în corpul mai mare.

b) $\mathbb{Q}(\sqrt{2})$ este subcorp în $\mathbb{R}$, iar $\mathbb{Q}(i)$ este subcorp în $\mathbb{C}$.

! c) Reamintim (vezi pag. 84) că un inel comutativ K este un corp $\Longleftrightarrow$ $\{0\}$ și K sunt singurele sale ideale!

Definiție Fie K și L două corpuri. O funcție $f: K \to L$ s.n. morfism de corpuri dacă f este morfism de inele.

Propoziție Orice morfism de corpuri $f : K \to L$ este injectiv.

Dem Fie $f : K \to L$ morfism de corpuri.

Atunci $Ker(f) \leq K$ e ideal în K și $Ker(f) \neq K$, căci $1 \in K$ și $1 \notin Ker(f)$ $(f(1) = 1 \neq 0)$. Cum K = corp și $Ker(f) \lneqq K \Rightarrow$ $Ker(f) = 0$, i.e. f e injectiv. ▨

Observație Dacă $f : K \to L$ e morfism de corpuri $\Rightarrow$ (f e injectiv) $K \simeq Im(f) \subseteq L$, i.e. K este izomorf cu un subcorp al lui L. Identificând $K \cong Im(f)$, putem pichi că L este o extindere a lui K. ▨

Definiție Un corp P s.n. corp prim dacă P nu are subcorpuri în afară de el însuși.

Exemple: $\mathbb{Z}_p$ (p = număr prim) și $\mathbb{Q}$ sunt corpuri prime.

În adevăr, fie $F \subseteq \mathbb{Z}_p$ un subcorp $\Rightarrow \hat{1} \in F$
$\Rightarrow \hat{x} = \underbrace{\hat{1} + \dots + \hat{1}}_{\text{de } x \text{ ori}} \in F, (\forall) \hat{x} \in \mathbb{Z}_p \Rightarrow$ $F = \mathbb{Z}_p$.

Fie acum $F \subseteq \mathbb{Q}$ subcorp $\Rightarrow 1 \in F \Rightarrow$ $\underline{\mathbb{N} \subseteq F}$. Cum $0 \in F \Rightarrow 0 - n \in F$, $(\forall)\, n \in \mathbb{N}$ $\Rightarrow \underline{\mathbb{Z} \subseteq F}$. Fie acum $\mathbb{Q} \ni r = \frac{m}{n} \Rightarrow$

$\frac{m}{n} = m \cdot n^{-1} \in F$ (căci F e subcorp și $m, n \in F$)

$\Rightarrow F = \mathbb{Q}$. $\boxtimes$

Reciproc,

Propoziție Fie P un corp prim $\Rightarrow$ P este izomorf cu $\mathbb{Q}$ sau P e izomorf cu $\mathbb{Z}_p$, $p =$ număr prim.

Dem. Fie P un corp prim și definim

$$\varphi : \mathbb{Z} \longrightarrow P, \quad \varphi(n) := n 1_P, \ (\forall)\, n \in \mathbb{Z}$$

unde
$$n 1_P := \begin{cases} \underbrace{1_P + \dots + 1_P}_{\text{de } n \text{ ori}}, & \text{dacă } n > 0 \\ 0, & \text{dacă } n = 0 \\ \underbrace{-1_P - \dots - 1_P}_{\text{de } -n \text{ ori}}, & \text{dacă } n < 0 \end{cases}$$

Atunci φ e un morfism de inele (Exercițiu!) $\Rightarrow$ $(\exists!)\, n \in \mathbb{N}$ a.î. $\underline{\mathrm{Ker}(\varphi) = n\mathbb{Z}}$.

Cazul 1: $n = 0 \Rightarrow \varphi$ e morfism injectiv de inele; în particular, $\underline{n 1_P \neq 0}$, $(\forall)\, n \in \mathbb{Z}, n \neq 0$

Fie $\overline{P} := \left\{ (m 1_p)(n 1_p)^{-1} \overset{not}{=} \frac{m 1_p}{n 1_p} \;\middle|\; m, n \in \mathbb{Z},\ n \neq 0 \right\}$

Atunci $\overline{P} \subseteq P$ este un subcorp în P (Exercițiu!)

și cum P e corp prim $\Rightarrow$ $\underline{\overline{P} = P}$. În plus,

$$\overline{\varphi} : \mathbb{Q} \xrightarrow{\sim} \overline{P} = P, \quad \overline{\varphi}\left(\frac{m}{n}\right) := \frac{m 1_p}{n 1_p}$$

este morfism de corpuri (Exercițiu), surjectiv $\Rightarrow$ (e și injectiv) deci $\underline{\mathbb{Q} \simeq \overline{P} = P}$.

