INELE

1. Generalităţi

Definiţia 1.1. *Se numeşte* inel *o mulţime nevidă R împreună cu două operaţii algebrice $(a, b) \mapsto a+b$ (numită* adunare*) şi $(a, b) \mapsto ab$ (numită* înmulţire*) care satisfac următoarele proprietăţi:*
1) $(R, +)$ este grup comutativ;
2) $a(bc) = (ab)c$ pentru orice $a, b, c \in R$ (înmulţirea este asociativă);
3) $a(b + c) = ab + ac$ şi $(b + c)a = ba + ca$ pentru orice $a, b, c \in R$ (înmulţirea este distributivă faţă de adunare la stânga şi la dreapta);
Dacă, în plus,
4) $ab = ba$ pentru orice $a, b \in R$,
atunci R se numeşte inel comutativ*.*
Dacă inelul R are element neutru în raport cu operaţia de înmulţire, atunci se numeşte inel unitar*.*

Elementul neutru la adunare (înmulţire) se notează cu 0 (respectiv, 1) şi se numeşte *elementul nul* (*elementul unitate*) al inelului. Un inel format doar din elementul nul se numeşte *inelul nul*.

Exerciţiul 1.2. Fie R un inel unitar cu proprietatea că $ab = 0$ pentru orice $a, b \in R$. Arătaţi că R este inelul nul. Mai rămâne adevărată concluzia dacă inelul nu este unitar?

Exemplul 1.3. (i) $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ sunt inele comutative şi unitare.
(ii) $(2\mathbb{Z}, +, \cdot)$ este inel comutativ, dar nu este unitar.
(iii) $(\mathbb{Z}_n, +, \cdot)$ este inel comutativ şi unitar.
(iv) Fie G grup comutativ. Atunci $(\mathrm{End}(G), +, \circ)$ este inel unitar şi se numeşte *inelul endomorfismelor lui G*.
(v) Fie R un inel (unitar) şi X o mulţime nevidă. Definim pe mulţimea R^X a funcţiilor $f : X \to R$ o structură de inel (unitar) astfel: dacă $f, g \in R^X$, atunci $(f + g)(x) = f(x) + g(x)$ şi $(fg)(x) = f(x)g(x)$ pentru orice $x \in X$. Acesta se numeşte *inelul funcţiilor definite pe X cu valori în R*. Elementul nul al acestui inel este funcţia $\mathbf{0} : X \to R$ definită prin $\mathbf{0}(x) = 0$ pentru orice $x \in X$ (elementul unitate este funcţia $\mathbf{1} : X \to R$ definită prin $\mathbf{1}(x) = 1$ pentru orice $x \in X$).
(vi) Fie R un inel (unitar). Atunci $(M_n(R), +, \cdot)$ este inel (unitar) şi se numeşte *inelul matricelor pătratice de ordin n peste R*. În cazul în care R este unitar, elementul unitate al lui $M_n(R)$ se notează cu I_n şi este matricea care are 1 pe diagonala principală şi 0 în rest. În general, $M_n(R)$ nu este inel comutativ.
(vii) Fie R_1, R_2 inele şi $R = R_1 \times R_2$. Atunci $(R, +, \cdot)$ este inel, unde

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2),$$

$$(a_1, a_2) \cdot (b_1, b_2) = (a_1b_1, a_2b_2),$$

pentru orice $a_1, b_1 \in R_1$, $a_2, b_2 \in R_2$. Inelul R se numeşte *produsul direct al inelelor* R_1, R_2.
Să observăm că R este inel unitar (comutativ) dacă şi numai dacă R_1 şi R_2 sunt inele unitare (comutative).

Construcţia de mai sus se generalizează imediat la o familie arbitrară de inele. Fie $(R_i)_{i\in I}$ o familie nevidă de inele. Pe produsul cartezian $R = \prod_{i\in I} R_i$ introducem următoarele operaţii algebrice:

$$(x_i)_{i\in I} + (y_i)_{i\in I} = (x_i + y_i)_{i\in I},$$

$$(x_i)_{i\in I} \cdot (y_i)_{i\in I} = (x_i y_i)_{i\in I},$$

pentru orice $x_i, y_i \in R$, $i \in I$. Atunci $(R, +, \cdot)$ este un inel numit *produsul direct al familiei de inele* $(R_i)_{i\in I}$.
Analog, R este inel unitar (comutativ) dacă şi numai dacă R_i, $i \in I$ sunt inele unitare (comutative).

Remarca 1.4. Inelul R^X din exemplul (v) este un caz particular de produs direct de inele. Mai precis, acesta este produsul direct al familiei de inele $(R_x)_{x\in X}$, unde $R_x = R$ pentru orice $x \in X$.

Exerciţiul 1.5. Să se arate că $(\mathbb{R}^{\mathbb{R}}, +, \circ)$ nu este inel.

