I. Recapitulare: Inele, ideale, morfisme, inele factor

I.1. Inele, subinele, ideale, morfisme, inele factor

Acest capitol conţine noţiuni şi rezultate parcurse în cadrul cursului de Structuri algebrice fundamentale. Este posibil ca unele notaţii sau terminologii să difere uşor faţă de cele folosite la acel curs. Chiar dacă sînteţi siguri că ştiţi noţiunile din acest capitol, o parcurgere rapidă a acestuia este obligatorie, pentru reamintire şi acomodarea cu notaţiile şi convenţiile din cursul prezent.

Un test al înţelegerii noţiunilor este rezolvarea tuturor exerciţiilor!

Simbolul □ marchează sfîrşitul unei demonstraţii (sau absenţa ei, caz în care ar trebui să faceţi voi o demonstraţie!).

1.1 Definiţie. Se numeşte *inel* o mulţime nevidă R înzestrată cu două operaţii, *adunarea* (notată cu $+$) şi *înmulţirea* (notată cu $\cdot$ sau doar prin juxtapunere), care are următoarele proprietăţi:[1]

a) $(R, +)$ este *grup comutativ*, adică:

- Adunarea este *asociativă*: $\forall x, y, z \in R, (x + y) + z = x + (y + z)$
- Există element *zero*: $\exists 0 \in R$ astfel încît: $\forall x \in R, x + 0 = 0 + x = x$
- Orice element din R are un *opus*: $\forall x \in R, \exists(-x) \in R$ astfel încît $x + (-x) = (-x) + x = 0$
- Adunarea este *comutativă*: $\forall x, y \in R, x + y = y + x$

b) $(R, \cdot)$ este *monoid*, adică:

- Înmulţirea este *asociativă*: $\forall x, y, z \in R, (x \cdot y) \cdot z = x \cdot (y \cdot z)$
- Există element *unitate*: $\exists 1 \in R$ astfel încît: $\forall x \in R, x \cdot 1 = 1 \cdot x = x$ (adică toate inelele sînt considerate *unitare*).

[1] Dacă vrem să fim pedanţi, se numeşte inel *tripletul* $(R, +, \cdot)$.

c) Înmulţirea este *distributivă la stînga şi la dreapta faţă de adunare*: $\forall x, y, z \in R$, $z\cdot(x+y) = z\cdot x + z\cdot y$ şi $(x+y)\cdot z = x\cdot z + y\cdot z$.

Dacă *înmulţirea este comutativă* ($\forall x, y \in R$, $xy = yx$), inelul se numeşte *comutativ*.

Din definiţie rezultă (*demonstraţi!*) că:

1. *Elementele* 0 *şi* 1 *sînt unic determinate* (căci elementul neutru într-un monoid este unic). *Opusul lui x faţă de adunare*, $-x$, *este unic determinat de x*.
2. $\forall x \in R$, $x\cdot 0 = 0\cdot x = 0$.
3. $\forall x, y \in R$, $(-x)\cdot y = x\cdot(-y) = -(xy)$.
4. *Dacă presupunem că* $1 = 0$*, atunci orice element din R este* 0.

1.2 Notaţii. a) $\forall x, y \in R$, $x - y$ notează elementul $x + (-y)$.

b) $\forall x \in R$, $\forall n \in \mathbb{N}$, se defineşte, recursiv după n, *multiplul* nx al lui x prin:

$$0\cdot x = 0;\ n\cdot x = (n-1)\cdot x + x, \text{ dacă } n > 0.$$

Dacă $n \in \mathbb{Z}$, $n < 0$, atunci $-n > 0$ şi definim $n\cdot x = (-n)(-x)$ aplicînd definiţia de mai sus.

Se demonstrează[2] că:

$$\forall m, n \in \mathbb{Z}, \forall x, y \in R, \text{ are loc } (m+n)\cdot x = mx + nx \text{ şi } n\cdot(x+y) = nx + ny.$$

Ar trebui să fiţi capabili să daţi cel puţin 5 *exemple de inele, comutative şi necomutative.*

În continuare, toate inelele considerate sînt unitare şi comutative (dacă nu se specifică altfel), cu $1 \neq 0$.

1.3 Definiţie. a) Fie R un inel şi $x \in R$. Spunem că x este *divizor al lui zero* dacă există $y \in R$, $y \neq 0$, astfel încît $xy = 0$. Un inel unitar, comutativ, fără divizori ai lui 0 diferiţi de 0, se numeşte *inel integru* sau *domeniu de integritate.*

b) Un inel R în care orice element nenul x este *inversabil* (adică $\exists y \in R$ astfel încît $xy = yx = 1$) se numeşte *corp*. Demonstraţi:

Dacă inelul R este corp, atunci $R \setminus \{0\}$ *este grup faţă de înmulţirea inelului (şi reciproc).*

Orice corp este inel integru.

