Rezolvarea exercițiilor din cursul de algebră

Cursul scris de dl. prof. Cornel Băețica
Rezolvări scrise de Gabriel Majeri *

Cuprins

*Mulțumiri dlui. prof. Gabriel Mincu pentru cursul de la seria 14 și explicațiile de la seminarii, Antoniei Biro-Bălan pentru materiale, feedback și explicații, și celorlalți colegi pentru feedback și susținere.

1 Inele

1.1 Generalități

Exercițiul (1.3)**.** Să se determine numărul structurilor:

(a) de inel, neizomorfe între ele, care pot fi definite pe grupul $(\mathbb{Z}_p, +)$, unde p este un număr prim.

Demonstrație. În acest exercițiu o să notăm cu $*$ legea de înmulțire pe care trebuie să o definim.

Pentru a defini în mod unic această lege de compoziție, este suficient să fixăm valoarea pentru $\hat{1} * \hat{1}$, deoarece $\hat{k} = \underbrace{\hat{1} + \cdots + \hat{1}}_{\text{de } k \text{ ori}}, \forall \hat{k} \in \mathbb{Z}_p$, și avem că

$$\begin{aligned}\hat{a} * \hat{b} &= (\underbrace{\hat{1} + \cdots + \hat{1}}_{\text{de } a \text{ ori}}) * (\underbrace{\hat{1} + \cdots + \hat{1}}_{\text{de } b \text{ ori}}) \\ &= \underbrace{\hat{1} * \hat{1} + \cdots + \hat{1} * \hat{1}}_{\text{de } a \cdot b \text{ ori}} \\ &= (ab)(\hat{1} * \hat{1})\end{aligned}$$

Dacă $\hat{1} * \hat{1} = \hat{0}$, atunci avem înmulțirea nulă pe $\mathbb{Z}_p$, $\hat{a} * \hat{b} = \hat{0}, \forall \hat{a}, \hat{b} \in \mathbb{Z}_p$.

Dacă $\hat{1} * \hat{1} = \hat{u} \neq \hat{0}$, atunci $\hat{a} * \hat{b} = (ab)\hat{u}$.

Putem să arătăm că pentru orice $\hat{u}$ toate aceste structuri sunt izomorfe între ele, arătând că toate sunt izomorfe cu $\mathbb{Z}_p$ cu înmulțirea obișnuită modulo p, definind izomorfismul $f \colon (\mathbb{Z}_p, +, *) \to (\mathbb{Z}_p, +, \cdot)$, $f(\hat{x}) = \hat{u}^{-1}\hat{x}$. □

(b) de inel unitar ce pot fi definite pe grupul $(\mathbb{Z}_n, +)$ și să se arate că acestea sunt izomorfe.

Demonstrație. Deoarece avem nevoie de inele unitare, excludem din start înmulțirea nulă ($a * b = 0, \forall a, b \in \mathbb{Z}_n$).

Toate elementele care sunt prime față de n au invers la înmulțire în $\mathbb{Z}_n$. Folosind morfismul de la sub punctul precedent, putem arăta că toate acestea sunt izomorfe cu $(\mathbb{Z}_n, +, \cdot)$, adică $\mathbb{Z}_n$ cu înmulțirea obișnuită modulo n. □

Exercițiul (1.4)**.** Arătați că pe grupul $(\mathbb{Q}/\mathbb{Z}, +)$ nu se poate defini o structură de inel unitar.

Demonstrație. Clasele de resturi din acest grup factor sunt de forma $\hat{\frac{1}{a}}$, cu $a \in \mathbb{Z}$. Observăm că pentru orice $n \in \mathbb{N}^*$, elementul $\widehat{\frac{1}{n}}$ are ordin n, deoarece $\underbrace{\widehat{\frac{1}{n}} + \cdots + \widehat{\frac{1}{n}}}_{\text{de } n \text{ ori}} = \widehat{\frac{n}{n}} = \hat{1} = \hat{0}$.

Presupunem că am definit o înmulțire pe acest inel, și că avem elementul unitate $\hat{\frac{1}{k}}, k \in \mathbb{Z}$. Atunci pentru orice $\widehat{1/a} \in \mathbb{Q}/\mathbb{Z}$:

$$\underbrace{\widehat{\frac{1}{a}} + \cdots + \widehat{\frac{1}{a}}}_{\text{de } k \text{ ori}} = \widehat{\frac{k}{a}} = \widehat{\frac{1}{k}} \cdot \widehat{\frac{k}{a}} = \hat{0}$$

Asta înseamnă că ordinul oricărui element este cel mult k, dar asta ar contrazice faptul că putem avea elemente cu ordin orice număr natural. □

Exercițiul (1.6)**.** Să se arate că $(\mathbb{R}^{\mathbb{R}}, +, \circ)$ nu este inel.

Demonstrație. Presupunem că această structură ar fi inel. Atunci compunerea ar trebui să fie distributivă față de adunare. Luăm contra exemplul $f, g, h \colon \mathbb{R} \to \mathbb{R}$, $f(x) = x^2, g(x) = 2x, h(x) = 3x$.

$$f \circ (g + h) = f(g(x) + h(x)) = f(2x + 3x) = (5x)^2 = 25x^2$$

$$f \circ g + f \circ h = f(g(x)) + f(h(x)) = f(2x) + f(3x) = 4x^2 + 9x^2 = 13x^2$$

Avem că $25x^2 \neq 13x^2$, deci $f \circ (g+h) \neq f \circ g + f \circ h$, deci nu este inel. □

Exercițiul (1.7)**.** Fie R un inel și $n \geq 2$. Să se arate că inelul de matrice $M_n(R)$ este comutativ dacă și numai dacă $ab = 0$ pentru orice $a, b \in R$.

Demonstrație. $\implies$ Fie $a, b \in R$. Considerăm matricile din $A, B \in M_n(R)$, unde A este matricea care îl are pe a pe poziția $(2, 1)$ și zerouri în rest, și B îl are pe b pe $(1, 2)$.

Dacă calculăm produsul AB, obținem matricea care îl are pe ab în poziția (2, 2), iar din produsul BA obținem 0 în acea poziție.

Deoarece știm din ipoteză că $AB = BA$, rezultă că $ab = 0$.

$\impliedby$ Fie $A, B \in M_n(R)$. Când calculăm produsul AB, respectiv BA, calculăm expresii de forma $\sum a_i b_j$. Deoarece știm din ipoteză că $ab = 0, \forall a, b \in R$, aceste expresii vor fi toate 0. Deci $AB = BA = \mathbf{0}_n$.

□

Exercițiul (1.10)**.** Arătați că dacă un inel are un divizor al lui zero la stânga (dreapta) nenul, atunci are un divizor al lui zero nenul.

Demonstrație. Fie $a \in R$, $a \neq 0$ un divizor al lui zero la stânga, nenul. Atunci, din definiție $\exists b \in R$, $b \neq 0$ astfel încât $a \cdot b = 0$. Asta înseamnă că b este un divizor al lui zero *la dreapta* nenul.

Considerăm acum elementul $b \cdot a$. Dacă acesta este 0, atunci înseamnă că a este un divizor al lui zero și la dreapta, deci am terminat demonstrația. Altfel, observăm ce se întâmplă când înmulțim acest element cu b la dreapta, respectiv cu a la stânga:

$$(b \cdot a) \cdot b = b \cdot (a \cdot b) = b \cdot 0 = 0$$
$$a \cdot (b \cdot a) = (a \cdot b) \cdot a = 0 \cdot a = 0$$

Deci $b \cdot a$ este sigur divizor al lui zero.

Demonstrația decurge analog dacă pornim cu un divizor al lui zero la dreapta nenul. □

Exercițiul (1.11)**.** Arătați că în inelul $M_n(R)$ orice divizor al lui zero la stânga (dreapta) este divizor al lui zero la dreapta (stânga).

Demonstrație. Fie $A \in M_n(R)$, $A \neq 0$ o matrice care este divizor al lui zero la stânga.

Fiind divizor al lui zero, sigur nu este inversabilă, deci $\det A = 0$. De asemenea, $\det A^\top = 0$.

Considerând matricea $A^\top$ o transformare liniară între spații vectoriale, din teorema dimensiunii, trebuie să existe cel puțin un vector nenul $v \in R^n$ pentru care $A^\top v = 0$.

Construim matricea V punând copii ale vectorului v pe fiecare coloană. Avem că $A^\top V = 0$. Atunci $(A^\top V)^\top = 0 \iff V^\top A = 0$.

Deci A este divizor al lui zero și la dreapta. □

Exercițiul (1.15)**.**

- Arătați că $f \in \mathbb{R}^\mathbb{R}$ este divizor al lui zero dacă și numai dacă există $x_0 \in \mathbb{R}$ astfel încât $f(x_0) = 0$.

  Demonstrație. $\implies$ Deoarece f este divizor al lui zero, înseamnă că există un $g \in \mathbb{R}^\mathbb{R}, g \neq 0$ astfel încât $(f \cdot g)(x) = 0, \forall x \in \mathbb{R}$.
  Putem rescrie $g \neq 0$ ca $\exists x_0$ astfel încât $g(x_0) \neq 0$. Atunci:

  $$(f \cdot g)(x_0) = 0 \implies f(x_0)g(x_0) = 0 \implies f(x_0) = 0$$

$\Longleftarrow$ Definim $g\colon \mathbb{R} \to \mathbb{R}$, $g \neq 0$,

$$g(x) = \begin{cases} 1, \, x = x_0 \\ 0, \text{ altfel} \end{cases}$$

Se observă că $f(x)g(x) = (f \cdot g)(x) = 0, \forall x \in \mathbb{R}$. Deci f este divizor al lui 0.

□

- Fie $C(\mathbb{R}) = \{ \, f\colon \mathbb{R} \to \mathbb{R} \mid \text{f este continuă} \, \}$ cu operațiile de adunare și înmulțire a funcțiilor. Arătați că $f \in C(\mathbb{R})$ este divizor al lui zero dacă și numai dacă există $(a, b) \subseteq \mathbb{R}$ astfel încât $f(x) = 0$ pentru orice $x \in (a, b)$.

  Demonstrație. $\Longrightarrow$ Fie $f\colon \mathbb{R} \to \mathbb{R}$ continuă și divizor al lui zero. Asemenea sub-punctului precedent, trebuie să existe un $x_0 \in \mathbb{R}$ astfel încât $f(x_0) = 0$. Dar deoarece f este continuă, trebuie să fie 0 pe o vecinătate deschisă a lui x_0, și anume $(a, b) \subseteq \mathbb{R}$.

  $\Longleftarrow$ Trebuie să găsim o funcție continuă care înmulțită cu f să fie peste tot 0. Pentru a face acest lucru, funcția va fi 0 în afara lui (a, b), și în (a, b) va fi o parabolă care intersectează O_x în a, respectiv b. Definim $g\colon \mathbb{R} \to \mathbb{R}$ continuă,

  $$g(x) = \begin{cases} (x - a)(x - b), \, x \in (a, b) \\ 0, \text{ altfel} \end{cases}$$

  Atunci $g \neq 0$, dar $f(x)g(x) = 0$, $\forall x \in \mathbb{R}$. Deci f este divizor al lui 0.

  □

Exercițiul (1.17)**.** Arătați că în inelul $M_n(R)$ orice element inversabil la stânga (dreapta) este inversabil la dreapta (stânga).

Demonstrație. Fie $A \in M_n(R)$ o matrice inversabilă la stânga. Atunci există $B \in M_n(R)$ cu $BA = I_n$.

Dacă ne uităm la determinanți, $\det(BA) = \det I_n = 1$, deci atât $\det B$ cât și $\det A$ sunt nenuli.

Avem că

$$B = (BA)B = B(AB)$$

Din $B = B(AB)$ obținem că $B(AB - I_n) = 0_n$. Deoarece $\det B \neq 0$, știm că B nu este divizor al lui zero, deci îl putem simplifica. Rămâne că $AB = I_n$. De aici am obținut că A este inversabilă și la dreapta. □

Exercițiul (1.22)**.** Să se determine elementele nilpotente în inelul $\mathbb{Z}_n$ și să se afle numărul acestora.

Demonstrație. Elementele nilpotente sunt cele pentru care $\exists k \in \mathbb{N}$ astfel încât $\hat{x}^k = \hat{0}$. Deci $n \mid x^k$. Ridicând la putere, nu pot apărea noi factori primi, doar crește puterea celor deja existenți. Deci trebuie ca x să conțină toți factorii primi ai lui n, la puteri mai mici.

Fie descompunerea lui n în m factori primi $n = p_1^{r_1} \cdot \dots \cdot p_m^{r_m}$. Atunci $\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{r_1}} \times \dots \times \mathbb{Z}_{p_m^{r_m}}$. Nilpotenții din inelul inițial corespund perechilor care conțin nilpotenți în inelele din produs.

