

Capitolul III

INELE ȘI CORPURI

§ 1. INEL. SUBINEL. IDEAL. INELE DE MATRICE

Definiția 1.1. Se numește *inel* o mulțime nevidă R înzestrată cu două operații algebrice: $+ : R \times R \rightarrow R$ și $\cdot : R \times R \rightarrow R$, una notată aditiv și numită adunare, iar cealaltă notată multiplicativ și numită înmulțire, care satisfac următoarele condiții:

- 1) R este grup abelian față de operația de adunare;
- 2) operația de înmulțire este asociativă;
- 3) oricare ar fi $a, b, c \in R$, avem

$$a(b+c) = ab + ac,$$

$$(a+b)c = ac + bc.$$

Condiția 3) exprimă proprietățile de distributivitate ale înmulțirii față de adunare.

În cazul unui inel R , grupul abelian R față de adunare se numește *grupul aditiv subiacent inelului*. Elementul neutru al acestui grup se notează, de obicei, cu 0 și se numește *elementul zero* al inelului, iar *opusul* față de adunare al unui element oarecare $a \in R$ se notează, de obicei, cu $-a$.

Dacă, în plus, operația de înmulțire admite element neutru (unitate), spunem că inelul este cu element unitate, sau că este *inel unitar*. Elementul neutru la înmulțire se notează, de obicei, cu 1 și se numește *elementul unitate* sau *unitatea* inelului R .

Dacă înmulțirea este comutativă, inelul se numește *comutativ*.

Exemplu. 1) Mulțimile \mathbf{Z} , \mathbf{Q} , \mathbf{R} cu operațiile obișnuite de adunare și înmulțire formează inele comutative și unitare.

2) Dacă $n \in \mathbf{Z}$ este un număr întreg, atunci mulțimea $n\mathbf{Z} = \{nk \mid k \in \mathbf{Z}\}$ este inel comutativ față de adunarea și înmulțirea obișnuită a numerelor întregi.

3) Mulțimea $C([0, 1], \mathbf{R}) = \{f: [0, 1] \rightarrow \mathbf{R} \mid f \text{ continuă}\}$ cu adunarea și înmulțirea funcțiilor, $f+g$ și fg , definite în mod ușor: $(f+g)(x) = f(x)+g(x)$ și $(fg)(x) = f(x)g(x)$ este un inel comutativ și unitar.

4) Multimea $\{0, 1, 2\}$ cu adunarea și înmulțirea definite de tabelele:

| $+$ | 0 | 1 | 2 | . | 0 | 1 | 2 |
|-----|---|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 0 | 0 | 0 | 0 |
| 1 | 1 | 2 | 0 | 1 | 0 | 1 | 2 |
| 2 | 2 | 0 | 1 | 2 | 0 | 2 | 1 |

formează un inel, după cum se poate verifica direct prin calcul.

5) Fie G un grup abelian și

$$\text{End}(G) = \{f: G \rightarrow G \mid f \text{ morfism de grupuri}\}.$$

Multimea $\text{End}(G)$ împreună cu adunarea și compunerea morfismelor, $f+g$ și fog , definite prin

$$(f+g)(x) = f(x) + g(x) \text{ și } (fog)(x) = f(g(x))$$

este un inel unitar, numit inelul endomorfismelor grupului abelian G . Elementul unitate este morfismul identic al lui G .

6) Multimea $\mathbf{Z}_n = \{\hat{0}, \hat{1}, \dots, \hat{n-1}\}$ a claselor de resturi modulo n împreună cu adunarea și înmulțirea claselor, definite în cap. I, formează un inel comutativ și unitar numit inelul claselor de resturi modulo n .

7) Fie R un inel. Vom defini un nou inel R° în modul următor. Grupurile additive subiacente celor două inele coincid, adică $(R^\circ, +) = (R, +)$. Operația de înmulțire "*" din R° o definim prin $a * b = ba$, unde ba este produsul elementelor b și a în inelul R . Este clar că R este inel, iar dacă R este unitar, atunci R° este unitar, având același element unitate ca și R . Avem că inelele R și R° coincid dacă și numai dacă R este comutativ. Inelul R° se numește *inelul opus* al lui R .

Deoarece față de adunare, un inel R este grup abelian rezultă că, dacă $m, n \in \mathbf{Z}$ și $a, b \in R$, atunci

$$m(a+b) = ma + mb,$$

$$(m+n)a = ma + na,$$

$$[(mn)a = m(na)].$$

Vom da unele proprietăți care rezultă imediat din axiomele inelului și în care intervin ambele operații algebrice.

Propoziția 1.2. Dacă R este un inel, atunci

$$1) a0 = 0a = 0, \text{ oricare ar fi } a \in R;$$

$$2) a(-b) = (-a)b = -ab \text{ și } (-a)(-b) = ab, \text{ oricare ar fi } a, b \in R;$$

$$3) \quad a(b_1 + b_2 + \dots + b_n) = ab_1 + ab_2 + \dots + ab_n,$$

$(a_1 + a_2 + \dots + a_n)b = a_1b + a_2b + \dots + a_nb$, oricare ar fi $n \geq 2$

și $a, b, a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_n \in R$.

4) Dacă, în plus, R este comutativ, atunci

$$(a+b)^n = a^n + C_n^1 a^{n-1}b + C_n^2 a^{n-2}b^2 + \dots + C_n^{n-1} a b^{n-1} + b^n$$

(formula binomului lui Newton).

Demonstrație. 1) Avem

$$a0 = a(0+0) = a0 + a0.$$

Adunând $-a0$ în ambeii membri ai egalității $a0 = a0 + a0$, obținem $a0 = 0$. Analog, $0a = 0$.

2) Avem

$$0 = 0b = (a + (-a))b = ab + (-a)b,$$

care arată că $(-a)b = -ab$.

Analog, $a(-b) = -ab$. Deci $(-a)(-b) = -a(-b) = -(-ab) = ab$.

3) Se demonstrează prin inducție matematică după n .

Să arătăm, de exemplu, prima relație.

Pentru $n=2$, $a(b_1 + b_2) = ab_1 + ab_2$ rezultă din distributivitatea înmulțirii față de adunare.

Dacă presupunem că relația este adevărată pentru $n=k$, adică

$$a\left(\sum_{i=1}^k b_i\right) = \sum_{i=1}^k ab_i$$

atunci

$$\begin{aligned} a\left(\sum_{i=1}^{k+1} b_i\right) &= a\left(\sum_{i=1}^k b_i + b_{k+1}\right) = a\left(\sum_{i=1}^k b_i\right) + ab_{k+1} = \\ &= \sum_{i=1}^k ab_i + ab_{k+1} = \sum_{i=1}^{k+1} ab_i \end{aligned}$$

și deci relația este adevărată și pentru $n=k+1$.

4) Se demonstrează prin inducție matematică după n .

Pentru $n=1$, avem $(a+b)^1 = a+b = C_1^0 a + C_1^1 b$.

Să presupunem că formula este adevărată pentru $n=k$:

$$(a+b)^k = C_k^0 a^k + C_k^1 a^{k-1}b + \dots + C_k^m a^{k-m}b^m + \dots + C_k^k b^k.$$

Să arătăm că ea este adevărată pentru $n=k+1$.

Intr-adevăr,

$$(a+b)^{k+1} = (a+b)^k(a+b) = (C_k^0 a^k + C_k^1 a^{k-1}b + \dots + C_k^m a^{k-m}b^m + \dots + C_k^k b^k)(a+b)$$

$$\begin{aligned}
& + \dots + C_k^k b^k)(a+b) = C_k^0 a^{k+1} + C_k^1 a^k b + \dots + C_k^{m+1} a^{k-m} b^{m+1} + \dots + \\
& + C_k^k a b^k + C_k^0 a^k b + \dots + C_k^m a^{k-m} b^{m+1} + \dots + C_k^{k-1} a b^k + C_k^k b^{k+1} = \\
& = C_k^0 a^{k+1} + (C_k^0 + C_k^1) a^k b + \dots + (C_k^m + C_k^{m+1}) a^{k-m} b^{m+1} + \dots \\
& \quad \dots + (C_k^{k-1} + C_k^k) a b^k + C_k^k b^{k+1}.
\end{aligned}$$

Având în vedere că, $C_k^0 = C_{k+1}^0$, $C_k^k = C_{k+1}^{k+1}$ și $C_k^m + C_k^{m+1} = C_{k+1}^{m+1}$ pentru $0 \leq m \leq k-1$, atunci

$$\begin{aligned}
(a+b)^{k+1} &= C_{k+1}^0 a^{k+1} + C_{k+1}^1 a^k b + \dots + C_{k+1}^{m+1} a^{k-m} b^{m+1} + \dots \\
&\quad \dots + C_{k+1}^k a b^k + C_{k+1}^{k+1} b^{k+1}
\end{aligned}$$

și deci formula este adevărată pentru $n=k+1$.

Fie R un inel și $a \in R$. Spunem că elementul a este *divizor al lui zero la stînga* (respectiv la dreapta) dacă există $b \in R$, $b \neq 0$ astfel încît $ab=0$ (respectiv $ba=0$).

Un element a care este în același timp divizor al lui zero la stînga și la dreapta se numește simplu, *divizor al lui zero*.

Observăm că, dacă R este inel comutativ, noțiunile de divizor al lui zero la stînga și la dreapta coincid cu cea de divizor al lui zero.

Un inel unitar *nenul fără divizori ai lui zero la stînga și la dreapta nenuli* se numește inel *integru*. Dacă, în plus, inelul este și comutativ, va fi numit *domeniu de integritate*.

Observăm că un inel unitar R este integrul dacă și numai dacă sunt adevărate regulile de simplificare, adică, pentru orice $a \neq 0$, $ab = ac$ implică $b=c$ și $ba=ca$ implică $b=c$.

Intr-adevăr, dacă R este inel integrul și $ab=ac$, $a \neq 0$, atunci $a(b-c)=0$, de unde $b-c=0$ sau $b=c$. La fel, dacă $ba=ca$, rezultă că $b=c$. Reciproc, fie R inel unitar în care sunt adevărate regulile de simplificare. Atunci, din $ab=0$, $a \neq 0$, avem $ab=a0$ și deci $b=0$. La fel, din $ba=0$, $a \neq 0$, rezultă $b=0$ și deci R este integrul.

Dacă R este inel unitar, un element $a \in R$ se numește *inversabil* dacă există $b \in R$ astfel încît

$$ab=ba=1.$$

Vom nota cu $U(R) = \{a \in R \mid a \text{ inversabil}\}$.

Avem că, dacă $a, b \in U(R)$, atunci

$$(ab)^{-1} = b^{-1}a^{-1}$$

și deci $ab \in U(R)$.

Este clar că $U(R)$ are o structură de grup față de operația de înmulțire din R . Acest grup se numește *grupul elementelor inversabile ale inelului R* .

De exemplu, $U(\mathbf{Z}) = \{-1, 1\}$, $U(\mathbf{Q}) = \mathbf{Q} \setminus \{0\}$, $U(\mathbf{R}) = \mathbf{R} \setminus \{0\}$, $U(\mathbf{Z}_n) = \{\hat{a} \in \mathbf{Z}_n \mid (a, n) = 1\}$ (vezi cap. I).

Dacă R este un inel unitar, orice element inversabil al lui R nu este divizor al lui zero.

Într-adevăr, fie $a \in R$ astfel încât există $b \in R$ cu $ab = ba = 1$. Atunci $a \neq 0$ și dacă $ac = 0$, atunci $b(ac) = b0$, adică $(ba)c = 0$, de unde $c = 0$.

La fel, dacă $da = 0$, atunci $(da)b = 0b$, adică $d(ab) = 0$, de unde $d = 0$.

Definiția 1.3. Fie R un inel. O submulțime nevidă S a lui R se numește *subinel* al lui R dacă S împreună cu operațiile induse de cele două operații algebrice de pe R formează la rîndul său un inel.

Propoziția 1.4. Fie R un inel și $S \subset R$ o submulțime nevidă a sa. Atunci S este un subinel al lui R dacă și numai dacă:

1° oricare ar fi $x, y \in S$, rezultă $x - y \in S$;

2° oricare ar fi $x, y \in S$, rezultă $xy \in S$.

Demonstratie. Condițiile 1° și 2° arată că operațiile de pe R induc pe S operații algebrice. Mulțimea S împreună cu acestea formează un inel după cum se poate vedea cu ușurință, ținând cont că S este o submulțime a inelului R .

Din condiția 1° rezultă că S , împreună cu adunarea, este un subgrup al grupului aditiv al inelului R . Deci $0 \in S$ și oricare ar fi $x \in S$, avem că $-x \in S$.

Dacă, în plus, inelul R este unitar și elementul unitate aparține subinului S , spunem că S este subinel unitar.

Exemple. 1) Dacă R este un inel, atunci R și $\{0\}$ sunt evident subinile ale saie.

2) $\mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R}$ sunt subinile unul în altul, cu adunarea și înmulțirea numerelor.

3) Fie inelul $C([0, 1], \mathbf{R}) = \{f: [0, 1] \rightarrow \mathbf{R} \mid f \text{ continuă}\}$.

Atunci submulțimea $D([0, 1], \mathbf{R}) = \{f: [0, 1] \rightarrow \mathbf{R} \mid f \text{ derivabilă}\}$ a inelului $C([0, 1], \mathbf{R})$ formează un subinel al acestuia.

4) Dacă $n \in \mathbf{Z}$, atunci este clar că mulțimea $n\mathbf{Z} = \{nk \mid k \in \mathbf{Z}\}$ este un subinel al lui \mathbf{Z} . Deci orice subgrup al grupului aditiv $(\mathbf{Z}, +)$ este subinel al inelului \mathbf{Z} . Reciproca fiind mereu adevărată, rezultă că subinilele lui \mathbf{Z} sunt tocmai subgrupurile lui $(\mathbf{Z}, +)$. Deci subinile inelului \mathbf{Z} sunt date de mulțimea $\{n\mathbf{Z}\}_{n \geq 0}$.

5) Fie inelul \mathbf{Z}_n al claselor de resturi modulo n . Subgrupurile grupului aditiv subiacent lui \mathbf{Z}_n sunt ciclice și deci sunt de forma

$$\langle d \rangle = \{\hat{a}a \mid a \in \mathbf{Z}\}, \text{ unde } \hat{d} \in \mathbf{Z}_n.$$

Dar, este clar că orice subgrup este în același timp subinel. Prin urmare, subinile inelului \mathbf{Z}_n coincid cu subgrupurile grupului aditiv \mathbf{Z}_n .

Propoziția 1.5. Fie R un inel și $\{S_\alpha\}_{\alpha \in A}$ o familie de subinile ale lui R . Atunci $\bigcap_{\alpha \in A} S_\alpha$ este un subinel al lui R .

Demonstrație. Faptul că $\bigcap_{\alpha \in A} S_\alpha$ este un subgrup al grupului aditiv subiacent lui R , rezultă din cele prezentate la grupuri. Dacă, acum, $x, y \in \bigcap_{\alpha \in A} S_\alpha$, atunci $x, y \in S_\alpha$, oricare ar fi $\alpha \in A$. Dar fiecare S_α este subinel și deci $xy \in S_\alpha$, oricare ar fi $\alpha \in A$, de unde $xy \in \bigcap_{\alpha \in A} S_\alpha$.

Definiția 1.6. Fie R un inel și $I \subset R$ o submulțime nevidă a sa. Spunem că I este un *ideal la stînga* (respectiv *la dreapta*) al inelului R dacă:

1° oricare ar fi $x, y \in I$, rezultă $x - y \in I$;

2° oricare ar fi $a \in R$ și $x \in I$, rezultă $ax \in I$, (respectiv $xa \in I$).

Un ideal care este în același timp ideal la stînga și ideal la dreapta se numește ideal *bilateral*.

Dacă R este inel comutativ, atunci este clar că noțiunea de ideal la stînga coincide cu cea de ideal la dreapta și cu cea de ideal bilateral. În acest caz vom spune, simplu, ideal al inelului R .

Din definiție rezultă că orice ideal la stînga (la dreapta sau bilateral) este un subinel al inelului, pe cînd reciproc nu este adevărat. Astfel \mathbf{Z} este un subinel al lui \mathbf{Q} însă nu este ideal deoarece, de exemplu,

$3 \in \mathbf{Z}$ și $\frac{1}{4} \in \mathbf{Q}$, iar $3 \cdot \frac{1}{4} = \frac{3}{4} \notin \mathbf{Z}$.

Exemple. 1) Dacă R este un inel, atunci R și $\{0\}$ sunt evident ideale bilaterale ale sale.

2) Am văzut că subinelele inelului \mathbf{Z} sunt submulțimile sale de tipul $n\mathbf{Z}$ cu $n \in \mathbf{N}$. Este clar că orice astfel de submulțime este un ideal al lui \mathbf{Z} și deci idealele lui \mathbf{Z} coincid cu subinelele sale adică sunt date de $\{n\mathbf{Z}\}_{n \geq 0}$.

3) Am arătat mai înainte la exemplul 5) că subinelele inelului \mathbf{Z}_n al claselor de resturi modulo n coincid cu subgrupurile grupului aditiv subiacent lui \mathbf{Z}_n , fiind de forma $\langle \bar{d} \rangle = \{\bar{da} \mid a \in \mathbf{Z}\}$. Dar, este clar că orice subgrup este ideal al inelului \mathbf{Z}_n . Deci, idealele și subinelele lui \mathbf{Z}_n coincid, fiind aceleași cu subgrupurile grupului aditiv \mathbf{Z}_n . De exemplu, să considerăm inelul \mathbf{Z}_6 . Cum $\hat{1}$ și $\hat{5}$ sunt inversabile, rezultă că $\langle \hat{1} \rangle = \langle \hat{5} \rangle = \mathbf{Z}_6$ (vezi și propoziția 1.7). Luînd pe rînd celelalte elemente ale lui \mathbf{Z}_6 , obținem:

$$\langle \hat{0} \rangle = \{ \hat{0} \}, \langle \hat{2} \rangle = \langle \hat{4} \rangle = \{ \hat{0}, \hat{2}, \hat{4} \}, \langle \hat{3} \rangle = \{ \hat{0}, \hat{3} \}.$$

Prin urmare, inelul \mathbf{Z}_6 are următoarele patru ideale care sunt în același timp și subinelele sale:

$$\{ \hat{0} \}, \{ \hat{0}, \hat{3} \}, \{ \hat{0}, \hat{2}, \hat{4} \}, \mathbf{Z}_6.$$

4) Dacă R este inel unitar și $a \in R$, atunci considerăm următoarele submulțimi ale lui R :

$$Ra = \{xa \mid x \in R\},$$

$$aR = \{ax \mid x \in R\} \text{ și}$$

$$RaR = \left\{ \sum_{i=1}^n x_i a y_i \mid n \in \mathbb{N}, x_i, y_i \in R, i = 1, 2, \dots, n \right\}.$$

Se verifică ușor că acestea sunt ideale, respectiv, la stînga, la dreapta și bilateral.

Dacă R este un inel și $a \in R$ un element oarecare, atunci Ra , aR și RaR se numesc *ideale principale*, respectiv, la stînga, la dreapta și bilateral.

Observăm că în cazul în care R este inel comutativ noțiunile de ideal principal la stînga, la dreapta și bilateral coincid. În acest caz se va numi, simplu, ideal principal și-l vom nota și cu (a) .

Exemplele 2) și 3) de mai înainte ne arată că orice ideal al inelilor \mathbf{Z} și \mathbf{Z}_n este principal.

Propoziția 1.7. Fie R un inel unitar și $I \subset R$ un ideal la stînga (respectiv la dreapta) al lui R . Atunci $I=R$ dacă și numai dacă I conține un element inversabil.

Demonstrație. Într-adevăr, dacă $I=R$, atunci $1 \in I$ care este inversabil.

Reciproc, fie I ideal la stînga, elementul inversabil $u \in I$ și $v \in R$ astfel încît $uv=vu=1$. Dacă $x \in I$, atunci $x=x \cdot 1=x(vu)=(xv)u$ și cum u aparține idealului la stînga I , rezultă $xv \in I$. Deci $x \in I$. La fel se demonstrează pentru cazul unui ideal la dreapta.

Propoziția 1.8. Fie R un inel și $\{I_\alpha\}_{\alpha \in A}$ o familie de ideale la stînga (respectiv la dreapta, bilaterale) ale lui R . Atunci $\bigcap_{\alpha \in A} I_\alpha$ este un ideal la stînga (respectiv la dreapta, bilateral).

Demonstrație. De la grupuri rezultă că $\bigcap_{\alpha \in A} I_\alpha$ este un subgrup al grupului subiacent lui R . Presupunind că idealele familiei sunt ideale la stînga, fie $a \in R$ și $x \in \bigcap_{\alpha \in A} I_\alpha$. Atunci $x \in I_\alpha$, oricare ar fi $\alpha \in A$ și deci $ax \in I_\alpha$, oricare ar fi $\alpha \in A$, de unde $ax \in \bigcap_{\alpha \in A} I_\alpha$. Prin urmare $\bigcap_{\alpha \in A} I_\alpha$ este un ideal la stînga. La fel, se demonstrează pentru cazul idealelor la dreapta și bilaterale.

Definiția 1.9. Fie R un inel unitar și E o submulțime a lui R . Intersecția tuturor idealelor la stînga (respectiv la dreapta, bilaterale) ale lui R care conțin mulțimea E , se numește *idealul la stînga* (respectiv *la dreapta, bilateral*) generat de mulțimea E în inelul R . Se spune că E este un *sistem de generatori* pentru (sau că generează) acest ideal. Mulțimea vidă generează idealul (0) .

Un ideal la stînga (respectiv la dreapta, bilateral) care are o mulțime finită de generatori se numește de *tip finit* sau *finit generat*.