1.4 Exemple. a) Cel mai important exemplu de inel este *inelul* $\mathbb{Z}$ *al numerelor întregi*, înzestrat cu operaţiile uzuale. *Acesta este primul exemplu de inel care trebuie să vă vină in minte cînd auziţi „Fie R un inel”*. $\mathbb{Z}$ este inel comutativ, integru. $\mathbb{Z}$ nu este corp (*de ce?*).

[2] Aceste proprietăţi au fost date deja în cursul de Structuri algebrice fundamentale pentru puterile unui element dintr-un grup; de obicei se dau in notaţie multiplicativă. Este util să le demonstraţi şi în notaţie aditivă.

b) Mulţimea numerelor raţionale $\mathbb{Q}$, înzestrată cu operaţiile uzuale, este corp. Din acest motiv, $\mathbb{Q}$ se numeşte *corpul numerelor raţionale.* Tot corpuri sînt şi $\mathbb{R}$ (*corpul numerelor reale*) şi $\mathbb{C}$ (*corpul numerelor complexe*).

c) Dacă $(R, +, \cdot)$ şi $(S, +, \cdot)$ sînt inele[3], atunci produsul cartezian $R\times S$ se dotează cu două operaţii astfel încît să devină inel, numit *inelul produs direct al inelelor R* şi *S*, astfel:

$\forall (r, s), (r', s') \in R\times S, \qquad (r, s) + (r', s') := (r + r', s + s'); \qquad (r, s)\cdot(r', s') := (rr', ss')$

Demonstraţi că $R\times S$ este inel şi că nu este integru. Generalizaţi construcţia la n inele $R_1, R_2, \ldots, R_n$. (Se obţine un inel notat $R_1\times R_2\times \ldots\times R_n$, numit produsul direct al inelelor $R_1, R_2, \ldots, R_n$.)

1.5 Definiţie. Fie R un inel şi S o submulţime nevidă a sa. Spunem că S este *subinel* în R dacă:

- S este parte stabilă în R faţă de adunare şi înmulţire: $\forall s, t \in S,$ au loc $s + t \in S$ şi $st \in S$;
- S devine inel în raport cu operaţiile induse.

Un subinel al lui R se numeşte *subinel unitar* dacă 1 (unitatea lui R) este în S.

1.6 Exerciţiu. a) Este $\mathbb{N}$ subinel al lui $\mathbb{Z}$? De ce?

b) S este subinel al inelului $R \Leftrightarrow \forall s, t \in S,$ au loc $s - t \in S$ şi $st \in S$.

c) Daţi 3 exemple de subinele ale lui $\mathbb{Z}$.

d) Singurul subinel unitar al lui $\mathbb{Z}$ este $\mathbb{Z}$.

e) Daţi 3 exemple de subinele unitare ale lui $\mathbb{Q}$.

f) Daţi exemplu de 2 subinele unitare ale lui $\mathbb{R}$, care includ $\mathbb{Z}$.

g) Orice subinel al lui $\mathbb{C}$ care include strict pe $\mathbb{R}$ coincide cu $\mathbb{C}$.

h) Este posibil ca S să fie subinel al lui R, S să aibă unitate, dar S să nu fie subinel unitar al lui R? (Ind. Uitaţi-vă la $\mathbb{Z}\times\mathbb{Z}$.)

1.7 Propoziţie. *Fie R un inel şi $(S_i)_{i\in I}$ o familie oarecare de subinele (unitare) ale sale. Atunci $\bigcap_{i\in I} S_i$ este subinel (unitar) în R.* □

1.8 Definiţie. Fie A o submulţime nevidă a inelului R. Se numeşte *subinel (unitar) al lui R generat de A* intersecţia tuturor subinelelor (unitare) ale lui R care includ A. Propoziţia precedentă asigură că această intersecţie este într-adevăr subinel (unitar).

În continuare, toate subinelele considerate sînt unitare.

[3] Adunarea în R am notat-o cu acelaşi simbol, +, la fel ca adunarea în S (deşi sînt obiecte diferite!). Astfel de "abuzuri de notaţie" sînt frecvente în matematică şi trebuie conştientizate şi identificate. Am mai facut un astfel de abuz, mai devreme. Unde?

