

INELE

1. GENERALITĂȚI

Definiția 1.1. Se numește inel o mulțime nevidă R împreună cu două operații algebrice $(a, b) \mapsto a + b$ (numită adunare) și $(a, b) \mapsto ab$ (numită înmulțire) care satisfac următoarele proprietăți:

- 1) $(R, +)$ este grup comutativ;
- 2) $a(bc) = (ab)c$ pentru orice $a, b, c \in R$ (înmulțirea este asociativă);
- 3) $a(b + c) = ab + ac$ și $(b + c)a = ba + ca$ pentru orice $a, b, c \in R$ (înmulțirea este distributivă față de adunare la stânga și la dreapta);

Dacă, în plus,

- 4) $ab = ba$ pentru orice $a, b \in R$,

atunci R se numește inel comutativ.

Dacă inelul R are element neutru în raport cu operația de înmulțire, atunci se numește inel unitar.

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

Exemplul 1.2. Pe orice grup abelian netrivial $(G, +)$ se poate introduce o structură de inel (neunitar) definind înmulțirea astfel: $ab = 0$ pentru orice $a, b \in G$.

Exercițiul 1.3. (i) Să se determine numărul structurilor neizomorfe de inel care pot fi definite pe grupul $(\mathbb{Z}_p, +)$, unde p este un număr prim.

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

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

Exemplul 1.5. (i) $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ sunt inele comutative și unitare.

(ii) $(2\mathbb{Z}, +, \cdot)$ este inel comutativ, dar nu este unitar.

(iii) $(\mathbb{Z}_n, +, \cdot)$ este inel comutativ și unitar.

(iv) Fie G grup comutativ. Atunci $(\text{End}(G), +, \circ)$ este inel unitar și se numește inelul endomorfismelor lui G .

(v) Fie R un inel (unitar) și X o mulțime nevidă. Definim pe mulțimea R^X a funcțiilor $f : X \rightarrow R$ o structură de inel (unitar) astfel: dacă $f, g \in R^X$, atunci

$$(f + g)(x) = f(x) + g(x)$$

$$(fg)(x) = f(x)g(x)$$

pentru orice $x \in X$. Acesta se numește inelul funcțiilor definite pe X cu valori în R . Elementul nul al acestui inel este funcția $\mathbf{0} : X \rightarrow R$ definită prin $\mathbf{0}(x) = 0$ pentru orice $x \in X$ (elementul unitate este funcția $\mathbf{1} : X \rightarrow R$ 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) și se numește 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 și este matricea care are 1 pe diagonala principală și 0 în rest. În general, $M_n(R)$ nu este inel comutativ.

(vii) Fie R_1, R_2 inele și $R = R_1 \times R_2$. Atunci $(R, +, \cdot)$ este inel, unde

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

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

pentru orice $a_1, b_1 \in R_1, a_2, b_2 \in R_2$. Inelul R se numește *produsul direct* al inelelor R_1 și R_2 .

Să observăm că R este inel unitar (comutativ) dacă și numai dacă R_1 și R_2 sunt inele unitare (comutative).

Exercițiul 1.6. Să se arate că $(\mathbb{R}^{\mathbb{R}}, +, \circ)$ 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 $a, b \in R$.

Avem următoarele reguli de calcul într-un inel:

Propoziția 1.8. Fie R un inel. Atunci

- (i) $0a = a0 = 0$ pentru orice $a \in R$.
- (ii) $a(-b) = (-a)b = -(ab)$ și $(-a)(-b) = ab$ pentru orice $a, b \in R$.
- (iii) $(na)b = a(nb) = n(ab)$ pentru orice $n \in \mathbb{Z}$ și $a, b, c \in R$.
- (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

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

Definiția 1.9. Fie R un inel și $a \in R$. Atunci a se numește 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 și 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.

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.

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

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 $\hat{a} \in \mathbb{Z}_n$ 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 în $M_2(R)$.
(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 $\mathcal{C}(\mathbb{R}) = \{f : \mathbb{R} \rightarrow \mathbb{R} \mid f \text{ este continuă}\}$ 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.** Arătați că în inelul $M_n(\mathbb{R})$ orice element inversabil la stânga (dreapta) este inversabil la dreapta (stânga).

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

- 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. (În schimb există elemente inversabile la dreapta și care sunt divizori ai lui zero la stânga.)