<u>Cazul 2</u>: $n \neq 0$, i.e. $\mathrm{Ker}(\varphi) = n\mathbb{Z} \neq 0$

$\Rightarrow$ (T.F.I. pentru inele) există un izomorfism de inele $\mathbb{Z}_n \simeq \mathrm{Im}(\varphi) \subseteq P$.

Cum P = corp $\Rightarrow$ P e integru $\Rightarrow$ $\mathrm{Im}(\varphi)$ este inel integru $\Rightarrow$ $\mathbb{Z}_n$ e inel integru

$\Rightarrow$ n este număr prim $\left(n = \underset{>1, >1}{a b} \Rightarrow \hat{a}\hat{b} = \hat{0}, \text{ fals!} \right)$

$\Rightarrow \mathbb{Z}_n$ este corp $\Rightarrow \mathrm{Im}(\varphi)$ este corp $\Rightarrow$ (P e prim) $\mathrm{Im}(\varphi) = P \Rightarrow P \simeq \mathbb{Z}_n$, $\underline{n = \text{prim}}$

$\boxtimes$

<u>Obs</u>: Dacă $(F_\lambda)_{\lambda \in \Lambda}$ este o familie de subcorpuri în corpul K $\Rightarrow$ $\bigcap_{\lambda \in \Lambda} F_\lambda \subseteq K$ este un subcorp în K. (Exercițiu)

<u>Propoziție - Definiție</u> Fie K un corp și

$$P_K := \bigcap_{\substack{F \subseteq K \\ \text{subcorp}}} F \,. \quad \text{Atunci } P_K \subseteq K$$

este un subcorp, P_K este un <u>corp prim</u>, numit <u>corpul prim al lui K</u>.

<u>Dem</u> $P_K \subseteq K$ este subcorp în K, fiind o intersecție de subcorpuri. Să arătăm că P_K este corp prim. În adevăr, dacă $L \subseteq P_K$ este subcorp în $P_K \subseteq K \Rightarrow L$ este subcorp în K $\Rightarrow L$ participă la intersecția care definește P_K $\Rightarrow P_K \subseteq L \Rightarrow \underline{L = P_K}$, i.e. P_K este corp prim. ▨

<u>Definiție</u> Fie K = corp. Spunem că K are <u>caracteristică zero</u> (și notăm $\mathrm{char}(K) = 0$) dacă $P_K \simeq \mathbb{Q}$.

Spunem că K are <u>caracteristică $p > 0$</u> (și notăm $\mathrm{char}(K) = p > 0$) dacă $P_K \simeq \mathbb{Z}_p$, p = <u>nr. prim</u>.

<u>Observații</u> 1) $\mathrm{char}(K) = 0 \iff n 1_K \neq 0$, $(\forall) n \in \mathbb{Z}^*$

2) Fie $\mathrm{char}(K) = p > 0 \Rightarrow \underline{p = \sigma(1_K)}$, în grupul $(K, +)$ (vezi definiția ordinului!)

i.e. $p = \min\{n \in \mathbb{N}^* \mid n \cdot 1_K = 0_K\}$.

3) Fie K = corp finit $\Rightarrow (\exists)$ p = nr. prim a.î. $\mathrm{char}(K) = p > 0$. Fie extinderea de corpuri:

$$\mathbb{Z}_p \simeq P_K \subseteq K$$

$\Rightarrow$ K are o structură de $\mathbb{Z}_p$-spațiu vectorial. Fie $n = \dim_{\mathbb{Z}_p}(K) \Rightarrow \boxed{|K| = p^n}$

i.e. orice corp finit K are p^n elemente, unde p = nr. prim = $\mathrm{char}(K)$, $n \in \mathbb{N}^*$.

4) Fie K = corp, $\mathrm{char}(K) = p > 0$ și fie $x, y \in K$ cu $\underline{xy = yx}$. Atunci

$$(x+y)^p = x^p + y^p \quad (\text{"regula școlarului leneș"})$$

(Exercițiu!).

În particular, dacă K este comutativ atunci

$$\varphi_p : K \to K, \quad \varphi_p(x) := x^p, \quad (\forall)\, x \in K$$

este un morfism de corpuri, numit morfismul lui Frobenius.