În $\mathbb{Z}_{p_i^{r_i}}$ se vede mult mai clar câți nilpotenți avem. Înmulțim cu p_i tot inelul original $\mathbb{Z}_{p_i^{r_i}}$ ca să obținem numere în care apare factorul prim p_i, și obținem un sub inel

$$p_i\mathbb{Z}_{p_i^{r_i}} = p_i(\mathbb{Z}/p_i^{r_i}\mathbb{Z}) = \mathbb{Z}/p_i^{r_i-1}\mathbb{Z} = \mathbb{Z}_{p_i^{r_i-1}}$$

care are $p_i^{r_i-1}$ elemente.

Per total, în $\mathbb{Z}_n$ avem

$$p_1^{r_1-1} \cdot \dots \cdot p_m^{r_m-1} = \frac{p_1^{r_1} \cdot \dots \cdot p_m^{r_m}}{p_1 \cdot \dots \cdot p_m} = \frac{n}{p_1 \cdot \dots \cdot p_m}$$

nilpotenți. □

Exercițiul (1.23)**.** Fie R un inel și $x, y \in R$ elemente nilpotente.

1. Dacă $xy = yx$ atunci xy și $x + y$ sunt nilpotente.

   Demonstrație. Fie $x, y \in R$ nilpotente. Atunci $\exists n, m \in \mathbb{N}^*$ astfel încât $x^n = 0$, $y^m = 0$. Vrem să găsim o putere pentru care atât x și y să fie 0. Alegem $k = \max(n, m)$. Atunci $x^k = y^k = 0$.

   Luăm prima expresie și vedem ce se întâmplă când o ridicăm la k:

   $$(xy)^k = \underbrace{(xy) \dots (xy)}_{\text{k ori}}$$

   Deoarece $xy = yx$ putem să rearanjăm termenii: $(xy)^k = x^k y^k = 0$. Deci xy nilpotent.

   Pentru $x+y$ ne folosim de binomul lui Newton pentru a ridica la putere (avem voie deoarece $xy = yx$). Deoarece vrem ca toți termenii să se

anuleze, nu este suficient să ridicăm la puterea k, ci cel puțin la puterea $2k$. Dezvoltăm $(x+y)^{2k}$ după binomul lui Newton:

$$(x+y)^{2k} = \sum_{i=0}^{2k} \binom{2k}{i} a^{2k-i} b^i$$

Termenii cu i de la 0 până la k se anulează deoarece avem $k-i \geq 0$, putem rescrie $a^{2k-i} = a^k a^{k-i} = 0$, cei de la $k+1$ până la $2k$ se anulează deoarece avem $i-k \geq 0$, putem rescrie $b^i = b^k b^{i-k} = 0$. Deci $x+y$ nilpotent. □

2. Dați exemple care să arate că proprietatea 1 nu mai rămâne adevărată dacă $xy \neq yx$.

Demonstrație. De exemplu, în $M_2(\mathbb{R})$, avem nilpotenții $X = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ și $Y = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, cu $X^2 = Y^2 = \mathbf{0}_2$, care nu comută: $XY \neq YX$. Suma lor nu este nilpotentă: $X+Y = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $(X+Y)^2 = \mathbf{I}_2$, $(X+Y)^3 = (X+Y)$. □

Exercițiul (1.27)**.** Fie R un inel boolean. Să se arate că R este comutativ.

Demonstrație. Din definiția inelului boolean, toate elementele sunt idempotente: $x^2 = x$, $\forall x \in R$.

Observăm că avem următoarele identități:

$$\left.\begin{aligned} &x+x = (x+x)^2 = (x+x)(x+x) = x^2+x^2+x^2+x^2 \\ &x+x = (x^2)+(x^2) \end{aligned}\right\} \implies$$
$$\implies x^2+x^2+x^2+x^2 = x^2+x^2$$
$$\implies x^2+x^2 = 0$$
$$\implies x^2 = -x^2$$
$$\implies x = -x, \forall x \in R$$

Deci orice element este propriul său invers la adunare.

Pentru a arăta că acest inel este comutativ, trebuie să obținem cumva că $xy = yx$, $\forall x, y \in R$, folosindu-ne de proprietățile pe care le știm deja.

$$\left.\begin{aligned} &x + y = (x + y)^2 = x^2 + xy + yx + y^2 \\ &x + y = x^2 + y^2 \end{aligned}\right\} \implies$$
$$\implies (x^2 + y^2) + (xy + yx) = x^2 + y^2$$
$$\implies xy + yx = 0$$
$$\implies xy = -yx$$
$$\implies xy = yx$$

□

Exercițiul (1.28)**.**

- Se consideră numărul natural $n \geq 2$ care are r factori primi distincți în descompunerea sa. Să se arate că numărul idempotenților lui $\mathbb{Z}_n$ este 2^r.

  Demonstrație. Descompunem pe n în factori primi, $n = p_1^{q_1} p_2^{q_2} \dots p_r^{q_r}$. Atunci $\mathbb{Z}_n$ este izomorf cu $\mathbb{Z}_{p_1^{q_1}} \times \cdots \times \mathbb{Z}_{p_r^{q_r}}$.

  Singurele elemente idempotente în $\mathbb{Z}_{p_i^{r_i}}$ sunt $\overline{0}$ și $\overline{1}$. Deci idempotentele lui $\mathbb{Z}_n$ corespund prin izomorfism elementelor de forma $(0, \dots, 0, 0)$, $(0, \dots, 0, 1)$, ..., $(1, \dots, 1, 1)$. Există 2^r astfel de r-tupluri.

  Pentru a găsi idempotenții în inelul inițial, construim un sistem de congruențe liniare. De exemplu, pentru $(1, 0, \dots, 0, 1)$ sistemul ar fi:

$$\begin{cases} x \equiv 1 \mod p_1^{q_1} \\ x \equiv 0 \mod p_2^{q_2} \\ \vdots \\ x \equiv 0 \mod p_{r-1}^{q_{r-1}} \\ x \equiv 1 \mod p_r^{q_r} \end{cases}$$

  Din lema chineză a resturilor și din faptul că toți factorii primi sunt numere prime între el, acest sistem sigur are soluții. □

- Să se determine idempotenții inelului $\mathbb{Z}_{36}$.

Demonstrație. Pe baza descompunerii în factori primi avem că

$$\mathbb{Z}_{36} \cong \mathbb{Z}_{2^2} \times \mathbb{Z}_{3^2}$$

În inelul produs, avem idempotenții $(\overline{0}, \overline{\overline{0}})$, $(\overline{1}, \overline{\overline{1}})$, $(\overline{0}, \overline{\overline{1}})$ și $(\overline{1}, \overline{\overline{0}})$.

Primii doi idempotenți corespund lui $\hat{0}$, respectiv $\hat{1}$. Pentru a afla corespondenții ultimilor doi idempotenți trebuie să rezolvăm două sisteme de congruențe:

$$\begin{cases} x \equiv 0 \mod 4 \\ x \equiv 1 \mod 9 \end{cases} \qquad \begin{cases} x \equiv 1 \mod 4 \\ x \equiv 0 \mod 9 \end{cases}$$

Soluția primei ecuații este $\widehat{28}$. Putem rezolva și a doua ecuație, sau ne putem folosi de faptul că $\hat{1} - \widehat{28}$ este tot idempotent, de unde obținem că $\widehat{1-28} = \widehat{-27} = \hat{9}$ este cealaltă soluție. □

Exercițiul (1.29)**.** Fie $R = M_2(\mathbb{Z}_2)$.

- Să se determine numărul elementelor lui R.

  Demonstrație. Elementele lui R sunt matrici 2×2 cu elemente din $\mathbb{Z}_2$:

  $$A = \begin{pmatrix} \hat{a} & \hat{b} \\ \hat{c} & \hat{d} \end{pmatrix} \in R$$

  În R avem $|\mathbb{Z}_2|^4 = 2^4 = 16$ matrici distincte. □

- Să se determine numărul divizorilor lui zero ai lui R.

  Demonstrație. Dacă o matrice are determinantul $\hat{0}$, atunci există un vector nenul astfel încât $Av = 0$, și dacă punem copii ale acestui vector pentru a obține o matrice, obținem că $AB = 0$. Deci este suficient să găsim matricile cu determinant nul.

  Avem 10 matrici cu determinant nul:

  $$\begin{pmatrix} \hat{0} & \hat{0} \\ \hat{0} & \hat{0} \end{pmatrix}, \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{0} & \hat{0} \end{pmatrix}, \begin{pmatrix} \hat{0} & \hat{1} \\ \hat{0} & \hat{0} \end{pmatrix}, \begin{pmatrix} \hat{0} & \hat{0} \\ \hat{1} & \hat{0} \end{pmatrix}, \begin{pmatrix} \hat{0} & \hat{0} \\ \hat{0} & \hat{1} \end{pmatrix},$$
  $$\begin{pmatrix} \hat{1} & \hat{1} \\ \hat{0} & \hat{0} \end{pmatrix}, \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{1} & \hat{0} \end{pmatrix}, \begin{pmatrix} \hat{0} & \hat{1} \\ \hat{0} & \hat{1} \end{pmatrix}, \begin{pmatrix} \hat{0} & \hat{0} \\ \hat{1} & \hat{1} \end{pmatrix}, \begin{pmatrix} \hat{1} & \hat{1} \\ \hat{1} & \hat{1} \end{pmatrix}$$

  □

- Aflați câte elemente nilpotente are R.

  Demonstrație. Pentru ca A să fie nilpotent, trebuie ca $A^k = 0$. Din proprietățile determinantului, obținem că $\det A$ trebuie să fie $\hat{0}$. Putem să plecăm de la lista de divizori ai lui zero / matrici cu determinant nul, și să verificăm fiecare matrice dacă este nilpotentă.

  Obținem 4 nilpotenți:

$$\begin{pmatrix} \hat{0} & \hat{0} \\ \hat{0} & \hat{0} \end{pmatrix}, \begin{pmatrix} \hat{0} & \hat{1} \\ \hat{0} & \hat{0} \end{pmatrix}, \begin{pmatrix} \hat{0} & \hat{0} \\ \hat{1} & \hat{0} \end{pmatrix}, \begin{pmatrix} \hat{1} & \hat{1} \\ \hat{1} & \hat{1} \end{pmatrix}$$

  □

- Aflați câte elemente idempotente are R.

  Demonstrație. Din faptul că vrem ca $A^2 = A$, ajungem la concluzia că fie nu este inversabilă și are determinant zero, fie este inversabilă, și atunci este matricea unitate (deoarece $A^2 = A \iff A^{-1}A^2 = A^{-1}A \iff A = I$).

  Verificând matricile cu determinant nul, obținem 8 idempotenți:

$$\begin{pmatrix} \hat{0} & \hat{0} \\ \hat{0} & \hat{0} \end{pmatrix}, \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{0} & \hat{1} \end{pmatrix}, \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{0} & \hat{0} \end{pmatrix}, \begin{pmatrix} \hat{0} & \hat{0} \\ \hat{0} & \hat{1} \end{pmatrix},$$
$$\begin{pmatrix} \hat{1} & \hat{1} \\ \hat{0} & \hat{0} \end{pmatrix}, \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{1} & \hat{0} \end{pmatrix}, \begin{pmatrix} \hat{0} & \hat{1} \\ \hat{0} & \hat{1} \end{pmatrix}, \begin{pmatrix} \hat{0} & \hat{0} \\ \hat{1} & \hat{1} \end{pmatrix}$$

  □

1.2 Subinele. Ideale

Exercițiul (2.7)**.** Fie R_1, R_2 inele unitare $R = R_1 \times R_2$. Să se arate că idealele la stânga (la dreapta, bilaterale) ale lui R sunt de forma $I = I_1 \times I_2$ unde I_1, I_2 sunt ideale la stânga (la dreapta, bilaterale) în R_1, respectiv R_2.

Demonstrație. $\implies$ Presupunem că avem două ideale $I_1 \trianglelefteq R_1$, $I_2 \trianglelefteq R_2$. Trebuie să arătăm că $I_1 \times I_2 = I \trianglelefteq R$.

Avem că $I = I_1 \times I_2 = \{\, (a, b) \in R \mid a \in I_1, b \in I_2 \,\}$.

Arătăm că această mulțime este închisă la adunare:

$$(a, b) + (c, d) = (\underbrace{a + c}_{\in I_1}, \underbrace{b + d}_{\in I_2}) \in I$$

și la înmulțirea cu un element din inel:

$$(m,n)(a,b) = (\underbrace{ma}_{\in I_1}, \underbrace{nb}_{\in I_2}) \in I$$

(ne-am folosit de faptul că I_1 și I_2 sunt ideale în inelele respective, și adunarea/înmulțirea se face pe componente).

Deci I este ideal (la stânga, la dreapta, sau bilateral, în funcție de cum erau I_1 și I_2).

$\Longleftarrow$ Presupunem că avem $I \trianglelefteq R$. Trebuie să arătăm că există două ideale $I_1 \trianglelefteq R_2$, $I_2 \trianglelefteq R_2$ astfel încât $I_1 \times I_2 = I$.

Observație: dacă perechea (a,b) aparține lui I, atunci și perechile $(a,0)$, respectiv $(0,b)$ aparțin idealului: putem să înmulțim (a,b) cu $(1,0)$, respectiv $(0,1)$ (avem voie, I este ideal).