Exerciţiul 1.6. Fie R un inel. Să se arate că inelul de matrice $M_n(R)$ este comutativ dacă şi numai dacă este satisfăcută una din următoarele două condiţii:
(i) $n = 1$ şi R este comutativ;
(ii) $ab = 0$ pentru orice $a, b \in R$.

Exerciţiul 1.7. Fie M o mulţime nevidă. Arătaţi că $(\mathcal{P}(M), \Delta, \cap)$ este inel comutativ şi unitar.

Avem următoarele reguli de calcul într-un inel:

Propoziţia 1.8. *Fie R un inel. Atunci*
(i) $0a = a0 = 0$ *pentru orice* $a \in R$.
(ii) $a(-b) = (-a)b = -(ab)$ *şi* $(-a)(-b) = ab$ *pentru orice* $a, b \in R$.
(iii) $(na)b = a(nb) = n(ab)$ *pentru orice* $n \in \mathbb{Z}$ *şi* $a, b, c \in R$.
(iv) $(\sum_{i=1}^m a_i)(\sum_{j=1}^n b_j) = \sum_{i=1}^m \sum_{j=1}^n a_i b_j$ *pentru orice* $a_i, b_j \in R$.
(v) (Formula binomului lui Newton) *Fie* $a, b \in R$ *cu proprietatea că* $ab = ba$. *Atunci*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.$$

Definiţia 1.9. *Fie R un inel şi $a \in R$. Atunci a se numeşte* divizor al lui zero la stânga (la dreapta) *dacă există $b \in R$, $b \neq 0$ astfel încât $ab = 0$ (respectiv, $ba = 0$). Dacă a este divizor al lui zero la stânga şi la dreapta, atunci se va numi* divizor al lui zero.

Să observăm că dacă R nu este inelul nul, atunci 0 este divizor al lui zero.

Exerciţiul 1.10. Arătaţi că dacă un inel are un divizor al lui zero la stânga (dreapta) nenul, atunci are un divizor al lui zero nenul.

Exercițiul 1.11. * Fie V un spațiu vectorial de dimensiune numărabilă și $R = (\mathrm{End}(V), +, \circ)$. Găsiți un element $a \in R$ care să fie divizor al lui zero la stânga, dar nu și la dreapta.

Definiția 1.12. *Fie R un inel nenul. Dacă R nu are divizori ai lui zero nenuli, atunci R se numește* inel integru. *Un inel integru și comutativ se numește* domeniu de integritate.

Propoziția 1.13. *Fie R un inel nenul. Atunci R este inel integru dacă și numai dacă oricare ar fi $a, b \in R$ cu $ab = 0$ rezultă $a = 0$ sau $b = 0$.*

Exemplul 1.14. (i) $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ sunt domenii de integritate.
(ii) Un element $\widehat{a} \in \mathbb{Z}_n$ este divizor al lui zero dacă și numai dacă $(a, n) \neq 1$. Așadar $\mathbb{Z}_n$ este domeniu de integritate dacă și numai dacă n este număr prim.
(iii) Dacă R este un inel unitar nenul și $n \geq 2$, atunci $(M_n(R), +, \cdot)$ nu este inel integru. De exemplu, matricea $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$ este divizor al lui zero.
(iv) Dacă R_1, R_2 sunt inele nenule, atunci $R_1 \times R_2$ nu este inel integru. De exemplu, perechea $(a_1, 0)$, unde $a_1 \in R_1$, $a_1 \neq 0$, este divizor al lui zero.
(v) Fie M o mulțime cu $|M| \geq 2$. Atunci inelul $(\mathcal{P}(M), \Delta, \cap)$ nu este integru.

Exercițiul 1.15. (i) 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 $f(x_0) = 0$.
(ii) Fie $\mathcal{C}(\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ este continuă}\}$ cu operațiile de adunare și înmulțire a funcțiilor. Arătați că $f \in \mathcal{C}(\mathbb{R})$ este divizor al lui zero dacă și numai dacă există $(a, b) \subset \mathbb{R}$ astfel încât $f(x) = 0$ pentru orice $x \in (a, b)$.

Definiția 1.16. *Fie R un inel unitar. Un element $a \in R$ se numește* inversabil la stânga (la dreapta) *dacă există $a' \in R$ astfel încât $a'a = 1$ (respectiv, $aa' = 1$). Dacă a este inversabil la stânga și la dreapta, atunci se va numi* inversabil.

Exercițiul 1.17. * Fie V un spațiu vectorial de dimensiune numărabilă și $R = (\mathrm{End}(V), +, \circ)$. Găsiți un element $a \in R$ care să fie inversabil la stânga, dar nu și la dreapta.

Notație: $U(R) = \{a \in R : a \text{ inversabil}\}$.