- Exemplul 1.19.** (i) $U(\mathbb{Z}) = \{-1, 1\}$, $U(\mathbb{Q}) = \mathbb{Q} \setminus \{0\}$, $U(\mathbb{R}) = \mathbb{R} \setminus \{0\}$.
(ii) $U(\mathbb{Z}_n) = \{\hat{a} \in \mathbb{Z}_n : (a, n) = 1\}$.
(iii) $U(\text{End}(G)) = \text{Aut}(G)$.
(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.

Definiția 1.20. Fie R un inel și $x \in R$. Elementul x se numește 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.

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

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

- (i) Dacă $xy = yx$, atunci xy și $x + y$ sunt nilpotente.
- (ii) Dați exemple care să arate că proprietatea (i) nu mai rămâne adevărată dacă $xy \neq yx$.

Definiția 1.24. Fie R un inel și $x \in R$. Elementul x se numește idempotent dacă $x^2 = x$.

Remarca 1.25. (i) 0 și 1 sunt elemente idempotente. (Acestea se mai numesc și idempotenți triviali.)

(ii) Dacă R este inel unitar și $x \in R$ este idempotent, atunci $1 - x$ este idempotent.

(iii) Un inel integru nu are idempotenți netriviali.

Exemplul 1.26. Fie X o mulțime nevidă. În inelul \mathbb{Z}_2^X orice element este idempotent. (Un inel cu proprietatea că orice element al său este idempotent se numește inel boolean.)

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

Exercițiul 1.28. (i) 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 .

(ii) Să se determine idempotenții inelului \mathbb{Z}_{36} .

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

- (i) Să se determine numărul elementelor lui R ;
- (ii) Să se afle numărul divizorilor lui zero ai lui R ;
- (iii) Aflați câte elemente nilpotente are R ;
- (iv) Aflați câte elemente idempotente are R .

2. SUBINELE. IDEALE

Definiția 2.1. Fie $(R, +, \cdot)$ un inel și $S \subseteq R$ o submulțime nevidă. Atunci S se numește subinel al lui R dacă $(S, +, \cdot)$ este un inel. Dacă R este inel unitar și S un subinel cu proprietatea că $1 \in S$, atunci S se numește subinel unitar.

Propoziția 2.2. Fie R un inel și $S \subseteq R$ o submulțime nevidă. Atunci S este subinel al lui R dacă și numai dacă sunt satisfăcute următoarele condiții:

(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 $\{0\}$ și 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 totuși element unitate, pe $\widehat{5}$. (Mai general, dacă R este inel comutativ unitar și $e \in R$ 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.

Definiția 2.4. Fie R un inel și $I \subseteq R$ o submulțime nevidă. Atunci I se numește ideal la stânga (dreapta) al lui R dacă sunt satisfăcute următoarele condiții:

- (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 $a \in R$ și $x, y \in I$.

Un ideal la stânga și la dreapta al lui R se numește ideal bilateral al lui R .

Notății: $I \leq_s R$, $I \leq_d R$, respectiv $I \leq R$.

Remarca 2.5. (i) Fie R un inel comutativ și $I \subseteq R$ o submulțime nevidă. Atunci I este ideal la stânga al lui R dacă și numai dacă I este ideal la dreapta al lui R dacă și numai dacă I este ideal bilateral al lui R . În acest caz, I se numește ideal al lui R .

(ii) Evident, orice ideal este subinel, dar nu și reciproc: $\mathbb{Z} \subset \mathbb{Q}$ este subinel, dar nu este ideal.

(iii) Fie R inel unitar și $I \subseteq R$ un ideal la stânga (la dreapta, bilateral). Atunci $I = R$ dacă și numai dacă I conține un element inversabil.

Exemplul 2.6. (i) Dacă R este un inel, atunci $\{0\}$ și R sunt ideale bilaterale.

(ii) Idealele lui \mathbb{Z} sunt $n\mathbb{Z}$, $n \in \mathbb{N}$.

(iii) Idealele lui \mathbb{Z}_n sunt $\hat{d}\mathbb{Z}_n$, $d \mid n$.

(iv) Idealele lui \mathbb{Q} sunt $\{0\}$ și \mathbb{Q} . (Analog pentru \mathbb{R} .)

(v) Fie $R = M_2(\mathbb{Q})$ și

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

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

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

Exercițiul 2.7. Fie R_1, R_2 inele unitare și $R = R_1 \times R_2$. 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, R_2 , respectiv.

Exercițiul 2.8. Fie R un inel unitar.

(i) Să se arate că idealele bilaterale ale lui $M_2(R)$ sunt de forma $M_2(I)$, unde I este ideal bilateral al lui R .