Definim două mulțimi

$$I_1 = \{\, a \in R_1 \mid \exists y \in R_2 \text{ a.î. } (a,y) \in I \,\} \subseteq R_1$$

$$I_2 = \{\, b \in R_2 \mid \exists x \in R_1 \text{ a.î. } (x,b) \in I \,\} \subseteq R_2$$

Vrem să arătăm că acestea sunt ideale în inelele de care aparțin. Se arată ușor prin calcule că sunt închise la adunare. În ceea ce privește închiderea la înmulțirea cu un element din inel:

Fie $r \in R_1$, $a \in I_1$. Pentru ca $ra \in I_1$ trebuie să existe un y' astfel încât $(ra, y') \in I$. Noi știm că $a \in I_1 \implies \exists y$ astfel încât $(a,y) \in I$. Pe baza observației de mai sus, $(a,0) \in I$. Atunci și $(ra,0) \in I$. Deci $y' = 0$ și $ra \in I_1$.

Demonstrația decurge analog pentru I_2, dar interschimbăm componentele.

Mai rămâne de arătat că $I_1 \times I_2 = I$ (prin dublă incluziune):

1. Dacă avem $a \in I_1$, $b \in I_2$, înseamnă că există $x \in I_1, y \in I_2$ astfel încât $(a,y) \in I$ și $(x,b) \in I$, deci sigur $(a,b) \in I$
2. Pentru orice $(a,b) \in I$, avem $a \in I_1$ și $b \in I_2$.

□

1.3 Morfisme de inele

Exercițiul (3.9)**.** Arătați că avem următoarele izomorfisme de grupuri:

- $\text{End}((\mathbb{Z}, +)) \cong \mathbb{Z}$

  Demonstrație. Fie $f \colon \mathbb{Z} \to \mathbb{Z}$ un morfism. Știm că $f(0) = 0$. Notăm $f(1) = a \in \mathbb{Z}$.

  Atunci, pentru un k pozitiv

  $$f(k) = f(\underbrace{1 + \cdots + 1}_{k \text{ ori}}) = f(1) + \cdots + f(1) = k \cdot f(1) = k \cdot a, \forall k > 0$$

  Pentru un k negativ, ne folosim de faptul că pentru orice morfism de grupuri $f(-x) = -f(x)$. Atunci

  $$f(k) = -f(-k) = -k \cdot a, \forall k < 0$$

  Deci $f(k) = k \cdot a, \forall k \in \mathbb{Z}$. Fiecare dintre aceste morfisme este identificat prin valoarea lui a, deci avem câte unul pentru fiecare număr din $\mathbb{Z}$.

  De asemenea, acestea formează un grup în raport cu compunerea. Fie $f_a \colon \mathbb{Z} \to \mathbb{Z}$ morfismul cu $f_a(k) = k \cdot a$, $\forall k \in \mathbb{Z}$. Atunci:

  $$(f_a \circ f_b)(k) = f_a(f_b(k)) = k \cdot ab = f_{ab}$$
  $$f_{-a}(k) = k \cdot (-a) = -k \cdot a = -f_a$$

  Deci $\text{End}((\mathbb{Z}, +)) \cong \mathbb{Z}$. □

- $\text{End}((\mathbb{Q}, +)) \cong \mathbb{Q}$

  Demonstrație. Asemănător cu exercițiul precedent, endomorfismele lui $\mathbb{Q}$ sunt de forma $f_{\frac{p}{q}}(x) = \frac{p}{q}x$. □

- $\text{End}((\mathbb{Z}_n, +)) \cong \mathbb{Z}_n$

  Demonstrație. Asemănător cu exercițiile precedente, endomorfismele sunt de forma $f_{\hat{k}}(\hat{x}) = \hat{k} \cdot \hat{x}$. □

- $\text{End}((\mathbb{Z} \times \mathbb{Z}, +)) \cong M_2(\mathbb{Z})$

Demonstrație. Plecând de la cunoștințele pe care le avem legate de endomorfismele lui $\mathbb{Z}$, putem construi endomorfisme scriind combinații liniare ale celor două componente:

$$f((x,y)) = (ax + by, cx + dy)$$

Dacă scriem fiecare pereche din $\mathbb{Z} \times \mathbb{Z}$ ca un vector coloană, obținem:

$$f(\begin{pmatrix} x \\ y \end{pmatrix}) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix}$$

□

Exercițiul (3.10)**.** Determinați endomorfismele (și automorfismele) următoarelor inele:

- $(\mathbb{Z}, +, \cdot)$

  Demonstrație. Plecăm de la endomorfismele grupului $(\mathbb{Z}, +)$, și punem condiția și ca $f(a \cdot b) = f(a) \cdot f(b)$, $\forall a, b \in \mathbb{Z}$. Dacă înlocuim cu forma generală a unui morfism pe $\mathbb{Z}$ obținem

  $$k \cdot ab = ka \cdot kb = k^2 \cdot ab$$

  Din $k = k^2$ ajungem la concluzia că singurele endomorfisme de inele sunt morfismul identitate, $f(x) = x$, și morfismul nul, $f(x) = 0$. Dintre acestea, morfismul identitate este și automorfism. □

- $(\mathbb{Q}, +, \cdot)$

  Demonstrație. Asemănător cu exercițiul precedent. □

- $(\mathbb{R}, +, \cdot)$

  Demonstrație. Asemănător cu exercițiile precedente. □

- $(\mathbb{Z}_n, +, \cdot)$

  Demonstrație. Din faptul că vrem ca $\hat{k} = \hat{k}^2$, trebuie ca $\hat{k}$ să fie element idempotent. Deci putem obține un endomorfism diferit pentru fiecare idempotent al lui $\mathbb{Z}_n$. □

- $(\mathbb{Z} \times \mathbb{Z}, +, \cdot)$

  Demonstrație. Asemănător exercițiilor precedente, trebuie să căutăm morfisme ale grupului $(\mathbb{Z} \times \mathbb{Z}, +)$ care să se comporte bine și cu înmulțirea.

  Deoarece deja știm că aceste morfisme sunt unic determinate de o matrice din $M_2(\mathbb{Z})$, endomorfismele inelului $\mathbb{Z} \times \mathbb{Z}$ sunt cele care corespund matricilor idempotente. □

Exercițiul (3.11)**.**

- Arătați că există un morfism *unitar* de inele $\mathbb{Z}_m \to \mathbb{Z}_n$ dacă și numai dacă $n \mid m$.

  Demonstrație. Vom nota cu $\hat{a}$ clasele de resturi din $\mathbb{Z}_m$ și cu $\tilde{b}$ clasele de resturi din $\mathbb{Z}_n$.

  Observație: la acest sub-punct contează foarte mult că ne referim numai la morfisme *unitare*. Indiferent de n și m, întotdeauna avem de exemplu morfismul neunitar $f(\hat{x}) = \tilde{0}$.

  $\Longrightarrow$ Fie $f \colon \mathbb{Z}_m \to \mathbb{Z}_n$ morfism unitar de inele. Atunci avem proprietățile:

  $$f(\hat{0}) = \tilde{0} \qquad (f \text{ este morfism de inele})$$
  $$f(\hat{1}) = \tilde{1} \qquad (f \text{ este morfism } \textit{unitar} \text{ de inele})$$

  Acum vedem ce se întâmplă când introducem clasa lui m în morfism:

  $$f(\widehat{m}) = f(\hat{0}) = \tilde{0} \qquad (\text{restul lui } m \text{ la împărțirea cu } m \text{ este } 0)$$
  $$f(\widehat{m}) = f(\underbrace{\hat{1} + \cdots + \hat{1}}_{m \text{ ori}})$$
  $$f(\widehat{m}) = \underbrace{f(\hat{1}) + \cdots + f(\hat{1})}_{m \text{ ori}} = \underbrace{\tilde{1} + \cdots + \tilde{1}}_{m \text{ ori}} = \widetilde{m}$$

  Punând totul la un loc, obținem că $\widetilde{m} = \tilde{0}$. Cu alte cuvinte, m este multiplu de n, deci $n \mid m$.

$\Longleftarrow$ Presupunem că $n \mid m$. Definim $f\colon \mathbb{Z}_m \to \mathbb{Z}_n$, cu legea $f(\hat{x}) = \tilde{\hat{x}} = \tilde{x}$. Cu alte cuvinte, f ia fiecare rest la împărțirea cu m și îi face restul la împărțirea cu n.

Trebuie să arătăm mai întâi că această funcție este bine definită. Indiferent de ce reprezentanți am alege pentru aceeași clasă de resturi, trebuie să ne asigurăm că funcția ia aceeași valoare. Altfel spus, $\forall \hat{x}, \hat{y} \in \mathbb{Z}_m$ cu $\hat{x} = \hat{y}$ și $x \neq y$, vrem ca $f(\hat{x}) = f(\hat{y})$.

$$\left.\begin{array}{l} \hat{x} = \hat{y} \iff m \mid (x-y) \\ n \mid m \end{array}\right\} \implies n \mid (x-y)$$
$$\iff \tilde{x} = \tilde{y}$$
$$\iff f(\hat{x}) = f(\hat{y})$$

Acum trebuie să demonstrăm că f este morfism unitar de inele. Acest lucru se poate face destul de simplu, deoarece "căciula" comută cu operațiile uzuale. Deci $f(\hat{a} + \hat{b}) = f(\widehat{a+b}) = \widetilde{a+b} = \tilde{a} + \tilde{b}$, și analog pentru înmulțire.

□

- Arătați că un morfism de inele $f\colon \mathbb{Z}_m \to \mathbb{Z}_n$ este unic determinat de condițiile: $mf(\hat{1}) = \tilde{0}$ și $f(\hat{1}) = f(\hat{1})^2$.

Demonstrație. Cerința poate fi rescrisă ca $f\colon \mathbb{Z}_m \to \mathbb{Z}_n$ morfism de inele dacă și numai dacă $mf(\hat{1}) = \tilde{0}$ și $f(\hat{1}) = f(\hat{1})^2$.

$\Longrightarrow$ Fie $f\colon \mathbb{Z}_m \to \mathbb{Z}_n$ morfism de inele. Atunci

$$\begin{aligned} & \widehat{m} = \hat{0} \\ \Longrightarrow\ & f(\widehat{m}) = f(\hat{0}) \\ \Longrightarrow\ & f(\hat{1} + \cdots + \hat{1}) = \tilde{0} \\ \Longrightarrow\ & f(\hat{1}) + \cdots + f(\hat{1}) = \tilde{0} \\ \Longrightarrow\ & mf(\hat{1}) = \tilde{0} \end{aligned}$$

Pentru a doua condiție, avem că

$$f(\hat{1}) = f(\hat{1} \cdot \hat{1}) = f(\hat{1}) \cdot f(\hat{1}) = f(\hat{1})^2$$

$\Longleftarrow$ Fie $f\colon \mathbb{Z}_m \to \mathbb{Z}_n$, $f(\hat{k}) = kf(\hat{1})$. Notăm $f(\hat{1}) = \tilde{a}$. Știm că $m\tilde{a} = \tilde{0}$ și $\tilde{a} = \tilde{a}^2$.

Trebuie să arătăm mai întâi că această funcție este bine definită. Fie $\hat{k}, \hat{l} \in \mathbb{Z}_m$ cu $k \neq l$ și $\hat{k} = \hat{l}$. Vrem să arătăm că

$$\begin{aligned} & f(\hat{k}) = f(\hat{l}) \\ \Longleftrightarrow\ & k\tilde{a} = l\tilde{a} \\ \Longleftrightarrow\ & k\tilde{a} - l\tilde{a} = \tilde{0} \\ \Longleftrightarrow\ & (k-l)\tilde{a} = \tilde{0} \end{aligned}$$

Din $\hat{k} = \hat{l}$ avem că $\hat{k} - \hat{l} = \hat{0}$, deci $k - l$ este multiplu de m. Deoarece $m\tilde{a} = \tilde{0}$, avem că $(k-l)\tilde{a} = \tilde{0}$.

Ca să arătăm că este morfism, ne folosim de cealaltă proprietate:

$$\begin{aligned} f(\hat{k} \cdot \hat{l}) &= f(\widehat{k \cdot l}) \\ &= (k \cdot l)\tilde{a} = (k \cdot l)\tilde{a}^2 \qquad \text{(din proprietatea } \tilde{a}^2 = \tilde{a}) \\ &= k\tilde{a} \cdot l\tilde{a} \\ &= f(\hat{k}) \cdot f(\hat{l}) \end{aligned}$$

□

- Să se determine toate morfismele de inele de la $\mathbb{Z}_{12}$ la $\mathbb{Z}_{28}$.

Demonstrație. Fie $f\colon \mathbb{Z}_{12} \to \mathbb{Z}_{28}$. Notăm $f(\hat{1}) = \tilde{a}$. Atunci, conform subpunctului anterior, $\tilde{a}$ trebuie să îndeplinească condițiile:

$$\begin{cases} \tilde{a}^2 = \tilde{a} \\ 12\tilde{a} = \tilde{0} \end{cases}$$

Trebuie să găsim toate $\tilde{a} \in \mathbb{Z}_{28}$ pentru care $\tilde{a}^2 = \tilde{a}$. Cu alte cuvinte, căutăm elementele idempotente.