Remarca 1.18. (i) $a \in U(R)$ dacă și numai dacă există $a' \in R$ astfel încât $aa' = a'a = 1$.
(ii) $U(R)$ este grup în raport cu înmulțirea și se numește *grupul unităților lui R*.
(iii) Elementele inversabile nu sunt divizori ai lui zero.

Exemplul 1.19. (i) $U(\mathbb{Z}) = \{-1, 1\}$, $U(\mathbb{Q}) = \mathbb{Q} \setminus \{0\}$, $U(\mathbb{R}) = \mathbb{R} \setminus \{0\}$.
(ii) $U(\mathbb{Z}_n) = \{\widehat{a} \in \mathbb{Z}_n : (a, n) = 1\}$.
(iii) $U(\mathrm{End}(G)) = \mathrm{Aut}(G)$.
(iv) Fie R un inel comutativ și unitar. Atunci

$$U(M_n(R)) = \{A \in M_n(R) : \det A \in U(R)\}.$$

(v) Fie R_1, R_2 inele unitare. Atunci $U(R_1 \times R_2) = U(R_1) \times U(R_2)$.

În afara elementelor inversabile și a divizorilor lui zero, mai există și alte elemente remarcabile într-un inel.

Definiţia 1.20. *Fie R un inel şi $x \in R$. Elementul x se numeşte* nilpotent *dacă există $n \in \mathbb{N}^*$ astfel încât $x^n = 0$.*

Remarca 1.21. (i) 0 este element nilpotent.
(ii) Un inel integru nu are elemente nilpotente nenule.

Exerciţiul 1.22. Să se determine elementele nilpotente în inelul $\mathbb{Z}_n$ şi să se afle numărul acestora.

Exerciţiul 1.23. Fie R un inel şi $x, y \in R$ elemente nilpotente.
(i) Dacă $xy = yx$, atunci xy şi $x + y$ sunt nilpotente.
(ii) Daţi exemple care să arate că proprietatea (i) nu mai rămâne adevărată dacă $xy \neq yx$.

Definiţia 1.24. *Fie R un inel şi $x \in R$. Elementul x se numeşte* idempotent *dacă $x^2 = x$.*

Remarca 1.25. (i) 0 şi 1 sunt elemente idempotente. (Acestea se mai numesc şi *idempotenţi triviali.*)
(ii) Dacă R este inel unitar şi $x \in R$ este idempotent, atunci şi $1-x$ este idempotent.
(iii) Un inel integru nu are idempotenţi netriviali.

Exemplul 1.26. Fie M o mulţime nevidă. În inelul $\mathcal{P}(M)$ orice element este idempotent. (Un inel cu proprietatea că orice element al său este idempotent se numeşte *inel boolean.*)

Exerciţiul 1.27. (i) Se consideră numărul natural $n \geq 2$ care are r factori primi distincţi în descompunerea sa. Să se arate că numărul idempotenţilor lui $\mathbb{Z}_n$ este 2^r.
(ii) Să se determine idempotenţii inelului $\mathbb{Z}_{36}$.

Exerciţiul 1.28. Fie R un inel boolean. Să se arate că R este comutativ.

Exerciţiul 1.29. * Fie R un inel cu proprietatea că $x^3 = x$ pentru orice $x \in R$. Să se arate că R este comutativ.

2. Subinele. Ideale

Definiţia 2.1. *Fie $(R, +, \cdot)$ un inel şi $S \subseteq R$ o submulţime nevidă. Atunci S se numeşte* subinel *al lui R dacă $(S, +, \cdot)$ este un inel. Dacă R este inel unitar şi S un subinel cu proprietatea că $1 \in S$, atunci S se numeşte* subinel unitar.

Propoziţia 2.2. *Fie R un inel şi $S \subseteq R$ o submulţime nevidă. Atunci S este subinel al lui R dacă şi numai dacă sunt satisfăcute următoarele condiţii:*
(i) $x, y \in S \implies x - y \in S$,
(ii) $x, y \in S \implies xy \in S$,
pentru orice $x, y \in S$.

Exemplul 2.3. (i) Dacă R este un inel, atunci $\{0\}$ şi R sunt subinele.
(ii) $\mathbb{Z} \subset \mathbb{Q}$ este subinel unitar.
(iii) $2\mathbb{Z} \subset \mathbb{Z}$ este subinel, dar nu este unitar.
(iv) $\widehat{5}\,\mathbb{Z}_{10} \subset \mathbb{Z}_{10}$ este subinel, dar nu este subinel unitar. Să remarcăm că $\widehat{5}\,\mathbb{Z}_{10}$ are totuşi element unitate, pe $\widehat{5}$. (Mai general, dacă R este inel comutativ unitar şi

$e \in R$ un idempotent netrivial, atunci $Re \subset R$ este subinel, $1 \notin Re$, dar Re are element unitate pe e.)
(v) $\mathcal{C}(\mathbb{R}) \subset \mathbb{R}^{\mathbb{R}}$ este subinel unitar.
(vi) Fie R un inel. Atunci $C(R) = \{a \in R : ax = xa, \forall x \in R\}$ este un subinel numit *centrul lui* R.

