



$R$  măre,  $a \in R$  nu divizor al lui zero dacă  $\exists b \in R, b \neq 0$  astfel că  $ab = 0$ .

field = corp comutativ  
division ring = corp

Def  $\mathbb{F}$  este  $R$  domeniu de integrabilitate (comutativ + întreg) fără zero divizori

Dem Fie  $a \in R$ ,  $a \neq 0$  și funcția  $\varphi_a: R \rightarrow R$ ,  $\varphi_a(b) = ab$ .

$\varphi_a$  injectivă,  $R$  finit  
 $\Rightarrow \varphi_a$  surjectivă

1.  $\varphi_a$  este mijlocire de grupuri (distribuționalitate)

2.  $\text{Ker } \varphi_a = \{b \in R \mid \varphi_a(b) = 0 \Leftrightarrow ab = 0\} = \{0\}$ :  $ab = 0 \xrightarrow[a \neq 0]{R \text{ domeniu}} b = 0 \Rightarrow \exists b \text{ astfel că } ab = 0$

$(R \times R)$  este măre (cu operațiile de adunare și înmulțire și conjugat)

nu este domeniu:  $(1, 0) \cdot (0, 1) = (0, 0)$

!  $H$  corpul creătorialor

D (Wedderburn) Orice corp finit este comutativ!

2. a)  $Z_n$ ,  $n \geq 2$

$$\mathbb{Z}_n = \mathbb{Z} / n\mathbb{Z} = \{ \hat{0}, \hat{1}, \dots, \hat{n-1} \} = \{ \hat{a} \text{ mod } n \mid a \in \mathbb{Z} \},$$

$\hat{a} = \hat{b} \Leftrightarrow a - b \in n\mathbb{Z} \Leftrightarrow a \text{ und } b \text{ sind einachsektive } m \text{-erresten}$

$$\Leftrightarrow a - b \vdots n$$

$$\begin{aligned}\widehat{25} &= \widehat{4} \quad (\text{mod } 7) \\ &= \widehat{11}\end{aligned}$$

• Elemente invertierbar :  $\frac{\hat{a} \in \mathbb{Z}_n \quad \hat{a}^{-1} \text{ (a, n)} = 1}{\parallel}$

$\hat{a} \in \mathbb{Z}_n$  invertierbar  $\Leftrightarrow \exists \hat{b} \in \mathbb{Z}_n \text{ mit } \hat{a} \cdot \hat{b} = \hat{1} \Leftrightarrow$

$\hat{a}\hat{b} - 1 \vdots n \Leftrightarrow \exists k \in \mathbb{Z} \text{ mit } \hat{a}\hat{b} - 1 = nk \Leftrightarrow \boxed{\hat{a}\hat{b} - 1 = 1} \uparrow$

$$\Rightarrow (a, n) = 1.$$

Algorithmus von Euklid

Ex: Affatto, da aby der Euklid, ( $a, b$ ), und:

a)  $a = 1349, \quad b = 57$

b)  $a = 459, \quad b = 111$

c)  $\overbrace{\quad \quad \quad \quad \quad}$

$$U(\mathbb{Z}_n) = \{ \hat{a} \in \mathbb{Z}_n \mid (a, n) = 1 \}, \quad |U(\mathbb{Z}_n)| = \varphi(n)$$

indiziert den Euler

!  $\mathbb{Z} \text{ e. v. } \Leftrightarrow \text{m. p. f. } \Leftrightarrow \varphi(n) = n - 1$

$\exists \lambda \in \mathbb{Z}_m \Leftrightarrow m \in \text{prim} \Leftrightarrow \varphi(n) = n-1$

• direzione  $\leftarrow$ : zero :

$$\mathcal{D}(\mathbb{Z}_n) = \{a \in \mathbb{Z}_n \mid \exists b \neq 0 \text{ s.t. } ab = 0\}$$