Avem că $\mathbb{Z}_{28} = \mathbb{Z}_4 \times \mathbb{Z}_7$. Idempotenții corespund perechilor $(\overline{0}, \overline{\overline{0}})$, $(\overline{0}, \overline{\overline{1}})$, $(\overline{1}, \overline{\overline{0}})$ și $(\overline{1}, \overline{\overline{1}})$. Idempotenții lui $\mathbb{Z}_{28}$ sunt $\left\{ \tilde{0}, \tilde{1}, \tilde{8}, \widetilde{21} \right\}$.

Dintre aceștia, doar $\tilde{0}$ și $\widetilde{21}$ îndeplinesc și a doua condiție. Deci singurele morfisme sunt $f(\hat{k}) = \tilde{0}$ și $f(\hat{k}) = \widetilde{21}\tilde{k}$. □

1.4 Inele factor

Exercițiul (4.8)**.** Fie R_1, R_2 inele unitare, $R = R_1 \times R_2$ și $I = I_1 \times I_2$ unde I_1, I_2 sunt ideale bilaterale în R_1, respectiv R_2. Să se arate că inelele R/I și $R_1/I_1 \times R_2/I_2$ sunt izomorfe.

Demonstrație. Se poate rezolva definind $f \colon R/I \to R_1/I_1 \times R_2/I_2$, cu

$$f(\widehat{(a,b)}) = (\overline{a}, \overline{\overline{b}})$$

și demonstrând că această funcție este izomorfism. □

Exercițiul (4.9)**.** Fie R un inel unitar și I ideal bilateral al lui R. Să se arate că inelele $M_2(R)/M_2(I)$ și $M_2(R/I)$ sunt izomorfe.

Demonstrație. Vrem să folosim teorema fundamentală de izomorfism pentru inele. Avem nevoie de un morfism f pentru care $\ker f = M_2(I)$.

- Definim $f \colon M_2(R) \to M_2(R/I)$, $f(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) = \begin{pmatrix} \hat{a} & \hat{b} \\ \hat{c} & \hat{d} \end{pmatrix}, \forall a, b, c, d \in R$.
- Se arătă prin calcule că f este morfism unitar de inele.
- Studiem nucleul morfismului:

$$f(\begin{pmatrix} a & b \\ c & d \end{pmatrix}) = \begin{pmatrix} \hat{0} & \hat{0} \\ \hat{0} & \hat{0} \end{pmatrix} \iff \begin{pmatrix} \hat{a} & \hat{b} \\ \hat{c} & \hat{d} \end{pmatrix} = \begin{pmatrix} \hat{0} & \hat{0} \\ \hat{0} & \hat{0} \end{pmatrix}$$

$$\iff \begin{cases} \hat{a} = \hat{0} \\ \hat{b} = \hat{0} \\ \hat{c} = \hat{0} \\ \hat{d} = \hat{0} \end{cases} \iff a, b, c, d \in I$$

  Deci $\ker f = M_2(I)$.
- Imaginea lui f este întregul codomeniul $M_2(R/I)$, f este surjectiv.

  Fie $y \in M_2(R/I)$, $y = \begin{pmatrix} \hat{a} & \hat{b} \\ \hat{c} & \hat{d} \end{pmatrix}$. Atunci luăm $x \in M_2(R)$, $x = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Se observă că $f(x) = y$.
- Din teorema fundamentală de izomorfism, $M_2(R)/M_2(I) \cong M_2(R/I)$.

□

1.5 Teorema chineză a resturilor pentru ideale

Exercițiul (5.4)**.** Arătați că

- $\mathbb{Q}[X]/(X^2-1) \cong \mathbb{Q} \times \mathbb{Q}$

  Demonstrație. Putem rescrie $\mathbb{Q}[X]/(X^2-1) = \mathbb{Q}[X]/((X-1)(X+1))$.

  Pentru a arăta că $(X-1)$ și $(X+1)$ sunt comaximale, trebuie să arătăm că suma lor generează tot $\mathbb{Q}[X]$. Este suficient să arătăm că suma idealelor conține elementul unitate.

  Observăm că $(X+1)-(X-1) = 2$. Înmulțind cu $\frac{1}{2}$ (avem voie, deoarece lucrăm în $\mathbb{Q}$) obținem 1.

  Putem aplica **Remarca 5.2** din curs, și obținem că

  $$\mathbb{Q}[X]/((X-1)(X+1)) = \mathbb{Q}[X]/((X-1) \cap (X+1))$$

  Acum ne folosim de **Teorema 5.3** din curs. Obținem că

  $$\mathbb{Q}[X]/((X-1) \cap (X+1)) \cong \mathbb{Q}[X]/(X-1) \times \mathbb{Q}[X]/(X+1)$$

  Clasele de echivalență ale lui $\mathbb{Q}[X]/(X-1)$ sunt resturile obținute prin împărțirea oricărui polinom la $X-1$, deci sunt polinoame de grad 0, de forma $\{\, \hat{a} \mid a \in \mathbb{Q} \,\}$, deci $\mathbb{Q}[X]/(X-1) \cong \mathbb{Q}$. Analog pentru $\mathbb{Q}[X]/(X+1) \cong \mathbb{Q}$.

  În concluzie, $\mathbb{Q}[X]/(X^2-1) \cong \mathbb{Q} \times \mathbb{Q}$. □

- $\mathbb{Z}[X]/(X^2-X) \cong \mathbb{Z} \times \mathbb{Z}$

  Demonstrație. Demonstrația decurge asemănător pentru $\mathbb{Z}[X]/(X^2-X)$, cu observația că $X^2-X = X(X-1)$. Sunt comaximale deoarece $X-(X-1) = 1$. □

- $\mathbb{Z}[X]/(X^2-1) \ncong \mathbb{Z} \times \mathbb{Z}$

  Demonstrație. Demonstrația începe la fel ca prima, însă nu mai putem să înmulțim cu $\frac{1}{2}$ deoarece lucrăm în $\mathbb{Z}$, deci nu mai putem folosi această metodă pentru a arăta că sunt izomorfe.

  Presupunem că inelul factor ar fi izomorf cu $\mathbb{Z} \times \mathbb{Z}$. Ne uităm la elementele idempotente ale acestor două inele.

  Observație: deoarece X^2-1 aparține idealului prin care factorizăm, avem că $\widehat{X^2-1} = \hat{0}$, de unde $\widehat{X^2} = \hat{1}$.

– În $\mathbb{Z}[X]/(X^2-1)$, fie $\hat{a}\widehat{X}+\hat{b}$ un idempotent. Atunci

$$\begin{aligned}
&(\hat{a}\widehat{X}+\hat{b})^2 = \hat{a}\widehat{X}+\hat{b}\\
\iff &\hat{a}^2\widehat{X}^2 + \widehat{2ab}\widehat{X} + \hat{b}^2 = \hat{a}\widehat{X}+\hat{b}\\
\iff &\hat{a}^2\cdot\hat{1} + \widehat{2ab}\widehat{X} + \hat{b}^2 = \hat{a}\widehat{X}+\hat{b}\\
\iff &\begin{cases}\widehat{a^2}+\widehat{b^2}=\hat{b}\\ \widehat{2ab}=\hat{a}\end{cases}
\end{aligned}$$

Singura soluție care convine în $\mathbb{Z}$ este $a=0$ și $b\in\{0,1\}$. Deci singurii idempotenți sunt $\hat{0}$ și $\hat{1}$.

– În $\mathbb{Z}\times\mathbb{Z}$, avem idempotenții $(0,0)$, $(0,1)$, $(1,0)$ și $(1,1)$.

Cele două inele nu pot fi izomorfe, având un număr diferit de idempotenți. □

2 Corpuri

2.1 Generalități

Exercițiul (1.4)**.** Orice inel unitar ($1\neq 0$) integru și finit este corp.

Demonstrație. Fie $a\in R$ un element diferit de 0. Trebuie să arătăm că are invers la înmulțire.

Luăm în considerare puterile lui a: a^n, $\forall n\in\mathbb{N}^*$. Inelul fiind finit, acestea nu pot fi toate distincte. La un moment dat trebuie să existe $m\neq n$ pentru care $a^m=a^n$. Să presupunem că $m<n$.

Atunci $a^m-a^n=0 \iff a^m(1-a^{n-m})=0$.

Fiind inel integru, rezultă că $a^m=0$ sau $a^{n-m}-1=0$. Prima posibilitate este exclusă deoarece un inel integru nu are nilpotenți netriviali.

Rămâne deci că $a^{n-m}-1=0 \iff a^{n-m}=1 \iff a\cdot a^{n-m-1}=1$.

Astfel am găsit un invers multiplicativ pentru a, și anume a^{n-m-1}. □

3 Inele de polinoame

3.1 Inele de polinoame într-o nedeterminată

Exercițiul (2.4)**.** Fie R un inel comutativ și unitar, și fie $\alpha\in R$. Atunci $R[X]/(X-\alpha)\cong R$.

Demonstrație. Vrem să ne folosim de teorema fundamentală de izomorfism.

Trebuie să găsim un morfism de inele al cărui nucleu să fie exact idealul generat de $X - \alpha$, iar imaginea acestuia să fie întreg R-ul. Cu alte cuvinte, vrem să avem un morfism $\varphi\colon R[X] \to R$ surjectiv pentru care $\varphi(f) = 0 \iff f$ este multiplu de $X - \alpha, \forall f \in R[X]$. Acesta este chiar morfismul care evaluează polinomul în α: $\varphi(f) = f(\alpha)$.

Morfismul este și surjectiv, deoarece $\forall y \in R$, y este și element în $R[X]$, iar $\varphi(y) = y$. Acum trebuie să îi determinăm nucleul:

$$\begin{aligned}
& f \in \ker \varphi \\
\iff & \varphi(f) = 0 \\
\iff & f(\alpha) = 0 \\
\iff & X - \alpha \mid f && \text{(din Bézout)} \\
\iff & f \text{ multiplu de } X - \alpha \\
\iff & f \in (X - \alpha)
\end{aligned}$$

Deci $\ker \varphi = (X - \alpha)$, $\operatorname{im} \varphi = R$.

Aplicăm teorema fundamentală de izomorfism pentru inele:

$$R[X]/\ker \varphi \cong \operatorname{im} \varphi \iff R[X]/(X - \alpha) \cong R$$

□

3.2 Teorema de împărțire cu rest pentru polinoame într-o nedeterminată

Exercițiul (2.5)**.** Arătați că:

1. $\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}$

   Demonstrație. Definim $\varphi\colon \mathbb{R}[X] \to \mathbb{C}$, $\varphi(f) = f(i)$, adică funcția care evaluează polinomul în i. Aceasta este morfism unitar de inele.

   Demonstrăm că $\ker \varphi = (X^2 + 1)$ prin dublă incluziune:

   - Dacă f este multiplu de $X^2 + 1$, atunci $f(i) = 0$, deci $f \in \ker \varphi$.
   - Fie $f \in \ker \varphi$.
     $\varphi(f) = 0 \implies f(i) = 0 \implies i$ este o rădăcină a polinomului f
     Deoarece lucrăm cu polinoame cu coeficienți reali, și conjugatul $-i$ este o rădăcină a polinomului f.
     Din Bézout, f se divide prin $X - i$ și prin $X + i$, deci se divide și prin $(X - i)(X + i) = X^2 + 1$.
     Deci $f \in (X^2 + 1)$.

Pentru orice număr complex $z = a + bi$, avem că $\varphi(a + bX) = a + bi$, deci φ este surjectiv. Imaginea lui φ este $\mathbb{C}$.

Aplicăm teorema fundamentală de izomorfism pentru inele și avem că

$$\mathbb{R}[X]/\ker\varphi \cong \operatorname{im}\varphi \iff \mathbb{R}[X]/(X^2+1) \cong \mathbb{C}$$

□

2. $\mathbb{Z}[X]/(X^2-2) \cong \mathbb{Z}[\sqrt{2}]$

Demonstrație. Aplicăm teorema fundamentală de izomorfism pentru

$$\varphi\colon \mathbb{Z}[X] \to \mathbb{Z}[\sqrt{2}]$$

$$\varphi(f) = f(\sqrt{2})$$

□

Exercițiul (2.6)**.** Să se arate că $R = \mathbb{Z}[X]/(2, X^2+1)$ este un inel cu 4 elemente, dar nu este izomorf cu $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Demonstrație. Factorizând prin (2), toți coeficienții polinoamelor sunt înlocuiți cu resturi modulo 2. Deci $\mathbb{Z}[X]/(2, X^2+1) \cong \mathbb{Z}_2[X]/(\widehat{X^2+1})$.

Factorizând mai departe prin $(\widehat{X^2+1})$, clasele de resturi obținute sunt de forma $\hat{a}X + \hat{b}$. De aceea R are $2^2 = 4$ elemente:

$$R = \mathbb{Z}[X]/(2, X^2+1) = \left\{\hat{0}, \hat{1}, \widehat{X}, \widehat{X}+\hat{1}\right\}$$

Pentru a demonstra că nu este izomorf cu $\mathbb{Z}_2 \times \mathbb{Z}_2$, ne uităm la numărul de nilpotenți ale acestor inele.