• Corpul de fracții al unui domeniu de integritate

Punct de plecare: ce este un număr rațional?
De ce $\frac{2}{4} = \frac{1}{2}$? Ce înseamnă expresia "simplificăm fracția"?

La aceste întrebări vom răspunde mai jos.

Fie R un domeniu de integritate, i.e. R este un inel comutativ ($ab = ba$, $(\forall)\, a, b \in R$) și integru (dacă $ab = 0$, $a, b \in R \Rightarrow a = 0$ sau $b = 0$).

Exemple: $\mathbb{Z}$, $\mathbb{Z}[i]$, orice corp $\overset{\text{com.}}{\,}$, $\mathbb{Z}[X]$, $K[X]$ (unde K e corp comutativ) sunt domenii de integritate (prescurtat d. i.)

$\mathbb{Z} \times \mathbb{Z}$, $\mathbb{Z}_4$ nu sunt d. i. $\boxtimes$

• Construcția corpului de fracții

Fie R = domeniu de integritate. Pe mulțimea $A := R \times R^*$ ($R^* := R - \{0\}$) definim relația binară:

$$(a, s) \sim (b, t) \overset{def}{\iff} at = sb$$

$(\forall)\, (a, s), (b, t) \in R \times R^*$.

<u>Afirm</u>: $\sim$ e o relație de echivalență pe $R \times R^*$.

În adevăr, $\sim$ e reflexivă și simetrică (exercițiu banal!) și arătăm că e și tranzitivă:

Pp. că $(a,s) \sim (b,t) \sim (c,r) \Longrightarrow$

$$\begin{cases} at = sb & \mid \cdot r \\ br = tc & \mid \cdot s \end{cases} \Longrightarrow \begin{cases} rat - rsb = 0 \\ sbr - stc = 0 \end{cases} \Longrightarrow$$

(adunăm relațiile) $\underset{\neq 0}{t}(ra - sc) = 0 \xRightarrow[d.i]{R\,e}$

$ra = sc$, i.e. $\underline{(a,s) \sim (c,r)}$, și deci

$\sim$ e relație de echivalență pe $R \times R^*$.

Dacă $(a,s) \in R \times R^*$ atunci

$$\boxed{\widehat{(a,s)} \overset{def}{:=} \{(b,t) \in R \times R^* \mid at = sb\}} \overset{not}{=} \boxed{\frac{a}{s}}$$

și o numim <u>fracție</u> cu numărători din R și numitori din R^*. Mulțimea factor $R \times R^*/_\sim$ o notăm: $Q(R) \overset{not}{:=} R \times R^*/_\sim$.

<u>Teorema - Definiție</u> Fie R = <u>domeniu de integritate</u>. Atunci $Q(R)$ are o structură de <u>corp comutativ</u> cu operațiile:

$$\boxed{\frac{a}{s} + \frac{b}{t} := \frac{at + bs}{st}} \text{ și } \boxed{\frac{a}{s} \cdot \frac{b}{t} := \frac{ab}{st}}$$

$(\forall)\ \frac{a}{s}, \frac{b}{t} \in Q(R)$; $0_{Q(R)} = \frac{0}{1}$, $1_{Q(R)} = \frac{1}{1}$

numit <u>corpul de fracții</u> al lui R. În plus,

$\varphi : R \longrightarrow Q(R)$, $\varphi(r) := \frac{r}{1}$, $(\forall) r \in R$

este un morfism injectiv de inele.

Dem: • Arătăm mai întâi că operațiile sunt corect definite. Presupunem că:

$$\frac{a}{s} = \frac{a'}{s'} \text{ și } \frac{b}{t} = \frac{b'}{t'} \Longrightarrow \begin{cases} s'a = sa' & | \cdot tt' \\ t'b = tb' & | \cdot ss' \end{cases}$$

$$\Rightarrow \begin{cases} tt'(s'a - sa') = 0 \\ ss'(t'b - tb') = 0 \end{cases} \Longrightarrow \text{(adunându-le ecuațiile)}$$

$s't'(at + sb) - st(a't' + b's') = 0$, i.e.

$$\frac{at+bs}{st} = \frac{a't' + b's'}{s't'}$$, i.e. „+" e corect definită.

În plus, din $\begin{cases} s'a = sa' \\ t'b = tb' \end{cases} \Longrightarrow$ (le înmulțim)

$s't'ab = sta'b'$, i.e. $\frac{ab}{st} = \frac{a'b'}{s't'}$, i.e.

și „·" e corect definită.