Exerciţiul 2.4. Fie R un inel unitar. Arătaţi că $C(M_n(R)) = \{aI_n : a \in C(R)\}$.

Definiţia 2.5. *Fie* R *un inel şi* $I \subseteq R$ *o submulţime nevidă. Atunci* I *se numeşte* ideal la stânga (dreapta) *al lui* R *dacă sunt satisfăcute următoarele condiţii:*
(i) $x, y \in I \implies x - y \in I$,
(ii) $a \in R$, $x \in I \implies ax \in I$ *(respectiv,* $xa \in I$*),*
pentru orice $a \in R$ *şi* $x, y \in I$.
Un ideal la stânga şi la dreapta al lui R *se numeşte* ideal bilateral *al lui* R.

Notaţii: $I \leq_s R$, $I \leq_d R$, respectiv $I \trianglelefteq R$.

Remarca 2.6. (i) Fie R un inel comutativ şi $I \subseteq R$ o submulţime nevidă. Atunci I este ideal la stânga al lui R dacă şi numai dacă I este ideal la dreapta al lui R dacă şi numai dacă I este ideal bilateral al lui R. În acest caz, I se numeşte *ideal* al lui R.
(ii) Evident, orice ideal este subinel, dar nu şi reciproc: $\mathbb{Z} \subset \mathbb{Q}$ este subinel, dar nu este ideal.
(iii) Fie R inel unitar şi $I \subseteq R$ un ideal la stânga (la dreapta, bilateral). Atunci $I = R$ dacă şi numai dacă I conţine un element inversabil.

Exemplul 2.7. (i) Dacă R este un inel, atunci $\{0\}$ şi R sunt ideale bilaterale.
(ii) Idealele lui $\mathbb{Z}$ sunt $n\mathbb{Z}$, $n \in \mathbb{N}$.
(iii) Idealele lui $\mathbb{Z}_n$ sunt $\widehat{d}\,\mathbb{Z}_n$, $d \mid n$.
(iv) Idealele lui $\mathbb{Q}$ sunt $\{0\}$ şi $\mathbb{Q}$. (Analog pentru $\mathbb{R}$.)
(v) Fie $R = M_2(\mathbb{Z})$ şi

$$I = \left\{ \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} : a, b \in \mathbb{Z} \right\},$$
$$J = \left\{ \begin{pmatrix} 0 & 0 \\ a & b \end{pmatrix} : a, b \in \mathbb{Z} \right\}.$$

Atunci I este ideal la stânga, dar nu şi la dreapta, iar J este ideal la dreapta, dar nu şi la stânga.

Exerciţiul 2.8. (i) Fie $R_1, \dots, R_n$ inele unitare şi $R = R_1 \times \cdots \times R_n$. Să se arate că idealele la stânga (la dreapta, bilaterale) ale lui R sunt de forma $I = I_1 \times \cdots \times I_n$, unde $I_1, \dots, I_n$ sunt ideale la stânga (la dreapta, bilaterale) în $R_1, \dots, R_n$, respectiv.
(ii) Să se arate că rezultatul de la (i) nu mai rămâne adevărat când avem un produs infinit de inele.

Exerciţiul 2.9. Fie R un inel unitar şi $n \in \mathbb{N}^*$.
(i) Să se arate că idealele bilaterale ale lui $M_n(R)$ sunt de forma $M_n(I)$, unde I este ideal bilateral al lui R.
(ii) Este adevărat că orice ideal la stânga al lui $M_n(R)$ este de forma $M_n(J)$, cu J ideal la stânga al lui R?

Lema 2.10. *Fie R un inel şi $I_\alpha \leq_s R$, $\alpha \in A$ o familie de ideale la stânga ale lui R. Atunci $\bigcap_{\alpha\in A} I_\alpha \leq_s R$. (Analog pentru ideale la dreapta, respectiv bilaterale.)*

Definiţia 2.11. *Fie R un inel unitar şi $X \subseteq R$ o submulţime. Notăm cu $(X)_s$ intersecţia tuturor idealelor la stânga care conţin pe X. Acesta este un ideal la stânga al lui R şi se numeşte* idealul la stânga generat de X.

Analog se defineşte $(X)_d$, idealul la dreapta generat de X, *respectiv (X),* idealul bilateral generat de X.

Remarca 2.12. Idealul la stânga (la dreapta, bilateral) generat de X este cel mai mic ideal la stânga (la dreapta, bilateral) care conţine pe X.