1.9 Observaţie. *Subinelul lui R generat de A este cel mai mic (in raport cu incluziunea) subinel al lui R care include pe A. Mai precis, T este subinelul generat de A dacă şi numai dacă T satisface condiţiile:*

- T este subinel, $T \supseteq A$;

- $\forall S$ subinel, $S \supseteq A$ implică *$S \supseteq T$.*

În practică, subinelul generat de o submulţime se determină cu ajutorul propoziţiei următoare:

1.10 Propoziţie. (Subinelul generat de o submulţime) *Fie R un inel, S un subinel al său şi $A = \{a_1, \ldots, a_n\}$ o submulţime finită a lui R. Subinelul generat de $S \cup A$ în R se notează $S[A]$ şi este format din combinaţiile liniare cu coeficienţi din S de produse finite de elemente din A,*

$$S[A] = \left\{ \sum\nolimits'_{(i_1,\ldots,i_n)\in\mathbb{N}^n} s_{i_1,\ldots,i_n} a_1^{i_1} \ldots a_n^{i_n} \,\middle|\, s_{i_1,\ldots,i_n} \in S, a_1, \ldots a_n \in A, \forall (i_1,\ldots,i_n) \in \mathbb{N}^n \right\}.$$

Notaţia $\sum'$ semnifică faptul că este vorba de o sumă finită, adică doar un număr finit dintre $s_{i_1,\ldots,i_n}$ sînt nenuli. □

1.11 Exerciţii. a) Subinelul generat de $\mathbb{Z}$ şi $\frac{1}{2}$ în $\mathbb{Q}$ este $\mathbb{Z}\left[\frac{1}{2}\right] = \left\{ \frac{a}{2^n} \,\middle|\, a \in \mathbb{Z}, n \in \mathbb{N} \right\}$.

Demonstraţie: Se verifică mai întîi că orice subinel care include $\mathbb{Z}$ şi $\frac{1}{2}$ conţine şi $\frac{a}{2^n}$, $\forall a \in \mathbb{Z}$, $\forall n \in \mathbb{N}$. Apoi se arată că mulţimea $\left\{ \frac{a}{2^n} \,\middle|\, a \in \mathbb{Z}, n \in \mathbb{N} \right\}$ este parte stabilă la scădere şi înmulţire.

b) Determinaţi subinelul $\mathbb{Z}\left[\frac{1}{10}\right]$.

c) Subinelul generat de $\mathbb{Z}$ şi $i = \sqrt{-1}$ în $\mathbb{C}$ este $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$.

d) Determinaţi $\mathbb{Z}\left[\sqrt[3]{2}\right]$, subinelul generat de $\mathbb{Z}$ şi $\sqrt[3]{2}$ în $\mathbb{C}$.

e) Determinaţi $\mathbb{Z}\left[\sqrt{2}, \sqrt{3}\right]$, subinelul generat de $\mathbb{Z}$ şi $\left\{\sqrt{2}, \sqrt{3}\right\}$ în $\mathbb{C}$.

1.12 Definiţie. Fie *R* şi *S* două inele. Se numeşte *morfism de inele de la R la S* o funcţie $\varphi : R \to S$ astfel încît,

$$\forall x, y \in R,\ \varphi(x + y) = \varphi(x) + \varphi(y);\ \varphi(xy) = \varphi(x)\varphi(y).$$

Dacă, în plus, φ satisface condiţia $\varphi(1) = 1$ (φ duce unitatea lui *R* în unitatea lui *S*), φ se numeşte *morfism unitar de inele*.

În continuare, toate morfismele de inele vor fi considerate unitare.

Un morfism de inele care este bijectiv se numeşte *izomorfism de inele.* Inelele *R* şi *S* se numesc *izomorfe* (notat $R \cong S$) dacă există un izomorfism $\varphi : R \to S$. Relaţia de izomorfism (pe clasa inelelor) este reflexivă, tranzitivă, simetrică (relaţie de echivalenţă). *Demonstraţi!*

Ca şi la alte structuri, două inele izomorfe au „aceleaşi proprietăţi de inel". De exemplu, dacă $R \cong S$ şi R este integru, atunci S este integru (*demonstraţi!*). *Puteţi da alt exemplu?*

1.13 Propoziţie. *a) Fie* $\varphi : R \to S$ *şi* $\psi : S \to T$ *morfisme de inele. Atunci* $\psi \circ \varphi$ *este morfism de inele.*

b) Dacă $\varphi : R \to S$ *este morfism de inele şi B este subinel în R, atunci imaginea lui B în S,* $\varphi(B)$*, este subinel în S.* □

1.14 Definiţie. Fie R un inel. Se numeşte *ideal* în R o submulţime nevidă I a lui R cu proprietăţile:

- $\forall i, j \in I$, rezultă $i + j \in I$ (*I este parte stabilă la adunare*);
- $\forall i \in I$, $\forall r \in R$ rezultă $ri \in I$ (*I este stabilă la înmulţirea cu orice element din R*).