• $(Q(R), +, \cdot)$ este un inel comutativ? Toate detaliile vă rămân ca exercițiu! De exemplu,

$$\frac{a}{s} + \frac{-a}{s} = \frac{0}{s^2} = \frac{0}{1} \; ; \; \frac{a}{s} \cdot \frac{1}{1} = \frac{a}{s}$$

$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st} = \frac{b}{t} \cdot \frac{a}{s}.$$

Arătăm acum că $Q(R)$ este corp. Fie

$\underline{\frac{a}{s} \neq \frac{0}{1}} \Longrightarrow \underline{a \neq 0}$ (dacă $a = 0 \Rightarrow \frac{0}{s} = \frac{0}{1}$)

$\Longrightarrow$ are sens și fracția $\frac{s}{a}$, căci $a \in R \setminus \{0\}$.

$$\Longrightarrow \frac{a}{s} \cdot \frac{s}{a} = \frac{as}{as} = \frac{1}{1} \Longrightarrow \frac{a}{s} \text{ este inversabil}$$

$$\text{și } \left(\frac{a}{s}\right)^{-1} = \frac{s}{a}. \quad \blacksquare$$

- $\varphi : R \longrightarrow Q(R)$, $\varphi(r) := \frac{r}{1}$ e morfism de inele (Exercițiu bonus!) și este $\underline{\text{injectiv}}$ căci

$$\underline{r \in \operatorname{Ker}(\varphi)} \Longleftrightarrow \varphi(r) = 0_{Q(R)} \Longleftrightarrow \frac{r}{1} = \frac{0}{1} \Longleftrightarrow$$

$$r \cdot 1 = 0 \cdot 1 \Longleftrightarrow \underline{r = 0}, \text{ i.e. } \operatorname{Ker}(\varphi) = \{0\}.$$

$\blacksquare$

<u>observații</u>: 1) Cum $\varphi : R \longrightarrow Q(R)$, $\varphi(r) := \frac{r}{1}$ este morfism injectiv de inele avem

$$R \simeq \operatorname{Im}(\varphi) = \left\{ \frac{r}{1} \;\middle|\; r \in R \right\} \subseteq Q(R)$$

i.e. putem identifica R cu un $\underline{\text{subinel}}$ în $\underline{\text{corpul}}$ său de fracții și putem face identificarea "$r = \frac{r}{1}$", $(\forall) r \in R$.

2) În corpul de fracții avem că:

$\boxed{\frac{0}{s} = \frac{0}{1}}$, $(\forall)\ s \in R^*$, $\boxed{\frac{t}{t} = \frac{1}{1}}$, $(\forall)\ t \in R^*$

$\boxed{\frac{at}{st} = \frac{a}{s}}$, $(\forall)\ a \in R,\ s, t \in R^*$,

ultima relaţie fiind ceea ce numeaţi "simplificarea fracţiilor".

3) Dacă $R := \mathbb{Z}$, atunci $\underline{Q(\mathbb{Z}) := \mathbb{Q}}$, s.n. corpul numerelor raţionale. Deci, un număr raţional $r \in \mathbb{Q}$ este de forma

$$\boxed{r \overset{not}{=} \frac{m}{n} \overset{def}{:=} \{(a, b) \in \mathbb{Z} \times \mathbb{Z}^* \mid mb = na\}},$$

unde $m \in \mathbb{Z}$, $n \in \mathbb{Z}^*$. În particular,

$$\boxed{\frac{1}{2} = \{(a, b) \in \mathbb{Z} \times \mathbb{Z}^* \mid b = 2a\} = \{(a, 2a) \mid a \in \mathbb{Z} \setminus \{0\}\}} \quad :) .$$

4) • Dacă $R := \mathbb{Z}[i]$, $\underline{Q(\mathbb{Z}[i]) \overset{not}{=} \mathbb{Q}(i)}$
$= \{r + is \mid r, s \in \mathbb{Q}\}$ (Exerciţiu!)

• Dacă $R = K[X]$, unde K = corp comutativ
$\Rightarrow Q(K[X]) \overset{not}{=} K(X)$ şi s.n. corpul funcţiilor raţionale pe K, i.e.

$$K(X) = \left\{ \frac{f}{g} \;\middle|\; f, g \in K[x],\ g \neq 0 \right\}.$$

Exercițiu: Fie $R := K$ corp comutativ.

Arătați că există un izomorfism de corpuri

$\underline{Q(K) \simeq K}$, i.e. pentru corpuri, construcția nu dă nimic nou!

