

* **Biblioteca
profesorului de matematică**
C. NĂSTĂSESCU C. NIȚĂ C. VRACIU
*

**BAZELE
ALGEBREI
VOL. I**

Coordonator C. NĂSTĂSESCU

**EDITURA ACADEMIEI
REPUBLICII SOCIALISTE ROMÂNIA
București, 1986**

BASES ALGEBRAS
ОСНОВЫ АЛГЕБРЫ

Lucrarea a fost elaborată după cum urmează:

- | | |
|---------------|-----------------------|
| C. NĂSTASESCU | capitolele I, IV, VI. |
| C. NITĂ | capitolele III, V. |
| C. VRACIU | capitolul II. |

PREFATĂ

Algebra este una dintre ramurile cele mai importante ale matematicii, cunoscând în ultimul timp o dezvoltare foarte mare. Problematica de care se ocupă a devenit mai vastă și mai variată. Totodată ea constituie pentru matematicieni și alții specialiști un instrument de cercetare necesar și eficace.

În "BAZELE ALGEBREI" ne propunem să prezentăm în două volume, noțiunile și rezultatele de bază ale algebrei, într-o formă ușor accesibilă, căt și cîteva direcții în care acestea se dovedesc utile pentru cercetarea matematică.

În acest prim volum din "BAZELE ALGEBREI" ne propunem următoarele:

Primul capitol are ca scop fixarea notășilor și definirea unor noțiuni folosite în mod curent în matematică, cum sunt: funcție, familie de mulțimi, relație de echivalență, numere cardinale, mulțimi ordonate.

Capitolul al II-lea prezintă mai întâi unele rezultate de bază referitoare la grupuri. Se dă apoi noțiunea de grup liber și metoda enumerării claselor, prin care se obțin rezultate importante, privind structura grupurilor, cu ajutorul calculatoarelor electronice. Studiul grupurilor finite se bazează pe noțiunea de acțiune a unui grup pe o mulțime și pe teoremele lui Sylow. Sunt date de asemenea rezultate importante asupra grupurilor rezolvabile și nilpotente.

În capitolul al III-lea, mai întâi se expune în contextul inelelor rezultatele fundamentale din primul capitol, referitoare la grupuri. Se prezintă diverse construcții importante de inele care apar curent în matematică: inele de matrice, inele de fracții, inele de polinoame. Totodată se dau unele elemente asupra corpurilor. Ultima parte a capitolului este

dedicată polinoamelor simetrice și teoremei fundamentale a algebrei.

Capitolul al IV-lea se ocupă de studiul proprietăților aritmetice ale inelilor urmărindu-se prezentarea unor rezultate utile în teoria algebrică a numerelor. Se studiază factorialitatea inelilor de serii formale. Se dau criterii de ireductibilitate a polinoamelor.

Capitolul al V-lea prezintă mai întâi rezultatele fundamentale pentru module și spații vectoriale.

O atenție deosebită se acordă modulelor libere, studiindu-se invariația cardinalului bazei unui modul liber peste un inel comutativ. Finalul capitolului este rezervat endomorfismelor unui modul liber de rang finit.

Ultimul capitol, al VI-lea, studiază teoria determinanților și a sistemelor de ecuații liniare. Se dau metode algoritmice de rezolvare a acestora. În final, se prezintă formula de inversiune a lui Möbius cu aplicații în combinatorică.

Cartea cuprinde numeroase exemple, aplicații și exerciții, evidențiindu-se importanța instrumentului de cercetare a algebrei în diversele ramuri ale matematicii.

Prin conținutul și modul de realizare al cărții, ea se adresează profesorilor de matematică în vederea perfecționării activității la catedră. De asemenea, ea este utilă studenților din primii ani ai facultăților de matematică, punându-le la dispoziție un material accesibil și util pentru formarea lor ca viitori profesori și pentru studiul altor discipline matematice. Se adresează și elevilor cu aptitudini mai deosebite pentru matematică. Totodată cartea cuprinde un material necesar oricărui matematician sau specialist care, în activitatea sa, utilizează cunoștințe de algebră.

AUTORII

C U P R I N S

Capitolul I NOȚIUNI PRELIMINARE	9
§ 1. Multimi	9
§ 2. Funcții	11
§ 3. Produs cartezian al unei familii de multimi	14
§ 4. Relații de echivalență	15
§ 5. Multimi ordonate. Latici	17
§ 6. Numere cardinale	19
Capitolul II GRUPURI	20
§ 1. Legi de compoziție. Monoizi. Grupuri	20
§ 2. Subgrupuri și exemple de grupuri	27
§ 3. Grupuri factor. Teoreme de izomorfism	46
§ 4. Grupuri libere	60
§ 5. Acțiuni ale grupurilor pe mulimi	71
§ 6. p -grupuri și teoremele lui Sylow	95
§ 7. Grupuri rezolvabile și nilpotente	110
Exercitii	124
Capitolul III INELE ȘI CORPURI	130
§ 1. Inel. Subinel. Ideal. Inele de matrice	130
§ 2. Morfisme de inele. Produs direct de inele. Aplicații	143
§ 3. Inel factor. Teoreme de izomorfism pentru inele	149
§ 4. Corp. Subcorp. Morfisme de coruri Exemple	153
§ 5. Ideale prime și maximale.	161
§ 6. Inele de fracții	165
§ 7. Inele de polinoame	172
§ 8. Proprietăți ale rădăcinilor unui polynom. Derivata unui polynom	185
§ 9. Polinoame simetrice	190
§ 10. Teorema fundamentală a algebrei	197
Exercitii	202

Capitolul IV	
PROPRIETĂȚI ARITMETICE ALE INELELOR	208
§ 1. Divizibilitatea în inele	208
§ 2. Inele factoriale	213
§ 3. Factorialitatea inelelor de fracții	216
§ 4. Inele principale și inele euclidiene	218
§ 5. Exemple de inele euclidiene	220
§ 6. Factorialitatea inelelor de polinoame	228
§ 7. Factorialitatea inelelor de serii formale	232
§ 8. Criterii de ireductibilitate pentru polinoame	233
Exerciții	238
Capitolul V	
MODULE ȘI SPAȚII VECTORIALE	242
§ 1. Modul. Submodul. Morfisme de module	242
§ 2. Modul factor. Teoreme de izomorfism pentru module	250
§ 3. Module libere	253
§ 4. Dimensiunea spațiilor vectoriale. Rangul modulelor libere ..	259
§ 5. Schimbarea coordonatelor. Matricea asociată unui morfism de module libere de rang finit	264
Exerciții	270
Capitolul VI	
DETERMINANȚI. SISTEME DE ECUAȚII LINIARE	275
§ 1. Determinanți de ordin mic	275
§ 2. Definiția determinanților de ordinul n	279
§ 3. Proprietățile determinanților	282
§ 4. Calculul determinanților	288
§ 5. Formula Binet-Cauchy. Determinantul produsului a două matrice	293
§ 6. Definirea determinantului unei matrice prin inducție	296
§ 7. Matrice inversabile. Inversa unei matrice. Regula lui Cramer ...	302
§ 8. Rangul unei matrice	306
§ 9. Transformări elementare de matrici	309
§10. Sisteme de ecuații liniare	313
§11. Metoda lui Gauss de rezolvare a unui sistem de ecuații liniare ...	320
§12. Formula de inversiune Möbius. Aplicații	324
Exerciții	342
Bibliografie	347

Capitolul I

NOTIUNI PRELIMINARE

§ 1. MULTIMI

Prin multime înțelegem o colecție de obiecte care se numesc *elementele multimii*.

Vom nota cu litere mari multimile, cu litere mici elementele lor. Dacă A este o multime și x un element al său, vom scrie $x \in A$ și vom citi „ x aparține lui A “. Dacă x nu se găsește în A , atunci vom scrie $x \notin A$ și vom citi „ x nu aparține lui A “.

Există două moduri de definire (de determinare) a unei multimi:

i) *Numind individual elementele sale.* În acest caz, multimea se specifică scriind între acolade elementele sale $\{x, y, z, \dots\}$. De exemplu, $A = \{0, 1, 2, 3\}$, adică multimea formată din primele patru numere naturale; $B = \{a, b, c, d, e\}$ adică multimea formată din primele cinci litere mici ale alfabetului latin.

ii) *Specificind o proprietate pe care o au elementele sale și nu le au alte elemente.* Mai precis, dată o proprietate se poate vorbi de multimea acestor obiecte pentru care proprietatea respectivă are loc. Multimile definite în acest mod se vor nota prin $A = \{x \mid P(x)\}$ adică multimea acestor obiecte x pentru care are loc $P(x)$.

De exemplu să considerăm proprietatea: „ a fi număr natural par“; în acest caz multimea A va fi multimea numerelor naturale pare. O multime care are un număr finit de elemente se zice *finită*. În caz contrar se numește *infinită*.

Pentru cîteva multimi care vor fi des utilizate avem notări speciale: cu N vom nota multimea numerelor naturale, adică $N = \{0, 1, 2, 3, \dots\}$. Cu N^* vom nota multimea numerelor naturale nenule, adică $N^* = \{1, 2, 3, \dots\}$.

Cu Z vom nota *multimea numerelor întregi*; cu Q *multimea numerelor raționale*, cu R *multimea numerelor reale*, iar cu C *multimea numerelor complexe*.

În teoria mulțimilor se admite existența unei mulțimi care nu are nici un element, aceasta se numește mulțimea *vidă* și se notează cu simbolul \emptyset .

Dacă A și B sunt două mulțimi, vom spune că A este o *submulțime* a lui B (sau A este *conținută* în B) și vom scrie $A \subset B$ dacă orice element al mulțimii A este și element al mulțimii B . Simbolic scriem astfel $\forall x, x \in A \Rightarrow x \in B$.

Mulțimea *vidă* este o submulțime a oricărei mulțimi. Între mulțimile considerate mai înainte avem inclusiunile: $N^* \subset N \subset Z \subset Q \subset R \subset C$.

Două mulțimi A și B se zice că *coincid* sau sunt *egale* dacă au aceeași elemente, adică: $A = B \Leftrightarrow A \subset B$ și $B \subset A$ (\Leftrightarrow înseamnă „dacă și numai dacă“).

Relația de inclusiune (resp. relația de egalitate) între mulțimi are proprietățile următoare:

- este *reflexivă*, adică $A \subset A$ (resp. $A = A$);
- este *antisimetrică*, adică din $A \subset B$ și $B \subset A$ rezultă $A = B$ (resp. este *simetrică* adică $A = B \Rightarrow B = A$);
- este *tranzitivă*, adică $A \subset B$ și $B \subset C \Rightarrow A \subset C$ (resp. $A = B$ și $B = C \Rightarrow A = C$).

Relația de inclusiune ne permite să definim *mulțimea părților unei mulțimi* T , notată cu $\mathcal{P}(T)$, adică $\mathcal{P}(T)$ are ca elemente toate submulțimile mulțimii T .

Cu mulțimi se fac următoarele operații:

intersecția a două mulțimi A și B înseamnă mulțimea

$$A \cap B = \{x \mid x \in A \text{ și } x \in B\};$$

reuniunea mulțimilor A și B înseamnă mulțimea

$$A \cup B = \{x \mid x \in A \text{ sau } x \in B\}.$$

În cazul cînd $A \cap B = \emptyset$, atunci spunem că mulțimile A și B sunt *disjuncte*.

Operațiile de intersecție și reuniune satisfac egalitățile

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C),$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Prin *diferența mulțimilor* B și A înțelegem mulțimea

$$B - A = \{x \in B \mid x \notin A\}.$$

Dacă A este o submulțime a lui B , atunci diferența $B - A$ se numește *complementara* mulțimii A în B și se notează cu $\complement_B A$.

De exemplu $\complement_B \emptyset = B$ iar $\complement_B B = \emptyset$.

Dacă A și A' sunt două submulțimi ale mulțimii B au loc egalitățile:

$$\complement_B(A \cup A') = (\complement_B A) \cap (\complement_B A')$$

$$\complement_B(A \cap A') = (\complement_B A) \cup (\complement_B A')$$

numite *formulele lui de Morgan*.

Fie A și B două mulțimi arbitrară. Dacă $a \in A$ și $b \in B$, atunci putem forma *perechea ordonată* (cuplu) (a, b) , adică pereche formată din elementele a și b unde este stabilită o anumită ordine în sensul că a este primul element iar b este al doilea element în această pereche.

Rezultă că două perechi (a_1, b_1) și (a_2, b_2) sunt egale dacă și numai dacă $a_1 = a_2$ și $b_1 = b_2$.

Prin *produsul cartezian* al mulțimilor A și B înțelegem mulțimea

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

Cind $B = A$, atunci notăm $A^2 = A \times A$.

Se observă că dacă una dintre mulțimile A sau B este mulțimea vidă, atunci $A \times B = \emptyset$.

În plus, dacă A are m elemente iar B are n elemente, atunci mulțimea $A \times B$ are mn elemente.

§ 2. FUNCȚII

Fiind date mulțimile A și B , prin *funcție* (sau *aplicație*) definită pe mulțimea A , cu valori în mulțimea B se înțelege o lege f , în baza căreia oricărui element $a \in A$ i se asociază un unic element, notat $f(a)$ din B .

Mulțimea A se numește *domeniu de definiție* al funcției f , iar mulțimea B se numește *domeniu valorilor* funcției f (sau *codomeniu* funcției f).

O funcție f este perfect determinată cind se dă domeniul de definiție și codomeniul său și modul cum acționează f . O funcție f definită pe mulțimea A cu valori în B se notează $f: A \rightarrow B$ sau $A \xrightarrow{f} B$.

Dacă $f: A \rightarrow B$ este o funcție și $A' \subset A$ este o submulțime a mulțimii A , notăm

$$f(A') = \{f(a) \mid a \in A'\}$$

nuțită *imaginea* directă a lui A' prin funcția f .

În cazul particular cind $A' = A$, notăm $f(A) = \text{Im } f$ și se numește *imaginea funcției* f .

Similar, dacă $B' \subset B$ este o submulțime a lui B , atunci notăm cu

$$f^{-1}(B') = \{a \in A \mid f(a) \in B'\}$$

care este o submulțime a lui A ; această submulțime se numește *imaginea inversă* a lui B' prin funcția f . O funcție $f: A \rightarrow B$ se numește *injectivă*, dacă oricare ar fi $a, a' \in A$ cu $a \neq a'$ rezultă $f(a) \neq f(a')$ sau echivalent din egalitatea $f(a) = f(a')$ rezultă $a = a'$.

Funcția $f: A \rightarrow B$ se numește *surjectivă* dacă oricare ar fi $b \in B$ există $a \in A$ astfel încât $f(a) = b$, sau echivalent $\text{Im } f = B$.

O funcție care este injectivă și surjectivă se numește *bijecțivă*.

Dacă A și B sunt două mulțimi oarecare, vom nota cu $B^A = \{f:A \rightarrow B\}$, adică mulțimea tuturor funcțiilor definite pe A cu valori în B .

Dacă A este o mulțime oarecare, funcția $1_A:A \rightarrow A$, unde $1_A(a) = a$ oricare ar fi $a \in A$ se numește *funcția identică* a mulțimii A .

Dacă $A \subset B$ este o submulțime a lui B , atunci funcția $i:A \rightarrow B$ unde $i(a) = a$ oricare ar fi $a \in A$ se numește *funcția incluziune* a submulțimii A a lui B .

O funcție $f:A \rightarrow B$ se numește *restricția* funcției $g:A' \rightarrow B'$ dacă $A \subset A'$, $B \subset B'$ și $f(a) = g(a)$, oricare ar fi $a \in A$. În această situație g se numește o *extindere* a lui f .

Fieind date funcțiile $f:A \rightarrow B$ și $g:B \rightarrow C$, funcția notată cu $g \circ f$, unde $g \circ f:A \rightarrow C$ și $(g \circ f)(a) = g(f(a))$ oricare ar fi $a \in A$ se numește *componerea* funcțiilor f și g .

Sunt evidente egalitățile: dacă $f:A \rightarrow B$ este o funcție, atunci

$$1_B \circ f = f \text{ și } f \circ 1_A = f.$$

O proprietate importantă a compunerii funcțiilor este următoarea:

Teorema 2.1. *Componerea funcțiilor este asociațivă, adică fiind date funcțiile $f:A \rightarrow B$, $g:B \rightarrow C$ și $h:C \rightarrow D$ are loc egalitatea*

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Demonstrație. Într-adevăr, se vede mai întii că funcțiile $h \circ (g \circ f)$ și $(h \circ g) \circ f$ au domeniul de definiție A iar cōdomeniul D . Fie acum $a \in A$; avem

$$(h \circ (g \circ f))(a) = h((g \circ f)(a)) = h(g(f(a)))$$

și

$$((h \circ g) \circ f)(a) = (h \circ g)(f(a)) = h(g(f(a)))$$

de unde rezultă că

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

O funcție $f:A \rightarrow B$ se numește *inversabilă* dacă există o funcție $g:B \rightarrow A$ astfel încit $g \circ f = 1_A$ și $f \circ g = 1_B$. Următoarea teoremă caracterizează funcțiile inversabile.

Teorema 2.2. *Dacă $f:A \rightarrow B$ este o funcție, atunci f este inversabilă dacă și numai dacă f este bijecțivă.*

Demonstrație. Presupunem că f este inversabilă. Atunci există funcția $g:B \rightarrow A$ astfel încit $g \circ f = 1_A$ și $f \circ g = 1_B$. Fie $a, a' \in A$ astfel încit $f(a) = f(a')$. Atunci avem că $g(f(a)) = g(f(a'))$ adică $(g \circ f)(a) =$

$= (g \circ f)(a')$ de unde obținem că $1_A(a) = 1_A(a')$ și deci $a = a'$. Deci f este o funcție injectivă.

Fie acum $b \in B$; punem $a = g(b) \in A$. Deci $f(a) = f(g(b)) = (f \circ g)(b) = 1_B(b) = b$ ceea ce ne arată că f este și surjectivă și deci f este bijectivă. Invers, presupunem că f este bijectivă. Fie $b \in B$ un element oarecare. Cum f este surjectivă există elementul $a_b \in A$ astfel încât $f(a_b) = b$. Cum f este injectivă, elementul a_b este unic determinat de b . Atunci definim funcția $g: B \rightarrow A$ astfel $g(b) = a_b$. Se verifică imediat că $g \circ f = 1_A$ și $f \circ g = 1_B$.

Să presupunem din nou că funcția $f: A \rightarrow B$ este inversabilă. În acest caz funcția $g: B \rightarrow A$ cu proprietățile $g \circ f = 1_A$ și $f \circ g = 1_B$ este unic determinată. Într-adevăr, să presupunem că mai există o funcție $g': B \rightarrow A$ astfel încât $g' \circ f = 1_A$ și $f \circ g' = 1_B$. În acest caz avem $(g' \circ f) \circ g = 1_A \circ g = g$. Cum $(g' \circ f) \circ g = g' \circ (f \circ g) = g' \circ 1_B = g'$ rezultă $g = g'$. Funcția g fiind unică se notează cu f^{-1} și se numește inversa funcției f .

Teorema 2.3.i) Dacă funcția $f: A \rightarrow B$ este inversabilă, atunci inversa sa $f^{-1}: B \rightarrow A$ este inversabilă și are loc egalitatea $(f^{-1})^{-1} = f$.

ii) Dacă funcțiile $f: A \rightarrow B$ și $g: B \rightarrow C$ sunt inversabile, atunci funcția $g \circ f: A \rightarrow C$ este inversabilă și are loc egalitatea

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

Demonstrație. i) Cum avem egalitățile $f \circ f^{-1} = 1_B$ și $f^{-1} \circ f = 1_A$ rezultă că și f^{-1} este inversabilă și inversa sa este f , adică $(f^{-1})^{-1} = f$.

ii) Calculăm

$$\begin{aligned} (g \circ f) \circ (f^{-1} \circ g^{-1}) &= g \circ ((f \circ f^{-1}) \circ (g^{-1})) = g \circ (1_B \circ g^{-1}) = g \circ g^{-1} = 1_C \text{ și} \\ (f^{-1} \circ g^{-1}) \circ (g \circ f) &= f^{-1} \circ (g^{-1} \circ (g \circ f)) = f^{-1} \circ ((g^{-1} \circ g) \circ f) = f^{-1} \circ (1_B \circ f) = \\ &= f^{-1} \circ f = 1_A. \end{aligned}$$

Aceste egalități ne arată că $g \circ f$ este inversabilă și inversa sa este $f^{-1} \circ g^{-1}$, adică $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Un rezultat important foarte util în cele ce urmează este următorul.

Teorema 2.4. Fie A o mulțime finită și $f: A \rightarrow A$ o funcție. Următoarele afirmații sunt echivalente:

- 1) f este bijectivă; 2) f este injectivă; 3) f este surjectivă.

Demonstrație. 1) \Rightarrow 2) și 1) \Rightarrow 3) sunt evidente. 2) \Rightarrow 1). Deoarece A este o mulțime finită, atunci putem scrie că $A = \{a_1, a_2, \dots, a_n\}$. Cum f este injectivă, atunci $f(A) = \{f(a_1), f(a_2), \dots, f(a_n)\}$ unde $f(a_i) \neq f(a_j)$, oricare ar fi $i \neq j$. Deci $f(A)$ are n elemente. Cum $f(A) \subseteq A$ rezultă neapărat că $A = f(A)$ și deci f este și surjectivă, adică bijectivă.

3) \Rightarrow 1). Fie $b \in A$ și notăm cu $f^{-1}(b) = \{a \in A \mid f(a) = b\}$. Evident că $f^{-1}(b)$ este o submulțime a lui A . Cum f este surjectivă, atunci $f^{-1}(b) \neq \emptyset$ oricare ar fi $b \in A$. Deoarece $A' = \bigcup_{b \in A} f^{-1}(b)$ și mulțimile $f^{-1}(b)$

sunt disjuncte două cîte două, rezultă că $f^{-1}(b)$ are un singur element, deoarece în caz contrar ar rezulta că $\bigcup_{b \in A} f^{-1}(b)$ ar avea un număr mai mare de elemente decît mulțimea A . Aceasta ne arată că f este neapărat o funcție injectivă.

Observație. Dacă A nu este finită, teorema 2.4 nu este adevărată. De exemplu, să luăm $A = \mathbb{N}$ iar $f: \mathbb{N} \rightarrow \mathbb{N}$ să fie funcția $f(n) = n+1$. Se vede că f este injectivă dar nu este surjectivă deoarece $0 \notin \text{Im } f$.

§ 3. PRODUS CARTEZIAN AL UNEI FAMILII DE MULȚIMI

Fie $I \neq \emptyset$ și A o mulțime oarecare; o funcție $\varphi: I \rightarrow A$ se mai numește și mulțime *indexată* de elemente din A după mulțimea de indici I (sau familie de elemente din A indexată după I). Se notează

$$\varphi = (a_i)_{i \in I} = (a_i), \text{ unde } a_i = \varphi(i).$$

Dacă $I = \{1, 2, \dots, n\}$, atunci folosim notația $(a_i)_{i \in I} = (a_1, a_2, \dots, a_n)$ și (a_1, a_2, \dots, a_n) se mai numește *n-cuplu*.

Dacă elementele lui A sunt mulțimi (sau submulțimi ale unei mulțimi T) obținem noțiunea de familie de mulțimi (resp. familie de submulțimi a lui T). Fie $(A_i)_{i \in I}$ o familie de mulțimi, atunci mulțimile

$$\bigcup_{i \in I} A_i = \{x \mid \exists i \in I, x \in A_i\}$$

$$\bigcap_{i \in I} A_i = \{x \mid \forall i \in I, x \in A_i\}$$

se numește *reuniunea*, resp. *intersecția* familiei $(A_i)_{i \in I}$.

Fie $(A_i)_{i \in I}$ o familie de mulțimi. Mulțimea

$$\prod_{i \in I} A_i = \{\varphi: I \rightarrow \bigcup_{i \in I} A_i \mid \varphi(i) \in A_i, \forall i \in I\}$$

se numește *produs cartezian* sau *produs direct* al familiei $(A_i)_{i \in I}$.

Astfel, putem scrie:

$$\prod_{i \in I} A_i = \{(a_i)_{i \in I} \mid a_i \in A_i, \forall i \in I\}.$$

Dacă $A_i = A$ oricare ar fi $i \in I$, atunci produsul cartezian nu este altcineva decît mulțimea $A^I = \{\varphi: I \rightarrow A\}$. Dacă $I = \{1, 2, \dots, n\}$, atunci notăm $\prod_{i \in I} A_i = A_1 \times A_2 \times \dots \times A_n$. Deci $A_1 \times A_2 \times \dots \times A_n = \{(a_1, a_2, \dots, a_n) \mid a_1 \in A_1, \dots, a_n \in A_n\}$. În cazul $n=2$ obținem produsul cartezian a două mulțimi introdus în §1. Dacă $A_1 = A_2 = \dots = A_n = A$ vom nota $A^n = A_1 \times A_2 \times \dots \times A_n$.

Fie $i \in I$; funcția $p_i: \prod_{j \in I} A_j \rightarrow A_i$, definită prin egalitatea $p_i(\varphi) = \varphi(i) \in A_i$, unde $\varphi \in \prod_{j \in I} A_j$, (sau $p_i((x_j)_{j \in I}) = x_i$) se numește i -proiecția canonică a produsului cartezian pe mulțimea A_i .

În teoria mulțimilor se admite următoarea axiomă:

Axioma alegerii. Dacă $(A_i)_{i \in I}$ este o familie nevidă de mulțimi nevide, atunci $\prod_{i \in I} A_i \neq \emptyset$.

Echivalentă cu axioma alegerii este următoarea afirmație: dacă \mathcal{G} este o colecție nevidă de mulțimi nevide disjuncte două cîte două, atunci există o mulțime A numită *mulțime selectivă*, astfel încît $A \cap X$ este formată dintr-un singur element oricare ar fi $X \in \mathcal{G}$.

§ 4. RELAȚII DE ECHIVALENȚĂ

Fie A și B două mulțimi; o submulțime $\rho \subset A \times B$ se numește *relație binară* între A și B . Dacă elementul $(a, b) \in \rho$, unde $a \in A$ și $b \in B$ spunem că a este în relația ρ cu b și notăm $a \rho b$. Cind scriem $a \rho b$ înseamnă că elementele $a \in A$ și $b \in B$ nu sunt în relația ρ . De exemplu dacă $f: A \rightarrow B$ este o funcție, atunci mulțimea $\Gamma(f) = \{(a, b) \mid a \in A, b \in B \text{ și } b = f(a)\}$ este relația binară între A și B . Mulțimea $\Gamma(f)$ se numește *graficul* funcției f .

Invers, dacă $G \subset A \times B$ este o relație A și B cu proprietatea că oricare ar fi $a \in A$ există un unic $b \in B$ astfel încît $(a, b) \in G$, atunci putem defini funcția $f: A \rightarrow B$ așa încît $f(a) = b$. Se observă imediat că $\Gamma(f) = G$.

Cind $B = A$ o relație binară ρ între A și A se numește simplu *relație binară pe mulțimea A* . Relația binară pe o mulțime se notează de regulă cu unul din simbolurile: ρ , \sim , \mathcal{R} , \approx , etc.

Exemplu. 1) Fie A o mulțime oarecare; mulțimea $\Delta = \{(a, a) \mid a \in A\}$ se numește *diagonala mulțimii A* și este o relație binară pe A .

2) Dacă A este o mulțime de numere naturale, atunci mulțimea

$$< = \{(m, n) \in A \times A \mid m < n\}$$

este o relație binară pe A . În particular, dacă $A = \{1, 2, 3, 4\}$, atunci $< = \{(1, 2), (1, 3), (1, 4), (2, 3), (2, 4), (3, 4)\}$.

Definiția 4.1. O relație binară notată „ \sim ” pe A se numește *relație de echivalență* dacă următoarele condiții sunt verificate pentru orice $a, b, c \in A$:

- i) $a \sim a$ (reflexivitatea);
- ii) $a \sim b \Rightarrow b \sim a$ (simetria);
- iii) $a \sim b$ și $b \sim c \Rightarrow a \sim c$ (tranzitivitatea).

De exemplu, dacă considerăm \mathbb{Z} și $n > 0$ un număr natural, atunci relația binară notată „ \equiv ” (mod n) (congruență modulo n):

$$a \equiv b \pmod{n} \Leftrightarrow n | a - b$$

este o relație de echivalență pe \mathbb{Z} .

Sau dacă considerăm mulțimea R a numerelor reale relația „ \sim ”:

$$a \sim b \Leftrightarrow a - b \in \mathbb{Z}$$

este o relație de echivalență pe R .

Dată o relație de echivalență „ \sim ” pe A atunci pentru orice $a \in A$ definim mulțimea:

$$\hat{a} = \{b \in A \mid b \sim a\}$$

care se numește *clasa de echivalență* a elementului a .

Clasa de echivalență a elementului a se mai notează, de la caz la caz, și astfel: a , \hat{a} , \bar{a} , $[a]$ etc.

Teorema 4.2. Fie A o mulțime nevidă și „ \sim ” o relație de echivalență pe A . Atunci clasele de echivalență determinate de „ \sim ” pe A au proprietățile:

1) $a \in \hat{a}$ oricare ar fi $a \in A$. În particular $\hat{a} \neq \emptyset$.

2) $\hat{a} = \hat{b} \Leftrightarrow a \sim b$.

3) Dacă \hat{a} și \hat{b} sunt două clase de echivalență, atunci

$$\hat{a} = \hat{b} \text{ sau } \hat{a} \cap \hat{b} = \emptyset.$$

4) Reuniunea tuturor claselor de echivalență este egală cu A .

Demonstrație. 1) Deoarece $a \sim a$ rezultă că $a \in \hat{a}$.

2) Dacă $\hat{a} = \hat{b}$ cum $a \in \hat{a}$, atunci $a \in \hat{b}$ și deci $a \sim b$. Invers, presupunem că $a \sim b$. Fie $x \in \hat{a}$; deci $x \sim a$ și „ \sim ” este tranzitivă; obținem că $x \sim b$ adică $x \in \hat{b}$. Deci $\hat{a} \subset \hat{b}$. Similar, rezultă inclusiunea $\hat{b} \subset \hat{a}$ și deci avem egalitatea $\hat{a} = \hat{b}$.

3) Presupunem că $\hat{a} \cap \hat{b} \neq \emptyset$. Deci există un $x \in \hat{a} \cap \hat{b}$. Atunci $x \sim a$ și $x \sim b$. Cum „ \sim ” este simetrică avem $a \sim x$ și deci $a \sim b$. Din afirmația 2) rezultă că $\hat{a} = \hat{b}$.

4) Rezultă din 1).

Dată relația de echivalență „ \sim ” pe A , atunci mulțimea claselor de echivalență determinate de „ \sim ” se notează cu A/\sim și se numește *mulțimea factor* (sau *cil*) a lui A prin relația „ \sim ”. Funcția $p: A \rightarrow A/\sim$, $p(a) = \hat{a}$ este o funcție surjectivă și se numește *surjecția canonică*.

Definiția 4.3. Fie A o mulțime nevidă și „ \sim ” o relație de echivalență pe A . Familia de elemente din A , $(a_i)_{i \in I}$, se numește un *sistem de reprezentanți* relativ la relația de echivalență \sim , dacă are următoarele proprietăți:

i) Oricare ar fi $i \neq j$, $a_i \sim a_j$.

ii) Oricare ar fi $a \in A$, există $i \in I$ astfel încât $a \sim a_i$.
 Se observă că i) și ii) pot fi formulate concentrat astfel: oricare ar fi $a \in A$ există un unic $i \in I$ astfel încât $a \sim a_i$.

Înălțind datea o relație de echivalență „~” pe mulțimea nevidă A există întotdeauna un sistem de reprezentanți asociat relației „~”. Într-adevăr, fie $(C_i)_{i \in I}$ mulțimea tuturor claselor de echivalență asociate relației „~”. Cum $C_i \neq \emptyset$ oricare ar fi $i \in I$, conform axiomei alegerii, există o familie de elemente $(a_i)_{i \in I}$ astfel încât $a_i \in C_i$ oricare ar fi $i \in I$. Evident că $(a_i)_{i \in I}$ este un sistem de reprezentanți pentru relația „~”. Trebuie să observăm că acest sistem de reprezentanți nu este unic.

Dacă $(a_i)_{i \in I}$ este un sistem de reprezentanți relativ la relația „~” din teorema 4.2 rezultă că $A = \bigcup_{i \in I} a_i$, iar mulțimile a_i , $i \in I$, sunt disjuncte două cîte două.

Exemplu. Pe mulțimea Z a numerelor întregi considerăm relația „~”: $a \sim b \Leftrightarrow |a| = |b|$. Se observă imediat că ~ este o relație de echivalență pe Z . Dacă $a \in Z$ avem

$$\hat{a} = \{a, -a\} \quad \text{dacă } a \neq 0 \text{ și } \hat{a} = \{0\} \text{ dacă } a = 0.$$

Un sistem de reprezentanți poate fi considerat sistemul de numere: $0, 1, 2, 3, \dots$ adică mulțimea numerelor naturale N .

Un alt sistem de reprezentanți poate fi considerat și sistemul de numere $0, -1, -2, -3, \dots$, adică mulțimea numerelor întregi negative.

§ 5. MULȚIMI ORDONATE. LATICI

Definiția 5.1. Fie A o mulțime nevidă; o relație binară \leq pe A se zice de *ordine* dacă următoarele condiții sunt verificate pentru orice $a, b, c \in A$:

- i) $a \leq a$ (reflexivitatea).
- ii) $a \leq b$ și $b \leq a \Rightarrow a = b$ (antisimetria).
- iii) $a \leq b$ și $b \leq c \Rightarrow a \leq c$ (tranzitivitatea).

O mulțime A pe care s-a definit o relație de ordine „ \leq ” se numește *mulțime ordonată* și se notează (A, \leq) . Fiind dată o relație de ordine „ \leq ” pe mulțimea A , i se asociază relația „ $<$ ” definită prin $a < b \Leftrightarrow a \leq b$ și $a \neq b$, care este o relație tranzitivă.

Dacă pentru orice $a, b \in A$ avem $a \leq b$ sau $b \leq a$, mulțimea (A, \leq) se numește total *ordonată* sau *lanț*. Dacă $A' \subset A$ este o submulțime a mulțimii ordonate (A, \leq) , atunci A' cu relația de ordine indușă de \leq pe A' este o mulțime ordonată.

Exemplu. Dacă T este o mulțime, pe mulțimea părților $\mathcal{P}(T)$ a lui T , relația de inclusiune „ \subset ” este o relație de ordine. Dacă T are cel puțin două elemente, atunci $(\mathcal{P}(T), \subset)$ nu este o mulțime total ordonată.

Fie (A, \leq) o mulțime ordonată. Un element $a \in A$ se numește *prim element* (resp. *ultim element*) al lui A dacă $a \leq x$ (resp. $x \leq a$) oricare ar fi $x \in A$. Elementul $a \in A$ se zice *maximal* (resp. *minimal*) dacă din $a \leq x$ (resp. $x \leq a$) rezultă $a = x$. Fie $B \subset A$; un element $a \in A$ se zice *majorant* (resp. *minorant*) al lui B dacă $x \leq a$ (resp. $a \leq x$) oricare ar fi $x \in B$.

Elementul $a \in A$ se numește *superiorul* (resp. *inferiorul*) mulțimii B , dacă $x \leq a$ oricare ar fi $x \in B$ și dacă există un $a' \in A$ cu proprietatea că $x \leq a'$, atunci $a \leq a'$ (resp. $a \leq x \forall x \in B$ și dacă $a' \leq x \forall x \in B$, atunci $a' \leq a$). Elementul a (dacă există) se notează cu $\text{sup}(B)$ (resp. $\text{inf}(B)$).