(ii) Dați exemplu de ideal la stânga al lui $M_2(R)$ care nu este de forma $M_2(J)$, cu J ideal la stânga al lui R .

Lema 2.9. Fie R un inel și $I_\alpha \leq_s R$, $\alpha \in A$ 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.)

Definiția 2.10. Fie R un inel unitar și $X \subseteq R$ o submulțime. Notăm cu $(X)_s$ intersecția tuturor idealelor la stânga care conțin pe X . Acesta este un ideal la stânga al lui R și se numește idealul la stânga generat de X .

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

Remarca 2.11. Idealul la stânga (la dreapta, bilateral) generat de X este cel mai mic ideal la stânga (la dreapta, bilateral) care conține pe X .

Definiția 2.12. Fie R un inel unitar și $X \subseteq R$ o submulțime. Elementele lui X se numesc generatori pentru $(X)_s$.

Dacă $I \leq_s R$ și există $X \subseteq I$ o submulțime finită astfel încât $I = (X)_s$, atunci idealul I se numește finit generat. Dacă X are un singur element, atunci idealul I se numește principal.

Exemplul 2.13. Orice ideal al lui \mathbb{Z} (sau \mathbb{Z}_n) este principal.

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

Propoziția 2.14. Fie R un inel unitar și $X \subseteq R$ o submulțime. 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,

$$(x)_s = \{y \in R : y = ax, a \in R\},$$

$$(x)_d = \{y \in R : y = xa, a \in R\},$$

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

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

3. MORFISME DE INELE

Definiția 3.1. Fie R, R' inele și $f : R \rightarrow R'$ o funcție. Aceasta se numește 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 și $f(1) = 1'$, atunci f se numește morfism unitar.

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

Exemplul 3.3. (i) Funcția $f : R \rightarrow R'$ definită prin $f(x) = 0'$ pentru orice $x \in R$ este morfism de inele și se numește morfismul nul.

(ii) Incluziunea $i : \mathbb{Z} \rightarrow \mathbb{Q}$ definită prin $i(x) = x$ pentru orice $x \in \mathbb{Z}$ este morfism unitar și injectiv de inele.

(iii) Surjecția canonică $p : \mathbb{Z} \rightarrow \mathbb{Z}_n$ definită prin $p(x) = \hat{x}$ pentru orice $x \in \mathbb{Z}$ este

morfism unitar și surjectiv de inele.

(iv) Dacă R este un inel și $f : R \rightarrow M_n(R)$ se definește prin

$$f(a) = \begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & a & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & a \end{pmatrix},$$

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) și X o mulțime nevidă. Pentru orice $x \in X$ definim un morfism de inele (unitare) $\varphi_x : R^X \rightarrow R$ prin $\varphi_x(f) = f(x)$. Acesta se numește *morfismul de evaluare în x* .

Propoziția 3.4. *Fie $f : R \rightarrow R'$ și $g : R' \rightarrow R''$ morfisme (unitare) de inele. Atunci $g \circ f : R \rightarrow R''$ este morfism (unitar) de inele.*

Definiția 3.5. *Fie $f : R \rightarrow R'$ un morfism de inele. Atunci f se numește izomorfism de inele dacă există $g : R' \rightarrow R$ morfism de inele cu proprietatea că $f \circ g = 1_{R'}$ și $g \circ f = 1_R$.*

Notăție: $R \simeq R'$.

Propoziția 3.6. *Fie $f : R \rightarrow R'$ un morfism de inele. Atunci f este izomorfism dacă și numai dacă f este bijecție.*

Definiția 3.7. *Fie R un inel și $f : R \rightarrow R$ un morfism de inele. Atunci f se numește endomorfism al lui R . Dacă, în plus, f este bijectiv, atunci se va numi automorfism al lui R .*

Exercițiul 3.8. Arătați că orice inel boolean finit nenul este izomorf cu \mathbb{Z}_2^n pentru un $n \in \mathbb{N}^*$.

Exercițiul 3.9. Arătați că avem următoarele izomorfisme de inele:

$\text{End}((\mathbb{Z}, +)) \simeq \mathbb{Z}$, $\text{End}((\mathbb{Q}, +)) \simeq \mathbb{Q}$, $\text{End}((\mathbb{Z}/n\mathbb{Z}, +)) \simeq \mathbb{Z}/n\mathbb{Z}$, $\text{End}((\mathbb{Z} \times \mathbb{Z}, +)) \simeq M_2(\mathbb{Z})$. Pe de altă parte, $\text{End}((\mathbb{R}, +)) \not\simeq \mathbb{R}$.