Problemă de studiu* Fie R, S domenii de integritate a.î. $Q(R) \simeq Q(S)$ (izomorfism de corpuri). Rezultă că $R \simeq S$ (izo de inele)?

• Corpul cuaternionilor (Hamilton, 1843)

Dacă $\alpha \in \mathbb{C}$, $\alpha = a + bi$, atunci $\overline{\alpha} = a - bi$ s.n. conjugatul lui α. $|\alpha| = \sqrt{a^2+b^2} \in \mathbb{R}_+$ și

$\underline{\alpha\overline{\alpha} = |\alpha|^2}$, $(\forall)\ \alpha \in \mathbb{C}$, $\overline{\overline{\alpha}} = \alpha$.

Teoremă Fie $M_2(\mathbb{C})$ inelul de matrici uzual și

$$\mathbb{H} := \left\{ \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \;\middle|\; \alpha, \beta \in \mathbb{C} \right\} \subseteq M_2(\mathbb{C})$$

Atunci $\mathbb{H}$ este un subinel necomutativ în $M_2(\mathbb{C})$ și orice element nenul din $\mathbb{H}$ este inversabil în $\mathbb{H}$, i.e. $\mathbb{H}$ este corp necomutativ.

Dem Evident $I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathbb{H}$, $\overline{1} = 1$ și $O_2 = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \in \mathbb{H}$.

• $\mathbb{H}$ este <u>parte stabilă</u> în raport cu adunarea (Exercițiu banal!) și înmulțirea matricilor. Arătăm doar pentru înmulțire. Dacă

$$x = \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \in \mathbb{H} \text{ și } y = \begin{pmatrix} c & d \\ -\overline{d} & \overline{c} \end{pmatrix} \in \mathbb{H}, \text{ atunci}$$

$$xy = \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}\begin{pmatrix} c & d \\ -\overline{d} & \overline{c} \end{pmatrix} = \begin{pmatrix} ac - bd\overline{d} & ad + b\overline{c} \\ -\left(\overline{ad+b\overline{c}}\right) & \overline{ac - b\overline{d}} \end{pmatrix}$$

$\in \mathbb{H}$, căci $\underline{-\overline{b}c - \overline{a}\,\overline{d}} = -(\overline{a}\,\overline{d} + \overline{b}c) =$

$= -\left(\overline{ad + b\overline{c}}\right)$, căci $\overline{\overline{\beta}} = \beta$, $(\forall)\ \beta \in \mathbb{C}$

și $\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$, $\overline{\alpha\beta} = \overline{\alpha}\,\overline{\beta}$, $(\forall)\ \alpha, \beta \in \mathbb{C}$

și similar $-\overline{b}d + \overline{a}\,\overline{c} = \overline{ac - b\overline{d}}$. Am arătat că $\mathbb{H}$ e subinel în $M_2(\mathbb{C})$ și este evident <u>necomutativ</u> căci:

$$\underbrace{\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}}_{\in \mathbb{H}}\underbrace{\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}}_{\in \mathbb{H}} \neq \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

• <u>$\mathbb{H}$ este corp?</u> Fie $x = \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ în $\mathbb{H}$ $\Rightarrow$ $\Rightarrow$ a și b <u>nu</u> sunt simultan nule $\Rightarrow$ $\Rightarrow$ $|a|^2 + |b|^2 \neq 0$. Atunci $x \in U(\mathbb{H})$ cu inversul

$$\underline{x^{-1}} = \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix}^{-1} := \underline{\frac{1}{|a|^2+|b|^2}\begin{pmatrix} \overline{a} & -b \\ \overline{b} & a \end{pmatrix}} \in \mathbb{H}$$

(Exercițiu banal!), i.e. $\mathbb{H}$ este corp. ▨

Observație : 1) Elementele lui $\mathbb{H}$ s.n. cuaternioni.

2) Fie $\varphi : \mathbb{R} \to \mathbb{H}$, $\varphi(r) := \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix}$, $\bar{r} = r$ $(\forall)\, r \in \mathbb{R}$. Atunci φ este morfism (Exercițiu) de corpuri, i.e. este injectiv $\Longrightarrow$

$\mathbb{R} \simeq \mathrm{Im}(\varphi) \subseteq \mathbb{H}$ i.e. $\mathbb{R}$ se poate identifica cu un subcorp în $\mathbb{H}$ și $(\forall)\, r \in \mathbb{R}$ vom identifica, via izomorfismul de mai sus,

$r \cong \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix}$, $r \in \mathbb{R}$. Similar,