O mulțime (A, \leq) se zice *inductivă* dacă orice submulțime a lui A care este un lanț are un majorant. Foarte important este următorul rezultat:

Lema lui Zorn. *Orice mulțime ordonată nevidă care este inductivă are cel puțin un element maximal.*

O mulțime ordonată (A, \leq) se zice *bine ordonată* dacă orice submulțime nevidă a sa are un prim element. Evident, orice mulțime bine ordonată este total ordonată. În plus, se vede ușor că (A, \leq) este bine ordonată dacă și numai dacă (A, \leq) este total ordonată și orice lanț descendant de elemente al lui A este staționar.

Un exemplu de mulțime bine ordonată este mulțimea \mathbb{N} cu relația de ordine obișnuită.

În teoria mulțimilor se demonstrează

Teorema lui Zermelo. *Dacă A este o mulțime nevidă, atunci există o relație de ordine \leq astfel încât (A, \leq) este o mulțime bine ordonată.*

De asemenea se demonstrează că: *Axioma alegerii, Lema lui Zorn și Teorema lui Zermelo sunt afirmații echivalente.*

O mulțime ordonată (A, \leq) se numește *latice* dacă pentru orice două elemente $a, b \in A$ există superiorul și inferiorul.

Vom nota cu $a \vee b = \text{sup}\{a, b\}$ și $a \wedge b = \text{inf}\{a, b\}$.

Evident că o mulțime total ordonată este o latice.

O latice A se zice *completă* dacă orice submulțime nevidă a lui A are superior și inferior în A .

O latice (A, \leq) se zice *modulară* dacă pentru orice $a, b, c \in A$ cu proprietatea $b \leq a$ avem egalitatea $a \wedge (b \vee c) = b \vee (a \wedge c)$

Dacă (A, \leq) și (B, \leq) sunt două latici, o funcție $f: A \rightarrow B$ se numește *omomorfism de latici* (sau simplu morfism) dacă pentru orice $a, b \in A$,

$$f(a \vee b) = f(a) \vee f(b) \text{ și } f(a \wedge b) = f(a) \wedge f(b).$$

Este clar că orice morfism de latici este o aplicație crescătoare. Un morfism de latici care este bijectiv se numește *izomorfism de latici*.

§ 6. NUMERE CARDINALE

Două mulțimi A și B se zic *cardinal echivalente* sau *echipotente* dacă există o bijecție de la A la B . Această relație este o relație de echivalență în clasa tuturor mulțimilor. Clasele de echivalență se numesc *numere cardinale*. Cardinalul mulțimii A se notează cu $\text{card } A$ sau $|A|$. Numerele cardinale se notează cu literele m, n, p, \dots .

Dacă A este o mulțime finită avind n elemente, atunci o mulțime B este cardinal echivalentă cu A dacă și numai dacă B are n elemente. Deci numărul cardinal $|A|$ este perfect determinat de numărul de elemente al mulțimii A . Din aceste motive $|A|$ se identifică cu numărul de elemente din A , adică $|A| = n$. Vom nota $|\emptyset| = 0$. Dacă A și B sunt două mulțimi, atunci vom scrie că $|A| \leq |B|$ dacă A este cardinal echivalentă cu o submulțime a lui B . Relația „ \leq ” este independentă de alegerea reprezentanților A și B și se verifică faptul că este o relație de ordine totală în clasa tuturor numerelor cardinale.

Se notează $|N| = \aleph_0$ (*alef zero*). Orice mulțime cardinal echivalentă cu N se numește numărabilă. Dacă mulțimea A este finită (resp. infinită) cardinalul său $|A|$ se zice finit (resp. infinit).

Dacă $(m_i)_{i \in I}$ este o familie de numere cardinale cu $m_i = |A_i|$, atunci se definesc operațiile aritmetice:

$$\sum_{i \in I} m_i = |\bigcup_{i \in I} (A_i \times \{i\})|, \quad \prod_{i \in I} m_i = |\prod_{i \in I} A_i|$$

$$m^n = |A^B|, \text{ unde } m = |A| \text{ și } n = |B|.$$

Este bine săiut că operațiile definite nu depind de alegerea reprezentanților. Dacă $I = \{1, 2, \dots, n\}$ scriem $\sum_{i \in I} m_i = m_1 + m_2 + \dots + m_n$ și $\prod_{i \in I} m_i = m_1 \cdot m_2 \cdot \dots \cdot m_n$.

Fie m, n, p trei numere cardinale. Au loc relațiile:

- 1) m este infinit, atunci $m+n = \sup(m, n)$;
- 2) m este infinit și $n \neq 0$, atunci $mn = \sup(m, n)$;
- 3) dacă $n \geq 2$, atunci $m < n^m$;
- 4) $(m^n)^p = m^{np}$, $m^{n+p} = m^n \cdot m^p$ și $(mn)^p = m^p \cdot n^p$.

Capitolul II GRUPURI

§ 1. LEGI DE COMPOZIȚIE. MONOIZI. GRUPURI

Definiția 1.1. Fie A o mulțime nevidă și n un număr natural. Se numește *lege de compozitie* n -ară pe A o aplicație $\varphi: A^n \rightarrow A$.

Pentru $n=0$ avem $A^0 = \{\cdot\}$, o mulțime cu un singur element, astfel că, a da o lege de compozitie 0 -ară pe un A revine la a da un element $e \in A$. Pentru $n=1$, avem $A^1 = A$ și o lege de compozitie unară pe A este o aplicație $\varphi: A \rightarrow A$. Pentru $n=2$, avem legi de compozitie binare $\varphi: A^2 \rightarrow A$.

O lege de compozitie binară $\varphi: A^2 \rightarrow A$ se numește *asociativă* dacă:

$$\varphi(a, \varphi(b, c)) = (\varphi(a, b), c) \text{ oricare ar fi } a, b, c \in A.$$

Legea de compozitie φ se notează de regulă multiplicativ: $\varphi(a, b) = ab$ sau $\varphi(a, b) = a \cdot b$ sau aditiv: $\varphi(a, b) = a + b$, $a, b \in A$. Evident, în notație multiplicativă condiția de asociativitate se scrie: $a(bc) = (ab)c$, iar, în notație aditivă, $a + (b + c) = (a + b) + c$.

Un element $e \in A$ se numește *element neutru* pentru legea de compozitie $\varphi: A^2 \rightarrow A$ dacă

$$\varphi(a, e) = \varphi(e, a) = a \text{ pentru orice } a \in A.$$

Un element neutru pentru φ dacă există este unic. Într-adevăr, dacă e și e' sunt amândouă element neutru pentru φ , atunci $\varphi(e, e') = e'$ deoarece e este element neutru și $\varphi(e, e') = e$ deoarece e' este element neutru și, în concluzie, $e = e'$. Notația multiplicativă pentru elementul neutru este 1, în care caz spunem că 1 este elementul unitate pentru φ (sau identitatea lui φ); notația aditivă este 0 și spunem că 0 este elementul nul pentru φ (sau zeroul lui φ).

O pereche $M = (A, \varphi)$, unde A este o mulțime și φ o lege de compozitie binară pe A se numește *monoid* dacă sînt satisfăcute următoarele condiții:

1) φ este asociativă, 2) φ are element neutru.

Mulțimea A se numește *mulțimea subiacentă a monoidului M* (sau

mulțimea elementelor lui M). De regulă mulțimea subiacentă a unui monoid se notează cu aceeași literă ca și monoidul. ϕ se numește legea de compoziție a monoidului M (în notație multiplicativă ϕ se numește înmulțire iar în notație aditivă, adunare). În loc de a spune că (A, ϕ) este monoid, spunem adesea că A este monoid în raport cu legea de compoziție ϕ .

De regulă, cind vorbim despre legi de compoziție sau monoizi la modul general, folosim notația multiplicativă; notația aditivă se folosește numai în unele cazuri concrete, unde ea apare în mod natural.

Fie M un monoid. Un element $a \in M$ se numește *inversabil* dacă există un element $a' \in M$, astfel încât $aa' = a'a = 1$. În această situație a' se numește un *invers* al lui a . Dacă elementele $a', a'' \in M$ sunt inverse ale lui a , deci $aa' = a'a = 1$ și $aa'' = a''a = 1$, atunci

$$a' = 1a' = (a''a)a' = a''(aa') = a''1 = a''.$$

Astfel, dacă un element $a \in M$ este inversabil, inversul său este unic. Notația multiplicativă a inversului unui element $a \in M$ este a^{-1} , iar notația aditivă este $-a$; în al doilea caz $-a$ se numește și opusul lui a .

Se numește *grup* un monoid G în care orice element $a \in G$ este inversabil. Din cele de mai sus rezultă că putem defini un grup ca fiind o mulțime nevidă G împreună cu o lege de compoziție binară pe G satisfăcind următoarele condiții (numite axiomele grupului):

- 1) legea de asociativitate: $a(bc) = (ab)c$ oricare ar fi $a, b, c \in G$;
- 2) legea elementului neutru: există un element $1 \in G$, astfel ca, $a1 = 1a = a$ oricare ar fi $a \in G$.
- 3) legea inversului: pentru orice $a \in G$ există un element $a^{-1} \in G$, astfel ca $aa^{-1} = a^{-1}a = 1$.

Exemplu. $(\mathbb{N}, +)$ unde \mathbb{N} este mulțimea numerelor naturale și „+“ este adunarea numerelor naturale este un monoid. Elementul neutru al acestui monoid este numărul natural 0; 0 este de asemenea singurul element inversabil al monoidului $(\mathbb{N}, +)$; (\mathbb{N}^*, \cdot) unde \mathbb{N}^* este mulțimea numerelor naturale nenule și „.“ este înmulțirea numerelor naturale este un monoid al cărui element neutru este numărul natural 1.

$(\mathbb{Z}, +)$ unde \mathbb{Z} este mulțimea numerelor întregi și „+“ este adunarea numerelor întregi este grup. (\mathbb{Z}, \cdot) este monoid, singurele elemente inversabile ale acestui monoid fiind 1 și -1 .

$(\mathbb{Q}, +)$, unde \mathbb{Q} este mulțimea numerelor raționale este grup. (\mathbb{Q}, \cdot) este monoid, în care 0 este singurul element neinversabil. (\mathbb{Q}^*, \cdot) , unde \mathbb{Q}^* este mulțimea numerelor raționale nenule este grup.

Propoziția 1.2. Fie G un grup. Pentru orice două elemente $a, b \in G$ ecuația

$$ax = b \text{ (respectiv } xa = b)$$

are o unică soluție $x \in G$. În particular, pentru $x, y \in G$,

$$ax = ay \Rightarrow x = y \quad (\text{respectiv, } xa = ya \Rightarrow x = y).$$

Demonstrație. Dacă $x \in G$ și $ax = b$, atunci:

$$x = 1x = (a^{-1}a)x = a^{-1}(ax) = a^{-1}b,$$

deci soluția ecuației $ax = b$ dacă există este unică. Pe de altă parte, $x = a^{-1}b$ este o soluție a ecuației $ax = b$ deoarece:

$$ax = a(a^{-1}b) = (aa^{-1})b = 1b = b.$$

Pentru ecuația $xa = b$ se lucrează, în mod analog, cu $x = ba^{-1}$.

Definiția 1.3. Fie A o mulțime nevidă și φ o lege de compozиție binară pe A . Pentru orice număr întreg pozitiv n , definim recursiv o lege de compozиție n -ară $\varphi_n: A^n \rightarrow A$ prin:

$\varphi_1 = 1_A$, aplicația identică a lui A ,

$$\varphi_{n+1}(a_1, a_2, \dots, a_{n+1}) = \varphi(\varphi_n(a_1, a_2, \dots, a_n), a_{n+1}), \text{ unde}$$

$$a_1, a_2, \dots, a_{n+1} \in A,$$

Propoziția 1.4. (Legea de asociativitate generalizată). Presupunem că legea de compozиție φ este asociativă. Atunci pentru orice două numere întregi pozitive m și n și orice $m+n$ elemente $a_1, a_2, \dots, a_{m+n} \in A$ avem: $\varphi(\varphi_m(a_1, a_2, \dots, a_m), \varphi_n(a_{m+1}, a_{m+2}, \dots, a_{m+n})) = \varphi_{m+n}(a_1, a_2, \dots, a_{m+n})$.

Demonstrație. Inducție după n . Pentru $n=1$, egalitatea are loc în virtutea definiției lui φ_{m+1} . Presupunem egalitatea adevărată pentru n și avem:

$$\begin{aligned} \varphi(\varphi_m(a_1, a_2, \dots, a_m), \varphi_{n+1}(a_{m+1}, a_{m+2}, \dots, a_{m+n+1})) &= \varphi(\varphi_m(a_1, a_2, \dots, a_m), \\ \varphi(\varphi_n(a_{m+1}, a_{m+2}, \dots, a_{m+n}), a_{m+n+1})) &= (\text{prin definiția lui } \varphi_{n+1}) = \\ = \varphi(\varphi(\varphi_m(a_1, a_2, \dots, a_m), \varphi_n(a_{m+1}, a_{m+2}, \dots, a_{m+n})), a_{m+n+1}) &(\text{deoarece } \varphi \text{ este asociativă}) = \varphi(\varphi_{m+n}(a_1, a_2, \dots, a_{m+n}), a_{m+n+1}) \text{ (prin ipoteza de inducție)} = \varphi_{m+n+1}(a_1, a_2, \dots, a_{m+n+1}) \text{ (prin definiția lui } \varphi_{m+n+1}). \end{aligned}$$

Observație. Presupunem că legea de compozиție binară este notată multiplicativ. Atunci vom nota, pentru orice număr întreg pozitiv n și orice n elemente $a_1, a_2, \dots, a_n \in A$,

$$a_1a_2\dots a_n = \varphi_n(a_1, a_2, \dots, a_n).$$

Avem, prin definiție:

$$\begin{aligned} a_1a_2\dots a_n &= (a_1a_2\dots a_{n-1})a_n = ((a_1a_2\dots a_{n-2})a_{n-1})a_n = \\ &\dots = (\dots((a_1a_2)a_3)\dots a_{n-1})a_n. \end{aligned}$$

În acest fel, avem posibilitatea de a forma un „produs“ a n elemente $a_1, a_2, \dots, a_n \in A$ disponind în modul indicat parantezele în sirul a_1, a_2, \dots, a_n și folosind „produsul“ binar φ . Evident există mai multe posibilități de a dispune parantezele pentru a forma un produs n -ar. Legea de asociativitate generalizată nu spune altceva decât că toate aceste produse n -are coincid.

Dacă legea de compozitie binară φ are element neutru atunci definim $\varphi_0: A^0 \rightarrow A$ ca fiind acest element neutru. În această situație este evident că legea de asociativitate generalizată are loc pentru orice două numere naturale m și n .

Definiția 1.5. Fie A o mulțime și φ o lege de compozitie binară pe A notată multiplicativ. Două elemente $a, b \in A$ se numesc *permutable* (în raport cu φ) dacă $ab = ba$, iar legea de compozitie φ se numește *comutativă* dacă orice două elemente $a, b \in A$ sint permutable. Un monoid se numește *comutativ* dacă legea sa de compozitie este comutativă. Un grup comutativ se numește de obicei grup abelian.

Propoziția 1.6. (Legea de comutativitate generalizată). *Fie A o mulțime și φ o lege de compozitie binară pe A , asociativă, notată multiplicativ. Fie n un număr întreg pozitiv și $a_1, a_2, \dots, a_n \in A$, n elemente permutable două cîte două. Atunci, pentru orice aplicație bijectivă $\sigma: \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}$ avem*

$$a_1 a_2 \dots a_n = a_{\sigma(1)} a_{\sigma(2)} \dots a_{\sigma(n)}$$

(alfel spus, produsul $a_1 a_2 \dots a_n$ nu depinde de ordinea factorilor).

Demonstrație. Afirmația este evidentă pentru $n=1$ și $n=2$. presupunem $n > 2$ și că produsul a oricărora m elemente din A permutable două cîte două nu depinde de ordinea factorilor pentru orice $m < n$. Fie $\sigma(k) = n$. Atunci

$$\begin{aligned} a_{\sigma(1)} a_{\sigma(2)} \dots a_{\sigma(n)} &= (a_{\sigma(1)} \dots a_{\sigma(k-1)}) (a_n a_{\sigma(k+1)} \dots a_{\sigma(n)}) = \\ &= (a_{\sigma(1)} \dots a_{\sigma(k-1)}) (a_{\sigma(k+1)} \dots a_{\sigma(n)} a_n) = (a_{\sigma(1)} \dots a_{\sigma(k-1)} a_{\sigma(k+1)} \dots a_{\sigma(n)}) a_n. \end{aligned}$$

Deoarece aplicația $\tau: \{1, 2, \dots, n-1\} \rightarrow \{1, 2, \dots, n-1\}$ definită prin

$$\tau(i) = \begin{cases} \sigma(i) & \text{dacă } i \in \{1, 2, \dots, k-1\} \\ \sigma(i+1) & \text{dacă } i \in \{k, \dots, n\} \end{cases}$$

este evident bijectivă, avem $a_{\sigma(1)} \dots a_{\sigma(k-1)} a_{\sigma(k+1)} \dots a_{\sigma(n)} = a_{\tau(1)} a_{\tau(2)} \dots a_{\tau(n-1)} = a_1 a_2 \dots a_{n-1}$ deci

$$a_{\sigma(1)} a_{\sigma(2)} \dots a_{\sigma(n)} = (a_1 a_2 \dots a_{n-1}) a_n = a_1 a_2 \dots a_n.$$

Propoziția 1.7. Fie M un monoid, n un număr natural și $x_1, x_2, \dots, x_n \in M$. Dacă x_1, x_2, \dots, x_n sunt elemente inversabile, atunci $x_1 x_2 \dots x_n$ este element inversabil și $(x_1 x_2 \dots x_n)^{-1} = x_n^{-1} \dots x_2^{-1} x_1^{-1}$.

Demonstrație. Pentru $n=0$ și $n=1$ afirmația este evidentă (în cazul $n=0$ ar trebui demonstrat că 1 este element inversabil și $1^{-1}=1$; acest lucru rezultă imediat deoarece $1 \cdot 1 = 1$). Pentru $n=2$ avem:

$$(x_1 x_2)(x_2^{-1} x_1^{-1}) = x_1(x_2 x_2^{-1}) x_1^{-1} = x_1 x_1^{-1} = 1$$

și

$$(x_2^{-1} x_1^{-1})(x_1 x_2) = x_2^{-1}(x_1^{-1} x_1) x_2 = x_2^{-1} x_2 = 1,$$

deci $x_1 x_2$ este inversabil și $(x_1 x_2)^{-1} = x_2^{-1} x_1^{-1}$. Presupunând că enunțul este adevărat pentru $n-1$ elemente avem:

$$x_1 x_2 \dots x_n = (x_1 x_2 \dots x_{n-1}) x_n$$

deci $x_1 x_2 \dots x_n$ este inversabil, fiind produsul a două elemente inversabile și

$$(x_1 x_2 \dots x_n)^{-1} = [(x_1 x_2 \dots x_{n-1}) x_n]^{-1} =$$

$$= x_n^{-1} (x_1 x_2 \dots x_{n-1})^{-1} = x_n^{-1} (x_{n-1}^{-1} \dots x_2^{-1} x_2^{-1}) = x_n^{-1} \dots x_2^{-1} x_1^{-1}.$$

Definiția 1.8. Fie A o mulțime și ϕ o lege de compozitie binară pe A , asociativă, notată multiplicativ. Pentru un element $a \in A$ și n un număr întreg pozitiv, se numește puterea $n-a$ a lui a (în raport cu ϕ) elementul

$$a^n = a_1 a_2 \dots a_n, \text{ unde } a_1 = a_2 = \dots = a_n = a.$$

Aveam $a^1 = a$, $a^{n+1} = a^n a$. Dacă ϕ are element neutru, putem defini $a^0 = 1$. Pentru orice două numere întregi pozitive m și n (numere naturale, dacă ϕ are element neutru), avem, conform legii de asociativitate generalizată: $a^m a^n = a^{m+n}$. De asemenea $(a^m)^n = a^{mn}$; aceasta se demonstrează prin inducție după n , astfel;

$$(a^m)^{n+1} = (a^m)^n \cdot a^m = a^{mn} a^m = a^{mn+m} = a^{m(n+1)}.$$

Dacă $a, b \in A$ și $ab = ba$, legea de comutativitate generalizată arată că pentru orice număr întreg pozitiv n (număr natural dacă ϕ are element neutru), avem: $(ab)^n = a^n b^n$.

Egalitățile

$$(1.8.1) \quad \begin{cases} a^m a^n = a^{m+n} \\ (ab)^n = a^n b^n \text{ dacă } ab = ba, \\ (a^m)^n = a^{mn} \end{cases}$$

se numesc legile puterii. Ele au loc pentru orice două numere întregi pozitive m și n (numere naturale dacă ϕ are element neutru).

Fie M un monoid și $a \in M$ un element inversabil. Propoziția 1.6 arată că, pentru orice număr natural n , a^n este inversabil și $(a^n)^{-1} = (a^{-1})^n$. În această situație putem defini puterile negative ale lui a

luind $a^{-n} = (a^n)^{-1} = (a^{-1})^n$, n fiind număr întreg pozitiv. Dacă $a, b \in M$ sunt inversabile și $ab = ba$, putem demonstra că legile puterii (1.8.1) sunt valabile pentru orice două numere întregi m și n . Într-adevăr, dacă m și n sint numere întregi pozitive, avem:

- pentru $m \geq n$, $a^m a^{-n} = a^{m-n} a^n (a^{-1})^n = a^{m-n} (aa^{-1})^n = a^{m-n}$;
 - pentru $m < n$, $a^m a^{-n} = a^m (a^{-1})^m (a^{-1})^{n-m} = (a^{-1})^{n-m} = a^{m-n}$.
- $$a^{-m} a^{-n} = (a^{-1})^m (a^{-1})^n = (a^{-1})^{m+n} = a^{-m+(-n)};$$
- $$(ab)^{-n} = ((ba)^n)^{-1} = (b^n a^n)^{-1} = a^{-n} b^{-n};$$
- $$(a^m)^{-n} = ((a^m)^n)^{-1} = (a^{mn})^{-1} = a^{-mn};$$
- $$(a^{-m})^{-n} = (((a^m)^{-1})^n)^{-1} = (a^m)^n = (a^m)^n = a^{mn} = a^{(-m)(-n)};$$
- $$(a^{-m})^n = ((a^m)^{-1})^n = ((a^m)^n)^{-1} = (a^{mn})^{-1} = a^{-mn}.$$

În notație aditivă, scriem na în loc de a^n și spunem că na este al n -lea multiplu al lui a . Avem $0a=0$ (0 din membrul stîng este numărul natural 0 și 0 din membrul drept este elementul neutru al monoidului în care lucrăm), $1a=a$, $(n+1)a=na+a$ și, în general, legile puterii se scriu sub forma:

$$(1.8.2) \quad \begin{cases} ma + na = (m+n)a, \\ n(a+b) = na + nb \text{ dacă } a+b = b+a, \\ m(na) = (mn)a. \end{cases}$$

Propoziția 1.9. Fie M și M' doi monoizi. O aplicație $f: M \rightarrow M'$ se numește morfism de monoizi dacă sunt satisfăcute următoarele condiții:

$$(1) \quad f(ab) = f(a)f(b) \text{ pentru orice } a, b \in M$$

(2) $f(1) = 1$ (aici 1 din membrul stîng este elementul unitate pentru M iar 1 din membrul drept este elementul unitar pentru M').

Dacă în plus M și M' sint grupuri, f se numește morfism de grupuri dacă este satisfăcută condiția (1) de mai sus. De fapt, conform propoziției ce urmează, un morfism de grupuri satisfacă în mod automat și condiția (2) astfel încât orice morfism de grupuri este și morfism de monoizi.

Propoziția 1.10. Fie $f: G \rightarrow G'$ un morfism de grupuri. Atunci

- $f(1) = 1$;
- $f(a^{-1}) = f(a)^{-1}$ pentru orice $a \in G$;
- $f(a^n) = f(a)^n$ pentru orice $a \in G$ și $n \in \mathbb{Z}$.

Demonstrație. (i) Avem

$$\begin{aligned} \text{(i)} \quad f(1) &= f(1)1 = f(1)f(1)f(1)^{-1} = f(1)f(1)^{-1} = f(1)f(1)^{-1} = 1. \\ \text{(ii)} \quad f(a^{-1}) &= f(a^{-1})1 = f(a^{-1})f(a)f(a)^{-1} = f(a^{-1}a)f(a)^{-1} = f(1)f(a)^{-1} = \\ &= 1f(a)^{-1} = f(a)^{-1}. \end{aligned}$$

(iii) Afirmația este adevărată pentru $n=0$ în virtutea lui (i). Presupunind $f(a^n)=f(a)^n$, rezultă

$$f(a^{n+1}) = f(a^n a) = f(a^n)f(a) = f(a)^n f(a) = f(a)^{n+1}$$

ceea ce demonstrează că afirmația este adevărată pentru orice număr natural n . Presupunem acum că n este un număr întreg pozitiv. Atunci

$$f(a^{-n}) = f((a^n)^{-1}) = f(a)^n)^{-1} = (f(a)^n)^{-1} = f(a)^{-n}.$$

Propoziția 1.11. *Componerea a două morfisme de monoizi (respectiv grupuri) este un morfism de monoizi (respectiv grupuri).*

Demonstrație. Fie $f: M \rightarrow M'$ și $g: M' \rightarrow M''$ și pentru $a, b \in M$ avem:

$$\begin{aligned} (g \circ f)(ab) &= g(f(ab)) = g(f(a)f(b)) = g(f(a))g(f(b)) = \\ &= (g \circ f)(a)(g \circ f)(b). \end{aligned}$$

În plus, $(g \circ f)(1) = g(f(1)) = g(1) = 1$. Deci $g \circ f$ este morfism de monoizi. Pentru cazul grupurilor afirmația este evidentă din cele de mai sus.

Propoziția 1.12. *Fie $f: M \rightarrow M'$ un morfism de monoizi (respectiv de grupuri) și presupunem în plus că f este aplicație bijectivă. Atunci, aplicația inversă $f^{-1}: M' \rightarrow M$ este de asemenea un morfism de monoizi (respectiv de grupuri).*

Demonstrație. Pentru $a', b' \in M'$ avem

$$\begin{aligned} f^{-1}(a'b') &= f^{-1}(f(f^{-1}(a'))f(f^{-1}(b'))) \quad (\text{deoarece } f \circ f^{-1} = 1_{M'}) = \\ &= f^{-1}(f(f^{-1}(a')f^{-1}(b'))) \quad \text{deoarece } f \text{ este mormâfism} = f^{-1}(a')f^{-1}(b') \\ &\quad (\text{deoarece } f^{-1} \circ f = 1_M). \end{aligned}$$

În cazul monoizilor mai trebuie remarcat faptul că, deoarece

$$f(1) = 1 \text{ avem } f^{-1}(1) = f^{-1}(f(1)) = 1.$$

Definiția 1.13. Un morfism $f: M \rightarrow M'$ de monoizi (respectiv de grupuri) se numește izomorfism dacă există un morfism $g: M' \rightarrow M$ de monoizi (respectiv de grupuri) astfel ca $g \circ f = 1_M$ și $f \circ g = 1_{M'}$.

Conform propoziției precedente un morfism $f: M \rightarrow M'$ este izomorfism dacă și numai dacă f este aplicație bijectivă.

Doi monoizi M și M' (respectiv două grupuri) se numesc izomorfi dacă există un izomorfism de monoizi (respectiv de grupuri) $M \rightarrow M'$ ca în care scriem $M \simeq M'$. Relația de izomorfism \simeq este o relație de echivalență pe clasa tuturor monoizilor (respectiv grupurilor). Într-adevăr, pentru orice monoid (respectiv grup) M avem $M \simeq M$ deoarece aplicația identică $1_M: M \rightarrow M$ este evident un izomorfism. Dacă $M \simeq M'$, atunci propoziția 1.12 arată că și $M' \simeq M$, iar dacă $M \simeq M'$ și $M' \simeq M''$, atunci propoziția 1.11 arată că și $M \simeq M''$.

În cazul grupurilor, clasa de echivalență a unui grup G modulo relația de izomorfism se numește tipul grupului G . În teoria grupurilor se studiază numai acele proprietăți ale grupurilor care fiind adevărate pentru un grup G , sunt adevărate pentru orice grup izomorf G . Deci, practic, în teoria grupurilor, nu se face distincție între două grupuri izomorfe. Problemele fundamentale în teoria grupurilor sunt:

- 1) descrierea tuturor tipurilor posibile de grupuri;
- 2) obținerea unui procedeu prin care date două grupuri G și G' să se poată decide dacă ele au același tip sau nu.

§ 2. SUBGRUPURI ȘI EXEMPLE DE GRUPURI

Definiția 2.1. Fie A o mulțime nevidă și $\varphi: A^2 \rightarrow A$ o lege de compozitie binară pe A . O submulțime nevidă B a lui A se numește *parte stabilă* a lui A în raport cu φ dacă pentru orice două elemente $x, y \in B$ avem $\varphi(x, y) \in B$. În această situație putem defini legea de compozitie $\varphi': B^2 \rightarrow B$ prin $\varphi'(x, y) = \varphi(x, y)$, $x, y \in B$. φ' se numește legea de compozitie indușă de φ pe B .

Fie A un monoid. O submulțime B a lui A se numește submonoid (respectiv subgrup) al lui A dacă sunt satisfăcute următoarele condiții:

- 1) B este parte stabilă a lui A în raport cu legea de compozitie a lui A ;
- 2) B este monoid (respectiv grup) în raport cu legea de compozitie indușă.

Din această definiție se observă că dacă B este un submonoid al monoidului A , atunci sunt satisfăcute următoarele condiții:

- 1') B este monoid;
- 2') mulțimea elementelor lui B este inclusă în mulțimea elementelor lui A ;
- 3') aplicația $i: B \rightarrow A$ definită prin $i(x) = x$, $x \in B$, este morfism de monoizi (i se numește inclusiunea canonica a lui B în A).

Reciproc, dacă B satisfac condițiile 1'), 2') și 3'), atunci B este un submonoid al lui A . Într-adevăr, B este monoid, B este submulțime a lui A iar condiția 3') arată că B este parte stabilă a lui A și legea de compozitie a lui B coincide cu legea de compozitie indușă pe B de

legea de compoziție a lui A . Dacă A este grup, B este subgrup a lui A dacă și numai dacă sunt satisfăcute condițiile 1') 2') și 3') în care cuvântul monoid se înlocuiește cu grup.

Propoziția 2.2. Fie M un monoid. Atunci mulțimea $U(M)$ a tuturor elementelor inversabile ale monoidului M este un subgrup al lui M .

Demonstrație. Trebuie să verificăm condițiile 1) și 2) din 2.1 pentru submulțimea $U(M)$ a lui M . Dacă $x, y \in U(M)$, atunci $xy \in U(M)$ conform propoziției 1.6. Prin urmare $U(M)$ este parte stabilă a lui M în raport cu legea de compoziție a lui M . Legea de compoziție indușă pe $U(M)$ satisfacă atunci axiomele grupului: legea de asociativitate este satisfăcută deoarece legea de compoziție a lui M este asociativă; elementul unitar 1 al lui M aparține lui $U(M)$ ($1^{-1} = 1$) și evident este element neutru pentru legea de compoziție indușă pe $U(M)$; dacă $x \in U(M)$, atunci $x^{-1} \in U(M)$ ($(x^{-1})^{-1} = x$) și x^{-1} este inversul lui x în $U(M)$ în raport cu legea de compoziție indușă.

Propoziția 2.3. Fie G un grup și H o submulțime a lui G . Următoarele afirmații sunt echivalente:

a) H este subgrup al lui G ;

b) sunt satisfăcute condițiile:

1) $x, y \in H \Rightarrow xy \in H$; 2) $1 \in H$; 3) $x \in H \Rightarrow x^{-1} \in H$;

c) H este o submulțime nevidă a lui G și

$$x, y \in H \Rightarrow xy^{-1} \in H.$$

Demonstrație. a) \Rightarrow b). Condiția 1) este satisfăcută deoarece H este parte stabilă a lui G în raport cu legea de compoziție a lui G . Considerind că H este grup în raport cu legea de compoziție indușă, incluziunea canonica $i: H \rightarrow G$, $i(x) = x$, $x \in H$, este morfism de grupuri. Aplicind propoziția 1.9 vedem că dacă e este elementul unitate a lui H avem $i(e) = 1$, deci $1 = e \in H$. De asemenea, dacă $x \in H$ și x' este inversul lui x în H , avem $i(x') = x^{-1}$, deci $x^{-1} = x' \in H$.

b) \Rightarrow c). H este nevidă deoarece $1 \in H$. Pentru orice $x, y \in H$, avem $y^{-1} \in H$ prin condiția 3) și $xy^{-1} \in H$ prin condiția 1).

c) \Rightarrow b). Deoarece H este nevidă există un element $x_0 \in H$. Atunci $1 = x_0x_0^{-1} \in H$. Pentru orice $x, y \in H$ vom avea $x^{-1} = 1x^{-1} \in H$ și $xy = x(y^{-1})^{-1} \in H$.

b) \Rightarrow a). Condiția 1) arată că H este parte stabilă a lui G în raport cu legea de compoziție a lui G . Legea de compoziție indușă este asociativă (deoarece legea de compoziție a lui G este asociativă), are element neutru deoarece $1 \in H$ și orice element $x \in H$ are invers în H deoarece $x^{-1} \in H$.

Observație. Dacă H este un subgrup al unui grup G vom scrie $H \leqslant G$. Notația $H \subset G$ va indica faptul că H este o submulțime a lui G (care poate fi subgrup a lui G sau nu).

Pentru orice grup G , submulțimile $\{1\}$ și G ale lui G sunt evident subgrupuri ale lui G . $\{1\}$ se numește subgrupul trivial al lui G și, de regulă, se notează cu 1 (sau în notație aditivă cu 0, caz în care îl numim subgrupul nul al lui G). Subgrupul G al lui G se numește subgrupul impropriu al lui G .

Dacă $H \leqslant G$, pentru orice submulțime K a lui H avem evident

$$K \leqslant H \Leftrightarrow K \leqslant G.$$

Definiția 2.4. Fie G și G' două grupuri și $f:G \rightarrow G'$ un morfism de grupuri. Pentru fiecare submulțime H a lui G avem o submulțime

$$f(H) = \{f(h) | h \in H\} \subset G'$$

și, pentru orice submulțime K a lui G' , avem o submulțime

$$f^{-1}(K) = \{x \in G | f(x) \in K\} \subset G.$$

Propoziția 2.5 Fie $f:G \rightarrow G'$ un morfism de grupuri, $H \subset G$ și $K \subset G'$. Atunci, dacă $H \leqslant G$ avem $f(H) \leqslant G'$ și, dacă $K \leqslant G'$ avem $f^{-1}(K) \leqslant G$.

Demonstrație. Presupunem $H \leqslant G$. Atunci dacă $x, x' \in f(H)$, avem $x = f(h)$, $x' = f(h')$ cu $h, h' \in H$ și $xy = f(h)f(h') = f(hh')$ cu $hh' \in H$ deci $xy \in f(H)$. Deoarece $1 \in H$ avem $1 = f(1) \in f(H)$. În fine, dacă $x = f(h) \in f(H)$, $h \in H$, avem $x^{-1} = f(h)^{-1} = f(h^{-1})$ și $h^{-1} \in H$, deci $x^{-1} \in f(H)$. Rezultă $f(H) \leqslant G'$ în virtutea propoziției 2.3 (b). Presupunem acum $K \leqslant G'$. Dacă $x, y \in f^{-1}(K)$ rezultă $f(x) \in K$, $f(y) \in K$ și $f(xy) = f(x)f(y) \in K$, deci $xy \in f^{-1}(K)$. Avem $f(1) = 1 \in K$, deci $1 \in f^{-1}(K)$ și dacă $x \in f^{-1}(K)$, $f(x) \in K$, $f(x^{-1}) = f(x)^{-1} \in K$, deci $x^{-1} \in f^{-1}(K)$. Prin urmare și $f^{-1}(K) \leqslant G$.