- În R avem $\hat{0}^2 = \hat{0}$ și $(\widehat{X}+\hat{1})^2 = \widehat{X^2} + \hat{2}\widehat{X} + \hat{1} = \hat{0}$.
- În $\mathbb{Z}_2 \times \mathbb{Z}_2$ singurul nilpotent este $(\hat{0}, \hat{0})$.

Deci aceste două inele nu sunt izomorfe. □

Exercițiul (2.7)**.** Considerăm idealul $I = (3, X^3 - X^2 + 2X + 1)$ în $\mathbb{Z}[X]$. Să se arate că I nu este ideal principal și că $\mathbb{Z}[X]/I$ nu este inel integru.

Demonstrație. Dacă I ar fi ideal principal, atunci ar exista un singur polinom f astfel încât $I = (f)$. Ar însemna că f poate să genereze ambii generatori ai lui I. Deci $f \mid 3$ și $f \mid X^3 - X^2 + 2X + 1$.

Ar rezulta că $f = 1$, deci $I = (f) = \mathbb{Z}[X]$. Însă de exemplu $2 \in \mathbb{Z}[X]$, însă 2 nu poate fi scris ca o combinație liniară de 3 și $X^3 - X^2 + 2X + 1$.

Inelul factor rezultat este izomorf cu $\mathbb{Z}_3[X]/(X^3 - X^2 + \hat{2}X + \hat{1})$.

În inelul obținut, încercăm să scriem $X^3 - X^2 + \hat{2}X + \hat{1}$ (care corespunde lui 0) ca produs de alte polinoame. Avem că

$$(X + \hat{1})(X^2 + X + \hat{1}) = X^3 + \hat{2}X^2 + \hat{2}X + \hat{1} = X^3 - X^2 + \hat{2}X + \hat{1}$$

Deci inelul factor nu este integru, avem cel puțin doi divizori ai lui zero: $X + \hat{1}$ și $X^2 + X + \hat{1}$. □

Exercițiul (2.8)**.** Aflați inversul lui $\widehat{4X + 3}$ în inelul factor $R = \mathbb{Z}_{11}[X]/(X^2 + 1)$.

Demonstrație. Asemănător exercițiilor anterioare ajungem la concluzia că clasa asociată fiecărui polinom din $\mathbb{Z}_{11}[X]$ se poate găsi calculând restul la împărțirea cu $\widehat{X^2 + 1}$:

$$\mathbb{Z}_{11}[X]/(X^2 + 1) = \left\{ \hat{a}\widehat{X} + \hat{b} \;\middle|\; \hat{a}, \hat{b} \in \mathbb{Z}_{11} \right\}$$

Exercițiul ne cere să găsim un invers multiplicativ pentru $\widehat{4X + 3}$, adică un polinom de forma $\widehat{aX + b} \in R$ pentru care

$$(\widehat{4X + 3})(\widehat{aX + b}) = \hat{1} \iff (\hat{4}\widehat{X} + \hat{3})(\hat{a}\widehat{X} + \hat{b}) = \hat{1}$$

Dacă desfacem parantezele avem că

$$\widehat{4a}\widehat{X^2} + \widehat{3a}\widehat{X} + \widehat{4b}\widehat{X} + \widehat{3b} = \hat{1}$$

Deoarece lucrăm cu idealul generat de $X^2 + 1$, știm că $\widehat{X^2 + 1} = \hat{0}$ deoarece $X^2 + 1$ aparține idealului. Observăm că

$$\widehat{X^2 + 1} = \hat{0} \iff \widehat{X^2} + \hat{1} = \hat{0} \iff \widehat{X^2} = \widehat{-1}$$

Putem să rescriem rezultatul să fie de grad cel mult 1:

$$(\widehat{3a} + \widehat{4b})\widehat{X} + (\widehat{-4a} + \widehat{3b}) = \hat{1}$$

În acest moment, găsirea inversului se reduce la rezolvarea sistemului de ecuații

$$\begin{cases} \widehat{3a} + \widehat{4b} = \hat{0} \\ \widehat{-4a} + \widehat{3b} = \hat{1} \end{cases}$$

După calcule ajungem la soluția $\hat{a} = \hat{6}$ și $\hat{b} = \hat{1}$.

Deci inversul lui $\widehat{4X + 3}$ este $\widehat{6X + 1}$. □

3.3 Inele de polinoame într-un număr finit de nedeterminate

Exercițiul (3.9)**.** Fie R un inel comutativ și unitar, și fie $\alpha_1, \dots, \alpha_n \in R$. Atunci $R[X_1, \dots, X_n]/(X_1 - \alpha_1, \dots, X_n - \alpha_n)$ și R sunt izomorfe.

Demonstrație. Demonstrația decurge similar ca la exercițiul 2.4, dar vom defini $\varphi(f) = f(\alpha_1, \dots, \alpha_n)$, și ne folosim de proprietatea de universalitate a inelelor de polinoame într-un număr finit de nedeterminate. □

3.4 Polinoame simetrice

Exercițiul (4.19)**.** Să se arate că următoarele polinoame sunt simetrice și să se scrie fiecare dintre ele ca polinom de polinoame simetrice fundamentale:

1. $X_1^3X_2 + X_1^3X_3 + X_1X_2^3 + X_1X_3^3 + X_2^3X_3 + X_2X_3^3$

   Demonstrație. Notăm cu f polinomul din enunț. Pentru a arăta că este simetric, este suficient să verificăm că rămâne la fel dacă permutăm necunoscutele cu transpozițiile $(1, 2)$ și $(2, 3)$.

   $$f(X_2, X_1, X_3) = X_2^3X_1 + X_2^3X_3 + X_2X_1^3 + X_2X_3^3 + X_1^3X_3 + X_1X_3^3 = f$$

   $$f(X_1, X_3, X_2) = X_1^3X_3 + X_1^3X_2 + X_1X_3^3 + X_1X_2^3 + X_3^3X_2 + X_3X_2^3 = f$$

   Îl descompunem în polinom de polinoame simetrice fundamentale folosind algoritmul lui Newton.

   Polinoamele simetrice în 3 necunoscute sunt

   $$\begin{aligned} s_1 &= X_1 + X_2 + X_3 \\ s_2 &= X_1X_2 + X_1X_3 + X_2X_3 \\ s_3 &= X_1X_2X_3 \end{aligned}$$

   Termenul principal (primul în ordine lexicografică) este $X_1^3X_2$. Acesta este de grad 4 și are coeficientul 1. Scriem toate monoamele de grad 4 cu exponenții necunoscutelor descrescători, și le ordonăm lexicografic:

   $$\underbrace{X_1^3X_2}_{(3,1,0)} > \underbrace{X_1^2X_2^2}_{(2,2,0)} > \underbrace{X_1^2X_2X_3}_{(2,1,1)}$$

   Trebuie să obținem aceste monoame din produse de polinoame simetrice. Notăm coeficienții acestor polinoame simetrice cu a, b:

   $$f = s_1^2s_2 + as_2^2 + bs_1s_3$$

Acum putem să dăm valori convenabile lui X_1, X_2, X_3, astfel încât polinomul să fie 0, și să se anuleze unele dintre polinoamele simetrice fundamentale.

- Pentru $X_1 = 1, X_2 = -1, X_3 = 0$ avem $f = -2$ și $s_1 = 0, s_2 = -1, s_3 = 0$. Atunci $a(-1)^2 = -2 \iff \boxed{\text{a = -2}}$.
- Pentru $X_1 = 1, X_2 = 1, X_3 = 1$ avem $f = 6$ și $s_1 = 3, s_2 = 3, s_3 = 1$. Atunci $3^2 \cdot 3 - 2 \cdot 3^2 + b \cdot 3 \cdot 1 = 6 \iff 3b = -3 \iff \boxed{\text{b = -1}}$.

Deci $f = s_1^2 s_2 - 2s_2^2 - s_1 s_3$. □

2. $(X_1^2 + X_2^2)(X_1^2 + X_3^2)(X_2^2 + X_3^2)$

Demonstrație. Notăm polinomul dat cu f. Vedem ce se întâmplă când îl permutăm cu transpozițiile $(1, 2)$ și $(2, 3)$:

$$f(X_2, X_1, X_3) = (X_2^2 + X_1^2)(X_2^2 + X_3^2)(X_1^2 + X_3^2) = f$$

$$f(X_1, X_3, X_2) = (X_1^2 + X_3^2)(X_1^2 + X_2^2)(X_3^2 + X_2^2) = f$$

Deci f este polinom simetric.

Termenii pe care îi putem obține dacă desfacem parantezele o să fie de grad cel mult 6, iar $X_1^4 X_2^2$ este primul lexicografic. Monoamele de grad 6 ar veni, în ordine:

$$(4, 2, 0) > (4, 1, 1) > (3, 3, 0) > (3, 2, 1) > (2, 2, 2)$$

Care ar corespunde lui

$$f = s_1^2 s_2^2 + a s_1^3 s_3 + b s_2^3 + c s_1 s_2 s_3 + d s_3^2$$

- Pentru $X_1 = 1, X_2 = i, X_3 = 0$ avem $f = 0$ și $s_1 = 1 + i, s_2 = i, s_3 = 0$. Atunci $(1 + i)^2 \cdot (i^2) + b \cdot (i^3) = 0 \iff -2i - bi = 0 \iff \boxed{\text{b = -2}}$.
- Pentru $X_1 = 2, X_2 = -1, X_3 = -1$ avem $f = 50$ și $s_1 = 0, s_2 = -3, s_3 = 2$. Atunci $-2 \cdot (-3)^3 + d \cdot 2^2 = 50 \iff 54 + 4d = 50 \iff \boxed{\text{d = -1}}$.
- Pentru $X_1 = 2, X_2 = 2, X_3 = -1$ avem $f = 200$ și $s_1 = 3, s_2 = 0, s_3 = -4$. Atunci $a \cdot 3^3 \cdot (-4) - (-4)^2 = 200 \iff -108a = 216 \iff \boxed{\text{a = -2}}$.

- Pentru $X_1 = 1, X_2 = i, X_3 = -i$ avem $f = 0$ și $s_1 = 1, s_2 = 1, s_3 = 1$. Atunci $1 - 2 - 2 + c - 1 = 0 \iff \boxed{c = 4}$.

Deci $f = s_1^2 s2^2 - 2s_1^3 s_3 - 2s_2^3 + 4s_1 s_2 s_3 - s_3^2$. □

Exercițiul (4.22)**.** Să se calculeze:

1. $x_1^5 + x_2^5 + x_3^5$, unde x_1, x_2, x_3 sunt rădăcinile polinomului $X^3 - 3X + 1$.

Demonstrație. Dacă x_i este una dintre rădăcinile polinomului, atunci

$$x_i^3 - 3x_i + 1 = 0 \iff x_i^3 = 3x_i - 1$$

Înlocuind, expresia care trebuie calculată devine

$$\begin{gathered} x_1^2 x_1^3 + x_2^2 x_2^3 + x_3^2 x_3^3 \\ = x_1^2(3x_1 - 1) + x_2^2(3x_2 - 1) + x_3^2(3x_3 - 1) \\ = 3x_1^3 - x_1^2 + 3x_2^3 - x_2^2 + 3x_3^3 - x_3^2 \\ = 3(3x_1 - 1) + 3(3x_2 - 1) + 3(3x_3 - 1) - (x_1^2 + x_2^2 + x_3^2) \\ = (9x_1 - 3) + (9x_2 - 3) + (9x_3 - 3) - (x_1^2 + x_2^2 + x_3^2) \\ = 9(x_1 + x_2 + x_3) - 9 - (x_1^2 + x_2^2 + x_3^2) \end{gathered}$$

Din relațiile lui Viète avem $x_1 + x_2 + x_3 = 0$, $x_1x_2 + x_2x_3 + x_1x_3 = -3$ și

$$x_1^2 + x_2^2 + x_3^2 = (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_2x_3 + x_1x_3) = 6$$

Valoarea expresiei $x_1^5 + x_2^5 + x_3^5$ este $9 * 0 - 9 - 6 = -15$. □

2. $x_1^3 + x_2^3 + x_3^3 + x_4^3$, unde x_1, x_2, x_3, x_4 sunt rădăcinile polinomului $X^4 + X^3 + 2X^2 + X + 1$.

Exercițiul (4.23)**.** Considerăm elementele $x_1, \dots, x_n \in \mathbb{C}$ cu proprietatea că $x_1^k + \cdots + x_n^k = 0, \forall k \in \overline{1, n}$. Arătați că $x_1 = \cdots = x_n = 0$.

Demonstrație. În cele ce urmează notăm cu s_i polinoamele simetrice fundamentale. Încercăm să vedem ce obținem dacă îi dăm diferite valori lui k.

Pentru $k = 1$ avem că $x_1 + \cdots + x_n = 0 \iff s_1 = 0$.