Fix  $a \in \mathcal{D}(\mathbb{Z}_n) \Rightarrow \exists b \neq 0 \text{ s.t. } ab = 0 \Leftrightarrow \exists b \in \mathbb{Z} \text{ s.t. } n \mid ab \text{ and } b \neq 0$

$$\Rightarrow (a, n) \neq 1.$$

$$\Rightarrow \mathcal{U}(\mathbb{Z}_n) \cup \mathcal{D}(\mathbb{Z}_n) = \mathbb{Z}_n$$

• Eliminate multato : Fix  $a \in \mathbb{Z}_n$  s.t.  $\exists l \in \mathbb{N}^*$  s.t.  $a^l = 0$ .

$$\begin{array}{c} \exists l \in \mathbb{N}^* \\ (\Rightarrow) \sqrt{n \mid a^l} \end{array} \quad \boxed{\Leftrightarrow} \quad p_1 p_2 \dots p_k \mid a$$

$$n = p_1^{d_1} p_2^{d_2} \dots p_k^{d_k}$$

$$a^l = (2 \cdot 5 \cdot 7 \cdot 11)^l$$

$$= 2^l \cdot 5^l \cdot 7^l \cdot 11^l \mid n$$

$$n = 2^3 \cdot 5^2 \cdot 7 \cdot 11^5$$

$$a = 2 \cdot 5 \cdot 7 \cdot 11, \quad a = 2^{100} \cdot 5^2 \cdot 7^8 \cdot 11^8$$

$$a = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$$

$$\begin{cases} a = 2^2 \cdot 5^2 \cdot 7^2 \cdot 11^3 \\ l \text{ minima s.t. } 2 \end{cases}$$

Mean re: numeri acci  $0 \leq a < n$  s.t.  $p_1 p_2 \dots p_k \mid a$ .

$$0, 1 \cdot p_1 p_2 - p_8, 2 \cdot p_1 p_2 - p_8, 3 \cdot p_1 p_2 - p_8, \dots$$

$$\dots (p_1^{d_1-1} p_2^{d_2-1} \dots p_8^{d_8-1} - 1) \cdot p_1 p_2 \dots p_8$$

$$\Rightarrow \text{Nil}(Z_m) = p_1^{d_1-1} \dots p_8^{d_8-1} = \frac{m}{p_1 p_2 \dots p_8}$$

Qe) Date exemple de nmbre rationnel au exact 36 de clément négatifs.

$$\text{Cent } m \neq m \text{ a } 36 = p_1^{d_1-1} \dots p_8^{d_8-1}$$

$$n = p_1^{d_1} \dots p_8^{d_8}$$

$$= q_1^{p_1-1} \dots q_8^{p_8-1}$$

$$m = q_1^{p_1} \dots q_8^{p_8}$$

$$\text{Exemple, } n = 2^3 \cdot 3^3$$

$$36 = 2^2 \cdot 3^2$$

$$m = 2^3 \cdot 3^3 \cdot 19$$

$$n \neq m = 2^3 \cdot 3^3 \cdot 5$$

3. a) Fie  $R$  nmbri  $a \in R$  care este nr la care nu există la dreapta  $\Rightarrow a$  este ineleabil

a înălță rta:  $\exists b \in R$  cu  $b < a$

de:  $\exists c \in R$  cu  $c < a$

a inversabil :  $\exists d \in R$  astă  $da = ad = 1$

$$a = \cancel{da} \cdot c$$

$$\underbrace{ac}_{1} = \cancel{da} \cancel{ac}_1 \Rightarrow ac = 1 \Rightarrow \text{este inversă la } da$$

Dacă vădăm  $b = c$ :  $ab = ac \Rightarrow a(b - c) = 0 \mid b - c$

$$\Rightarrow \underbrace{ba}_{1} (b - c) = 0 \Leftrightarrow b = c$$

Deci  $b = bac = (ba) \cdot c = c$   $\leftarrow$

b) Dateaza că în  $R$  cu  $a \in R$  este inversabil

la stânga , dacă nu la dreapta  
dreapta stânga

$(\mathcal{F} = \{f: \mathbb{R} \rightarrow \mathbb{R} \text{ mărfură de grupă}\}, +, \circ)$