Definiția 2.6. Fie $f:G \rightarrow G'$ un morfism de grupuri. Conform propoziției precedente $f(G)$ este un subgrup al lui G' (G este subgrupul impropriu al lui G) și $f^{-1}(1)$ este un subgrup al lui G (1 este subgrupul trivial al lui G'). Subgrupul $f(G)$ al lui G' se numește imaginea lui f și se notează $\text{Im } f$:

$$\text{Im } f = \{f(x) | x \in G\}.$$

Subgrupul $f^{-1}(1)$ al lui G se numește nucleul lui f și se notează $\text{Ker } f$:

$$\text{Ker } f = \{x \in G | f(x) = 1\}.$$

Propoziția 2.7. Fie $f:G \rightarrow G'$ un morfism de grupuri. Au loc următoarele afirmații:

- i) f este aplicație surjectivă $\Leftrightarrow \text{Im } f = G'$;
- ii) f este aplicație injectivă $\Leftrightarrow \text{Ker } f = \{1\}$;
- iii) f este izomorfism $\Leftrightarrow \text{Im } f = G'$ și $\text{Ker } f = \{1\}$.

Demonstrație. i) rezultă imediat din definiția aplicației surjective.
 ii) Dacă f este aplicație injectivă și $x \in \text{Ker } f$, avem $f(x)=1=f(1)$ deci $x=1$; astfel $\text{Ker } f=\{1\}$. Reciproc, presupunem că $\text{Ker } f=\{1\}$ și fie $x, y \in G$ astfel ca $f(x)=f(y)$. Avem:

$$f(x \cdot y^{-1}) = f(x)f(y)^{-1} = f(x)f(x)^{-1} = 1,$$

deci $xy^{-1} \in \text{Ker } f=\{1\}$, $xy^{-1}=1$, $y=1$, $y=xy^{-1}y=x$. Prin urmare f este injectivă.

iii) Rezultă din i) și ii) aplicind propoziția 1.12.

Observație. Fie G un grup și $H \leqslant G$. Conform definiției 2.1, incluziunea canonica $i: H \rightarrow G$ este un morfism de grupuri. Pentru acest morfism avem evident $\text{Ker } i=\{1\}$ și $\text{Im } i=H$.

Dacă $f: G \rightarrow G'$ este un morfism de grupuri și $H \leqslant G$, atunci aplicația $f': H \rightarrow f(H)$ indușă de f (adică definită prin $f'(h)=f(h)$, $h \in H$) este tot un morfism de grupuri. Avem $\text{Im } f'=\{f(h) \mid h \in H\} = f(H)$ deci f' este aplicație surjectivă și $\text{Ker } f'=H \cap \text{Ker } f$; deci, dacă f este aplicație injectivă, rezultă și f' injectivă și astfel f' este izomorfism de grupuri: $H \cong f(H)$. În particular, dacă f este un morfism de grupuri injectiv, $f: G \rightarrow G'$, avem $G \cong \text{Im } f \leqslant G'$. Reciproc, dacă avem $G \cong K \leqslant G'$, considerind un izomorfism $f: G \rightarrow K$ și incluziunea canonica $i: K \rightarrow G'$, compunerea $i \circ f: G \rightarrow G'$ este un morfism de grupuri injectiv.

Spunem că un grup G se poate scufunda într-un grup G' dacă există un morfism de grupuri injectiv $f: G \rightarrow G'$; conform celor de mai sus acest lucru este echivalent cu faptul că grupul G este izomorf cu un subgrup al lui G' .

Propoziția 2.8. (Teorema de corespondență). *Fie $f: G \rightarrow G'$ un morfism de grupuri surjectiv. Atunci pentru orice subgrup $K \leqslant G'$ există un unic subgrup $H \leqslant G$ astfel încât $\text{Ker } f \leqslant H$ și $f(H)=K$. (Cu alte cuvinte aplicația $H \sim \rightarrow f(H)$ de la mulțimea subgrupurilor lui G care conțin $\text{Ker } f$ în mulțimea subgrupurilor lui G' este bijectivă).*

Demonstrație. Fie $K \leqslant G'$. Presupunem că $H \leqslant G$, $\text{Ker } f \leqslant H$ și $f(H)=K$. Pentru $h \in H$ avem $f(h) \in f(H)=K$, deci $h \in f^{-1}(K)$; astfel $H \subseteq f^{-1}(K)$. Reciproc, fie $x \in f^{-1}(K)$, deci $f(x) \in K=f(H)$; există un $h \in H$ cu $f(x)=f(h)$ deci $xh^{-1} \in \text{Ker } f \leqslant H$ și $x=(xh^{-1})h \in H$. În concluzie $H=f^{-1}(K)$. Prin urmare dacă există un $H \leqslant G$ cu $\text{Ker } f \leqslant H$ și $f(H)=K$, acesta este unic și anume, trebuie să avem $H=f^{-1}(K)$. Luăm acum $H=f^{-1}(K)$. Stîm că $H \leqslant G$ și, dacă $x \in \text{Ker } f$, avem $f(x)=1 \in K$, deci $x \in f^{-1}(K)=H$, adică $\text{Ker } f \leqslant H$. În fine, dacă $x \in H$ avem $f(x) \in K$, deci $f(H) \subseteq K$. Reciproc dacă $y \in K$, avem $y=f(x)$ cu $x \in G$ deoarece f este aplicație surjectivă; dar $f(x)=y \in K$ implică $x \in f^{-1}(K)$, deci $y=f(x) \in f(H)$. Astfel $f(H)=K$.

Propoziția 2.9. *Pentru orice familie $\{H_i\}_{i \in I}$ de subgrupuri ale unui grup G , intersecția $\bigcap_{i \in I} H_i$ este de asemenea un subgrup al lui G .*

Demonstrație. Avem $1 \in H_i$ pentru orice $i \in I$, deci $1 \in \bigcap_{i \in I} H_i$. Pentru $x, y \in \bigcap_{i \in I} H_i$ avem, pentru orice $i \in I$, $x, y \in H_i$, deci $xy^{-1} \in H_i$ și rezultă $xy^{-1} \in \bigcap_{i \in I} H_i$. Prin urmare $\bigcap_{i \in I} H_i \leq G$ conform propoziției 2.3 (c).

Definiția 2.10. Fie G un grup și S o submulțime a lui G . Notăm cu $\langle S \rangle$ intersecția tuturor subgrupurilor lui G care conțin pe S . Evident sunt satisfăcute următoarele condiții:

$$(1) \quad S \subseteq \langle S \rangle \leq G;$$

$$(2) \quad \text{dacă } S \subseteq H \leq G, \text{ atunci } \langle S \rangle \leq H.$$

$\langle S \rangle$ se numește subgrupul lui G general de S (sau subgrupul generat de S în G). Dacă $\langle S \rangle = G$ spunem că S este o mulțime de generatori pentru G (sau că G este generat de submulțimea S). Grupul G se numește finit generat dacă există o submulțime finită S a lui G astfel ca $\langle S \rangle = G$. Dacă $S = \{x_1, x_2, \dots, x_n\}$ scriem $\langle x_1, x_2, \dots, x_n \rangle$ în loc de $\langle S \rangle$. Grupul G se numește ciclic dacă există un element $x \in G$ astfel ca $\langle x \rangle = G$; un astfel de element $x \in G$ cu $\langle x \rangle = G$ se numește un generator al grupului G .

Avem evident $\langle \emptyset \rangle = 1$ și $\langle H \rangle = H$ pentru orice subgrup H al lui G .

Notăm cu $\mathcal{L}(G)$ mulțimea tuturor subgrupurilor lui G . Mulțimea $\mathcal{L}(G)$ este o mulțime ordonată, relația de ordine fiind incluziunea, sau mai precis relația \leq .

Propoziția 2.9 arată că $\mathcal{L}(G)$ este o lattice completă, infimumul oricărei familii $\{H_i\}_{i \in I}$ de elemente din $\mathcal{L}(G)$ fiind intersecția $\bigcap_{i \in I} H_i$. Supremumul familiei $\{H_i\}_{i \in I}$ este, conform condițiilor (1) și (2) de mai sus, exact subgrupul $\langle \bigcup_{i \in I} H_i \rangle$ generat în G de reuniunea $\bigcup_{i \in I} H_i$.

În cazul unei familii $\{H, K\}$ formată din două subgrupuri notăm acest supremum cu $H \vee K$: $H \vee K = \langle H \cup K \rangle$.

Propoziția 2.11. Fie G un grup și S o submulțime a lui G . Avem: $S = \{x_1 x_2 \dots x_n \mid n \in \mathbb{N}, x_i \in S \text{ sau } x_i^{-1} \in S \text{ pentru orice } i \in \{1, 2, \dots, n\}\}$.

Demonstrație. Fie

$$H = \{x_1 x_2 \dots x_n \mid n \in \mathbb{N}, x_i \in S \text{ sau } x_i^{-1} \in S \text{ pentru orice } i \in \{1, 2, \dots, n\}\}.$$

H este un subgrup al lui G . Într-adevăr, $1 \in H$ (vezi definiția producției 0-ar dată în 1.3). În plus, dacă $x, y \in H$ avem:

$$x = x_1 x_2 \dots x_m \text{ cu } x_i \in S \text{ sau } x_i^{-1} \in S \text{ pentru orice } i \in \{1, 2, \dots, m\},$$

$$y = y_1 y_2 \dots y_n \text{ cu } y_i \in S \text{ sau } y_i^{-1} \in S \text{ pentru orice } i \in \{1, 2, \dots, n\}.$$

Rezultă

$$xy = x_1x_2 \dots x_m y_1y_2 \dots y_n \in H \text{ și } x^{-1} = x_m^{-1} \dots x_2^{-1} x_1^{-1} \in H.$$

Evident avem $S \subset H$, deci $\langle S \rangle \subseteq H$. Pe de altă parte, pentru orice $x \in H$, $x = x_1x_2 \dots x_n$, avem, oricare ar fi $i \in \{1, 2, \dots, n\}$, $x_i \in S \subset \langle S \rangle$ sau $x^{-1} \in S \subset \langle S \rangle$ și în ultimul caz $x_i = (x_i^{-1})^{-1} \in \langle S \rangle$, deoarece $\langle S \rangle$ este subgrup; din același motiv $x = x_1x_2 \dots x_n \in \langle S \rangle$. Deci $\langle S \rangle = H$.

Observație. Dacă elementele $x_1, x_2, \dots, x_m \in G$ sunt permutabile două cite două, avem:

$$\langle x_1, x_2, \dots, x_m \rangle = \{x_1^{k_1} x_2^{k_2}, \dots x_m^{k_m} \mid k_1, k_2, \dots, k_m \in \mathbb{Z}\}.$$

Acest lucru rezultă din propoziția precedentă grupind însă într-un produs n -ar, $x_1x_2 \dots x_n$, întii toți factorii care coincid cu x_1 sau cu x_1^{-1} , apoi toți factorii care coincid cu x_2 sau x_2^{-1} etc. Rezultă de asemenea că $\langle x_1, x_2, \dots, x_m \rangle$ este un grup abelian. În particular, pentru orice $x \in G$, $\langle x \rangle = \{x^m \mid m \in \mathbb{Z}\}$ și $\langle x \rangle$ este abelian. Deci orice grup ciclic este abelian.

În notație aditivă avem:

$$\begin{aligned} \langle x_1, x_2, \dots, x_m \rangle &= \{k_1x_1 + k_2x_2 + \dots + k_mx_m \mid k_1, k_2, \dots, k_m \in \mathbb{Z}\} \\ \langle x \rangle &= \{mx \mid m \in \mathbb{Z}\}. \end{aligned}$$

Definiția 2.12. Fie G un grup. Pe mulțimea $P(G)$ a tuturor submulțimilor lui G definim o lege de compoziție binară astfel: dacă $A, B \in P(G)$, atunci $AB = \{ab \mid a \in A, b \in B\}$. Această lege de compoziție este asociativă:

$$(AB)C = A(BC) = \{abc \mid a \in A, b \in B, c \in C\}.$$

și are ca element neutru subgrupul trivial $1 = \{1\}$. Prin urmare $P(G)$ este monoid. Pentru orice $a \in G$, $\{a\} \in P(G)$ este element inversabil în monoidul $P(G)$, inversul său în $P(G)$ fiind $\{a^{-1}\}$. Se constată ușor că aplicația $\varphi: G \rightarrow U(P(G))$ definită prin $\varphi(a) = \{a\}$ este un morfism de grupuri injective. φ este chiar un izomorfism. Într-adevăr, fiind dat $A \in U(P(G))$ avem $AB = \{1\}$ pentru un $B \in P(G)$. A și B sunt evident nevide și luând $a \in A$, $b \in B$, avem, pentru orice $a' \in A$, $ab = a'b = 1$, deci $a = a'$. Astfel $A = \{a\} = \varphi(a)$.

Pentru orice $A \in P(G)$ vom nota $A^{-1} = \{a^{-1} \mid a \in A\}$, deși, conform celor de mai sus, A^{-1} nu este în general inversul lui A în $P(G)$. Pentru orice $A, B \in P(G)$, avem

$$(AB)^{-1} = \{(ab)^{-1} \mid a \in A, b \in B\} = \{b^{-1}a^{-1} \mid a \in A, b \in B\} = B^{-1}A^{-1}.$$

Dacă $A = \{a\}$, $a \in G$, vom scrie aB și Ba în loc de AB și BA : $aB = \{ab \mid b \in B\}$, $Ba = \{ba \mid b \in B\}$. În notație aditivă vom scrie $A+B$ și $a+B$ în loc de AB și aB :

$$A+B = \{a+b \mid a \in A, b \in B\}, \quad a+B = \{a+b \mid b \in B\}.$$

Propoziția 2.13. Fie G un grup și H o submulțime nevidă a lui G . Atunci H este subgroup al lui G dacă și numai dacă $HH = H$ și $H^{-1} = H$. Presupunând în plus că H este o submulțime finită, H este subgroup al lui G dacă și numai dacă $HH \subset H$.

Demonstrație. Presupunem că H este subgroup. Atunci în virtutea lui 1) și 3) din 2.2 (b), avem $HH \subset H$ și $H^{-1} \subset H$. În plus, $1 \in H$, deci, pentru orice $x \in H$ avem $x = x \cdot 1 \in HH$; rezultă $HH = H$. De asemenea, pentru $x \in H$, avem $x^{-1} \in H$ deci $x = (x^{-1})^{-1} \in H^{-1}$; astfel $H \subset H^{-1}$, deci $H^{-1} = H$. Reciproc, presupunem că $HH = H$ și $H^{-1} = H$. Atunci, pentru $x, y \in H$ rezultă $xy \in HH = H$, și $x^{-1} \in H^{-1} = H$, deci $xy \in H$ și $x^{-1} \in H$. Rezultă că $H \leq G$ conform propoziției 2.3 (c). Presupunem acum că H este o mulțime finită și $HH \subset H$. Atunci, pentru un $x \in H$, aplicația $\varphi_x: H \rightarrow H$ definită prin $\varphi_x(h) = xh$, $h \in H$ este injectivă conform propoziției 1.2. Deoarece H este mulțime finită, φ_x este și aplicație surjectivă. Rezultă $x = \varphi_x(h) = xh$ pentru un $h \in H$, deci $1 = h \in H$. În plus, $1 = \varphi_x(h) = xh$ pentru un $h \in H$, deci $x^{-1} = h \in H$.

Propoziția 2.14. Fie H, K subgrupuri ale unui grup G . Atunci HK este un subgroup al lui G dacă și numai dacă $HK = KH$.

Demonstrație. Dacă HK este subgroup al lui G , atunci, conform propoziției precedente, avem $HK = (HK)^{-1} = K^{-1}H^{-1} = KH$. Reciproc, presupunem $HK = KH$. Deoarece $1 = 1 \cdot 1 \in HK$, HK este o mulțime nevidă. Avem

$$(HK)(HK) = H(KH)K = H(HK)K = (HH)(KK) = HK$$

și $(HK)^{-1} = K^{-1}H^{-1} = KH = HK$, ceea ce arată, conform aceleiași propoziții, că $HK \leq G$.

Observație. Dacă H și K sunt subgrupuri ale lui G astfel ca HK este de asemenea un subgroup al lui G avem $HK = H \vee K$.

Definiția 2.15. Fie G un grup și H un subgroup al lui G . Pe mulțimea elementelor lui G considerăm relația \equiv_H (mod H) definită prin:

$$x \equiv_H y \pmod{H} \Leftrightarrow x^{-1}y \in H$$

și numită relația de congruență la stînga modulo H .

Se constată că aceasta este o relație de echivalență: pentru $x, y, z \in G$ avem $x^{-1}x = 1 \in H$, deci $x \equiv_H x \pmod{H}$; dacă $x \equiv_H y \pmod{H}$, atunci $x^{-1}y \in H$, deci $y^{-1}x = (x^{-1}y)^{-1} \in H$ și rezultă $y \equiv_H x \pmod{H}$; dacă $x \equiv_H y \pmod{H}$ și $y \equiv_H z \pmod{H}$, atunci $x^{-1}y \in H$ și $y^{-1}z \in H$ și rezultă $x^{-1}z = (x^{-1}y)(y^{-1}z) \in H$, deci $x \equiv_H z \pmod{H}$.

Mulțimea factor $G/\equiv_H \pmod{H}$ se notează simplificat (G/H) , iar elementele sale se numesc clase de congruență la stînga modulo H . Clasa de congruență la stînga modulo H a unui element $x \in G$ este $\{y \in G \mid x^{-1}y \in H\} = \{y \in G \mid y \in xH\} = xH$. Dacă $M \subseteq (G/H)$, un element $x \in M$ se numește reprezentant al clasei de congruență M . Evi-

dent, elementul $x \in G$ este reprezentant al clasei de congruență la stînga M dacă și numai dacă $M = xH$. În plus, pentru două elemente $x, y \in G$ avem

$$xH = yH \Leftrightarrow x \equiv_s y \pmod{H} \Leftrightarrow x^{-1}y \in H.$$

Reamintim de asemenea că $(G/H)_s$ este o partiție a lui G , adică o submultime a lui $P(G)$ ale cărei elemente sunt mulțimi nevide, disjuncte două cîte două a căror reuniune este G .

În mod asemănător se definește relația de congruență la dreapta modulo H :

$$x \equiv_d y \pmod{H} \Leftrightarrow xy^{-1} \in H.$$

Clasa de congruență la dreapta modulo H a unui element $x \in G$ este Hx , iar mulțimea factor $G/\equiv_d (mod H)$ se notează $(G/H)_d$.

Propoziția 2.16. *Mulțimile $(G/H)_s$ și $(G/H)_d$ sunt cardinal echivalente.*

Demonstrație. Dacă $M \in (G/H)_s$, avem $M = xH$, $x \in G$ și $M^{-1} = (xH)^{-1} = H^{-1}x^{-1} = Hx^{-1} \in (G/H)_d$. În mod analog, dacă $N \in (G/H)_d$ avem $N^{-1} \in (G/H)_s$. Prin urmare putem defini aplicațiile $\varphi: (G/H)_s \rightarrow (G/H)_d$, $\varphi(M) = M^{-1}$ și $\psi: (G/H)_d \rightarrow (G/H)_s$, $\psi(N) = N^{-1}$. Aplicațiile φ și ψ sunt evident inverse una alteia. Prin urmare, oricare din ele este o aplicație bijectivă.

Definiția 2.17. Numărul cardinal $|(G/H)_s| = |(G/H)_d|$ se notează $|G:H|$ și se numește *indicele subgrupului* H în G . De obicei spunem că H este un subgrup de indice finit în G dacă $|G:H|$ este un număr natural; în caz contrar spunem că H este de indice infinit în G și scriem $|G:H| = \infty$.

Definiția 2.18. Un grup G se numește *grup finit* dacă mulțimea G a elementelor sale este finită. În acest caz numărul natural $|G|$ se numește *ordinul* lui G . Problemele fundamentale ale teoriei grupurilor (vezi § 1) se referă în special la grupuri finite.

Dacă G este un grup infinit, numărul cardinal $|G|$ se numește de asemenea ordinul lui G . De obicei însă, în acest caz, vom scrie $|G| = \infty$ și vom spune că ordinul lui G este infinit.

Exemplu. Fie G un grup. Considerind subgrupul trivial 1 al lui G avem

$$x \equiv_s y \pmod{1} \Leftrightarrow x^{-1}y \in 1 \Leftrightarrow x = y.$$

Prin urmare relația de congruență la stînga modulo 1 (ca și relația de congruență la dreapta de altfel), coincide cu relația de egalitate pe G . Clasa de congruență la stînga modulo 1 a unui element $x \in G$ este $\{x\}$, iar

$$(G/1)_s = \{\{x\} \mid x \in G\}$$

este mulțimea tuturor submulțimilor cu un singur element ale lui G . Rezultă $|G : 1| = |G|$.

Putem considera și subgrupul impropriu G al lui G . În acest caz, pentru orice două elemente $x, y \in G$ avem $x \equiv y \pmod{G}$. Prin urmare orice clasă de congruență la stînga modulo G coincide cu G , deci

$$(G/G)_s = \{G\} \text{ și } |G : G| = 1.$$

Propoziția 2.19. (Teorema lui Lagrange.) *Pentru orice subgrup H al unui grup G avem:*

$$|G| = |H| \cdot |G : H|.$$

Demonstrație. Mulțimea factor $(G/H)_s$, fiind o partiție a lui G avem $|G| = \sum_{M \in (G/H)} |M|$. Dacă arătăm că pentru orice $M \in (G/H)_s$, avem $|M| = |H|$,

$= |H|$, va rezulta $|G| = |H| \cdot |(G/H)_s| = |H| \cdot |G : H|$. Fie atunci $M \in (G/H)_s$, deci $M = xH$ cu $x \in G$. Aplicația $\phi: H \rightarrow xH = M$ definită prin $\phi(h) = xh$, $h \in H$ este evident bijectivă și deci $|M| = |H|$.

Observație. Dacă G este un grup finit, teorema lui Lagrange arată că ordinul oricărui subgrup al lui G este un divizor al ordinului lui G . De exemplu un grup de ordinul 6 nu poate avea subgrupuri de ordinul 4.

Exemple de grupuri. Din § 1 reținem următoarele exemple de grupuri:

$Z = (Z, +)$ care se numește grupul aditiv al numerelor întregi;

$Q = (Q, +)$, grupul aditiv al numerelor raționale;

$Q^* = (Q^*, \cdot)$, grupul multiplicativ al numerelor raționale.

Analog avem:

$R = (R, +)$, grupul aditiv al numerelor reale;

$R^* = (R^*, \cdot)$, grupul multiplicativ al numerelor reale.

Foarte multe exemple de grupuri se obțin însă pe baza propoziției 2.2.

Grupuri de permutări. Fie A o mulțime și $E(A)$ mulțimea tuturor aplicațiilor $\sigma: A \rightarrow A$. Componerea aplicațiilor definește în mod evident o lege de compoziție ϕ pe mulțimea $E(A)$:

$$\phi: E(A)^2 \rightarrow E(A)$$

$$\phi(\sigma, \tau) = \sigma \circ \tau, \quad \sigma, \tau \in E(A).$$

Mulțimea $E(A)$ este monoid în raport cu legea de compoziție ϕ . Într-adevăr, se știe că compunerea aplicațiilor este asociativă, iar aplicația identică 1_A este elementul neutru. Elementele inversibile ale monoidului $E(A)$ sunt exămt aplicațiile bijective $\sigma: A \rightarrow A$; acestea se mai numesc și permutări ale mulțimii A . Grupul $U(E(A))$ al elemen-

telor inversabile ale monoidului $E(A)$ se notează cu $S(A)$ sau S_A și se numește grupul simetric pe mulțimea A , sau grupul permutărilor lui A . Un grup de permutări pe mulțimea A este un subgrup al grupului $S(A)$.

Propoziția 2.20. Dacă două mulțimi A și B sunt cardinal echivalente atunci grupurile simetrice $S(A)$ și $S(B)$ sunt izomorfe.

Demonstrație. Mulțimile A și B fiind cardinal echivalente există aplicațiile $f: A \rightarrow B$ și $g: B \rightarrow A$ astfel ca $fog = 1_B$ și $gof = 1_A$. Definim aplicațiile:

$$\varphi: S(A) \rightarrow S(B):$$

$$\varphi(\sigma) = f \circ \sigma \circ g, \quad \sigma \in S(A)$$

$(B \xrightarrow{f} A \xrightarrow{\sigma} A \xrightarrow{g} B; f \circ \sigma \circ g \in S(A))$ deoarece compunerea $f \circ \sigma \circ g$ fiind compunerea a trei aplicații bijective este de asemenea o aplicație bijectivă). Analog definim

$$\psi: S(B) \rightarrow S(A),$$

$$\psi(\tau) = g \circ \tau \circ f, \quad \tau \in S(B).$$

Aplicația φ este morfism de grupuri:

$$\varphi(\sigma \circ \sigma') = f \circ (\sigma \circ \sigma') \circ g = (f \circ \sigma \circ g) \circ (f \circ \sigma' \circ g) = \varphi(\sigma) \circ \varphi(\sigma'), \quad \sigma, \sigma' \in S(A).$$

În plus, pentru $\tau \in S(B)$,

$$(\varphi \circ \psi)(\tau) = \varphi(\psi(\tau)) = \varphi(g \circ \tau \circ f) = f \circ (g \circ \tau \circ f) \circ g = (f \circ g) \circ \tau \circ (g \circ f) = \tau,$$

deci $\varphi \circ \psi = 1_{S(B)}$. Analog $\psi \circ \varphi = 1_{S(A)}$. Aceasta arată că φ este un izomorfism de grupuri.

Importanța grupurilor de permutări rezultă din faptul că orice grup este izomorf cu un grup de permutări. Într-adevăr, avem:

Propoziția 2.21. (Teorema lui Cayley). Orice grup G este izomorf cu un grup de permutări pe mulțimea G .

Demonstrație. Este suficient să definim un morfism de grupuri injectiv $\varphi: G \rightarrow S(G)$. Fie $x \in G$ și fie $\varphi_x: G \rightarrow G$ aplicația definită prin $\varphi_x(g) = xg$. Pentru $x, y \in G$ avem

$$(\varphi_x \circ \varphi_y)(g) = \varphi_x(\varphi_y(g)) = \varphi_x(yg) = x(yg) = (xy)g = \varphi_{xy}(g)$$

deci $\varphi_x \circ \varphi_y = \varphi_{xy}$. De asemenea

$$\varphi_1(g) = 1g = g = 1_G(g),$$

deci $\varphi_1 = 1_G$, aplicația identică a mulțimii G . Prin urmare, pentru $x \in G$ avem

$$\varphi_x \circ \varphi_{x^{-1}} = \varphi_{xx^{-1}} = \varphi_1 = 1_G,$$

$$\varphi_{x^{-1}} \circ \varphi_x = \varphi_{x^{-1}x} = \varphi_1 = 1_G.$$

Aceasta arată că pentru orice $x \in G$ avem $\varphi_x \in S(G)$. Putem deci defini aplicația $\varphi: G \rightarrow S(G)$ luind $\varphi(x) = \varphi_x$, $x \in G$. φ este morfism de grupuri deoarece

$$\varphi(xy) = \varphi_{xy} = \varphi_x \circ \varphi_y = \varphi(x) \circ \varphi(y).$$

În fine, φ este morfism injectiv deoarece pentru $x \in \text{Ker } \varphi$ avem $\varphi_x = 1_G$ deci $1 = 1_G(1) = \varphi_x(1) = x$, adică $\text{Ker } \varphi = 1$.

Grupuri de automorfisme. Fie G un grup. Morfismele $f: G \rightarrow G$ se numesc și endomorfisme ale lui G . Mulțimea $\text{End}(G)$ a tuturor endomorfismelor grupului G este evident un submonoid al monoidului $E(G)$. Elementele inversabile ale monoidului $\text{End}(G)$ sunt exact izomorfismele $f: G \rightarrow G$; acestea se numesc și *automorfisme* ale lui G iar grupul $U(\text{End}(G))$ se notează cu $\text{Aut}(G)$ și se numește *grupul automorfismelor lui G*. Bineînțeles $\text{Aut}(G)$ este un subgrup al lui $S(G)$, deci $\text{Aut}(G)$ este un grup de permutări pe mulțimea G .

Un subgrup al lui $\text{Aut}(G)$ se numește grup de automorfisme ale grupului G .

Grupuri de izometrii. Reamintim că un spațiu metric este o mulțime nevidă X împreună cu o funcție distanță, adică o funcție $d: X^2 \rightarrow \mathbb{R}$ satisfăcând următoarele condiții:

- 1) $d(a, b) \geq 0$ și $d(a, b) = 0 \Leftrightarrow a = b$ pentru orice $a, b \in X$;
- 2) $d(a, b) = d(b, a)$ pentru orice $a, b \in X$;
- 3) $d(a, b) \leq d(a, c) + d(c, b)$ pentru orice $a, b, c \in X$.

Fiind dat un spațiu metric X cu funcția distanță d , o aplicație bijectivă $\sigma: X \rightarrow X$ se numește izometrie a lui X dacă $d(\sigma(a), \sigma(b)) = d(a, b)$ pentru orice $a, b \in X$. Mulțimea $\text{Izom}(X)$ a tuturor izometriilor lui X este subgrup în grupul simetric $S(X)$. Într-adevăr, se verifică condițiile 1), 2) și 3) ale propoziției 2.3 (b), astfel:

- 1) dacă $\sigma, \tau \in \text{Izom}(X)$ avem:

$$d((\sigma \circ \tau)(a), (\sigma \circ \tau)(b)) = d(\sigma(\tau(a)), \sigma(\tau(b)))$$

$$\sigma(\tau(b)) = d(\tau(a), \tau(b)) = d(a, b)$$

astfel că $\sigma \circ \tau \in \text{Izom}(X)$;

- 2) $1 \in \text{Izom}(X)$ evident;
- 3) dacă $\sigma \in \text{Izom}(X)$, avem

$$d(\sigma^{-1}(a), \sigma^{-1}(b)) = d(\sigma(\sigma^{-1}(a)), \sigma(\sigma^{-1}(b))) = d(a, b).$$

Acum dacă Y este o submulțime a spațiului metric X , notăm $\sigma(Y) = \{\sigma(y) \mid y \in Y\}$. Notăm de asemenea $S_X(Y) = \{\sigma \in \text{Izom}(X) \mid$

$\{\sigma(Y) = Y\}$ și se verifică imediat (tot pe baza propoziției 2.3 (b)) că $S_X(Y)$ este un subgrup al lui Izom (X) . Grupul $S_X(Y)$ se numește grupul de simetrie al lui Y în X . În cazul cînd X este planul euclidian E^2 (sau spațiul E^3) cu funcția distanță uzuală, $S_X(Y)$ măsoară simetria lui Y ca figură geometrică în plan (în spațiu).

Exemple de grupuri finite. Fie G un grup finit de ordinul n (sau, mai general, o mulțime finită cu n elemente împreună cu o lege de compozиție binară ϕ pe G). Legea de compозиție a grupului G (respectiv legea de compозиție ϕ) se poate descrie explicit printr-un tablou cu n linii și n coloane, aceste linii și coloane fiind indexate cu elementele x_1, x_2, \dots, x_n ale lui G , luate într-o ordine arbitrară și la intersecția liniei x_i cu coloana x_j se află elementul $x_i x_j \in G$ (sau $\phi(x_i, x_j) \in G$). Acest tablou se numește tabla de înmulțire a grupului G (sau *tabla legii de compозиție* ϕ).

Grupul C_n . Mulțimea C^* a numerelor complexe nenule este evident grup în raport cu înmulțirea numerelor complexe. Pentru fiecare număr întreg pozitiv n , notăm $C_n = \{z \in C \mid z^n = 1\}$. Evident C_n este un subgrup al lui C^* . Elementele lui C_n se numesc n -rădăcini complexe ale unității. Avem $C_1 = \{1\}$, $C_2 = \{1, -1\}$. În general, pentru orice număr întreg pozitiv n , avem

$$C_n = \{z_0, z_1, \dots, z_{n-1}\},$$

unde

$$z_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}, \quad k \in \{0, 1, \dots, n-1\}.$$

Prin urmare, C_n este un grup finit de ordin n . De exemplu

$$C_3 = \{1, z, z^2\},$$

unde

$$z = \cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3} = \frac{-1+i\sqrt{3}}{2}.$$

Avem $z^3 = 1$, de unde se poate construi imediat tabla de înmulțire a lui C_3 .

Grupul simetric S_n . Fie A o mulțime finită cu n elemente, să zicem $A = \{x_1, x_2, \dots, x_n\}$. O aplicație $\sigma: A \rightarrow A$ se poate descrie printr-un tablou cu două linii, în linia de sus apărind elementele lui A într-o ordine arbitrară, iar, în linia de jos, imaginile lor prin σ :

$$\sigma = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ \sigma(x_1) & \sigma(x_2) & \dots & \sigma(x_n) \end{pmatrix}.$$

σ este o permutare a lui A (adică o aplicație bijectivă) dacă și numai dacă σ este aplicație injectivă (adică, în linia de jos, pe locuri distincte apar elemente distincte) sau dacă și numai dacă σ este aplicație surjectivă (adică, în linia de jos apar toate elementele lui A). Putem descrie acum operațiile în grupul simetric $S(A)$ astfel:

$$\text{dacă } \sigma, \tau \in S(A), \quad \sigma = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ y_1 & y_2 & \dots & y_n \end{pmatrix}, \quad \tau = \begin{pmatrix} y_1 & y_2 & \dots & y_n \\ z_1 & z_2 & \dots & z_n \end{pmatrix}, \text{ atunci}$$

$$\sigma \circ \tau = \begin{pmatrix} x_1 x_2 & \dots & x_n \\ z_1 z_2 & \dots & z_n \end{pmatrix},$$

$$1 = \begin{pmatrix} x_1 x_2 & \dots & x_n \\ x_1 x_2 & \dots & x_n \end{pmatrix}, \quad \sigma^{-1} = \begin{pmatrix} y_1 y_2 & \dots & y_n \\ x_1 x_2 & \dots & x_n \end{pmatrix}.$$

Conform propoziției 2.20, tipul grupului $S(A)$ nu depinde de natură elementelor lui A ci numai de numărul de elemente ale lui A . De obicei se ia $A = \{1, 2, \dots, n\}$, mulțimea primelor n numere naturale și $S_n = S(A)$.

Grupul S_n este un grup finit și $|S_n| = n!$.

Pentru a demonstra aceasta, să observăm că putem defini o permutare $\sigma \in S_n$ luând imaginea primului element $1 \in A = \{1, 2, \dots, n\}$ în mod arbitrar; deci sunt n posibilități de a defini pe $\sigma(1)$. Dacă $\sigma(1)$ a fost definit, $\sigma(2)$ poate fi orice element din A diferit de $\sigma(1)$; deci sunt $n(n-1)$ posibilități de a defini perechea $(\sigma(1), \sigma(2))$. Dacă $\sigma(1)$ și $\sigma(2)$ au fost definite, $\sigma(3)$ poate fi orice element din A diferit și de $\sigma(1)$ și de $\sigma(2)$; deci sunt $n(n-1)(n-2)$ posibilități de a defini tripletul $(\sigma(1), \sigma(2), \sigma(3))$. Continuând în acest mod vedem că numărul tuturor permutărilor $\sigma \in S_n$ este $n(n-1)\dots 3.2.1 = n!$

Avem $S_1 = 1$, deoarece $|S_1| = 1$. Avem $|S_2| = 2! = 2$, și șănume

$$S_2 = \{1, \sigma\} \text{ cu } \sigma = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}. \text{ Avem evident } \sigma^2 = 1.$$

Se observă, examinând tablele de înmulțire ale grupurilor S_2 și C_2 , că avem $S_2 \cong C_2$.