Propoziția 1.10. Fie R un inel unitar și E o submulțime nevidă a sa. Idealul la stînga (respectiv la dreapta, bilateral) I al lui R este generat de E dacă și numai dacă

$$I = \left\{ \sum_{i=1}^n a_i x_i \mid a_i \in R, x_i \in E, n \in \mathbb{N} \right\} \quad (\text{respectiv})$$

$$I = \left\{ \sum_{i=1}^n x_i a_i \mid x_i \in E, a_i \in R, n \in \mathbb{N} \right\},$$

$$I = \left\{ \sum_{i=1}^n a_i x_i b_i \mid a_i, b_i \in R, x_i \in E, n \in \mathbb{N} \right\}.$$

Demonstrație. Să demonstrăm pentru cazul în care I este ideal la stînga, în celelalte două cazuri demonstrația fiind analoagă. Observăm mai întîi că

$$I' = \left\{ \sum_{i=1}^n a_i x_i \mid a_i \in R, x_i \in E, n \in \mathbb{N} \right\}$$

este un ideal la stînga al lui R care conține submulțimea E . Deci $I' \supset I$. Pe de altă parte, deoarece $I \supset E$, I ideal la stînga, avem că oricare ar fi $x \in I'$, $x = \sum_{i=1}^n a_i x_i$, unde $a_i \in R$, $x_i \in E$ aparține în mod clar lui I .

Deci $I = I'$ ceea ce termină demonstrația.

Observăm că I este cel mai mic ideal la stînga (respectiv la dreapta, bilateral) în raport cu incluziunea care conține submulțimea E .

Din propoziția precedentă rezultă că idealele principale sunt cele generate de o mulțime formată dintr-un singur element.

Definiția 1.11. Fie R un inel și $\{I_\alpha\}_{\alpha \in A}$ o familie de ideale la stînga (respectiv la dreapta, bilaterale) ale lui R . Idealul la stînga (respectiv la dreapta, bilateral) generat de submulțimea $\bigcup_{\alpha \in A} I_\alpha$ a lui R

se numește *suma* familiei de ideale $\{I_\alpha\}_{\alpha \in A}$ și o vom nota cu $\sum_{\alpha \in A} I_\alpha$.

Avînd în vedere propoziția 1.9 rezultă că

$$\sum_{\alpha \in A} I_\alpha = \left\{ \sum_{i=1}^n x_{\alpha_i} \mid x_{\alpha_i} \in I_{\alpha_i}, \alpha_i \in A, n \in \mathbb{N} \right\}.$$

În particular, dacă I_1, I_2, \dots, I_n sunt ideale ale inelului R , atunci

$$\sum_{k=1}^n I_k = \left\{ \sum_{k=1}^n x_k \mid x_k \in I_k, k = 1, 2, \dots, n \right\}.$$

Definiția 1.12. Fie R un inel și I, J ideale la stînga (respectiv la dreapta, bilaterale) ale lui R . Este clar că mulțimea

$$IJ = \left\{ \sum_{i=1}^n x_i y_i \mid n \in \mathbf{N}, x_i \in I, y_i \in J, i = 1, 2, \dots, n \right\}$$

este un ideal la stînga (respectiv la drepta, bilateral) al lui R . Acest ideal se numește *produsul* idealelor I și J .

Exemplu. Fie $p, q \in \mathbf{Z}$ și să notăm cu $d = \text{c.m.m.d.c.}(p, q)$ și $m = \text{c.m.m.m.c.}(p, q)$. Atunci

- 1) $p\mathbf{Z} + q\mathbf{Z} = d\mathbf{Z}$,
- 2) $p\mathbf{Z} \cap q\mathbf{Z} = m\mathbf{Z}$.

Să demonstrăm 1). Cum $d = \text{c.m.m.d.c.}(p, q)$, există $u, v \in \mathbf{Z}$ astfel încît $d = pu + qv$. Dacă $x \in p\mathbf{Z} + q\mathbf{Z}$, atunci $x = dd'$, $d' \in \mathbf{Z}$ și deci $x = (pu + qv)d' = p(ud') + q(vd') \in p\mathbf{Z} + q\mathbf{Z}$. Astfel am arătat că $p\mathbf{Z} + q\mathbf{Z} \supset d\mathbf{Z}$. Reciproc, dacă $x \in p\mathbf{Z} + q\mathbf{Z}$, fie $p = dp'$, $q = dq'$ și atunci $x = pr + qs = dp'r + dq's = d(p'r + q's) \in d\mathbf{Z}$. Astfel, $p\mathbf{Z} + q\mathbf{Z} \subset d\mathbf{Z}$ și deci $p\mathbf{Z} + q\mathbf{Z} = d\mathbf{Z}$.

Să demonstrăm acum 2). Dacă $m = \text{c.m.m.m.c.}(p, q)$ este clar că $m\mathbf{Z} \subset p\mathbf{Z} \cap q\mathbf{Z}$. Fie acum $x \in p\mathbf{Z} \cap q\mathbf{Z}$, adică $x \in p\mathbf{Z}$ și $x \in q\mathbf{Z}$. Deci $p \mid x$, $q \mid x$ și cum $m = \text{c.m.m.m.c.}(p, q)$, avem că $m \mid x$, adică $x \in m\mathbf{Z}$. Astfel am arătat că $p\mathbf{Z} \cap q\mathbf{Z} \subset m\mathbf{Z}$ și deci egalitatea 2).

§ 2. MORFISME DE INELE. PRODUS DIRECT DE INELE. APLICAȚII

Definiția 2.1. Fie R și R' două inele. Se numește *morfism* de inele de la R la R' o funcție $f: R \rightarrow R'$, astfel încât să fie satisfăcute următoarele condiții:

$$1) f(a+b)=f(a)+f(b),$$

$$2) f(ab)=f(a)f(b),$$

oricare ar fi $a, b \in R$.

Dacă R și R' sunt inele, iar $f: R \rightarrow R'$ un morfism de inele, după prima condiție din definiția morfismului rezultă că f este morfism al grupurilor additive ale celor două inele și deci avem:

$$f(0)=0 \text{ și } f(-a)=-f(a), \text{ oricare ar fi } a \in R.$$

Observăm că funcția $\theta: R \rightarrow R'$, definită prin $\theta(a)=0$, este în mod evident un morfism de inele numit *morfismul nul*. Dacă R și R' sunt inele unitare nenule, morfismul nul $\theta: R \rightarrow R'$ are proprietatea că $\theta(1)=-0 \neq 1$, adică nu duce pe 1 în 1.

Un morfism $f: R \rightarrow R'$, unde R și R' sunt inele unitare, care satisface în plus condiția

$$f(1)=1$$

se numește *morfism unitar* de inele.

Vom da în continuare unele proprietăți de bază ale morfismelor de inele.

1° Dacă R, R', R'' sunt inele iar $f: R \rightarrow R', g: R' \rightarrow R''$ sunt morfisme de inele, atunci compunerea $g \circ f: R \rightarrow R''$ este un morfism de inele.

Într-adevăr, de la grupuri rezultă că $g \circ f$ este morfism al grupurilor additive subiacente inelelor R și R'' .

În plus, oricare ar fi $a, b \in R$, avem

$$(g \circ f)(ab)=g(f(ab))=g(f(a)f(b))=g(f(a))g(f(b))=((g \circ f)(a))((g \circ f)(b)).$$

2° Pentru orice inel R , funcția identică $1_R: R \rightarrow R$ este un morfism de inele, numit *morfismul identic* al lui R . Avem că oricare ar fi $f: R \rightarrow R'$ un morfism de inele, atunci

$$f \circ 1_R=f \text{ și } 1_{R'} \circ f=f.$$

Definiția 2.2. Fie R și R' două inele. Un morfism de inele $f: R \rightarrow R'$ astfel încât funcția f să fie injectivă (respectiv surjectivă) se numește *morfism injectiv* (respectiv *surjectiv*) de inele.

Un morfism de inele $f: R \rightarrow R'$ se numește *izomorfism* de inele dacă există un morfism de inele $g: R' \rightarrow R$ astfel încât

$$f \circ g=1_{R'} \text{ și } g \circ f=1_R.$$

2.2. Teoremă. Fie $f: R \rightarrow R'$ un morfism de inele. Atunci f este izomorfism dacă și numai dacă funcția f este bijectivă.

Demonstrație. Având în vedere rezultatul corespunzător pentru grupuri este suficient să demonstrăm că, dacă $g: R' \rightarrow R$ este o funcție

astfel încit $f \circ g = 1_{R'}$ și $g \circ f = 1_R$, atunci $g(bb') = g(b)g(b')$, oricare ar fi $b, b' \in R'$. Dacă $b, b' \in R'$, atunci

$$bb' = 1_{R'}(bb') = (f \circ g)(bb') = f(g(bb')).$$

Pe de altă parte,

$$bb' = 1_{R'}(b)1_{R'}(b') = (f \circ g)(b)(f \circ g)(b') = f(g(b))f(g(b')) = f(g(b)g(b')).$$

Deci $f(g(bb')) = f(g(b)g(b'))$ și cum f este injectivă, rezultă

$$g(bb') = g(b)g(b').$$

Exemplu. 1) Am remarcat mai înainte că pentru orice două inele R și R' , există morfismul nul $0: R \rightarrow R'$. De asemenea, pentru orice inel R avem morfismul identic $1_R: R \rightarrow R$.

2) Funcția $i: \mathbf{Z} \rightarrow \mathbf{Q}$, $i(n) = n$ este un morfism injectiv de inele.

3) Dacă $n > 0$ este un număr natural, funcția $p: \mathbf{Z} \rightarrow \mathbf{Z}_n$, definită prin $p(a) = \bar{a}$ este un morfism surjectiv de inele.

Intr-adevăr, dacă $a, b \in \mathbf{Z}$, atunci

$$p(a+b) = \widehat{a+b} = \widehat{a} + \widehat{b} = p(a) + p(b) \text{ și}$$

$$p(ab) = \widehat{ab} = \widehat{a}\widehat{b} = p(a)p(b).$$

Mai mult, după definiție p este morfism surjectiv.

4) Fie R inel comutativ și unitar și $\mathcal{M}_n(R)$ inelul matricelor patratice de ordinul n peste R , care este de asemenea unitar.

Dacă $n = 1$, funcția

$$\varphi: R \rightarrow \mathcal{M}_1(R),$$

care asociază elementului a din R matricea cu o singură linie și coloană (a) , adică $\varphi(a) = (a)$, este evident un izomorfism de inele.

Pentru $n \geq 2$, să considerăm matricea unitate $I_n = (\delta_{ij})_{1 \leq i, j \leq n} \in$

$\mathcal{M}_n(R)$, unde $\delta_{ij} = \begin{cases} 1, & \text{dacă } i=j \\ 0, & \text{dacă } i \neq j \end{cases}$ este simbolul lui Kronecker.

Definim funcția

$$\psi: R \rightarrow \mathcal{M}_n(R), \text{ prin}$$

$$\psi(a) = (a\delta_{ij})_{1 \leq i, j \leq n}.$$

Evident că $(a\delta_{ij})_{1 \leq i, j \leq n}$ este matricea, ale căror componente sunt uale, în afară de cele de pe diagonala principală care sunt egale cu a .

Avem că ψ este un morfism unitar de inele.

Intr-adevăr, dacă $a, b \in R$, atunci

$$\begin{aligned}\psi(a+b) &= ((a+b)\delta_{ij})_{1 \leq i, j \leq n} = (a\delta_{ij} + b\delta_{ij})_{1 \leq i, j \leq n} = \\ &= (a\delta_{ij})_{1 \leq i, j \leq n} + (b\delta_{ij})_{1 \leq i, j \leq n} = \psi(a) + \psi(b).\end{aligned}$$

De asemenea, $\psi(ab) = ((ab)\delta_{ij})_{1 \leq i, j \leq n}$, iar dacă $\psi(a)\psi(b) = (c_{ij})_{1 \leq i, j \leq n}$, atunci

$$c_{ij} = \sum_{k=1}^n (a\delta_{ik})(b\delta_{kj}) = (ab)\delta_{ij}.$$

Deci $\psi(ab) = \psi(a)\psi(b)$.

Este clar că $\psi(1) = I_n$, adică ψ este unitar.

Mai mult, dacă $a, b \in R$ astfel încât $\psi(a) = \psi(b)$, atunci $(a\delta_{ij})_{1 \leq i, j \leq n} = (b\delta_{ij})_{1 \leq i, j \leq n}$, de unde $a = b$.

Am arătat astfel că ψ este morfism injectiv de inele.

Propoziția 2.3. Fie $f: R \rightarrow S$ un morfism de inele. Atunci:

1) Dacă $R' \subset R$ este subinel, atunci $f(R') \subset S$ este subinel și dacă $S' \subset S$ este subinel, atunci $f^{-1}(S') \subset R$ este subinel.

2) Dacă $J \subset S$ este ideal la stînga (respectiv la dreapta, bilateral), atunci $f^{-1}(J) \subset R$ este ideal la stînga (respectiv la dreapta, bilateral). Mai mult, dacă f este surjectiv și $I \subset R$ este ideal la stînga (respectiv la dreapta, bilateral), atunci $f(I) \subset S$ este ideal la stînga (respectiv la dreapta, bilateral).

Demonstrație. 1) Dacă considerăm structurile de grupuri abeliene subiacente celor două inele, f este în particular morfism de grupuri. De la grupuri avem că $f(R')$ este subgrup al lui S și, de asemenea, $f^{-1}(S')$ este subgrup al lui R . Mai mult, dacă $b, b' \in f(R')$, atunci $b = f(a), b' = f(a')$ cu $a, a' \in R'$. Deci $bb' = f(a)f(a') = f(aa') \in f(R')$, deoarece $aa' \in R'$. Dacă avem $a, a' \in f^{-1}(S')$, atunci $f(a), f(a') \in S'$ și deci $f(a)f(a') \in S'$, de unde $f(aa') \in S'$ adică $aa' \in f^{-1}(S')$.

2) Ca mai înainte $f^{-1}(J)$ este subgrup al lui R . Să presupunem că J este ideal la stînga și fie $a \in R$ și $x \in f^{-1}(J)$. Atunci $f(ax) = f(a)f(x) \in J$, de unde $ax \in f^{-1}(J)$. Analog, se demonstrează pentru cazurile în care J este ideal la dreapta sau bilateral. Dacă acum I este ideal la stînga al lui R , avem că $f(I)$ este subgrup al grupului aditiv subiacent lui S .

Fie $b \in S$ și $y \in f(I)$. Avem $y = f(x)$, $x \in I$, și dacă f este morfism surjectiv există $a \in R$ astfel încât $f(a) = b$. Atunci $by = f(a)f(x) = f(ax) \in f(I)$. La fel se demonstrează în celelalte cazuri.

Definiția 2.4. Fie $f: R \rightarrow S$ un morfism de inele. Notăm cu $\text{Im } f = f(R)$ și cu $\text{Ker } f = \{a \in R \mid f(a) = 0\}$ și le numim respectiv *imaginăea* și *nucleul* morfismului f .

Corolarul 2.5. Fie $f: R \rightarrow S$ un morfism de inele. Atunci $\text{Im } f$ este un subinel al lui S , iar $\text{Ker } f$ este un ideal bilateral al lui R .

Demonstrație. Rezultă imediat din propoziția precedentă. Cum R este subinel al lui R , atunci $\text{Im } f$ este subinel al lui S . Apoi $\text{Ker } f = f^{-1}((0))$, iar (0) este evident bilateral al lui S .

Fie $\{R_\alpha\}_{\alpha \in A}$ o familie de inele. Pe produsul direct al familiilor de grupuri subiacente inelelor R_α , $\prod_{\alpha \in A} R_\alpha = \{(a_\alpha)_\alpha \mid a_\alpha \in R_\alpha \text{ pentru orice } \alpha \in A\}$, definim o operație algebrică multiplicativă. Astfel, dacă $a = (a_\alpha)_\alpha$ și $b = (b_\alpha)_\alpha$ sunt două elemente din $\prod_{\alpha \in A} R_\alpha$, punem prin definiție $ab = (a_\alpha b_\alpha)_\alpha$, unde pentru orice $\alpha \in A$, $a_\alpha b_\alpha$ se efectuează în R_α .

Avem că $\prod_{\alpha \in A} R_\alpha$ împreună cu cele două operații algebrice, adunarea și înmulțirea, are o structură de inel.

Am remarcat deja că $\prod_{\alpha \in A} R_\alpha$ împreună cu adunarea este grup abelian și înmulțirea satisface următoarele condiții:

1° este asociativă,

2° este distributivă față de adunare.

Să verificăm, de exemplu, una din egalitățile care ne dă distributivitatea. Dacă $a, b, c \in \prod_{\alpha \in A} R_\alpha$, unde $a = (a_\alpha)_\alpha$, $b = (b_\alpha)_\alpha$, $c = (c_\alpha)_\alpha$, avem

$$\begin{aligned} a(b+c) &= (a_\alpha)_\alpha((b_\alpha)_\alpha + (c_\alpha)_\alpha) = (a_\alpha)_\alpha(b_\alpha + c_\alpha)_\alpha = (a_\alpha(b_\alpha + c_\alpha))_\alpha = \\ &= (a_\alpha b_\alpha + a_\alpha c_\alpha)_\alpha = (a_\alpha b_\alpha)_\alpha + (a_\alpha c_\alpha)_\alpha = (a_\alpha)_\alpha(b_\alpha)_\alpha + (a_\alpha)_\alpha(c_\alpha)_\alpha = ab + ac. \end{aligned}$$

Definiția 2.6. Inelul $\prod_{\alpha \in A} R_\alpha$ se numește *produsul direct* al familiei de inele $\{R_\alpha\}_{\alpha \in A}$.

Observăm că dacă inelele R_α , $\alpha \in A$, sunt comutative, atunci produsul lor direct este inel comutativ.

De asemenea, dacă inelele R_α , $\alpha \in A$, sunt unitare, atunci produsul lor direct este inel unitar, al cărui element unitate este $1 \in \prod_{\alpha \in A} R_\alpha$, $1 = (1_\alpha)_\alpha$, unde 1_α este elementul unitate al inelului R_α , $\alpha \in A$.

Dacă R este un inel am notat cu $U(R)$ grupul elementelor inversabile ale lui R .

Propoziția 2.7. Fie $\{R_\alpha\}_{\alpha \in A}$ o familie de inele unitare și $R = \prod_{\alpha \in A} R_\alpha$ produsul lor direct. Atunci

$$U(R) = \prod_{\alpha \in A} U(R_\alpha).$$

Demonstrație. Deoarece produsul a două elemente din R se efectuează pe componente, rezultă imediat că $(a_\alpha)_\alpha$ din R este inversabil dacă și numai dacă fiecare a_α , $\alpha \in A$, este inversabil în R_α .

De exemplu, $U(\mathbf{Z} \times \mathbf{Z}) = \{(1, 1), (1, -1), (-1, 1), (-1, -1)\}$,

$U(\mathbf{Z} \times \mathbf{Q}) = \{-1, 1\} \times \mathbf{Q}^*$, $U(\mathbf{Q} \times \mathbf{Q}) = \mathbf{Q}^* \times \mathbf{Q}^*$, unde $\mathbf{Q}^* = \mathbf{Q} \setminus \{0\}$.

Dacă $\{R_\alpha\}_{\alpha \in A}$ este o familie de inele iar $R = \prod_{\alpha \in A} R_\alpha$ produsul lor direct, atunci pentru orice $\beta \in A$, funcția $p_\beta: R \rightarrow R_\beta$ definită prin $p_\beta((a_\alpha)_\alpha) = a_\beta$ este evident un morfism surjectiv de inele. Acest morfism se numește proiecția produsului direct pe componenta R_β .

Vom face în continuare unele aplicații, în scopul determinării unei formule de calcul pentru funcția lui Euler.

Propoziția 2.8. Fie m, n numere întregi pozitive astfel încât $(m, n) = 1$. Atunci inelele \mathbf{Z}_{mn} și $\mathbf{Z}_m \times \mathbf{Z}_n$ sunt izomorfe.

Demonstrație. Considerăm $\mathbf{Z}_m = \{\hat{0}, \hat{1}, \dots, \hat{m-1}\}$, $\mathbf{Z}_n = \{\bar{0}, \bar{1}, \dots, \bar{n-1}\}$, $\mathbf{Z}_{mn} = \{\bar{\bar{0}}, \bar{\bar{1}}, \dots, \bar{\bar{mn-1}}\}$ și $\mathbf{Z}_m \times \mathbf{Z}_n = \{(\hat{a}, \bar{b}) \mid \hat{a} \in \mathbf{Z}_m, \bar{b} \in \mathbf{Z}_n\}$.

Definim funcția $\varphi: \mathbf{Z}_{mn} \rightarrow \mathbf{Z}_m \times \mathbf{Z}_n$, prin $\varphi(\bar{\bar{a}}) = (\hat{a}, \bar{a})$.

Vom arăta că φ este bine definită și stabilește izomorfismul de inele căutat.

Dacă $\bar{\bar{a}} = \bar{\bar{a}'}$, atunci $a \equiv a' \pmod{mn}$, adică $mn \mid a - a'$, de unde $m \mid a - a'$ și $n \mid a - a'$. Deci $a \equiv a' \pmod{m}$ și $a \equiv a' \pmod{n}$, sau $\hat{a} = \hat{a}'$ și $\bar{a} = \bar{a}'$ adică $\varphi(\bar{\bar{a}}) = \varphi(\bar{\bar{a}'})$. Deci φ este bine definită. Funcția φ este un morfism de inele.

Intr-adevăr, $\varphi(\bar{\bar{a}} + \bar{\bar{a}'}) = \varphi(\bar{\bar{a+a'}}) = (\hat{a+a'}, \bar{a+a'}) = (\hat{a}, \bar{a}) + (\hat{a'}, \bar{a'}) = \varphi(\bar{\bar{a}}) + \varphi(\bar{\bar{a'}})$. De asemenea, $\varphi(\bar{\bar{aa'}}) = \varphi(\bar{\bar{aa'}}) = (\hat{aa'}, \bar{aa'}) = (\hat{a}, \bar{a})(\hat{a'}, \bar{a'}) = \varphi(\bar{\bar{a}})\varphi(\bar{\bar{a'}})$.

Fie acum $\varphi(\bar{\bar{a}}) = \varphi(\bar{\bar{a}'})$. Atunci $(\hat{a}, \bar{a}) = (\hat{a'}, \bar{a'})$, de unde $\hat{a} = \hat{a}'$ și $\bar{a} = \bar{a}'$ și deci $m \mid a - a'$ și $n \mid a - a'$. Deoarece $(m, n) = 1$ rezultă că $mn \mid a - a'$, adică $\bar{\bar{a}} = \bar{\bar{a}'}$ și deci φ este funcție injectivă. Având în vedere că multimile \mathbf{Z}_{mn} și $\mathbf{Z}_m \times \mathbf{Z}_n$ au fiecare același număr mn de elemente, rezultă că φ este bijectivă. Deci φ este un izomorfism de inele.