Se demonstrează uşor (faceţi-o!) că: *orice ideal I este subgrup al grupului* $(R, +)$. În consecinţă, *orice ideal conţine elementul* 0.

Notaţie: Faptul că I este ideal în R se notează $I \leq R$ sau $I \leq {}_R R$.

Idealul I se numeşte *propriu* dacă $I \neq R$.

1.15 Exemplu. Mulţimea $2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\}$ este ideal în $\mathbb{Z}$. Demonstraţi! Idealele lui $\mathbb{Z}$ sînt $n\mathbb{Z}$, $n \in \mathbb{N}$ (unde $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$, mulţimea multiplilor lui n).

La fel ca la subinele, intersecţia unei familii de ideale este tot ideal:

1.16 Propoziţie. *Fie R un inel şi* $(A_i)_{i \in I}$ *o familie oarecare de ideale ale sale. Atunci* $\bigcap_{i \in I} A_i$ *este ideal în R.* □

1.17 Definiţie. Fie A o submulţime nevidă a inelului R. Se numeşte *ideal generat de A* intersecţia tuturor idealelor lui R care includ pe A. Propoziţia precedentă asigură că această intersecţie este într-adevăr ideal. Idealul generat de A este cel mai mic (în sensul incluziunii) ideal al lui R care include pe A.

1.18 Propoziţie. (Idealul generat de o submulţime) *Fie R un inel, şi* $A = \{a_1, \ldots, a_n\}$ *o submulţime finită a lui R. Idealul generat de A în R se notează*[4] ${}_R\langle A \rangle$ *sau* ${}_R(a_1, \ldots, a_n)$ *şi este format din combinaţiile liniare cu coeficienţi în R de elemente din A,* $\langle A \rangle = \left\{ \sum_{i=1}^{n} r_i a_i \mid r_i \in R, \forall i \in \mathbb{N} \right\}$*. Dacă* $A = \{a\}$*, idealul generat de* $\{a\}$ *se notează Ra sau aR sau* (a) *şi are loc* $Ra = \{ra \mid r \in R\}$. □

[4] Se omite R din notaţie dacă este clar din context.

1.19 Exemplu. Fie $\mathbb{Q}[X]$ inelul polinoamelor în nedeterminata X cu coeficienţi în $\mathbb{Q}$. Idealul generat de polinomul X este $(X) = \{Xg \mid g \in \mathbb{Q}[X]\}$.

1.20 Definiţie. Fie $\varphi : R \to S$ un morfism de inele. Definim *nucleul lui f,* $\operatorname{Ker} f := \{r \in R \mid f(r) = 0\}$. Demonstraţi că $\operatorname{Ker} f$ este ideal în R.

Mai general, contraimaginea unui ideal printr-un morfism este tot ideal:

1.21 Propoziţie. *a) Fie $\varphi : R \to S$ un morfism de inele şi $J \leq S$. Atunci $\varphi^{-1}(J) \leq R$.*
b) Dacă φ este surjectiv şi $I \leq R$, atunci $\varphi(I) \leq S$. □

1.22 Definiţie. a) Fie I, J ideale în inelul R. Idealul generat de $I \cup J$ se numeşte *suma idealelor I şi J* şi se notează $I + J$.

b) Mai general, dacă $(A_i)_{i \in I}$ este o familie oarecare de ideale ale lui R, atunci idealul generat de $\bigcup_{i \in I} A_i$ se numeşte *suma idealelor* $(A_i)_{i \in I}$ şi se notează $\sum_{i \in I} A_i$.