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

$$f \circ (g+h) = f \circ g + f \circ h \leftarrow f \text{ mărfură de grupă}$$

fără inversă la stânga  $\exists g \in \mathcal{F}$  astă  $gf = id_{\mathbb{R}}$

$\Rightarrow$  f este injectivă

Iată Dacă există un număr de elemente  $f: \mathbb{R} \rightarrow \mathbb{R}$  care sunt injective, dacă nu sunt surjective.

c) Dacă  $a \in \mathbb{R}$  este un inele în dreptă, dacă la astăzi există o infinitate de inele în dreptă.

Există  $a' \in \mathbb{R}$  cu  $aa' = 1$

Tie  $M = \{b \in \mathbb{R} \mid ab = 1\}$  și  $f: M \rightarrow M, f(b) = ba + a' - 1$ .

$$\begin{aligned} & - \text{colect definită i.e. } f(b) \in M : a(ba + a' - 1) = aba + aa' - a \\ & \qquad \qquad \qquad = a + 1 - a = 1 \end{aligned}$$

$$\begin{aligned} & - f \text{ injectivă: Dacă } b+c \text{ și } f(b) = f(c) \Rightarrow ba + a' - 1 = ca + a' - 1 \\ & \qquad \qquad \qquad (\Rightarrow) ba = ca \quad (\Rightarrow) (b-c)a = 0 \cdot a' \end{aligned}$$

$$(\Rightarrow) b-c=0 \Rightarrow b=c \text{ și}$$

$$\begin{aligned} & - f \text{ nu este surjectivă: } a' \notin f(M) . \text{ Afirmație: } \exists b \in M \text{ cu } f(b) = a' \\ & \qquad \qquad \qquad (\Rightarrow) ba + a' - 1 = a' \quad (\Rightarrow) ba = 1 \end{aligned}$$

do

$\Rightarrow M$  infinită.

4. a) Für  $R$  mit  $a, b \in R$ .

Atmen  $1 - ab$  invertierbar lösbar ( $\Rightarrow 1 - ba$  invertierbar in  $R$ )

$$\text{Denn } \frac{1}{1-ab} = 1 + ab + abab + ab \cdot ab \cdot ab + \dots \leftarrow \begin{array}{l} \text{Kette folgen,} \\ \text{alle } ab \text{ aus in } R \end{array}$$

$$\begin{aligned} \frac{1}{1-ba} &= 1 + (ba + ba ba + ba ba ba + \dots) \\ &= 1 + b \underbrace{\left(1 + a + aa + \dots\right)}_a \end{aligned}$$

Da  $ca$   $1 - ab$  in  $R$  lösbar  $\Rightarrow \exists n \in \mathbb{N} (1 - ab)^n = 1$

Aber  $v = 1 + b n a$

$$v(1 - ba) = (1 + bna)(1 - ba) = 1 - ba + bna - \cancel{ba} \cancel{ba}$$

$$= 1 - ba + bna - b(n-1)a = 1 - ba + \cancel{bna} - \cancel{ba} + ba = 1$$

le) Fie  $R$  un inel și  $A \in M_{m,m}(R)$ ,  $B \in M_{n,n}(R)$ .

At  $I_m - AB$  este în  $M_m(R) \Leftrightarrow I_m - BA$  este în  $M_n(R)$

Dem La fel!

5. Fie  $L = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\} \subseteq M_2(\mathbb{R})$

Demonstrați că  $(L, +, \cdot)$  este o c.c. comutativă  
admitând înmulțirea matricelor

Mai mult, aplicarea  $\varphi: \mathbb{C} \rightarrow L$ ,  $\varphi(a+bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$   
este izomorfism de corpuri.