Corolarul 2.9. Dacă m_1, m_2, \dots, m_k sunt numere întregi pozitive și $(m_i, m_j) = 1$, pentru orice $i \neq j$, atunci inelele $\mathbf{Z}_{m_1 m_2 \dots m_k}$ și $\prod_{i=1}^k \mathbf{Z}_{m_i}$ sunt izomorfe.

Demonstrație. Rezultă imediat din propoziția precedență prin inducție matematică.

Dacă n este un număr întreg pozitiv, funcția lui Euler $\varphi(n)$ este numărul numerelor naturale nenule prime cu n și mai mici decât n . Deci $\varphi(n)$ este ordinul grupului $U(\mathbf{Z}_n)$.

Izomorfismul precedent și propoziția 2.7 ne dă

$$U(\mathbf{Z}_{m_1 m_2 \cdots m_k}) = \prod_{i=1}^k U(\mathbf{Z}_{m_i}),$$

de unde $\text{ord } U(\mathbf{Z}_{m_1 m_2 \cdots m_k}) = \prod_{i=1}^k \text{ord } U(\mathbf{Z}_{m_i})$.

Prin urmare, dacă m_1, m_2, \dots, m_k sunt numere întregi pozitive și $(m_i, m_j) = 1$, pentru orice $i \neq j$, atunci

$$\varphi(m_1 m_2 \cdots m_k) = \varphi(m_1) \varphi(m_2) \cdots \varphi(m_k).$$

Putem da acum o formulă de calcul pentru funcția lui Euler.

Propoziția 2.10. Fie n un număr întreg ≥ 2 și $n = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$ descompunerea sa în produs de numere prime, unde $p_i \neq p_j$, pentru orice $i \neq j$. Atunci

$$\varphi(n) = n \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right).$$

Demonstratie. Din cele de mai sus rezultă că $\varphi(n) = \varphi(p_1^{m_1}) \varphi(p_2^{m_2}) \cdots \varphi(p_k^{m_k})$. Pentru un număr p^k cu p prim avem că $\varphi(p^k) = p^k - p^{k-1}$. Într-adevăr, dacă a este număr natural $< p^k$, atunci a nu este prin cu p^k dacă și numai dacă $p \nmid a$. Este clar că sunt p^{k-1} astfel de numere și deci $\varphi(p^k) = p^k - p^{k-1}$. Atunci

$$\varphi(n) = \prod_{i=1}^k \varphi(p_i^{m_i}) = \prod_{i=1}^k (p_i^{m_i} - p_i^{m_i-1}) = \prod_{i=1}^k p_i^{m_i} \left(1 - \frac{1}{p_i}\right) = n \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right).$$

$$\begin{aligned} \text{De exemplu, } \varphi(720) &= \varphi(2^4 \cdot 3^2 \cdot 5) = 720 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) = \\ &= 192. \end{aligned}$$

INELE DE POLINOAME

§ 1. Construcția inelului de polinoame într-o nedeterminată. Proprietăți generale

Fie R un inel comutativ și unitar. Se va da mai întii o construcție a inelului de polinoame într-o nedeterminată peste R . Fie $R^{(N)}$ mulțimea sirurilor

$$f = (a_0, a_1, \dots, a_n, \dots), \quad a_i \in R$$

care au numai un număr finit de termeni a_i nenuli.

Deci un sir ai cărui termeni sunt elemente din R aparține lui $R^{(N)}$ dacă și numai dacă există un număr natural m , astfel încât $a_i = 0$, pentru orice $i > m$.

Sirurile $f = (a_0, a_1, \dots, a_n, \dots)$ și $g = (b_0, b_1, \dots, b_n, \dots)$ sunt egale dacă și numai dacă $a_i = b_i$ pentru orice i .

Pe mulțimea $R^{(N)}$ definim două operații algebrice, adunarea și înmulțirea, în raport cu care $R^{(N)}$ devine un inel comutativ și unitar.

Dacă $f, g \in R^{(N)}$

$$f = (a_0, a_1, a_2, \dots), \quad g = (b_0, b_1, b_2, \dots),$$

adunarea se definește astfel:

$$f + g = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \dots).$$

Avem că $f + g \in R^{(N)}$. Într-adevăr, fie numerele naturale m și n astfel încât $a_i = 0$, pentru orice $i > m$ și $b_j = 0$, pentru orice $j > n$. Atunci $a_k + b_k = 0$ pentru orice $k > \max(m, n)$.

Se verifică ușor că $R^{(N)}$ împreună cu adunarea formează un grup abelian, adică adunarea este asociativă, comutativă, are element nul și orice element are un opus.

Elementul nul (zero) este

$$(0, 0, 0, \dots),$$

iar dacă $f = (a_0, a_1, a_2, \dots)$ aparține lui $R^{(N)}$, atunci opusul său este

$$-f = (-a_0, -a_1, -a_2, \dots).$$

Înmulțirea pe $R^{(N)}$ se definește astfel:

Dacă $f = (a_0, a_1, a_2, \dots)$ și $g = (b_0, b_1, b_2, \dots)$ aparțin lui $R^{(N)}$, atunci
 $fg = (c_0, c_1, c_2, \dots)$,

unde

$$c_k = a_0 b_k + a_1 b_{k-1} + \dots + a_k b_0 = \sum_{i+j=k} a_i b_j, \text{ pentru orice } k=0, 1, 2, \dots$$

Să arătăm că $fg \in R^{(N)}$. Într-adevăr, dacă $a_i = 0$ pentru orice $i > m$ și $b_j = 0$ pentru orice $j > n$, atunci $c_k = 0$ pentru orice $k > m+n$.

Înmulțirea pe $R^{(N)}$ este asociativă, comutativă și are element unitate $(1, 0, 0, \dots)$.

Să demonstrăm asociativitatea înmulțirii.

Fie $f, g, h \in R^{(N)}$, unde

$f = (a_0, a_1, a_2, \dots)$, $g = (b_0, b_1, b_2, \dots)$, $h = (c_0, c_1, c_2, \dots)$ și să arătăm că $(fg)h = f(gh)$. Dacă $fg = (d_0, d_1, d_2, \dots)$, atunci $d_k = \sum_{i+j=k} a_i b_j$ și fie $(fg)h = (e_0, e_1, e_2, \dots)$, unde $e_m = \sum_{k+l=m} d_k c_l$.

$$\text{Avem } e_m = \sum_{k+l=m} d_k c_l = \sum_{k+l=m} \left(\sum_{i+j=k} a_i b_j \right) c_l = \sum_{\substack{k+l=m \\ i+j=k}} a_i b_j c_l = \sum_{i+j+l=m} a_i b_j c_l.$$

Dacă $gh = (d'_0, d'_1, d'_2, \dots)$ unde $d'_k = \sum_{j+l=k} b_j c_l$ iar $f(gh) = (e'_0, e'_1, e'_2, \dots)$, unde

$$\begin{aligned} e'_m &= \sum_{i+k=m} a_i d'_k, \text{ avem } e'_m = \sum_{i+k=m} a_i d_k = \sum_{i+k=m} a_i \left(\sum_{j+l=k} b_j c_l \right) = \sum_{\substack{i+k=m \\ j+l=k}} a_i b_j c_l = \\ &= \sum_{i+j+l=m} a_i b_j c_l. \end{aligned}$$

Deci $e_m = e'_m$ pentru orice m , adică $(fg)h = f(gh)$.

Comutativitatea înmulțirii rezultă imediat. Mai mult, înmulțirea este distributivă față de adunare. Într-adevăr, cu notațiile de mai înainte, rezultă

$$f(g+h) = (d_0, d_1, d_2, \dots), \text{ unde } d_k = \sum_{i+j=k} a_i(b_j+c_j), \text{ iar}$$

$$fg+fh = (d'_0, d'_1, d'_2, \dots), \text{ unde } d'_k = \sum_{i+j=k} a_i b_j + \sum_{i+j=k} a_i c_j.$$

Cum operația de înmulțire pe R este distributivă față de adunare, rezultă

$$f(g+h) = fg + fh.$$

Analog are loc și relația

$$(f+g)h = fh + gh.$$

În concluzie, am demonstrat că $R^{(N)}$ împreună cu adunarea și înmulțirea formează un inel comutativ și unitar. Elementele acestui inel se numesc *polinoame peste R* , sau *polinoame cu coeficienți în R* .

Dacă $f = (a_0, a_1, a_2, \dots)$ este un polinom nenul atunci $n = \max\{i \mid a_i \neq 0\}$ se numește gradul polinomului f . Gradul unui polinom f se notează prin $\text{grad}(f)$, iar coeficientul a_n , unde $n = \text{grad}(f)$, se numește coeficientul dominant al polinomului f . Pentru polinomul nul, convenim să considerăm gradul său ca fiind $-\infty$, adoptând convențiile uzuale și anume: $-\infty < n$, $-\infty + n = -\infty$, pentru orice număr natural n , $-\infty + (-\infty) = -\infty$. Dacă $n = \text{grad}(f)$ atunci $a_0, a_1, a_2, \dots, a_n$ se numesc coeficienții polinomului f .

Fie funcția $u: R \rightarrow R^{(N)}$, definită prin

$$u(a) = (a, 0, 0, \dots).$$

Arătăm că u este un morfism injectiv de inele. Într-adevăr, dacă $a, b \in R$, atunci

$$\begin{aligned} u(a+b) &= (a+b, 0, 0, \dots) = (a, 0, 0, \dots) + (b, 0, 0, \dots) = \\ &= u(a) + u(b) \text{ și } u(ab) = (ab, 0, 0, \dots) = \\ &= (a, 0, 0, \dots)(b, 0, 0, \dots) = u(a)u(b). \end{aligned}$$

Mai mult, dacă $u(a) = u(b)$, atunci $(a, 0, 0, \dots) = (b, 0, 0, \dots)$ deci $a = b$.

Morfismul u dă un izomorfism al lui R pe subinelul $R' = \{(a, 0, 0, \dots) \mid a \in R\}$ al lui $R^{(N)}$, ceea ce permite să se identifice elementul a din R cu imaginea sa prin u , adică cu polinomul $(a, 0, 0, \dots)$ din $R^{(N)}$. Astfel R se poate considera ca un subinel al lui $R^{(N)}$.

Pe de altă parte, notăm prin X polinomul $(0, 1, 0, \dots)$ care se numește nedeterminata X . Înmulțirea polinoamelor ne dă $X^2 = (0, 0, 1, 0, \dots)$ și, mai general pentru orice număr natural i

$$X^i = \underbrace{(0, 0, \dots, 0)}_{i \text{ ori}},$$

Fie f un polinom de grad n ai cărui coeficienți sunt $a_0, a_1, a_2, \dots, a_n$, adică $f = (a_0, a_1, a_2, \dots, a_n, 0, 0, \dots)$.

Folosind adunarea și înmulțirea definite pe $R^{(N)}$ se obține

$$\begin{aligned} f &= (a_0, a_1, a_2, \dots, a_n, 0, 0, \dots) = (a_0, 0, 0, 0, \dots) + (0, a_1, 0, 0, \dots) + \\ &\quad + (0, 0, a_2, 0, \dots) + \dots + (0, 0, \dots, 0, a_n, 0, \dots) = \\ &= (a_0, 0, 0, 0, \dots) + (a_1, 0, 0, 0, \dots)(0, 1, 0, \dots) + (a_2, 0, 0, \dots) \cdot \\ &\quad \cdot (0, 0, 1, 0, \dots) + (a_n, 0, 0, 0, \dots) \underbrace{(0, 0, \dots, 0)}_{n \text{ ori}}, \text{ ceilalți coeficienți} \end{aligned}$$

fiind nuli, nu-i mai scriem.

Mai mult, după cele de mai înainte

$$f = a_0 + a_1 X + a_2 X^2 + \dots + a_n X^n,$$

obținind astfel scrierea obișnuită a unui polinom.

Inelul $R^{(N)}$ se numește inelul polinoamelor în nedeterminata X , cu coeficienți în inelul R și se notează prin $R[X]$. Inelul $R[X]$ se mai numește și inelul polinoamelor într-o nedeterminată.

Un polinom de gradul n în nedeterminata X îl vom scrie, condensat,

$$f = \sum_{i=0}^n a_i X^i, \quad a_n \neq 0.$$

1.1. Propoziție. Fie R un inel și f, g polinoame din $R[X]$.

Atunci

$$1) \text{ grad}(f+g) \leq \max(\text{grad}(f), \text{grad}(g)),$$

2) $\text{grad}(fg) \leq \text{grad}(f) + \text{grad}(g)$. Mai mult, dacă f și g sunt nenule și cel puțin unul dintre coeficienții dominanti ai lui f și g nu este divizor al lui zero atunci avem egalitate.

Demonstrație. Dacă cel puțin unul dintre polinoamele f și g este nul, atunci 1) și 2) rezultă evident având în vedere convențiile uzuale: $-\infty < n$, $-\infty + n = -\infty$, oricare ar fi n număr natural și $-\infty + (-\infty) = -\infty$. Dacă f și g sunt nenule afirmațiile 1) și 2) rezultă imediat din definiția sumei și produsului a două polinoame.

Fie $f = \sum_{i=0}^m a_i X^i$, $a_m \neq 0$, $g = \sum_{j=1}^n b_j X^j$, $b_n \neq 0$, astfel încât a_m sau b_n să nu fie divizor al lui zero. Atunci coeficientul dominant al produsului fg este $a_m b_n$ care este nenul. Deci în acest caz, $\text{grad}(fg) = \text{grad}(f) + \text{grad}(g)$.

Din pct. 2) al propoziției precedente rezultă

1.2. Corolar. Dacă R este domeniu de integritate și f, g polinoame din $R[X]$, atunci

$$\text{grad}(fg) = \text{grad}(f) + \text{grad}(g).$$

1.3. Observație. Dacă R nu este domeniu de integritate inegalitatea 2) poate fi strictă. De exemplu, fie polinoamele $f = \hat{1} + \hat{2}X$ și $g = \hat{2}X$ din inelul $\mathbb{Z}_2[X]$. Atunci $fg = (\hat{1} + \hat{2}X)\hat{2}X^2 = \hat{2}X^2$ și deci $\text{grad}(fg) = 2 < 3 = \text{grad}(f) + \text{grad}(g)$.

Amintim că pentru un inel R , am notat cu $U(R)$ mulțimea elementelor sale inversabile.

1.4. Propoziție. Fie R un inel comutativ și unitar și inelul polinoamelor $R[X]$. Atunci au loc afirmațiile:

1) Un element $a \in R$ este inversabil în R dacă și numai dacă a este inversabil în $R[X]$.

2) Dacă R este domeniu de integritate, atunci $R[X]$ este domeniu de integritate și $U(R) = U(R[X])$.

Demonstrație. 1) Dacă a este inversabil în R , avem $ab = 1$ cu $b \in R$. Această relație considerată în $R[X]$, a și b fiind polinoame de grad zero, spune că a este inversabil în $R[X]$. Reciproc, dacă a este inversabil în $R[X]$, atunci există $f \in R[X]$ astfel încât $af = 1$. Presupunând că $f = a_0 + a_1X + a_2X^2 + \dots + a_nX^n$, $a_n \neq 0$, avem $aa_0 + aa_1X + aa_2X^2 + \dots + aa_nX^n = 1$, de unde $aa_0 = 1$ și deci a este inversabil în R .

2) Dacă R este domeniu de integritate, din corolarul 1.2. este clar că $R[X]$ este domeniu de integritate. Din punctul precedent rezultă că $U(R) \subseteq U(R[X])$. Pentru a demonstra incluziunea contrară, fie $f = a_0 + a_1X + a_2X^2 + \dots + a_mX^m$, $a_m \neq 0$, un polinom inversabil din $R[X]$. Deci există $g = b_0 + b_1X + b_2X^2 + \dots + b_nX^n$ astfel încât $fg = 1$. Avem $\text{grad}(fg) = \text{grad}(1)$, de unde $\text{grad}(f) + \text{grad}(g) = 0$ sau $m + n = 0$ și deci $m = n = 0$. Astfel rezultă că $f = a_0 \in R$, $g = b_0 \in R$ și cum $1 = fg = a_0b_0$ obținem că $f = a_0 \in U(R)$.

1.5. Observație. Dacă R nu este un domeniu de integritate putem avea $U(R) \neq U(R[X])$. Într-adevăr, polinomul neconstant $\hat{1} + \hat{2}X \in \mathbb{Z}_4[X]$ este inversabil, deoarece $(\hat{1} + \hat{2})X(\hat{1} + \hat{2}X) = \hat{1}$.

Dacă R este un inel comutativ și unitar, $R[X]$ inelul polinoamelor în nedeterminata X cu coeficienți în R , am definit, mai înainte morfismul unitar de inele,

$$u: R \rightarrow R[X], \quad u(a) = a$$

numit morfismul canonic de la R la $R[X]$.

Vom da acum o proprietate importantă numită proprietatea de universalitate a inelelor de polinoame de o nedeterminată.

1.6. Teorema. Fie R un inel comutativ și unitar, $R[X]$ inelul polinoamelor de o nedeterminată cu coeficienți în R și $u: R \rightarrow R[X]$ morfismul canonic. Atunci oricare ar fi inelul comutativ unitar S , morfismul unitar de inele $v: R \rightarrow S$ și $x \in S$, există un unic morfism de inele $\varphi: R[X] \rightarrow S$ astfel încât $u(X) = x$ și diagrama

$$\begin{array}{ccc} R & \xrightarrow{u} & R[X] \\ & \searrow v & \swarrow \varphi \\ & S & \end{array}$$

să fie comutativă, adică $\varphi u = v$.

Demonstrație. Să definim mai întâi morfismul φ . Dacă $f \in R[X]$, $f = \sum_{i=0}^m a_i X^i$, atunci

$$\varphi(f) = \sum_{i=0}^m v(a_i) x^i.$$

Arătăm că φ are proprietățile din enunț. Fie $g = \sum_{i=0}^n b_i X^i$ un alt polinom din $R[X]$ și să presupunem că $m \leq n$. Completând eventual polinomul f cu termeni ai căror coeficienți sunt zero putem scrie $f = \sum_{i=0}^n a_i X^i$, unde $a_{m+1} = \dots = a_n = 0$. Atunci

$$\begin{aligned} \varphi(f+g) &= \varphi\left(\sum_{i=0}^n (a_i + b_i) X^i\right) = \sum_{i=0}^n v(a_i + b_i) x^i = \\ &= \sum_{i=0}^n (v(a_i) + v(b_i)) x^i = \sum_{i=0}^n v(a_i) x^i + \sum_{i=0}^n v(b_i) x^i = \\ &= \sum_{i=0}^m v(a_i) x^i + \sum_{i=0}^n v(b_i) x^i = \varphi(f) + \varphi(g). \end{aligned}$$

Dacă notăm cu c_k , coeficienții produsului fg , avem $c_k = \sum_{i+j=k} a_i b_j$ și cum v este morfism de inele obținem $v(c_k) = \sum_{i+j=k} v(a_i) v(b_j)$. Înțind seama de

acest lucru se verifică imediat că $v(fg) = v(f)v(g)$. Deci φ este morfism de inele. Mai mult, $\varphi(X) = \varphi(1 \cdot X) = v(1)x = 1 \cdot x = x$. Să verificăm acum comutativitatea diagramei. Într-adevăr, dacă $a \in R$, $(\varphi \circ u)(a) = \varphi(u(a)) = \varphi(a) = \varphi(aX^0) = v(a)x^0 = v(a)$ și deci $\varphi \circ u = v$.

Să presupunem că $\bar{\varphi}: R[X] \rightarrow S$ este un alt morfism de inele astfel încât $\bar{\varphi}(X) = x$ și $\bar{\varphi} \circ u = v$. Atunci, pentru $f = \sum_{i=0}^m a_i X^i$ avem $\bar{\varphi}(f) = \bar{\varphi}\left(\sum_{i=0}^m a_i X^i\right) = \sum_{i=0}^m \bar{\varphi}(a_i) \bar{\varphi}(X^i) = \sum_{i=0}^m \bar{\varphi}(u(a_i)) (\bar{\varphi}(X))^i = \sum_{i=0}^m v(a_i) x^i = \varphi(f)$ și deci $\bar{\varphi} = \varphi$.

Astfel am demonstrat unicitatea lui φ .

Fie acum S un inel, $R \subseteq S$ un subinel al său și $v: R \rightarrow S$ incluziunea, adică $v(a) = a$. Teorema precedentă aplicată în acest caz, ne dă pentru fiecare $x \in S$ un morfism de inele $\varphi: R[X] \rightarrow S$, astfel încât

$$\varphi(f) = \varphi\left(\sum_{i=0}^m a_i X^i\right) = \sum_{i=1}^m a_i x^i.$$

Spunem că $\varphi(f)$ este valoarea polinomului f în x pe care o vom nota cu $f(x)$. Spunem că elementul $x \in S$ anulează polinomul $f = \sum_{i=0}^m a_i X^i$ din $R[X]$ sau că x este o rădăcină sau un zero al lui f dacă $f(x) = 0$, adică $\sum_{i=0}^m a_i x^i = 0$.

Fiind dat un polinom arbitrar din $R[X]$ putem să definim funcția $f_S: S \rightarrow S$ prin $f_S(x) = f(x)$, oricare ar fi $x \in S$. Astfel fiecarui polinom f din $R[X]$ și fiecarui inel S care conține pe R , iți corespunde o funcție definită pe S cu valori în S .

Oricare funcție de la S la S care poate fi pusă sub forma f_S pentru un anumit f din $R[X]$ se numește *funcție polinomială* pe S sau funcție pe S asociată polinomului f .

În particular, dacă $S = R$, se obține funcția polinomială f_R de la R la R pe care o vom nota și cu \tilde{f} .

Deci, dacă $f \in R[X]$, atunci $\tilde{f}: R \rightarrow R$ este funcția definită prin $\tilde{f}(x) = f(x)$, numită funcție polinomială asociată polinomului f .