1.23 Propoziţie. *a) Fie R un inel şi I, J ideale în R. Atunci $I + J = \{i + j \mid i \in I, j \in J\}$.*
b) Fie $A_1, \ldots, A_n$ ideale în R. Atunci $A_1 + \ldots + A_n = \{a_1 + \ldots + a_n \mid a_1 \in A_1, \ldots, a_n \in A_n\}$.
c) Fie $(A_i)_{i \in I}$ o familie oarecare de ideale în R. Atunci

$$\sum_{i \in I} A_i = \left\{ \sum_{i \in I} a_i \mid a_i \in A_i, \forall i \in I, \operatorname{supp}((a_i)_{i \in I}) \text{ finit} \right\}$$

(Am notat cu $\operatorname{supp}((a_i)_{i \in I})$ *suportul familiei* de elemente $(a_i)_{i \in I}$, adică $\{i \in I \mid a_i \neq 0\}$.) □

Mulţimea idealelor unui inel R, notată $\mathcal{L}(R)$, este mulţime ordonată faţă de incluziune; mai mult, este o *latice*: pentru orice două ideale I şi J ale lui R, există $\inf\{I, J\} = I \cap J$, $\sup\{I, J\} = I + J$.

I.2. Inele factor şi teoremele de izomorfism

Prezentăm mai întîi, pe scurt, etapele *construcţiei inelului de clase de resturi modulo n*, $\mathbb{Z}_n$. Apoi vom da construcţia generală a inelului factor al unui inel R în raport cu un ideal I al său. Inelele factor intervin în multe alte construcţii importante în matematică: corpurile $\mathbb{R}$ şi $\mathbb{C}$, corpurile finite.

Fie n un număr întreg, fixat (numit *modùl*).

2.1 Definiţie. Spunem că numerele întregi a şi b sînt *congruente modulo n* dacă n divide $a - b$. Scriem aceasta sub forma $a \equiv b \pmod{n}$.

2.2 Propoziţie. *Relaţia „* $\equiv \pmod n$*” de congruenţă modulo n este o relaţie de echivalenţă pe* $\mathbb{Z}$*.* □

Pentru orice $a \in \mathbb{Z}$, se notează cu $\widehat{a}$ clasa lui a în raport cu relaţia de congruenţă modulo n. Avem deci:

$$\widehat{a} = \{b \in \mathbb{Z} \mid a \equiv b \pmod n\}.$$

Observăm că notaţia este ambiguă, în sensul că nu precizează modulul (numărul n); este deci necesară atenţie şi notaţii adecvate pentru evitarea confuziilor ce pot apărea în cazul folosirii mai multor relaţii de congruenţă.

Mulţimea factor $\mathbb{Z}/\equiv \pmod n$ (adică $\{\widehat{a} \mid a \in \mathbb{Z}\}$) se notează cu $\mathbb{Z}_n$ şi se numeşte *mulţimea claselor de resturi modulo n*.

2.3 Exerciţiu. a) Două numere întregi a şi b sînt congruente modulo n dacă şi numai dacă „dau acelaşi rest la împărţirea cu n”.

b) Clasa de congruenţă a lui 0 modulo 3 este $\widehat{0} = \{3k \mid k \in \mathbb{Z}\}$(notată cu $3\mathbb{Z}$). Clasa de congruenţă a lui 1 modulo 3 este $\widehat{1} = \{1 + 3k \mid k \in \mathbb{Z}\}$(notată cu $1 + 3\mathbb{Z}$). Determinaţi clasa lui 2 modulo 3. Observaţi că clasele modulo 3 sînt disjuncte două cîte două şi reuniunea tuturor claselor este egală cu $\mathbb{Z}$. Este valabilă această afirmaţie pentru orice modul? De ce?

c) Ce devine relaţia de congruenţă modulo n, care sînt clasele modulo n şi care este mulţimea $\mathbb{Z}_n$ dacă $n = 0$ sau $n = 1$?

Pe $\mathbb{Z}_n$ se pot defini două operaţii (numite *adunarea*, respectiv *înmulţirea modulo n*), în raport cu care $\mathbb{Z}_n$ devine *inel comutativ şi unitar*. Pentru orice $a, b \in \mathbb{Z}$, definim:

$$\widehat{a} + \widehat{b} := \widehat{a + b}$$
$$\widehat{a} \cdot \widehat{b} := \widehat{a \cdot b}$$

Demonstrarea corectitudinii definiţiilor de mai sus (adică independenţa de alegerea reprezentanţilor) şi a axiomelor inelului este propusă cititorului.

Vom aplica ideea construcţiei de mai sus într-o situaţie mai generală. În acest scop, observăm că putem defini relaţia de congruenţă modulo n pe $\mathbb{Z}$ şi în felul următor:

Notăm $n\mathbb{Z} := \{nk \mid k \in \mathbb{Z}\}$. Avem atunci, $\forall a, b \in \mathbb{Z}$:

$$a \equiv b \pmod n \Leftrightarrow a - b \in n\mathbb{Z}.$$

Mai mult, se vede imediat că $\widehat{a} = \{a + nk \mid k \in \mathbb{Z}\}$, motiv pentru care $\widehat{a}$ se mai notează cu $a + n\mathbb{Z}$. Deci, $\widehat{0} = n\mathbb{Z}$, $\widehat{1} = 1 + n\mathbb{Z}$ etc.