$\psi : \mathbb{C} \longrightarrow \mathbb{H}$, $\psi(\alpha) := \begin{pmatrix} \alpha & 0 \\ 0 & \overline{\alpha} \end{pmatrix}$ este morfism injectiv de corpuri $\Longrightarrow$

$\mathbb{C} \simeq \mathrm{Im}(\psi) \subseteq \mathbb{H}$ și putem identifica

$\alpha \cong \begin{pmatrix} \alpha & 0 \\ 0 & \overline{\alpha} \end{pmatrix}$, $(\forall)\, \alpha \in \mathbb{C}$

3) Fie cuaternionii

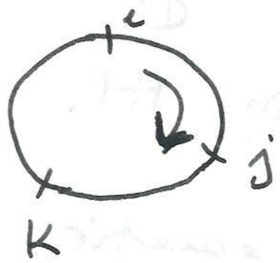
$i := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $j := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $k := \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \in \mathbb{H}$

Atunci, în inelul $\mathbb{H}$ au loc relațiile:

$$(*) \begin{cases} i^2 = j^2 = k^2 = -1_{\mathbb{H}} \\ ij = k = -ji, \; jk = i = -kj, \\ ki = j = -ik \end{cases}$$

(Exercițiu!)

Pentru a reține formulele de mai sus e suficientă o "plimbare" pe cercul de mai jos în sensul săgeții



4) Fie acum $x = \begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} \in \mathbb{H}$, cu

$\alpha = a_0 + a_1 i$, $\beta = b_0 + b_1 i$, $a_0, a_1, b_0, b_1 \in \mathbb{R}$

$\Longrightarrow$ în corpul $\mathbb{H}$ are loc descompunerea:

$$x = \begin{pmatrix} a_0 & 0 \\ 0 & a_0 \end{pmatrix} + \begin{pmatrix} a_1 & 0 \\ 0 & a_1 \end{pmatrix}\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} +$$

$$+ \begin{pmatrix} b_0 & 0 \\ 0 & b_0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + \begin{pmatrix} b_1 & 0 \\ 0 & b_1 \end{pmatrix}\begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} =$$

$$= \text{(via identificări) } a_0 + a_1 i + b_0 j + b_1 K$$

i.e. orice element $x \in \mathbb{H}$ se poate reprezenta în mod unic sub forma

$x = a_0 + a_1 i + b_0 j + b_1 k$, unde $a_0, a_1, b_0, b_1 \in \mathbb{R}$

$\Longrightarrow$

$\mathbb{H} = \{ a + bi + cj + dk \mid a, b, c, d \in \mathbb{R},\ i, j, k$ verifică $(*) \}$

și așa a fost definit inițial $\mathbb{H}$ de Hamilton.

Obs 1) $\dim_{\mathbb{R}}(\mathbb{H}) = 4$, cu $\{1, i, j, k\}$ o $\mathbb{R}$-bază în $\mathbb{H}$ și $\dim_{\mathbb{C}}(\mathbb{H}) = 2$, cu $\{j, k\}$ o $\mathbb{C}$-bază în $\mathbb{H}$.

2) Exercițiu Arătați că ecuația $x^2 = -1$ are în $\mathbb{H}$ o infinitate de soluții.

Corolar Fie $\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$ corpul cuaternionilor. Atunci mulțimea

$$Q := \{\pm 1, \pm i, \pm j, \pm k\} \subseteq \mathbb{H}$$

cu opt elemente este un subgrup finit în $U(\mathbb{H})$, numit grupul cuaternionilor.

Facultativ: Ideale prime, ideale maximale. Lema lui Krull

Definiție Fie R = inel comutativ.

1) Un ideal $\mathfrak{p}$ al lui R s.n. ideal prim dacă $\mathfrak{p} \neq R$ și $(\forall)\ a, b \in R$ a.î. $ab \in \mathfrak{p} \Rightarrow a \in \mathfrak{p}$ sau $b \in \mathfrak{p}$. (Dedekind, 1871)

2) Un ideal $\mathfrak{m}$ al lui R s.n. ideal maximal dacă $\mathfrak{m} \neq R$ și $(\forall)\ I$ un ideal în R a.î. $\mathfrak{m} \subseteq I \subseteq R \Rightarrow I = \mathfrak{m}$ sau $I = R$.

Notații: $\operatorname{Spec}(R) \overset{\text{not}}{:=} \{\mathfrak{p} \mid \mathfrak{p}$ ideal prim în $R\}$ s.n. spectrul lui R.