Definiţia 2.13. *Fie R un inel unitar şi $X \subseteq R$ o submulţime. Elementele lui X se numesc* generatori *pentru $(X)_s$.*
Dacă $I \leq_s R$ şi există $X \subseteq I$ o submulţime finită astfel încât $I = (X)_s$, atunci idealul I se numeşte finit generat*. Dacă X are un singur element, atunci idealul I se numeşte* principal.

De exemplu, orice ideal al lui $\mathbb{Z}$ (sau $\mathbb{Z}_n$) este principal.

Definiţia 2.14. *Un inel comutativ cu proprietatea că orice ideal al său este principal se numeşte* inel principal.

Exerciţiul 2.15. (i) Fie R_1, R_2 inele comutative şi $R = R_1 \times R_2$. Atunci R este inel principal dacă şi numai dacă R_1, R_2 sunt inele principale.
*(ii) Daţi un exemplu care să arate că, în general, un produs direct infinit de inele principale nu este neapărat un inel principal.

Exerciţiul 2.16. Fie M o mulţime nevidă.
(i) Arătaţi că dacă M este finită, atunci $(\mathcal{P}(M), \Delta, \cap)$ este inel principal.
*(ii) Arătaţi că dacă M nu este finită, atunci $(\mathcal{P}(M), \Delta, \cap)$ nu este inel principal.

Să determinăm acum forma elementelor din idealele generate de o submulţime.

Propoziţia 2.17. *Fie R un inel unitar şi $X \subseteq R$ o submulţime. Atunci*

$$(X)_s = \{y \in R : y = \sum_{i=1}^{n} a_i x_i, a_i \in R, x_i \in X, n \in \mathbb{N}\},$$

$$(X)_d = \{y \in R : y = \sum_{i=1}^{n} x_i a_i, a_i \in R, x_i \in X, n \in \mathbb{N}\},$$

$$(X) = \{y \in R : y = \sum_{i=1}^{n} a_i x_i b_i, a_i, b_i \in R, x_i \in X, n \in \mathbb{N}\}.$$

În particular,

$$(x)_s = \{y \in R : y = ax, a \in R\},$$
$$(x)_d = \{y \in R : y = xa, a \in R\},$$
$$(x) = \{y \in R : y = \sum_{i=1}^{n} a_i x b_i, a_i, b_i \in R, n \in \mathbb{N}\}.$$

Notaţii: $(x)_s = Rx$, $(x)_d = xR$, $(x) = RxR$.

3. Morfisme de inele

Definiţia 3.1. *Fie R, R' inele şi $f : R \to R'$ o funcţie. Aceasta se numeşte* morfism de inele *dacă*
$$f(x+y) = f(x) + f(y),$$
$$f(xy) = f(x)f(y),$$
pentru orice $x, y \in R$.
Dacă R, R' sunt inele unitare şi $f(1) = 1'$, atunci f se numeşte morfism unitar.

Remarca 3.2. Un morfism de inele este, în particular, un morfism de grupuri, aşadar $f(0) = 0$ şi $f(-x) = -f(x)$ pentru orice $x \in R$.

Exemplul 3.3. (i) Funcţia $f : R \to R'$ definită prin $f(x) = 0'$ pentru orice $x \in R$ este morfism de inele şi se numeşte *morfismul nul.*
(ii) Incluziunea $i : \mathbb{Z} \to \mathbb{Q}$ definită prin $i(x) = x$ pentru orice $x \in \mathbb{Z}$ este morfism unitar şi injectiv de inele.
(iii) Surjecţia canonică $p : \mathbb{Z} \to \mathbb{Z}_n$ definită prin $p(x) = \widehat{x}$ pentru orice $x \in \mathbb{Z}$ este morfism unitar şi surjectiv de inele.
(iv) Dacă R este un inel şi $f : R \to M_n(R)$ se defineşte prin
$$f(a) = \begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & a & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & a \end{pmatrix},$$
atunci f este morfism injectiv de inele. Dacă, în plus, R este unitar, atunci f este de asemenea morfism unitar.
(v) Fie R un inel (unitar) şi X o mulţime nevidă. Pentru orice $x \in X$ definim un morfism de inele (unitare) $\varphi_x : R^X \to R$ prin $\varphi_x(f) = f(x)$. Acesta se numeşte *morfismul de evaluare în x.*
(vi) Fie $(R_i)_{i \in I}$ o familie nevidă de inele (unitare). Pentru orice $j \in I$ definim un morfism de inele (unitare) $\pi_j : \prod_{i \in I} R_i \to R_j$ prin $\pi_j((x_i)_{i \in I}) = x_j$. Acesta se numeşte *proiecţia canonică pe componenta j.*

Propoziţia 3.4. *Fie $f : R \to R'$ şi $g : R' \to R''$ morfisme (unitare) de inele. Atunci $g \circ f : R \to R''$ este morfism (unitar) de inele.*

Definiţia 3.5. *Fie $f : R \to R'$ un morfism de inele. Atunci f se numeşte* izomorfism de inele *dacă există $g : R' \to R$ morfism de inele cu proprietatea că $f \circ g = 1_{R'}$ şi $g \circ f = 1_R$.*

Notaţie: $R \simeq R'$.