Avem $|S_3| = 3! = 6$. Considerind permutările $\sigma, \tau \in S_3$, $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ și $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ avem:

$$\sigma^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \sigma^3 = 1, \quad \tau^2 = 1,$$

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \sigma^2 \circ \tau = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad \tau \circ \sigma = \sigma^2 \circ \tau.$$

Rezultă $S_3 = \{1, \sigma, \sigma^2, \tau, \sigma \circ \tau, \sigma^2 \circ \tau\}$. În plus, relațiile $\sigma^3 = 1, \tau^2 = 1, \tau \circ \sigma = \sigma^2 \circ \tau$ ne permit să construim imediat tabla de înmulțire a lui S_3 .

Grupul diedral D_n . Reamintim că printre izometriile planului euclidian E^2 sunt: translațiile, rotațiile în jurul unui punct, simetriile în raport cu o dreaptă. De asemenea este clar că o izometrie $\sigma \in \text{Izom}(E^2)$ este unic determinată de imaginile a trei puncte necoliniare; mai precis, dacă $\sigma, \tau \in \text{Izom}(E^2)$ și $x_1, x_2, x_3 \in E^2$ sunt trei puncte necoliniare astfel ca $\sigma(x_i) = \tau(x_i)$, $i \in \{1, 2, 3\}$, atunci $\sigma = \tau$.

Acum fie n un număr natural, $n \geq 3$ și P_n un poligon regulat cu n laturi în E^2 . Grupul de simetrie $D_n = SE^2(P_n)$ se numește grupul diedral de grad n . Fie O centrul poligonului P_n , A_1, A_2, \dots, A_n vîrfurile sale și $r = d(O, A_1) = \dots = d(O, A_n)$ raza cercului circumscris poligonului P_n . Pentru orice $A \in P_n$, avem $d(O, A) \leq r$ și punctul O este unic determinat de această proprietate; în plus, pentru $A \in P_n$, $d(O, A) = r$ dacă și numai dacă $A \in \{A_1, A_2, \dots, A_n\}$. Pentru $\sigma \in D_n$ și orice $A' = \sigma(A) \in P_n$, avem $d(\sigma(O), A') = d(\sigma(O), \sigma(A)) = d(O, A) \leq r$, ceea ce arată că $\sigma(O) = O$; în plus $d(O, \sigma(A)) = d(\sigma(O), \sigma(A)) = d(O, A)$, deci $A \in \{A_1, A_2, \dots, A_n\}$ dacă și numai dacă $\sigma(A) \in \{A_1, A_2, \dots, A_n\}$. Astfel, orice izometrie $\sigma \in D_n$ induce o permutare $\bar{\sigma}$ a mulțimii $\{A_1, A_2, \dots, A_n\}$ și aplicația $\phi: D_n \rightarrow S_n$, $\phi(\sigma) = \bar{\sigma}$ este un morfism de grupuri injectiv (ϕ este aplicație injectivă deoarece există cel puțin trei vîrfuri A_1, A_2, A_3 și acestea sint necoliniare). Prin urmare grupul D_n se poate scufunda în S_n .

Pentru a defini o izometrie $\sigma \in D_n$, $\sigma(A_1)$ poate fi oricare din cele n vîrfuri A_1, A_2, \dots, A_n dar, dacă $\sigma(A_1)$ a fost definit, $\sigma(A_2)$ nu poate fi decât unul din cele două vîrfuri alăturate lui $\sigma(A_1)$ (deoarece $d(\sigma(A_1), \sigma(A_2)) = d(A_1, A_2)$ și distanța între două vîrfuri nealăturate este $> d(A_1, A_2)$). Dacă $\sigma(A_1)$ și $\sigma(A_2)$ sint definite, izometria este perfect determinată ($(\sigma(O) = O)$ și σ este unic determinată de imaginile a trei puncte necoliniare). Rezultă că există cel mult $2n$ posibilități de a defini o izometrie $\sigma \in D_n$; altfel spus $|D_n| \leq 2n$. Pe de altă parte, rotațiile de unghi $\frac{2k\pi}{n}$, $k \in \{0, 1, \dots, n-1\}$, în jurul lui O și simetriile în cele n axe de simetrie ale poligonului P_n sint izometrii aparținând lui D_n . Prin urmare $2n \leq |D_n|$ și deci $|D_n| = 2n$. Dacă σ este rotația de unghi $\frac{2\pi}{n}$ în jurul lui O și τ este simetria intr-una din axele de simetrie ale lui P_n , avem $\sigma^n = 1, \tau^2 = 1, \rho \circ \sigma = \sigma^{n-1} \circ \rho$ și

$$D_n = \{1, \sigma, \sigma^2, \dots, \sigma^{n-1}, \rho, \sigma \circ \rho, \sigma^2 \circ \rho, \dots, \sigma^{n-1} \circ \rho\}.$$

Deoarece D_3 se poate scufunda în S_3 și $|D_3| = |S_3| = 6$, rezultă $D_3 \cong S_3$. Pentru a descrie grupul diedral D_4 , observăm că

$$D_4 = \{1, \sigma, \sigma^2, \sigma^3, \rho, \sigma\circ\rho, \sigma^2\circ\rho, \sigma^3\circ\rho\} \quad \text{și} \quad \sigma^4=1, \quad \rho^2=1, \quad \rho\circ\sigma = \sigma^3\circ\rho$$

și se poate obține imediat tabla de înmulțire a grupului D_4 .

Puteam defini grupul diedral D_n și pentru numere naturale $n \leq 2$. Astfel D_2 se definește ca grupul de simetrie al unui dreptunghi care nu este pătrat. Notind cu σ și τ simetriile în raport cu cele două axe de simetrie ale dreptunghiului, $\sigma\circ\tau = \tau\circ\sigma$ este simetria în raport cu centrul dreptunghiului. Avem

$$D_2 = \{1, \sigma, \tau, \sigma\circ\tau\} \quad \text{cu} \quad \sigma^2=1, \quad \tau^2=1, \quad \tau\circ\sigma=\sigma\circ\tau.$$

Grupul D_2 se numește de obicei grupul lui Klein.

Grupul D_1 se definește ca fiind grupul de simetrie al unui segment. Notind cu σ simetria în raport cu mijlocul segmentului avem $D_1 = \{1, \sigma\}$ cu $\sigma^2=1$. Se vede imediat că grupurile D_1 și C_2 sunt izomorfe.

Grupul D_0 se poate defini ca fiind grupul trivial $D_0 = 1$.

Grupul cauterionilor. Considerind matricele complexe $j = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$,

$k = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ se observă imediat că avem $j^4=1$ (aici 1 este matricea identică $1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $j^2=k^2$, $kj=j^3k$ (pentru detalii privind înmulțirea matricilor vezi cap. III, § 1). Datorită relațiilor de mai sus, mulțimea $Q = \{1, j, j^2, j^3, k, jk, j^2k, j^3k\}$ este parte stabilă în raport cu înmulțirea matricilor. Înmulțirea matricilor, în general, este asociativă și are ca element neutru matricea identică $1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Examinând tabla de înmulțire a legii de compoziție induse de înmulțirea matricilor pe Q , se constată imediat că Q este grup în r. ort cu această lege de compoziție indușă. Grupul Q se numește *grupul cauterionilor*.

Grupul aditiv al numerelor întregi. După cum am mai remarcat $(\mathbb{Z}, +)$, unde \mathbb{Z} este mulțimea numerelor întregi și $+$ este adunarea numerelor întregi, este un grup. Acest grup se numește grupul aditiv al numerelor întregi și, pentru comoditate, îl vom nota tot cu \mathbb{Z} , ca și mulțimea numerelor întregi. (În capitolul următor, vom nota cu \mathbb{Z} inelul numerelor întregi și cu \mathbb{Z}^+ grupul aditiv al numerelor întregi). Grupul \mathbb{Z} este un grup ciclic, un generator al său fiind numărul întreg 1:

$$\langle 1 \rangle = \{m \mid m \in \mathbb{Z}\} = \mathbb{Z}.$$

Evident, avem și $\langle -1 \rangle = \mathbb{Z}$. 1 și -1 sint singurii generatori ai lui \mathbb{Z} . Într-adevăr, dacă $n \in \mathbb{Z}$ și $\langle n \rangle = \mathbb{Z}$, avem $1 \in \langle n \rangle$, deci $1 = mn$ cu $m \in \mathbb{Z}$ de unde rezultă $n = \pm 1$. În general, pentru un număr $n \in \mathbb{Z}$ subgrupul lui \mathbb{Z} generat de n este: $\langle n \rangle = \{nk \mid k \in \mathbb{Z}\}$. Notăm acest subgrup cu $n\mathbb{Z}$.

Propoziția 2.22. i) Pentru orice subgrup H al lui \mathbb{Z} există un unic număr natural n , astfel ca $H = n\mathbb{Z}$.

ii) Pentru $m, n \in \mathbb{Z}$ avem: $m\mathbb{Z} \leq n\mathbb{Z} \Leftrightarrow m|n$

iii) Pentru $m, n \in \mathbb{Z}$ avem:

$$m\mathbb{Z} + n\mathbb{Z} = (m, n)\mathbb{Z} \text{ și } m\mathbb{Z} \cap n\mathbb{Z} = [m, n]\mathbb{Z},$$

(unde (m, n) este cel mai mare divizor comun al lui m și n iar $[m, n]$ este cel mai mic multiplu comun al lor).

Demonstrație. Fie $H \leq \mathbb{Z}$. Dacă H este subgrupul trivial avem $H = \{0\} = 0\mathbb{Z}$. Presupunem că H este netrivial. Atunci există un $n \in H$, $n \neq 0$. Avem $n > 0$ sau $n < 0$ și, în ultimul caz, avem $-n \in H$, $-n > 0$. Deci, există un $n \in H$, $n > 0$. Putem considera atunci cel mai mic număr întreg pozitiv n care aparține lui H . Deoarece $n \in H$ avem $n\mathbb{Z} = \langle n \rangle \leq H$. Fie $m \in H$. Aplicind teorema împărțirii cu rest avem $m = nq + r$ cu $q, r \in \mathbb{Z}$ și $0 \leq r < n$. Deoarece $m \in H$ și $nq \in n\mathbb{Z} \leq H$, avem $r = m - nq \in H$. Astfel $H \leq n\mathbb{Z}$, deci $H = n\mathbb{Z}$. Unicitatea numărului natural n cu $H = n\mathbb{Z}$ rezultă după ce demonstrăm (ii).

Pentru $m, n \in \mathbb{Z}$ avem:

$$m\mathbb{Z} \leq n\mathbb{Z} \Leftrightarrow \langle m \rangle \leq n\mathbb{Z} \Leftrightarrow m \in n\mathbb{Z} \Leftrightarrow n|m$$

ceea ce demonstrează (ii). Acum dacă $H = m\mathbb{Z} = n\mathbb{Z}$ cu m și n numere naturale, rezultă $m|n$ și $n|m$, deci $m = n$.

Deoarece \mathbb{Z} este grup abelian, $m\mathbb{Z} + n\mathbb{Z}$ este subgrup al lui \mathbb{Z} conform propoziției 2.14. Prin urmare $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$, cu d număr natural. Avem $m\mathbb{Z} \leq m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$, deci $d|m$; analog $d|n$. Pentru orice număr întreg d' cu $d'|m$ și $d'|n$, rezultă $m\mathbb{Z} \leq d'\mathbb{Z}$ și $n\mathbb{Z} \leq d'\mathbb{Z}$, deci

$$d\mathbb{Z} = m\mathbb{Z} + n\mathbb{Z} = m\mathbb{Z} \vee n\mathbb{Z} \leq d'\mathbb{Z}, \text{ de unde } d'|d.$$

Astfel $d = (m, n)$ și $m\mathbb{Z} + n\mathbb{Z} = (m, n)\mathbb{Z}$. Egalitatea $m\mathbb{Z} \cap n\mathbb{Z} = (m, n)\mathbb{Z}$ se demonstrează într-un mod analog.

Observație. Propoziția precedentă ne permite să demonstrăm unele fapte de aritmetică elementară. Astfel, date două numere întregi m și n , m și n sint prime între ele (adică $(m, n) = 1$), dacă și numai dacă există două numere întregi m' și n' astfel că $mm' + nn' = 1$:

$$(m, n) = 1 \Leftrightarrow m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z} \Leftrightarrow 1 \in m\mathbb{Z} + n\mathbb{Z} \Leftrightarrow \exists m', n' \in \mathbb{Z}: 1 = mm' + nn'.$$

Propoziția 2.23. Pentru orice număr natural n , avem:

$$|\mathbb{Z}:n\mathbb{Z}| = \begin{cases} n & \text{dacă } n \geq 1, \\ \infty & \text{dacă } n=0. \end{cases}$$

Demonstrație. Pentru $n=0$, $0\mathbb{Z}$ este subgrupul trivial deci $|\mathbb{Z}:0\mathbb{Z}| = |\mathbb{Z}| = \infty$. Presupunem $n \geq 1$. Pentru orice $x \in \mathbb{Z}$ avem $x = nq + r$ cu $q, r \in \mathbb{Z}$ și $0 \leq r < n$; deoarece $x - r = nq \in n\mathbb{Z}$, avem $x \equiv r \pmod{n\mathbb{Z}}$ deci $x + n\mathbb{Z} = r + n\mathbb{Z}$. Astfel

$$(\mathbb{Z}/n\mathbb{Z})_d = \{x + n\mathbb{Z} | x \in \mathbb{Z}\} = \{r + n\mathbb{Z} | 0 \leq r < n\}.$$

Este suficient să demonstrăm că mulțimea $\{r + n\mathbb{Z} | 0 \leq r < n\}$ are exact n

elemente. Pentru aceasta observăm că dacă $i, j \in \{0, 1, \dots, n-1\}$ și $i < j$, atunci $i+n\mathbb{Z} \neq j+n\mathbb{Z}$; într-adevăr, egalitatea $i+n\mathbb{Z} = j+n\mathbb{Z}$ ar implica $j-i \in n\mathbb{Z}$, deci $0 < j-i < n$ și totodată $n|j-i$, ceea ce este absurd.

Observație. De obicei, pentru $x, y \in \mathbb{Z}$ scriem $x \equiv y \pmod{n}$ în loc de $x \equiv_{n\mathbb{Z}} y \pmod{n\mathbb{Z}}$ (de fapt, în acest caz, relația de congruență la stânga modul $n\mathbb{Z}$ coincide cu relația de congruență la dreapta).

Notând pe scurt clasa de congruență $x+n\mathbb{Z}$ cu \bar{x} , avem: $(\mathbb{Z}/n\mathbb{Z})_d = \{\bar{0}, \bar{1}, \dots, \bar{n-1}\}$ și această mulțime are n elemente.

Numărul tipurilor de grupuri de ordinul n . Pentru orice număr întreg pozitiv n se notează cu $v(n)$ numărul tipurilor de grupuri de ordin n . Nu se cunoaște nici o „formulă” generală pentru funcția v . Se cunosc însă diferite majorări ale sale și una din aceste majorări rezultă imediat din teorema lui Cayley (vezi propoziția 2.21). : $v(n) \leq 2^n!$. Deoarece pentru orice n există cel puțin un grup de ordinul n , avem $1 \leq v(n)$. Evident, $v(1) = 1$.

Pentru orice număr prim p , avem $v(p) = 1$. Aceasta rezultă imediat folosind următoarele două propoziții:

Propoziția 2.24. *Orice grup finit G de ordin p , unde p este număr prim, este ciclic.*

Demonstrație. Fie $1 \neq g \in G$ și $H = \langle g \rangle$, subgrupul ciclic al lui G generat de g . Deoarece $|H| |G| = p$ și $1 \neq |H|$ avem $|H| = |G|$, astfel că $G = H = \langle g \rangle$.

Propoziția 2.25. *Orice două grupuri ciclice având același ordin sunt izomorfe.*

Demonstrație. O demonstrație clară a acestei propoziții se obține în paragraful următor, pe baza teoremei fundamentale de izomorfism (vezi propoziția 3.15). Momentan sugerăm cititorului să improvizeze singur demonstrația în unele cazuri particulare: cele două grupuri ciclice au ordinul n , unde $n = 2, 3, 4, 5$ etc.

Grupuri de ordinul 4. Fie G un grup de ordinul 4. Presupunem că există un element $x \in G$ cu $x^2 \neq 1$. Nu putem avea $x^3 = 1$ deoarece în acest caz $\{1, x, x^2\}$ ar fi un subgrup de ordinul 3 al lui G , contrar teoremei lui Lagrange. Prin urmare $x^3 \neq 1$ și evident $x^3 \neq x$, $x^3 \neq x^2$. Aceasta arată că $G = \{1, x, x^2, x^3\} = \langle x \rangle$, deci G este un grup ciclic. Presupunem acum că pentru orice element $x \in G$ avem $x^2 = 1$. Fie $x, y \in G$ cu $x \neq 1, y \neq 1, x \neq y$. Deoarece $xy = x$ implică $y = 1$, $xy = y$ implică $x = 1$ iar $xy = 1$ implică $x = 1 = xy^2 = xyy^{-1} = y = y$, rezultă $G = \{1, x, y, xy\}$. În plus, avem $yx = y^{-1}x^{-1} = (xy)^{-1} = xy$ (ultima egalitate are loc deoarece $(xy)^2 = 1$). Relațiile $x^2 = 1$, $y^2 = 1$ și $xy = yx$ arată că tabla de înmulțire a lui G coincide cu tabla de înmulțire a grupului D_2 , de unde rezultă $G \cong D_2$. Prin urmare G este ciclic sau $G \cong D_2$. Deoarece orice două grupuri ciclice având același ordin sunt izomorfe, avem $G \cong C_4$ sau $G \cong D_2$. Pe de altă parte, este evident că $C_4 \not\cong D_2$. Astfel $v(4) = 2$.

Grupuri de ordinul 6. Fie G un grup de ordinul 6. Atunci există un element $x \in G$ cu $x^2 \neq 1$. Într-adevăr, dacă pentru orice $x \in G$ avem $x^2 = 1$, atunci, alegind două elemente $x, y \in G$ cu $x \neq 1, y \neq 1, x \neq y$, se constată, ca mai sus, că $xy = yx$ și relațiile $x^2 = 1, y^2 = 1, xy = yx$ arată că $\{1, x, y, xy\}$ este un subgrup de ordinul 4 al lui G , contrar teoremei lui Lagrange. Fie deci $x \in G$ cu $x^2 \neq 1$ și fie $H = \langle x \rangle$, subgrupul ciclic al lui G generat de x . Dacă $x^3 \neq 1$, atunci 1, x, x^2, x^3 sunt patru elemente distincte, două cîte două, din H , deci $3 < |H| \leq 6$. Aceasta arată că $|H| = 6 = |G|$, deci $H = G$ și G este ciclic. Noi vom presupune că G nu este ciclic. Atunci $x^3 = 1$ și $H = \{1, x, x^2\}$. Alegem un element $y \in G - H$ și avem, deoarece $|G:H| =$

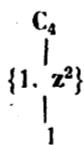
$$= \frac{|G|}{|H|} = \frac{6}{3} = 2, \quad (G/H)_d = \{H, Hy\} \text{ și } G = H \cup Hy = \{1, x, x^2, y, xy, x^2y\}.$$

Nu putem avea $y^2 = xy$ sau $y^2 = x^2y$ ($y^2 = xy$ implică $y = x \in H$, iar $y^2 = x^2y$ implică $y = x^2 \in H$). De asemenea nu putem avea $y^2 = x$ sau $y^2 = x^2$ (dacă $y^2 = x$, atunci $G = \{1, y^2, y^4, y, y^3, y^5\} = \langle y \rangle$ și dacă $y^2 = x^2$, atunci $1 = x^3 = x^2x = y^2x$, deci $x = y^{-2}$ și iarăși, rezultă $G = \langle y \rangle$). Prin urmare $y^2 = 1$. Nu putem avea $yx = 1, yx = x, yx = x^2, yx = y(yx = 1 \Rightarrow y = x^{-1} \in H, yx = x \Rightarrow y = 1, yx = x^2 \Rightarrow y = x, yx = y \Rightarrow x = 1)$. De asemenea nu putem avea $yx = xy$. (Dacă $yx = xy$, atunci $(xy)^2 = x^2y^2 = x^2, (xy)^3 = x^3y^3 = y, (xy)^4 = x^4y^4 = x, (xy)^5 = x^5y^5 = x^2y$ și rezultă $G = \langle xy \rangle$). Prin urmare $yx = x^2y$. Relațiile $x^3 = 1, y^2 = 1, yx = x^2y$ arată imediat că tabla de înmulțire a lui G este identică cu tabla de înmulțire a grupului S_3 . Astfel $G \cong S_3$.

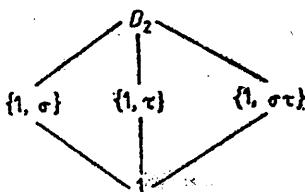
Prin urmare, pentru orice grup G de ordin 6, avem $G \cong C_6$ sau $G \cong S_3$. Deoarece evident $C_6 \not\cong S_3$, rezultă $v(6) = 2$.

După cum se știe, orice latice cu un număr finit de elemente se poate reprezenta printr-o diagramă în care liniile unesc două elemente, alăturate. În continuare vom descrie laticea subgrupurilor $\mathcal{L}(G)$ pentru unele din grupurile finite care au apărut pînă acum.

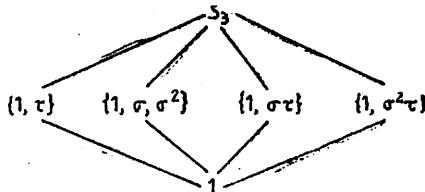
Laticea subgrupurilor lui C_4 . După cum am văzut avem $C_4 = \{1, z, z^2, z^3\}$ cu $z^4 = 1$ sau altfel spus $C_4 = \{1, -1, i, -i\} \subset C^*$. În afara subgrupurilor evidente 1 și C_4 de ordin 1 și respectiv de ordin 4, C_4 mai poate avea, conform teoremei lui Lagrange, subgrupuri de ordin 2. Un subgrup H de ordin 2 este de forma $H = \{1, x\}$ cu $x \in C_4$ și $x^2 = 1, x \neq 1$. Se vede ușor că singurul element $x \in C_4$ cu $x^2 = 1, x \neq 1$ este $x = z^2$. Prin urmare $H = \{1, z^2\}$ este unicul subgrup de ordinul 2 al lui C_4 iar laticea subgrupurilor lui C_4 se prezintă prin:



Laticea subgrupurilor lui D_2 . Avem $D_2 = \{1, \sigma, \tau, \sigma\tau\}$ cu $\sigma^2 = 1$, $\tau^2 = 1$, $\sigma\tau = \tau\sigma$. Se vede că elementele $x \in D_2$ cu $x^2 = 1$, $x \neq 1$ sunt σ, τ și $\sigma\tau$. Prin urmare D_2 are trei subgrupuri de ordin 2, anume $\{1, \sigma\}$, $\{1, \tau\}$, $\{1, \sigma\tau\}$ și laticea subgrupurilor lui D_2 se reprezintă prin:



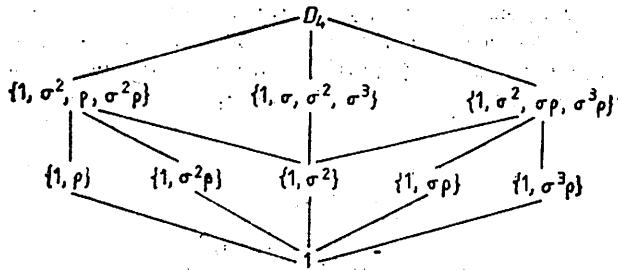
Laticea subgrupurilor lui S_3 . Conform teoremei lui Lagrange subgrupurile lui S_3 pot avea ordinele 1, 2, 3 sau 6. Subgrupurile de ordinul 2 ale lui S_3 sunt de forma $H = \{1, x\}$ cu $x \in S_3$, $x^2 = 1$, $x \neq 1$. Examînînd tabla de înmulțire a lui S_3 găsim trei astfel de subgrupuri: $\{1, \tau\}$, $\{1, \sigma\tau\}$, $\{1, \sigma^2\tau\}$. Subgrupurile de ordinul 3 ale lui S_3 sunt de forma $H = \{1, x, x^2\}$ cu $x \in S_3$, $x^3 = 1$, $x \neq 1$. Găsim un singur subgrup de ordinul 3, anume $\{1, \sigma, \sigma^2\}$. Laticea subgrupurilor lui S_3 se reprezintă deci prin:



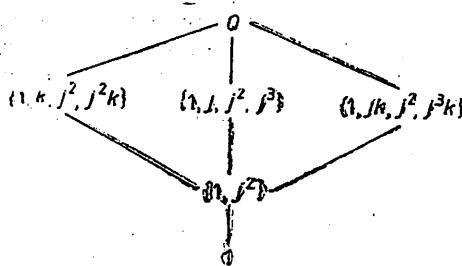
Laticea subgrupurilor lui D_4 . Subgrupurile lui D_4 pot avea ordinele 1, 2, 4 sau 8. Subgrupurile de ordinul 2 sunt de forma $H = \{1, x\}$ cu $x \in D_4$, $x^2 = 1$, $x \neq 1$. Examînînd tabla de înmulțire a lui D_4 găsim cinci astfel de subgrupuri:

$$\{1, \rho\}, \{1, \sigma\rho\}, \{1, \sigma^2\rho\}, \{1, \sigma^3\rho\}, \{1, \sigma^2\}.$$

Subgrupurile de ordinul 4 ale lui D_4 sunt fie ciclice, deci de forma $\{1, x, x^2, x^3\}$ cu $x \in D_4$, $x \neq 1$, $x^4 = 1$, fie de tipul grupului lui Klein D_2 , deci de forma $\{1, x, y, xy\}$ cu $x, y \in D_4$, $x \neq 1$, $y \neq 1$, $x^2 = 1$, $y^2 = 1$; $xy = yx$. Găsim un unic subgrup ciclic de ordinul 4, anume $\{1, \sigma, \sigma^2, \sigma^3\}$ și două subgrupuri de tipul grupului lui Klein, anume $\{1, \sigma^2, \rho, \sigma^2\rho\}$, $\{1, \sigma^2, \sigma\rho, \sigma^3\rho\}$. Laticea subgrupurilor lui D_4 se reprezintă prin:



Laticea subgrupurilor lui Q . Conform tablei sale de înmulțire grupul Q are un unic subgrup de ordinul doi, anume $\{1, j^2\}$ și trei subgrupuri ciclice de ordinul 4. Datorită faptului că singurul element $x \in Q$ cu $x \neq 1, x^2 = 1$ este j^2 , Q nu are subgrupuri de tipul grupului lui Klein. Laticea subgrupurilor lui Q se reprezintă prin



§ 3. GRUPURI FACTOR. TEOREME DE IZOMORFISM

Propoziția 3.1. Fie G un grup și H un subgrup al lui G . Următoarele afirmații sunt echivalente:

- pentru orice $x \in G$ avem $xHx^{-1} \subseteq H$,
- pentru orice $x \in G$ avem $xHx^{-1} = H$,
- pentru orice $x \in G$ avem $xH = Hx$,
- $(G/H)_s = (G/H)_d$.

Demonstrație. a) \Rightarrow a'). Pentru orice $x \in G$ avem, prin ipoteză, atât $xHx^{-1} \subseteq H$ cât și $x^{-1}Hx \subseteq H$; din ultima inclusiune rezultă $H = x(x^{-1}Hx)x^{-1} \subseteq xHx^{-1}$, deci $xHx^{-1} = H$.

a') \Rightarrow a) este evident.
- a') \Rightarrow b) Dacă $xHx^{-1} = H$, atunci $xH = (xHx^{-1})x = Hx$.
- b) \Rightarrow a') Dacă $xH = Hx$, atunci $xHx^{-1} = (Hx)x^{-1} = H$.
- b) \Rightarrow c) este evident.

c) \Rightarrow b). Fie $x \in G$. Atunci $xH \in (G/H)_s = (G/H)_d$, deci $xH = Hy$ pentru un $y \in G$. Deoarece $x^{-1}x \in xH = Hy$, avem $Hx = Hy$, deci $xH = Hy$.

Definiția 3.2. Un subgrup H al unui grup G se numește *subgrup normal* al lui G (sau *subgrup normal* în G) dacă este satisfăcută una din afirmațiile echivalente ale propoziției precedente. Pentru a indica faptul că H este un subgrup normal al lui G , vom scrie $H \trianglelefteq G$.

Propoziția 3.3. Orice subgrup H al unui grup G cu $|G:H|=2$ este normal în G .

Demonstrație. Avem $H = 1$ și $H \in (G/H)_s$, și deoarece $|(G/H)_s| = |G:H| = 2$, rezultă $(G/H)_s = \{H, G-H\}$. De asemenea, $H = H_1 \in (G/H)_d$ și deoarece $|(G/H)_d| = |G:H| = 2$, avem $(G/H)_d = \{H, G-H\}$. Prin urmare $(G/H)_s = (G/H)_d$ și $H \trianglelefteq G$ conform punctului c) al propoziției 3.1.

Propoziția 3.4. Pentru orice familie $\{H_i\}_{i \in I}$ de subgrupuri normale ale unui grup G , intersecția $\bigcap_{i \in I} H_i$ este de asemenea un subgrup normal în G .

Demonstrație. Știm deja că $\bigcap_{i \in I} H_i \leqslant G$. Vom verifica că $\bigcap_{i \in I} H_i$ satisface condiția a) a propoziției 3.1, astfel: pentru $h \in \bigcap_{i \in I} H_i$ și $x \in G$, avem, oricare ar fi $i \in I$, $h \in H_i$ și deoarece $H_i \trianglelefteq G$, $xhx^{-1} \in xH_i x^{-1} \subset H_i$, deci $xhx^{-1} \in \bigcap_{i \in I} H_i$.

Observație. Multimea $L_n(G)$ a tuturor subgrupurilor normale ale unui grup G este o multime ordonată, relația de ordine fiind inclusiunea. Propoziția 3.4 arată că $L_n(G)$ este o latică completă, înfimul oricărei familii $\{H_i\}_{i \in I}$ de elemente din $L_n(G)$ fiind intersecția $\bigcap_{i \in I} H_i$. Cel mai mic element al laticii $L_n(G)$ este subgrupul trivial 1, iar cel mai mare element este subgrupul impróprietății G .

Propoziția 3.5. (Teorema de corespondență pentru subgrupuri normale.) Fie $f: G \rightarrow G'$ un morfism de grupe. Au loc următoarele afirmații:

i) Dacă $K \trianglelefteq G'$, atunci $f^{-1}(K) \trianglelefteq G$.

ii) Dacă f este surjectiv și $H \trianglelefteq G$, atunci $f(H) \trianglelefteq G'$.

iii) Dacă f este surjectiv, aplicația $H \sim \rightarrow f(H)$, de la mulțimea subgrupurilor normale ale lui G care conțin $\text{Ker } f$ în mulțimea subgrupurilor normale ale lui G' , este bijectivă.

Demonstrație. i) Avem $f^{-1}(K) \leqslant G$, conform propoziției 2.5. Pentru $x \in G$ și $h \in f^{-1}(K)$ avem $f(h) \in K$ și $f(xhx^{-1}) = f(x)f(h)f(x)^{-1} \in K$ deoarece $K \trianglelefteq G'$, deci $xhx^{-1} \in f^{-1}(K)$. Aceasta arată că $f^{-1}(K) \trianglelefteq G$.

ii) Avem $f(H) \leq G'$ conform propoziției 2.5. Pentru $y \in G'$ și $k \in f(H)$ avem $y = f(x)$, $x \in G$, deoarece f este aplicație surjectivă și $k = f(h)$, $h \in H$, conform definiției lui $f(H)$. Prin urmare $yky^{-1} = f(x)f(h)f(x)^{-1} = -f(xhx^{-1}) \in f(H)$ deoarece $xhx^{-1} \in H$. Aceasta arată că $f(H) \trianglelefteq G'$.

iii) Rezultă imediat din cele două puncte precedente și teorema de corespondență 2.8.

Propoziția 3.6. Fie $f: G \rightarrow G'$ un morfism de grupuri. Atunci $\text{Ker } f \trianglelefteq G'$.

Demonstrație. Avem $\text{Ker } f = f^{-1}(1)$ și $1 \trianglelefteq G'$, deci $\text{Ker } f \trianglelefteq G$ conform punctului i) al propoziției de mai sus.

Definiția 3.6. Fie G un grup, $g \in G$ și considerăm aplicația $\tau_g: G \rightarrow G$ definită prin $\tau_g(x) = gxg^{-1}$, pentru $g, g' \in G$. Avem:

$$(\tau_g \circ \tau_{g'})(x) = \tau_g(g'xg'^{-1}) = gg'xg'^{-1}g^{-1} = \tau_{gg'}(x).$$

În plus, este clar că $\tau_1 = 1_G$. Rezultă $\tau_g \circ \tau_{g^{-1}} = \tau_1 = 1_G$, $\tau_{g^{-1}} \circ \tau_g = \tau_1 = 1_G$, deci τ_g este o permutare a lui G cu $\tau_{g^{-1}} = \tau_{g^{-1}}$. τ_g este de fapt un automorfism al lui G :

$$\tau_g(xy) = g(xy)g^{-1} = (gxg^{-1})(gyg^{-1}) = \tau_g(x)\tau_g(y).$$

τ_g se numește *automorfismul interior* al lui G definit de elementul $g \in G$. Deoarece $\tau_g \circ \tau_{g'} = \tau_{gg'}$, pentru orice $g, g' \in G$, aplicația $\tau: G \rightarrow \text{Aut}(G)$, definită prin $\tau(g) = \tau_g$, este un morfism de grupuri. Prin urmare, multimea $\text{Inn}(G) = \text{Im } \tau$ a tuturor automorfismelor interioare ale lui G este un subgrup al lui $\text{Aut}(G)$. Deoarece, pentru orice $\sigma \in \text{Aut}(G)$ și orice $g \in G$, avem

$$(\sigma \tau_g \sigma^{-1})(x) = \sigma(g\sigma^{-1}(x)g^{-1}) = \sigma(g)x\sigma(g)^{-1} = \tau_{\sigma(g)}(x),$$

rezultă $\sigma \tau_g \sigma^{-1} = \tau_{\sigma(g)} \in \text{Inn}(G)$, ceea ce arată că $\text{Inn}(G) \trianglelefteq \text{Aut}(G)$.

Fie H un subgrup al lui G . Pentru orice element $x \in G$ avem $\tau_x(H) = xHx^{-1}$. Aceasta arată că, pentru orice $x \in G$, xHx^{-1} este de asemenea un subgrup al lui G și, în plus, $H \trianglelefteq G$ dacă și numai dacă $\tau_x(H) = H$ pentru orice automorfism interior τ_x al lui G .

Un subgrup H al lui G se numește caracteristic în G dacă pentru orice $\sigma \in \text{Aut}(G)$ avem $\sigma(H) = H$. Conform celor de mai sus, orice subgrup caracteristic în G este normal în G .

Propoziția 3.7. Fie $K \leq H \leq G$. Presupunem că K este caracteristic în H și H este normal în G . Atunci K este normal în G .

Demonstrație. Fie $g \in G$. Avem $\tau_g(H) = H$ deci putem defini aplicația $\sigma: H \rightarrow H$ prin $\sigma(h) = \tau_g(h)$. Deoarece τ_g este un automorfism al lui G , rezultă $\sigma \in \text{Aut}(H)$. Avem $K = \sigma(K) = \tau_g(K)$, deci $K \trianglelefteq G$.

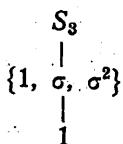
Propoziția 3.8. Fie H un subgrup finit al unui grup G . Presupunem că $|H| = n$ și că H este unicul subgrup de ordin n al lui G . Atunci H este caracteristic în G și, în particular, $H \trianglelefteq G$.

Demonstrație. Fie $\sigma \in \text{Aut}(G)$. Atunci, conform propoziției 2.5., $\sigma(H) \leq G$. În plus, $|\sigma(H)| = |H| = n$ și în virtutea ipotezei, $\sigma(H) = H$.

