CORPURI

1. Generalităţi

Definiţia 1.1. *Un inel unitar K cu $1 \neq 0$ se numeşte* corp *dacă orice element nenul al său este inversabil.*
Dacă înmulţirea pe K este comutativă, atunci K se numeşte corp comutativ.

Notaţie: $K^\times = K \setminus \{0\}$.

Exemplul 1.2. (i) $(\mathbb{Q}, +, \cdot)$ şi $(\mathbb{R}, +, \cdot)$ sunt corpuri comutative.
(ii) $\mathbb{Z}_n$ este corp dacă şi numai dacă n este număr prim.
(iii) $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ este corp comutativ.

Remarca 1.3. Orice corp este inel integru.

Exerciţiul 1.4. Arătaţi că orice inel unitar ($1 \neq 0$) integru şi finit este corp.

Propoziţia 1.5. *Fie R un inel unitar cu $1 \neq 0$. Atunci R este corp dacă şi numai dacă $\{0\}$ şi R sunt singurele ideale la stânga (la dreapta) ale lui R.*

Proof. "$\Rightarrow$" Fie I un ideal la stânga al lui R. Presupunem că $I \neq \{0\}$. Atunci există $a \in I$, $a \neq 0$. Deoarece R este corp, elementul a este inversabil şi cum $a^{-1}a \in I$ rezultă $1 \in I$. De aici se obţine că $r = r1 \in I$ pentru orice $r \in R$, deci $I = R$.
"$\Leftarrow$" Fie $a \in R$, $a \neq 0$. Idealul la stânga Ra este nenul, deoarece $a = 1a \in Ra$. Din ipoteză $Ra = R$, deci există $a' \in R$ astfel încât $a'a = 1$. Evident $a' \neq 0$ şi un raţionament analog ne arată că există $a'' \in R$ cu proprietatea că $a''a' = 1$. Înmulţind la dreapta cu a obţinem $a''a'a = a$, adică $a'' = a$. În concluzie, $aa' = 1$, deci a este inversabil. □

Remarca 1.6. Deşi în orice corp $\{0\}$ şi corpul însuşi sunt singurele ideale bilaterale, reciproc este fals: în inelul $R = M_2(\mathbb{Q})$ singurele ideale bilaterale sunt $\{0\}$ şi R şi acesta nu este corp. (Un inel cu proprietatea că nu are ideale bilaterale netriviale se numeşte *inel simplu*).

Definiţia 1.7. *Fie K un corp şi $K' \subseteq K$ o submulţime nevidă. Atunci K' se numeşte* subcorp *al lui K dacă $(K', +, \cdot)$ este corp. În acest caz se mai spune că K este o* extindere *a lui K'.*

Propoziţia 1.8. *Fie K un corp şi $K' \subseteq K$ o submulţime nevidă. Atunci K' este subcorp al lui K dacă şi numai dacă sunt satisfăcute următoarele condiţii:*
(i) $x, y \in K' \implies x - y \in K'$,
(ii) $x, y \in K', x \neq 0 \implies x^{-1}y \in K'$,
pentru orice $x, y \in K'$.

Să observăm că din (ii) rezultă imediat că $1 \in K'$.

Exemplul 1.9. (i) Orice corp este un subcorp al său.
(ii) $\mathbb{Q} \subseteq \mathbb{R}$ este subcorp.
(iii) $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$ este subcorp.

Remarca 1.10. Corpurile $\mathbb{Z}/p\mathbb{Z}$ şi $\mathbb{Q}$ nu au subcorpuri proprii.

Definiţia 1.11. *Fie K, K' corpuri şi $f : K \to K'$ o funcţie. Aceasta se numeşte* morfism de corpuri *dacă*

$$f(x+y) = f(x) + f(y),$$
$$f(xy) = f(x)f(y),$$
$$f(1) = 1',$$

pentru orice $x, y \in K$.

Remarca 1.12. (i) În definiţia de mai sus f este morfism de corpuri dacă este morfism unitar de inele.
(ii) Dacă f este morfism de corpuri, atunci $f(x^{-1}) = f(x)^{-1}$ pentru orice $x \in K^\times$.