Mulţimea $n\mathbb{Z}$ este *ideal în* $\mathbb{Z}$, în sensul că este parte stabilă la adunare şi, $\forall x \in \mathbb{Z}$, $\forall a \in n\mathbb{Z}$, rezultă că $xa \in n\mathbb{Z}$ ($\mathbb{Z}$ este parte stabilă la înmulţirea cu *orice* element din $\mathbb{Z}$).

Se observă imediat că orice ideal I al lui R este subgrup al grupului aditiv $(R, +)$ (demonstraţi!) şi deci $0 \in I$.

Propoziţia următoare arată că ideea de construcţie a lui $\mathbb{Z}_n$ pornind de la $\mathbb{Z}$ şi un ideal al său (de forma $n\mathbb{Z}$) se generalizează cuvînt cu cuvînt la cazul unui inel R şi al unui ideal I al său.[5] Demonstraţia constă în verificarea directă a proprietăţilor enunţate şi o lăsăm cititorului (şi poate fi găsită în orice carte introductivă de algebră „modernă").

2.4 Propoziţie. *Fie R un inel comutativ unitar şi I un ideal al său.*

a) Relaţia (*de* congruenţă modulo I)*, definită de:*

$$a \equiv b \pmod{I} \Leftrightarrow a - b \in I$$

este o relaţie de echivalenţă pe I. Notînd cu $\widehat{a} = \{b \in R \mid a \equiv b \pmod{I}\}$ (*numită* clasa lui a modulo I)*, are loc* $\widehat{a} = \{a + x \mid x \in I\}$ ($\widehat{a}$ *se mai notează* $a + I$ *din acest motiv*).

b) Relaţia de congruenţă modulo I este compatibilă cu adunarea şi înmulţirea din R, *în sensul că,* $\forall a, a', b, b' \in R$, *au loc implicaţiile:*

$$a \equiv a' \pmod{I} \text{ şi } b \equiv b' \pmod{I} \Rightarrow a + b \equiv a' + b' \pmod{I} \text{ şi } a \cdot b \equiv a' \cdot b' \pmod{I}.$$

c) Operaţiile pe mulţimea factor $R/I := \{\widehat{a} \mid a \in R\}$, *date de:*

$$\widehat{a} + \widehat{b} := \widehat{a + b} \text{ şi } \widehat{a} \cdot \widehat{b} \equiv \widehat{a \cdot b}, \forall a, b \in R,$$

sînt corect definite şi înzestrează pe R/I *cu o structură de inel comutativ unitar* (*numit* inelul factor al lui R în raport cu I).

d) Aplicaţia $\pi : R \to R/I$, $\pi(r) = \widehat{r} = r + I$, $\forall r \in R$, *este un morfism surjectiv de inele* (*numit* surjecţia canonică a inelului factor R/I). □

În termeni mai puţin riguroşi, trecerea de la inelul R la inelul factor R/I „duce toate elementele din I în zero" sau „anulează elementele lui I". Multe afirmaţii referitoare la idealul I în R se traduc prin afirmaţii referitoare la idealul 0 în R/I (un exemplu este **2.8**), idee aplicată adesea în raţionamente.

2.5 Exerciţiu. Fie $(X^2 + 1)$ idealul generat de polinomul $X^2 + 1$ în $\mathbb{R}[X]$. Urmaţi etapele construcţiei de mai sus pentru a construi inelul factor $\mathbb{R}[X]/(X^2 + 1)$. Demonstraţi că $\mathbb{R}[X]/(X^2 + 1) \cong \mathbb{C}$.

Este de aşteptat ca un rol esenţial în ce priveşte proprietăţile inelului factor R/I să îl aibă idealul I. În acest sens, sînt importante următoarele noţiuni:

2.6 Definiţie. Fie R un inel comutativ. Un ideal P al lui R se numeşte *ideal prim* dacă $P \neq R$ şi oricare ar fi $x, y \in P$, din $xy \in P$ rezultă $x \in P$ sau $y \in P$. Un ideal M al lui R se numeşte *ideal maximal* dacă $M \neq R$ şi nu există ideale proprii ale lui R care includ strict pe M: pentru orice $J \leq R$, din $M \leq J$ rezultă $M = J$ sau $J = R$.

