Seminar corpuri

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

Soluţie. Presupunem că numărul $\text{char}(F) = n \in \mathbb{N}^\star$ 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 obţinem $a1_F = 0$ sau $b1_F = 0$, deci $\text{ord}_{(F,+)}(1_F) < n$, contradicţie.

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

Ex. 2. a) Arătaţi că intersecţia 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) Demonstraţi că

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

Soluţie. 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, rezută 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, rezută că $\forall i \in I, xy^{-1} \in K_i$. Deci $xy^{-1} \in \bigcap_{i\in I} K_i$.

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

b) Fie $P(F)$ intersecţia 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 intersecţia considerată. Deci $F(F) \subseteq K$ şi demonstraţia este completă.

c) Cazul $\text{char}(F) = \infty$: Considerăm funcţia $\alpha : \mathbb{Q} \to F$ definită de $\alpha(\frac{m}{n}) = (m1_F)(n1_F)^{-1}$ pentru orice $m \in \mathbb{Z}$ şi $n \in \mathbb{Z}^\star$.

Demonstrăm că α este bine definită. In primul rând, din $n \neq 0$ şi $\text{char}(F) = \infty$, rezultă $n1_f \neq 0_F$, deci există $(n1_F)^{-1}$.

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

In general, pentru $k \in \mathbb{N}^\star$ şi $x \in F$ 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 $k \in \mathbb{Z}$ şi orice $x \in F$ avem $(k1_F)x = x(k1_F)$.

Din $\frac{m}{n} = \frac{a}{b}$ rezultă $mb = an$, aşadar $(m1_F)(b1_F) = (a1_F)(n1_F)$. Aplicând observaţia anterior a 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

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

deci α este aditivă.

Analog se demonstrează că α este multiplicativă.

Se constată că α este funcţie injectivă:

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

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 $n \in \mathbb{N}^\star$ avem $0_F \neq n1_F \in K$, deci $(m1_F)(n1_F)^{-1} \in K$ prntru 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 şi avem $\alpha(\mathbb{Q}) = P(F)$.

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

Observaţia 0.2. Subcorpul $P(F)$ se numeşte *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) Demonstraţi că orice morfism de corpuri este injectiv.

Indicaţie. Se calculează nucleul morfismului folosind caracterizarea corpurilor prin absenţa idealelor şi faprul că orice morfism de corpuri trebuie să fie unital.

Ex. 4. Fie $F = \{0, 1, a, b\}$ un corp cu 4 elemente. Demonstraţi că
a) $ab = ba = 1$;
b) $a^2 = b$, $a^3 = 1$, $a^2 + a + 1 = 0$;
c) $1 + 1 = 0$.

Soluţie. 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 şi $ba = 1$.

b) Ştim că $(F^\star, \cdot)$ 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 $2 \nmid 3$, contradicţie. Analog, din $a^2 = 2$ am obţine $a = 1$, imposibil. Deci singura variantă este $a^2 = b$.

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

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

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

Ex. 5. Demonstraţi 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 faţă de operaţiile obiŋuite $+$ şi $\cdot$.

Soluţie. a) Pentru prima cerinţă se verifică toate condiţiile din teorema de caracterizare a subinelelor.

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

Dar pentru $a = \widehat{1}$ şi $b = \widehat{2}$ 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 raţionament analog cu cel anterior deducem că trebuie să demonstrăm căm matricile nenule din L sunt inversabile în $\mathcal{M}_2(\mathbb{Z}_7)$ şi 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 $\mathbb{Z}_7$ şi obţinem următorul tabel de valori:

$$\begin{array}{c|c|c|c|c|c|c|c} x & \widehat{0} & \widehat{1} & \widehat{2} & \widehat{3} & \widehat{4} & \widehat{5} & \widehat{6} \\ \hline x^2 & \widehat{0} & \widehat{1} & \widehat{4} & \widehat{2} & \widehat{2} & \widehat{4} & \widehat{1} \end{array}.$$

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

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

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

Observaţia 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 $p = 4k + 3$ şi $a^2 + b^2 = \widehat{0}$ în $\mathbb{Z}_p$, atunci $a = b = \widehat{0}$.

O variantă pentru a obţine această implicaţie este următoarea:

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

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

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%27s_theorem_on_sums_of_two_squares.`

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

Ex. 6. Fie K şi L corpuri comutative de caracteristica ∞. Demonstraţi că o funcţie $f : K \to L$ este un morfism de corpuri dacă şi 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) $f(1) = 1$.

Soluţie. Demonstraţia pentru $\Rightarrow$ se realizează prin aplicarea definiţiei 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 $2f(xy) = f((x+y)^2) - f(x^2) - f(y^2) = f(x+y)^2 - f(x)^2 - f(y)^2 = (f(x)+f(y))^2 - f(x)^2 - f(y)^2 = 2f(x)f(y)$. In final deducem că $f(xy) = f(x)f(y)$ pentru orice $x, y \in K$?

Observaţia 0.4. (Temă) Verificaţi care din axiomele corpului sunt într-adevăr necesare în soluţia exerciţiului precdent şi încercaţi să daţi un enunţ în care ipotezele să fie minimală. Este necesar să cerem $\mathrm{char}(K) = \mathrm{char}(K) = \infty$?

Temă

Ex. 7. Fie p un număr prim şi

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

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

respectiv

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

a) Demonstraţi că L_p, L_{-1}, M_p şi M_{ip} sunt domenii de integritate faţă de operaţiile obişnuite de $+$ şi $\cdot$ care nu sunt corpuri.
b) Demonstraţi că $L_p \cong M_p$.
c) Demonstraţi că $L_{-p} \cong M_{ip}$.
d) Demonstraţi că $L_2 \ncong M_3$.
e) Demonstraţi că $L_2 \ncong M_{-2}$.
f) Demonstraţi că dacă $p \neq q$ sunt numere prime, atunci $M_p \ncong M_q$, $M_p \ncong M_{iq}$, $M_{ip} \ncong M_{iq}$.

Ex. 8. Fie p un număr prim şi

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

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

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) Demonstraţi că L_p, L_{-1}, M_p şi M_{ip} sunt corpuri faţă de operaţiile obişnuite de $+$ şi $\cdot$.
b) Demonstraţi că $L_p \cong M_p$.
c) Demonstraţi că $L_{-p} \cong M_{ip}$.
d) Demonstraţi că $L_2 \ncong M_3$.
e) Demonstraţi că $L_2 \ncong M_{-2}$.
f) Demonstraţi că dacă $p \neq q$ sunt numere prime, atunci $M_p \ncong M_q$, $M_p \ncong M_{iq}$, $M_{ip} \ncong M_{iq}$.