Propoziţia 1.13. *Orice morfism de corpuri este injectiv.*

Proof. Fie $f : K \to K'$ un morfism de corpuri. Deoarece $\operatorname{Ker} f$ este ideal bilateral al lui K rezultă că $\operatorname{Ker} f = \{0\}$, deci f este morfism injectiv. □

Lema 1.14. *Fie K un corp şi $K_\alpha \subseteq K$, $\alpha \in A$ o familie de subcorpuri ale lui K. Atunci $\bigcap_{\alpha \in A} K_\alpha$ este un subcorp al lui K.*

Dacă considerăm intersecţia tuturor subcorpurilor unui corp dat obţinem un subcorp care nu are subcorpuri proprii.

Definiţia 1.15. *Un corp care nu are subcorpuri proprii se numeşte* corp prim.

Deci orice corp conţine ca subcorp un corp prim. După cum am observat deja, $\mathbb{Z}/p\mathbb{Z}$ şi $\mathbb{Q}$ sunt corpuri prime. Este adevărat însă şi reciproc.

Propoziţia 1.16. *Orice corp prim este izomorf cu $\mathbb{Q}$ sau cu $\mathbb{Z}/p\mathbb{Z}$, p prim.*

Proof. Fie K un corp prim şi $\varphi : \mathbb{Z} \to K$ dată prin $\varphi(n) = n \cdot 1$. Este clar că φ este morfism de inele şi avem două posibilităţi:
(i) $\operatorname{Ker} \varphi = \{0\}$, caz în care $\mathbb{Z} \simeq \operatorname{Im} \varphi$, deci K conţine un subinel izomorf cu $\mathbb{Z}$. Rezultă că K conţine un subcorp izomorf cu $\mathbb{Q}$ şi cum K este corp prim obţinem $K \simeq \mathbb{Q}$.
(ii) $\operatorname{Ker} \varphi = p\mathbb{Z}$, $p \in \mathbb{N} \setminus \{0, 1\}$. Avem $\mathbb{Z}/p\mathbb{Z} \simeq \operatorname{Im} \varphi \subseteq K$, deci $\mathbb{Z}/p\mathbb{Z}$ este inel integru. De aici rezultă că p este număr prim, deci $\mathbb{Z}/p\mathbb{Z}$ este corp şi cum K este corp prim obţinem $K \simeq \mathbb{Z}/p\mathbb{Z}$. □

Definiţia 1.17. *Fie K un corp. Dacă K conţine un subcorp prim izomorf cu $\mathbb{Q}$, atunci spunem că K este* corp de caracteristică zero *şi scriem* $\operatorname{char} K = 0$. *Dacă K conţine un subcorp prim izomorf cu $\mathbb{Z}/p\mathbb{Z}$, atunci spunem că K este* corp de caracteristică p *şi scriem* $\operatorname{char} K = p$.

Remarca 1.18. (i) $\operatorname{char} K = 0$ dacă şi numai dacă $\operatorname{ord}(1) = \infty$ în grupul $(K, +)$, iar $\operatorname{char} K = p$ dacă şi numai dacă $\operatorname{ord}(1) = p$ în grupul $(K, +)$.
(ii) Dacă $K' \subseteq K$ este o extindere de corpuri, atunci $\operatorname{char} K' = \operatorname{char} K$.

Exemplul 1.19. (i) $\operatorname{char}\mathbb{Q} = 0$ şi $\operatorname{char}\mathbb{Z}/p\mathbb{Z} = p$.
(ii) $\operatorname{char}\mathbb{R} = 0$ şi $\operatorname{char}\mathbb{Q}(\sqrt{2}) = 0$.

Propoziţia 1.20. *Fie K un corp,* $\operatorname{char} K = p > 0$ *şi $a, b \in K$ cu $ab = ba$. Atunci $(a+b)^{p^n} = a^{p^n} + b^{p^n}$ pentru orice $n \geq 1$.*

Proof. Este suficient să demonstrăm cazul $n = 1$. Pentru aceasta folosim formula binomului lui Newton. Avem $(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k$. Însă $p \mid \binom{p}{k}$ pentru orice $k \in \{1, \ldots, p-1\}$, deci $\binom{p}{k} = 0$ în K. În concluzie, $(a+b)^p = a^p + b^p$. □

Corolarul 1.21. *Fie K un corp comutativ cu* $\operatorname{char} K = p > 0$. *Atunci aplicaţia $\varphi : K \to K$ definită prin $\varphi(x) = x^p$ este morfism de corpuri.*

Morfismul definit în corolarul precedent se numeşte *endomorfismul lui Frobenius.*

2. Construcţii de corpuri

Vom construi acum trei exemple importante de corpuri.

