

SEMINAR CORPURI

Ex. 1. Fie $(F, +, \cdot)$ un corp. Notăm cu $\text{char}(F)$ ordinul lui 1_F în $(F, +)$. Demonstrați că dacă $\text{char}(F) < \infty$, atunci $\text{char}(F)$ este număr prim.

Soluție. Presupunem că numărul $\text{char}(F) = n \in \mathbb{N}^*$ nu este prim. Rezultă că există $a, b \in \mathbb{N}$ cu $1 < a, b < n$ astfel încât $n = ab$. Din $n1_F = 0_F$ rezultă $(a1_F)(b1_F) = 0_F$. Dar F nu are divizori ai lui zero. De aici obținem $a1_F = 0$ sau $b1_F = 0$, deci $\text{ord}_{(F,+)}(1_F) < n$, contradicție.

Observația 0.1. Ordinul $\text{char}(F)$ al lui 1_F în $(F, +)$ se numește caracteristica inelului (corpului) F . La curs caracteristica a fost definită ca fiind numărul n pentru care $\text{Ker}(\phi) = n\mathbb{Z}$, unde $\phi : \mathbb{Z} \rightarrow F$ este morfismul definit de $\phi(k) = k1_F$. Cazul $n = 0$ corespunde cazului $\text{ord}_{(F,+)}(1_F) = \infty$. În literatură sunt întâlnite ambele variante, adică: dacă un inel are caracteristica 0, atunci $\text{ord}_{(F,+)}(1_F) = \infty$.

Ex. 2. a) Arătați că intersecția de subcorpuri este subcorp.

b) Dacă F este un corp, atunci există $P(F)$ cel mai mic (relativ la \subseteq) subcorp al lui F .

c) Demonstrați că

$$\begin{cases} \text{char}(F) = \infty \Rightarrow P(F) \cong \mathbb{Q}; \\ \text{char}(F) = p \in \mathbb{N}^* \Rightarrow P(F) \cong \mathbb{Z}_p. \end{cases}$$

Soluție. a) Fie $K_i, i \in I$, o familie de subcorpuri ale corpului F . Atunci i) $\forall i \in I, 0, 1 \in K_i \Rightarrow 0, 1 \in \bigcap_{i \in I} K_i$.

ii) Fie $x, y \in \bigcap_{i \in I} K_i$. Atunci $\forall i \in I, x, y \in K_i$. Cum K_i sunt subcorpuri, rezultă că $\forall i \in I, x - y \in K_i$. Deci $x - y \in \bigcap_{i \in I} K_i$.

iii) Fie $x, y \in \bigcap_{i \in I} K_i$ cu $y \neq 0$. Atunci $\forall i \in I, x, y \in K_i$. Cum K_i sunt subcorpuri, rezultă că $\forall i \in I, xy^{-1} \in K_i$. Deci $xy^{-1} \in \bigcap_{i \in I} K_i$.

Așadar $\bigcap_{i \in I} K_i$ verifică toate condițiile din caracterizarea subcorpurilor, deci $\bigcap_{i \in I} K_i$ este un subcorp al lui F .

b) Fie $P(F)$ intersecția tuturor subcorpurilor lui F . Din a) rezultă că $P(F)$ este subcorp în F . Oricare ar fi K un subcorp al lui F el apare ca factor în intersecția considerată. Deci $P(F) \subseteq K$ și demonstrația este completă.

c) Cazul $\text{char}(F) = \infty$: Considerăm funcția $\alpha : \mathbb{Q} \rightarrow F$ definită de $\alpha\left(\frac{m}{n}\right) = (m1_F)(n1_F)^{-1}$ pentru orice $m \in \mathbb{Z}$ și $n \in \mathbb{Z}^*$.

Demonstrăm că α este bine definită. În primul rând, din $n \neq 0$ și $\text{char}(F) = \infty$, rezultă $n1_F \neq 0_F$, deci există $(n1_F)^{-1}$.

Presupunem că $\frac{m}{n} = \frac{a}{b}$. Trebuie să demonstrăm că $(m1_F)(n1_F)^{-1} = (a1_F)(b1_F)^{-1}$.

In general, pentru $k \in \mathbb{N}^*$ și $x \in F$ avem

$$(k1_F)x = \underbrace{(1_F + \cdots + 1_F)}_{\text{de } n \text{ ori}}x = \underbrace{(x + \cdots + x)}_{\text{de } n \text{ ori}} = x \underbrace{(1_F + \cdots + 1_F)}_{\text{de } n \text{ ori}} = x(k1_F).$$

De aici se deduce că pentru orice $k \in \mathbb{Z}$ și orice $x \in F$ avem $(k1_F)x = x(k1_F)$.