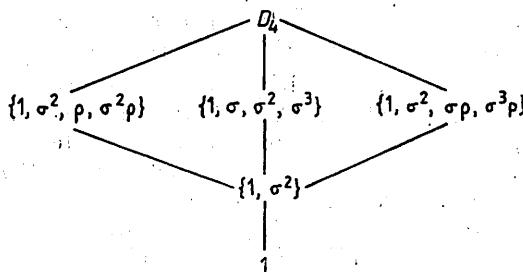
Alte exemple de subgrupuri normale. Dacă G este un grup abelian, orice subgrup H al lui G este normal în G . Aceasta este evident, egalitatea $xH=Hx$ rezultând din comutativitatea legii de compoziție a lui G .

Subgrupurile normale ale lui S_3 . Subgrupul $\{1, \sigma, \sigma^2\}$ al lui S_3 este normal în S_3 deoarece are indicele 2 în S_3 . Subgrupurile $\{1, \tau\}$, $\{1, \sigma\tau\}$, $\{1, \sigma^2\tau\}$ ale lui S_3 nu sunt normale în S_3 :

$\{1, \tau\}$ nu este normal deoarece $\sigma\tau\sigma^{-1}=\sigma^2\tau \notin \{1, \tau\}$; $\{1, \sigma\tau\}$ nu este normal deoarece $\sigma(\sigma\tau)\sigma^{-1}=\tau \notin \{1, \sigma\tau\}$; $\{1, \sigma^2\tau\}$ nu este normal deoarece $\sigma(\sigma^2\tau)\sigma^{-1}=\sigma\tau \notin \{1, \sigma^2\tau\}$. Laticea subgrupurilor normale ale lui S_3 este:



Subgrupurile normale ale lui D_4 . Subgrupurile $\{1, \sigma, \sigma^2, \sigma^3\}$, $\{1, \sigma^2, \rho, \sigma^2\rho\}$, $\{1, \sigma^2, \sigma\rho, \sigma^3\rho\}$ ale lui D_4 sunt normale deoarece au indicele 2 în D_4 . $\{1, \sigma^2\}$ este normal fiind intersecția a două subgrupuri normale: $\{1, \sigma^2\} = \{1, \sigma^2, \rho, \sigma^2\rho\} \cap \{1, \sigma^2, \sigma\rho, \sigma^3\rho\}$. Subgrupurile $\{1, \rho\}$, $\{1, \sigma\rho\}$, $\{1, \sigma^2\rho\}$, $\{1, \sigma^3\rho\}$ ale lui D_4 nu sunt normale: $\sigma\rho\sigma^{-1}=\sigma^2\rho \notin \{1, \rho\}$, $\sigma(\sigma\rho)\sigma^{-1}=\sigma^3\rho \notin \{1, \sigma\rho\}$, $\sigma(\sigma^2\rho)\sigma^{-1}=\rho \notin \{1, \sigma^2\rho\}$, $\sigma(\sigma^3\rho)\sigma^{-1}=\sigma\rho \notin \{1, \sigma^3\rho\}$. Laticea subgrupurilor normale ale lui D_4 este:



Se observă că deși $\{1, \rho\} \trianglelefteq \{1, \sigma^2, \rho, \sigma^2\rho\} \trianglelefteq D_4$ nu avem $\{1, \rho\} \trianglelefteq D_4$. Conform propoziției 3.7, rezultă că $\{1, \rho\}$ nu este subgrup caracteristic în $\{1, \sigma^2, \rho, \sigma^2\rho\}$.

Subgrupurile normale ale lui Q . Subgrupurile de ordinul 4 ale lui Q sunt normale deoarece au indicele 2. Unicul subgrup $\{1, j^2\}$ de ordinul 2 este de asemenea normal în virtutea propoziției 3.8. Rezultă că, deși Q nu este grup abelian, orice subgrup al lui Q este normal.

Fie G un grup și H un subgrup al lui G . Multimea (G/H) este o submulțime a monoidului $P(G)$ definit în §2.

Propoziția 3.9. H este subgrup normal al lui G dacă și numai dacă (G/H) , este subgrup al monoidului $P(G)$.

Demonstrație. Presupunem $H \trianglelefteq G$. Luând două elemente $xH, yH \in (G/H)$, $x, y \in G$ și aplicând propoziția 3.1. c) avem:

$$(xH)(yH) = x(Hy)H = x(yH)H = (xy)HH = xyH.$$

Aceasta arată că (G/H) , este parte stabilă a lui $P(G)$. Legea de compozitie indusă pe (G/H) , este asociativă deoarece legea de compozitie a lui $P(G)$ este asociativă. Avem $H = 1H \in (G/H)$, și H este element unitate pentru legea de compozitie indusă pe $P(G)$:

$$(1H)(xH) = (1x)H = xH \text{ pentru orice } xH \in (G/H).$$

În fine, orice element $xH \in (G/H)$, are un invers în (G/H) , în raport cu legea de compozitie indusă, anume $x^{-1}H \in (G/H)$:

$$(xH)(x^{-1}H) = (xx^{-1})H = 1H = H$$

$$(x^{-1}H)(xH) = (x^{-1}x)H = 1H = H.$$

Prin urmare (G/H) , este subgrup al monoidului $P(G)$. Reciproc, presupunem că (G/H) , este subgrup al monoidului $P(G)$. Pentru $xH \in (G/H)$, avem $(xH)H = xHH = xH$ ceea ce arată că $1H = H$ este elementul unitate al grupului (G/H) . În plus, există un element $yH \in (G/H)$, astfel ca $(xH)(yH) = (yH)(xH) = H$. Atunci $yH \subset HyH = x^{-1}(xH)(yH) = x^{-1}H$, deci $yH = x^{-1}H$. Deoarece $(x^{-1}H)(xH) = H$, avem $Hx \subset HxH = x(x^{-1}H)(xH) = xH$. Analog, deoarece $(xH)(x^{-1}H) = H$ avem $Hx^{-1} \subset Hx^{-1}H = x^{-1}(xH)(x^{-1}H) = x^{-1}H$, deci $xH = x(Hx^{-1})x \subset x(x^{-1}H)x = Hx$. Rezultă $Hx = xH$ pentru orice $x \in G$, deci $HG \trianglelefteq$ conform propoziției 3.1.b).

Definiția 3.10. Fie H un subgrup normal al grupului G . Subgrupul $(G/H) = (G/H)_a$ al monoidului $P(G)$ definit în propoziția precedentă se numește **grupul factor** al lui G prin H și se notează G/H . Reținem din demonstrația acestei propoziții că elementele lui G/H sunt clase de congruență xH , $x \in G$ și avem $xH = yH$ dacă și numai dacă $x^{-1}y \in H$ iar legea de compozitie în G/H este definită prin $(xH)(yH) = xyH$; elementul unitate în G/H este $1H = H$ iar inversul lui xH este $(xH)^{-1} = xH$.

Aplicația $\pi: G \rightarrow G/H$ definită prin $\pi(x) = xH$, $x \in G$, se numește **proiecția canonica** a lui G pe G/H . π este evident un morfism de grupuri surjectiv, deci $\text{Im } \pi = G/H$. În plus, pentru $x \in G$, $x \in \text{Ker } \pi \Leftrightarrow xH = H \Leftrightarrow x \in H$, deci $\text{Ker } \pi = H$. Astfel are loc o reciprocă a propoziției 3.6: Orice subgrup normal $H \trianglelefteq G$ este nucleul unui morfism de grupuri.

Exemplu. 1) După cum am văzut, subgrupul trivial 1 și subgrupul impropriu G sunt subgrupuri normale ale lui G . Avem $G/1 = \{\{x\} \mid x \in G\}$ și proiecția canonica $\pi: G \rightarrow G/1$, $\pi(x) = \{x\}$ este un izomorfism: $G/1 \cong G$; de asemenea G/G este grupul trivial: $G/G = 1$.

2) După cum am văzut în 3.6, avem $\text{Inn}(G) \trianglelefteq \text{Aut}(G)$. Grupul factor $\text{Aut}(G)/\text{Inn}(G)$ se numește **grupul automorfismelor exterioare**

ale lui G . Această denumire este însă abuzivă deoarece elementele grupului factor $\text{Aut}(G)/\text{Inn}(G)$ nu sunt automorfisme ale lui G .

3) Pentru orice $H \trianglelefteq G$ avem evident $|G/H| = |G:H|$. În particular, pentru orice număr întreg pozitiv n , subgrupul $n\mathbb{Z}$ al lui \mathbb{Z} (vezi 2.22) este normal în \mathbb{Z} (deoarece \mathbb{Z} este abelian) și, conform propoziției 2.23, grupul factor $\mathbb{Z}/n\mathbb{Z}$ are ordinul n . Grupul factor $\mathbb{Z}/n\mathbb{Z}$ se notează de obicei cu \mathbb{Z}_n și se numește grupul claselor de resturi modulo n . În general, orice grup factor al unui grup ciclic este ciclic: dacă $H \trianglelefteq G = \langle x \rangle$, atunci $G/H = \langle xH \rangle$. În particular, \mathbb{Z}_n este un grup ciclic, un generator al său fiind $\bar{1} = 1 + n\mathbb{Z}$.

Propoziția 3.11. (Teorema fundamentală de izomorfism.) *Dacă $f: G \rightarrow G'$ este un morfism de grupuri. Atunci $G/\text{Ker } f \cong \text{Im } f$. Mai precis, există un unic omomorfism de grupuri $\tilde{f}: G/\text{Ker } f \rightarrow \text{Im } f$, astfel că $f = \text{iof}\circ\pi$, unde $\pi: G \rightarrow G/\text{Ker } f$ este proiecția canonică și \tilde{f} este izomorfism.*

Demonstrație. Pentru simplificare, să notăm $N = \text{Ker } f$. Să presupunem că $I: G/N \rightarrow \text{Im } f$ și $f = \text{iof}\circ\pi$. Atunci, pentru orice $x \in G$, avem

$$f(x) = I(\tilde{f}(\pi(x))) = \tilde{f}(xN).$$

Aceasta demonstrează că dacă există un omomorfism $\tilde{f}: G/N \rightarrow \text{Im } f$ cu proprietatea $f = \text{iof}\circ\pi$, atunci acesta este unic. Acum fie $x, y \in G$. Avem

$$xN = yN \Leftrightarrow y^{-1}x \in N = \text{Ker } f \Leftrightarrow f(y^{-1}x) = 1 \Leftrightarrow f(y)^{-1}f(x) = 1 \Leftrightarrow f(x) = f(y).$$

Aceasta arată că putem defini aplicația $\tilde{f}: G/N \rightarrow \text{Im } f$ prin $\tilde{f}(xN) = f(x)$, $x \in G$. Această aplicație satisfacă evident egalitatea $f = \text{iof}\circ\pi$. Aplicația \tilde{f} este injectivă:

$$\tilde{f}(xN) = \tilde{f}(yN) \Leftrightarrow f(x) = f(y) \Leftrightarrow xN = yN$$

(conform sirului de echivalențe de mai sus) și este surjectivă deoarece orice element din $\text{Im } f$ este de forma $f(x)$, $x \in G$, deci de forma $f(x) = \tilde{f}(xN)$. În fine, \tilde{f} este morfism de grupuri deoarece

$$\tilde{f}((xN)(yN)) = \tilde{f}((xy)N) = f(xy) = f(x)f(y) = \tilde{f}(xN)\tilde{f}(yN).$$

Aceasta arată că \tilde{f} este izomorfism și teorema este demonstrată.

Exemplu: 1) Considerăm grupul aditiv \mathbf{R} al numerelor reale (adică mulțimea numerelor reale \mathbf{R} considerată ca grup în raport cu adunarea numerelor reale) și grupul multiplicativ \mathbf{C}^* al numerelor complexe ne-nule. Din regula de înmulțire a numerelor complexe, scrisă sub formă trigonometrică, rezultă că aplicația $f: \mathbf{R} \rightarrow \mathbf{C}^*$ definită prin: $f(x) = -\cos 2\pi x + i \sin 2\pi x$, $x \in \mathbf{R}$, este un morfism de grupuri. $\text{Im } f$ se notează de obicei cu D ; D este, deci, subgrupul lui \mathbf{C}^* , format din toate numerele

complexe de modul 1. Se constată imediat că $\text{Ker } f = \mathbb{Z}$. Aplicind teorema fundamentală de izomorfism, rezultă $\mathbb{R}/\mathbb{Z} \cong D$.

Putem considera și grupul aditiv \mathbb{Q} al numerelor raționale și restricția $g: \mathbb{Q} \rightarrow \mathbb{C}^*$ a lui f la \mathbb{Q} : $g\left(\frac{m}{n}\right) = \cos \frac{2\pi m}{n} + i \sin \frac{2\pi m}{n}$ pentru orice număr rațional $\frac{m}{n}$. Se constată imediat că

$$\text{Im } g = \{z \in \mathbb{C}^* \mid \text{există } n \in \mathbb{N}^*: z^n = 1\} = \bigcup_{n>0} \mathbb{C}_n,$$

adică $\text{Im } g$ este mulțimea tuturor rădăcinilor complexe ale unității. Notăm $\text{Im } g = \tilde{\mathbb{C}}_\infty$. Evident, $\text{Ker } g = \mathbb{Z}$ și, în virtutea teoremei fundamentale de izomorfism, rezultă $\mathbb{Q}/\mathbb{Z} \cong \tilde{\mathbb{C}}_\infty$.

2) Fie n un număr întreg pozitiv și considerăm aplicația $f: \mathbb{Z} \rightarrow \mathbb{C}^*$ definită prin $f(x) = \cos \frac{2\pi x}{n} + i \sin \frac{2\pi x}{n}$. Evident f este un morfism de grupuri și $\text{Ker } f = n\mathbb{Z}$, $\text{Im } f = \mathbb{C}_n$. Aplicind teorema fundamentală de izomorfism rezultă $\mathbb{Z}_n \cong \mathbb{C}_n$.

3) Fie G un grup. Considerăm morfismul de grupuri $\tau: G \rightarrow \text{Aut}(G)$ definit în 3.6. Avem $\text{Im } \tau = \text{Inn}(G)$, grupul automorfismelor interioare ale lui G . $\text{Ker } \tau$ se notează de obicei cu $Z(G)$ și se numește centrul grupului G . Din definiția lui τ rezultă imediat că

$$Z(G) = \{g \in G \mid gx = xg, \text{ pentru orice } x \in G\}.$$

Elementele lui $Z(G)$ se numesc elemente centrale ale lui G iar subgrupurile lui $Z(G)$ se numesc subgrupuri centrale ale lui G . Aplicind teorema fundamentală de izomorfism, obținem $G/Z(G) \cong \text{Inn}(G)$. Remarcăm că grupul G este abelian dacă și numai dacă $Z(G) = G$.

Propoziția 3.12. Fie N un subgrup central al unui grup G . Au loc următoarele afirmații:

i) $N \trianglelefteq G$.

ii) Dacă G/N este ciclic, atunci G este abelian.

Demonstrație. Dacă $g \in N$ și $x \in G$ avem $gx = xg$, deci $xgx^{-1} = g \in N$. Aceasta arată că $N \trianglelefteq G$.

ii) Presupunem $G/N = \langle xN \rangle$, $x \in G$. Atunci, pentru orice element $g \in G$, avem $gN = (xN)^n = x^nN$, deci $g = x^n u$ cu $n \in \mathbb{Z}$, $u \in N$.

Considerind două elemente $g, g' \in G$, vom avea: $y = x^n u$, $g' = x^{n'} u'$ cu $n, n' \in \mathbb{Z}$, $u, u' \in N$, deci $gg' = x^n ux^{n'} u' = x^n x^{n'} uu' = x^{n+n'} uu'$ și $g'g = x^{n'} u' x^n u = x^{n'} x^n u' u = x^{n+n'} uu'$; prin urmare $gg' = g'g$ și G este abelian.

Definiția 3.13. Fie G un grup, $x \in G$ și $\varphi_x: \mathbb{Z} \rightarrow G$ aplicația definită prin $\varphi_x(m) = x^m$, $m \in \mathbb{Z}$. Conform lui (1.8.1), φ_x este morfism de grupuri. Avem $\text{Ker } \varphi_x = \{m \in \mathbb{Z} \mid x^m = 1\}$ și, conform propoziției 2.22 (i), există

un unic număr natural n astfel încit $\text{Ker } \varphi_x = n\mathbb{Z}$; acest unic număr natural se numește ordinul elementului x și se notează $n = o(x)$.

Deoarece pentru $m \in \mathbb{Z}$ avem $m \in n\mathbb{Z}$ dacă și numai dacă $n|m$, numărul natural $n = o(x)$ este caracterizat de următoarea proprietate:

pentru $m \in \mathbb{Z}$, $x^m = 1 \Leftrightarrow n|m$.

Propoziția 3.14. Fie G un grup, $x \in G$ și $o(x) = n$. Atunci

$$|\langle x \rangle| = \begin{cases} n & \text{dacă } n > 0, \\ \infty & \text{dacă } n = 0. \end{cases}$$

Demonstrație. Avem evident $\text{Im } \varphi_x = \langle x \rangle$. Pe de altă parte, conform teoremei fundamentale de izomorfism, avem $\mathbb{Z}/\text{Ker } \varphi_x \simeq \text{Im } \varphi_x$, adică $\mathbb{Z}/n\mathbb{Z} \simeq \langle x \rangle$. Rezultă $|\langle x \rangle| = |\mathbb{Z}/n\mathbb{Z}| =$

$$= \begin{cases} n & \text{dacă } n > 0 \\ \infty & \text{conform propoziției 2.23.} \end{cases}$$

$\text{dacă } n = 0.$

Propoziția 3.15. Pentru orice grup ciclic G avem $G \simeq \mathbb{Z}_n$ dacă G este finit și $n = |G|$ și $G \simeq \mathbb{Z}$ dacă G este infinit.

Demonstrație. Există un element $x \in G$ cu $G = \langle x \rangle$, și, ca și în demonstrația propoziției precedente, avem $G \simeq \mathbb{Z}/n\mathbb{Z}$, unde $n = o(x)$. Dacă $n > 0$, avem $|G| = n$ și $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$ și, dacă $n = 0$, G este infinit și $\mathbb{Z}/0\mathbb{Z} \simeq \mathbb{Z}$.

Propoziția 3.15.' Fie G un grup finit de ordin m . Atunci, pentru orice element $x \in G$, avem $x^m = 1$.

Demonstrație. Fie $H = \langle x \rangle \leqslant G$ și $n = o(x)$. Deoarece H este finit, avem $n > 0$ și $n = |H| = |G| = m$, conform teoremei lui Lagrange. Rezultă $x^m = 1$, din definiția lui $o(x)$.

Definiția 3.16. Fie n un număr întreg pozitiv. Multimea $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \dots, \overline{n-1}\}$ a claselor de resturi modulo n este grup în raport cu adunarea claselor de resturi: $\bar{x} + \bar{y} = \overline{x+y}$. (acesta este grupul factor $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$). Pe multimea \mathbb{Z}_n definim și o înmulțire (adică o lege de compozitie binară notată multiplicativ), astfel: $\bar{x}\bar{y} = \overline{xy}$. Această înmulțire este bine definită deoarece $\bar{x} = \bar{x}'$ și $\bar{y} = \bar{y}'$ implică $x - x' \in n\mathbb{Z}$ și $y - y' \in n\mathbb{Z}$ deci $x - x' = np$ și $y - y' = nq$ cu $p, q \in \mathbb{Z}$; rezultă $xy = (x'+np)(y'+nq) = xn' + n(py' + qx' + npq)$, deci $\overline{xy} = \overline{(x'+np)(y'+nq)} = \overline{xn'} + \overline{n(py' + qx' + npq)} = \overline{xn'} + \overline{n}(\overline{py'} + \overline{qx'}) = \overline{xn'} + \overline{n}(\bar{x}\bar{y}) = \bar{x}\bar{y}$. Împreună cu înmulțirea astfel definită este un monoid: legea de asociativitate se verifică imediat, iar elementul unitate este 1; grupul elementelor inversabile ale acestui monoid se notează cu $U(\mathbb{Z}_n)$ (în capitolul următor \mathbb{Z}_n va fi inelul claselor de resturi modulo n , grupul aditiv \mathbb{Z}_n se va nota cu \mathbb{Z}_n^+ iar monoidul multiplicativ \mathbb{Z}_n cu \mathbb{Z}_n^*).

Propoziția 3.17. Fie n un număr întreg pozitiv și $x \in \mathbb{Z}$. Următoarele afirmații sunt echivalente:

a) În grupul aditiv \mathbb{Z}_n , $\langle \bar{x} \rangle = \mathbb{Z}_n$;

b) $\bar{x} \in U(\mathbb{Z}_n)$;

c) $(x, n) = 1$.

Demonstrație. a) \Rightarrow b). Avem $\bar{1} \in \mathbb{Z}_n = \langle \bar{x} \rangle$ deci $\bar{1} = k\bar{x}$, cu $k \in \mathbb{Z}$. Se verifică imediat că în \mathbb{Z}_n avem $k\bar{x} = \bar{kx}$ pentru orice $k, x \in \mathbb{Z}$. Vom avea deci $\bar{1} = \bar{kx} = \bar{k}\bar{x}$, deci $\bar{x} \in U(\mathbb{Z}_n)$.

b) \Rightarrow c). Dacă $\bar{x} \in U(\mathbb{Z}_n)$ avem $\bar{1} = \bar{k}\bar{x} = \bar{kx}$ pentru un $k \in \mathbb{Z}$, deci $1 - kx \in n\mathbb{Z}$, $1 - kx = nm$ cu $m \in \mathbb{Z}$. Evident rezultă $(x, n) = 1$.

c) \Rightarrow a). Conform lui 2.22, dacă $(x, n) = 1$, atunci există $k, m \in \mathbb{Z}$, cu $1 = kx + nm$. Atunci $\bar{1} = \bar{kx} = \bar{k}\bar{x} \in \langle \bar{x} \rangle$, deci $\mathbb{Z}_n = \langle \bar{1} \rangle = \langle \bar{x} \rangle$.

Definiția 3.18. Conform propoziției precedente, ordinul grupului $U(\mathbb{Z}_n)$ este numărul numerelor întregi pozitive mai mici ca n și prime cu n . Ordinul $|U(\mathbb{Z}_n)|$ se numește *indicatorul Euler* al lui n și se notează cu $\phi(n)$. Avem $\phi(1) = 1$ și, evident, pentru orice număr prim p , $\phi(p) = p - 1$. Conform propoziției 3.15, avem, pentru orice $\bar{x} \in U(\mathbb{Z}_n)$, $\bar{x}^{\phi(n)} = 1$, adică, pentru orice număr întreg x , prim cu n , $x^{\phi(n)} \equiv 1 \pmod{n}$. Acest rezultat se numește, în teoria numerelor, teorema lui Euler. Dacă p este număr prim și $x \in \mathbb{Z}$ este prim cu p (ceea ce revine la faptul că $(p \nmid x)$, rezultă, în particular, $x^{p-1} \equiv 1 \pmod{p}$, rezultat ce se numește teorema lui Fermat.

Propoziția 3.19. (Prima teoremă de izomorfism pentru grupuri). Fie $f: G \rightarrow G'$ un morfism de grupuri surjectiv și $H \trianglelefteq G$. Atunci $f(H) \trianglelefteq G'$ și $G/H \cong G'/f(H)$.

Demonstrație. Avem $f(H) \trianglelefteq G'$ conform lui 3.5. Fie $\pi: G' \rightarrow G'/f(H)$ proiecția canonică și $f' = \pi \circ f: G \rightarrow G'/f(H)$. Fiind compunerea a două morfisme, ambele surjective, f' este un morfism surjectiv, deci $\text{Im } f' = G'/f(H)$. Pentru $x \in G$ avem:

$$x \in \text{Ker } f' \Leftrightarrow f'(x) = 1 \Leftrightarrow \pi(f(x)) = 1 \Leftrightarrow$$

$$f(x) \in \text{Ker } \pi = f(H).$$

Rezultă $f(\text{Ker } f') = f(H)$ și conform punctului iii) al lui 3.5, rezultă $\text{Ker } f' = H$. Obținem $G/H \cong G'/f(H)$ în virtutea teoremei fundamentale de izomorfism.

Observație. Fie G un grup și $H \trianglelefteq G$, $H \leq K \leq G$. Considerăm proiecția canonică $\pi: G \rightarrow G/H$ și incluziunea canonică $i: K \rightarrow G$ și fie $f = \pi \circ i: K \rightarrow G/H$. Aveni evident $\text{Ker } f = H$ și $\text{Im } f = f(K)$ astfel că, există un izomorfism canonic $\tilde{f}: K/H \rightarrow \pi(K)$ definit prin $\tilde{f}(xH) = f(x) = \pi(x)$, $x \in K$; xH este clasa de congruență la stînga modulo H a elementului $x \in K$, iar $\pi(x)$ este clasa de congruență la stînga modulo H a aceluiși element x dar, privim, $x \in G$; izomorfismul de mai sus ne permite să identificăm aceste două clase, deci, să identificăm K/H cu $\pi(K)$.

Deoarece π este un morfism de grupuri surjectiv, teorema de corespondență 2.8 arată că aplicația $K \sim K/H$ de la mulțimea subgrupurilor lui G care conțin $\text{Ker } \pi = H$ în mulțimea subgrupurilor lui G/H este bijectivă.

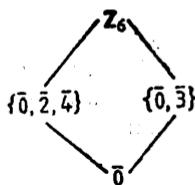
Conform lui 3.5 pentru un subgrup K cu $H \leq K \leq G$ avem $K \trianglelefteq G$ dacă și numai dacă $K/H \trianglelefteq G/H$ și, conform teoremei de izomorfism de mai sus, $(G/H)/(K/H) \cong G/K$.

Subgrupurile lui Z_n . Fie n un număr întreg pozitiv. Z_n fiind abelian orice subgrup în Z_n este normal în Z_n . Deoarece $Z_n = Z/nZ$ avem, conform teoremei de corespondență, că orice subgrup al lui Z_n este de forma H/nZ , unde H este un subgrup al lui Z care conține pe nZ . Conform lui 2.22 avem $H = dZ$ unde d este un număr natural cu $d \mid n$. Deci, orice subgrup al lui Z_n este de forma dZ/nZ , unde d este un divizor natural al lui n . Conform primei teoreme de izomorfism avem:

$$Z_n/(dZ/nZ) = (Z/nZ)/(dZ/nZ) \cong Z/dZ$$

și deci $d = |Z/dZ| = Z_n / |dZ/nZ| = n / |dZ/nZ|$, deci $|dZ/nZ| = n / d$.

Spre exemplificare să considerăm subgrupurile lui $Z_6 = \{0, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$. Divizori naturali ai lui 6 fiind 1, 2, 3, 6, aceste subgrupuri sunt $1Z/6Z = Z_6$, $2Z/6Z = \{\bar{0}, \bar{2}, \bar{4}\}$, $3Z/6Z = \{\bar{0}, \bar{3}\}$, $6Z/6Z = \bar{0}$. Astfel lățicea subgrupurilor lui Z_6 este:



Subgrupurile unui grup ciclic. Structura grupurilor ciclice este dată de propoziția 3.15. Dacă G este un grup ciclic infinit avem $G \cong Z$. În virtutea propoziției 2.22 rezultă că orice subgrup al lui G netrivial este un grup ciclic infinit și orice grup factor al lui G este ciclic (finit, dacă factorizarea se face printr-un subgrup netrivial). Mai precis, dacă fixăm un generator x al lui $G: G = \langle x \rangle$, avem un izomorfism canonico $\varphi_x: Z \rightarrow G$ cu $\varphi_x(n) = x^n$, $n \in Z$ și rezultă că orice subgrup al lui G este de forma $\langle x^d \rangle$, unde d este un număr natural.

Presupunem acum că G este un grup ciclic finit de ordin n . Avem $G \cong Z_n$ și cunoșcind subgrupurile lui Z_n , deducem că orice subgrup al lui G este ciclic (subgrupul dZ/nZ al lui Z_n este evident ciclic generat de d). Mai mult, pentru fiecare divizor natural d al lui n , există un unic subgrup G_d al lui G de ordin d (în cazul $G = Z_n$, avem $G_d = d'Z/nZ$, unde

$d' = n|d$). Putem descrie acest subgrup G_d astfel: $G_d = \{x \in G \mid x^d = 1\}$. Într-adevăr, deoarece G_d are ordinul d , avem, conform lui 3.15, $G_d \subset \{x \in G \mid x^d = 1\}$. Deoarece G este grup abelian, este clar că $\{x \in G \mid x^d = 1\}$ este un subgrup al lui G , deci $\{x \in G \mid x^d = 1\} = G_d'$, unde d' este un divizor natural al lui n . Incluziunea $G_d \subset G_d'$ implică $d|d'$ și, pe de altă parte, considerind un generator x' al lui G_d avem $o(x') = d'$ și $x'^d = 1$, deci $d'|d$. Astfel $d = d'$ și $G_d = G_d' = \{x \in G \mid x^d = 1\}$.

Propoziția 3.20. 1) Pentru orice număr întreg pozitiv n avem $n = \sum_{d|n} \phi(d)$.

ii) Fie G un grup finit de ordin n cu proprietatea că, pentru orice divizor natural d al lui n , există cel mult un subgrup G al lui G de ordin d . Atunci G este ciclic.

Demonstrație. Fie G un grup finit de ordin n și, pentru fiecare divizor natural d al lui n , fie $M_d = \{x \in G \mid o(x) = d\}$. Evident mulțimile M_d sunt disjuncte două cîte două și reuniunea lor este G astfel că avem $|G| = \sum_{d|n} |M_d|$. Presupunem acum că grupul satisface proprietatea din enunț și fie d un divizor natural al lui n . Dacă mulțimea M_d este nevidă și $x \in M_d$, $\langle x \rangle$ este unicul subgrup de ordin d al lui G , astfel că $M_d = \{y \in G \mid \langle y \rangle = \langle x \rangle\}$ și, conform propoziției 3.18, $|M_d| = \phi(d)$. Prin urmare

$$1) \quad n = \sum_{d|n} |M_d| \text{ cu } |M_d| \leq \phi(d) \text{ pentru orice } d.$$

Un grup ciclic de ordin n , de exemplu \mathbf{Z}_n , satisface proprietatea din enunț și, în plus, pentru orice divizor natural d al lui n există un subgrup de ordin n al lui G și acesta este ciclic, deci mulțimea M_d este nevidă și $M_d = \phi(d)$. Prin urmare

$$(2) \quad n = \sum_{d|n} \phi(d).$$

Din (1) și (2) rezultă $|M_d| = \phi(d)$ pentru orice d și, în particular, mulțimea M_n este nevidă. Considerind un element $x \in M_n$ avem $\langle x \rangle \leq G$ și $|\langle x \rangle| = |G| = n$, deci $\langle x \rangle = G$ și G este un grup ciclic.

Propoziția 3.21. (A doua teoremă de izomorfism pentru grupuri.) Fie G un grup și H, K subgrupuri ale lui G . Presupunem că $H \leq H \vee K$. Atunci

- i) $H \vee K = HK$ și $H \cap K \trianglelefteq K$.
- ii) $HK/H \cong K/H \cap K$.

Demonstrație. Deoarece $K \leq H \vee K$, avem, pentru orice $k \in K$, $hk = kh$, deci $HK = \bigcup_{k \in K} hk = \bigcup_{k \in K} kh = KH$.

Conform propoziției 2.14 avem $HK \leq G$. Considerind incluziunea canonică $i: K \rightarrow HK$ și proiecția canonică $\pi: HK \rightarrow HK/H$ obținem un morfism de grupuri $f = \pi \circ i: K \rightarrow HK/H$. Pentru orice $x \in$

$\in HK$ avem $x=hk$, $h \in H$, $k \in K$ și, deoarece $H=\text{Ker } \pi$, avem $\pi(x)=\pi(hk)=\pi(h)\pi(k)=\pi(k)=\pi(i(k))=f(k)$. Deoarece π este surjectiv, rezultă f surjectiv. Pe de altă parte, este evident că $\text{Ker } f=K \cap \text{Ker } \pi=H \cap K$ și prin urmare $H \cap K \trianglelefteq K$; în virtutea teoremei fundamentale de izomorfism $\text{Im } f \cong K/\text{Ker } f$, adică $HK/H \cong K/H \cap K$.

Aplicație. Fie m și n două numere întregi pozitive. Conform propoziției 2.22 avem $m\mathbf{Z}+n\mathbf{Z}=(m, n)\mathbf{Z}$ și $m\mathbf{Z} \cap n\mathbf{Z}=[m, n]\mathbf{Z}$. Aplicind a doua teoremă de izomorfism, obținem $(m, n)\mathbf{Z}/n\mathbf{Z} \cong m\mathbf{Z}/[m, n]\mathbf{Z}$. Pe de altă parte avem $|(m, n)\mathbf{Z}/n\mathbf{Z}|=n/(m, n)$ și $|m\mathbf{Z}/[m, n]\mathbf{Z}|=[m, n]/m$; rezultă deci $n/(m, n)=m/[m, n]$, adică $mn=(m, n)[m, n]$, relație bine cunoscută în aritmetică elementară.

Propoziția 3.22. Dacă H și K sunt două subgrupuri normale ale unui grup G , atunci HK este de asemenea un subgrup normal al lui G .

Demonstrație. Deoarece $H \trianglelefteq G$, avem $H \trianglelefteq H \vee K$, deci conform lui 3.21 (i), $HK \trianglelefteq G$. Faptul că $HK \trianglelefteq G$ rezultă ușor: pentru orice $x \in G$, $xHK=xKx=HKx$.

Definiția 3.23. Un grup G se numește grup *simplu* dacă $G \neq 1$ și 1 și G sunt singurele subgrupuri normale ale lui G .

Stadiul grupurilor simple este fundamental în teoria grupurilor finite, existând posibilitatea ca orice grup finit să se obțină după anumite procedee (care nu sunt încă clare) din grupuri finite simple.

Un subgrup normal H al unui grup G se numește *subgrup normal maximal* al lui G dacă $H \neq G$ și $H \trianglelefteq G$ implică $H=K$ sau $K=G$; analog, H se numește *subgrup normal minimal* al lui G dacă $H \neq 1$ și $N \trianglelefteq H$ cu $N \trianglelefteq G$ implică $N=1$ sau $N=G$. Altfel spus, subgrupurile normale maximale ale lui G sunt elementele maximale în mulțimea subgrupurilor proprii ale lui G ordonată prin inclusiune, iar subgrupurile normale minimele sunt elementele minimele în mulțimea subgrupurilor normale netriviale ale lui G , ordonată prin inclusiune.

Exemple. Fie H un subgrup normal al unui grup G . Considerind proiecția canonică $\pi: G \rightarrow G/H$ și aplicind teorema de corespondență pentru subgrupuri normale, (propoziția 3.5), vedem că H este subgrup normal maximal al lui G dacă și numai dacă G/H este grup simplu.

Fie p un număr întreg pozitiv. Deoarece, în grupul aditiv \mathbf{Z} al numerelor întregi, avem $p\mathbf{Z} \trianglelefteq n\mathbf{Z} \Leftrightarrow p|n$, vedem că $p\mathbf{Z}$ este un subgrup normal maximal al lui \mathbf{Z} dacă și numai dacă p este număr prim. În particular, pentru p număr prim, grupul $\mathbf{Z}_p=\mathbf{Z}/p\mathbf{Z}$ este grup simplu. Reciproc, fie G un grup simplu abelian. Deoarece, pentru $1 \neq x \in G$, avem $1 \neq \langle x \rangle \trianglelefteq G$, rezultă $\langle x \rangle = G$ și G este grup ciclic. Prin urmare, $G \cong \mathbf{Z}$ sau $G \cong \mathbf{Z}_n$, unde n este un număr întreg pozitiv; deoarece \mathbf{Z} nu este grup simplu, avem $G \cong \mathbf{Z}_n$, unde n este un număr întreg pozitiv; conform celor de mai sus, $n=p$, un număr prim. Prin urmare, structura grupurilor simple abeliene este clară: un grup abelian G este simplu dacă și numai dacă $G \cong \mathbf{Z}_p$, unde p este un număr prim.