[5] Afirmaţiile rămîn valabile pentru un inel nu neapărat comutativ R şi un ideal *bilateral* I al lui R.

2.7 Exemple. *a)* Dacă p este un număr întreg prim, atunci idealul generat de p în $\mathbb{Z}$, notat $p\mathbb{Z}$, este ideal prim în $\mathbb{Z}$. Reciproc, dacă $p\mathbb{Z}$ este ideal prim, atunci p este număr prim.

b) Un ideal I este maximal în inelul R dacă este element maximal al mulţimii ordonate (cu incluziunea) a idealelor proprii ale lui R. În inelul $\mathbb{Z}$, orice ideal este de forma $n\mathbb{Z}$, cu $n \in \mathbb{Z}$. De aici rezultă că idealul $n\mathbb{Z}$ este maximal dacă şi numai dacă n este număr prim. Într-adevăr, fie $n\mathbb{Z}$ ideal maximal. Atunci, $\forall m \in \mathbb{Z}$, din $n\mathbb{Z} \subseteq m\mathbb{Z}$ rezultă $n\mathbb{Z} = m\mathbb{Z}$ sau $m\mathbb{Z} = \mathbb{Z}$; cu alte cuvinte, din $m|n$ rezultă $m \sim n$ sau $m = 1$. Ştiind în plus că $n\mathbb{Z} \neq \mathbb{Z}$, aceasta înseamnă că n este ireductibil, deci prim. Reciproca se obţine în acelaşi mod.

c) Inelul R este integru dacă şi numai dacă (0) este ideal prim.

d) Dacă K este corp, (0) este singurul său ideal propriu; (0) este şi ideal maximal şi ideal prim.

O caracterizare utilă a idealelor maximale (respectiv prime), des folosită în aplicaţii, este dată cu ajutorul inelului factor.

2.8 Teoremă. *Fie R un inel comutativ şi I un ideal propriu în R.*

a) I este ideal prim dacă şi numai dacă inelul factor R/I este integru.

b) I este ideal maximal dacă şi numai dacă inelul factor R/I este corp.

Demonstraţie. *a)* Fie I un ideal prim. Fie $\alpha = a + I$, $\beta = b + I$ (cu $a, b \in R$) elemente din R/I. Dacă $\alpha\beta = 0$, atunci $(a + I)(b + I) = 0 + I$, adică $ab \in I$. Cum I este prim, obţinem $a \in I$ sau $b \in I$, adică $a + I = \alpha = 0 + I$ sau $b + I = \beta = 0 + I$. Aşadar, R/I este integru. Reciproc, presupunem că R/I este integru şi fie a, $b \in R$ cu $ab \in I$. Aceasta înseamnă că $(a + I)(b + I) = 0 + I$, deci $a + I = 0 + I$ sau $b + I = 0 + I$. Astfel, $a \in I$ sau $b \in I$.

b) Presupunem că I este ideal maximal în R. Vrem să arătăm că orice element nenul al inelului R/I este inversabil. Fie deci $\alpha = a + I$, cu $\alpha \neq 0 + I$, deci $a \notin I$. Atunci idealul generat de I şi a, adică $I + Ra$, include strict pe I; din maximalitatea lui I obţinem $I + Ra = R$. În particular, $1 \in R$ se scrie sub forma $i + ra$, cu $i \in I$ şi $r \in R$. Avem deci $1 + I = (ra + i) + I = ra + I = (r + I)(a + I)$, ceea ce arată că $a + I$ este inversabil. Fie acum R/I corp şi J un ideal care include strict pe I. Există aşadar $x \in J$, $x \notin I$. Aceasta înseamnă că $x + I \neq 0 + I$, deci $x + I$ este inversabil. Putem scrie atunci $1 + I = (r + I)(x + I)$, cu $r \in R$, adică există $i \in I$ astfel încît $1 = rx + i$. De aici rezultă că $1 \in J$, adică $J = R$. □

2.9 Corolar. *Orice ideal maximal în inelul R este prim.* □

Reciproca acestui rezultat este falsă: idealul (X) al inelului $\mathbb{Z}[X]$ este prim şi nu este maximal, după cum se vede considerînd inelul factor: $\mathbb{Z}[X]/(X) \cong \mathbb{Z}$, care e integru dar nu e corp. Propunem cititorului să demonstreze aceste fapte cu ajutorul definiţiei idealului prim, respectiv maximal.