Dacă $f = a \in R$, atunci funcția \tilde{f} este constantă, $\tilde{f}(x) = a$ pentru orice $x \in R$. De aceea elementele inelului R , considerate ca polinoame, se vor numi polinoame constante. Pot fi funcții polinomiale \tilde{f} care să fie constante, chiar cînd $f \notin R$. Dar numai acele polinoame care sunt în R se numesc constante.

1.7. *Observație.* Dacă R este un inel și f, g sunt polinoame egale din $R[X]$, atunci este evident că funcțiile polinomiale \tilde{f} și \tilde{g} sunt egale. Există însă și polinoame diferite care să aibă funcțiile polinomiale egale. De exemplu, să considerăm $f = X + \hat{1}$ și $g = X^2 + \hat{1}$ polinoame din $\mathbb{Z}_2[X]$ și fie $\tilde{f}: \mathbb{Z}_2 \rightarrow \mathbb{Z}_2$, $\tilde{g}: \mathbb{Z}_2 \rightarrow \mathbb{Z}_2$ funcțiile polinomiale asociate lui f și g .

$$\tilde{f}(\hat{0}) = \tilde{g}(\hat{0}) = \hat{1} \quad \text{și} \quad \tilde{f}(\hat{1}) = \tilde{g}(\hat{1}) = \hat{0} \quad \text{deci} \quad \tilde{f} = \tilde{g}, \text{ dar evident } f \neq g.$$

§ 3. Inele de matrice

3.1. Definiție. Fie R un inel comutativ și unitar, iar m și n numere naturale. Notăm cu $M = \{1, 2, \dots, m\}$ și $N = \{1, 2, \dots, n\}$ și fie $M \times N$ produsul lor cartezian. Se numește matrice de tip (m, n) peste inelul R , orice funcție

$$A : M \times N \rightarrow R$$

definită pe produsul cartezian $M \times N$ cu valori în inelul R .

Să notăm $A(i, j) = a_{ij}$, unde $1 \leq i \leq m$ și $1 \leq j \leq n$.

Spunem că elementele $a_{i1} a_{i2} \dots a_{in}$, unde $1 \leq i \leq m$, definesc linia de rang i a matricei A . În mod analog, elementele (scrise de obicei pe verticală)

$$\begin{matrix} a_{1j} \\ a_{2j} \\ \vdots & , & 1 \leq j \leq m, \\ \vdots \\ a_{nj} \end{matrix}$$

ormează coloana de rang j a matricei A .

Rezultă că oricărei matrice A de tipul (m, n) cu elemente din inelul R , îi se asociază un tablou cu m linii și n coloane în care sunt așezate

$$\left(\begin{array}{ccc} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{array} \right).$$

Reciproc, un astfel de tablou cu m linii și n coloane de elemente din inelul R , determină în mod unic o matrice A :

$$A : M \times N \rightarrow R, \text{ dată prin } A(i, j) = a_{ij}.$$

Deci putem scrie matricea A sub forma unui astfel de tablou și anume:

$$A = \begin{pmatrix} a_{11} & a_{12} \dots a_{1n} \\ a_{21} & a_{22} \dots a_{2n} \\ \dots & \dots \\ a_{m1} & a_{m2} \dots a_{mn} \end{pmatrix}$$

sau, condensat, $A = (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$

Fie $\mathcal{M}(m, n, R)$ mulțimea matricelor cu m linii și n coloane cu elemente din inelul R .

3.2. Definiție. Vom defini pe $\mathcal{M}(m, n, R)$ o operație algebrică internă și anume adunarea matricelor, în modul următor:

Dacă $A, B \in \mathcal{M}(m, n, R)$, atunci

$$(A + B)(i, j) = A(i, j) + B(i, j), \text{ oricare ar fi } (i, j) \in M \times N.$$

Folosind scrierea matricelor sub formă de tablou, fie

$$A = (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} \text{ și } B = (b_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}, \text{ atunci}$$

$$A + B = C,$$

unde $C = (c_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ este o matrice de același tip cu A și B , ale cărei componente sunt date prin

$$c_{ij} = a_{ij} + b_{ij}, \quad 1 \leq i \leq m, \quad 1 \leq j \leq n.$$

Deci, date matricele A și B de același tip (m, n) , matricea sumă $A + B$ are drept componentă în linia i și coloana j suma componentelor din liniile de rang i și coloanele de rang j ale celor două matrice.

3.3. Proprietăți ale adunării matricelor

1) Adunarea matricelor este asociativă, adică $(A + B) + C = A + (B + C)$ oricare ar fi $A, B, C \in \mathcal{M}(m, n, R)$.

2) Adunarea matricelor este comutativă, adică $A + B = B + A$ oricare ar fi $A, B \in \mathcal{M}(m, n, R)$.

3) Matricea 0 de tip (m, n) care are toate componente egale cu zero este elementul nul, adică $A + 0 = 0 + A = A$, oricare ar fi $A \in \mathcal{M}(m, n, R)$.

4) Dacă $A \in \mathcal{M}(m, n, R)$ este o matrice oarecare, atunci matricea $-A$ ale cărei componente sunt opusele componentelor matricei A este opusă matricei A , adică $A + (-A) = (-A) + A = 0$.

Demonstrație. Deoarece demonstrația proprietăților adunării matricelor se poate face pe componente, aceasta se realizează cu ușurință bazându-ne pe proprietățile analoage ale adunării în inelul R .

De exemplu, dacă $A = (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ și $B = (b_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ atunci

$$\begin{aligned} A + B &= (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} + (b_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} = (a_{ij} + b_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} = (b_{ij} + a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} = \\ &= (b_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} + (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} = B + A. \end{aligned}$$

Menționăm, de asemenea, că dacă $A = (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$, atunci opusa lui A este matricea $-A = (-a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$.

Având în vedere cele de mai înainte, rezultă că mulțimea $\mathcal{M}(m, n, R)$ a matricelor de același tip (m, n) peste inelul R împreună cu adunarea matricelor are o structură de grup abelian.

3.4. Definiție. Fie $A = (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ o matrice de tipul (m, n) și $B = (b_{jk})_{\substack{1 \leq j \leq n \\ 1 \leq k \leq p}}$ o matrice de tipul (n, p) peste inelul R . Deci numărul de coloane ale matricei A este egal cu numărul de linii ale matricei B .

Vom defini o nouă matrice $C = (c_{ik})_{\substack{1 \leq i \leq m \\ 1 \leq k \leq p}}$ de tip (m, p) , ale cărei componente sunt date de formulele

$$c_{ik} = \sum_{j=1}^n a_{ij} b_{jk}, \quad 1 \leq i \leq m, \quad 1 \leq k \leq p.$$

Așadar componenta c_{ik} a matricei C este suma produselor componentelor de pe linia i ale matricei A cu componente de pe coloana j ale matricei B .

Matricea C astfel obținută se numește *produsul* matricei A cu matricea B și se notează

$$C = AB.$$

3.5. Proprietăți:

1° Dacă $A = (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ este o matrice de tip (m, n) , $B = (b_{jk})_{\substack{1 \leq j \leq n \\ 1 \leq k \leq p}}$ este o matrice de tip (n, p) , iar $C = (c_{kl})_{\substack{1 \leq k \leq p \\ 1 \leq l \leq q}}$ este o matrice de tip (p, q) , atunci

$$(AB)C = A(BC),$$

adică înmulțirea matricelor este asociativă.

Demonstrație. Observăm mai întâi că produsele din ambii membri ai egalității sunt definite.

Dacă $AB = D = (d_{ik})_{\substack{1 \leq i \leq m \\ 1 \leq k \leq p}}$ și $(AB)C = DC = E = (e_{il})_{\substack{1 \leq i \leq m \\ 1 \leq l \leq q}}$ avem

$$e_{il} = \sum_{k=1}^p d_{ik} c_{kl} = \sum_{k=1}^p \left(\sum_{j=1}^n a_{ij} b_{jk} \right) c_{kl} = \sum_{k=1}^p \sum_{j=1}^n a_{ij} b_{jk} c_{kl}.$$

Fie acum $BC = F = (f_{jl})_{\substack{1 \leq j \leq n \\ 1 \leq l \leq p}}$ și $A(BC) = AF = G = (g_{il})_{\substack{1 \leq i \leq m \\ 1 \leq l \leq p}}$

$$\text{Atunci } g_{il} = \sum_{j=1}^n a_{ij} f_{jl} = \sum_{j=1}^n a_{ij} \left(\sum_{k=1}^p b_{jk} c_{kl} \right) = \sum_{j=1}^n \sum_{k=1}^p a_{ij} b_{jk} c_{kl}.$$

Deci $e_{il} = g_{il}$, oricare $1 \leq i \leq m$, $1 \leq l \leq q$, adică $E = G$, sau $(AB)C = A(BC)$.

2° Dacă $A = (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ este o matrice de tipul (m, n) , iar $B = (b_{jk})_{\substack{1 \leq j \leq n \\ 1 \leq k \leq p}}$ și

$C = (c_{jk})_{\substack{1 \leq j \leq n \\ 1 \leq k \leq p}}$ sunt matrice de tip (n, p) , atunci

$$A(B+C) = AB + AC.$$

De asemenea, dacă $D = (d_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ și $E = (e_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ sunt matrice de tipul (m, n) , iar $F = (f_{jk})_{\substack{1 \leq j \leq n \\ 1 \leq k \leq p}}$ este o matrice de tipul (n, p) , atunci

$$(D+E)F = DF + EF.$$

Demonstrație. Dacă $A(B+C)=M=(m_{ik})_{\substack{1 \leq i \leq m \\ 1 \leq k \leq p}}$, atunci $m_{ik} = \sum_{j=1}^n a_{ij}(b_{jk} + c_{jk}) = \sum_{j=1}^n a_{ij}b_{jk} + \sum_{j=1}^n a_{ij}c_{jk}$, iar dacă $AB+AC=N=(n_{ik})_{\substack{1 \leq i \leq m \\ 1 \leq k \leq p}}$ avem $n_{ik} = \sum_{j=1}^n a_{ij}b_{jk} + \sum_{j=1}^n a_{ij}c_{jk}$. Deci $m_{ik} = n_{ik}$, pentru oricare $1 \leq i \leq m$, $1 \leq k \leq p$, adică $M=N$, sau

$$A(B+C)=AB+AC.$$

Analog, se demonstrează egalitatea a doua din enunț.

3° Fie I_m și I_n matricele de tip (m, m) și respectiv (n, n) ale căror componente sunt nule în afară de cele de pe diagonala principală care sunt egale cu 1.

Dacă $A \in \mathcal{M}(m, n, R)$ este o matrice de tipul (m, n) , atunci

$$I_m A = A \quad \text{și} \quad A I_n = A.$$

În cazul în care matricea A are același număr n de linii și coloane, o vom numi *matrice pătratică* de ordinul n . Vom nota cu $\mathcal{M}_n(R)$ sau cu $\mathcal{M}(n, R)$ mulțimea matricelor pătratice de ordinul n peste inelul R .

3.6. *Propoziție.* Mulțimea matricelor pătratice $\mathcal{M}_n(R)$ cu componente din inelul comutativ și unitar R , formează un inel unitar în raport cu adunarea și înmulțirea matricelor.

Demonstrație. Pe mulțimea $\mathcal{M}_n(R)$ sunt definite atât adunarea cât și înmulțirea matricelor. Având în vedere proprietățile adunării și înmulțirii demonstrate mai înainte, rezultă că $\mathcal{M}_n(R)$ este un inel, matricea I_n fiind elementul unitate al său.

Observăm că, dacă R este un inel comutativ și unitar nenul, atunci $\mathcal{M}_n(R)$, pentru $n \geq 2$, nu este comutativ.

De exemplu, pentru $n=2$, avem

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

$$\text{iar} \quad \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}, \quad \text{adică}$$

$$\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}.$$

În aceleasi condiții inelul $\mathcal{M}_n(R)$ are divizori ai lui zero. De exemplu,

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{și} \quad \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix},$$

$$\text{iar} \quad \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

3.7. *Transpusa unei matrice.* Fie $A = (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ o matrice de tip (m, n) pește inelul R .

Matricea ${}^t A = ({}^t a_{kl})_{\substack{1 \leq k \leq n \\ 1 \leq l \leq m}}$ de tip (n, m) , unde ${}^t a_{kl} = a_{lk}$, oricare ar fi $1 \leq k \leq n$, $1 \leq l \leq m$, se numește transpusa matricei A .

Deci liniile, respectiv coloanele matricei transpuște ${}^t A$ sunt coloanele, respectiv liniile, matricei A .

În particular, dacă A este o matrice pătratică de ordinul n , atunci transpusa sa ${}^t A$ este o matrice pătratică în același ordin n . Dacă $k=l$, atunci ${}^t a_{kk} = a_{kk}$ și deci elementele de pe diagonala principală a matricei ${}^t A$ sunt aceleași cu cele de pe diagonala principală a matricei A .

Următoarele proprietăți se verifică fără dificultate:

1) Dacă $A, B \in \mathcal{M}(m, n, R)$, atunci

$${}^t(A+B) = {}^tA + {}^tB.$$

2) Dacă $A \in \mathcal{M}(m, n, R)$ și $B \in \mathcal{M}(n, p, R)$, atunci

$${}^t(AB) = {}^tB {}^tA.$$

Într-adevăr, dacă $A = (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ și $B = (b_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$, fie

$$\begin{aligned} A+B &= (c_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}. Avem {}^t(A+B) = ({}^t c_{kl})_{\substack{1 \leq k \leq n \\ 1 \leq l \leq m}}, \text{ unde } {}^t c_{kl} = c_{lk} = a_{lk} + b_{lk} = \\ &= {}^t a_{kl} + {}^t b_{kl}. \end{aligned}$$

$$\begin{aligned} \text{Deci } {}^t(A+B) &= ({}^t c_{kl})_{\substack{1 \leq k \leq n \\ 1 \leq l \leq m}} = ({}^t a_{kl} + {}^t b_{kl})_{\substack{1 \leq k \leq n \\ 1 \leq l \leq m}} = ({}^t a_{kl})_{\substack{1 \leq k \leq n \\ 1 \leq l \leq m}} + ({}^t b_{kl})_{\substack{1 \leq k \leq n \\ 1 \leq l \leq m}} = \\ &= {}^t A + {}^t B. \end{aligned}$$

Demonstrarea celei de-a doua proprietăți o lăsăm ca exercițiu.

3.8. Am observat că inelul $\mathcal{M}_n(R)$ pentru $n \geq 2$ nu este comutativ. Să justificăm prin exemple că există ideale la stînga care nu sunt ideale la dreapta și invers. Într-adevăr, R fiind un inel comutativ și unitar, se verifică ușor că

$$I = \left\{ \begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} \mid a, b \in R \right\}$$

este un ideal la stînga al inelului $\mathcal{M}_2(R)$ dar nu este ideal la dreapta. De asemenea,

$$I = \left\{ \begin{pmatrix} 0 & 0 \\ a & b \end{pmatrix} \mid a, b \in R \right\}$$

este un ideal la dreapta al inelului $\mathcal{M}_2(R)$ dar nu este ideal la stînga.

§3. INEL FACTOR

Noțiunea de ideal a fost definită pornind de la proprietățile pe care le au nucleele morfismelor de inele. În continuare vom constata că pentru orice ideal bilateral există un morfism de inele al cărui nucleu este chiar idealul dat. În acest mod, noțiunea de ideal bilateral joacă în teoria inelelor același rol pe care îl joacă noțiunea de subgrup normal în teoria grupurilor.

Fie $(R, +, \cdot)$ un inel și I un ideal bilateral al său. În particular I este un subgrup (normal) al grupului abelian $(R, +)$. Relația definită pe R în modul următor:

$$(1) \quad x \equiv y \pmod{I} \Leftrightarrow x - y \in I$$

este o relație de echivalență compatibilă cu operația aditivă pe R . Această proprietate a făcut posibilă în Capitolul IV §5 extinderea operației „+“ de la elementele lui R la clasele de echivalență în raport cu relația „ \equiv “, prin

$$(2) \quad \widehat{x} + \widehat{y} = \widehat{x+y}$$

O clasă de echivalență în raport cu relația „ \equiv “ este de forma $\widehat{x} = x + I = \{x + a \mid a \in I\}$.

În raport cu această operație mulțimea R/\equiv a claselor de echivalență are o structură de grup abelian. Elementul neutru al acestui grup este $\widehat{0} = I$.

Vom studia în continuare comportarea relației „ \equiv “ în raport cu înmulțirea.

3.1. Lemă. *Dacă I este un ideal bilateral al inelului $(R, +, \cdot)$ atunci relația de echivalență „ \equiv “ definită prin (1) este compatibilă cu operația „ \cdot “ din inelul R .*

Demonstratie. Fie $x \equiv x_1 \pmod{I}$ și $y \equiv y_1 \pmod{I}$. Există $a, b \in I$ astfel încât $x - x_1 = a \in I$ și $y - y_1 = b \in I$.

$$x \cdot y = (x_1 + a)(y_1 + b) = x_1 y_1 + a y_1 + x_1 b + ab$$

$$xy - x_1 y_1 = a y_1 + x_1 b + ab \in I$$

Ultima relație rezultă din faptul că I este ideal bilateral și arată tocmai $xy \equiv x_1 y_1 \pmod{I}$.

Ca și în cazul grupurilor, mulțimea claselor de echivalență în raport cu idealul I o vom nota cu R/I .

3.2. Teoremă. *Mulțimea R/I are o structură de inel în raport cu operațiile definite astfel:*

$$\widehat{x} + \widehat{y} = \widehat{x+y}$$

$$\widehat{x} \cdot \widehat{y} = \widehat{xy}$$

Demonstrație. Pentru a nu complica scrierea am folosit notațiile „+“ și „·“ pentru operațiile cu clase de echivalență ca și pentru operațiile cu elementele din R . Vom putea distinge operațiile din R de operațiile din R/I după natura elementelor cu care se lucrează.

După cum am amintit la începutul paragrafului, mulțimea R/I are o strucțură de grup abelian în raport cu „+“. Din lema 3.1 rezultă că operația multiplicativă cu clasele de echivalență este bine definită. Prin calcul verificăm că această operație este asociativă:

$$(\widehat{x} \cdot \widehat{y}) \cdot \widehat{z} = \widehat{xy} \cdot \widehat{z} = \widehat{(xy)z} = \widehat{x(yz)} = \widehat{x} \cdot \widehat{yz} = \widehat{x} \cdot (\widehat{y} \cdot \widehat{z})$$

și distributivă față de adunare:

$$\widehat{x} \cdot (\widehat{y} + \widehat{z}) = \widehat{x} \cdot \widehat{y + z} = \widehat{x(y + z)} = \widehat{xy + xz} = \widehat{xy} + \widehat{xz} = \widehat{x} \cdot \widehat{y} + \widehat{x} \cdot \widehat{z}.$$

$$(\widehat{x} + \widehat{y}) \cdot \widehat{z} = \widehat{x + y} \cdot \widehat{z} = \widehat{(x + y)z} = \widehat{xz + yz} = \widehat{xz} + \widehat{yz} = \widehat{x} \cdot \widehat{z} + \widehat{y} \cdot \widehat{z}.$$

Inelul $(R/I, +, \cdot)$ poartă numele de inel factor al inelului R în raport cu idealul său bilateral I .

Dacă R este inel unitar și 1 este elementul său unitate, atunci $\widehat{1}$ este element unitate al inelului R/I . În adevăr, pentru orice $\widehat{x} \in R/I$, deducem:

$$\widehat{x} \cdot \widehat{1} = \widehat{x \cdot 1} = \widehat{x} \text{ și } \widehat{1} \cdot \widehat{x} = \widehat{1 \cdot x} = \widehat{x}.$$

De asemenea, dacă R este inel comutativ, atunci printr-un calcul simplu putem arăta că și R/I este inel comutativ.

Aplicația $\varphi_I : R \rightarrow R/I$, definită prin:

$$\varphi_I(x) = \widehat{x}$$

este un morfism surjectiv de inele. În adevăr, pentru orice $x, y \in R$ deducem:

$$\varphi_I(x + y) = \widehat{x + y} = \widehat{x} + \widehat{y} = \varphi_I(x) + \varphi_I(y)$$

$$\varphi_I(x \cdot y) = \widehat{x \cdot y} = \widehat{x} \cdot \widehat{y} = \varphi_I(x) \cdot \varphi_I(y).$$

În plus, orice element din R/I este de forma $\widehat{x} = \varphi_I(x)$, $x \in R$.

Morfismul φ_I poartă numele de surjecție canonica a inelului R pe inelul său factor R/I . Nucleul acestui morfism este chiar idealul bilateral I :

$$\text{Ker } \varphi_I = \{x \in R \mid \varphi_I(x) = \widehat{0}\} = \{x \in R \mid \widehat{x} = x + I = I\} = I.$$

Dacă R este inel unitar, atunci φ_I este morfism unitar pentru că $\varphi_I(1) = \widehat{1}$. Un exemplu important de inel factor este prezentat în paragraful 5.

În stabilirea unor proprietăți ale inelelor, un rol important revine următoarelor rezultate care poartă numele de teoreme de izomorfism pentru inele.

4.1. Teorema fundamentală de izomorfism. *Dacă $f : A \rightarrow B$ este un morfism de inele, atunci există un izomorfism canonic.*

$$\theta : A/\text{Ker } f \rightarrow \text{Im } f$$

Demonstratie. Fie $\hat{x} = x + \text{Ker } f$ un element oarecare al inelului $A/\text{Ker } f$. Dacă $z \in \hat{x}$, atunci există $a \in \text{Ker } f$ astfel încât

$$z = x + a \text{ și } f(z) = f(x + a) = f(x) + f(a) = f(x).$$

Egalitatea $f(z) = f(x)$, pentru $z \in \hat{x}$ arată că putem defini

$$\theta : A/\text{Ker } f \rightarrow \text{Im } f$$

punind $\theta(\hat{x}) = f(x)$. Se observă că aplicația θ este surjectivă. În plus, dacă $\theta(\hat{x}) = \theta(\hat{z})$, atunci $f(x) = f(z)$, $f(x - z) = 0$, $x - z \in \text{Ker } f$ și $\hat{x} = \hat{z}$, adică θ este chiar o aplicație bijectivă. Pentru $\hat{x}, \hat{z} \in A/\text{Ker } f$, oarecare deducem:

$$\begin{aligned} \theta(\hat{x} + \hat{z}) &= \theta(\hat{x} + \hat{z}) = f(x + z) = f(x) + f(z) = \theta(\hat{x}) + \theta(\hat{z}) \\ \theta(\hat{x} \cdot \hat{z}) &= \theta(\hat{x} \cdot \hat{z}) = f(x \cdot z) = f(x) \cdot f(z) = \theta(\hat{x}) \cdot \theta(\hat{z}). \end{aligned}$$

Deci θ este morfism bijectiv de inele, prin urmare θ este un izomorfism.