Rezultă imediat că grupul \mathbf{Z} nu are subgrupuri (normale) minime. Într-adevăr, orice subgrup netrivial al lui \mathbf{Z} este de forma $n\mathbf{Z}$, unde n este un număr întreg, $n > 1$; atunci $2n\mathbf{Z} < n\mathbf{Z}$ deci $n\mathbf{Z}$ nu este un subgrup normal minimal.

Definiția 3.24. Fie G un grup. O mulțime $\mathbf{H} = \{H_0, H_1, \dots, H_n\}$ de subgrupuri ale lui G se numește serie a lui G dacă $1 = H_0 \leq H_{n-1} \leq \dots \leq H_1 \leq H_0 = G$ și pentru fiecare $i \in \{1, 2, \dots, n\}$, $H_i \trianglelefteq H_{i-1}$. n se numește lungimea seriei \mathbf{H} . H_0, H_1, \dots, H_n se numesc termenii săi, iar grupurile factor $H_0/H_1, H_1/H_2, \dots, H_{n-1}/H_n$ se numesc factorii seriei \mathbf{H} . Seria \mathbf{H} se numește serie de compoziție a lui G dacă toți factorii săi sunt grupuri simple.

Două serii $\mathbf{H} = \{H_0, H_1, \dots, H_m\}$ și $\mathbf{K} = \{K_0, K_1, \dots, K_n\}$ ale unui grup G se numesc echivalente dacă $m = n$ și există o aplicație bijectivă f de la mulțimea factorilor lui \mathbf{H} pe mulțimea factorilor lui \mathbf{K} , astfel ca pentru orice factor H_{i-1}/H_i al lui \mathbf{H} , $i \in \{1, 2, \dots, n\}$, să avem $H_{i-1}/H_i \simeq f(H_{i-1}/H_i)$.

Legătura între două serii de compoziție ale unui grup G este dată de célébra teoremă a lui Jordan-Hölder, teoremă care se poate formula și demonstra în situații mult mai generale decât cea pe care o vom considera mai jos.

Exemplu. Grupul \mathbf{Z} nu are nici o serie de compoziție; într-adevăr, dacă $\{H_0, H_1, \dots, H_n\}$ ar fi o serie de compoziție a lui \mathbf{Z} , neapărat $n > 0$ și $H_{n-1}/H_n = H_{n-1}/1 = H_{n-1}$ este grup simplu; dar orice subgrup netrivial al lui \mathbf{Z} este izomorf cu \mathbf{Z} și nu este grup simplu.

Pe de altă parte, se vede ușor că orice grup finit are cel puțin o serie de compoziție. Într-adevăr, fie G un grup finit. Putem presupune că G este netrivial (grupul trivial are o serie de compoziție de lungime 0).

Construim subgrupurile $H_0, H_1, \dots, H_n, \dots$ ale lui G inductiv, astfel: $H_0 = G$; presupunem că H_n a fost construit; dacă $H_n \neq 1$, definim H_{n+1} ca un subgrup normal maximal al lui H_n (un astfel de subgrup există deoarece H_n este finit); dacă $H_n = 1$, luăm $H_{n+1} = 1$. Deoarece $H_n \neq 1$ implică $H_{n+1} < H_n$, există un număr natural n cu $H_n = 1$ și dacă n este cel mai mic număr natural cu această proprietate, atunci $\{H_0, H_1, \dots, H_n\}$ este o serie de compoziție a lui G .

Lema 3.25. Fie G un grup, $\mathbf{H} = \{H_0, H_1, \dots, H_n\}$ o serie de compoziție a lui G de lungime n și K_1 un subgrup normal maximal al lui G . Atunci, există o serie de compoziție a lui G de forma $\{K_0, K_1, K_2, \dots, K_m\}$ și orice astfel de serie de compoziție este echivalentă cu \mathbf{H} .

Demonstrație. Facem inducție după n . Pentru $n = 1$, G este un grup simplu și afirmația din enunț este evidentă.

Presupunem că afirmația este adevărată pentru grupuri care au o serie de compoziție de lungime i , unde $i < n$. Dacă $K_1 = H_1$, atunci

$\{H_1, H_2, \dots, H_n\}$ este o serie de compoziție a lui H_1 , de lungime $n-1$ și afirmația lemei rezultă imediat aplicând ipoteza de inducție. Pre-supunem acum $K_1 \neq H_1$. Atunci $H_1 < H_1 K_1 \trianglelefteq G$, deci $H_1 K_1 = G$ deoarece H_1 este subgrup normal maximal. Fie $L_2 = H_1 \cap K_1$. Avem

$$H_1/L_2 = H_1/H_1 \cap K_1 \simeq H_1 K_1 / K_1 = G/K_1.$$

$$K_1/L_2 = K_1/H_1 \cap K_1 \simeq H_1 K_1 / H_1 = G/H_1.$$

G/K_1 și G/H_1 fiind grupuri simple, rezultă H_1/L_2 și K_1/L_2 grupuri simple. În particular L_2 este subgrup normal maximal al lui H_1 . În virtutea ipotezei de inducție există o serie de compoziție a lui H_1 de forma $\{H_1, L_2, \dots, L_t\}$ și orice asemenea serie de compoziție este echivalentă cu $\{H_1, H_2, \dots, H_n\}$. În particular avem $n=t$. Rezultă că $\{H_0, H_1, L_2, \dots, L_n\}$ este o serie de compoziții a lui G echivalentă cu \mathbf{H} . În mod evident $\{K_1, L_2, \dots, L_n\}$ este o serie de compoziție a lui K_1 , deci $\{K_0, K_1, L_2, \dots, L_n\}$ este o serie de compoziție a lui G . Izomorfismele $H_1/L_2 \cong \cong G/K_1$ și $K_1/L_2 \cong G/H_1$ arată că seriile $\{H_0, H_1, L_2, \dots, L_n\}$ și $\{K_0, K_1, L_2, \dots, L_n\}$ ale lui G sunt echivalente. Dacă $\{K_0, K_1, \dots, K_m\}$ este o serie de compoziție a lui G , ipoteza de inducție aplicată lui K_1 (care are seria de compoziție $\{K_1, L_2, \dots, L_n\}$ de lungime $n-1 < n$) arată că seriile $\{K_1, \dots, K_m\}$ și $\{K_1, L_2, \dots, L_n\}$ ale lui K_1 sunt echivalente. În particular $m=n$ și seriile $\{K_0, K_1, \dots, K_m\}$ și $\{G, K_1, L_2, \dots, L_n\}$ ale lui G sunt echivalente; seria $\{G, K_1, L_2, \dots, L_n\}$ este echivalentă cu $\{G, H_1, L_2, \dots, L_n\}$ la rîndul ei echivalentă cu \mathbf{H} . Deoarece echivalența seriilor este evident o relație de echivalență, rezultă seria $\{K_0, K_1, \dots, K_m\}$ echivalentă cu \mathbf{H} .

Propoziția 3.26. (Teorema Jordan-Hölder). *Orice două serii de compoziție $H = \{H_0, H_1, \dots, H_n\}$ și $K = \{K_0, K_1, \dots, K_m\}$ ale unui grup G sunt echivalente.*

Demonstrație. Se aplică lema 3.25 seriei H și subgrupului normal maximal K_1 .

Aplicație. Ca aplicație la teorema Jordan-Hölder vom demonstra teorema fundamentală a aritmeticii: orice număr natural $n > 1$ are o descompunere în factori primi unică, abstracție făcind de ordinea factorilor.

Fie n un număr natural $n > 1$ și considerăm grupul $\mathbf{Z}_n = \mathbf{Z}/n\mathbf{Z}$. Orice subgrup al lui \mathbf{Z}_n este de forma $d\mathbf{Z}/n\mathbf{Z}$, unde d este un divizor natural al lui n ; în plus, pentru alt divizor natural d' al lui n , avem:

$$d'\mathbf{Z}/n\mathbf{Z} \leq d\mathbf{Z}/n\mathbf{Z} \Leftrightarrow d' \leq d \Leftrightarrow d | d'.$$

Fie k și d divizori naturali ai lui n astfel ca $d | k$, deci $k\mathbf{Z}/n\mathbf{Z} \leq d\mathbf{Z}/n\mathbf{Z}$; conform celor de mai sus, $k\mathbf{Z}/n\mathbf{Z}$ este un subgrup maximal al lui $d\mathbf{Z}/n\mathbf{Z}$ dacă și numai dacă k/d este un număr prim. Acum fie $\{H_0, H_1, \dots, H_m\}$ o serie de compoziție a lui \mathbf{Z}_n ; avem $H_i = d_i\mathbf{Z}/n\mathbf{Z}$ cu d_i divizor natural

al lui n , $1=d_0 \mid d_1 \mid \dots \mid d_{n-1} \mid d_n=n$ și, pentru fiecare $i \in \{1, 2, \dots, n\}$, $d_i/d_{i-1}=p_i$ este un număr prim; în plus

$$n = \frac{d_n}{d_{n-1}} \cdots \frac{d_2}{d_1} \frac{d_1}{d_0} = p_1 p_2 \cdots p_n.$$

Considerăm acum o altă descompunere în factori primi ai lui n : $n=q_1 q_2 \cdots q_r$, q_j numere prime pentru orice $j \in \{1, 2, \dots, r\}$. Pentru fiecare $j \in \{0, 1, \dots, r-1\}$, luăm $d'_j = q_{j+1} \cdots q_r$ și $d'_r = 1$. Atunci, pentru fiecare $j \in \{0, 1, \dots, r\}$, $K_j = d'_j \mathbf{Z}/n\mathbf{Z} \leq \mathbf{Z}_n$ și $\{K_0, K_1, \dots, K_r\}$ este o serie de compoziție a lui \mathbf{Z}_n . Conform teoremei Jordan-Hölder, seriile $\{H_0, H_1, \dots, H_m\}$ și $\{K_0, K_1, \dots, K_r\}$ sunt echivalente. Rezultă $m=r$ și, fiecare factor H_{i-1}/H_i , $i \in \{1, \dots, m\}$, este izomorf cu un factor K_{j-1}/K_j , $j \in \{1, \dots, m\}$; deoarece $|H_{i-1}/H_i| = |d_{i-1}\mathbf{Z}/d_i\mathbf{Z}| = d_i/d_{i-1} = p_i$ și, analog, $|K_{j-1}/K_j| = q_j$, rezultă că fiecare p_i , $i \in \{1, \dots, m\}$ este egal cu un q_j , $j \in \{1, \dots, m\}$.

Definiția 3.27. Fie G un grup și $\mathbf{H} = \{H_0, H_1, \dots, H_n\}$ o serie de compoziție a lui G . Din teorema Jordan-Hölder rezultă că numărul natural n nu depinde de seria de compoziție \mathbf{H} , ci numai de grupul G , motiv pentru care n se numește lungimea de compoziție a lui G . De asemenea factorii seriei \mathbf{H} , H_{i-1}/H_i , $i \in \{1, 2, \dots, n\}$ sunt unic determinați pînă la un izomorfism de grupul G . Ei se numesc factorii de compoziție ai grupului G .

Evident nu putem vorbi despre lungimea de compoziție a lui G sau despre factorii de compoziție ai lui G decit dacă grupul G are cel puțin o serie de compoziție. În particular, putem vorbi despre lungimea de compoziție sau despre factorii de compoziție ai unui grup finit.

§ 4. GRUPURI LIBERE

Definiția 4.1. Fie A o mulțime și $FM(A) = \bigcup_{n \in \mathbb{N}} A^n$. Elementele lui $FM(A)$ se numesc cuvinte în alfabetul A , ele fiind n -tuple (x_1, x_2, \dots, x_n) de elemente din A , $n \in \mathbb{N}$; pentru $n=0$, A^0 este o mulțime cu un singur element și, acest unic cuvînt cu „zero litere” desî se numește de obicei „cuvîntul vid”, noi îl vom nota cu 1. Pe mulțimea $FM(A)$ se definește o lege de compoziție binară prin juxtapunere, adică

$$(x_1, x_2, \dots, x_m)(y_1, y_2, \dots, y_n) = (x_1, x_2, \dots, x_m, y_1, y_2, \dots, y_n).$$

Evident juxtapunerea cuvîntelor este o lege de compoziție asociativă și are ca element neutru cuvîntul vid 1. Prin urmare, $FM(A)$ este un monoid; $FM(A)$ se numește monoidul liber generat de mulțimea A .

Pentru orice cuvînt (x_1, x_2, \dots, x_n) în alfabetul A avem: $(x_1, x_2, \dots, x_n) = (x_1)(x_2) \cdots (x_n)$ și, renunțînd la paranteze pentru cuvîntele cu o singură literă (în fond $A^1 = A$), putem scrie $(x_1, x_2, \dots, x_n) = x_1 x_2 \cdots x_n$.

Vom nota cu $i_A: A \rightarrow FM(A)$ incluziunea canonica a lui $A = A^1$ in $FM(A)$.

Propozitie 4.2. (Proprietatea de universalitate a monoidului liber.) Fie A o multime. Pentru orice monoid M si orice aplicatie $f: A \rightarrow M$ exista un unic morfism de monoizi $\tilde{f}: FM(A) \rightarrow M$ astfel ca $\tilde{f} \circ i_A = f$, sau, altfel spus, astfel ca diagrama

$$\begin{array}{ccc} A & \xrightarrow{i_A} & FM(A) \\ & \searrow \tilde{f} & \downarrow f \\ & M & \end{array}$$

să fie comutativa.

Demonstratie. Dacă $\tilde{f}: FM(A) \rightarrow M$ este un morfism de monoizi, avem:

$$\begin{aligned} \tilde{f}(x_1, x_2, \dots, x_n) &= \tilde{f}((x_1)(x_2) \dots (x_n)) = \\ &= \tilde{f}(x_1)\tilde{f}(x_2) \dots \tilde{f}(x_n) = (\tilde{f} \circ i)(x_1)(\tilde{f} \circ i)(x_2) \dots (\tilde{f} \circ i)(x_n) \end{aligned}$$

astfel că, dacă în plus $\tilde{f} \circ i = f$ (bineîntelese $i = i_A$):

$$(*) \quad \tilde{f}(x_1, x_2, \dots, x_n) = f(x_1)f(x_2) \dots f(x_n).$$

Aceasta demonstrează afirmația de unicitate din enunț. Pentru a demonstra afirmația de existență, trebuie definițit morfismul $\tilde{f}: FM(A) \rightarrow M$. Definiția lui \tilde{f} este exact $(*)$ și, este evident, din această definiție, că \tilde{f} este morfism de monoizi și că $\tilde{f} \circ i = f$.

Definiția 4.3. Fie M un monoid. O relație de echivalență \equiv pe mulțimea M se numește congruență a lui M dacă pentru orice $a, a', b, b' \in M$ avem $a \equiv a'$ și $b \equiv b'$ implică $ab \equiv a'b'$.

Fiind dată congruența \equiv a monoidului M , vom nota cu \bar{M} mulțimea factor M/\equiv și, pentru fiecare element $a \in M$, vom nota cu \bar{a} clasa de echivalență a lui a modulo \equiv :

$$\bar{a} = \{x \in M \mid a \equiv x\}.$$

Dacă $\bar{a} = \bar{a}'$ și $\bar{b} = \bar{b}'$, avem $a \equiv a'$ și $b \equiv b'$, deci $ab \equiv a'b'$, adică $\overline{ab} = \overline{a'b'}$. Aceasta ne permite să definim o lege de compozitie pe \bar{M} luind $\bar{a}\bar{b} = \overline{ab}$; această lege de compozitie este asociativă (deoarece este asociativă legea de compozitie a lui M) și are ca element neutru pe $\bar{1}$, unde 1 este elementul neutru al lui M . Monoidul \bar{M} se numește monoidul factor al lui M prin \equiv .

Noțiunile de congruență și monoid factor sunt generalizări naturale ale noțiunilor de subgrup normal și grup factor din paragraful precedent. Acest lucru rezultă clar din următoarea propoziție.

Propoziția 4.4. Fie G un grup, \equiv o congruență pe G și \tilde{G} monoidul factor corespunzător. Atunci \tilde{G} este grup, $H=I$ este un subgrup normal al lui G și există un unic morfism $f: \tilde{G} \rightarrow G/H$ astfel ca $f(\tilde{x}) = Hx$ pentru orice $x \in G$, acesta fiind un izomorfism de grupuri. În plus, nășind subgrupul H definit mai sus cu $\Phi(\equiv)$, φ este o aplicație bijectivă de la mulțimea congruențelor lui G pe mulțimea subgrupurilor normale ale lui G .

Demonstrație. \tilde{G} este grup deoarece pentru $a \in G$ avem $\tilde{a} \tilde{a}^{-1} = \tilde{a}^{-1} \tilde{a} = \tilde{1} = \tilde{a}^{-1}a = \tilde{a}^{-1}\tilde{a}$, deci \tilde{a} este inversabil în \tilde{G} și $(\tilde{a})^{-1} = \tilde{a}^{-1}$. Considerăm aplicația $p: G \rightarrow \tilde{G}$ definită prin $p(a) = \tilde{a}$, $a \in G$. Deoarece

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

p este morfism de grupuri. În plus, avem $a \in \text{Ker } p \Leftrightarrow \tilde{a} = \tilde{1} \Leftrightarrow a \in \tilde{H} = H$, deci $\text{Ker } p = H$, ceea ce demonstrează că $H \trianglelefteq G$.

Deoarece p este un morfism de grupuri surjectiv și $\text{Ker } p = \text{Ker } \pi = H$, unde $\pi: G \rightarrow G/H$ este proiecția canonică, rezultă că există un unic morfism $f: \tilde{G} \rightarrow G/H$ cu $f \circ p = \pi$, adică $f(\tilde{x}) = Hx$ pentru orice $x \in G$ și acesta este un izomorfism. Lăsăm demonstrația faptului că φ este o aplicație bijectivă ca exercițiu.

Propoziția 4.5. Fie M un monoid, \equiv o congruență a lui M , \tilde{M} monoidul factor și $p: M \rightarrow \tilde{M}$ aplicația definită prin $p(x) = \tilde{x}$, $x \in M$. Atunci p este morfism de monoizi și, pentru orice morfism de monoizi $f: M \rightarrow M'$ astfel ca $x \equiv x'$ implică $f(x) = f(x')$, există un unic morfism de monoizi $f': \tilde{M} \rightarrow M'$, astfel ca $f' \circ p = f$.

Demonstrație. Faptul că p este morfism de monoizi este evident: $p(xy) = \tilde{xy} = \tilde{x}\tilde{y} = p(x)p(y)$ și $p(1) = \tilde{1}$ = elementul neutru al lui \tilde{M} . Pentru două elemente $x, x' \in M$ avem

$$\tilde{x} = \tilde{x}' \Rightarrow x \equiv x' \Rightarrow f(x) = f(x').$$

Aceasta arată că putem defini aplicația $f': \tilde{M} \rightarrow M'$ prin $f'(\tilde{x}) = f(x)$, $x \in M$. Există, f' este morfism de monoizi și $f' \circ p = f$. Unicitatea lui f' rezultă imediat din faptul că p este aplicație surjectivă.

Propoziția 4.6. Fie $\{\equiv_i\}_{i \in I}$ o familie de congruențe ale monoidului M . Atunci $\bigcap_{i \in I} \equiv_i$ este de asemenea o congruență a lui M .

Demonstrația acestei propoziții este evidentă și o lăsăm ca exercițiu.

Definiția 4.7. Fie A o mulțime. Atunci putem alege o mulțime A' cardinal echivalentă cu A , astfel încât $A \cap A' = \emptyset$. Alegem de asemenea o bijecție $\alpha: A \rightarrow A'$ și notăm $\alpha(a) = a'$, $a \in A$. Vom nota și pentru un element $x \in A'$, $x' = \alpha^{-1}(x)$, astfel că $x'' = x$ pentru orice $x \in A \cup A'$. Considerăm monoidul $FM(A \cup A')$ și fie \equiv_0 intersecția tuturor congruențelor \equiv ale lui $FM(A \cup A')$, astfel ca $aa' \equiv 1$ și $a'a \equiv 1$ pentru orice $a \in A'$. În virtutea lui (4.6), \equiv_0 este o congruență pe $FM(A \cup A')$;

notăm monoidul factor al lui $FM(A)$ prin \equiv_0 cu $FG(A)$. Avem deci un morfism

$$p: FM(A \cup A') \rightarrow FG(A), \quad p(x) = \bar{x}, \quad x \in FG(A \cup A').$$

Vom nota cu j_A compunerea

$$A \xrightarrow{i} A \cup A' \xrightarrow{FM(A \cup A')} FM(A \cup A') \xrightarrow{p} FG(A).$$

i fiind incluziunea canonica a lui A în $A \cup A'$. Deci $j_A: A \rightarrow FG(A)$ și $j_A(a) = \bar{a}$. Pentru orice $a \in A$ avem, în $FG(A)$, $\bar{a}\bar{a}' = \bar{aa'} = \bar{1} = \bar{a'a} = \bar{a}\bar{a}$, astfel că \bar{a} și \bar{a}' sunt inversabile în monoidul $FG(A)$. Pe de altă parte, orice element din $FG(A)$ este de forma $\bar{x} = p(x)$ cu $x \in FM(A \cup A')$, deci $x = \alpha_1 \alpha_2 \dots \alpha_n$ cu $\alpha_i \in A \cup A'$ pentru orice $i \in \{1, 2, \dots, n\}$. Deoarece $\bar{x} = \bar{\alpha}_1 \bar{\alpha}_2 \dots \bar{\alpha}_n$ și $\bar{\alpha}_i$ sunt inversabile în $FG(A)$ pentru orice $i \in \{1, 2, \dots, n\}$, rezultă \bar{x} inversabil în $FG(A)$. Astfel $FG(A)$ este un grup; $FG(A)$ se numește grupul liber generat de mulțimea A .

Propoziția 4.8. (Proprietatea de universalitate a grupului liber): *Fie A o mulțime. Pentru orice grup G și orice aplicație $f: A \rightarrow G$ există un unic morfism de grupuri $\tilde{f}: FG(A) \rightarrow G$ astfel ca $\tilde{f} \circ j_A = f$:*

$$\begin{array}{ccc} A & \xrightarrow{j_A} & FG(A) \\ & \searrow f & \swarrow \tilde{f} \\ & G & \end{array}$$

Demonstrație. Definim aplicația $f': A \cup A' \rightarrow G$ prin:

$$f'(x) = \begin{cases} f(x) & \text{dacă } x \in A, \\ f(x')^{-1} & \text{dacă } x \in A'. \end{cases}$$

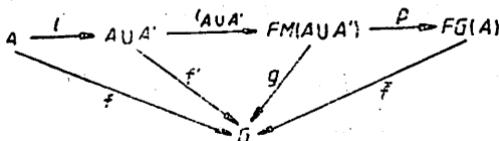
Evident avem $f' \circ i = f$. Aplicând proprietatea de universalitate a monoidului liber (4.2), rezultă un morfism de monoizi $g: FM(A \cup A') \rightarrow G$ astfel că $g \circ i_{A \cup A'} = f'$. Definim relația \equiv pe $FM(A \cup A')$ astfel:

$$x \equiv y \Leftrightarrow g(x) = g(y).$$

Deoarece g este morfism de monoizi, se constată imediat că \equiv este o congruență pe $FM(A \cup A')$. În plus, pentru orice element $a \in A$ avem $g(aa') = g(a)g(a') = f'(a)f'(a') = f'(a)f(a)^{-1} = 1$ și analog $g(a'a) = 1$, adică $aa' \equiv 1$ și $a'a \equiv 1$. Din definiția congruenței \equiv_0 pe $FM(A \cup A')$ rezultă că, pentru orice $x, y \in FM(A \cup A')$, avem

$$x \equiv_0 y \text{ implică } x \equiv y, \text{ adică } g(x) = g(y).$$

În virtutea propoziției (4.5) rezultă că există un morfism $\tilde{f}: FG(A) \rightarrow G$ astfel ca $\tilde{f} \circ p = g$.



Relațiile $f' \circ i = f$, $g \circ i|_{A \cup A'} = f'$, $f \circ p = g$ implică

$$f \circ j_A = f \circ p \circ i|_{A \cup A'} = g \circ i|_{A \cup A'} \circ i = f' \circ i = f.$$

Să considerăm un alt morfism $h: FG(A) \rightarrow G$ cu $h \circ j_A = f$, deci $h(\bar{a}) = f(a)$ pentru orice $a \in A$. Deoarece h este morfism de grupuri avem $h(\bar{a}^{-1}) = h((\bar{a})^{-1}) = h(\bar{a})^{-1} = f(a)^{-1}$ pentru orice $a \in A$, ceea ce demonstrează că $h \circ p \circ i|_{A \cup A'} = f \circ p \circ i|_{A \cup A'}$. Aplicând afirmația de unicitate din 4.2, rezultă $h \circ p = f \circ p$ și deci $h = f$ deoarece p este aplicație surjectivă.

Definiția 4.9. Fie I o mulțime și $\{G_i\}_{i \in I}$ o familie de grupuri indexată cu mulțimea I . Considerăm mulțimea produs cartezian $\prod_{i \in I} G_i$ și, pe această mulțime, definim o lege de compoziție astfel: dacă $x, y \in \prod_{i \in I} G_i$,

$$(*) \quad (x \cdot y)(i) = x(i)y(i) \text{ pentru orice } i \in I.$$

Spunem că am definit legea de compoziție pe $\prod_{i \in I} G_i$, „pe componente”.

Legea de compoziție astfel definită este asociativă:

$$\begin{aligned}
 ((x \cdot y)z)(i) &= (x \cdot y)(i)z(i) = (x(i)y(i))z(i) = \\
 &= x(i) \cdot (y(i)z(i)) = x(i) \cdot (y \cdot z)(i) = (x \cdot (y \cdot z))(i),
 \end{aligned}$$

elementul $1 \in \prod_{i \in I} G_i$, definit prin $1(i) = 1$ ($=$ elementul unitate în G_i) este evident element neutru al său și dacă $x \in \prod_{i \in I} G_i$, definim $x^{-1} \in \prod_{i \in I} G_i$ prin $x^{-1}(i) = x(i)^{-1}$ și avem evident $xx^{-1} = x^{-1}x = 1$. Astfel $\prod_{i \in I} G_i$, cu operația definită prin egalitatea $(*)$, este grup relativ la legea de compoziție $(*)$. Acest grup se numește *produsul direct* al familiei de grupuri $\{G_i\}_{i \in I}$ și se notează cu $\prod_{i \in I} G_i$.

În cazul cînd este dat un grup G și $G_i = G$ pentru orice $i \in I$ produsul direct $\prod_{i \in I} G_i$ se notează cu G^I . Reamintim că $G^I = \{x \mid x: I \rightarrow G\}$.

De asemenea, în cazul cînd mulțimea de indici I este finită, $I = \{1, 2, \dots, n\}$, produsul direct $\prod_{i \in I} G_i$ se notează cu $G_1 \times G_2 \times \dots \times G_n$.

Un element $x \in G_1 \times G_2 \times \dots \times G_n$ este o aplicație $x: \{1, 2, \dots, n\} \rightarrow G_1 \cup G_2 \cup \dots \cup G_n$, cu $x(i) \in G_i$ pentru orice $i \in \{1, 2, \dots, n\}$ și notind $x_i = x(i)$, putem scrie

$$x = (x_1, x_2, \dots, x_n).$$

În particular, cînd $n=2$, produsul direct $G_1 \times G_2$ are ca mulțime subiacentă produsul cartezian $G_1 \times G_2$ al mulțimilor subiacente lui G_1 și G_2 . Legea de compoziție pe $G_1 \times G_2 \times \dots \times G_n$ se scrie:

$$(x_1, x_2, \dots, x_n) (y_1, y_2, \dots, y_n) = (x_1 y_1, x_2 y_2, \dots, x_n y_n).$$

Propoziția 4.10. (Proprietatea de universalitate a produsului direct.) Fie I o mulțime și $\{G_i\}_{i \in I}$ o familie de grupuri și pentru fiecare $j \in I$ definim proiecția canonică $\pi_j: \prod_{i \in I} G_i \rightarrow G_j$ prin $\pi_j(x) = x(j)$, $x \in \prod_{i \in I} G_i$.

Atunci, pentru orice $i \in I$, π_i este un morfism de grupuri și pentru orice grup G și oricăre familie $\{f_i\}_{i \in I}$ de morfisme $f_i: G \rightarrow G_i$, există un unic morfism $f: G \rightarrow \prod_{i \in I} G_i$ astfel ca $\pi_i \circ f = f_i$ pentru orice $i \in I$.

Demonstrație. Faptul că proiecția canonică π_i este un morfism este evident. Dacă $f: G \rightarrow \prod_{i \in I} G_i$ este un morfism de grupuri astfel ca $\pi_i \circ f = f_i$ pentru orice $i \in I$, atunci, pentru orice $x \in G$ și orice $i \in I$, avem

$$f(x)(i) = \pi_i(f(x)) = (\pi_i \circ f)(x) = f_i(x).$$

Aceasta demonstrează unicitatea morfismului f din enunț și ne indică nouă că pentru a demonstra existența sa trebuie să definim aplicația $f: G \rightarrow \prod_{i \in I} G_i$ prin

$$f(x)(i) = f_i(x), \quad x \in G, \quad i \in I.$$

Aplicația f astfel definită este morfism deoarece pentru $x, y \in G$, $i \in I$ avem

$$f(xy)(i) = f_i(xy) = f_i(x)f_i(y) = f(x)(i) f(y)(i) = (f(x)f(y))(i),$$

deci

$$f(xy) = f(x)f(y)$$

și de asemenea

$$(\pi_i \circ f)(x) = \pi_i(f(x)) = f(x)(i) = f_i(x),$$

deci

$$\pi_i \circ f = f_i.$$

Prin urmare

Propoziția 4.11. Pentru orice mulțime A , aplicația $j_A: A \rightarrow FG(A)$ este injectivă.

Demonstrație. Considerăm grupul aditiv \mathbf{Z} al numerelor întregi și produsul direct \mathbf{Z}^A . Definim aplicația $f: A \rightarrow \mathbf{Z}^A$ prin

$$f(a)(b) = \begin{cases} 0 & \text{dacă } b \neq a, \\ 1 & \text{dacă } b = a \end{cases} \quad a, b \in A.$$

Aplicația f este injectivă. Într-adevăr, dacă $a, a' \in A$ și $a \neq a'$, avem $f(a)(a)=1$ și $f(a')(a)=0$, deci $f(a) \neq f(a')$. Aplicând proprietatea de universalitate a grupului liber, rezultă un morfism de grupuri $\tilde{f}:FG(A) \rightarrow Z^A$ astfel ca $\tilde{f} \circ j_A = f$. Deoarece f este aplicație injectivă, rezultă și j_A aplicație injectivă.

Observație. Aplicația $j_A:A \rightarrow FG(A)$ fiind injectivă, putem identifica elementele $a \in A$ cu imaginile lor $\tilde{a}=j_A(a)$ în $FG(A)$. Atunci mulțimea A este o mulțime de generatori pentru grupul $FG(A)$.

Definiția 4.12. Fie A o mulțime și R o submulțime a lui $FG(A)$. Spunem că o aplicație $\alpha:A \rightarrow G$, unde G este un grup, satisfac relațiile R dacă unicul morfism $f:FG(A) \rightarrow G$ astfel ca $f \circ j_A = \alpha$ are proprietatea că $f(r)=1$ pentru orice $r \in R$. Vom nota cu $N(R)$ intersecția tuturor subgrupurilor normale ale lui $FG(A)$ care conțin pe R , cu $G(A/R)$ grupul factor $FG(A)/N(R)$ și cu $\pi(A, R)$ compunerea de aplicații $p \circ j_A$:

$$A \xrightarrow{j_A} FG(A) \xrightarrow{p} FG(A)/N(R) = G(A, R) \text{ unde } p \text{ este proiecția canonică.}$$

Propoziția 4.13. Fie A o mulțime, R o submulțime a lui $FG(A)$ și $\alpha:A \rightarrow G$, G grup. Atunci α satisfac relațiile R dacă și numai dacă există un morfism $\tilde{\alpha}:G(A/R) \rightarrow G$ astfel ca $\tilde{\alpha} \circ \pi(A, R) = \alpha$. În această situație $\tilde{\alpha}$ este morfism surjectiv dacă $\alpha(A) = \{\alpha(a) \mid a \in A\}$ este sistem de generatori pentru G .

Demonstrație. Fie $f:FG(A) \rightarrow G$ unicul morfism, astfel ca $f \circ j_A = \alpha$ și fie $\pi = \pi(A, R) = p \circ j_A$, unde $p:FG(A) \rightarrow G(A/R) = FG(A)/N(R)$ este proiecția canonică. Presupunem că există un morfism $\tilde{\alpha}:G(A/R) \rightarrow G$ astfel ca $\tilde{\alpha} \circ \pi = \alpha$. Atunci $\tilde{\alpha} \circ p \circ j_A = \tilde{\alpha} \circ \pi = \alpha = f \circ j_A$, deci $\tilde{\alpha} \circ p = f$ conform afirmației de unicitate a propoziției 4.8. Pentru $r \in R \subseteq N(R) = \text{Ker } p$, avem $p(r)=1$, deci $f(r) = \tilde{\alpha}(p(r)) = 1$, adică α satisfac relațiile R . Reciproc, presupunem că α satisfac relațiile R . Atunci $R \subseteq \text{Ker } f \trianglelefteq FG(A)$, deci $\text{Ker } p = N(R) \trianglelefteq \text{Ker } f$. Atunci rezultă un mic morfism $\tilde{\alpha}:G(A/R) \rightarrow G$ cu $\tilde{\alpha} \circ p = f$ și avem $\tilde{\alpha} \circ \pi = \tilde{\alpha} \circ p \circ j_A = \alpha$. Dacă avem un alt morfism $\beta:G(A/R) \rightarrow G$ cu $\beta \circ \pi = \alpha$ egalitatea $(\beta \circ p) \circ j_A = \beta \circ \pi = \alpha = f \circ j_A$ arată că $\beta = \tilde{\alpha}$. Presupunem acum că morfismul $\tilde{\alpha}$ există. Pentru orice $a \in A$ avem $\alpha(a) = \tilde{\alpha}(\pi(a))$ și $\alpha(a)^{-1} = \tilde{\alpha}(\pi(a))^{-1}$. Conform propoziției 2.11, rezultă $\text{Im } \tilde{\alpha} = \langle \alpha(A) \rangle$. Ultima afirmație a propoziției noastre este acum evidentă.

Corolarul 4.14. Cu aceleși notății ca în propoziția 4.13, presupunem în plus că $\alpha(A)$ este un sistem de generatori pentru G și că există un număr natural n astfel ca $|G(A/R)| \leq n \leq |G|$. Atunci $\tilde{\alpha}$ este izomorfism și $|G(A/R)| = n = |G|$.

Demonstrație. Conform lui 4.13, $\tilde{\alpha}:G(A/R) \rightarrow G$ este un morfism surjectiv. Atunci $G(A/R)/\text{Ker } \tilde{\alpha} \cong G$, deci $|G(A/R)| = |G| \cdot |\text{Ker } \tilde{\alpha}|$. Rezultă $|G| \leq |G| \cdot |\text{Ker } \tilde{\alpha}| \leq |G|$, deci $|\text{Ker } \tilde{\alpha}| = 1$, și $\tilde{\alpha}$ este izomorfism.

Definiția 4.15. Fie G un grup și A un sistem de generatori al lui G . Atunci, unicul morfism $f:FG(A) \rightarrow G$, astfel ca $f \circ j_A = i$, unde $i:A \rightarrow G$ este incluziunea canonică, este surjectiv. Rezultă $G \cong FG(A)/\text{Ker } f$. Astfel orice grup G este izomorf cu un grup factor al unui grup liber. Elementele lui $\text{Ker } f$ se numesc *relații între generatorii* $a \in A$ ai grupului G .