$\operatorname{Max}(R) \overset{\text{not}}{:=} \{\mathfrak{m} \mid \mathfrak{m}$ ideal maximal în $R\}$.

Observații 1) $\{0\} \in \operatorname{Spec}(R) \Leftrightarrow R$ este domeniu de integritate. (Exercițiu!)

2) $\{0\} \in \operatorname{Max}(R) \Leftrightarrow R$ este corp.

3) $\operatorname{Spec}(\mathbb{Z}) = \{\{0\}, p\mathbb{Z} \mid p = \text{număr prim}\}$

$\operatorname{Max}(\mathbb{Z}) = \{p\mathbb{Z} \mid p = \text{număr prim}\}$

(Exercițiu)

Propoziție Fie R un inel <u>comutativ</u> și $\underline{p} \subsetneq R$, $\underline{m} \subsetneq R$ ideale în R. Atunci:

1) $\underline{p} \in \mathrm{Spec}(R) \Longleftrightarrow R/_{\underline{p}}$ este domeniu de integritate.

2) $\underline{m} \in \mathrm{Max}(R) \Longleftrightarrow R/_{\underline{m}}$ este corp.

În particular, $\underline{\mathrm{Max}(R) \subseteq \mathrm{Spec}(R)}$, pentru orice inel R.

<u>Dem</u> 1) "$\Longrightarrow$" Pp. că $\underline{p} \in \mathrm{Spec}(R)$ și fie $\hat{a}, \hat{b} \in R/_{\underline{p}}$ a.î. $\underline{\hat{a} \cdot \hat{b} = \hat{0}} \Longrightarrow \widehat{ab} = \hat{0} \Longrightarrow ab \in \underline{p}$
$\Longrightarrow$ ($\underline{p}$ e ideal prim) $a \in \underline{p}$ sau $b \in \underline{p} \Longrightarrow$
$\hat{a} = \hat{0}$ sau $\hat{b} = \hat{0}$, i.e. $R/_{\underline{p}}$ este d.i.

"$\Longleftarrow$" Pp. că $R/_{\underline{p}}$ e d.i. și fie $a, b \in R$ a.î. $\underline{ab \in \underline{p}} \Longrightarrow \widehat{ab} = \hat{0}$ în $R/_{\underline{p}} \Longrightarrow$
$\hat{a}\hat{b} = \hat{0} \Longrightarrow \hat{a} = \hat{0}$ sau $\hat{b} = \hat{0} \Longrightarrow$
$\underline{a \in \underline{p} \text{ sau } b \in \underline{p}}$ i.e. $\underline{p}$ e ideal prim.

2) $\underline{m} \in \mathrm{Max}(R) \Longleftrightarrow$ singurele ideale care conțin pe $\underline{m}$ sunt $\underline{m}$ și $R \Longleftrightarrow$ (teorema de corespondență între ideale) singurele ideale ale lui $R/_{\underline{m}}$ sunt $\underline{m}/_{\underline{m}} = \{0\}$ și $R/_{\underline{m}} \Longleftrightarrow R$ e corp. $\boxtimes$

Exercițiul 1 Fie $f : R \to S$ morfism de inele comutative. Atunci:

1) Dacă $\underline{q} \in Spec(S) \Rightarrow f^{-1}(\underline{q}) \in Spec(R)$

2) Dacă f = surjectiv și $\left.\begin{array}{l} \underline{p} \in Spec(R) \\ \underline{p} \supseteq Ker(f) \end{array}\right\} \Rightarrow$ $f(\underline{p}) \in Spec(S)$.

3) $\underline{m} \in Max(S) \Rightarrow f^{-1}(\underline{m}) \in Max(R)$

4) Dacă f este surjectiv și $\underline{m} \in Max(R)$ a.î. $\underline{m} \supseteq Ker(f) \Rightarrow f(\underline{m}) \in Max(S)$.

Exercițiul 2 Fie $n \in \mathbb{N}$, $n \geq 2$. Atunci:

$$Spec(\mathbb{Z}_n) = Max(\mathbb{Z}_n) = \{(\hat{p}) \mid p \mid n, \ p = \text{prim}\}$$

Teoremă (Lema lui Krull) Fie R = inel comutativ și $I \subsetneq R$ un ideal. Atunci $(\exists)\ \underline{m} \in Max(R)$ a.î. $I \subseteq \underline{m}$.

În particular, $Max(R) \neq \phi$.