4.2. Observație. Izomorfismul θ este singurul morfism de inele de la $A/\text{Ker } f$ cu valori în $\text{Im } f$ care face următoarea diagramă comutativă:

$$\begin{array}{ccc} A & \xrightarrow{\bar{f}} & \text{Im } f \\ & \varphi \searrow \nearrow \theta & \\ & A/\text{Ker } f & \end{array}$$

adică $\bar{f} = \theta \circ \varphi$, unde φ este surjecția canonică, iar \bar{f} este restricția lui f la $\text{Im } f$ ($\bar{f}(x) = f(x)$, pentru orice $x \in A$). În adevăr, pentru $x \in A$, $\theta(\varphi(x)) = \theta(\hat{x}) = f(x) = \bar{f}(x)$ sau $\theta \circ \varphi = \bar{f}$. Dacă $\alpha : A/\text{Ker } f \rightarrow \text{Im } f$ este un morfism de inele, care face diagrama comutativă, adică $\bar{f} = \alpha \circ \varphi$, atunci pentru orice $\hat{x} \in A/\text{Ker } f$

$$\alpha(\hat{x}) = \alpha(\varphi(x)) = (\alpha \circ \varphi)(x) = \bar{f}(x) = f(x) = \theta(\hat{x})$$

deci $\alpha = \theta$.

§ 5. Corp. Subcorp. Morfisme de corpuri

5.1. Definiție. Un inel unitar K cu $1 \neq 0$ se numește *corp* dacă orice element nenul al său este inversabil, relativ la înmulțire.

Dacă, în plus, înmulțirea este comutativă corpul se numește *comutativ*.

Pentru un corp K se evidențiază două grupuri. Astfel, avem grupul aditiv al inelului $(K, +)$ și grupul multiplicativ (K^*, \cdot) al elementelor nenule ale corpului. Aceste două structuri se numesc grupurile subiacente corpului K .

Dacă K este un corp, atunci grupul elementelor inversabile ale sale este $U(K) = K \setminus \{0\} = K^*$.

5.2. Exemple

1) Multimile \mathbb{Q} , \mathbb{R} cu operațiile obișnuite de adunare și înmulțire sunt corpuri comutative.

2) Fie p un număr natural prim. Atunci inelul \mathbb{Z}_p al claselor de resturi modulo p este corp.

Într-adevăr, dacă $\hat{a} \in \mathbb{Z}_p$, $\hat{a} \neq 0$, atunci $(\hat{a}, p) = 1$ și conform propoziției 2.6, rezultă că \hat{a} este element inversabil în \mathbb{Z}_p .

3) Multimea

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$$

împreună cu operațiile de adunare și înmulțire a numerelor formează un corp.

Dacă $a + b\sqrt{2}$, $c + d\sqrt{2} \in \mathbb{Q}(\sqrt{2})$, atunci

$$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \text{ și}$$

$$(a + b\sqrt{2})(c + d\sqrt{2}) = (ac + 2bd) + (ad + bc)\sqrt{2}$$

sunt operațiile algebrice în raport cu care se verifică cu ușurință că $\mathbb{Q}(\sqrt{2})$ este un corp.

Observăm doar că, dacă $a + b\sqrt{2} \neq 0$ atunci

$$(a + b\sqrt{2})^{-1} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}.$$

5.3. Propoziție. Un inel unitar nenul R este corp dacă și numai dacă $\{0\}$ și R sunt singurele ideale la stânga și ideale la dreapta ale lui R .

Demonstrație. Din propoziția 1.14, rezultă că într-un corp $\{0\}$ și R sunt și singurele ideale la stânga și ideale la dreapta. Reciproc, dacă presupunem că singurele ideale la stânga și ideale la dreapta ale lui R sunt $\{0\}$ și R atunci fie $a \in R$, $a \neq 0$.

Avem că idealul la stînga Ra este nenul și deci $Ra=R$ adică există $b \in R$ astfel încît $ba=1$. La fel, idealul la dreapta aR este nenul și deci $aR=R$, adică există $c \in R$ astfel încît $ac=1$. Din relațiile $ba=1$ și $ac=1$, rezultă $b=b \cdot 1=b(ac)=(ba)c=1 \cdot c=c$ și deci $ab=ba=1$, adică a este inversabil. Cum orice element nenul din K este inversabil, rezultă că inelul K este corp.

Din 1.7. rezultă că un corp nu are divizori ai lui zero diferiți de zero.

5.4. Definiție. Fie K un corp. O submulțime nevidă F a lui K se numește subcorp al lui K dacă operațiile algebrice de pe K induc pe F operații algebrice față de care F este un corp. Dacă F este un subcorp al lui K , atunci K se numește extindere a lui F .

5.5. Propoziție. Fie K un corp și $F \subset K$ o submulțime nevidă a sa. Atunci F este un subcorp al lui K , dacă și numai dacă:

- 1° oricare ar fi $x, y \in F$, rezultă $x-y \in F$;
- 2° oricare ar fi $x, y \in F$, $y \neq 0$, rezultă $xy^{-1} \in F$.

Demonstrație. Echivalența celor două afirmații din propoziție este imediată. Se poate vedea în acest sens și propoziția 1.9.

Observăm că elementul unitate din K este element unitate și pentru F .

5.6. Exemple.

- 1) Fie K un corp. Atunci K este evident subcorp al lui K .
- 2) $\mathbb{Q} \subset \mathbb{R}$ este un subcorp.
- 3) $\mathbb{Q}(\sqrt{2})$ este în mod clar un subcorp al corpului \mathbb{R} al numerelor reale (vezi 5.2. ex. 3)).
- 4) \mathbb{Z}_p și \mathbb{Q} nu au alte subcorpuri în afară de ele însese.

Într-adevăr, dacă $F \subseteq \mathbb{Z}_p$ este un subcorp al lui \mathbb{Z}_p , atunci F este un subgrup al grupului său aditiv. Cum $|\mathbb{Z}_p|$ este egal cu numărul prim p , după teorema lui Lagrange rezultă că singurele subgrupuri ale lui $(\mathbb{Z}_p, +)$ sunt: subgrupul nul și \mathbb{Z}_p însuși. Deci singurul subcorp al corpului \mathbb{Z}_p este însuși \mathbb{Z}_p .

Fie acum $F \subseteq \mathbb{Q}$ un subcorp al lui \mathbb{Q} . Cum $1 \in F$, rezultă că oricare ar fi $n \in \mathbb{N}$, avem $\underbrace{1+1+\dots+1}_{n \text{ ori}} \in F$. Dar $0 \in F$ implică $0-n \in F$ cu $n \in \mathbb{N}$ și

deci $\mathbb{Z} \subseteq F$. Dacă $\frac{m}{n} \in \mathbb{Q}$, atunci $\frac{m}{n} = mn^{-1}$, unde $m, n \in \mathbb{Z} \subseteq F$ și din definiția subcorpului rezultă că $mn^{-1} \in F$. Astfel $\mathbb{Q} \subseteq F$, adică $\mathbb{Q} = F$ și deci singurul subcorp al lui \mathbb{Q} este el însuși.

5.7. Definiție. Fie K și K' două corpuri. Se numește *morfism de corpuri* de la K la K' o funcție $f: K \rightarrow K'$, astfel încît să fie satisfăcute următoarele condiții:

- 1) $f(a+b) = f(a) + f(b)$, oricare ar fi $a, b \in K$.
- 2) $f(ab) = f(a)f(b)$, oricare ar fi $a, b \in K$.
- 3) $f(1) = 1$.

Deci $f: K \rightarrow K'$ este un morfism de corpuri dacă este un morfism unitar de inele.

Deoarece f este, în particular, un morfism de grupuri de la K^* la K'^* , rezultă că $\varphi(a^{-1}) = \varphi(a)^{-1}$, pentru orice $a \neq 0$.

5.8. Observație. Orice morfism de corpuri este injectiv.

Într-adevăr, fie $f: K \rightarrow K'$ morfism de corpuri și $a, b \in K$ astfel încît $a \neq b$. Atunci $a-b \neq 0$ și deci există $c \in K$ astfel încît $(a-b)c=1$, de unde $f((a-b)c) = f(1)$ sau $f(a-b)f(c)=1$. Prin urmare, este clar că $f(a-b) \neq 0$ adică $f(a)-f(b) \neq 0$ sau $f(a) \neq f(b)$.

5.9. Definiție. Fie K un corp comutativ. Atunci ordinul elementului $1 \in K$ în grupul aditiv $(K, +)$ poate fi finit sau infinit. Spunem că, corpul K are caracteristica zero (sau este de caracteristică zero) dacă $\text{ord}(1)$ este infinit și spunem că este de caracteristică n , dacă $\text{ord}(1)=n$.

Din definiția ordinului unui element într-un grup rezultă că, corpul K are caracteristica zero și scriem că $K=0$ dacă $m \cdot 1 \neq 0$, oricare ar fi m număr întreg pozitiv. De asemenea, caracteristica n a unui corp K este cel mai mic număr întreg pozitiv astfel încât $n \cdot 1=0$. În acest caz scriem că $K=n$.

5.10. Propoziție. Caracteristica unui corp este 0 sau un număr prim.

Demonstrație. Fie K un corp. Dacă car $K=0$ nu mai este nimic de demonstrat. Dacă car $K=n$, $n \neq 0$, să presupunem prin absurd că n nu este număr prim. Atunci $n=pq$ cu $1 < p < n$ și $1 < q < n$, iar $0=n \cdot 1=(p \cdot q)1=(p \cdot 1)(q \cdot 1)$. Deoarece un corp nu are divizori ai lui zero, atunci $p \cdot 1=0$ sau $q \cdot 1=0$, ceea ce contrazice alegerea lui n .

Observăm că dacă $E \supseteq K$ este o extindere comutativă a unui corp comutativ K , atunci E și K au aceeași caracteristică.

5.11. Exemple.

1) Corpurile \mathbb{Q} , \mathbb{R} au caracteristica zero.

2) Dacă p este un număr prim, corpul \mathbb{Z}_p este în mod clar un corp de caracteristică p .

3) Fie mulțimea $K=\{(a, b) \mid a, b \in \mathbb{Z}_2\}$ pe care definim operațiile algebrice:

$$(a, b) + (\hat{a}, \hat{b}) = (a+\hat{a}, b+\hat{b}),$$

$$(a, b)(\hat{a}, \hat{b}) = (a\hat{a}+b\hat{b}, a\hat{b}+b\hat{a}+\hat{b}\hat{b})$$

oricare ar fi $(a, b), (\hat{a}, \hat{b}) \in K$.

Se verifică ușor că mulțimea K împreună cu cele două operații devine un corp comutativ.

Elementele acestuia sunt: $(\hat{0}, \hat{0})$, $(\hat{1}, \hat{0})$, $(\hat{0}, \hat{1})$, $(\hat{1}, \hat{1})$, adică avem de-a face cu un corp cu 4 elemente. Funcția $\varphi: \mathbb{Z}_2 \rightarrow K$, definită prin $\varphi(\hat{a})=(\hat{a}, \hat{0})$ este un morfism de corpuri. Pe baza acestuia putem identifica elementul a din \mathbb{Z}_2 cu perechea $(\hat{a}, \hat{0})$ din K . Astfel, \mathbb{Z}_2 se identifică cu subcorpul $K'=\{(\hat{0}, \hat{0}), (\hat{1}, \hat{0})\}$ al lui K . Să notăm $\alpha=(0, \hat{1})$ și atunci, ținând cont de cele de mai înainte elementele corpului K sunt:

$$(\hat{0}, \hat{0})=\hat{0}, (\hat{1}, \hat{0})=\hat{1}, (\hat{0}, \hat{1})=\alpha \text{ și}$$

$(\hat{1}, \hat{1})=(\hat{1}, \hat{0})+(\hat{0}, \hat{1})=1+\alpha$. Deci $K=\{\hat{0}, \hat{1}, \alpha, \hat{1}+\alpha\}$, unde $\alpha\alpha=1+\alpha$ iar $\alpha(\hat{1}+\alpha)=\hat{1}$.

Acest corp având un subcorp izomorf cu corpul \mathbb{Z}_2 de caracteristică 2, are la rîndul său caracteristica 2.

5.12. Propoziție. Fie K un corp comutativ cu car $K=p$, $p \neq 0$.

Atunci avem:

$$1) pa=0,$$

$$2) (ab)^p=a^pb^p,$$

$$3) (a \pm b)^p=a^p+b^p \text{ (semnele se corespund), oricare ar fi } a, b \in K.$$

Demonstrație. 1) Avem $pa = p(1 \cdot a) = (p \cdot 1)a = 0 \cdot a = 0 \cdot 2$. Este evidentă.
 3) Observăm mai întâi că dacă p este un număr prim, coeficienții binomiali C_p^k , $1 \leq k \leq p-1$, sunt multiplii de p . Atunci dezvoltând $(x \pm y)^p$ după formula binomului lui Newton și având în vedere relația 1) avem $(a \pm b)^p = a^p \pm (-1)^p b^p$. Dacă $p \neq 2$, atunci p este impar și deci $(a \pm b)^p = a^p \pm b^p$. Dacă $p=2$, avem $(a \pm b)^2 = a^2 + b^2$ și cum $2b^2 = 0$, adică $b^2 = -b^2$, putem scrie $(a-b)^2 = a^2 - b^2$.

Observăm că relațiile 2) și 3) ale propoziției precedente, împreună cu cea evidentă $\varphi_p(1)=1$, arată că

$$\varphi_p : K \rightarrow K,$$

definită prin $\varphi_p(a) = a^p$, este un morfism de corpuri.

§ 6. Corpul numerelor complexe. Corpul cuaternionilor

6.1. *Corpul numerelor complexe.* Să ne propunem rezolvarea unei ecuații de gradul al doilea cu coeficienți în corpul \mathbb{R} al numerelor reale. Acest corp se dovedește insuficient de larg din punctul de vedere al existenței rădăcinilor oricărei ecuații de acest tip. De exemplu, ecuația $x^2 + 1 = 0$ nu are rădăcini reale. Se pune problema obținerii unui corp \mathbb{C} care să fie o extindere a corpului \mathbb{R} , astfel încât ecuațiile de gradul al doilea să aibă rădăcinile în \mathbb{C} .

Fie produsul cartezian

$$\mathbb{R} \times \mathbb{R} = \{(a, b) \mid a, b \in \mathbb{R}\}.$$

Considerind \mathbb{R} cu structura de grup aditiv, atunci $\mathbb{R} \times \mathbb{R}$, împreună cu operația algebrică de adunare:

$$(a, b) + (a', b') = (a+a', b+b'),$$

oricare ar fi $(a, b), (a', b') \in \mathbb{R} \times \mathbb{R}$, devine în mod clar un grup abelian (vezi VI, 2.7).

Vom defini pe $\mathbb{R} \times \mathbb{R}$ încă o operație, înmulțirea, punind pentru $(a, b), (a', b') \in \mathbb{R} \times \mathbb{R}$,

$$(a, b)(a', b') = (aa' - bb', ab' + a'b).$$

$\mathbb{R} \times \mathbb{R}$ împreună cu cele două operații algebrice, adunarea și înmulțirea, formează un corp comutativ. Am remarcat deja că $\mathbb{R} \times \mathbb{R}$ împreună cu adunarea este grup abelian, iar înmulțirea satisfac următoarele condiții:

- 1) este asociativă;
- 2) este distributivă față de adunare;
- 3) este comutativă;
- 4) are element neutru;
- 5) orice element nenul este inversabil.

Lăsăm ca exercițiu verificarea acestora, observînd că în demonstrații se folosesc proprietățile analoage ale înmulțirii și adunării numerelor reale.

Menționăm că elementul neutru este $(1, 0)$. De asemenea, fie $(a, b) \neq (0, 0)$ un element din $\mathbb{R} \times \mathbb{R}$, adică $a^2 + b^2 \neq 0$ și să arătăm că este inversabil. Dacă (x, y) este astfel încât $(a, b)(x, y) = (1, 0)$ atunci

$$(ax - by, ay + bx) = (1, 0).$$

De aici se obțin $ax - by = 1$ și $bx + ay = 0$, de unde $x = \frac{a}{a^2 + b^2}$ și $y = \frac{-b}{a^2 + b^2}$.

$$\text{Deci } (a, b)^{-1} = \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right).$$

Prin urmare, $\mathbb{R} \times \mathbb{R}$ împreună cu operațiile de adunare și înmulțire definite mai înainte formează un corp, care se notează cu \mathbb{C} și se numește *corpul numerelor complexe*.

Fiecare element al acestui corp se numește *număr complex*. Definim funcția

$$\varphi: \mathbb{R} \rightarrow \mathbb{C}, \text{ prin } \varphi(a) = (a, 0).$$

Este clar că φ este un morfism de coruri, deci injectiv.

Pe baza acestuia rezultă că \mathbb{R} este izomorf cu subcorpul $\mathbb{C}' = \{(a, 0) \mid a \in \mathbb{R}\}$ al corpului \mathbb{C} . Astfel putem identifica corpul \mathbb{R} al numerelor reale cu subcorpul \mathbb{C}' de numere complexe și numărul real a cu numărul complex $(a, 0)$. Așadar în loc de elementul $(a, 0)$ din \mathbb{C} vom scrie a .

Vom nota cu i numărul complex $(0, 1)$. Avem $i^2 = (0, 1)(0, 1) = (-1, 0) = -1$ și deci i este o rădăcină a ecuației $x^2 + 1 = 0$.

Fie acum $\alpha = (a, b)$ un element din \mathbb{C} . Atunci $\alpha = (a, b) = (a, 0) + (0, b) = (a, 0) + (b, 0)(0, 1) = a + bi$.

Deci orice număr complex $\alpha = (a, b)$ se scrie în mod unic sub forma $\alpha = a + bi$, numită formă algebraică a numărului complex α .

Vom indica acum un corp izomorf cu corpul \mathbb{C} al numerelor complexe și care astfel ne sugerează o nouă construcție a acestuia.

$$\text{Fie } \mathcal{X} = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R} \right\}.$$

Se verifică cu ușurință că adunarea și înmulțirea obișnuite a matricelor conferă acestei mulțimi o structură de corp comutativ. Funcția

$$\psi: \mathbb{C} \rightarrow \mathcal{X}, \text{ definită prin}$$

$$\psi(a+bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

ne dă un izomorfism între cele două coruri. Lăsăm ca exercițiu demonstrația afirmațiilor precedente.

6.2. *Corpul quaternionilor*. Fie inelul $\mathcal{M}(2, \mathbb{C})$ al matricelor pătratice de ordin 2, peste corpul \mathbb{C} și $H \subset \mathcal{M}(2, \mathbb{C})$, unde

$$H = \left\{ \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \mid \alpha, \beta \in \mathbb{C} \right\}.$$

H este un subinel al lui $\mathcal{M}(2, \mathbb{C})$.

Într-adevăr, ținând seama că suma, respectiv produsul conjugatilor a două numere complexe este conjugatul sumei respectiv produsul numerelor, avem,

$$1^\circ \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} - \begin{pmatrix} \gamma & \delta \\ -\bar{\delta} & \bar{\gamma} \end{pmatrix} = \begin{pmatrix} \alpha - \gamma & \beta - \delta \\ -\bar{\beta} + \bar{\delta} & \bar{\alpha} - \bar{\gamma} \end{pmatrix} =$$

$$\begin{pmatrix} \alpha - \gamma & \beta - \delta \\ -\beta + \delta & \alpha - \gamma \end{pmatrix} \in H \quad \text{și}$$

$$2 \cdot \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \begin{pmatrix} \gamma & \delta \\ -\bar{\delta} & \bar{\gamma} \end{pmatrix} = \begin{pmatrix} \alpha\gamma - \beta\bar{\delta} & \alpha\delta + \beta\bar{\gamma} \\ -\bar{\beta}\gamma - \bar{\alpha}\bar{\delta} & -\bar{\beta}\delta + \bar{\alpha}\bar{\gamma} \end{pmatrix} =$$

$$= \begin{pmatrix} \alpha\gamma - \beta\bar{\delta} & \alpha\delta + \beta\bar{\gamma} \\ -\alpha\bar{\delta} + \beta\bar{\gamma} & \alpha\gamma - \beta\bar{\delta} \end{pmatrix} \in H$$

oricare ar fi

$$\begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix}, \begin{pmatrix} \gamma & \delta \\ -\bar{\delta} & \bar{\gamma} \end{pmatrix} \in H.$$

Așadar H împreună cu adunarea și înmulțirea obișnuite a matricelor este la rîndul său un inel.

Matricea $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$ este elementul unitate al lui H .

Mai mult, vom arăta că H este corp. Într-adevăr, dacă $h = \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$,

atunci numărul real $\Delta = |\alpha|^2 + |\beta|^2$ este nenul. Inversul lui h este $h^{-1} =$

$$= \begin{pmatrix} \bar{\alpha} & -\bar{\beta} \\ \Delta & \Delta \end{pmatrix} \quad \text{după cum se vede ușor.}$$

Dacă H este un corp numit corpul cuaternionilor, elementele sale le vom numi cuaternioni.

Definim funcția

$$\varphi: \mathbb{R} \rightarrow H, \text{ prin } \varphi(a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix},$$

care este evident un morfism de corpuri, deci injectiv.

Acesta ne permite să identificăm numărul real a cu cuaternionul $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$.

$$\text{Dacă notăm } i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, k = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},$$

avem că $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$.

Se observă că H este un corp necomutativ.