Fie $R \subset \text{Ker } f$ o mulțime de astfel de relații. Atunci există un unic morfism $\tilde{\alpha}:G(A/R) \rightarrow G$, astfel ca $\tilde{\alpha} \circ \pi(A, R) = i$ sau, echivalent, $\tilde{\alpha} \circ p = f$, unde $p:FG(A) \rightarrow FG(A)/N(R) = G(A/R)$ este proiecția canonică. $\tilde{\alpha}$ este morfism surjectiv și este izomorfism dacă și numai dacă $\text{Ker } p = \text{Ker } f$, adică, dacă și numai dacă $N(R) = \text{Ker } f$. În această situație spunem că R este o mulțime de relații de definiție pentru G . Spunem de asemenea că G este un grup de prezentare A/R prin generatori și relații și scriem $G = \langle A/R \rangle$.

Spunem că grupul G este de prezentare finită dacă există A și R mulțimi finite, astfel ca $G = \langle A/R \rangle$. De regulă pentru $A = \{a_1, a_2, \dots, a_m\}$ și $R = \{r_1, r_2, \dots, r_n\}$ vom scrie $\langle a_1, a_2, \dots, a_m/r_1, r_2, \dots, r_n \rangle$ în loc de $\langle A/R \rangle$.

Exemplu. *Metoda enumerării claselor.* Vom exemplifica prezentarea prin generatori și relații a unor grupuri cunoscute. Vom discuta cu această ocazie, într-o formă primitivă, metoda enumerării claselor, metodă care datorită caracterului ei algoritmic a putut beneficia de calculatoarele electronice moderne, aducând mari servicii teoriei grupurilor în ultimii 20 de ani.

Grupul C_n . Luăm $A = \{z\}$, unde $z = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n} \in C_n$. Atunci A este un sistem de generatori pentru C_n și $z^n = 1$ astfel că incluziunea $i:A \rightarrow C_n$ satisface relațiile

$$R = \{z^n\} \subseteq FG(A).$$

Conform lui 4.13 avem un morfism surjectiv $\tilde{\alpha}:G(A/R) \rightarrow C_n$ astfel ca $\tilde{\alpha} \circ \pi(A, R) = i$. Luăm $x = \pi(A, R)(z)$. Atunci $\{x\}$ este un sistem de generatori pentru $G(A/R)$ și $x^n = 1$. Prin urmare $G(A/R) = \{x^i \mid i \in \{0, 1, \dots, n-1\}\}$ și deci $|G(A/R)| \leq n = |C_n|$. Conform lui 4.14, $\tilde{\alpha}$ este izomorfism și deci $C_n = \langle z / z^n \rangle$.

Grupul diedral D_n . Luăm $A = \{\sigma, \rho\} \subseteq D_n$ (vezi § 2). Avem $\sigma^n = 1$, $\rho^2 = 1$, $(\sigma\rho)^2 = \sigma(\sigma\rho)\rho = \sigma(\sigma^{n-1}\rho)\rho = \sigma^n\rho^2 = 1$, deci incluziunea $i:A \rightarrow D_n$ satisface relațiile $R = \{\sigma^n, \rho^2, (\sigma\rho)^2\} \subseteq FG(A)$. Deoarece A este sistem de generatori pentru D_n , există un morfism surjectiv $\tilde{\alpha}:G(A/R) \rightarrow D_n$ cu $\tilde{\alpha} \circ \pi(A, R) = i$. Luăm $x = \pi(A, R)(\sigma)$ și $y = \pi(A, R)(\rho)$. Atunci $\{x, y\}$ este un sistem de generatori pentru $G = G(A/R)$ și avem $x^n = 1$, $y^2 = 1$, $(xy)^2 = 1$. Lăum $H = \langle x \rangle \leq G$. Vom enumera clasele la dreapta ale lui G modulo H , aceste clase fiind notate cu numerele naturale 1, 2, Luăm 1 = H , clasa elementului unitate și 2 = $1y = Hy$. Atunci $2y = Hy^2 =$

$=H=1$ și $2y=1=1(xy)^2=1\cdot xy\cdot xy=1\cdot xy\cdot 2xy$, deci $2=2x$. Avem deci următoarea tablă de înmulțire a claselor 1 și 2 cu generatorii x și y ai lui G :

	x	y
1	1	2
2	2	1

Fie K reuniunea claselor 1 și 2 ale lui G . Din tablă de mai sus rezultă $Kx=K$ și $Ky=K$, deci $KG=K$ deoarece x și y generează pe G ; în fine, deoarece elementul unitate al lui G aparține lui K avem $G \leq KG = K$, deci $G=K$. Aceasta demonstrează că 1 și 2 sunt singurele clase la dreapta ale lui G modulo H . Am stabilit astfel că $|G:H| \leq 2$ și deoarece evident $|H| \leq n$, avem $|G| \leq 2n=D_n$. Conform lui 4.14, $\tilde{\alpha}$ este un izomorfism, deci $D_n = \langle \sigma, \rho | \sigma^n, \rho^2, (\sigma\rho)^2 \rangle$.

Grupul cuaternionilor Q . Luăm $A=\{j, k\}$ și $R=\{j^4, j^2k^{-2}, jk, jk^{-1}\}$. Atunci A este un sistem de generatori pentru Q și incluziunea canonica $i:A \rightarrow G$ satisfacă relațiile R deci există un morfism surjectiv $\tilde{\alpha}:G(A/R) \rightarrow Q$ astfel ca $\tilde{\alpha} \circ \pi(A, R)=i$:

Luăm $x=\pi(A, R)(j)$, $y=\pi(A, R)(k)$. Atunci $\{x, y\}$ este un sistem de generatori pentru $G=G(A/R)$ și $x^4=1$, $x^2y^{-2}=1$, $xyxy^{-1}=1$. Luăm $H=\langle x \rangle \leq G$. Numerotăm clasele la dreapta ale lui G modulo H cu numerele naturale 1, 2, Luăm $1=H$, deci $1x=1$. Luăm $1y^{-1}=2$, deci avem $2y=1$ și $1=1x^2y^{-2}=1y^{-1}y^{-1}=2y^{-1}$, deci $1y=2$. În fine, $2y^{-1}=1=1xyxy^{-1}=2xy^{-1}$, deci $1=2x$. Rezultă următoarea tablă de înmulțire a claselor 1, 2 cu generatorii x, y ai lui G :

	x	y
1	1	2
2	2	1

Că și la D_n , rezultă $|G:H| \leq 2$, și, cum $|H| \leq 4$ avem $|G| \leq 8=|Q|$. Prin urmare $Q=\{j, k | j^4j^2k^{-2}, jkjk^{-1}\}$.

Grupul $G(X, Y | X^3, Y^3, (XY)^2)$. Luăm $G=G(X, Y | X^3, Y^3, (XY)^2)$ și $x=p(X)$, $y=p(Y)$, unde $p:FG(\{X, Y\}) \rightarrow G$ este proiecția canonica. $\{x, y\}$ este atunci un sistem de generatori pentru G și avem $x^3=1$, $y^3=1$, $(xy)^2=1$. Luăm $H=\langle x \rangle \leq G$ și $1=H$, deci $1x=1$. Pentru a enumera clasele la dreapta ale lui G modulo H vom considera niște coloane având la capătul de sus litere x sau y , corespunzător relațiilor $x^3=1$, $y^3=1$, $(xy)^2=1$, astfel:

x	x	x	,	y	y	y	,	x	y	x	y

În stînga unei coloane vom pune una din clasele cunoscute, 1, 2, 3 ... și la dreapta ei rezultatul înmulțirii ei cu generatorul x sau y aflat în capătul de sus al liniei. Vom începe punînd în stînga primei coloane clasa 1. Deoarece $1x=1$, urmează imediat trei de 1, astfel:

x	x	x	,	y	y	y	,	x	y	x	y
1	1	1	1	2	3	1	1	2	4	1	

Luăm $1y=2$ și $2y=3$ și, deoarece $y^3=1$, vom avea $3y=1$. Luăm $2x=4$ și, deoarece $xyxy=1$, avem $4y=1$. Începem să completăm tabla înmulțirii claselor cu generatorii x, y :

	x	y
1	1	2
2	4	3
3		1
4		1

și observăm că $3y=4y$, deci $3=4$. Momentan tabla de înmulțire arată deci astfel:

	x	y
1	1	2
2	3	3
3		1

Vom pune acum la stînga primei coloane, 2, vom face înmulțirile conform tableei de mai sus, iar noile clase ce vor apărea le vom numera 4, 5, ...

x	x	x	,	y	y	y	,	x	y	x	y
2	3	4	2	3	1	2	3	1	1	2	

Completăm apoi tabla de înmulțire cu rezultatele nou apărute:

	x	y
1	1	2
2	3	3
3	4	1
4	2	

Vom pune la stînga primei coloane 3

x	x	x	$, y$	y	y	$, x$	y	x	y
3	4	2	3	1	2	3	4	5	6

și completăm tabla de înmulțire cu $4y=5$, $5x=6$, $6y=3$

	x	y
1	1	2
2	3	3
3	4	1
4	2	5
5	6	
6		3

Deoarece $2y=6y=3$, vedem că $6=2$, și $5x=6=2=4x$, deci $5=4$. Astfel tabla de înmulțire devine

	x	y
1	1	2
2	3	3
3	4	1
4	2	4

și este completă. Ca și la celealte exemple, deducem că $|G : H| \leq 4$, și deoarece $|H| \leq 3$, avem $|G| \leq 12$. Vom putea deduce ușor că $|G| = 12$ (și mai precis că $G \cong A_4$ — grupul altern pe patru elemente), din rezultatele privind grupul altern A_4 din capitolul următor.

§ 5. ACȚIUNI ALE GRUPURILOR PE MULȚIMI

Definiția 5.1. Fie G un grup și M o mulțime. Se numește *acțiune a lui G pe M* o aplicație $\alpha: G \times M \rightarrow M$ astfel ca:

a) pentru $g, g' \in G$ și $x \in M$ avem:

$$\alpha(gg', x) = \alpha(g, \alpha(g', x));$$

b) pentru $x \in M$ avem

$$\alpha(1, x) = x.$$

De regulă, pentru $g \in G$ și $x \in M$ folosim notația multiplicativă, $\alpha(g, x) = gx$, iar condițiile a) și b) de mai sus se scriu respectiv astfel:
a) $(gg')x = g(g'x)$, b) $1x = x$.

Spunem de asemenea că grupul G acționează pe mulțimea M cu acțiunea α , iar acțiunea elementului $g \in G$ pe elementul $x \in M$ este $\alpha(g, x)$.

Definiția 5.2. Fie G un grup și M o mulțime. Se numește *reprezentare a lui G prin permutări ale mulțimii M* un morfism de grupuri $\varphi: G \rightarrow S(M)$, unde $S(M)$ este grupul simetric pe mulțimea M .

Propoziția 5.3. Fie α o acțiune a grupului G pe mulțimea M notată multiplicativ. Atunci pentru fiecare element $g \in G$, aplicația $\varphi_g: M \rightarrow M$ definită prin $\varphi_g(x) = gx$, $x \in M$, este o permulare a mulțimii M iar aplicația $\varphi: G \rightarrow S(M)$ definită prin $\varphi(g) = \varphi_g$, $g \in G$, este un morfism de grupuri (φ se numește reprezentarea lui G prin permutări ale mulțimii M asociată acțiunii α).

Demonstrație. Fie $g, g' \in G$. Avem $\varphi_{gg'}(x) = (gg')x = g(g'x) = = \varphi_g(\varphi_{g'}(x))$ pentru orice $x \in M$, deci $\varphi_{gg'} = \varphi_g \circ \varphi_{g'}$. În plus $\varphi_1(x) = 1x = x$ pentru orice $x \in M$, deci $\varphi_1 = 1_M$ — aplicația identică a mulțimii M . Prin urmare, pentru $g \in G$, $\varphi_g \circ \varphi_{g^{-1}} = \varphi_{g \circ g^{-1}} = \varphi_1 = 1_M$ și $\varphi_{g^{-1}} = \varphi_{g^{-1}} = \varphi_1$. Aceasta demonstrează că φ_g este aplicație bijectivă și inversa sa este $\varphi_{g^{-1}}$. În particular $\varphi_g \in S(M)$ pentru orice $g \in G$ și putem deci considera aplicația $\varphi: G \rightarrow S(M)$ din enunț. Avem $\varphi(gg') = \varphi_g \circ \varphi_{g'} = \varphi_g \circ \varphi_{g'}$, pentru orice $g, g' \in G$, ceea ce demonstrează că φ este un morfism de grupuri (deci o reprezentare a lui G prin permutări ale mulțimii M).

Propoziția 5.4. Fie $\varphi: G \rightarrow S(M)$ o reprezentare a grupului G prin permutări ale mulțimii G . Pentru fiecare $g \in G$ notăm $\varphi_g = \varphi(g)$ și definim $\alpha: G \times M \rightarrow M$ prin $\alpha(g, x) = \varphi_g(x)$. Atunci α este o acțiune a lui G pe M (α se numește acțiunea lui G pe M asociată reprezentării prin permutări φ).

Demonstrație. Pentru $g, g' \in G$ și $x \in M$ avem $\alpha(gg', x) = \varphi_{gg'}(x) = = (\varphi_g \circ \varphi_{g'})(x) = \varphi_g(\varphi_{g'}(x)) = \alpha(g, \alpha(g', x))$ și $\alpha(1, x) = \varphi_1(x) = x$, ceea ce demonstrează că α este o acțiune a lui G pe M .

Observație. Fie G un grup și M o mulțime. Se poate demonstra imediat (și lăsăm aceasta ca un exercițiu), faptul că aplicația care duce o acțiune a lui G pe M în reprezentarea prin permutări asociată ei (propoziția 5.3) și aplicația care duce o reprezentare a lui G prin permutări ale mulțimii M în acțiunea asociată ei (propoziția 5.4) sunt aplicații in-

verse una altăea între mulțimea acțiunilor lui G pe M și mulțimea reprezentărilor lui G prin permutări ale lui M .

Definiția 5.5. Considerăm grupul G care acționează pe mulțimea M cu acțiunea α și fie $\varphi: G \rightarrow S(M)$ reprezentarea prin permutări asociată acțiunii. Deoarece φ este un morfism de grupuri, nucleul său $\text{Ker } \varphi$ este un subgrup normal al lui G care se va numi și nucleul acțiunii α și se va nota cu $\text{Ker } \alpha$. Folosind notațiile standard din (5.1) avem:

$$\text{Ker } \alpha = \{g \in G \mid \varphi_g = 1_M\} = \{g \in G \mid gx = x \text{ pentru orice } x \in M\}.$$

Acțiunea α se numește fidelă dacă reprezentarea prin permutări α este un morfism injectiv, adică, dacă nucleul $\text{Ker } \alpha$ este trivial. Prin urmare acțiunea este fidelă dacă și numai dacă:

$$gx = x \text{ oricare ar fi } x \in G \text{ implică } g = 1.$$

Definiția 5.6. Considerăm o acțiune a lui G pe M ca mai sus. Atunci, pentru fiecare element $x \in M$, notăm

$$\text{Stab}_G(x) = \{g \in G \mid gx = x\} \subset G.$$

Mulțimea $\text{Stab}_G(x)$ care se numește stabilizatorul lui x în G (relativ la acțiunea dată) este un subgrup al lui G . Într-adevăr, dacă $g_1, g_2 \in \text{Stab}_G(x)$, atunci $(g_1g_2)x = g_1(g_2x) = g_1x = x$, deci $g_1g_2 \in \text{Stab}_G(x)$; avem $1x = x$, deci $1 \in \text{Stab}_G(x)$ și dacă $g \in \text{Stab}_G(x)$, atunci $g^{-1}x = g^{-1}(gx) = (g^{-1}g)x = 1x = x$, deci $g^{-1} \in \text{Stab}_G(x)$.

Aveam

$$g \in \text{Ker } \alpha \Leftrightarrow gx = x \text{ pentru orice } x \in G \Leftrightarrow$$

$$g \in \text{Stab}_G(x) \text{ pentru orice } x \in G \Leftrightarrow g \in \bigcap_{x \in M} \text{Stab}_G(x).$$

Prin urmare $\text{Ker } \alpha = \bigcap_{x \in M} \text{Stab}_G(x)$

Definiția 5.7. Considerăm o acțiune a grupului G pe mulțimea M notată multiplicativ și definim o relație \sim pe M luând pentru $x_1, x_2 \in M$, $x_1 \sim x_2$ dacă și numai dacă există un $g \in G$ astfel că $gx_1 = x_2$. Relația \sim este o relație de echivalență pe M . Într-adevăr, pentru orice $x \in M$ avem $x = 1x$, deci $x \sim x$; dacă $x_1, x_2 \in M$ și $x_1 \sim x_2$ avem $gx_1 = x_2$ pentru un $g \in G$ și atunci $g^{-1}x_2 = g^{-1}(gx_1) = (g^{-1}g)x_1 = 1x_1 = x_1$, deci $x_2 \sim x_1$; dacă $x_1, x_2, x_3 \in M$ și $x_1 \sim x_2$ și $x_2 \sim x_3$, atunci $gx_1 = x_2$ și $g'x_2 = x_3$ pentru $g, g' \in G$, de unde rezultă $(g'g)x_1 = g'(gx_1) = g'x_2 = x_3$, deci $x_1 \sim x_3$.

Clasa de echivalență a unui element $x \in G$ relativ la relația \sim se numește orbită lui x relativ la acțiunea α și se notează cu Gx . Avem:

$$Gx = \{y \in M \mid x \sim y\} = \{y \in M \mid \text{există } g \in G : gx = y\} = \{gx \mid g \in G\}.$$

Mulțimea factor M/\sim este o partitie a mulțimii M și prin urmare, avem

$$|M| = \sum_{Gx \in M/\sim} |Gx|.$$

Aceasta este forma originară a ceea ce se numește ecuația claselor pentru acțiunea α . Vom vedea că această ecuație a claselor capătă în unele cazuri particulare o semnificație deosebită în teoria grupurilor.

Propoziția 5.8. Pentru orice element $x \in M$ avem:

$$|Gx| = |G:\text{Stab}_G(x)|.$$

Demonstrație. Pentru două elemente $g_1, g_2 \in G$, avem $g_1 \text{Stab}_G(x) = g_2 \text{Stab}_G(x) \Leftrightarrow g_1^{-1}g_2 \in \text{Stab}_G(x) \Leftrightarrow g_1^{-1}g_2x = x \Leftrightarrow g_1x = g_2x$.

Rezultă că putem defini o aplicație

$$\psi: (G/\text{Stab}_G(x)) \rightarrow Gx$$

prin $\psi(g/\text{Stab}_G(x)) = gx$ și că, această aplicație este bijecțivă.

Observație. Ecuația claselor pentru acțiunea α capătă, în virtutea propoziției precedente, forma

$$|M| = \sum_{Gx \in M/\sim} |G:\text{Stab}_G(x)|.$$

Pentru fiecare element $x \in G$, numărul cardinal $|Gx|$ se numește și lungimea orbitei Gx . Orbitele de lungime 1 se numesc orbite triviale. Evident orbita Gx este trivială dacă și numai dacă $Gx = \{x\}$, adică, dacă și numai dacă $gx = x$ pentru orice element $g \in G$. Un element $x \in M$ a cărui orbită Gx este trivială se va numi element fixat de acțiunea α și vom nota cu

$$\text{Fix}_G(M) = \{x \in M \mid Gx = \{x\}\}$$

mulțimea elementelor fixate de acțiunea α . Ecuația claselor pentru acțiunea α devine atunci

$$|M| = |\text{Fix}_G(M)| + \sum_{Gx \text{ orbită netivială}} |Gx|$$

sau

$$|M| = |\text{Fix}_G(M)| + \sum_{Gx \text{ orbită netivială}} |G:\text{Stab}_G(x)|$$

Definiția 5.9. Considerăm că grupul G acționează pe o mulțime M cu acțiunea α și fie H un subgrup al lui G . Atunci α induce o acțiune α' a lui H pe M definită prin

$$\alpha': H \times M \rightarrow M, \quad \alpha'(h, x) = \alpha(h, x) = hx, \quad h \in H, \quad x \in M.$$

Dacă $\varphi: G \rightarrow S(M)$ este reprezentarea prin permutări asociată lui α , atunci reprezentarea prin permutări asociată acțiunii induse α' este restricția $\varphi': H \rightarrow S(M)$ a lui φ la H . α' se numește și restricția acțiunii α la H .

Pentru fiecare element $x \in M$ avem evident

$$\text{Stab}_H(x) = H \cap \text{Stab}_G(x).$$

și, de asemenea, $\text{Ker } \alpha' = H \cap \text{Ker } \alpha$.

Presupunem acum că H este un subgrup normal în G și că $H \trianglelefteq \text{Ker } \alpha$ adică, că $hx = x$ pentru orice $h \in H$ și $x \in M$ (se spune și că H acționează trivial pe M). Considerind proiecția canonica $\pi: G \rightarrow G/H$ și reprezentarea prin permutări $\varphi: G \rightarrow S(M)$ asociată acțiunii α avem $\text{Ker } \pi = H \trianglelefteq \text{Ker } \alpha = \text{Ker } \varphi$ și atunci există un morfism $\varphi': G/H \rightarrow S(M)$ astfel ca $\varphi' \circ \pi = \varphi$, adică $\varphi'(gH) = \varphi(g)$ pentru orice element $g \in G$. Morfismul φ' este o reprezentare a grupului G/H prin permutări ale mulțimii M și acțiunea corespunzătoare $\alpha': G/H \times M \rightarrow M$ este evident definită prin $\alpha'(gH, x) = \alpha(g, x)$, pentru orice $g \in G$ și $x \in M$. Spunem că α' este acțiunea lui G/H pe mulțimea M , indușă de acțiunea α .

Pentru fiecare element $x \in M$ avem $H \trianglelefteq \text{Ker } \alpha \trianglelefteq \text{Stab}_G(x)$ și evident

$$\text{Stab}_{G/H}(x) = \text{Stab}_G(x)/H.$$

În particular, $\text{Ker } \alpha' = \text{Ker } \alpha/H$.

Definiția 5.10. Fie α o acțiune a grupului G pe o mulțime M . O submulțime M' a lui M se numește α -stabilă dacă pentru orice $x \in M'$ și orice $g \in G$ avem $gx = \alpha(g, x) \in M'$. În această situație putem defini

$$\alpha': G \times M' \rightarrow M'$$

prin $\alpha'(g, x) = \alpha(g, x)$ ($g \in G$, $x \in M'$) și α' este evident o acțiune a grupului G pe mulțimea M' . Spunem că acțiunea α' este indușă de acțiunea α .

În particular, o orbită, să zicem orbita $O = Gx$, relativă la acțiunea α este α -stabilă: pentru orice element $y \in O$ avem $y = \sigma x$ pentru un $\sigma \in G$ și atunci, pentru orice $g \in G$, $gy = g(\sigma x) = (g\sigma)x \in Gx = O$.

Definiția 5.11. O acțiune α a grupului G pe o mulțime M se numește tranzitivă dacă pentru orice două elemente $x, x' \in M$ există un element $g \in G$ astfel încât $x' = gx = \alpha(g, x)$. În particular rezultă că pentru orice element $x \in G$ avem $Gx = M$, astfel încât o acțiune tranzitivă α are o unică orbită.

Dacă α este o acțiune oarecare a lui G pe M și O este o orbită a acestei acțiuni, acțiunea α' indușă de α pe O este tranzitivă.

Definiția 5.12. Fie α și α' două acțiuni ale grupului G pe mulțimile M și respectiv M' . Spunem că acțiunile α și α' sunt echivalente dacă există o aplicație bijectivă $f: M \rightarrow M'$ astfel încât

$$\alpha'(g, f(x)) = f(\alpha(g, x))$$

pentru orice $g \in G$ și $x \in M$, sau în notația standard:

$$gf(x) = f(gx)$$

pentru orice $g \in G$, $x \in M$.

Dacă acțiunile α și α' sunt echivalente, pentru fiecare element $x \in G$ avem:

$$\text{Stab}_G(x) = \text{Stab}_G(f(x)) \text{ și în particular } \text{Ker } \alpha = \text{Ker } \alpha', \quad f(Gx) = Gf(x)$$

și, în general, cele două acțiuni α și α' au aceleasi proprietăți. În particular, dacă acțiunea α este tranzitivă, atunci și α' este tranzitivă și reciproc.

Acțiuni prin multiplicare la dreapta. Fie G un grup și definim o acțiune α a grupului G pe mulțimea G a elementelor lui G , $\alpha: G \times G \rightarrow G$ ca fiind exact legea de compozitie binară a grupului G . Condițiile a) și b) din definiția acțiunii (vezi (5.1)) sunt verificate datorită faptului că legea de compozitie a grupului este asociativă și are element unitate. Acțiunea α se numește acțiunea lui G pe el însuși prin multiplicare la dreapta.

Relativ la acțiunea α , avem, pentru fiecare element $x \in G$, $\text{Stab}_G(x) = \{g \in G \mid gx = x\} = \{1\}$, astfel că $\text{Stab}_G(x) = 1$ și $\text{Ker } \alpha = 1$, deci acțiunea α este fidelă. Rezultă că reprezentarea prin permutări $\varphi: G \rightarrow S(G)$ asociată acțiunii α este un morfism injectiv și regăsim astfel teorema lui Cayley (vezi 2.21).

O altă acțiune a grupului G pe mulțimea elementelor lui G se definește prin $\alpha': G \times G \rightarrow G$, $\alpha'(g, x) = xg^{-1}$. Verificarea condițiilor a) și b) din definiția unei acțiuni se face astfel:

$$\alpha'(gg', x) = x(gg')^{-1} = x(g'^{-1}g^{-1}) = (xg'^{-1})g^{-1} = \alpha'(g, xg'^{-1}) = \alpha'(g, \alpha'(g', x)),$$

$$\alpha'(1, x) = x \cdot 1^{-1} = x \cdot 1 = x.$$

Spunem că α' este acțiunea lui G pe el însuși prin multiplicare la stânga.

Acum fie α acțiunea lui G pe el însuși prin multiplicare la dreapta și α' acțiunea lui G pe el însuși prin multiplicare la stânga. Putem defini aplicația $f: G \rightarrow G$ prin $f(x) = x^{-1}$ și evident f este o aplicație bijectivă. Deoarece

$$\begin{aligned} \alpha'(g, f(x)) &= \alpha'(g, x^{-1}) = x^{-1}g^{-1} = (g \cdot x)^{-1} = \\ &= f(gx) = f(\alpha(g, x)), \end{aligned}$$

rezultă că acțiunile α și α' sunt echivalente.

Fie G un grup și H un subgrup al lui G . Consider acțiunea lui G pe el însuși prin multiplicare la dreapta și apoi restricția acestei acțiuni la H (vezi definiția 5.9). Orbita unui element $x \in G$ relativ la această

restricție este exact clasa de congruență la dreapta Hx . Conform propoziției 5.8 avem:

$$|Hx| = |\{H : \text{Stab}_H(x)\}|$$

și conform definiției 5.9.

$$\text{Stab}_H(x) = H \cap \text{Stab}_G(x) = H \cap 1 = 1$$

astfel încât rezultă $|Hx| = |H|$, pentru orice $x \in G$. În plus ecuația claselor pentru acțiunea noastră devine:

$$|G| \sum_{Hx \in (G/H)_d} |Hx| = |(G/H)_d| \cdot |H| = |G:H| \cdot |H|$$

și reobținem astfel teorema lui Lagrange 2.19.

Fie G un grup, H un subgrup al lui G și considerăm acțiunea α a lui G pe mulțimea $(G/H)_d$, definită prin $\alpha(g, xH) = gxH$. Condițiile din definiția unei acțiuni sunt evident satisfăcute. α se numește acțiunea lui G pe mulțimea $(G/H)_d$, prin multiplicare la dreapta.

Aveam, pentru un element $g \in G$,

$$g \in \text{Ker } \alpha \Leftrightarrow gxH = xH \text{ pentru orice } x \in G \Leftrightarrow x^{-1}gx \in H \text{ pentru orice } x \in G \Leftrightarrow g \in xHx^{-1} \text{ pentru orice } x \in G.$$

Prin urmare,

$$\text{Ker } \alpha = \bigcap_{x \in G} xHx^{-1}.$$

$\text{Ker } \alpha$ este un subgrup normal al lui G care se notează de obicei cu H_G și se numește interiorul normal al lui H în G . Dacă K este un subgrup normal al lui G inclus în H avem, pentru orice $x \in G$,

$$K = xKx^{-1} \leq xHx^{-1},$$

deci $K \leq \bigcap_{x \in G} xHx^{-1} = H_G$. Astfel H_G este cel mai mare subgrup normal al lui G inclus în H .

Considerăm acum reprezentarea prin permutări $\varphi: G \rightarrow S((G/H)_d)$ asociată acțiunii α , și proiecția canonică $\pi: G \rightarrow G/H_G$. Deoarece $\text{Ker } \pi = \text{Ker } \varphi = H_G$, există un morfism $\varphi': G/H_G \rightarrow S((G/H)_d)$ astfel ca $\varphi' \circ \pi = \varphi$ și în plus φ' este un morfism injectiv. Prin urmare grupul G/H_G se poate scufunda în $S((G/H)_d)$. În particular dacă indicele lui H în G este finit și $|G:H| = n$, atunci G/H_G se poate scufunda în S_n .

Propoziția 5.13. Fie G un grup finit și p cel mai mic număr prim prin care divide ordinul lui G . Atunci orice subgrup H al lui G de indice p este normal în G .

Demonstratie. Rezultatele precedente arată că grupul G/H_G se poate scufunda în S_p și, prin teorema lui Lagrange, obținem $|G:H_G| = |p!$. Deoarece $H_G \leq H \leq G$, tot prin teorema lui Lagrange avem $|G:H_G| = |G:H| \cdot |H:H_G| = p \cdot |H:H_G|$ și rezultă $|H:H_G| = 1$.

$|H_G| \mid |(p-1)!|$. Dacă $|H:H_G| \neq 1$, există un număr prim q care divide $|H:H_G|$, deci $q \mid (p-1)!$, de unde rezultă $q < p$; pe de altă parte, $|H:H_G| \mid |G|$, deci q divide $|G|$ ceea ce contrazice faptul că p este cel mai mic număr prin care dixide ordinul lui G . Prin urmare $|H:H_G|=1$, adică $H=H_G$ și astfel H este normal în G .

Fie G un grup și H, K subgrupuri ale lui G . Considerăm acțiunea α a lui G pe (G/H) , prin multiplicare la dreapta și fie α' restricția acestei acțiuni la K . Orbita unui element $xH \in (G/H)$, relativ la acțiunea α' este mulțimea

$$K(xH) = \{kxH \mid k \in K\}$$

și reuniunea tuturor claselor din (G/H) , aparținind acestei mulțimi se notează cu KxH :

$$KxH = \bigcup_{k \in K} kxH = \{kxh \mid k \in K, h \in H\}$$

și se numește clasa dublă a lui x relativ la K și H . Deoarece clasele la stînga din mulțimea $K(xH)$ sunt disjuncte două cîte două și au toate cardinalul egal cu H , rezultă

$$|KxH| = |H| \cdot |K(xH)|.$$

Pentru a calcula $|K(xH)|$ vom folosi propoziția 5.8. Mai întîi avem, pentru un element $g \in G$,

$$g \in \text{Stab}_G(xH) \Leftrightarrow gxH = xH \Leftrightarrow x^{-1}gx \in H \Leftrightarrow g \in xHx^{-1},$$

deci $\text{Stab}_G(xH) = xHx^{-1}$ și rezultă:

$$\text{Stab}_K(xH) = K \cap \text{Stab}_G(xH) = K \cap xHx^{-1}.$$

Prin urmare orbita $K(xH)$ are lungimea

$$|K(xH)| = |K : \text{Stab}_K(xH)| = |K : K \cap xHx^{-1}|,$$

și astfel:

$$|KxH| = |H| \cdot |K : K \cap xHx^{-1}|.$$

În particular, pentru $x=1$, obținem

$$|KH| = |H| \cdot |K : K \cap H|,$$

iar în cazul cînd H și K sunt finite, putem scrie egalitățile de mai sus sub forma

$$|KxH| = \frac{|K| \cdot |H|}{|K \cap xHx^{-1}|} \text{ respectiv } |KH| = \frac{|K| \cdot |H|}{|K \cap H|}$$

Propoziția 5.14. O acțiune α a grupului G pe o mulțime M este tranzitivă dacă și numai dacă α este echivalentă cu acțiunea lui G pe o mulțime de forma $(G/H)_s$, $H \leq G$, prin multiplicare la dreapta.

Demonstrație. Fie $H \leq G$ și α' acțiunea lui G pe $(G/H)_s$, prin multiplicare la dreapta. α' este o acțiune tranzitivă deoarece pentru orice două elemente $xH, yH \in (G/H)_s$, avem $g = yx^{-1} \in G$ și $\alpha'(g, xH) = g(xH) = yx^{-1}xH = yH$. Evident, orice acțiune a lui G echivalentă cu α' este de asemenea tranzitivă. Reciproc, să presupunem că α este o acțiune a grupului G pe mulțimea M , tranzitivă. Atunci, fixăm un element $a_0 \in M$ și fie $H = \text{Stab}_G(a_0)$, astfel că, pentru două elemente $x, y \in G$, avem (presupunind acțiunea α notată multiplicativ):

$$xa_0 = ya_0 \Leftrightarrow (x^{-1}y)a_0 = a_0 \Leftrightarrow x^{-1}y \in H \Leftrightarrow xH = yH.$$

Rezultă că putem defini aplicația $f: M \rightarrow (G/H)_s$, prin $f(xa_0) = xH$ și această aplicație este bijectivă. În plus, este clar că

$$f(g(xa_0)) = f((gx)a_0) = (gx)H = g(xH) = gf(xa_0)$$

adică

$$f(\alpha(g, xa_0)) = \alpha'(g, f(xa_0)),$$

ceea ce demonstrează că acțiunile α și α' , α' fiind acțiunea lui G pe $(G/H)_s$, prin multiplicare la dreapta, sunt echivalente.

Structura elementelor din grupul S_n . Fie M o mulțime și G un grup de permutări pe mulțimea M , adică G este un subgrup al grupului simetric $S(M)$. Aplicația $\alpha: G \times M \rightarrow M$ definită prin $\alpha(\sigma, x) = \sigma(x)$ este atunci o acțiune a grupului G pe mulțimea M . Într-adevăr, avem, pentru $\sigma, \tau \in G$, $(\sigma \circ \tau)(x) = \sigma(\tau(x))$ și $1(x) = x$. Acțiunea σ se numește acțiunea canonică a lui G pe mulțimea M . Vom nota adesea, pentru $\sigma \in G$ și $x \in M$, $\sigma x = \sigma(x)$.

În particular, să considerăm acțiunea canonică a grupului S_n pe mulțimea $M = \{1, 2, \dots, n\}$ a primelor n numere naturale. Presupunând $n \geq 2$, se vede ușor că

$$\text{Stab}_{S_n}(n) = \{\sigma \in S_n \mid \sigma n = n\} \cong S_{n-1}$$

și deoarece evident această acțiune este tranzitivă, avem

$$n = |M| = |S_n : \text{Stab}_{S_n}(n)| = \frac{|S_n|}{|\text{Stab}_{S_n}(n)|},$$

adică $|S_n| = n \cdot |\text{Stab}_{S_n}(n)|$.

Deoarece evident $|S_1| = 1$, din relația de mai sus, rezultă, prin inducție după n , $|S_n| = n!$

Definiția 5.15. Fie n un număr natural, $\sigma \in S_n$ și $G = \langle \sigma \rangle$, subgrupul lui S_n generat de σ . Considerăm acțiunea canonica a grupului G pe mulțimea $M = \{1, 2, \dots, n\}$. Orbitele acestei acțiuni le vom numi și σ -orbite.

Permutarea σ este permutarea identică, $\sigma = 1$, dacă și numai dacă toate σ -orbitele sunt triviale. Dacă există o singură σ -orbită netrivială, permutarea σ se numește ciclu; σ -orbită netrivială se numește orbită de definiție a ciclului σ , iar lungimea sa se numește lungimea ciclului σ .