Dem O să folosim lema lui Zorn pentru:

$$\mathcal{P} := \{ J \mid J \subsetneq R, \ I \subseteq J \}.$$

$\mathcal{P} \neq \phi$, căci $I \in \mathcal{P}$ și $(\mathcal{P}, \subseteq)$ este o mulțime parțial ordonată.

Afirm: $(\mathcal{P}, \subseteq)$ este inductiv ordonată!

În adevăr, fie $(I_\lambda)_{\lambda \in \Lambda}$ o parte total ordonată a lui $\mathcal{P}$. Atunci vom arăta că:

$I_0 := \bigcup_{\lambda \in \Lambda} I_\lambda$ este un majorant a lui $(I_\lambda)_{\lambda \in \Lambda}$ ce aparține lui $\mathcal{P}$.

Să demonstrăm că $I_0 \in \mathcal{P}$. Fie $x, y \in I_0$ $\Rightarrow (\exists)\ \alpha, \beta \in \Lambda$ a.î. $x \in I_\alpha$ și $y \in I_\beta$ $\Rightarrow$

Pp. că $I_\alpha \subseteq I_\beta$ (cazul celălalt e analog) $\Rightarrow$

$x, y \in I_\beta \Rightarrow x - y \in I_\beta \subseteq I_0 \Rightarrow$

$x - y \in I_0$), i.e. $I_0 \leq (R, +)$. Fie acum $r \in R$. Atunci, $rx \in I_\alpha \subseteq I_0 \Rightarrow$

$rx \in I_0 \Rightarrow I_0$ e ideal în R și evident, $I \subseteq I_0$, căci $I_\lambda \supseteq I_0$, $(\forall)\lambda \in \Lambda$

Să arătăm că $I_0 \neq R$. Dacă

$I_0 = R \ni 1 \Rightarrow (\exists)\lambda \in \Lambda$ a.î. $1 \in I_\lambda \subseteq R$

$\Rightarrow I_\lambda = R$, fals! căci $I_\lambda \in \mathcal{P}$.

Am arătat deci că $(\mathcal{P}, \subseteq)$ este inductiv ordonată.

Din Lema lui Zorn $\Rightarrow \mathcal{P}$ are un element maximal $\underline{m}$, i.e. $\underline{m} \subsetneqq R$ și $\underline{m} \supseteq I$

Atunci, $\underline{m} \in Max(R)$, căci dacă

$\underline{m} \subseteq K \subsetneqq R \Rightarrow$ ($\underline{m}$ e element maximal în $\mathcal{P}$

$\Rightarrow K = \underline{m}$, i.e. $\underline{m}$ e ideal maximal al lui R. $\boxed{/\!/}$

$\boxed{\text{Corolar}}$ Fie R = inel comutativ. $\Rightarrow U(R) = R \setminus \bigcup_{\underline{m} \in Max(R)} \underline{m}$

Dem „$\subseteq$" Fie $r \in U(R)$. Dacă $r \in \bigcup_{\underline{m} \in Max(R)} \underline{m} \Rightarrow$ $(\exists)$ $\underline{m} \in Max(R)$ a.î. $r \in \underline{m} \Rightarrow$ (r e inversabil) $\underline{m} = R$, fals! Deci, $r \notin \bigcup_{\underline{m} \in Max(R)} \underline{m}$.

„$\supseteq$" Fie $r \in R \setminus \bigcup_{\underline{m} \in Max(R)} \underline{m}$. Dacă $r \notin U(R)$

$\Rightarrow Rr \subsetneqq R \underset{\text{Krull}}{\Longrightarrow} (\exists)$ $\underline{m}_0 \in Max(R)$ a.î.

$Rr \subseteq \underline{m}_0 \Rightarrow r \in \underline{m}_0$, fals! $\boxed{/\!/}$

Observație 1) Și idealele prime servesc la construcții de corpuri. Fie $p \in Spec(R) \Rightarrow$ $R/_p$ este domeniu de integritate $\Rightarrow$

$Q(R/_p)$ = corpul de fracții al lui $R/_p$ este un corp comutativ.

2) Lema lui Krull este unul din cele mai folosite rezultate în algebră. Demonstrația ei se bazează însă pe Lema Zorn (⇔) axioma alegerii din sistemul de axiome Z-F.

Dacă lema lui Zorn "pică" (i.e. sistemul de axiome ZF este contradictoriu) atunci aproape toată algebra modernă se prăbușește!

Așa că mă opresc aici! :)

Mulțumesc pentru audierea/citirea acestui curs!

Toate cele bune,

Gigel Militaru.