Pentru $k = 2$ obținem

$$\begin{aligned} & x_1^2 + \cdots + x_n^2 = 0 \\ \iff & (\underbrace{x_1 + \cdots + x_n}_{=0 \text{ din } k=1})^2 - 2(x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n) = 0 \\ \iff & x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n = 0 \\ \iff & s_2 = 0 \end{aligned}$$

Prin inducție, putem demonstra că $s_i = 0, \forall i \in \overline{1,n}$. Din relațiile lui Viète obținem că $x_1 = x_2 = \cdots = x_n = 0$. □

Exercițiul (4.24)**.** Să se rezolve în $\mathbb{R}$ ecuația $\sqrt[4]{97 - x} + \sqrt[4]{x} = 5$.

Demonstrație. **Condiții de existență.** Observăm că numerele de sub radicalul de ordin 4 trebuie să fie pozitive. Deci pentru început $0 \leq x \leq 97$.

Fie $t = \sqrt[4]{x}$. Atunci ecuația devine:

$$\begin{aligned} & \sqrt[4]{97 - t^4} + t = 5 \\ \iff & \sqrt[4]{97 - t^4} = 5 - t && \text{Condiție de existență: } t \leq 5 \\ \iff & 97 - t^4 = t^4 - 20t^3 + 150t^2 - 500t + 625 \\ \iff & 2t^4 - 20t^3 + 150t^2 - 500t + 528 = 0 \\ \iff & t^4 - 10t^3 + 75t^2 - 250t + 264 = 0 \end{aligned}$$

În acest moment, știm că dacă acest polinom are soluții reale, acestea sunt în intervalul $t \in [0, 5]$. Prin încercări, găsim soluțiile $t = 2$ și $t = 3$. Dacă factorizăm polinomul la $t - 2$ și la $t - 3$ obținem:

$$(t - 2)(t - 3)(t^2 - 5t + 44) = 0$$

Calculând Δ pentru polinomul de grad 2 rămas, observăm că este negativ, deci nu mai avem alte soluții în $\mathbb{R}$.

Scoatem x din t și avem soluțiile $x = 16$, respectiv $x = 81$. □

Exercițiul (4.25)**.** Să se rezolve în $\mathbb{R}$ sistemul de ecuații

$$\begin{cases} x + y = 3 \\ x^5 + y^5 = 33 \end{cases}$$

Demonstrație. Toate polinoamele care apar în acest sistem sunt simetrice. O să le descompunem în polinoame simetrice fundamentale.

Notăm polinoamele simetrice fundamentale în două necunoscute cu $S = x + y$, $P = xy$.

Din prima ecuație avem că $x + y = 3 \implies S = 3$.
Încercăm să descompunem $x^5 + y^5$:

$$\begin{aligned} x^5 + y^5 &= \underline{(x+y)}^5 - (5x^4y + 10x^3y^2 + 10x^2y^3 + 5xy^4) \\ &= S^5 - 5\underline{xy}(x^3 + 2x^2y + 2xy^2 + y^3) \\ &= S^5 - 5P(\underline{(x+y)}^3 - (x^2y + xy^2)) \\ &= S^5 - 5P(S^3 - \underline{xy}\underline{(x+y)}) \\ &= S^5 - 5P(S^3 - PS) \end{aligned}$$

Sistemul devine:

$$\begin{aligned} &\begin{cases} S = 3 \\ S^5 - 5P(S^3 - PS) = 33 \end{cases} \\ &\iff 3^5 - 5P(3^3 - 3P) = 33 \\ &\iff 243 - 5P(27 - 3P) = 33 \\ &\iff 5P^2 - 45P + 70 = 0 \\ &\iff P \in \{ 2, 7 \} \end{aligned}$$

Acum trebuie să găsim două numere reale care să aibă suma egală cu 3 și produsul egal cu 2 (respectiv, suma 3 și produsul 7). Putem să le ghicim, sau putem să aplicăm invers relațiile lui Viète.

Numerele care au suma S și produsul P sunt soluțiile ecuației $x^2 - Sx + P = 0$.

$$x^2 - 3x + 2 = 0 \iff x \in \{ 1, 2 \}$$

$$x^2 - 3x + 7 = 0 \iff \text{nu are soluții pe } \mathbb{R}$$

Deci soluțiile găsite sunt $(x = 1, y = 2)$ și $(x = 2, y = 1)$.

(Sistemul fiind simetric, dacă (a, b) este soluție, atunci și (b, a) este soluție) □

4 Aritmetica în $\mathbb{Z}$ și $K[X]$

4.1 Divizibilitate. Algoritmul lui Euclid

Exercițiul (1.15)**.** Calculați $(24, 54)$ în $\mathbb{Z}$ cu algoritmul lui Euclid.

Demonstrație. Împărțim cu rest pe 54 la 24 (dacă am urma exact algoritmul ar trebui să împărțim pe 24 la 54 mai întâi, dar apoi tot la pasul acesta ajungem):

$$54 = 24 \cdot 2 + 6$$

Acum împărțim cu rest pe 24 la 6:

$$24 = 6 \cdot 4 + 0$$

Deoarece restul obținut este 0, algoritmul se termină. În concluzie, un c.m.m.d.c. al lui 24 și 54 este 6. □

Exercițiul (1.16)**.** Calculați $(X^4 - 4X^3 + 1, X^3 - 3X^2 + 1)$ în $\mathbb{R}[X]$ cu algoritmul lui Euclid.

Demonstrație. Notăm $f = X^4 - 4X^3 + 1$, $g = X^3 - 3X^2 + 1$. Împărțim cu rest pe f la g:

$$\begin{array}{rr} X^4 - 4X^3 & +1 \\ \hline -X^4 + 3X^3 & -X \\ \hline -X^3 & -X+1 \\ X^3 - 3X^2 & +1 \\ \hline -3X^2 & -X+2 \end{array} \quad = \left(X^3 - 3X^2 + 1\right)\left(X - 1\right) - 3X^2 - X + 2$$

Deci $f = (X-1)g + (-3X^2 - X + 2)$. Notăm $r_1 = -3X^2 - X + 2$. Acum împărțim cu rest pe g la r_1:

$$\begin{array}{rr} X^3 - 3X^2 & +1 \\ \hline -X^3 - \frac{1}{3}X^2 & +\frac{2}{3}X \\ \hline -\frac{10}{3}X^2 & +\frac{2}{3}X+1 \\ \frac{10}{3}X^2 + \frac{10}{9}X & -\frac{20}{9} \\ \hline \frac{16}{9}X & -\frac{11}{9} \end{array} \quad = \left(-3X^2 - X + 2\right)\left(-\tfrac{1}{3}X + \tfrac{10}{9}\right) + \tfrac{16}{9}X - \tfrac{11}{9}$$

Deci $g = \left(-\frac{1}{3}X + \frac{10}{9}\right) r_1 + \left(\frac{16}{9}X - \frac{11}{9}\right)$.

Dacă înmulțim un polinom cu un element inversabil din inelul de coeficienți, noul polinom este asociat în divizibilitate cu cel precedent. Deci o să înmulțim cu numitorul comun (care este inversabil, deoarece lucrăm în $\mathbb{R}$) și notăm $r_2 = 16X - 11$ pentru a simplifica calculele.

Împărțim cu rest pe r_1 la r_2:

$$\begin{array}{rr} -3X^2 & -X+2 \\ \hline 3X^2 - \frac{33}{16}X & \\ \hline -\frac{49}{16}X & +2 \\ \frac{49}{16}X - \frac{539}{256} & \\ \hline -\frac{27}{256} & \end{array} \quad = \left(16X - 11\right)\left(-\tfrac{3}{16}X - \tfrac{49}{256}\right) - \tfrac{27}{256}$$

Deci $r_1 = \left(-\frac{3}{16}X - \frac{49}{256}\right) r_2 + \left(-\frac{27}{256}\right)$. O să înmulțim restul obținut cu $-\frac{256}{27}$. Notăm $r_3 = 1$.

Împărțim cu rest pe r_2 la r_3:

$$\begin{array}{r} 16X-11 = 1\cdot\big(16X-11\big) \\ \underline{-\,16X} \\ -\,11 \\ \underline{\quad 11} \\ 0 \end{array}$$

De unde rezultă $r_2 = 1 \cdot r_3 + 0$. Ultimul rest nenul este 1, deci cele două polinoame sunt prime între ele: $(X^4 - 4X^3 + 1, X^3 - 3X^2 + 1) = 1$. □

Exercițiul (1.22)**.** Determinați $(X^2 - 1)\mathbb{Q}[X] \cap (X^3 - 1)\mathbb{Q}[X]$ și $(X^2 - 1)\mathbb{Q}[X] + (X^3 - 1)\mathbb{Q}[X]$.

Demonstrație. Ne folosim de proprietățile din curs: intersecția a două ideale generate de un singur element este idealul generat de c.m.m.m.c.-ul al celor două elemente, respectiv pentru adunare de c.m.m.d.c.-ul celor două elemente.

Pentru a fi mai ușor să găsim c.m.m.d.c.-ul și c.m.m.m.c.-ul, descompunem polinoamele în factori ireductibili din $\mathbb{Q}[X]$:

$$X^2 - 1 = (X - 1)(X + 1)$$
$$X^3 - 1 = (X - 1)(X^2 + X + 1)$$

Obținem $[X^2-1, X^3-1] = (X-1)(X+1)(X^2+X+1)$ și $(X^2-1, X^3-1) = X - 1$.

Deci

$$(X^2 - 1)\mathbb{Q}[X] \cap (X^3 - 1)\mathbb{Q}[X] = ((X - 1)(X + 1)(X^2 + X + 1))\mathbb{Q}[X]$$
$$(X^2 - 1)\mathbb{Q}[X] + (X^3 - 1)\mathbb{Q}[X] = (X - 1)\mathbb{Q}[X]$$

□

4.2 Elemente prime. Elemente ireductibile

Exercițiul (2.10)**.** Determinați polinoamele ireductibile de grad ≤ 5 din $\mathbb{Z}_2[X]$.

Demonstrație. Sunt cel mult $2^6 = 64$ polinoame de grad ≤ 5 în $\mathbb{Z}_2[X]$. Ca să nu fie nevoie să le încercăm pe toate, facem câteva observații ajutătoare:

1. Polinoamele de grad ≤ 1 sunt sigur ireductibile: $\hat{0}, \hat{1}, \widehat{X}, \widehat{X+1}$.

2. Polinoamele de grad ≥ 2 care nu au un termen liber $\hat{1}$ sunt sigur reductibile, pentru că se divid prin $\widehat{X}$.

3. Dacă un polinom are rădăcina α, atunci sigur este reductibil (din Bézout, se divide prin $X - \alpha$). Deoarece lucrăm în $\mathbb{Z}_2$, este suficient să încercăm să înlocuim X cu $\hat{0}$ și $\hat{1}$.

4. Pentru că $\mathbb{Z}_2$ este corp de caracteristică 2 (deoarece $\hat{1} + \hat{1} = \hat{0}$), avem că $(a+b)^2 = a^2 + b^2$ (sau mai general, $(\sum x)^2 = \sum(x^2)$).

   Deci orice polinom din $\mathbb{Z}_2[X]$ cu toate monoamele de grad par este reductibil. De exemplu, $X^4 + X^2 + \hat{1} = (X^2 + X + \hat{1})^2$.

5. În $\mathbb{Z}_2[X]$, dacă suma coeficienților unui polinom este un număr par, atunci acel polinom sigur are rădăcina $\hat{1}$, deci este reductibil.

6. Pe măsură ce construim lista, dacă observăm că un polinom este egal cu produsul altor polinoame deja scrise, atunci este reductibil.

Lista polinoamelor ireductibile de grad ≤ 5 din $\mathbb{Z}_2[X]$:

- Grad ≤ 1: 0, 1, X, $X+1$
- Grad 2: $X^2 + X + 1$
- Grad 3: $X^3 + X^2 + 1$, $X^3 + X + 1$
- Grad 4: $X^4 + X^3 + X^2 + X + 1$, $X^4 + X^3 + 1$, $X^4 + X + 1$
- Grad 5: $X^5 + X^2 + 1, X^5 + X^3 + 1, X^5 + X^3 + X^2 + X + 1, X^5 + X^4 + X^2 + X + 1, X^5 + X^4 + X^3 + X + 1, X^5 + X^4 + X^3 + X^2 + 1$

□

Exercițiul (2.11)**.** Descompuneți polinomul $f = X^{56} - X^{49} - X^7 + \hat{1}$ în produs de polinoame ireductibile în $\mathbb{Z}_7[X]$.

Demonstrație. Notăm $Y = X^7$. Polinomul inițial este $f = Y^8 - Y^7 - Y + \hat{1}$.