Propoziţia 3.6. *Fie $f : R \to R'$ un morfism de inele. Atunci f este izomorfism dacă şi numai dacă f este bijecţie.*

Definiţia 3.7. *Fie R un inel şi $f : R \to R$ un morfism de inele. Atunci f se numeşte* endomorfism *al lui R. Dacă, în plus, f este bijectiv, atunci se va numi* automorfism *al lui R.*

Exerciţiul 3.8. Fie M o mulţime nevidă. Arătaţi că $(\mathcal{P}(M), \Delta, \cap) \simeq (\mathbb{Z}_2^M, +, \cdot)$.

Exercițiul 3.9. Arătați că avem următoarele izomorfisme de inele:
$\mathrm{End}((\mathbb{Z},+)) \simeq \mathbb{Z}$, $\mathrm{End}((\mathbb{Q},+)) \simeq \mathbb{Q}$, $\mathrm{End}((\mathbb{Z}/n\mathbb{Z},+)) \simeq \mathbb{Z}/n\mathbb{Z}$, $\mathrm{End}((\mathbb{Z}\times\mathbb{Z},+)) \simeq M_2(\mathbb{Z})$. Pe de altă parte, $\mathrm{End}((\mathbb{R},+)) \not\simeq \mathbb{R}$.

Exercițiul 3.10. Determinați endomorfismele (automorfismele) următoarelor inele: $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$, $(\mathbb{Z}/n\mathbb{Z},+,\cdot)$, $(\mathbb{Z}\times\mathbb{Z},+,\cdot)$.

Propoziția 3.11. *Fie $f : R \to R'$ un morfism de inele.*
(i) Dacă $S \subseteq R$ este subinel, atunci $f(S) \subseteq R'$ este subinel.
Dacă $S' \subseteq R'$ este subinel, atunci $f^{-1}(S') \subseteq R$ este subinel.
(ii) Dacă $I \leq_s R$ și f este surjectiv*, atunci $f(I) \leq_s R'$.*
Dacă $I' \leq_s R'$, atunci $f^{-1}(I') \leq_s R$.
(Analog pentru ideale la dreapta, respectiv bilaterale.)

Exemplul 3.12. Imaginea unui ideal printr-un morfism nu este neapărat un ideal. De exemplu, imaginea lui $2\mathbb{Z}$ prin morfismul incluziune $i : \mathbb{Z} \to \mathbb{Q}$ nu este ideal.

Definiția 3.13. *Fie $f : R \to R'$ un morfism de inele. Atunci* $\mathrm{Im}\, f \subseteq R'$ *este un subinel numit* imaginea lui f*, iar* $\mathrm{Ker}\, f = f^{-1}(0)$ *este un ideal bilateral numit* nucleul lui f.

Din cele demonstrate în capitolul despre grupuri știm că f este morfism injectiv dacă și numai dacă $\mathrm{Ker}\, f = \{0\}$.

Teorema 3.14. (Teorema de corespondență pentru ideale) *Fie $f : R \to R'$ un morfism* surjectiv *de inele. Există o corespondență bijectivă între mulțimea idealelor la stânga (la dreapta, bilaterale) ale lui R care conțin pe* $\mathrm{Ker}\, f$ *și mulțimea tuturor idealelor la stânga (la dreapta, bilaterale) ale lui R', dată prin $I \mapsto f(I)$.*

4. Inele factor

Fie R un inel și $I \subseteq R$ un ideal *bilateral*. În particular, I este subgrup al lui $(R,+)$, iar $(R/I,+)$ este grup comutativ. Definim pe R/I o operație algebrică numită înmulțire astfel:

$$\widehat{a} \cdot \widehat{b} = \widehat{ab}.$$

Să arătăm că aceasta este bine definită: dacă $\widehat{a} = \widehat{a'}$ și $\widehat{b} = \widehat{b'}$, atunci $a - a' \in I$ și $b - b' \in I$. Scriem $ab - a'b' = a(b-b') + (a-a')b'$ și deoarece I este ideal bilateral $a(b-b') \in I$ și $(a-a')b' \in I$, deci $ab - a'b' \in I$ ceea ce este echivalent cu $\widehat{ab} = \widehat{a'b'}$. Acum rezultă cu ușurință că $(R/I,+,\cdot)$ este un inel.