Dacă $\alpha = a_0 + a_1i$ și $\beta = b_0 + b_1i$ sunt numere complexe putem scrie

$$\begin{aligned} \begin{pmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{pmatrix} &= \begin{pmatrix} a_0 + a_1i & b_0 + b_1i \\ -b_0 + b_1i & a_0 - a_1i \end{pmatrix} = \\ &= \begin{pmatrix} a_0 & 0 \\ 0 & a_0 \end{pmatrix} + \begin{pmatrix} a_1 & 0 \\ 0 & a_1 \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} + \begin{pmatrix} b_0 & 0 \\ 0 & b_0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} + \begin{pmatrix} b_1 & 0 \\ 0 & b_1 \end{pmatrix} \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = \\ &= a_0 + a_1i + b_0j + b_1k. \end{aligned}$$

Deci orice cuaternion $h \in H$, poate fi scris în mod unic sub forma $h = a + bi + cj + dk$, unde a, b, c, d sunt numere reale.

Este important să observăm că o ecuație cu coeficienți în corpul necomutativ H poate să aibă mai multe rădăcini decât gradul său. De exemplu i, j, k sunt rădăcini ale ecuației $x^2+1=0$.

După cum vom vedea, în cazul corpurilor comutative acest lucru nu este posibil. Mai precis, K fiind un corp comutativ, orice ecuație de grad n cu coeficienți în K , are în acesta cel mult n rădăcini.

§ 7. Corpul de fracții al unui domeniu de integritate

În capitolul IV, §5, plecînd de la inelul \mathbb{Z} al numerelor întregi am construit corpul \mathbf{Q} al numerelor raționale, astfel încît \mathbb{Z} să fie subinel al lui \mathbf{Q} .

Ne punem o problemă analoagă acesteia, considerînd în locul inelului \mathbb{Z} un domeniu de integritate oarecare.

Fie deci R un domeniu de integritate și R^* mulțimea elementelor nenule din R . Considerăm produsul direct de mulțimi

$$R \times R^* = \{(a, b) \mid a, b \in R, b \neq 0\}.$$

Pe mulțimea $R \times R^*$ definim relația binară „~“ astfel

$(a, b) \sim (c, d)$ dacă și numai dacă $ad = cb$.

Avem că „~“ este o relație de echivalență. Într-adevăr,

1° Dacă $(a, b) \in R \times R^*$, atunci $(a, b) \sim (a, b)$ deoarece $ab = ab$. Deci relația este reflexivă.

2° Fie $(a, b), (c, d) \in R \times R^*$ astfel încît $(a, b) \sim (c, d)$. Atunci $ad = cb$ sau $cb = ad$, adică $(c, d) \sim (a, b)$. Deci relația este tranzitivă.

3° Fie $(a, b), (c, d), (e, f) \in R \times R^*$ astfel încît $(a, b) \sim (c, d)$ și $(c, d) \sim (e, f)$. Atunci $ad = cb$ și $cf = ed$, de unde $adf = bcf = bdc$ și cum $d \neq 0$, iar R este domeniu de integritate egalitatea $adf = bde$ implică $af = be$ adică $(a, b) \sim (e, f)$. Deci relația este tranzitivă.

Relația de echivalență „~“ împarte mulțimea $R \times R^*$ în clase de echivalență. Clasa de echivalență a perechii (a, b) se numește *fracție rațională* și

se notează $\frac{a}{b}$. Atunci avem $\frac{a}{b} = \frac{c}{d}$ dacă și numai dacă $ad = cb$.

Fie $K(R) = R \times R^*/\sim$ mulțimea factor a lui $R \times R^*$ în raport cu relația de echivalență “~“. Pe $K(R)$ se definesc două operații algebrice, adunarea și înmulțirea, în raport cu care $K(R)$ devine un corp comutativ.

Dacă $\frac{a}{b}$ și $\frac{c}{d}$ sunt două fracții raționale, deoarece $b \neq 0$ și $d \neq 0$, atunci $bd \neq 0$ și deci există fracțiiile raționale $\frac{ad+cb}{bd}$ și $\frac{ac}{bd}$. Atunci vom pune prin definiție:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+cb}{bd} \quad \text{și}$$

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

oricare ar fi $\frac{a}{b}, \frac{c}{d} \in K(R)$.

Să arătăm că cele două operații algebrice de mai sus nu depind de alegera reprezentanților, adică sunt bine definite.

Într-adevăr, dacă $\frac{a}{b} = \frac{a'}{b'}$ și $\frac{c}{d} = \frac{c'}{d'}$, atunci $ab' = a'b$ și $cd' = c'd$. Rezultă

$ab'dd' = a'b'dd'$ și $cd'bb' = c'dbb'$, de unde $ab'dd' + cd'bb' = a'bdd' + c'dbb'$, sau încă $(ad + cb)b'd' = (a'd' + c'b')bd$. Deci $(ad + cb, bd) \sim (a'd' + c'b', b'd')$ adică

$$\frac{ad + cb}{bd} = \frac{a'd' + c'b'}{b'd'}$$

La fel, din $\frac{a}{b} = \frac{a'}{b'}$ și $\frac{c}{d} = \frac{c'}{d'}$ avem $ab' = a'b$ și $cd' = c'd$, de unde $ab'cd' = a'b'c'd$ sau $(ac)(b'd') = (a'c')(bd)$. Deci $(ac, bd) \sim (a'c', b'd')$ adică

$$\frac{ac}{bd} = \frac{a'c'}{b'd'}$$

Astfel am arătat că adunarea și înmulțirea sunt bine definite.

Punem $0 = \frac{0}{1}$ și $1 = \frac{1}{1}$. Observăm că $0 = \frac{0}{b}$ și $1 = \frac{b}{b}$ oricare ar fi $b \in R^*$,

Adunarea și înmulțirea fracțiilor raționale au proprietățile:

$$1^\circ \quad \left(\frac{a}{b} + \frac{c}{d} \right) + \frac{e}{f} = \frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f} \right),$$

$$2^\circ \quad \frac{a}{b} + \frac{c}{d} = \frac{c}{d} + \frac{a}{b},$$

$$3^\circ \quad \frac{a}{b} + 0 = \frac{a}{b},$$

$$4^\circ \quad \frac{a}{b} + \frac{-a}{b} = 0,$$

$$5^\circ \quad \left(\frac{a}{b} \cdot \frac{c}{d} \right) \cdot \frac{e}{f} = \frac{a}{b} \left(\frac{c}{d} \cdot \frac{e}{f} \right),$$

$$6^\circ \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{c}{d} \cdot \frac{a}{b},$$

$$7^\circ \quad \frac{a}{b} \left(\frac{c}{d} + \frac{e}{f} \right) = \frac{a}{b} \cdot \frac{c}{d} + \frac{a}{b} \cdot \frac{e}{f};$$

$$8^\circ \quad \frac{a}{b} \cdot 1 = \frac{a}{b},$$

oricare ar fi $\frac{a}{b}, \frac{c}{d}, \frac{e}{f} \in K(A)$.

Verificarea acestora o omitem, deoarece este complet analoagă cu cea dată în cap. IV, §5, cînd am demonstrat proprietățile adunării și înmulțirii numerelor raționale.

Dacă acum $\frac{a}{b} \neq 0$, atunci $a \neq 0$ și deci există fracția rațională $\frac{b}{a} \in K(A)$.

Avem $\frac{a}{b} \cdot \frac{b}{a} = \frac{ab}{ab} = \frac{1}{1} = 1$. Așadar are loc

9° oricare ar fi $\frac{a}{b} \neq 0$, există $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$.

Deci $K(A)$ împreună cu adunarea și înmulțirea definite mai înainte are o structură de corp comutativ, numit *corpul de fracții* al domeniului de integritate A .

Fie funcția $j: R \rightarrow K(R)$, definită prin $j(a) = \frac{a}{1}$.

Avem $j(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = j(a) + j(b)$,

$j(ab) = \frac{ab}{1} = \frac{a}{1} \cdot \frac{b}{1} = j(a) \cdot j(b)$ și

$j(1) = \frac{1}{1} = 1$.

Deci j este un morfism unitar de inele. Mai mult, dacă $a, b \in A$ și $j(a) = j(b)$,

atunci $j(a-b) = 0$ sau $\frac{a-b}{1} = 0 = \frac{0}{1}$, de unde $(a-b) \cdot 1 = 1 \cdot 0 = 0$, adică $a = b$.

Astfel j este morfism injectiv de inele care ne dă un izomorfism al inelului

R pe subinelul $R' = \left\{ \frac{a}{1} \mid a \in R \right\}$ al lui $K(R)$. Acest izomorfism ne permite

identificarea lui R cu R' , și a elementului a cu fracția rațională $\frac{a}{1}$. Vom scrie

$a = \frac{a}{1}$. Atunci dacă $\frac{a}{b} \in K(R)$, putem scrie $\frac{a}{b} = \frac{a}{1} \cdot \frac{1}{b} = \frac{a}{1} \left(\frac{b}{1}\right)^{-1} = ab^{-1}$.

Pentru $R = \mathbb{Z}$ prin procedeul descris se obține evident $K(R) = \mathbf{Q}$.

§ 2. Proprietăți aritmetice ale inelelor de polinoame

Prezentăm o extensie a algoritmului de împărțire a polinoamelor cu coeficienți într-un corp.

Teorema 2.1 (a împărțirii cu rest). *Fie A un domeniu de integritate, $f, g \neq 0$ două polinoame din $A[X]$ astfel încât coefficientul termenului de grad maxim al lui g să fie inversabil în A . Atunci există polinoamele q și r din $A[X]$, unic determinate, astfel încât*

$$f = gq + r \text{ și } \text{grad}(r) < \text{grad}(g).$$

Demonstrație. Procedăm prin inducție după gradul lui f . Fie m gradul lui f iar n gradul lui g . Dacă $\text{grad}(f) = m < n = \text{grad}(g)$, atunci $q = 0$ și $r = f$. Dacă $m \geq n$, fie a_m și b_n coeficienții termenilor de grad maxim al lui f , respectiv al lui g . Prin ipoteză b_n este inversabil. Atunci fie

$$f - (a_m b_n^{-1}) X^{m-n} g = f_1.$$

Deoarece coeficienții lui X^m în f și în $(a_m b_n^{-1}) X^{m-n} g$ sunt egali, este clar că $\text{grad}(f_1) < \text{grad}(f)$. Prin urmare, după ipoteza inducției, există polinoamele q_1 și r_1 din $A[X]$ astfel încât

$$f_1 = gq_1 + r_1, \text{ unde } \text{grad}(r_1) < \text{grad}(g).$$

Atunci

$$f = a_m b_n^{-1} X^{m-n} g + gq_1 + r_1 = g(a_m b_n^{-1} X^{m-n} + q_1) + r_1,$$

unde $\text{grad}(r_1) < \text{grad}(g)$. Deci, $f = gq + r$, unde $\text{grad}(r) < \text{grad}(g)$, $q = a_m b_n^{-1} X^{m-n} + q_1$ iar $r = r_1$.

Să demonstrăm unicitatea lui q și r . Într-adevăr, dacă avem încă $f = gq' + r'$, unde $\text{grad}(r') < \text{grad}(g)$, atunci rezultă $g(q - q') = r' - r$, unde $\text{grad}(r' - r) < \text{grad}(g)$ și $g \neq 0$. Cum b_n este inversabil, deci nu este divizor al lui zero în A , dacă $q \neq q'$, rezultă că $\text{grad}(g(q - q')) \geq \text{grad}(g)$. Așadar, gradul polinomului din membrul întâi al egalității $g(q - q') = r' - r$ este $\geq n$, iar al celui din membrul al doilea este $< n$ și se obține contradicție. Deci, în mod necesar $q = q'$ și $r = r'$. Polinomul r poate fi nul (în acest caz, după convenția făcută, gradul său este $-\infty$).

Din această teoremă rezultă evident :

Corolarul 2.2. *Fie K un corp comutativ și $f, g \neq 0$ două polinoame din $K[X]$. Atunci există polinoamele q și r din $K[X]$, unic determinate, astfel încât*

$$f = gq + r \text{ și } \text{grad}(r) < \text{grad}(g).$$

Polinomul q se numește *cîtul* împărțirii lui f la g iar r , *restul* împărțirii.

Vom da acum câteva fapte referitoare la divizibilitate în inele de polinoame. Presupunem în cele ce urmează că A este

un domeniu de integritate. Atunci $A[X]$ este domeniu de integritate (vezi propoziția 1.2).

Fie f și g două polinoame din $A[X]$. Spunem că f divide g (în inelul $A[X]$) dacă există $h \in A[X]$ astfel încât $g = fh$. Dacă f divide g , scriem $f|g$; în caz contrar, spunem că f nu divide g în inelul $A[X]$. Când f divide g , se mai spune că g se divide prin f sau că g este un *multiplu* de f , sau, încă, f este un *divizor* al lui g (în inelul $A[X]$).

Propoziția 2.3. *Relația de divizibilitate pe $A[X]$ are proprietățile :*

- 1) $f|f$, oricare ar fi $f \in A[X]$;
- 2) dacă $f|g$ și $g|h$, atunci $f|h$, oricare ar fi $f, g, h \in A[X]$;
- 3) dacă $f|g_1$ și $f|g_2$, atunci $f|g_1h_1 + g_2h_2$, oricare ar fi h_1, h_2 din $A[X]$.

Demonstrația acestei propoziții este imediată.

Amintim (vezi propoziția 1.3) că elementele inversabile din $A[X]$ coincid cu elementele inversabile din A .

Fie $f, g \in A[X]$. Spunem că f este *asociat* în divizibilitate cu g și scriem $f \sim g$ dacă $f|g$ și $g|f$ în inelul $A[X]$.

Relația de asociere în divizibilitate este evident o relație de echivalență (vezi § 3, cap. II), adică este reflexivă, simetrică și tranzitivă.

Propoziția 2.4. *Fie A un domeniu de integritate și $A[X]$ inelul polinoamelor peste A . Dacă f, g sunt două polinoame din $A[X]$, atunci $f \sim g$ dacă și numai dacă există $a \in A$, a inversabil, astfel încât $f = ag$.*

Demonstrație. Presupunem $f \neq 0$ și $g \sim f$. Cum $f|g$ și $g|f$, rezultă $g = fh_1$ și $f = gh_2$ cu $h_1, h_2 \in A[X]$. Așadar, $f = fh_1h_2$, adică $f(1 - h_1h_2) = 0$. Cum $f \neq 0$ și inelul $A[X]$ este domeniu de integritate, rezultă $1 - h_1h_2 = 0$ sau $h_1h_2 = 1$. Deci h_1, h_2 sunt inversabile în $A[X]$ și conform propoziției 1.3 rezultă că h_1, h_2 sunt elemente din A inversabile. Deci, $f = gh_2$ cu $h_2 \in A$ inversabil. Reciproc, fie $f = ag$ cu $a \in A$ inversabil. Atunci $g = bf$, unde $b \in A$ este inversul lui a și deci $g|f$ și $f|g$, de unde $f \sim g$. Dacă $f = 0$, atunci și $g = 0$ și afirmația din enunț este evidentă.

Definiția 2.1. Fie A un domeniu de integritate și f, g două polinoame din $A[X]$. Un polinom $d \in A[X]$ se numește cel

mai mare divizor comun (c.m.m.d.c.) al lui f și g dacă sunt îndeplinite condițiile :

1° $d|f$ și $d|g$;

2° dacă $h \in A[X]$ iar $h|f$ și $h|g$, atunci $h|d$.

Dacă d' este un alt polinom din $A[X]$ care verifică 1° și 2°, rezultă că $d|d'$ și $d'|d$, deci $d \sim d'$. După propoziția precedentă, avem că există $a \in A$ inversabil cu $d' = ad$. Așadar, cel mai mare divizor comun a două polinoame din $A[X]$, în cazul că există, este unic, mai puțin o asociere în divizibilitate. În general, se alege unul dintre aceștia ca fiind cel mai mare divizor comun al polinoamelor f și g și se notează prin (f, g) .

Fie K un corp comutativ. Printre polinoamele asociate în divizibilitate cu un polinom dat există unul singur care este unitar, adică are coeficientul termenului de grad maxim egal cu 1. În acest caz, f și g fiind două polinoame din $K[X]$, vom nota prin (f, g) acel polinom unitar care este un cel mai mare divizor comun al lor. Cum pentru $f = g = 0$ polinomul (f, g) nu poate fi definit ca mai sus, convenim să punem în acest caz $(0, 0) = 0$.

Vom arăta în continuare că orice două polinoame din inelul $K[X]$ (K fiind un corp comutativ) au un cel mai mare divizor comun. Dacă $f|g$, atunci $(f, g) = f$; în particular, $(f, 0) = f$.

Teorema 2.5. *Fie $K[X]$ inelul polinoamelor cu coeficienți într-un corp comutativ K . Pentru orice două polinoame f, g din $K[X]$ există cel mai mare divizor comun al lor. Mai mult, dacă $d = (f, g)$, atunci există polinoamele $h_1, h_2 \in K[X]$ astfel încât*

$$d = fh_1 + gh_2.$$

Demonstrație. Dacă $f = g = 0$, teorema este evidentă. Fie $f \neq 0$ sau măcar $g \neq 0$ și fie

$$I = \{fu + gv \mid u, v \in A[X]\}.$$

Dacă $h|f$ și $h|g$, conform propoziției 2.3, 3), rezultă că $h|fu + gv$, oricare ar fi u, v din $A[X]$. Deci orice divizor al lui f și g divide orice element din I . Întrucât $f = f \cdot 1 + g \cdot 0$ și $g = f \cdot 0 + g \cdot 1$, rezultă că $f, g \in I$. Deci I conține elemente nenule. Atunci mulțimea

$$D_{f,g} = \{\text{grad } (h) \mid h \in I, h \neq 0\}$$

este o submulțime nevidă de numere naturale.

Fie $d = fh_1 + gh_2 \in I$ astfel încât grad (d) să fie cel mai mic număr natural din $D_{f,g}$. Să arătăm că $d = (f, g)$. Deoarece $d \in I$, orice divizor al lui f și g divide pe d , deci este verificată, condiția 2° din definiția 2.1. Să probăm că d are și proprietatea 1° a aceleiași definiții. Cum $d \neq 0$, după teorema 2.1 există $q, r \in A[X]$ astfel încât

$$f = dq + r \text{ și } \text{grad}(r) < \text{grad}(d).$$

Avem

$$r = f - dq = f - (fh_1 + gh_2)q = f(1 - h_1q) + g(-h_2q) \in I.$$

Intrucît $d \in I$ și este astfel încât grad (d) să fie minim în $D_{f,g}$, iar $\text{grad}(r) < \text{grad}(d)$, rezultă în mod necesar $r = 0$. Așadar, $f = dq$ și deci $d|f$. Analog, se arată că $d|g$. Deci $d = (f, g)$ și din demonstrație avem că

$$d = fh_1 + gh_2 \text{ cu } h_1, h_2 \in A[X].$$

Definiția 2.2. Două polinoame f și g din $K[X]$ se numesc prime între ele (sau relativ prime), dacă $(f, g) = 1$.

Avem că f și g sunt prime între ele dacă și numai dacă există h_1 și h_2 din $A[X]$:

$$fh_1 + gh_2 = 1.$$

O b s e r v a t i e. Există o metodă constructivă de calcul a celui mai mare divizor comun a două polinoame cunoscută sub numele de algoritmul lui Euclid. Noi nu ne oprim asupra ei.

§ 4. Polinoame ireductibile în inele de polinoame cu coeficienți într-un corp.

Descompunerea polinoamelor în factori ireductibili

Fie K un corp comutativ și $K[X]$ inelul polinoamelor de o ne-determinată cu coeficienți în K . Polinoamele inversabile din $K[X]$ coincid (v. propoziția 1.3.) cu elementele nenule din K .

Definiția 4.1. Un polinom p nenul și neinversabil se numește *ireductibil* dacă din $f|p$ rezultă $f \sim 1$ sau $f \sim p$.

Cu alte cuvinte, un polinom p nenul și neinversabil este ireductibil dacă singurii divizori ai săi sunt polinoamele inversabile și cele asociate în divizibilitate cu p (adică cele care diferă de p prin constante nenule) sau, încă, dacă p nu poate fi reprezentat ca produs de două polinoame din $K[X]$, ambele cu gradul strict mai mic decât grad (p).

Un polinom nenul și neinversabil care nu este ireductibil se numește *reductibil*.

Definiția 4.2. Un polinom q nenul și neinversabil din $K[X]$ se numește *prim* dacă, oricare ar fi f, g din $K[X]$, din $q|fg$ rezultă $q|f$ sau $q|g$.

Propoziția 4.1. *Un polinom din inelul $K[X]$ este ireductibil dacă și numai dacă este prim.*

Demonstrație. Fie p un polinom ireductibil și $p|fg$, $f, g \in K[X]$. Cum p este ireductibil, acesta nu are divizori decât polinoamele inversabile sau cele asociate cu p . Deci, $(p, f) \sim p$ sau $(p, f) = 1$. În primul caz, rezultă $p|f$. Dacă însă $(p, f) = 1$, atunci există $h_1, h_2 \in K[X]$ astfel încât $ph_1 + fh_2 = 1$, de unde, multiplicând cu g , avem $g = pgh_1 + fgh_2$. Or, cum $p|fg$, rezultă $p|pg + fg$, deci $p|g$. Reciproc, fie q un polinom prim și f un divizor al său, adică $q = fg$ cu $f, g \in K[X]$. Cum q este prim și $q|fg$, rezultă $q|f$ sau $q|g$. Dacă $q|f$ și cum $f|q$, rezultă $f \sim q$. Dacă însă $q|g$ și cum $g|q$, avem $g \sim q$ și deci $f \sim 1$. Așadar, q este ireductibil.

Teorema 4.2. *Orice polinom nenul și neinversabil din $K[X]$ este produsul unui număr finit de polinoame ireductibile. Mai mult, dacă $f \in K[X]$ cu $\text{grad}(f) \geq 1$ și*

$$f = p_1 p_2 \cdots p_m = p'_1 p'_2 \cdots p'_n,$$

unde p_i și p'_i sunt polinoame ireductibile în $K[X]$, atunci $m = n$ și există o permutare $\sigma \in \Sigma_n$ astfel încât

$$p_i \sim p'_{\sigma(i)}, \quad i = 1, 2, \dots, n.$$

Demonstrație. Să demonstrăm mai întii prima parte a teoremei. Fie pentru aceasta $f \in K[X]$. Dacă f este ireductibil, atunci totul este evident. Dacă nu, adică f este reductibil, există $g, h \in K[X]$ astfel încât $f = gh$, $1 \leq \text{grad}(g), \text{grad}(h) < \text{grad}(f)$. În acest caz, vom demonstra prin inducție după grad.