Observăm că $\hat{1}$ este o rădăcină (multiplă) a polinomului. Tot împărțim prin $Y - \hat{1}$ și obținem:

$$\begin{aligned}
f &= Y^8 - Y^7 - Y + 1 \\
&= (Y - \hat{1})(Y^7 - \hat{1}) \\
&= (Y - \hat{1})^2(Y^6 + Y^5 + Y^4 + Y^3 + Y^2 + Y + \hat{1}) \\
&= (Y - \hat{1})^3(Y^5 + \hat{2}Y^4 + \hat{3}Y^3 + \hat{4}Y^2 + \hat{5}Y - \hat{1}) \\
&= (Y - \hat{1})^4(Y^4 + \hat{3}Y^3 + \hat{6}Y^2 + \hat{3}Y + \hat{1}) \\
&= (Y - \hat{1})^5(Y^3 + \hat{4}Y^2 + \hat{3}Y - \hat{1}) \\
&= (Y - \hat{1})^6(Y^2 + \hat{5}Y + \hat{1}) \\
&= (Y - \hat{1})^7(Y - \hat{1}) \\
&= (Y - \hat{1})^8
\end{aligned}$$

Deci polinomul inițial este $f = (Y - \hat{1})^8 = (X^7 - \hat{1})^8$. Pe baza calculelor deja efectuate pentru Y, acesta este egal cu $((X - \hat{1})^7)^8 = (X - \hat{1})^{56}$. □

Exercițiul (2.17)**.** Determinați c.m.m.d.c. și c.m.m.m.c. pentru polinoamele $f = (X-1)(X^2-1)(X^3-1)(X^4-1)$ și $g = (X+1)(X^2+1)(X^3+1)(X^4+1)$ din $\mathbb{Q}[X]$.

Demonstrație. Deoarece polinoamele sunt deja scrise ca produs de alte polinoame, începem prin a descompune cele două polinoame în produs de factori ireductibili peste $\mathbb{Q}[X]$. Avem că

$$\begin{aligned}
f &= (X-1)(X-1)(X+1)(X-1)(X^2+X+1)(X-1)(X+1)(X^2+1) \\
&= (X-1)^3(X+1)^2(X^2+1)(X^2+X+1) \\
g &= (X+1)(X^2+1)(X^3+1)(X^4+1)
\end{aligned}$$

Pentru a găsi c.m.m.d.c.-ul, luăm toți factorii primi comuni la puterea cea mai mică.

$$(f, g) = (X+1)(X^2+1)$$

Pentru c.m.m.m.c., luăm toți factorii primi o singură dată, la puterea cea mai mare.

$$[f, g] = (X-1)^3(X+1)^2(X^2+1)(X^3+1)(X^2+X+1)(X^4+1)$$

□

4.3 Teorema fundamentală a algebrei

Exercițiul (3.7)**.** Arătați că polinomul X^n-2 este ireductibil în $\mathbb{Q}[X]$ pentru orice $n \geq 1$.

Demonstrație.

- Pentru $n = 1$, $X - 2$ este polinom de grad 1, deci ireductibil.
- Pentru $n = 2$, rădăcinile polinomului sunt $\pm\sqrt{2}$, care nu aparțin lui $\mathbb{Q}$, deci polinomul este ireductibil.
- Pentru $n \geq 3$, facem observația că polinomul este reductibil peste $\mathbb{C}[X]$, soluțiile fiind rădăcinile de ordin n ale lui 2. Deci $X^n - 2$ mai poate fi scris ca
$$X^n - 2 = (X - \varepsilon_0) \dots (X - \varepsilon_{n-1})$$
unde $\varepsilon_k = \sqrt[n]{2}(\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n})$. De aici rezultă că $(-1)^n \cdot \varepsilon_0 \cdot \dots \cdot \varepsilon_n = -2$.

  Să presupunem că putem scrie $X^n - 2$ ca produs de polinoame ireductibile peste $\mathbb{Q}[X]$:
$$X^n - 2 = (X^{k_1} + \dots + a_1) \dots (X^{k_r} + \dots + a_r)$$
  Toate aceste polinoame trebuie să fie de grad cel puțin 2, pentru că rădăcinile polinomului nu sunt numere raționale.

  Dacă egalăm cele două descompuneri, și ne uităm la termenii liberi care apar când calculăm produse dintre unii termeni, am obține că un produs de numere raționale $a_{i_1} \dots a_{i_p}$ este egal cu un produs de numere complexe $\varepsilon_{j_1} \dots \varepsilon_{j_r}$. Deci polinomul nu poate fi descompus peste $\mathbb{Q}$.

□

Exercițiul (3.8)**.** Descompuneți polinomul $X^n - 1, 1 \leq n \leq 6$, în produs de polinoame ireductibile în $\mathbb{Q}[X]$, $\mathbb{R}[X]$, respectiv $\mathbb{C}[X]$.

Demonstrație.

- Pentru $n = 1$, polinomul $X - 1$ este deja ireductibil, fiind de grad 1.
- Pentru $n = 2$, polinomul $X^2 - 1$ se descompune ca $(X - 1)(X + 1)$.
- Pentru $n = 3$, polinomul $X^3 - 1$ se descompune ca $(X-1)(X^2+X+1)$. Peste $\mathbb{Q}$ și $\mathbb{R}$, factorul $X^2 + X + 1$ este ireductibil, fiind de gradul 2, cu $\Delta < 0$.

  Peste $\mathbb{C}$, descompunerea completă este $(X - 1)(X - e^{i\frac{2\pi}{3}})(X - e^{i\frac{2\pi}{3}})$.

- Pentru $n = 4$, polinomul $X^4 - 1$ se descompune ca $(X^2 - 1)(X^2 + 1) = (X - 1)(X + 1)(X^2 + 1)$. Aceasta este descompunerea în factori ireductibili peste $\mathbb{Q}$ și $\mathbb{R}$.

  Peste $\mathbb{C}$ polinomul se descompune ca $(X - 1)(X + 1)(X - i)(X + i)$.

- Pentru $n = 5$, polinomul $X^5 - 1$ se descompune ca $(X - 1)(X^4 + X^3 + X^2 + X + 1)$. Această descompunere este ireductibilă peste $\mathbb{Q}$.

  Peste $\mathbb{R}$ mai putem descompune polinomul în $(X - 1)(X^2 + \frac{1-\sqrt{5}}{2}X + 1)(X^2 + \frac{1+\sqrt{5}}{2}X + 1)$.

  Peste $\mathbb{C}$ polinomul se descompune complet în $(X - \varepsilon_0) \dots (X - \varepsilon_4)$, unde $\varepsilon_k = \cos\frac{2k\pi}{5} + i \sin\frac{2k\pi}{5}$.

- Pentru $n = 6$, putem scrie $X^6 - 1$ ca $(X^3 - 1)(X^3 + 1)$. Deja am analizat descompunerea lui $X^3 - 1$.

  În ceea ce privește $X^3 + 1$, acest polinom se descompune în $(X + 1)(X^2 - X + 1)$. Aceasta este descompunerea finală peste $\mathbb{Q}$ și $\mathbb{R}$, dar peste $\mathbb{C}$ mai putem descompune $X^2 - X + 1$ în $(X - \varepsilon_1)(X - \varepsilon_2)$, unde $\varepsilon_k = -(\cos\frac{2k\pi}{3} + i \sin\frac{2k\pi}{3})$.

□

4.4 Teorema chineză a resturilor

Exercițiul (4.1)**.** Să se afle cea mai mică soluție pozitivă a sistemului de congruențe

$$\begin{cases} x \equiv 5 \mod 18 \\ x \equiv 27 \mod 35 \end{cases}$$

Demonstrație. Deoarece 18 și 35 sunt prime între ele, putem aplica teorema chineză a resturilor. Începem prin a găsi inversul modular al lui 18 în $\mathbb{Z}_{35}$, respectiv al lui 35 în $\mathbb{Z}_{18}$ (putem face asta folosind algoritmul lui Euclid extins):

$$\begin{cases} 18 \cdot 2 \equiv 1 \mod 35 \\ 35 \cdot 17 \equiv 1 \mod 18 \end{cases}$$

Atunci $x = 27 \cdot (18 \cdot 2) + 5 \cdot (35 \cdot 17)$ este o soluție pozitivă a sistemului. Pentru a găsi cea mai mică soluție pozitivă, calculăm restul împărțirii lui x la $18 \cdot 35$:

$$27 \cdot (18 \cdot 2) + 5 \cdot (35 \cdot 17) \equiv 167 \mod 18 \cdot 35$$

Verificare:

$$\begin{cases} 167 & \equiv 5 \mod 18 \\ 167 & \equiv 27 \mod 35 \end{cases}$$

□

Exercițiul (4.2)**.** Rezolvați sistemul de congruențe

$$\begin{cases} 6x \equiv 2 \mod 8 \\ 5x \equiv 5 \mod 6 \end{cases}$$

Demonstrație. Deoarece 8 și 6 nu sunt prime între ele, nu putem aplica teorema chineză a resturilor. Încercăm să mai simplificăm sistemul pentru a găsi o soluție manual.

În prima ecuație putem simplifica cu 2:

$$\begin{cases} 3x \equiv 1 \mod 4 \\ 5x \equiv 5 \mod 6 \end{cases}$$

Putem înmulți prima ecuație cu inversul modulo 4 al lui 3, și a doua ecuație cu inversul modulo 6 al lui 5. Sistemul devine:

$$\begin{cases} x \equiv 3 \mod 4 \\ x \equiv 1 \mod 6 \end{cases}$$

Trebuie să găsim soluția care este de forma $x = 4p + 3 = 6q + 1$ pentru un $p, q \in \mathbb{Z}$. De asemenea, este suficient să căutăm soluția printre numerele cuprinse între 0 și $4 \cdot 6 = 24$.

Observăm că 19 este o soluție:

$$\begin{cases} 19 \equiv 3 \mod 4 \\ 19 \equiv 1 \mod 6 \end{cases}$$

De asemenea, toate numerele de forma $24k + 19, \forall k \in \mathbb{Z}$ sunt soluții. □

5 Algebră liniară

Exercițiile alese de domnul profesor sunt din cartea "Algebra 1" de Tiberiu Dumitrescu, disponibilă pe internet.

5.1 Determinanți

Exercițiul (176)**.** Fie x_1, x_2, x_3 rădăcinile ecuației $x^3+px+q=0$. Calculați Δ^2 în funcție de p și q, unde

$$\Delta = \begin{vmatrix} 1 & 1 & 1 \\ x_1 & x_2 & x_3 \\ x_1^2 & x_2^2 & x_3^2 \end{vmatrix}$$

Demonstrație. Putem să dezvoltăm Δ ca un determinant Vandermonde, și astfel trebuie să calculăm $(x_2-x_1)^2(x_3-x_1)^2(x_3-x_2)^2$. Acesta este un polinom simetric, deci poate fi scris în funcție de polinoamele simetrice fundamentale s_1, s_2, s_3, pe care apoi le exprimăm în funcție de p și q.

Altfel, putem să ne folosim de faptul că $\det A = \det A^\top$, de unde

$$(\det A) \cdot (\det A^\top) = (\det A) \cdot (\det A) = (\det A)^2$$

Deci

$$\begin{aligned} \Delta^2 &= \det \left(\begin{pmatrix} 1 & 1 & 1 \\ x_1 & x_2 & x_3 \\ x_1^2 & x_2^2 & x_3^2 \end{pmatrix} \cdot \begin{pmatrix} 1 & x_1 & x_1^2 \\ 1 & x_2 & x_2^2 \\ 1 & x_3 & x_3^2 \end{pmatrix} \right) \\ &= \begin{vmatrix} 3 & x_1+x_2+x_3 & x_1^2+x_2^2+x_3^2 \\ x_1+x_2+x_3 & x_1^2+x_2^2+x_3^2 & x_1^3+x_2^3+x_3^3 \\ x_1^2+x_2^2+x_3^2 & x_1^3+x_2^3+x_3^3 & x_1^4+x_2^4+x_3^4 \end{vmatrix} \end{aligned}$$

Acum trebuie să obținem unele dintre aceste expresii în funcție de p și q.

$$\begin{aligned} x_1+x_2+x_3 &= 0 \\ x_1x_2+x_1x_3+x_2x_3 &= p \\ x_1x_2x_3 &= -q \\ x_1^2+x_2^2+x_3^2 &= -2p \\ x_1^3+x_2^3+x_3^3 &= -3q \\ x_1^4+x_2^4+x_3^4 &= 2p^2 \end{aligned}$$

Determinantul devine

$$\begin{aligned} \Delta^2 &= \begin{vmatrix} 3 & 0 & -2p \\ 0 & -2p & -3q \\ -2p & -3q & 2p^2 \end{vmatrix} \\ &= -4p^3 - 27q^2 \end{aligned}$$

□

Exercițiul (179)**.** Calculați determinantul

$$\Delta = \begin{vmatrix} a_1 & x & x & ... & x \\ x & a_2 & x & ... & x \\ x & x & a_3 & ... & x \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x & x & x & ... & a_n \end{vmatrix}$$

Demonstrație. Scădem prima linie din toate celelalte și scoatem factorii comuni:

$$\Delta = \begin{vmatrix} a_1 & x & x & ... & x \\ x-a_1 & a_2-x & 0 & ... & 0 \\ x-a_1 & 0 & a_3-x & ... & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x-a_1 & 0 & 0 & ... & a_n-x \end{vmatrix}$$

$$= (a_1-x)...(a_n-x) \begin{vmatrix} \frac{a_1}{a_1-x} & \frac{x}{a_2-x} & \frac{x}{a_3-x} & ... & \frac{x}{a_n-x} \\ -1 & 1 & 0 & ... & 0 \\ -1 & 0 & 1 & ... & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -1 & 0 & 0 & ... & 1 \end{vmatrix}$$