Din $\frac{m}{n} = \frac{a}{b}$ rezultă $mb = an$, așadar $(m1_F)(b1_F) = (a1_F)(n1_F)$. Aplicând observația anterioară se deduce că $(m1_F)(n1_F)^{-1} = (a1_F)(b1_F)^{-1}$, deci α este bine definită.

Demonstrăm că α este morfism de corpuri. Fie $\frac{m}{n}, \frac{a}{b} \in \mathbb{Q}$. Avem

$$\begin{aligned} \alpha\left(\frac{m}{n} + \frac{a}{b}\right) &= \alpha\left(\frac{mb + an}{nb}\right) = [(mb + an)1_F](nb1_F)^{-1} \\ &= (mb1_F)(nb1_F)^{-1} + (an1_F)(nb1_F)^{-1} \\ &= (m1_F)(b1_F)(n1_F)^{-1}(b1_F)^{-1} + (a1_F)(n1_F)(n1_F)^{-1}(b1_F)^{-1} \\ &= (m1_F)(n1_F)^{-1} + (a1_F)(b1_F)^{-1} = \alpha\left(\frac{m}{n}\right) + \alpha\left(\frac{a}{b}\right), \end{aligned}$$

deci α este aditivă.

Analog se demonstrează că α este multiplicativă.

Se constată că α este funcție injectivă:

$$\frac{m}{n} \in \text{Ker}(\alpha) \Leftrightarrow m1_F = 0 \Leftrightarrow m = 0.$$

Rezultă că α este un morfism de corpuri, deci

$$\alpha(\mathbb{Q}) = \{(m1_F)(n1_F)^{-1} \mid m, n \in \mathbb{Z}, n \neq 0\}$$

este un subcorp al lui F . Dacă luăm un subcorp K al lui F , rezultă că $1_F \in K$, deci pentru orice $m \in \mathbb{Z}$ avem $m1_F \in K$. Mai mult, dacă $n \in \mathbb{N}^*$ avem $0_F \neq n1_F \in K$, deci $(m1_F)(n1_F)^{-1} \in K$ pentru orice $m, n \in \mathbb{Z}$ cu $n \neq 0$. Am demonstrat că $\alpha(\mathbb{Q}) \subseteq K$, oricare ar fi K subcorp al lui F . Deci $\alpha(\mathbb{Q})$ este cel mai mic subcorp al lui F și avem $\alpha(\mathbb{Q}) = P(F)$.

Cazul $\text{char}(F) = p$, unde p este număr prim se tratează analog, folosind funcția $\beta : \mathbb{Z}_p \rightarrow F$, $\beta(\widehat{k}) = k1_F$.

Observația 0.2. Subcorpul $P(F)$ se numește *subcorpul prim* al lui F . Dacă $F = P(F)$, atunci spunem că F este un *corp prim*. Orice corp prim este izomorf cu \mathbb{Q} sau \mathbb{Z}_p (unde p este număr prim).

Ex. 3. (Temă) Demonstrați că orice morfism de corpuri este injectiv.

Indicație. Se calculează nucleul morfismului folosind caracterizarea corpurilor prin absența idealelor și faptul că orice morfism de corpuri trebuie să fie unital.

Ex. 4. Fie $F = \{0, 1, a, b\}$ un corp cu 4 elemente. Demonstrați că

- a) $ab = ba = 1$;
- b) $a^2 = b$, $a^3 = 1$, $a^2 + a + 1 = 0$;
- c) $1 + 1 = 0$.

Soluție. a) Evident $ab \in \{1, a, b\}$. Dacă $ab \neq 1$ se deduce că $b = 1$ (pt $ab = a$) sau $a = 1$, imposibil. Deci $ab = 1$. Analog și $ba = 1$.

b) Știm că (F^*, \cdot) este un grup. Deci $a^3 = b^3 = 1$ (Teorema lui Lagrange).

Apoi, $a^2 \in \{1, a, b\}$. Din $a^2 = 1$ se deduce că $\text{ord}(a) = 2$, dar $2 \nmid 3$, contradicție. Analog, din $a^2 = a$ am obține $a = 1$, imposibil. Deci singura variantă este $a^2 = b$.

[De fapt putem folosi izomorfismul $(F^*, \cdot) \cong (\mathbb{Z}_3, +)$ ca să obținem proprietățile de mai sus.]