Definiția 4.1. *Inelul R/I se numește* inelul factor *al lui R în raport cu idealul bilateral I. Funcția $p : R \to R/I$ definită prin $p(x) = \widehat{x}$ este un morfism surjectiv de inele și se numește* proiecția (surjecția) canonică *a lui R pe R/I.*

Remarca 4.2. (i) Dacă R este inel comutativ, atunci orice ideal al său este bilateral și deci putem vorbi de inelul factor al lui R în raport cu orice ideal al său.
(ii) Dacă R este inel unitar (comutativ), atunci R/I este inel unitar (comutativ).
(iii) Proiecția canonică $p : R \to R/\{0\}$ este izomorfism de inele.

Propoziţia 4.3. *Fie R un inel şi $I \subseteq R$ un ideal bilateral. Există o corespondenţă bijectivă între mulţimea idealelor la stânga (la dreapta, bilaterale) ale lui R care conţin pe I şi mulţimea tuturor idealelor la stânga (la dreapta, bilaterale) ale lui R/I, dată prin $J \mapsto J/I$.*

Exemplul 4.4. Idealele lui $\mathbb{Z}/n\mathbb{Z}$ sunt de forma $d\mathbb{Z}/n\mathbb{Z}$ cu $d \mid n$.

Teorema 4.5. (Proprietatea de universalitate a inelelor factor) *Fie $f : R \to R'$ un morfism de inele şi I un ideal bilateral al lui R. Dacă $I \subseteq \operatorname{Ker} f$, atunci există un morfism de inele $\overline{f} : R/I \to R'$ unic cu proprietatea că $\overline{f} \circ p = f$, unde $p : R \to R/I$ este proiecţia canonică. Mai mult:*
1) *$\overline{f}$ este injectiv dacă şi numai dacă $I = \operatorname{Ker} f$;*
2) *$\overline{f}$ este surjectiv dacă şi numai dacă $\overline{f}$ este surjectiv.*

Am observat mai înainte că dacă $f : R \to R'$ este un morfism de inele, atunci nucleul său, $\operatorname{Ker} f$, este ideal bilateral al lui R şi deci putem vorbi de inelul factor $R/\operatorname{Ker} f$. De asemenea, am arătat că $\operatorname{Im} f$ este un subinel al lui R'.

Teorema 4.6. (Teorema fundamentală de izomorfism pentru inele) *Fie $f : R \to R'$ un morfism de inele. Atunci există un izomorfism de inele*

$$\overline{f} : R/\operatorname{Ker} f \to \operatorname{Im} f.$$

Exerciţiul 4.7. (i) Fie $R_1, \dots, R_n$ inele unitare, $R = R_1 \times \cdots \times R_n$ şi $I = I_1 \times \cdots \times I_n$, unde $I_1, \dots, I_n$ sunt ideale bilaterale în $R_1, \dots, R_n$, respectiv. Să se arate că inelele R/I şi $R_1/I_1 \times \cdots \times R_n/I_n$ sunt izomorfe.

Exerciţiul 4.8. Fie R un inel unitar şi I ideal bilateral al lui R. Să se arate că inelele $M_n(R)/M_n(I)$ şi $M_n(R/I)$ sunt izomorfe.

Din teorema fundamentală de izomorfism pentru inele se obţin încă două teoreme de izomorfism foarte utile.

Teorema 4.9. (A doua teoremă de izomorfism pentru inele) *Fie R un inel, $S \subseteq R$ un subinel şi $J \subseteq R$ ideal bilateral. Atunci $S + J = \{s + j : s \in S, j \in J\}$ este subinel al lui R, J este ideal bilateral al lui $S + J$, $S \cap J$ este ideal bilateral al lui S şi*

$$(S + J)/J \simeq S/S \cap J.$$

Teorema 4.10. (A treia teoremă de izomorfism pentru inele) *Fie R un inel şi I, J ideale bilaterale ale lui R cu $J \subseteq I$. Atunci I/J este ideal bilateral al lui R/J şi*

$$(R/J)/(I/J) \simeq R/I.$$

Remarca 4.11. Dacă I, J sunt ideale la stânga (la dreapta, bilaterale) ale unui inel R, atunci $I + J = \{a + b : a \in I, b \in J\}$, respectiv $IJ = \{\sum_{k=1}^{n} a_k b_k : a_k \in I, b_n \in J, k \in \mathbb{N}\}$ este ideal la stânga (la dreapta, bilateral) al lui R şi se numeşte *suma*, respectiv *produsul* idealelor I şi J.

Exerciţiul 4.12. * Daţi un exemplu de inel şi de două subinele S_1, S_2 ale sale cu proprietatea că $S_1 + S_2$ nu este subinel.