Presupunând adevărată proprietatea pentru toate polinoamele de grad mai mic ca cel al lui f , polinoamele g și h se descompun în produs finit de polinoame ireductibile și deci $f = gh$.

se descompune. Rămîne să demonstrăm partea a două a teoremei. Demonstrăm prin inducție după m . Dacă $m = 1$, atunci $f = p_1$ și deci $n = 1$ și $p'_1 = p_1$. Să presupunem proprietatea adevărată pentru polinoamele ce se descompun în $m - 1$ factori și să demonstrăm pentru f . Cum p_1 este prim (vezi propoziția 4.1) și $p_1 | p'_1 p'_2 \dots p'_n$, rezultă că există i astfel încât $p_1 | p'_i$. Renumerotînd termenii, dacă este necesar, putem presupune că $p_1 | p'_1$. Cum p'_1 este ireductibil, rezultă $p_1 \sim p'_1$ și deci $p'_1 = p_1 \alpha_1$, cu $\alpha \in K$, $\alpha \neq 0$. Din $p_1 p_2 \dots p_m = p'_1 p'_2 \dots p'_n$ obținem

$$p_1 p_2 \dots p_m = \alpha_1 p_1 p'_2 \dots p'_n$$

și deci

$$p_2 p_3 \dots p_m = p''_2 p''_3 \dots p''_n,$$

unde $p''_2 = \alpha_1 p'_2$ și $p''_j = p'_j$ sunt ireductibili. Din ipoteza inducției $m - 1 = n - 1$ și după o eventuală renumerotare a termenilor $p_j \sim p''_j$. Deci $m = n$ și $p_i \sim p'_i$, $1 \leq i \leq n$, după o eventuală renumerotare a factorilor. Dar a face o renumerotare a factorilor revine la o aplica o permutare indicilor acestora, așa că totul este demonstrat.

Fie f un polynom din $K[V]$:

POLINOAME SIMETRICE. TEOREMA FUNDAMENTALĂ A ALGEBREI

§ 1. Polinoame simetrice

Fie R un inel unitar comutativ și $R[X_1, X_2, \dots, X_n]$ inelul polinoamelor în nedeterminatele X_1, X_2, \dots, X_n . Să considerăm S_n grupul permutărilor de grad n și $\sigma \in S_n$ o permutare oarecare. Să notăm cu $u: R \rightarrow R[X_1, X_2, \dots, X_n]$ morfismul canonic, $u(a) = a$. Folosind proprietatea de universalitate a inelelor de polinoame există un unic morfism de inele $\sigma^*: R[X_1, X_2, \dots, X_n] \rightarrow R[X_1, X_2, \dots, X_n]$ astfel încât $\sigma^*(X_i) = X_{\sigma(i)}$, oricare ar fi $1 \leq i \leq n$, și diagrama

$$\begin{array}{ccc} R & \xrightarrow{u} & R[X_1, X_2, \dots, X_n] \\ & \searrow u & \swarrow \sigma^* \\ & R[X_1, X_2, \dots, X_n] & \end{array}$$

să fie comutativă, adică $\sigma^* \circ u = u$.

Faptul că diagrama este comutativă înseamnă că $\sigma^*(a) = a$, oricare ar fi $a \in R$.

De exemplu, dacă luăm polinomul $f = aX_1X_2X_3 + X_1^2X_3 + X_1X_2X_3^2$ $a \neq 0$, din $R[X_1, X_2, X_3]$ și $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, atunci $\sigma^*(f) = \sigma^*(a) \sigma^*(X_1) \sigma^*(X_2) \sigma^*(X_3) + (\sigma^*(X_1))^2 \sigma^*(X_3) + \sigma^*(X_1) \sigma^*(X_2) (\sigma^*(X_3))^2 = aX_3X_1X_2 + X_3^2X_2 + X_3X_1X_2^2$.

În general, dacă $f(X_1, X_2, \dots, X_n)$ este un polinom din $R[X_1, X_2, \dots, X_n]$, atunci

$$\sigma^*(f(X_1, X_2, \dots, X_n)) = f(X_{\sigma(1)}, X_{\sigma(2)}, \dots, X_{\sigma(n)})$$

sau, dacă scriem

$$f = \sum_{i_1, i_2, \dots, i_n=0}^{k_1, k_2, \dots, k_n} a_{i_1 i_2 \dots i_n} X_1^{i_1} X_2^{i_2} \dots X_n^{i_n},$$

atunci

$$\sigma^*(f) = \sum_{i_1, i_2, \dots, i_n=0}^{k_1, k_2, \dots, k_n} a_{i_1 i_2, \dots, i_n} X_{\sigma(1)}^{i_1} X_{\sigma(2)}^{i_2} \dots X_{\sigma(n)}^{i_n}.$$

Este ușor de văzut că dacă $f \in R[X_1, X_2, \dots, X_n]$, sunt adevărate proprietățile:

1° Dacă $\sigma, \tau \in S_n$, atunci $(\sigma \circ \tau)^*(f) = \sigma^*(\tau^*(f))$,

2° Dacă $e \in S_n$ este permutarea identică, atunci $e^*(f) = f$.

3° Dacă $\sigma \in S_n$, atunci σ^* este un izomorfism de inele de la $R[X_1, X_2, \dots, X_n]$ în el însuși, inversul său fiind $(\sigma^{-1})^*$.

1.1. Definiție. Un polinom f din $R[X_1, X_2, \dots, X_n]$ se numește *simetric* dacă, pentru orice permutare σ din S_n avem $\sigma^*(f) = f$, adică polinomul rămîne invariant la orice permutare a nedeterminatelor sale.

Deoarece orice permutare este un produs de transpoziții, rezultă că polinomul f din $R[X_1, X_2, \dots, X_n]$ este simetric dacă și numai dacă f este invariant la toate transpozițiile din S_n .

Să notăm cu T mulțimea polinoamelor simetrice din inelul $R[X_1, X_2, \dots, X_n]$.

1.2. Propoziție. Mulțimea T a polinoamelor simetrice de n nedeterminate cu coeficienți într-un inel R formează un inel în raport cu adunarea și înmulțirea polinoamelor.

Demonstrație. Vom arăta că T este un subinel al inelului $R[X_1, X_2, \dots, X_n]$ și deci este la rîndul său un inel. Într-adevăr, dacă $f, g \in T$ și $\sigma \in S_n$ este o permutare oarecare, atunci:

$$\sigma^*(f-g) = \sigma^*(f) - \sigma^*(g) = f - g \text{ și}$$

$$\sigma^*(fg) = \sigma^*(f)\sigma^*(g) = fg,$$

adică $f-g$ și fg aparțin lui T .

Inelul T de mai înainte se numește inelul polinoamelor simetrice în n nedeterminate cu coeficienți în inelul R .

1.3. Lemă. Fie f un polinom din $R[X_1, X_2, \dots, X_n]$ de grad m și $f_i, 0 \leq i \leq m$, componente sale omogene. Dacă f este polinom simetric, atunci fiecare componentă omogenă f_i este polinom simetric.

Demonstrație. Polinomul f se scrie în mod unic sub forma $f = f_0 + f_1 + \dots + f_m$, unde fiecare f_i este un polinom omogen de grad i . Fie $\sigma \in S_n$ o permutare oarecare. Atunci $\sigma^*(f) = f$ și deci

$$f = \sigma^*(f) = \sigma^*(f_0) + \sigma^*(f_1) + \dots + \sigma^*(f_m).$$

Deoarece $\sigma^*(f_i), 0 \leq i \leq m$, este tot un polinom omogen de grad i , din unicitatea scrierii lui f ca sumă de polinoame omogene, rezultă $\sigma^*(f_i) = f_i$, oricare ar fi $i = 0, 1, \dots, m$. Deci polinoamele $f_i, 0 \leq i \leq m$, sunt simetrice.

1.4. Propoziție. Polinoamele $s_1, s_2, s_3, \dots, s_n$ din $R[X_1, X_2, \dots, X_n]$, definite prin:

$$s_1 = X_1 + X_2 + \dots + X_n = \sum_{i=1}^n X_i,$$

$$s_2 = X_1 X_2 + X_2 X_3 + \dots + X_{n-1} X_n = \sum_{1 \leq i < j \leq n} X_i X_j,$$

$$s_3 = X_1X_2X_3 + X_1X_2X_4 + \dots + X_{n-2}X_{n-1}X_n = \sum_{1 \leq i < j < k \leq n} X_iX_jX_k,$$

$$s_n = X_1X_2 \dots X_n$$

sunt simetrice.

Demonstrație. Fie polinomul $g(X) = (X - X_1)(X - X_2) \dots (X - X_n)$ din $R[X_1, X_2, \dots, X_n]$, care se mai scrie $g(X) = X^n - s_1X^{n-1} + s_2X^{n-2} - \dots + (-1)^ns_n$.

Dacă $\sigma \in S_n$ și $\sigma^*: R[X_1, X_2, \dots, X_n] \rightarrow R[X_1, X_2, \dots, X_n]$, definim $\sigma^{**}: R[X_1, X_2, \dots, X_n, X] \rightarrow R[X_1, X_2, \dots, X_n, X]$, prin $\sigma^{**}(X_i) = X_{\sigma(i)} = \sigma^*(X_i)$ oricare ar fi $i = 1, 2, \dots, n$, $\sigma^{**}(X) = X$ și $\sigma^{**}(a) = a$, oricare ar fi $a \in R$.

Atunci

$$\begin{aligned} \sigma^{**}(g(X)) &= \sigma^{**}((X - X_1)(X - X_2) \dots (X - X_n)) = \\ &= (X - X_{\sigma(1)})(X - X_{\sigma(2)}) \dots (X - X_{\sigma(n)}) = g(X). \end{aligned}$$

Pe de altă parte,

$$\begin{aligned} \sigma^{**}(g(X)) &= \sigma^{**}(X^n - s_1X^{n-1} + s_2X^{n-2} - \dots + (-1)^ns_n) = (\sigma^{**}(X))^n - \\ &- \sigma^{**}(s_1)(\sigma^{**}(X))^{n-1} + \sigma^{**}(s_2)(\sigma^{**}(X))^{n-2} - \dots + (-1)^n\sigma^{**}(s_n) = X^n - \\ &- \sigma^*(s_1)X^{n-1} + \sigma^*(s_2)X^{n-2} - \dots + (-1)^n\sigma^*(s_n). \end{aligned}$$

Din cele două expresii ale lui $\sigma^{**}(g(X))$ se obține $\sigma^*(s_i) = s_i$, $1 \leq i \leq n$, adică s_1, s_2, \dots, s_n sunt polinoame simetrice.

Polinoamele simetrice s_1, s_2, \dots, s_n se numesc *polinoame simetrice fundamentale* în nedeterminatele X_1, X_2, \dots, X_n .

§ 2. Teorema fundamentală a polinoamelor simetrice

2.1. Ordine lexicografică. Pentru un polinom f din $R[X_1, X_2, \dots, X_n]$ am definit ce înseamnă gradul său, observînd că poate avea mai mulți termeni al căror grad să fie egal cu gradul polinomului. De exemplu, fie polinomul

$$f = X_1^2X_2^3 + X_1X_2^3X_3 + X_1^2X_2 + X_1X_2X_3 + X_1^2X_3^2$$

din $R[X_1, X_2, X_3]$. Avem că grad $(f) = \text{grad}(X_1^2X_2^3) = \text{grad}(X_1X_2^3X_3) = 5$.

Prin urmare nu putem vorbi de un termen de grad maxim bine individualizat.

Pentru polinoamele de mai multe nedeterminate există un alt mod de a ordona termenii unui polinom care, în particular, pentru polinoamele într-o nedeterminată ne dă ordonarea obișnuită după puterile nedeterminatei. Această ordonare, numită lexicografică, este sugerată de metoda folosită la ordonarea cuvintelor într-un dicționar.

Să considerăm două monoame în n nedeterminate:

$$M_1 = aX_1^{i_1}X_2^{i_2} \dots X_n^{i_n}, \quad a \neq 0 \text{ și } M_2 = bX_1^{j_1}X_2^{j_2} \dots X_n^{j_n}, \quad b \neq 0.$$

Spunem că M_1 este *mai mare* (în ordine lexicografică) decât M_2 și scriem $M_1 > M_2$ dacă există un număr natural s , $1 \leq s \leq n$, astfel încît $i_1 = j_1, i_2 = j_2, \dots, i_{s-1} = j_{s-1}$, $i_s > j_s$. De exemplu, $X_1^8X_2 > X_1^5X_2^3X_3$ și $X_1^2X_2^4X_3 > X_1^2X_2^3X_3^7$.

Orice polinom nenul f din $R[X_1, X_2, \dots, X_n]$ se scrie în mod unic ca sumă de monoame diferite numite termenii lui f . Prin urmare, putem individualiza un termen al său (cu coeficient nenul) bine determinat care să fie cel mai mare în ordinea lexicografică. Acesta se numește *termenul principal* al polinomului.

2.2. Lemă. Fie monoamele $M_1 = X_1^{i_1} X_2^{i_2} \dots X_n^{i_n}$, $M_2 = X_1^{j_1} X_2^{j_2} \dots X_n^{j_n}$ astfel încât $M_1 > M_2$. Atunci

1) Oricare ar fi monomul $N_1 = X_1^{k_1} X_2^{k_2} \dots X_n^{k_n}$ rezultă $M_1 N_1 > M_2 N_2$.

2) Dacă $N_2 = X_1^{l_1} X_2^{l_2} \dots X_n^{l_n}$ este un alt monom astfel încât $N_1 > N_2$, rezultă $M_1 N_1 > M_2 N_2$.

Demonstrație. 1) Avem $M_1 N_1 = X_1^{i_1+k_1} X_2^{i_2+k_2} \dots X_n^{i_n+k_n}$, $M_2 N_1 = X_1^{j_1+k_1} X_2^{j_2+k_2} \dots X_n^{j_n+k_n}$. Deoarece $M_1 > M_2$, există s , $1 \leq s \leq n$, astfel încât $i_1 = j_1, \dots, i_{s-1} = j_{s-1}$, $i_s > j_s$ și deci $i_1 + k_1 = j_1 + k_1, \dots, i_{s-1} + k_{s-1} = j_{s-1} + k_{s-1}$, $i_s + k_s > j_s + k_s$, adică $M_1 N_1 > M_2 N_1$.

2) Folosind 1), avem $M_1 N_1 > M_1 N_2 > M_2 N_2$.

2.3. Propoziție. Dacă produsul termenilor principali a două polinoame este nenul, atunci acesta este termenul principal al produsului celor două polinoame.

Demonstrație. Fie f, g polinoame din $R[X_1, X_2, \dots, X_n]$ și $aX_1^{r_1} X_2^{r_2} \dots X_n^{r_n}$ respectiv $bX_1^{s_1} X_2^{s_2} \dots X_n^{s_n}$ termenii principali ai celor două polinoame, astfel încât $ab \neq 0$.

Din lema precedentă rezultă că $abX_1^{r_1+s_1} X_2^{r_2+s_2} \dots X_n^{r_n+s_n}$ este termenul principal al produsului celor două polinoame.

2.4. Lemă. Dacă $f \in R[X_1, X_2, \dots, X_n]$ este un polinom simetric, iar $aX_1^{k_1} X_2^{k_2} \dots X_n^{k_n}$ termenul său principal, atunci $k_1 \geq k_2 \geq \dots \geq k_n$.

Demonstrație. Să presupunem prin absurd că avem $k_i < k_{i+1}$ pentru un anumit i . Polinomul f fiind simetric, monomul

$$aX_1^{k_1} \dots X_{i+1}^{k_{i+1}} X_{i+1}^{k_{i+1}} \dots X_n^{k_n}$$

este un termen al lui f care ar fi mai mare decât termenul principal, contradicție.

2.5. Observație. Dacă $X_1^{k_1} X_2^{k_2} \dots X_n^{k_n}$ este un monom pentru care $k_1 \geq k_2 \geq \dots \geq k_n$, atunci există doar un număr finit de monoame $X_1^{m_1} X_2^{m_2} \dots X_n^{m_n}$, pentru care $m_1 \geq m_2 \geq \dots \geq m_n$ și $X_1^{k_1} X_2^{k_2} \dots X_n^{k_n} > X_1^{m_1} X_2^{m_2} \dots X_n^{m_n}$.

Într-adevăr, avem $r_1 \geq m_1$, deci există doar un număr finit de numere m_1 , iar pentru fiecare m_1 dat există cel mult m_1^{n-1} sisteme (m_2, m_3, \dots, m_n) pentru care $m_1 \geq m_2 \geq \dots \geq m_n$.

2.6. Teoremă. (Teorema fundamentală a polinoamelor simetrice). Fiecare polinom simetric f din $R[X_1, X_2, \dots, X_n]$ se poate exprima în mod unic cu un polinom de polinoame simetrice fundamentale. Cu alte cuvinte, există un unic polinom $g \in R[X_1, X_2, \dots, X_n]$ astfel încât

$$f = g(s_1, s_2, \dots, s_n),$$

unde s_1, s_2, \dots, s_n sunt polinoamele simetrice fundamentale.

Demonstrație. Fie $f \in R[X_1, X_2, \dots, X_n]$ de grad n , simetric. Polinomul f se scrie în mod unic sub forma

$$f = f_0 + f_1 + \dots + f_n,$$

unde fiecare f_i , $0 \leq i \leq n$, este un polinom omogen de grad i .

Fie $\sigma \in S_n$ o permutare oarecare. Atunci $\sigma^*(f) = f$ și deci

$$f = \sigma^*(f) = \sigma^*(f_0) + \sigma^*(f_1) + \dots + \sigma^*(f_n).$$

Deoarece $\sigma^*(f_i)$, $0 \leq i \leq n$, este tot un polinom omogen de grad i , din unicitatea scrierii lui f ca sumă de polinoame omogene rezultă $\sigma^*(f_i) = f_i$, oricare ar fi $i = 0, 1, \dots, n$. Deci f_i , $0 \leq i \leq n$, sunt polinoame simetrice omogene de grad i și atunci putem presupune, fără a restrînge generalitatea, că f este polinom simetric omogen. Fie grad $(f) = m$, iar $aX_1^{k_1} X_2^{k_2} \dots X_n^{k_n}$, $a \neq 0$, termenul său principal. Din lema precedentă rezultă $k_1 \geq k_2 \geq \dots \geq k_n$. Termenul principal al polinomului s_i este $X_1 X_2 \dots X_i$ și atunci după propoziția 2.3 termenul principal al lui $s_1^{k_1-k_2} s_2^{k_2-k_3} \dots s_{n-1}^{k_{n-1}-k_n} s_n^{k_n}$ este $X_1^{k_1} X_2^{k_2} \dots X_n^{k_n}$. Deci termenul principal al polinomului

$$f_1 = f - a s_1^{k_1-k_2} s_2^{k_2-k_3} \dots s_{n-1}^{k_{n-1}-k_n} s_n^{k_n}$$

este mai mic decât al lui f .

Continuăm acum procedeul pentru f_1 . Dacă $bX_1^{t_1} X_2^{t_2} \dots X_n^{t_n}$ este termenul său principal, fie

$$f_2 = f_1 - b s_1^{t_1-t_2} s_2^{t_2-t_3} \dots s_{n-1}^{t_{n-1}-t_n} s_n^{t_n}.$$

Termenul principal al lui f_2 este mai mic decât al lui f_1 și putem continua procedeul. Deoarece există doar un număr finit de monoame de grad m , procedeul se va sfîrși după un număr finit de pași. Astfel, se ajunge la o expresie a lui f ca polinom în s_1, s_2, \dots, s_n .

Să demonstrăm acum unicitatea. Pentru aceasta să arătăm că, dacă $h \in R[X_1, X_2, \dots, X_n]$ și $h(s_1, s_2, \dots, s_n) = 0$, atunci $h = 0$.

Fie deci $h(s_1, s_2, \dots, s_n) = \sum a_{i_1 i_2 \dots i_n} s_1^{i_1} s_2^{i_2} \dots s_n^{i_n} = 0$ și să arătăm că toți coeficienții $a_{i_1 i_2 \dots i_n}$ ai polinomului h sunt nuli. Presupunem prin absurd că există coeficienți nenuli și fie $a_{l_1 l_2 \dots l_n}$ unul dintre aceștia. Atunci polinomul $s_1^{l_1} s_2^{l_2} \dots s_n^{l_n}$ are termenul principal $X_1^{k_1} X_2^{k_2} \dots X_n^{k_n}$, unde $k_i = l_i + l_{i+1} + \dots + l_n$, al cărui grad este $m = \sum_{i=1}^n k_i = \sum_{i=1}^n l_i$. Mai mult, dacă $s_1^{l'_1} s_2^{l'_2} \dots s_n^{l'_n} \neq s_1^{l_1} s_2^{l_2} \dots s_n^{l_n}$, atunci termenii principali respectivi sunt diferenți. Într-adevăr, dacă $k_i = k'_i$ pentru $i = 1, 2, \dots, n$, atunci $l'_1 + l'_{i+1} + \dots + l'_n = l_1 + l_{i+1} + \dots + l_n$, pentru $i = 1, 2, \dots, n$, de unde rezultă $l'_i = l_i$ oricare ar fi $i = 1, 2, \dots, n$. Deci termenii principali în X_1, X_2, \dots, X_n ai diferențelor monoame distinse în s_1, s_2, \dots, s_n , care apar în expresia lui h , nu se reduc. Fie $X_1^{t_1} X_2^{t_2} \dots X_n^{t_n}$ cel mai mare termen principal. Atunci înlocuind s_1, s_2, \dots, s_n prin expresiile lor în X_1, X_2, \dots, X_n apare un polinom în X_1, X_2, \dots, X_n egal cu zero, care are un termen $a_{t_1 t_2 \dots t_n} X_1^{t_1} X_2^{t_2} \dots X_n^{t_n}$ nenul, ceea ce este în contradicție cu definiția polinomului nul.