Dem • Def/Obs  $L \subset M_2(\mathbb{R})$  este un inel, adică

$$\left\{ \begin{array}{l} M+N \in L, \quad M, N \in L \leftarrow \text{rulează în raport cu +} \\ M \cdot N \in L, \quad M, N \in L \leftarrow \text{nu este stabilită la} \\ I_2 \in L \end{array} \right.$$

$$\text{Die } M_1 = \begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix}, \quad M_2 = \begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix} \in L$$

$$M_1 + M_2 = \begin{pmatrix} (a_1+a_2) & (b_1+b_2) \\ -(b_1+b_2) & (a_1+a_2) \end{pmatrix} \in L, \quad M_1 \cdot M_2 = \begin{pmatrix} a_1a_2 - b_1b_2 & a_1b_2 + b_1a_2 \\ -(a_1b_2 + b_1a_2) & a_1a_2 - b_1b_2 \end{pmatrix} \in L$$

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in L \quad (a=1, b=0)$$

↑

$\Rightarrow L$  ist ein reeller.

- $\varphi: C \rightarrow L$  ist morphismus:

$$\varphi(a+bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

$$\varphi((a_1+b_1i) \cdot (a_2+b_2i)) = \varphi((a_1a_2 - b_1b_2) + (a_1b_2 + b_1a_2)i)$$

$$= \begin{pmatrix} a_1a_2 - b_1b_2 & a_1b_2 + b_1a_2 \\ -(a_1b_2 + b_1a_2) & a_1a_2 - b_1b_2 \end{pmatrix} \stackrel{\text{matrix}}{=} \begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix} \cdot \begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix}$$

$$= \varphi(a_1+b_1i) \cdot \varphi(a_2+b_2i)$$

Es folgt,  $\varphi((a_1+b_1i) + (a_2+b_2i)) = \varphi(a_1+b_1i) + \varphi(a_2+b_2i)$

$\Rightarrow \Psi$  e morfism de níveis.

•  $\Psi$  e dizer isomorfismo:  $\Psi: L \rightarrow \mathbb{C}$ , ai  $\Psi \circ \varphi = \text{id}_{\mathbb{C}}$   
 $\varphi \circ \Psi = \text{id}_L$

$$\Psi \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a+bi$$

$$3+2i \mapsto \begin{pmatrix} 3 & 2 \\ -2 & 3 \end{pmatrix}$$

$$\Rightarrow \Psi \circ \varphi = \text{id}_{\mathbb{C}}, \varphi \circ \Psi = \text{id}_L$$

$$5+4i \mapsto \begin{pmatrix} 5 & 4 \\ -4 & 5 \end{pmatrix}$$

$\Psi$  isomorfismo  $L$  e  $\mathbb{C}$  por

Matrizes invertíveis

$$\frac{1}{a^2+b^2} \begin{pmatrix} a & b \\ -b & a \end{pmatrix}^{-1} = \frac{1}{a^2+b^2} \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = \frac{1}{a^2+b^2} + i \frac{-b}{a^2+b^2}$$

$$\rightarrow \begin{pmatrix} a & b \\ -b & a \end{pmatrix}^{-1} = \begin{pmatrix} \frac{a}{a^2+b^2} & -\frac{b}{a^2+b^2} \\ \frac{b}{a^2+b^2} & \frac{a}{a^2+b^2} \end{pmatrix} = \frac{1}{a^2+b^2} \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

6. Matrizes cuadradas nel R re responden unto um nivéu de forma  
End(G), unde G e grupo abelian.

End(G),  $\circ$   $\circ$   $\circ$

re sonda:  $\exists \varphi: R \rightarrow \text{End}(G)$  morphismus injektiv de  $(\text{End}(G), +, \circ)$  in  $\mathbb{Z}$

Idee:  $\text{Ist } G = R \text{ zu } \varphi: R \rightarrow \text{End}(G)$ ,

$$\varphi(a) = \varphi_a \in \text{End}(G), \text{ und}$$

$$\varphi_a(b) = ab, \quad \forall b \in G$$

$$(\varphi(a))''(b)$$

- Correct def:  $\varphi_a \in \text{End}(R)$  i.e.  $\varphi_a$  endomorphismus ✓