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

Exercițiul 3.11. Fie $m, n \geq 2$.

(i) Arătați că există un morfism de inele unitare $\mathbb{Z}_m \rightarrow \mathbb{Z}_n$ dacă și numai dacă $n \mid m$.

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

(iii) Să se determine toate morfismele de inele de la \mathbb{Z}_{12} la \mathbb{Z}_{28} .

Propoziția 3.12. *Fie $f : R \rightarrow R'$ 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 3.13. Imaginea unui ideal printr-un morfism nu este neapărat un ideal. De exemplu, imaginea lui $2\mathbb{Z}$ prin morfismul incluziune $i : \mathbb{Z} \rightarrow \mathbb{Q}$ nu este ideal.

Definiția 3.14. Fie $f : R \rightarrow R'$ un morfism de inele. Atunci $\text{Im } f \subseteq R'$ este un subinel numit imaginea lui f , iar $\text{Ker } f = f^{-1}(0)$ 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 $\text{Ker } f = \{0\}$.

Teorema 3.15. (Teorema de corespondență pentru ideale) Fie $f : R \rightarrow R'$ un morfism surjectiv de inele. Există o corespondență bijectivă între mulțimea idealelor la stânga (la dreapta, bilaterale) ale lui R care conțin pe $\text{Ker } f$ 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 $p : R \rightarrow R/I$ 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 $p : R \rightarrow R/\{0\}$ este izomorfism de inele.

Propoziția 4.3. Fie R un inel și $I \subseteq R$ un ideal bilateral. Există o corespondență bijectivă între mulțimea idealelor la stânga (la dreapta, bilaterale) ale lui R care conțin pe I și mulțimea 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 $f : R \rightarrow R'$ un morfism de inele și I un ideal bilateral al lui R . Dacă $I \subseteq \text{Ker } f$, atunci există un morfism de inele $\bar{f} : R/I \rightarrow R'$ unic cu proprietatea că $\bar{f} \circ p = f$, unde $p : R \rightarrow R/I$ este proiecția canonică. Mai mult:

- 1) \bar{f} este injectiv dacă și numai dacă $I = \text{Ker } f$;
- 2) \bar{f} este surjectiv dacă și numai dacă \bar{f} este surjectiv.

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

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

$$\bar{f} : R/\text{Ker } f \rightarrow \text{Im } f.$$

Corolarul 4.7. Fie R un inel și I, J ideale bilaterale ale lui R cu $J \subseteq I$. Atunci I/J este ideal bilateral al lui R/J și

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

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.

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.

5. TEOREMA CHINEZĂ A RESTURILOR PENTRU IDEALE

Fie $n_1, n_2 \geq 2$ două numere întregi prime între ele. Funcția $f : \mathbb{Z}/(n_1 n_2)\mathbb{Z} \rightarrow \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ definită prin $f(\hat{x}) = (\bar{x}, \bar{x})$ este un izomorfism de inele. Se observă că dacă notăm $I_1 = n_1\mathbb{Z}$ și $I_2 = n_2\mathbb{Z}$, atunci $I_1 + I_2 = \mathbb{Z}$ și $I_1 I_2 = I_1 \cap I_2$. Aceasta ne sugerează următoarea generalizare:

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

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

Teorema 5.3. Fie R un inel și I_1, I_2 ideale comaximale ale lui R . Atunci morfismul

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

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

Proof. Se arată mai întâi că f este bine definit, iar apoi se arată că $(\bar{r}, \bar{0})$ și $(\bar{0}, \bar{s})$ sunt în imaginea lui f pentru orice $r, s \in R$: deoarece $I_1 + I_2 = R$ există $x_1 \in I_1$ și $x_2 \in I_2$ astfel încât $x_1 + x_2 = r$, respectiv există $y_1 \in I_1$ și $y_2 \in I_2$ astfel încât $y_1 + y_2 = s$. Atunci $f(\hat{x}_2) = (\bar{r}, \bar{0})$ și $f(\hat{y}_1) = (\bar{0}, \bar{s})$. De aici se obține $f(\widehat{x_2 + y_1}) = (\bar{r}, \bar{s})$, deci f este surjectiv. \square

Exercițiul 5.4. Arătați că $\mathbb{Q}[X]/(X^2 - 1) \simeq \mathbb{Q} \times \mathbb{Q}$, $\mathbb{Z}[X]/(X^2 - X) \simeq \mathbb{Z} \times \mathbb{Z}$, dar $\mathbb{Z}[X]/(X^2 - 1) \not\simeq \mathbb{Z} \times \mathbb{Z}$.