Pentru ultima afirmație, constatăm că $0 = a^3 - 1 = (a - 1)(a^2 + a + 1)$ și $a - 1 \neq 0$.

c) Ordinul lui 1 în $(F, +)$ poate să fie 2 sau 4. Dar din Ex. 1 știm că trebuie să fie număr prim. Deci $1 + 1 = 0$.

Ex. 5. Demonstrați că:

- a) $K = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{Z}_5 \right\}$ este un subinel al inelului matricilor $(\mathcal{M}_2(\mathbb{Z}_5), +, \cdot)$ care nu este corp.
- b) $L = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{Z}_7 \right\}$ este un corp față de operațiile obișnuite $+$ și \cdot .

Soluție. a) Pentru prima cerință se verifică toate condițiile din teorema de caracterizare a subinelurilor.

Pentru ce-a de-a doua, dacă $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in K^*$ este inversabilă, rezultă că există $B \in K$ astfel încât $AB = BA = I_2$. Deci A este inversabilă în inelul matricilor de tip 2×2 cu coeficienți în \mathbb{Z}_5 (și că $B = A^{-1}$). Rezultă că $\det(A) \neq \widehat{0}$. Așadar $a^2 + b^2 \neq \widehat{0}$.

Dar pentru $a = \widehat{1}$ și $b = \widehat{2}$ avem $a^2 + b^2 = \widehat{0}$, deci matricea $\begin{pmatrix} \widehat{1} & \widehat{2} \\ -\widehat{2} & \widehat{1} \end{pmatrix} \in$

K nu este inversabilă. Rezultă că inelul K nu este corp.

b) Analog cu a) se demonstrează că L este subinel în $\mathcal{M}_2(\mathbb{Z}_7)$. Ca să demonstrăm că este corp, trebuie să demonstrăm că oricare ar fi $A \in L$, $A \neq 0_2$, A este inversabilă în L . Cu un raționament analog cu cel anterior deducem că trebuie să demonstrăm că matricile nenule din L sunt inversabile în $\mathcal{M}_2(\mathbb{Z}_7)$ și că inversele lor sunt în L .

Dacă $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in L$, atunci $\det(L) = a^2 + b^2$. Calculăm pătratele elementelor din \mathbb{Z}_7 și obținem următorul tabel de valori:

x	$\widehat{0}$	$\widehat{1}$	$\widehat{2}$	$\widehat{3}$	$\widehat{4}$	$\widehat{5}$	$\widehat{6}$
x^2	$\widehat{0}$	$\widehat{1}$	$\widehat{4}$	$\widehat{2}$	$\widehat{2}$	$\widehat{4}$	$\widehat{1}$

Constatăm prin verificare directă ca din $a^2 + b^2 = \widehat{0}$ rezultă $a = b = \widehat{0}$.

Așadar, oricare ar fi $A = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \in L$ cu $A \neq 0_2$, A este inversabilă în $\mathcal{M}_2(\mathbb{Z}_7)$. Calculând $A^{-1} = (\det(A))^{-1} \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, constatăm că $A^{-1} \in L$.

Deci toate elementele nenule din L sunt inversabile și rezultă că $(L, +, \cdot)$ este un corp.

Observația 0.3. Am realizat verificarea că din $a^2 + b^2 = \widehat{0}$ în \mathbb{Z}_7 rezultă că $a = b = \widehat{0}$ pe cale empirică. De fapt se poate demonstra că dacă p este un număr prim de forma $p = 4k + 3$ și $a^2 + b^2 = \widehat{0}$ în \mathbb{Z}_p , atunci $a = b = \widehat{0}$.

O variantă pentru a obține această implicație este următoarea:

Presupunem că $a \neq \widehat{0}$ și $b \neq \widehat{0}$. Atunci $a^{p-1} = b^{p-1} = \widehat{1}$ (aceasta este mica teoremă a lui Fermat, dar identitatea poate fi obținută direct lucrând în grupul (\mathbb{Z}_p^*, \cdot) (vezi cursul cu aplicațiile teoriei grupurilor). Obținem

$$\widehat{2} = (a^2)^{2k+1} + (b^2)^{2k+1} = (a^2 + b^2)(\dots) = \widehat{0},$$

ceea ce este imposibil pt că p este impar.