2.7. Corolar. Fie K un subcorp al corpului F și $f \in K[X]$ un polinom de grad $(f) = n \geq 1$. Presupunem că f are rădăcinile x_1, x_2, \dots, x_n care aparțin lui F .

Atunci oricare ar fi, polinomul simetric $g(X_1, X_2, \dots, X_n)$ din $K[X_1, X_2, \dots, X_n]$, rezultă că $g(x_1, x_2, \dots, x_n)$ este din K .

Demonstrație. Deoarece $g(X_1, X_2, \dots, X_n)$ este simetric, există un polinom $h(X_1, X_2, \dots, X_n)$ cu coeficienți în K astfel încât $g = h(s_1, s_2, \dots, s_n)$. Având în

vedere relațiile lui Viète avem $s_i(x_1, x_2, \dots, x_n) \in K$, $1 \leq i \leq n$, și deci $g(x_1, x_2, \dots, x_n) = h(s_1(x_1, x_2, \dots, x_n), s_2(x_1, x_2, \dots, x_n), \dots, s_n(x_1, x_2, \dots, x_n))$ este un element din K .

2.8. Aplicație. Să se exprime ca polinom de polinoamele simetrice fundamentale, polinomul simetric

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

cu coeficienți reali.

Termenul principal al polinomului este $X_1^4 X_2^2$.

Atunci exponenții termenilor principali ai polinoamelor care vor rămâne după eliminarea succesivă a termenilor principali, ca în produsul descris în demonstrația teoremei 2.5, vor fi

$$(4, 2, 0), (4, 1, 1), (3, 3, 0), (3, 2, 1) \text{ și } (2, 2, 2).$$

Deci $f = s_1^2 s_2^2 + a s_1^3 s_3 + b s_2^3 + c s_1 s_2 s_3 + d s_3^2$, unde a, b, c, d sunt numere reale. Determinăm acești coeficienți dind valori numerice nedeterminatelor X_1, X_2, X_3 .

| X_1 | X_2 | X_3 | s_1 | s_2 | s_3 | f |
|-------|-------|-------|-------|-------|-------|-----|
| 1 | 1 | 0 | 2 | 1 | 0 | 2 |
| 2 | -1 | -1 | 0 | -3 | 2 | 50 |
| 1 | -2 | -2 | -3 | 0 | 4 | 200 |
| 1 | -1 | -1 | -1 | -1 | 1 | 8 |

Obținem astfel sistemul de ecuații

$2 = 4 + b; 50 = -27b + 4d; 200 = -108a + 16d, 8 = 1 - a - b + c + d$, de unde $b = -2, d = -1, a = -2, c = 4$. Prin urmare

$$(X_1^2 + X_2^2)(X_1^2 + X_3^2)(X_2^2 + X_3^2) = s_1^2 s_2^2 - 2s_1^3 s_3 - 2s_2^3 + 4s_1 s_2 s_3 - s_3^2.$$

§ 3. Teorema fundamentală a algebrei

Fie K un corp comutativ și $K[X]$ inelul polinoamelor într-o nedeterminată cu coeficienți în K . Plecind de la inelul $K[X]$ vom prezenta mai întii o construcție a unui nou inel, analoagă celei date în cap. VII, §2, unde am definit inelul claselor de resturi modulo n .

3.1. Fie $f \in K[X]$ un polinom nenul. Pe inelul $K[X]$ definim relația binară următoare:

Dacă $u, v \in K[X]$, spunem că u este congruent cu v modulo f și scriem $u \equiv v \pmod{f}$ dacă $f \mid u - v$. Dacă u nu este congruent cu v modulo f scriem $u \not\equiv v \pmod{f}$. Relația de congruență modulo f , o vom nota cu \equiv_f . Aceasta este o relație de echivalență. Demonstrația acestui fapt este la fel cu cea dată la congruență pe \mathbb{Z} și de aceea o omitem.

Fie f un polinom nenul din $K[X]$. Dacă $u, v \in K[X]$, din teorema împărțirii cu rest pentru polinoame avem

$$u = fq_1 + r_1, \text{ unde } \text{grad}(r_1) < \text{grad}(f),$$

și

$$v = fq_2 + r_2, \text{ unde } \text{grad}(r_2) < \text{grad}(f),$$

r_1 și r_2 fiind resturile împărțirii polinoamelor u și v la f .

Rezultă imediat că $u \equiv v \pmod{f}$ dacă și numai dacă $r_1 = r_2$. Prin urmare, două polinoame u și v sunt congruente modulo f dacă și numai dacă resturile împărțirii polinoamelor u și v la f , sunt egale.

Pentru $u \in K[X]$, notăm cu

$$\hat{u} = \{ v \in K[X] \mid u \equiv v \pmod{f} \},$$

clasa de echivalență a lui u , numită clasa de resturi a lui u modulo f .

Să considerăm mulțimea factor

$$K[X]/\equiv_f = \{\hat{u} \mid u \in K[X]\},$$

pe care o vom nota cu

$$K[X]_{(f)}.$$

Dacă $u \in K[X]$ este un polinom oarecare, atunci

$$u = fq + r, \text{ unde } \text{grad}(r) < \text{grad}(f).$$

Avem că $f \mid u - r$ și deci $u \equiv r \pmod{f}$, de unde $\hat{u} = \hat{r}$. Deci clasa de echivalență a unui polinom u , modulo f , este egală cu clasa restului împărțirii lui u la f .

Pe mulțimea $K[X]_{(f)}$ a claselor de resturi modulo f se definesc operații algebrice de adunare și înmulțire în modul următor:

$$\hat{u} + \hat{v} = \widehat{u+v},$$

$$\hat{u} \hat{v} = \widehat{uv},$$

oricare ar fi $u, v \in K[X]_{(f)}$.

Cele două operații algebrice nu depind de alegerea reprezentanților, adică sunt bine definite. Mai mult mulțimea $K[X]_{(f)}$, înzestrată cu operațiile de adunare și înmulțire definite mai sus formează un inel unitar și comutativ

Verificarea acestor afirmații o omitem, deoarece este analoagă cu cea dată la inelul claselor de resturi modulo n .

Funcția

$$p: K[X] \rightarrow K[X]_{(f)}$$

dată prin $p(u) = \hat{u}$ este un morfism unitar de inele, numit *morfismul canonic*.

3.2. Lemă. Fie K un corp comutativ și f un polinom ireductibil din $K[X]$. Atunci inelul $K[X]_{(f)}$ este un corp.

Demonstrație. Fie $g \neq 0$ un element nenul din inelul $K[X]_{(f)}$. Atunci $f \nmid g$ și cum f este ireductibil, rezultă că f și g sunt prime între ele. Deci există $u, v \in K[X]$ astfel încât $fu + gv = 1$, de unde prin trecerea la clase rezultă $\hat{g} \hat{v} = \hat{1}$. Prin urmare, \hat{g} este inversabil și cum $\hat{g} \neq \hat{0}$ este un element oarecare al lui $K[X]_{(f)}$, rezultă că acesta este un corp.

Fie $K \subset L$ corpuri comutative astfel încât K să fie un subcorp al lui L . Spunem că L este o extindere. De exemplu, corpul \mathbb{C} al numerelor complexe este o extindere a corpului \mathbb{R} al numerelor reale.

3.3. Propoziție. Fie K un corp comutativ și f un polinom de grad ≥ 1 din $K[X]$, de grad ≥ 1 . Atunci există o extindere L a lui K astfel încât f să aibă cel puțin o rădăcină în L .

Demonstrație. Deoarece $f \in K[X]$ are $\text{grad}(f) \geq 1$, rezultă că f nu este inversabil. Cum inelul $K[X]$ este factorial, există $f_1 \in K[X]$, polinom ireductibil, care divide f . Considerăm inelul $K[X]_{(f_1)}$ care, conform lemei precedente este un corp.

Fie

$$K \xrightarrow{i} K[X] \xrightarrow{p} K[X]_{(f_1)},$$

în care i este morfismul incluziune, iar p este morfismul canonic, adică $i(a) = a$, oricare ar fi $a \in K$ și $p(g) = \hat{g}$, oricare ar fi $g \in K[X]$. Să notăm corpul $K[X]_{(f_1)}$ cu F . Componerea $\varphi = p \circ i$, $\varphi : K \mapsto F$ este un morfism de corpuri și deci injectiv. Fie $f = a_0 + a_1 X + \dots + a_n X^n$ din $K[X]$ și să notăm cu $f^\varphi = \varphi(a_0) + \varphi(a_1)X + \dots + \varphi(a_n)X^n$ din $F[X]$. Dacă notăm $a = p(X) = \hat{X}$ din F , atunci

$$\begin{aligned} f^\varphi(a) &= \varphi(a_0) + \varphi(a_1)a + \dots + \varphi(a_n)a^n = \varphi(a_0) + \varphi(a_1)\hat{X} + \dots + \varphi(a_n)\hat{X}^n = \\ &= \hat{a}_0 + \hat{a}_1\hat{X} + \dots + \hat{a}_n\hat{X}^n = \overbrace{\hat{a}_0 + \hat{a}_1X + \dots + \hat{a}_nX^n}^{\hat{f}}. \end{aligned}$$

Dacă $f = f_1 f_2$ avem $f \equiv 0 \pmod{f_1}$, de unde $\hat{f} = \hat{0}$. Prin urmare $f^\varphi(a) = \hat{0}$, adică a este o rădăcină a polinomului $f^\varphi \in F[X]$.

Deoarece φ este injectiv, atunci $\varphi(K) = K^\varphi$ este un subcorp al lui F izomorf cu K . Să notăm cu E o mulțime astfel încât $E \cap K = \emptyset$ și există o funcție bijectivă $\psi : F \setminus K^\varphi \rightarrow E$.

Dacă $L = K \cup E$, avem în mod evident că funcția $\theta : L \rightarrow F$, definită prin

$$\theta(x) = \begin{cases} \varphi(x), & \text{dacă } x \in K, \\ \psi(x), & \text{dacă } x \in E, \end{cases}$$

este bijectivă.

Vom defini pe L o structură de corp astfel încât θ să fie morfism de corpuri, iar K să fie un subcorp al lui L .

Dacă $x, y \in L$, punem prin definiție $x \oplus y = \theta^{-1}(\theta(x) + \theta(y))$ și $x \odot y = \theta^{-1}(\theta(x)\theta(y))$. Se verifică ușor că L împreună cu adunarea \oplus și înmulțirea \odot are o structură de corp comutativ. Funcția θ este morfism de corpuri. Într-adevăr

$$\theta(x \oplus y) = \theta(\theta^{-1}(\theta(x) + \theta(y))) = \theta(x) + \theta(y) \text{ și}$$

$$\theta(x \odot y) = \theta(\theta^{-1}(\theta(x)\theta(y))) = \theta(x)\theta(y),$$

oricare ar fi $x, y \in L$. Deci θ este izomorfism, θ^{-1} fiind izomorfismul invers.

Mai mult, K este un subcorp al lui L . Într-adevăr, dacă $x, y \in K$, atunci

$$\begin{aligned} x \oplus y &= \theta^{-1}(\theta(x) + \theta(y)) = \theta^{-1}(\varphi(x) + \varphi(y)) = \theta^{-1}(\varphi(x+y)) = \\ &= \theta^{-1}(\theta(x+y)) = x+y \text{ și, analog, } x \odot y = xy. \end{aligned}$$

Astfel, operațiile algebrice ale corpului K sunt induse de cele de pe corpul L și deci K este un subcorp al lui L . Deci am obținut o extindere L a lui K în care vom arăta că f are o rădăcină. Vom nota operațiile algebrice de pe corpul L în mod simplu ca de obicei, aditiv și multiplicativ.

Fie $x = \theta^{-1}(a)$ și vom arăta că $f(x) = 0$. Într-adevăr, cum θ^{-1} este izomorfism, din $f^\varphi(a) = 0$ adică $\varphi(a_0) + \varphi(a_1)a + \dots + \varphi(a_n)a^n = 0$, rezultă $\theta^{-1}(\varphi(a_0)) + \theta^{-1}(\varphi(a_1)a) + \dots + \theta^{-1}(\varphi(a_n)a^n) = \theta^{-1}(0)$.

Coefficienții polinomului f fiind din K , avem în continuare

$$\theta^{-1}(\theta(a_0)) + \theta^{-1}(\theta(a_1))\theta^{-1}(a) + \dots + \theta^{-1}(\theta(a_n))\theta^{-1}(a) = 0 \text{ sau } a_0 + a_1x + \dots + a_nx^n = 0, \text{ adică } f(x) = 0.$$

3.4. Corolar. Fie K un corp comutativ și un polinom din $K[X]$ de grad ≥ 1 . Atunci există o extindere a lui K în care f să aibă toate rădăcinile.

Demonstrație. Procedăm prin inducție după $n = \text{grad}(f)$. Dacă $n = 1$ atunci $f = a_0 + a_1X$, $a_1 \neq 0$ și $f(-a_0a_1^{-1}) = 0$ unde $-a_0a_1^{-1} \in K$. Deci f are rădăcină în K . Presupunem că afirmația este adevărată pentru polinoame de grad $n - 1$ și să o dovedim pentru f de grad n . După propoziția precedentă există o extindere L_1 a lui K în care polinomul f are o rădăcină x . Deci în $L_1[X]$ polinomul f se descompune sub forma $f = (X - x)f_1$ unde $f_1 \in L_1[X]$ și al cărui grad este evident $n - 1$. Conform ipotezei inductive există o extindere L_2 a lui L_1 în care f_1 să aibă cele $n - 1$ rădăcini ale sale, fie acestea x_2, x_3, \dots, x_n . Dar x_2, x_3, \dots, x_n sunt și rădăcini ale lui f și deci cele n rădăcini ale sale sunt x, x_2, x_3, \dots, x_n care aparțin extinderii L_2 a lui K .

3.5. Lemă. Fie K un subcorp al unui corp F și $f \in K[X]$ un polinom de grad $\text{grad}(f) = n \geq 1$. Presupunem că f are rădăcinile x_1, x_2, \dots, x_n care aparțin lui F . Atunci oricare ar fi polinomul simetric $g(X_1, X_2, \dots, X_n)$ din $K[X_1, X_2, \dots, X_n]$, rezultă că $g(x_1, x_2, \dots, x_n)$ este din K .

Demonstrație. Deoarece $g(X_1, X_2, \dots, X_n)$ este simetric, după teorema fundamentală a polinoamelor simetrice există un polinom $h(X_1, X_2, \dots, X_n)$ cu coeficienți în K astfel încât $g = h(s_1, s_2, \dots, s_n)$. Având în vedere relațiile lui Viète avem că $s_i(x_1, x_2, \dots, x_n) \in K$, $1 \leq i \leq n$, și deci $g(x_1, x_2, \dots, x_n) = h(s_1(x_1, x_2, \dots, x_n), s_2(x_1, x_2, \dots, x_n), \dots, s_n(x_1, x_2, \dots, x_n))$ este un element din K .

Rezultatul următor este cunoscut sub numele de *teorema fundamentală a algebrei*.

3.6. Teoremă. Orice polinom de grad $n \geq 1$ cu coeficienți complecsi are cel puțin o rădăcină complexă.

Demonstrație. Mai întâi, observăm că orice polinom f cu coeficienți reali de grad impar are cel puțin o rădăcină reală. Într-adevăr funcția polomială $\tilde{f}: \mathbb{R} \rightarrow \mathbb{R}$ asociată lui f este continuă și pentru $a \in \mathbb{R}$ suficient de mare avem $\tilde{f}(a)\tilde{f}(-a) < 0$. Atunci după o proprietate fundamentală a funcțiilor continue rezultă că există $x \in \mathbb{R}$, astfel încât $\tilde{f}(x) = 0$, adică $f(x) = 0$. Deci există o rădăcină reală x a lui f .

Vom arăta acum că orice polinom cu coeficienți reali de grad oarecare are cel puțin o rădăcină complexă. Fie f din $\mathbb{R}[X]$ cu $\text{grad}(f) = n > 1$ și să considerăm k natural, astfel încât 2^k divide n iar 2^{k+1} nu divide n . Demonstrația se face prin inducție matematică după k . Pentru $k = 0$ rezultă n impar și afirmația a fost demonstrată mai înainte. Presupunem că afirmația este adevărată pentru toate polinoamele cu coeficienți reali al căror grad se divide cu 2^{k-1} și nu se divide cu 2^k . Conform corolarului 3.4 există o extindere a corpului \mathbb{C} al numerelor complexe în care f să aibă toate rădăcinile. Dacă x_1, x_2, \dots, x_n sunt rădăcinile lui f în L , pentru un număr real arbitrar a , considerăm elementele

$$z_{ij}^a = x_i x_j + a(x_i + x_j), \quad 1 \leq i < j \leq n.$$

Fie polinomul

$$h_a = \prod_{1 \leq i < j \leq n} (X - z_{ij}^a)$$

al cărui grad este egal cu numărul elementelor z_{ij}^a din L , adică $\text{grad}(h_a) = C_n^2$.

Deoarece $n = 2^k \cdot q$ și 2 nu divide q , rezultă $C_n^2 = \frac{n(n-1)}{2} = 2^{k-1}q(2^kq-1)$ și deci

$\text{grad}(h_a)$ se divide cu 2^{k-1} și nu se divide cu 2^k . Coeficienții polinomului h_a sunt polinoame simetrice elementare de z_{ij}^a . Mai mult, având în vedere expresiile lui z_{ij}^a , $1 \leq i < j \leq n$, rezultă că acești coeficienți ca polinoame de x_1, x_2, \dots, x_n sunt simetrice, deoarece orice permutare a acestora are ca efect schimbarea elementelor z_{ij}^a , $1 \leq i < j \leq n$, între ele. După lema 3.5, obținem că polinomul h_a are coeficienți reali. Cum 2^{k-1} divide $\text{grad}(h_a)$ și 2^k nu divide $\text{grad}(h_a)$, din ipoteza inducțivă rezultă că h_a are cel puțin o rădăcină complexă. Există deci o pereche (i, j) cu $1 \leq i < j \leq n$, astfel încât z_{ij}^a să aparțină lui \mathbb{C} . Făcind pe a să parcurgă mulțimea (infinită) \mathbb{R} a numerelor reale și cum mulțimea perechilor (i, j) , $1 \leq i < j \leq n$, este finită rezultă că există $a, b \in \mathbb{R}$, $a \neq b$, astfel încât z_{ij}^a și z_{ij}^b să aparțină lui \mathbb{C} .

Din $z_{ij}^a = x_i x_j + a(x_i + x_j)$ și $z_{ij}^b = x_i x_j + b(x_i + x_j)$, rezultă că $z_{ij}^a - z_{ij}^b = (a - b)(x_i + x_j)$ este număr complex și deci $x_i + x_j$ este număr complex. Dar atunci este clar că și $x_i x_j$ este complex. Așadar x_i, x_j sunt rădăcinile unui polinom de gradul al doilea cu coeficienți complecsi și deci, evident, sunt numere complexe. Am arătat astfel că polinomul f are rădăcini complexe. Să considerăm, în final, cazul unui polinom oarecare

$$f = a_0 + a_1 X + \dots + a_n X^n, \quad a_n \neq 0,$$

cu coeficienți complecsi. Fie de asemenea polinomul

$$\tilde{f} = \tilde{a}_0 + \tilde{a}_1 X + \dots + \tilde{a}_n X^n,$$

unde pentru orice $i = 0, 1, \dots, n$, \tilde{a}_i este conjugatul coeficientului a_i . Atunci $\tilde{f}\tilde{f}$ este un polinom cu coeficienți reali. Într-adevăr, dacă $b_k = \sum_{i+j=k} a_i \tilde{a}_j$, $0 \leq k \leq 2n$, este un coeficient oarecare al lui $\tilde{f}\tilde{f}$, atunci evident $\tilde{b}_k = b_k$ și deci b_k este un număr real. Prin urmare există numărul complex x , astfel încât $(\tilde{f}\tilde{f})(x) = 0$. Deci $0 = (\tilde{f}\tilde{f})(x) = f(x)\tilde{f}(x)$, de unde $f(x) = 0$ sau $\tilde{f}(x) = 0$. Dacă $f(x) = 0$, atunci x este o rădăcină complexă a lui f . Dacă $\tilde{f}(x) = 0$ este clar că $f(\bar{x}) = 0$ și deci \bar{x} este o rădăcină complexă a lui f .

Ca aplicații la teorema fundamentală a algebrei să descriem polinoamele ireductibile din $\mathbb{C}[X]$ și $\mathbb{R}[X]$.

1) Din teorema fundamentală a algebrei și teorema lui Bézout, rezultă că un polinom cu coeficienți complecsi este ireductibil în $\mathbb{C}[X]$ dacă și numai dacă este de gradul întii.

2) Dacă f este un polinom cu coeficienți reali,

$$f = a_0 + a_1 X + \dots + a_n X^n$$

și x este o rădăcină complexă a sa, avem $f(x) = 0$. Atunci

$0 = \overline{f(x)} = \overline{a_0 + a_1x + \dots + a_nx^n} = \bar{a}_0 + \bar{a}_1\bar{x} + \dots + \bar{a}_n\bar{x}^n = a_0 + a_1\bar{x} + \dots + a_n\bar{x}^n$,
adică \bar{x} este de asemenea o rădăcină a polinomului f din $\mathbb{R}[X]$. Deci rădăcinile complexe ale lui f , care nu sunt reale, sunt conjugate două cîte două. Mai mult,
două rădăcini conjugate au același ordin de multiplicitate.

Dacă $x = a + bi$, $b \neq 0$, este un număr complex și $\bar{x} = a - bi$ este conjugatul său, atunci

$$(X - (a + bi))(X - (a - bi)) = X^2 - 2aX + (a^2 + b^2),$$

care este un polinom cu coeficienți reali, de gradul al doilea, avînd discriminantul $4a^2 - 4(a^2 + b^2) = -4b^2 < 0$.

De aici, rezultă imediat că *un polinom cu coeficienți reali este ireductibil în $\mathbb{R}[X]$ dacă și numai dacă este de gradul întîi sau de gradul al doilea cu discriminantul negativ.*