Exerciţiul 4.13. * Daţi un exemplu de inel şi de două ideale I_1, I_2 ale sale cu proprietatea că $I_1 I_2 \neq I_2 I_1$.

5. Teorema Chineză a Resturilor

Fie $n_1, n_2 \geq 2$ două numere întregi prime între ele. Am demonstrat anterior că funcţia $f : \mathbb{Z}/(n_1n_2)\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ definită prin $f(\widehat{x}) = (\overline{x}, \overline{\overline{x}})$ este un izomorfism de inele. Se observă că dacă notăm $I_1 = n_1\mathbb{Z}$ şi $I_2 = n_2\mathbb{Z}$, atunci $I_1 + I_2 = \mathbb{Z}$ şi $I_1I_2 = I_1 \cap I_2$. Aceasta ne sugerează următoarea generalizare:

Definiţia 5.1. *Fie R un inel şi I_1, I_2 ideale bilaterale ale lui R cu proprietatea că $I_1 + I_2 = R$. Atunci idealele I_1 şi I_2 se numesc* comaximale.

Remarca 5.2. Dacă R este inel comutativ şi unitar, iar I_1, I_2 sunt ideale comaximale, atunci $I_1I_2 = I_1 \cap I_2$.

Exerciţiul 5.3. (i) Daţi un exemplu de inel comutativ R şi de două ideale comaximale $I_1, I_2 \subseteq R$ pentru care $I_1I_2 \neq I_1 \cap I_2$.
(ii) Fie R un inel unitar şi I_1, I_2 ideale comaximale. Atunci $I_1I_2 + I_2I_1 = I_1 \cap I_2$.
*(iii) Daţi un exemplu de inel necomutativ şi unitar R şi de două ideale comaximale $I_1, I_2 \subseteq R$ pentru care $I_1I_2 \neq I_1 \cap I_2$.

Teorema 5.4. *Fie R un inel şi I_1, I_2 ideale comaximale ale lui R. Atunci morfismul*

$$f : R/I_1 \cap I_2 \to R/I_1 \times R/I_2$$

definit prin $f(\widehat{x}) = (\overline{x}, \overline{\overline{x}})$ este un izomorfism de inele.

Proof. Se arată mai întâi că f este bine definit, iar apoi se arată că $(\overline{r}, \overline{\overline{0}})$ şi $(\overline{0}, \overline{\overline{s}})$ sunt în imaginea lui f pentru orice $r, s \in R$: deoarece $I_1 + I_2 = R$ există $x_1 \in I_1$ şi $x_2 \in I_2$ astfel încât $x_1 + x_2 = r$, respectiv există $y_1 \in I_1$ şi $y_2 \in I_2$ astfel încât $y_1 + y_2 = s$. Atunci $f(\widehat{x_2}) = (\overline{r}, \overline{\overline{0}})$ şi $f(\widehat{y_1}) = (\overline{0}, \overline{\overline{s}})$. De aici se obţine $f(\widehat{x_2 + y_1}) = (\overline{r}, \overline{\overline{s}})$, deci f este surjectiv. $\square$

Definiţia 5.5. *Dacă R este un inel şi $I_1, \ldots, I_n$, $n \geq 2$ sunt ideale bilaterale ale lui R cu proprietatea că $I_i + I_j = R$ pentru orice $i \neq j$, atunci acestea se numesc* comaximale în perechi.

Teorema 5.4 are următoarea generalizare:

Teorema 5.6. (Teorema chineză a resturilor) *Fie R un inel unitar, $I_1, \ldots, I_n$, $n \geq 2$ ideale bilaterale ale lui R şi $I = \bigcap_{i=1}^n I_i$. Definim*

$$f : R/I \to R/I_1 \times \cdots \times R/I_n$$

prin $f(x + I) = (x + I_1, \ldots, x + I_n)$.
(i) f este morfism injectiv de inele;
(ii) f este surjectiv dacă şi numai dacă $I_1, \ldots, I_n$ sunt comaximale în perechi.
În acest caz, f este izomorfism.

Proof. (ii) Se arată mai întâi că $I_1, \ldots, I_n$ sunt comaximale în perechi dacă şi numai dacă I_i şi $\bigcap_{j \neq i} I_j$ sunt comaximale, pentru orice $i = 1, \ldots, n$. $\square$

Remarca 5.7. Dacă R este inel comutativ şi unitar, iar $I_1, \ldots, I_n$ sunt ideale comaximale în perechi, atunci $\bigcap_{i=1}^n I_i = \prod_{i=1}^n I_i$.

Exerciţiul 5.8. Arătaţi că $\mathbb{Q}[X]/(X^2 - 1) \simeq \mathbb{Q} \times \mathbb{Q}$, dar $\mathbb{Z}[X]/(X^2 - 1) \not\simeq \mathbb{Z} \times \mathbb{Z}$.