-  $\varphi$  morphismus de  $\mathbb{Z}$ : 1.  $\varphi(a+b) = \varphi(a) + \varphi(b)$ ,  $\forall a, b \in R$

$$\text{Für } c \in R. \quad (\varphi(a+b))(c) = (a+b) \cdot c = ac + bc = (\varphi(a))(c) + (\varphi(b))(c)$$

$$2. \quad \varphi(a \cdot b) = \varphi(a) \circ \varphi(b), \quad \forall a, b \in R$$

$$\text{Für } c \in R. \quad (\varphi(ab))(c) = ab \cdot c = a \cdot (bc) = a \left[ (\varphi(b))(c) \right]$$

$$= \varphi(a) \left[ (\varphi(b))(c) \right] = \underbrace{(\varphi(a) \circ \varphi(b))(c)}$$

-  $\varphi$  injectivă: Dacă  $\varphi_a = \varphi_b \Rightarrow \varphi_a(1) = \varphi_b(1) \Leftrightarrow a = b$ .

EBC Determinați toate morfismele unitare ( $f: \mathbb{R} \rightarrow S$  și cu de  
inieție unită dacă  $f(1_R) = 1_S$ ) de inele:

- de la  $\mathbb{Z}$  la  $\mathbb{Z}$

Fie  $f: \mathbb{Z} \rightarrow \mathbb{Z}$  morfism unită de inieție.

$$\Rightarrow f(1) = 1. \quad \text{De } n > 0 \quad f(n) = f(\underbrace{1+1+\dots+1}_{n\text{ ori}}) = \underbrace{f(1)+\dots+f(1)}_{n\text{ ori}} = n \cdot f(1) = n$$

În plus,  $\forall m > 0 \quad f(-m) = -f(m) = -m \Rightarrow \boxed{f(k) = k, \forall k \in \mathbb{Z}}$

$$\Leftrightarrow f = \text{id}_{\mathbb{Z}}$$

- de la  $\mathbb{Z}$  la  $\mathbb{Q}$

La fel, dacă  $f: \mathbb{Z} \rightarrow \mathbb{Q}$  morfism unită de inieție, atunci  
 $f(n) = n, \quad \forall n \in \mathbb{Z} \Rightarrow f: \mathbb{Z} \hookrightarrow \mathbb{Q}$  este inclusiunea lui  $\mathbb{Z}$  în  $\mathbb{Q}$

• de la  $\mathbb{Q}$  în  $\mathbb{Z}$

Prin cînd  $f: \mathbb{Q} \rightarrow \mathbb{Z}$  m.u. de i.

$$\Rightarrow 1 = f(1) = f(n \cdot \frac{1}{n}) = f\left(\frac{1}{n} + \frac{1}{n} + \dots + \frac{1}{n}\right) \stackrel{\text{mod de grupă}}{=} n \cdot f\left(\frac{1}{n}\right)$$

$\Rightarrow n \neq 1$  în  $\mathbb{Z}$ ! do

• de la  $\mathbb{Z}_m$  la  $\mathbb{Z}_m$

Fie  $f: \mathbb{Z}_m \rightarrow \mathbb{Z}_m$  m.u. de măs.

$$f(1 \pmod{m}) = 1 \pmod{m}$$

$$\xrightarrow[\text{răs}]{} f(2 \pmod{m}) = 2 \pmod{m}$$

$$f(m \pmod{m}) = m \pmod{m} \xrightarrow[\text{răs}]{\text{Kern}} 0 \pmod{m}$$

$\Rightarrow m|m$  & recerat

Un reprezentat  $m=n$ :

$f: \mathbb{Z}_4 \rightarrow \mathbb{Z}_2$
$f: \begin{matrix} \hat{0} & \rightarrow 0 \\ \hat{1} & \rightarrow 1 \\ \hat{2} & \rightarrow 0 \\ \hat{3} & \rightarrow 1 \end{matrix}$

Dacă  $f: \mathbb{Z}_m \rightarrow \mathbb{Z}_n$  este un homomorfism de mulțimi

$\left\{ \begin{array}{l} \text{c.m.d. } m/n \\ \exists, \text{ mult.} \end{array} \right.$

• de la  $\mathbb{Q}$  la  $\mathbb{Q}$

Fie  $f: \mathbb{Q} \rightarrow \mathbb{Q}$ ,  $f$  moarcă de mulțimi.