1. Corpul numerelor complexe

Fie $\mathbb{C} = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R} \right\}$. Se verifică uşor că $\mathbb{C}$ este corp în raport cu adunarea şi înmulţirea matricelor. Există un morfism de corpuri $f : \mathbb{R} \to \mathbb{C}$ dat prin $f(a) = aI_2$. Astfel putem identifica pe $\mathbb{R}$ cu un subcorp al lui $\mathbb{C}$. Fie $i = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Atunci $i^2 = -I_2$ iar $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = aI_2 + bi$. Cum I_2 este elementul unitate al lui $\mathbb{C}$ vom scrie $a + bi$ în loc de $aI_2 + bi$. Deci $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$ este un corp cu adunarea şi înmulţirea date astfel:

$$(a + bi) + (c + di) = (a + c) + (b + d)i,$$

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i,$$

pentru orice $a, b, c, d \in \mathbb{R}$.

2. Corpul cuaternionilor

Fie $\mathbb{H} = \left\{ \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} : a, b \in \mathbb{C} \right\}$. Se verifică uşor că $\mathbb{H}$ este corp *necomutativ* în raport cu adunarea şi înmulţirea matricelor. Elementele lui $\mathbb{H}$ se numesc *cuaternioni.* Există un morfism de corpuri $f : \mathbb{C} \to \mathbb{H}$ dat prin $f(a) = \begin{pmatrix} a & 0 \\ 0 & \overline{a} \end{pmatrix}$. Astfel putem identifica pe $\mathbb{C}$ cu un subcorp al lui $\mathbb{H}$. Orice $a \in \mathbb{R}$ se identifică cu aI_2, iar $i \in \mathbb{C}$ se identifică cu $\mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$. Considerăm acum cuaternionii $\mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ şi $\mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$. Scriem $a = x + iy$, $b = z + it$, cu $x, y, z, t \in \mathbb{R}$. Atunci

$$\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} = x + \mathbf{i}y + \mathbf{j}z + \mathbf{k}t.$$

Deci $\mathbb{H} = \{x + \mathbf{i}y + \mathbf{j}z + \mathbf{k}t : x, y, z, t \in \mathbb{R}\}$ şi avem relaţiile:

$$\mathbf{ij} = \mathbf{k},\ \mathbf{ji} = -\mathbf{k},$$
$$\mathbf{jk} = \mathbf{i},\ \mathbf{kj} = -\mathbf{i},$$
$$\mathbf{ki} = \mathbf{j},\ \mathbf{ik} = -\mathbf{j},$$
$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1.$$

Remarca 2.1. Cuaternionii $\{\pm 1, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$ formează un grup necomutativ în raport cu înmulţirea numit *grupul cuternionilor*.

3. Corpul de fracţii al unui domeniu de integritate

Fie R un domeniu de integritate (cu $1 \neq 0$). Vom construi un corp comutativ care îl conţine pe R ca subinel şi care este cel mai mic corp cu această proprietate. Să considerăm produsul cartezian $R \times R^\times = \{(a, b) : a, b \in R, b \neq 0\}$. Pe această mulţime definim o relaţie binară astfel: $(a, b) \sim (c, d)$ dacă şi numai dacă $ad = bc$. Este imediat că "$\sim$" este o relaţie de echivalenţă. Fie $Q(R) = R \times R^\times / \sim$. Clasa de echivalenţă a unei perechi (a, b) în raport cu relaţia "$\sim$" se va nota $\frac{a}{b}$ şi se va numi *fracţie*. Definim pe $Q(R)$ două operaţii algebrice astfel:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd},$$
$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd},$$

pentru orice $a, b, c, d \in R$, $b \neq 0$, $d \neq 0$. Aceste operaţii sunt bine definite şi $(Q(R), +, \cdot)$ este un corp comutativ, numit *corpul de fracţii* al lui R.

Exemplul 2.2. (i) $Q(\mathbb{Z}) = \mathbb{Q}$.
(ii) Fie $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$. Atunci $Q(\mathbb{Z}[\sqrt{2}]) = \mathbb{Q}(\sqrt{2})$.

Există un morfism injectiv de inele unitare $\varphi : R \to Q(R)$ dat prin $\varphi(a) = \frac{a}{1}$.

Remarca 2.3. Fie R un domeniu de integritate. Atunci $Q(R)$ este cel mai mic corp comutativ cu proprietatea că îl conţine pe R ca subinel.