Adunăm toate coloanele la prima și dezvoltăm după prima linie:

$$= (a_1-x)...(a_n-x) \begin{vmatrix} \frac{a_1}{a_1-x}+\cdots+\frac{x}{a_n-x} & \frac{x}{a_2-x} & ... & \frac{x}{a_n-x} \\ 0 & 1 & ... & 0 \\ 0 & 0 & ... & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & ... & 1 \end{vmatrix}$$

$$= (a_1-x)...(a_n-x)\left(\frac{a_1}{a_1-x}+\frac{x}{a_2-x}+\cdots+\frac{x}{a_n-x}\right)$$

În cazul în care $x \in \{ a_1, ..., a_n \}$, trebuie să desfacem acel produs. Fracțiile dispar și formula rămâne validă. □

Exercițiul (180)**.** Calculați următorul determinant prin dezvoltare Laplace după liniile 1 și 2:

$$\Delta = \begin{vmatrix} 5 & 3 & 0 & 0 & 0 \\ 2 & 5 & 3 & 0 & 0 \\ 0 & 2 & 5 & 3 & 0 \\ 0 & 0 & 2 & 5 & 3 \\ 0 & 0 & 0 & 2 & 5 \end{vmatrix}$$

Demonstrație. Dezvoltăm cu regula lui Laplace după primele două linii:

$$\begin{aligned}\Delta = &\underbrace{(-1)^{1+1+2+2}}_{1}\underbrace{\begin{vmatrix}5 & 3\\ 2 & 5\end{vmatrix}}_{19}\underbrace{\begin{vmatrix}5 & 3 & 0\\ 2 & 5 & 3\\ 0 & 2 & 5\end{vmatrix}}_{95-30}\\ &+\underbrace{(-1)^{1+1+2+3}}_{-1}\underbrace{\begin{vmatrix}5 & 0\\ 2 & 3\end{vmatrix}}_{15}\underbrace{\begin{vmatrix}2 & 3 & 0\\ 0 & 5 & 3\\ 0 & 2 & 5\end{vmatrix}}_{2\cdot 19}\\ &+\underbrace{(-1)^{1+2+2+3}}_{1}\underbrace{\begin{vmatrix}3 & 0\\ 5 & 3\end{vmatrix}}_{9}\underbrace{\begin{vmatrix}0 & 3 & 0\\ 0 & 5 & 3\\ 0 & 2 & 5\end{vmatrix}}_{0}\\ &= 95\cdot 19 - 30\cdot 19 - 30\cdot 19\\ &= 19\cdot 35\end{aligned}$$

□

Exercițiul (185)**.** Determinați numărul de matrici inversabile din $M_3(\mathbb{Z}_2)$. Generalizare.

Demonstrație. Construim matricea în așa fel încât determinantul ei să nu fie $\hat{0}$.

1. Pentru a construi prima coloană, trebuie să alegem trei elemente din mulțimea $\left\{\hat{0}, \hat{1}\right\}$. Acestea nu pot fi toate $\hat{0}$, altfel determinantul ar fi nul. Deci avem $2^3 - 1$ posibilități.

2. A doua coloană trebuie să fie diferită de coloana nulă, și diferită de prima coloană (dacă două coloane sunt egale sau proporționale, determinantul este nul). Atunci avem $2^3 - 2$ posibilități.

3. Ultima coloană trebuie să fie diferită de coloana nulă, diferită de primele două, și să nu fie combinație liniară de primele două coloane. Singura combinație liniară posibilă în $\mathbb{Z}_2$ ar fi suma primelor două coloane. Astfel avem $2^3 - 4$ posibilități.

În concluzie, sunt $(2^3 - 1)(2^3 - 2)(2^3 - 4) = 168$ moduri de a construi o matrice inversabilă în $M_3(\mathbb{Z}_2)$.

Pe cazul general de matrici din $M_n(\mathbb{Z}_2)$ numărul de matrici inversabile este $(2^n - 2^0)\cdot(2^n - 2^1)\cdot\cdots\cdot(2^n - 2^{n-1})$. □

5.2 Eșalonare. Metoda lui Gauss

Exercițiul (212)**.** Eșalonați matricea

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

și găsiți baze în subspațiile generate de liniile, respectiv coloanele matricei.

Demonstrație.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

$$\overset{\substack{L_2-L_1 \\ \sim \\ L_3-2L_1}}{} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 0 & 1 & -1 \\ 0 & -1 & -5 & -4 \end{pmatrix}$$

$$\overset{\substack{(-1)L_3 \\ \sim \\ L_2 \leftrightarrow L_3}}{} \begin{pmatrix} 1 & 2 & 3 & 4 \\ 0 & 1 & 5 & 4 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

$$\overset{L_1-2L_2}{\sim} \begin{pmatrix} 1 & 0 & -7 & -4 \\ 0 & 1 & 5 & 4 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

$$\overset{\substack{L_1+7L_3 \\ \sim \\ L_2-5L_3}}{} \begin{pmatrix} 1 & 0 & 0 & -11 \\ 0 & 1 & 0 & 9 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

Vectorii coloană ai matricei sunt

$$C = \{(1,0,0), (0,1,0), (0,0,1), (-11,9,-1)\}$$

Aceștia generează întreg $\mathbb{R}^3$, deci o bază pentru ei este baza canonică $B_0 = \{ (1,0,0), (0,1,0), (0,0,1) \}$.

Vectorii linie sunt $L = \{(1,0,0,-11), (0,1,0,9), (0,0,1,-1)\}$. Deoarece avem 3 vectori din $\mathbb{R}^4$ care sunt și linear independenți, ei generează un hiperplan 3-dimensional în $\mathbb{R}^4$, și îi putem lua și ca bază pentru acest subspațiu. □

Exercițiul (213)**.** Rezolvați sistemul de ecuații liniare

$$\begin{cases} x - 2y + z + t = 1 \\ x - 2y + z - t = -1 \\ x - 2y + z + 5t = 5 \end{cases}$$

Demonstrație. Construim matricea extinsă a sistemului:

$$A^e = \left(\begin{array}{cccc|c} 1 & -2 & 1 & 1 & 1 \\ 1 & -2 & 1 & -1 & -1 \\ 1 & -2 & 1 & 5 & 5 \end{array}\right)$$
$$\overset{\substack{L_2-L_1 \\ L_3-L_1}}{\sim} \left(\begin{array}{cccc|c} 1 & -2 & 1 & 1 & 1 \\ 0 & 0 & 0 & -2 & -2 \\ 0 & 0 & 0 & 4 & 4 \end{array}\right)$$
$$\overset{\substack{L_3+2L_2 \\ (-\frac{1}{2})L_2}}{\sim} \left(\begin{array}{cccc|c} 1 & -2 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$
$$\overset{L_1-L_2}{\sim} \left(\begin{array}{cccc|c} 1 & -2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Acum putem rescrie sistemul echivalent din matrice:

$$\begin{cases} x - 2y + z = 0 \\ t = 1 \end{cases}$$

Rescriem necunoscutele principale x și t (necunoscutele pe coloanele cărora avem pivoții) în funcție de celelalte necunoscute (adică y, z).

Mulțimea soluțiilor este $S = \{\ (2y - z, y, z, 1) \mid y, z \in \mathbb{R}\ \}$.

Pentru a găsi soluția particulară, separăm termenii liberi de cei care depind de o variabilă, și rescriem vectorial ecuațiile:

$$S = (0, 0, 0, 1) + (2y + z, y, z, 0)$$

Pentru a determina o bază care să genereze subspațiul vectorial al soluțiilor, separăm componentele care depind de y, respectiv z:

$$\begin{aligned} S &= (0, 0, 0, 1) + y(2, 1, 0, 0) + z(-1, 0, 1, 0) \\ &= (0, 0, 0, 1) + \langle (2, 1, 0, 0), (-1, 0, 1, 0) \rangle \end{aligned}$$

□

Exercițiul (214)**.** Rezolvați sistemul de ecuații liniare

$$\begin{cases} x + y - 3z = -1 \\ 2x + y - 2z = 1 \\ x + y + z = 3 \\ x + 2y - 3z = 1 \end{cases}$$

Demonstrație. Scriem matricea extinsă a sistemului și rezolvăm prin metoda lui Gauss:

$$\left(\begin{array}{cccc|c} 1 & 1 & -3 & & -1 \\ 1 & 1 & -2 & & 1 \\ 1 & 1 & 1 & & 3 \\ 1 & 2 & -3 & & 1 \end{array}\right)$$

$$\begin{array}{l} L_2-L_1 \\ L_3-L_1 \\ \sim \\ L_4-L_1 \end{array} \left(\begin{array}{cccc|c} 1 & 1 & -3 & & -1 \\ 0 & 0 & 1 & & 2 \\ 0 & 0 & 4 & & 4 \\ 0 & 1 & 0 & & 2 \end{array}\right)$$

$$\begin{array}{l} (\frac{1}{4})L_3 \\ \sim \\ L_3-L_2 \end{array} \left(\begin{array}{cccc|c} 1 & 1 & -3 & & -1 \\ 0 & 0 & 1 & & 2 \\ 0 & 0 & 0 & & -1 \\ 0 & 1 & 0 & & 2 \end{array}\right)$$

Deoarece deja am obținut o contradicție pe linia 3 ($0 = -1$), sistemul este incompatibil. □

5.3 Inversa unei matrici prin eșalonare

Exercițiul (215)**.** Calculați inversa matricei următoare prin eșalonare

$$A = \begin{pmatrix} 2 & 1 & 0 & 0 \\ 3 & 2 & 0 & 0 \\ 1 & 1 & 3 & 4 \\ 2 & -1 & 2 & 3 \end{pmatrix}$$

Demonstrație. Scriem matricea extinsă, cu I_4 pe partea dreaptă:

$$\left(\begin{array}{cccc|cccc} 2 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 3 & 2 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 3 & 4 & 0 & 0 & 1 & 0 \\ 2 & -1 & 2 & 3 & 0 & 0 & 0 & 1 \end{array}\right)$$

$$\overset{L_1 \leftrightarrow L_3}{\sim} \left(\begin{array}{cccc|cccc} 1 & 1 & 3 & 4 & 0 & 0 & 1 & 0 \\ 3 & 2 & 0 & 0 & 0 & 1 & 0 & 0 \\ 2 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 2 & -1 & 2 & 3 & 0 & 0 & 0 & 1 \end{array}\right)$$

$$\begin{array}{l} L_2-3L_1 \\ (-1)L_2 \\ \sim \\ L_3-2L_1 \\ L_4-2L_1 \end{array} \left(\begin{array}{cccc|cccc} 1 & 1 & 3 & 4 & 0 & 0 & 1 & 0 \\ 0 & 1 & 9 & 12 & 0 & -1 & 3 & 0 \\ 0 & -1 & -6 & -8 & 1 & 0 & -2 & 0 \\ 0 & -3 & -4 & -5 & 0 & 0 & -2 & 1 \end{array}\right)$$

$$\begin{array}{l} L_3+L_2 \\ \sim \\ L_4+L_2 \end{array} \left(\begin{array}{cccc|cccc} 1 & 0 & -6 & -8 & 0 & 1 & -2 & 0 \\ 0 & 1 & 9 & 12 & 0 & -1 & 3 & 0 \\ 0 & 0 & 3 & 4 & 1 & -1 & 1 & 0 \\ 0 & 0 & 23 & 31 & 0 & -3 & 7 & 1 \end{array}\right)$$

$$\begin{array}{l} L_1+2L_3 \\ L_2-3L_3 \\ \sim \\ 8L_3 \end{array} \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 2 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & -3 & 2 & 0 & 0 \\ 0 & 0 & 24 & 32 & 8 & -8 & 8 & 0 \\ 0 & 0 & 23 & 31 & 0 & -3 & 7 & 1 \end{array}\right)$$

$$\overset{L_3-L_4}{\sim} \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 2 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & -3 & 2 & 0 & 0 \\ 0 & 0 & 1 & 1 & 8 & -5 & 1 & -1 \\ 0 & 0 & 23 & 31 & 0 & -3 & 7 & 1 \end{array}\right)$$

$$\overset{L_4-23L_4}{\sim} \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 2 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & -3 & 2 & 0 & 0 \\ 0 & 0 & 1 & 1 & 8 & -5 & 1 & -1 \\ 0 & 0 & 0 & 8 & -184 & 112 & -16 & 24 \end{array}\right)$$

$$\overset{\frac{1}{8}L_4}{\sim} \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 2 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & -3 & 2 & 0 & 0 \\ 0 & 0 & 1 & 1 & 8 & -5 & 1 & -1 \\ 0 & 0 & 0 & 1 & -23 & 14 & -2 & 3 \end{array}\right)$$

$$\overset{L_3-L_4}{\sim} \left(\begin{array}{cccc|cccc} 1 & 0 & 0 & 0 & 2 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & -3 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 & 31 & -19 & 3 & -4 \\ 0 & 0 & 0 & 1 & -23 & 14 & -2 & 3 \end{array}\right)$$

□