$\forall m, \exists n$  cele de mai sus:  $f(m) = m$ ,  $\forall m \in \mathbb{Z}$

$$1 = f(1) = f\left(\underbrace{\frac{1}{m} + \frac{1}{m} + \dots + \frac{1}{m}}_{n \text{ ori}}\right) = \underline{nf\left(\frac{1}{m}\right)} \Rightarrow f\left(\frac{1}{m}\right) = \frac{1}{m},$$

$\forall n \neq 0$   
 $n \in \mathbb{Z}$

$$\Rightarrow f\left(\frac{m}{n}\right) = f(m) \cdot f\left(\frac{1}{n}\right) = m \cdot \frac{1}{n} = \frac{m}{n}, \quad \forall m, n \in \mathbb{Z},$$

$n \neq 0$

$$\text{If } f(n) = f(m) \text{ then } n = m \text{ or } n \neq m$$

- de la R la R

Fie  $f: \mathbb{R} \rightarrow \mathbb{R}$  nofinc multe de inele

Din cele de mai sus,  $f|_{\mathbb{Q}} = \text{id}_{\mathbb{Q}}$  i.e.  $f(g) = g, \forall g \in \mathbb{Q}$

- Fie  $x > 0 \Rightarrow \exists y \in \mathbb{R}$  cu  $x = y^2$

$$\Rightarrow f(x) = f(y^2) \xrightarrow[\text{inele}]{\text{nofinc}} (f(y))^2 \geq 0$$

- Fie  $a < b \Rightarrow f(a) \leq f(b)$  (monotona)

Intrebare:  $\frac{f(b-a)}{b-a} \xrightarrow[\text{nofinc}]{>0} f(b)-f(a)$

- Dacă  $f: \mathbb{R} \rightarrow \mathbb{R}$  monotona și  $f(g) = g, \forall g \in \mathbb{Q}$ .

Fie  $x \in \mathbb{R} \Rightarrow \exists (g_n)_n \nearrow x, g_n \in \mathbb{Q}$

$$\exists (g_n')_n \searrow x, g_n' \in Q$$

$$\Rightarrow f(g_n' - g_n) > 0$$

$$\begin{aligned} & \left| f(g_n') - f(g_n) \right| \\ & g_n' - g_n \xrightarrow{n \rightarrow \infty} 0 \end{aligned} \quad \Rightarrow f(g_n') - f(g_n) \rightarrow 0$$

$$\begin{aligned} & \left| f(g_n) - f(x) \right| \\ & g_n \rightarrow x \end{aligned} \quad \Rightarrow f(g_n) \rightarrow f(x)$$

• de la C la C

Tie  $f: C \rightarrow C$  nofuntor de mèt.

$$f(a+bi) = a + b f(i), \quad \forall a, b \in Q.$$

! Tens  $f(a+bi) = a + b f(i), \quad \forall a, b \in R$

Qes  $f(i)^2 = -1 \Rightarrow f(i) = i \text{ rere } -i$

$$\begin{aligned} & \Rightarrow f \rightarrow id_C \\ & \qquad \downarrow \\ & f(z) = \bar{z}. \end{aligned}$$

$$\downarrow f(z) = \bar{z}.$$

• Tenzw.: de la  $\mathcal{O}(V_2)$  la  $\mathcal{O}(V_2)$

$$\mathcal{O}(V_2) = \{a + bV_2 \mid a, b \in \mathbb{Q}\} \quad \text{volg (van velen)}$$

Relevante data reuten.