2.10 Teoremă. (Teorema fundamentală de izomorfism) *Fie* $\varphi : R \to S$ *un morfism de inele. Atunci* $\dfrac{R}{\mathrm{Ker}\varphi} \cong \mathrm{Im}\varphi$.

Mai precis, există un izomorfism natural $\psi : R/\mathrm{Ker}\varphi \to \mathrm{Im}\varphi$, $\psi(x + \mathrm{Ker}\varphi) = \varphi(x)$, $\forall x \in M$.

Demonstraţie. Aplicaţia $\psi : R/\mathrm{Ker}\varphi \to \mathrm{Im}\varphi$ este corect definită: dacă $x, y \in R$, cu $x + \mathrm{Ker}\varphi = y + \mathrm{Ker}\varphi$, atunci $x - y \in \mathrm{Ker}\varphi$, adică $\varphi(x - y) = 0$; aceasta echivalează cu $\varphi(x) = \varphi(y)$. Aşadar, $\psi(x + \mathrm{Ker}\varphi)$ nu depinde de reprezentantul x, ci doar de clasa $x + \mathrm{Ker}\varphi$. Verificarea faptului că ψ este morfism este lăsată cititorului.

Morfismul ψ este surjectiv: $\mathrm{Im}\psi = \{\psi(x + \mathrm{Ker}\varphi) \mid x \in M\} = \{\varphi(x) \mid x \in M\} = \mathrm{Im}\varphi$. Pentru injectivitate, arătăm că $\mathrm{Ker}\psi = \{0 + \mathrm{Ker}\varphi\}$: dacă $x \in M$ cu $\psi(x + \mathrm{Ker}\varphi) = 0$, atunci $\varphi(x) = 0$, deci $x \in \mathrm{Ker}\varphi$, adică $x + \mathrm{Ker}\varphi = 0 + \mathrm{Ker}\varphi$. □

2.11 Observaţie. Teorema de izomorfism se foloseşte de obicei în modul următor: presupunem că $B \leq_R A$ şi se cere demonstrarea faptului că A/B este izomorf cu un C. Se caută definirea unui morfism surjectiv $\varphi : A \to C$, cu $\mathrm{Ker}\varphi = B$. Atunci teorema de izomorfism asigură existenţa izomorfismului cerut. Corolarele următoare ilustrează această tehnică (aplicabilă şi în cazul grupurilor, modulelelor, algebrelor…).

2.12 Corolar (Teorema I de izomorfism). *Fie R un inel şi E, F ideale în R astfel încît* $E \subseteq F$. *Atunci* F/E *este ideal în* R/E *şi:*

$$\frac{R/E}{F/E} \cong \frac{R}{F}$$

Demonstraţie. Întrucît $F/E = \{x + E \mid x \in F\}$, avem $F/E \subseteq R/E = \{x + E \mid x \in R\}$. Fie $\varphi : R/E \to R/F$, $\varphi(x + E) = x + F$, $\forall x \in R$. Aplicaţia φ este corect definită: dacă $x, y \in R$, cu $x + E = y + E$, atunci $x - y \in E$. Deci $x - y \in F$, adică $x + F = y + F$. Este imediat faptul că φ este morfism surjectiv de inele. $\mathrm{Ker}\varphi = \{x + E \mid x \in R,\ x + F = 0 + F\} = \{x + E \mid x \in R, x \in F\} = F/E$. Se aplică acum teorema fundamentală de izomorfism. □

Exerciţii

1. Fie R un inel comutativ unitar şi I un ideal al său. Demonstraţi că există o bijecţie crescătoare (care păstrează incluziunile) între $\mathcal{L}(R/I)$ (laticea idealelor lui R/I) şi laticea idealelor lui R care includ I, $\{J \leq R \mid I \subseteq J\}$.

2. Fie $R_1, R_2, \ldots, R_n$ inele. Fie $p_i : R_1 \times \ldots \times R_n \to R_i$, $p_i((r_1, \ldots, r_n)) = r_i$, pentru orice $(r_1, \ldots, r_n) \in R_1 \times \ldots \times R_n$ (p_i se numesc *proiecţiile canonice*).

a) Să se arate că p_i sînt morfisme surjective de inele.

b) Fie I ideal în inelul produs direct $R_1 \times \ldots \times R_n$. Demonstraţi că $I = p_1(I) \times \ldots \times p_n(I)$.

c) Demonstraţi că $R_1 \times \ldots \times R_n/I \cong R_1/p_1(I) \times \ldots \times R_n/p_n(I)$.

d) Determinaţi toate idealele inelului $\mathbb{Z} \times \mathbb{Z}$.