Pe de altă parte, orice număr prim de forma $4k + 1$ este suma a două pătrate perfecte

[https://en.wikipedia.org/wiki/Proofs_of_Fermat%](https://en.wikipedia.org/wiki/Proofs_of_Fermat%27s_theorem_on_sums_of_two_squares)

[27s_theorem_on_sums_of_two_squares.](https://en.wikipedia.org/wiki/Proofs_of_Fermat%27s_theorem_on_sums_of_two_squares)

Deci, dacă în a) înlocuim 5 cu un număr prim de forma $4k + 1$ atunci obținem un inel care nu este corp.

Ex. 6. Fie K și L corpuri comutative de caracteristica ∞ . Demonstrați că o funcție $f : K \rightarrow L$ este un morfism de corpuri dacă și numai

- a) $f(x + y) = f(x) + f(y)$ pentru orice $x, y \in K$;
- b) $f(x^3) = f(x)^3$ pentru orice $x \in K$
- c) $f(1) = 1$.

Soluție. Demonstrația pentru \Rightarrow se realizează prin aplicarea definiției morfismului.

(\Leftarrow) Fie $x \in K$. Din identitatea $f((1+x)^3) = f(1+x)^3$ se deduce că $3f(x^2) = 3f(x)^2$, iar ipoteza asupra caracteristicii implică $f(x^2) = f(x)^2$ (această egalitate este valabilă pentru orice $x \in R$).

Dacă $x, y \in K$, cum K este comutativ, avem $2xy = (x+y)^2 - x^2 - y^2$. Deci $2f(xy) = f((x+y)^2) - f(x^2) - f(y^2) = f(x+y)^2 - f(x)^2 - f(y)^2 = (f(x) + f(y))^2 - f(x)^2 - f(y)^2 = 2f(x)f(y)$. În final deducem că $f(xy) = f(x)f(y)$ pentru orice $x, y \in K$.

Observația 0.4. (Temă) Verificați care din axiomele corpului sunt într-adevăr necesare în soluția exercițiului precedent și încercați să dați un enunț în care ipotezele să fie minimale. Este necesar să cerem $\text{char}(K) = \infty$?

TEMĂ

Ex. 7. Fie p un număr prim și

$$L_p = \left\{ \begin{pmatrix} a & b \\ pb & a \end{pmatrix} \mid a, b \in \mathbb{Z} \right\},$$

$$L_{-p} = \left\{ \begin{pmatrix} a & b \\ -pb & a \end{pmatrix} \mid a, b \in \mathbb{Z} \right\},$$

respectiv

$$M_p = \{a + b\sqrt{p} \mid a, b \in \mathbb{Z}\}.$$

$$M_{ip} = \{a + bi\sqrt{p} \mid a, b \in \mathbb{Z}\}.$$

- Demonstrați că L_p , L_{-p} , M_p și M_{ip} sunt domenii de integritate față de operațiile obișnuite de $+$ și \cdot care nu sunt corpuri.
- Demonstrați că $L_p \cong M_p$.
- Demonstrați că $L_{-p} \cong M_{ip}$.
- Demonstrați că $L_2 \not\cong M_3$.
- Demonstrați că $L_2 \not\cong M_{-2}$.
- Demonstrați că dacă $p \neq q$ sunt numere prime, atunci $M_p \not\cong M_q$, $M_p \not\cong M_{iq}$, $M_{ip} \not\cong M_{iq}$.

Ex. 8. Fie p un număr prim și

$$L_p = \left\{ \begin{pmatrix} a & b \\ pb & a \end{pmatrix} \mid a, b \in \mathbb{Q} \right\},$$

$$L_{-p} = \left\{ \begin{pmatrix} a & b \\ -pb & a \end{pmatrix} \mid a, b \in \mathbb{Q} \right\},$$

respectiv

$$M_p = \{a + b\sqrt{p} \mid a, b \in \mathbb{Q}\}.$$

$$M_{ip} = \{a + bi\sqrt{p} \mid a, b \in \mathbb{Q}\}.$$

- a) Demonstrați că L_p , L_{-p} , M_p și M_{ip} sunt corpuri față de operațiile obișnuite de $+$ și \cdot .
- b) Demonstrați că $L_p \cong M_p$.
- c) Demonstrați că $L_{-p} \cong M_{ip}$.
- d) Demonstrați că $L_2 \not\cong M_3$.
- e) Demonstrați că $L_2 \not\cong M_{-2}$.
- f) Demonstrați că dacă $p \neq q$ sunt numere prime, atunci $M_p \not\cong M_q$, $M_p \not\cong M_{iq}$, $M_{ip} \not\cong M_{iq}$.