Dacă $\{i_1, i_2, \dots, i_m\}$ este o submulțime a lui M , permutarea notată $\sigma = (i_1, i_2, \dots, i_m)$ și definită prin $\sigma(i_1) = i_2, \dots, \sigma(i_{m-1}) = i_m, \sigma(i_m) = i_1$, $\sigma(i) = i$ pentru $i \notin \{i_1, i_2, \dots, i_m\}$ este evident un ciclu de lungime m a căruia orbită de definiție este $\{i_1, i_2, \dots, i_m\}$. Permutarea identică se consideră uneori ca fiind ciclu de lungime 1 și oricare din submulțimile cu un singur element ale lui M se poate considera ca orbită de definiție pentru ea.

Două cicluri σ_1 și σ_2 se numesc disjuncte dacă orbitele lor de definiție sunt submulțimi disjuncte ale lui M .

Propoziția 5.16. Fie $\sigma \in S_n$ și $i \in M = \{1, 2, \dots, n\}$. Atunci există un cel mai mic număr întreg pozitiv k astfel încât $\sigma^k i = i$; acest k este egal cu lungimea σ -orbitei lui i și avem

$$\langle \sigma \rangle i = \{\sigma^m i \mid m \in \mathbb{Z}\} = \{i, \sigma i, \sigma^2 i, \dots, \sigma^{k-1} i\}.$$

Demonstrație. Mulțimea $\{\sigma^m i \mid m \in \mathbb{Z}\}$ fiind o submulțime a lui M , este finită deci există numere întregi m' și m ; $m < m'$ și $\sigma^{m'} i = \sigma^m i$. Atunci $i = (\sigma^{-m} \sigma^{m'})i = \sigma^{-m} (\sigma^{m'} i) = (\sigma^{-m} \sigma^{m'})i = \sigma^{m'-m} i$ și $m' - m > 0$. Prin urmare există cel mai mic întreg pozitiv k astfel încât $\sigma^k i = i$. Pentru orice $m \in \mathbb{Z}$, fie $m = kq + r$ cu $0 \leq r < k$. Deoarece $\sigma^k i = i$ și $\sigma^{-k} i = \sigma^{-k} (\sigma^k i) = \sigma^0 i = i$, rezultă $(\sigma^k)^q i = i$ pentru orice $q \in \mathbb{Z}$, și deci

$$\sigma^m i = (\sigma^r \circ (\sigma^k)^q) i = \sigma^r ((\sigma^k)^q i) = \sigma^r i.$$

Aceasta demonstrează că σ -orbita $\langle \sigma \rangle i$ este

$$\langle \sigma \rangle i = \{\sigma^r i \mid 0 \leq r < k\}.$$

Dacă avem $0 \leq r < r' < k$ și $\sigma^r i = \sigma^{r'} i$, atunci $\sigma^{r'-r} i = i$ și $0 < r' - r \leq r' < k$, ceea ce contrazice alegerea săcătă asupra lui k . Aceasta demonstrează că mulțimea $\{\sigma^r i \mid 0 \leq r < k\}$ are k elemente și deci că σ -orbita $\langle \sigma \rangle i$ are lungimea k .

Propoziția 5.17. Dacă $\sigma_1, \sigma_2 \in S_n$ sunt două cicluri disjuncte, atunci $\sigma_1 \sigma_2 = \sigma_2 \sigma_1$.

Demonstrație. Fie O_1 și O_2 orbitele de definiție pentru ciclurile σ_1 și respectiv σ_2 . Dacă $i \in O_1$ avem $i \notin O_2$ deci $(\sigma_1 \sigma_2)i = \sigma_1(\sigma_2 i) = \sigma_1 i$; în plus, $\sigma_1 i \in O_1$, deci $\sigma_1 i \notin O_2$ și $(\sigma_2 \sigma_1)i = \sigma_2(\sigma_1 i) = \sigma_1 i$. Analog pentru $i \in O_2$ vom avea $(\sigma_1 \sigma_2)i = (\sigma_2 \sigma_1)i$. În fine pentru $i \notin O_1 \cup O_2$ avem $\sigma_1 i = \sigma_2 i = i$, deci $(\sigma_1 \sigma_2)i = (\sigma_2 \sigma_1)i = i$.

Propoziția 5.18. Fie $\sigma_1, \sigma_2, \dots, \sigma_m \in S_n$ cicluri disjuncte două căle două, orbitele lor de definiție fiind O_1, O_2, \dots, O_m și fie $\sigma = \sigma_1 \sigma_2 \dots \sigma_m$. Atunci ciclurile $\sigma_1, \sigma_2, \dots, \sigma_m$ sunt permutabile două căle două și pentru un $i \in \{1, 2, \dots, n\}$ σ -orbita $\langle \sigma \rangle i$ este trivială dacă $i \notin O_1 \cup O_2 \cup \dots \cup O_m$ și egală cu O_k dacă $i \in O_k$ pentru un $k \in \{1, 2, \dots, m\}$.

Demonstrație. Faptul că ciclurile $\sigma_1, \sigma_2, \dots, \sigma_m$ sunt permutabile două căle două rezultă din propoziția 5.17. Dacă $i \notin O_1 \cup O_2 \cup \dots \cup O_m$, atunci $\sigma_1 i = \sigma_2 i = \dots = \sigma_m i = i$, deci $\sigma i = i$ și $\langle \sigma \rangle i = \{i\}$. Acum fie $i \in O_k$, $k \in \{1, 2, \dots, m\}$. Deoarece ciclurile $\sigma_1, \sigma_2, \dots, \sigma_m$ sunt permutabile două căle două, este suficient să considerăm cazul $k=m$. Atunci $\sigma_m^j i \in O_m$ și $\sigma_m^j i \notin O_1 \cup \dots \cup O_{m-1}$ pentru orice $j \in \mathbb{Z}$ și în plus $\sigma^j = \sigma_1^j \sigma_2^j \dots \sigma_m^j$, deci $\sigma^j i = (\sigma_1^j \dots \sigma_{m-1}^j) (\sigma_m^j i) = \sigma_m^j i$, astfel că $\langle \sigma \rangle i = \langle \sigma_m \rangle i = O_m$.

Propoziția 5.19. Pentru orice permutare $\sigma \in S_n$ există un număr natural m și ciclurile $\sigma_1, \sigma_2, \dots, \sigma_m \in S_n$ disjuncte două căle două astfel ca $\sigma = \sigma_1 \sigma_2 \dots \sigma_m$. În plus ciclurile $\sigma_1, \sigma_2, \dots, \sigma_m$ sunt unic determinate (abstracție făcând de ordinea lor) de σ .

Demonstrație. Fie O_1, O_2, \dots, O_m toate σ -orbitele netriviale și fie l_k lungimea orbitei O_k , $k \in \{1, 2, \dots, m\}$. Pentru fiecare $k \in \{1, 2, \dots, n\}$ alegem un element $i \in O_k$ și propoziția 5.16 arată că

$$O_k = \{i, \sigma i, \dots, \sigma^{l_k-1} i\}.$$

Considerăm atunci ciclul

$$\sigma_k = (i, \sigma i, \dots, \sigma^{l_k-1} i)$$

a cărui orbită de definiție este exact O_k . Pentru orice $i' \in O_k$ avem $i' = \sigma^{j'} i = \sigma_k^j i$ pentru un j cu $0 \leq j < l_k$ și $\sigma^{j'} = \sigma^{j+1} i = \sigma_k^{j+1} i = \sigma_k \sigma_k^j i = \sigma_k i'$, ceea ce arată în particular că σ_k nu depinde de alegerea elementului $i \in O_k$. Ciclurile $\sigma_1, \sigma_2, \dots, \sigma_m$ sunt disjuncte două căle două. Pentru $i \notin O_1 \cup O_2 \cup \dots \cup O_m$ avem $\sigma_1 i = \sigma_2 i = \dots = \sigma_m i = i$ și $\sigma i = i$, deci $\sigma i = (\sigma_1 \sigma_2 \dots \sigma_m) i$. Acum să presupunem $i \in O_k$ pentru un $k \in \{1, 2, \dots, m\}$. Trebuie să demonstrăm egalitatea $\sigma i = (\sigma_1 \sigma_2 \dots \sigma_m) i$. Deoarece conform propoziției 5.18, ciclurile $\sigma_1, \sigma_2, \dots, \sigma_m$ sunt permutabile două căle două este suficient să facem demonstrația în cazul $k=m$. Aveam $\sigma i = \sigma_m i$ și deoarece $\sigma_m^j \notin O_1 \cup \dots \cup O_{m-1}$, $(\sigma_1 \sigma_2 \dots \sigma_m) i = (\sigma_1^j \dots \sigma_{m-1}^j) (\sigma_m^j i) = \sigma_m^j i = \sigma i$. Aveam astfel $\sigma = \sigma_1 \sigma_2 \dots \sigma_m$. Pentru a demonstra afirmația de unicitate să considerăm că $\sigma = \sigma'_1 \sigma'_2 \dots \sigma'_{m'}$, unde $\sigma'_1, \sigma'_2, \dots, \sigma'_{m'}$ sunt cicluri disjuncte două căle două, ale căror orbite de definiție sunt $O'_1, \dots, O'_{m'}$. Conform propoziției 5.18, $O'_1, \dots, O'_{m'}$ sunt toate σ -orbitele netriviale, astfel că $m'=m$ și abstracție făcând de ordinea ciclurilor $\sigma'_1, \sigma'_2, \dots, \sigma'_{m'}$ putem presupune $O_k = O'_k$ pentru orice $k \in \{1, 2, \dots, m\}$. Din demonstrația propoziției 5.18 se vede că pentru orice $i \in O_k = O'_k$ avem $\sigma'_k i = i = \sigma_k i$, și deci avem $\sigma'_k = \sigma_k$ pentru orice $k \in \{1, 2, \dots, m\}$.

Definiția 5.20 Fie $\sigma \in S_n$ și fie O_1, O_2, \dots, O_m toate σ -orbitele (triviale și netriviale) și pentru fiecare $k \in \{1, 2, \dots, m\}$ definim ciclul σ_k ca în demonstrația propoziției 5.19. Atunci $\sigma_1, \sigma_2, \dots, \sigma_m$ sunt *cicluri disjuncte* două cîte două și avem

$$\sigma = \sigma_1 \sigma_2 \dots \sigma_m.$$

Numim această descompunere a lui σ ca produs de cicluri disjuncte. Evident putem presupune că primele k_1 cicluri din această descompunere sunt de lungime 1, următoarele k_2 sunt de lungime 2 etc., deci pentru fiecare $j \in \{1, 2, \dots, n\}$, k_j este numărul ciclurilor de lungime j care apar în descompunerea lui σ . k_1, k_2, \dots, k_n sunt numere naturale și avem $k_1 + 2k_2 + \dots + nk_n = n$. Sistemul ordonat (k_1, k_2, \dots, k_n) se numește atunci tipul de descompunere a lui σ . Evident orice sistem ordonat de numere naturale (k_1, k_2, \dots, k_n) astfel încît $k_1 + 2k_2 + \dots + nk_n = n$, este tipul de descompunere al unei permutări $\sigma \in S_n$.

De exemplu, pentru permutarea

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 1 & 5 & 6 & 4 & 8 & 7 \end{pmatrix} \in S_8$$

avem descompunerea

$$\sigma = (2) (1, 3) (7, 8) (4, 5, 6) = (1, 3) (7, 8) (4, 5, 6)$$

(se negligează, ca de obicei, ciclurile de lungime 1 din descompunere), deci, tipul de descompunere al lui σ este $(1, 2, 1, 0, 0, 0, 0, 0)$.

Signatura unei permutări. Grupul altern A_n . Fie n un număr natural și considerăm o permutare $\sigma \in S_n$. O pereche ordonată (i, j) cu $1 \leq i < j \leq n$ și $\sigma(i) > \sigma(j)$ se numește inversiune a lui σ . Notăm cu $\text{Inv}(\sigma)$ numărul de inversiuni ale permutării σ . Permutarea σ se numește permutare pară dacă $\text{Inv}(\sigma)$ este un număr par și impară dacă $\text{Inv}(\sigma)$ este un număr impar.

Numărul

$$\text{sgn}(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$$

se numește signatura permutării σ . Putem scrie acest număr sub forma

$$\text{sgn}(\sigma) = \frac{\prod_{1 \leq i < j \leq n} (\sigma(j) - \sigma(i))}{\prod_{1 \leq i < j \leq n} (j - i)} = \frac{\prod_{1 \leq i < j \leq n} \epsilon(i, j) (j - i)}{\prod_{1 \leq i < j \leq n} (j - i)}$$

unde

$\epsilon(i, j) = \begin{cases} -1 & \text{dacă } (i, j) \text{ este o inversiune a lui } \sigma, \\ 1 & \text{dacă } (i, j) \text{ nu este o inversiune a lui } \sigma, \end{cases}$
 și găsim $\operatorname{sgn}(\sigma) = \prod_{1 \leq i < j \leq n} \sum_{(i, j)} (-1)^{\operatorname{Inv}(\sigma)}$. Prin urmare
 $\operatorname{sgn}(\sigma) = \begin{cases} 1 & \text{dacă } \sigma \text{ este permutare pară,} \\ -1 & \text{dacă } \sigma \text{ este permutare impară.} \end{cases}$

Propoziția 5.21. Pentru orice două permutări $\sigma, \tau \in S_n$ avem $\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma) \operatorname{sgn}(\tau)$.

Demonstrație. Avem

$$\begin{aligned} \operatorname{sgn}(\sigma\tau) &= \prod_{1 \leq i < j \leq n} \frac{(\sigma\tau)(j) - (\sigma\tau)(i)}{j - i} = \\ &= \prod_{1 \leq i < j \leq n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} \cdot \prod_{1 \leq i < j \leq n} \frac{\tau(j) - \tau(i)}{j - i}. \end{aligned}$$

Deoarece,

$$\frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} = \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i) - \tau(j)},$$

evident avem

$$\prod_{1 \leq i < j \leq n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i} = \operatorname{sgn}(\tau).$$

Rezultă $\operatorname{sgn}(\sigma\tau) = \operatorname{sgn}(\sigma) \operatorname{sgn}(\tau)$.

Definiția 5.22. Propoziția precedentă arată că aplicația $\operatorname{sgn}: S_n \rightarrow \mathbb{C}_2 = \{-1, 1\}$, este un morfism de grupuri. Nucleul acestui morfism de grupuri se notează cu A_n și se numește *grupul altern pe n elemente*. Explicit avem:

$$A_n = \operatorname{Ker}(\operatorname{sgn}) = \{\sigma \in S_n \mid \sigma \text{ este permutare pară}\}.$$

Dacă $n = 1$, avem $A_1 = S_1 = 1$. Dacă $n \geq 2$, morfismul $\operatorname{sgn}: S_n \rightarrow \mathbb{C}_2$ este surjectiv. Într-adevăr, $1 = \operatorname{sgn}(1)$ și, deoarece $n \geq 2$, putem considera cicluri de lungime 2, (i, j) , $i \neq j$. Ciclurile de lungime 2 se numesc transpoziții și, vom demonstra mai jos, că orice transpoziție este o permutare impară. În particular, vom avea $-1 = \operatorname{sgn}((i, j))$, ceea ce arată că intr-adevăr sgn este un morfism surjectiv. Aplicind teorema fundamentală de izomorfism, avem că A_n este subgrup normal al lui S_n și

$$S_n/A_n \cong \mathbb{C}_2.$$

Aplicind teorema lui Lagrange, rezultă că

$$n! = |S_n| = |A_n| \cdot |S_n/A_n| = 2 \cdot |A_n|,$$

deci $|A_n| = \frac{n!}{2}$ (pentru $n \geq 2$).

Propoziția 5.23. Orice transpoziție (i, j) , $i, j \in \{1, 2, \dots, n\}$, $i \neq j$ este o permutare impară.

Demonstrație. Deoarece $\sigma = (i, j) = (j, i)$, putem presupune $i < j$. Vom considera toate perechile ordonate (k, l) cu $k, l \in \{1, 2, \dots, n\}$, $k < l$. Dacă $k, l \notin \{i, j\}$, avem $\sigma(k) = k$, $\sigma(l) = l$ și (k, l) nu este inversiune a lui σ ; dacă $l = i$, avem $\sigma(k) = k < l = i < j = \sigma(l)$; deci nici în acest caz perechea (k, l) nu este inversiune; dacă $k < i < j = l$, avem $\sigma(k) = k < i = \sigma(l)$ și perechea (k, l) este inversiune; dacă $i < k < l = j$, avem $\sigma(l) = l < k = \sigma(k)$ și perechea (k, l) este inversiune, numărul inversiunilor de acest tip fiind $j - i - 1$; dacă $i = k < 1 = j$ avem $\sigma(l) = i < j = \sigma(k)$ și perechea (i, j) este inversiune; dacă $i = k < l < j$ avem $\sigma(l) = l < j = \sigma(k)$ și perechea (k, l) este inversiune, numărul inversiunilor de acest tip fiind $j - i - 1$; dacă $i = k < j < l$ avem $\sigma(k) = j < l = \sigma(l)$ și perechea (k, l) nu este inversiune. Rezultă că numărul total de inversiuni ale permutării $\sigma = (i, j)$ este $2(j - i) + 1$, deci σ este o permutare impară.

Observație. Pentru orice ciclu $(i_1, i_2, \dots, i_m) \in S_n$ avem evident

$$(i_1, i_2, \dots, i_m) = (i_1, i_2) (i_2, i_3) \dots (i_{m-1}, i_m)$$

de unde rezultă, folosind propozițiile 5.21 și 5.23, că

$$\text{sgn}(i_1, i_2, \dots, i_m) = (-1)^{m-1}.$$

În particular, dacă permutarea $\sigma \in S_n$ are tipul de descompunere

$$\sum_{k=1}^n (k-1)k_1 = (-1)^{k_1+2k_2+\dots+(n-1)k_n}.$$

Rezultă de asemenea că, orice permutare $\sigma \in S_n$ este un produs de transpoziții și anume σ este o permutare pară dacă și numai dacă este produsul unui număr par de transpoziții.

Aceiuni prin conjugare. Fie G un grup. Definim acțiunea α a grupului G pe mulțimea G a elementelor lui G prin $\alpha(g, x) = gxg^{-1}$, $g, x \in G$. Condițiile din definiția unei acțiuni se verifică astfel:

$$\begin{aligned} \alpha(gg', x) &= (gg')x(gg')^{-1} = g(g'xg'^{-1})g^{-1} = \\ &= \alpha(g, \alpha(g'x)), \quad \alpha(1, x) = 1x1^{-1} = x. \end{aligned}$$

Acțiunea α se numește acțiunea lui G pe el însuși prin conjugare și se folosește de obicei, pentru această acțiune, o notație exponențială:

$$(g)_x = \alpha(g, x) = gxg^{-1}.$$

Nucleul acțiunii prin conjugare α este:

$\text{Ker } \alpha = \{g \in G \mid {}^g x = x \text{ pentru orice } x \in G\} = \{g \in G \mid gxg^{-1} = x \text{ pentru orice } x \in G\} = \{g \in G \mid gx = xg \text{ pentru orice } x \in G\} = Z(G)$, centrul grupului G .

Pentru fiecare $x \in G$, stabilizatorul lui x în G relativ la acțiunea prin conjugare se numește centralizatorul lui x în G și se notează $C_G(x)$. Avem

$$C_G(x) = \{g \in G \mid {}^g x = x\} = \{g \in G \mid gx = xg\}$$

și

$$Z(G) = \bigcap_{x \in G} C_G(x).$$

Relația de echivalență \sim , introdusă în 5.7 pentru o acțiune oarecare a grupului G , devine, în cazul acțiunii prin conjugare, o relație de echivalență între elementele lui G , care se numește relația de conjugare pe G :

$$x \sim y \Leftrightarrow \exists g \in G: {}^g x = y \Leftrightarrow \exists g \in G: gxg^{-1} = y.$$

Orbita unui element $x \in G$ relativ la acțiunea prin conjugare:

$${}^a x = \{{}^a x \mid g \in G\} = \{gxg^{-1} \mid g \in G\}$$

se numește și clasa de conjugare a lui x . Conform lui 5.8 avem:

$$|{}^a x| = |G:C_G(x)|$$

iar ecuația claselor pentru acțiunea prin conjugare devine:

$$|G| = |Z(G)| + \sum_{\alpha_x \text{ netrivială}} |G:C_G(x)|$$

Relația de mai sus se numește și ecuația claselor pentru grupul G .

Propoziția 5.24. Fie G un grup finit și presupunem că $|G| = p^n$, unde p este un număr prim și m un număr întreg pozitiv. Atunci centrul $Z(G)$ al lui G este netrivial.

Demonstrație. Pentru orice element $x \in G$, $|G:C_G(x)|$ este un divizor al lui $|G| = p^n$ și dacă $|G:C_G(x)| \neq 1$, rezultă $|G:C_G(x)| = p^k$ pentru un număr întreg pozitiv k .

Ecuația claselor pentru grupul G devine atunci

$$p^n = |G| = |Z(G)| + p^{k_1} + \dots + p^{k_n}$$

unde n este numărul claselor de conjugare netriviale, iar k_1, k_2, \dots, k_n sunt numere întregi pozitive. Deoarece $p \mid (p^{k_1} + p^{k_2} + \dots + p^{k_n})$, ecuația de mai sus arată că $p \mid |Z(G)|$ deci $Z(G) \neq 1$.

Corolarul 5.25. Fie p un număr prim. Atunci orice grup G de ordin p^2 este abelian.

Demonstrație. Conform propoziției precedente avem $Z(G) \neq 1$ și deoarece $|Z(G)| \mid |G| = p^2$, rezultă $|Z(G)| = p$ sau $|Z(G)| = p^2$. Nu putem avea însă $|Z(G)| = p$, deoarece în acest caz $|G/Z(G)| = \frac{p^2}{p} = p$, deci grupul factor $G/Z(G)$ este ciclic (aceasta rezultă de exemplu din faptul că orice grup de ordin prim p este, conform teoremei lui Lagrange, grup simplu); aplicăm apoi propoziția 3.12 și rezultă G abelian, deci $Z(G) = G$, ceea ce nu se poate. Prin urmare singura posibilitate este $|Z(G)| = p^2 = |G|$, de unde rezultă $Z(G) = G$, deci G abelian.

Propoziția 5.26. (Teorema lui Cauchy.) *Fie G un grup finit și p un număr prim astfel ca $p \nmid |G|$. Atunci există un element $x \in G$ cu $o(x) = p$.*

Demonstrație. Vom face demonstrația prin inducție după ordinul $|G|$ al lui G . Presupunem întâi că G este abelian. Dacă G este simplu, atunci G este grup ciclic de ordin prim și pentru un generator x al lui G avem $o(x) = p$. Dacă G nu este simplu, atunci există un subgrup propriu și netrivial H al lui G și deoarece $|G| = |H||G/H|$ avem $p \nmid |H|$ sau $p \nmid |G/H|$. Dacă $p \nmid |H|$, atunci, conform ipotezei de inducție, există un element $x \in H$ cu $o(x) = p$. Dacă $p \nmid |G/H|$, atunci $p \nmid |G/H|$ și notând $m = |H|$ avem $(p, m) = 1$, deci există numere întregi k și n astfel încât $pk + mn = 1$. Pe de altă parte, conform ipotezei de inducție, există un element $x \in G$ astfel ca $o(xH) = p(xH)$ ca element în grupul factor G/H , deci $(xH)^p = H$ și $x^p \in H$. Luăm $y = x^{mn}$ și deoarece $p \nmid mn$ avem $x^{mn} \notin H$, deci $y \neq 1$. Pe de altă parte, deoarece $x^p \in H$ și $m = |H|$ avem $(x^p)^m = 1$, deci $y^p = 1$. Astfel $o(y) = p$. Acum presupunem G neabelian și considerăm ecuația claselor pentru grupul G :

$$|G| = |Z(G)| + \sum_{i=1}^r |G : C_G(x_i)|$$

unde x_1, x_2, \dots, x_r sunt elemente din G necentrale. Dacă $p \nmid |Z(G)|$ atunci, deoarece $Z(G)$ este abelian, există un element $x \in Z(G)$ cu $o(x) = p$. Dacă $p \nmid |Z(G)|$, atunci există un $i \in \{1, 2, \dots, r\}$ astfel ca $p \nmid |G : C_G(x_i)|$. Deoarece $p \nmid |G| = |C_G(x_i)| / |G : C_G(x_i)|$, rezultă $p \nmid |C_G(x_i)| < |G|$ și, conform ipotezei de inducție, există un element $x \in C_G(x_i)$ cu $o(x) = p$.

Definiția 5.27. Fie G un grup $g \in G$ și U o submulțime a lui G . Definim

$${}^g U = g U g^{-1} = \{gxg^{-1} \mid x \in U\}.$$

Atunci aplicația

$$\alpha : G \times P(G) \rightarrow P(G)$$

(unde $P(G)$ este mulțimea tuturor submulțimilor lui G , definită prin

$$\alpha(g, U) = {}^gU$$

este o acțiune. Condițiile din definiția unei acțiuni:

$${}^0({}^gU) = {}^{gg}U \text{ și } {}^1U = U,$$

se verifică în mod evident. Acțiunea α se numește acțiunea lui G pe mulțimea submulțimilor lui G prin conjugare.

Pentru fiecare submulțime U a lui G , stabilizatorul lui U relativ la această acțiune se numește normalizatorul lui U în G și se notează $N_G(U)$. Avem

$$\begin{aligned} N_G(U) &= \{g \in G \mid {}^gU = U\} = \{g \in G \mid gUg^{-1} = U\} = \\ &= \{g \in G \mid gU = Ug\}. \end{aligned}$$

În cazul unui subgrup H al lui G avem $H \leq N_G(H)$ și pentru orice subgrup K al lui G , $H \trianglelefteq K \Leftrightarrow N_G(H) \leq K$, sau altfel spus, $N_G(H)$ este cel mai mic subgrup al lui G care conține pe H ca subgrup normal.

Pentru fiecare submulțime U a lui G orbita lui U relativ la acțiunea prin conjugare ${}^gU = \{{}^gU \mid g \in G\}$ se numește și clasa de conjugare a lui U , iar două submulțimi U și U' care au aceeași clasă de conjugare se numesc conjugate. Conform lui 5.8 avem

$${}^gU = |G:N_G(U)|.$$

Pentru o submulțime U a lui G în afara normalizatorului $N_G(U)$, putem considera un alt subgrup important anume

$$C_G(U) = \bigcap_{x \in U} C_G(x) = \{g \in G \mid gx = xg \text{ pentru orice } x \in U\}$$

Evident avem $C_G(U) \leq N_G(U)$. Remarcăm faptul că pentru un subgrup H al lui G avem:

$$N_G(H) = G \Leftrightarrow H \trianglelefteq G \quad (H \text{ este subgrup normal});$$

$$C_G(H) = G \Leftrightarrow H \leq Z(G) \quad (H \text{ este subgrup central}).$$

Propoziția 5.28. Fie G un grup finit și H un subgrup al lui G . Atunci

$$|\bigcup_{g \in G} {}^gH| \leq 1 + |G| - |G:H|$$

și $\bigcup_{g \in G} {}^gH = G$ dacă și numai dacă $H = G$

Demonstrație. Numărul de termeni distincți ai reuniunii $\bigcup_{g \in G} {}^gH$ este $r = |{}^gH| = |G:N_G(H)|$. Pentru fiecare $g \in G$, notăm ${}^gH^* = {}^gH - \{1\}$ și avem

$$|\sigma H| = |gHg^{-1}| = |H|, \quad |\sigma H^*| = |H| - 1, \\ |\bigcup_{g \in G} \sigma H| = 1 + |\bigcup_{g \in G} \sigma H^*| \leq 1 + r(|H| - 1).$$

Pe de altă parte, avem $H \leq N_G(H)$, deci

$$r = |G : N_G(H)| \leq |G : H| \quad \text{și} \quad |G : H| |H| = |G|.$$

Prin urmare

$$|\bigcup_{g \in G} \sigma H| \leq 1 + r(|H| - 1) \leq 1 + |G : H| (|H| - 1) \leq 1 + |G| - |G : H|.$$

Dacă $\bigcup_{g \in G} \sigma H = G$ din inegalitatea de mai sus rezultă

$$|G| \leq 1 + |G| - |G : H|$$

deci $|G : H| \leq 1$, ceea ce implică $|G : H| = 1$, $G = H$.

Clasele de conjugare ale grupurilor S_n și A_n .

Propoziția 5.29. *Două permutări $\sigma, \sigma' \in S_n$ sunt conjugate dacă și numai dacă au același tip de descompunere.*

Demonstrație. Presupunem că permutările σ și σ' au același tip de descompunere. Atunci considerind descompunerile lui σ și σ' ca produse de cicluri disjuncte, putem scrie:

$$(1) \quad \sigma = (a_{11}, \dots, a_{1n_1})(a_{21}, \dots, a_{2n_2}) \dots (a_{s1}, \dots, a_{sn_s})$$

$$(2) \quad \sigma' = (b_{11}, \dots, b_{1n_1})(b_{21}, \dots, b_{2n_2}) \dots (b_{s1}, \dots, b_{sn_s})$$

unde n_1, n_2, \dots, n_s sunt numere întregi pozitive și $n_1 + n_2 + \dots + n_s = n$. Dacă luăm permutarea

$$(3) \quad \theta = \begin{pmatrix} a_{11} \dots a_{1n_1} & a_{21} \dots a_{2n_2} & \dots & a_{s1} \dots a_{sn_s} \\ b_{11} \dots b_{1n_1} & b_{21} \dots b_{2n_2} & \dots & b_{s1} \dots b_{sn_s} \end{pmatrix}$$

se verifică prin calcul direct că $\theta\sigma\theta^{-1} = \sigma'$, deci rezultă că σ și σ' sunt conjugate. Reciproc, să presupunem că σ și σ' sunt conjugate, deci că există o permuatare $\theta \in S_n$ astfel ca $\theta\sigma\theta^{-1} = \sigma'$. Să zicem că descompunerea în cicluri disjuncte a lui σ este (1), unde n_1, n_2, \dots, n_s sunt numere întregi pozitive și $n_1 + n_2 + \dots + n_s = n$. Atunci permuatarea θ se poate pune sub forma (3). Atunci

$$\sigma'(b_{ij}) = (\theta\sigma\theta^{-1})(b_{ij}) = (\theta\sigma)(a_{i,j+1}) = \theta(a_{i,j+1}) = b_{i,j+1}$$

pentru $1 \leq i \leq s$ și $1 \leq j < n_i$ și analog

$$\sigma'(b_{in_i}) = \theta(a_{i1}) = b_{i1}.$$

Aceasta demonstrează că descompunerea în cicluri disjuncte a lui σ' este exact (2) și deci, că σ și σ' au același tip de descompunere.

Partițiile unui număr natural. Numărul claselor de conjugare ale grupului simetric S_n . Propoziția predecentă arată că numărul claselor de conjugare ale grupului simetric S_n este egal cu numărul tipurilor de descompunere posibile ale permutărilor din S_n adică egal cu numărul soluțiilor (k_1, k_2, \dots, k_n) în numere naturale ale ecuației

$$(1) \quad k_1 + 2k_2 + \dots + nk_n = n.$$

La fiecare soluție (k_1, k_2, \dots, k_n) în numere naturale, asociem sistemul ordonat (m_1, m_2, \dots, m_n) definit prin

$$m_1 = k_n$$

$$m_2 = k_n + k_{n-1}$$

.....

$$m_n = k_n + \dots + k_2 + k_1.$$

Atunci m_1, m_2, \dots, m_n sunt numere naturale și avem $m_1 \leq m_2 \leq \dots \leq m_n$ și $m_1 + m_2 + \dots + m_n = n$.

Un sistem ordonat de numere naturale (m_1, m_2, \dots, m_n) astfel ca $m_1 \leq m_2 \leq \dots \leq m_n$, și $m_1 + m_2 + \dots + m_n = n$ se numește partiție a lui n . Am asociat astfel ca fiecare soluție în numere naturale a ecuației (1) o partiție a lui n . Reciproc, dacă (m_1, m_2, \dots, m_n) este o partiție a lui n , atunci (k_1, k_2, \dots, k_n) , unde

$$k_1 = m_n - m_{n-1}$$

$$k_2 = m_{n-1} - m_{n-2}$$

.....

$$k_{n-1} = m_2 - m_1$$

$$k_n = m_1$$

este o soluție în numere naturale a ecuației (1). Deducem astfel că numărul soluțiilor în numere naturale ale ecuației (1), deci și numărul claselor de conjugare ale grupului simetric S_n , este egal cu numărul partițiilor lui n .

De regulă în scrierea unei partiții (m_1, m_2, \dots, m_n) se omit evenualele m -uri care sunt egale cu 0. Numărul partițiilor lui n îl notăm cu $\pi(n)$. Avem

$$\pi(1) = 1; \pi(2) = 2;$$

$$\pi(3) = 3, \text{ partițiile lui } 3 \text{ fiind } (3), (1, 2), (1, 1, 1);$$

$$\pi(4) = 5, \text{ partițiile lui } 4 \text{ fiind } (4), (2, 2), (1, 3), \\ (1, 1, 2), (1, 1, 1, 1);$$

$$\pi(5) = 7, \text{ partițiile lui } 5 \text{ fiind } (5), (2, 3), (1, 4), (1, 2, 2), (1, 1, 3), \\ (1, 1, 1, 2), (1, 1, 1, 1, 1);$$

$$\pi(6) = 11, \text{ partițiile lui } 6 \text{ fiind } (6), (3, 3), (2, 4), (2, 2, 2), (1, 5), (1, 2, 3), \\ (1, 1, 4), (1, 1, 2, 2), (1, 1, 1, 3), (1, 1, 1, 1, 2), (1, 1, 1, 1, 1).$$

Exemple. Formula pentru numărul elementelor unei clase de conjugare. Vom determina clasele de conjugare ale grupurilor S_3 și S_4 astfel:

Corespunzător partițiilor (3), (1, 2), (1, 1, 1) ale lui 3 avem, pentru permutările lui S_3 , următoarele tipuri de descompunere: (3, 0, 0), (1, 1, 0), (0, 0, 1), astfel că S_3 are exact trei clase de conjugare:

C_1 formată din permutarea identică: $C_1 = \{1\}$;

C_2 formată din toate transpozițiile: $C_2 = \{(12), (13), (23)\}$;

C_3 formată din toate ciclurile de lungime 3:

$C_3 = \{(123), (132)\}$.

Corespunzător partițiilor (4), (2, 2), (1, 3), (1, 1, 2), (1, 1, 1, 1) ale lui 4, avem pentru permutările lui S_4 următoarele tipuri de descompunere: (4, 0, 0, 0), (0, 2, 0, 0), (2, 1, 0, 0), (1, 0, 1, 0), (0, 0, 0, 1), astfel că S_4 are următoarele clase de conjugare:

C_1 formată din permutarea identică: $C_1 = \{1\}$;

C_2 formată din toate produsele de două transpoziții disjuncte:

$C_2 = \{(12)(34), (13)(24), (14)(23)\}$;

C_3 formată din toate transpozițiile: $C_3 = \{(12), (13), (14), (23), (24), (34)\}$;

C_4 formată din ciclurile de lungime 3: $C_4 = \{(123), (132), (124), (142), (134), (143), (234), (243)\}$;

C_5 formată din ciclurile de lungime 4: $C_5 = \{(1234), (1243), (1324), (1342), (1423), (1432)\}$.

Se observă că pentru a forma o permutare care are tipul de descompunere (k_1, k_2, \dots, k_n) trebuie să luăm k_1 dintre numerele $\{1, 2, \dots, n\}$ cu care să formăm k_1 cicluri de lungime 1, $2 k_2$ dintre numerele rămasă cu care să formăm k_2 cicluri de lungime 2 etc. Însă cele k_i cicluri de lungime i pot fi schimbată între ele fără ca prin aceasta permutarea să se schimbe. De asemenea același ciclu de lungime i poate fi scris în i moduri diferite în funcție de litera cu care începem scrierea sa; de exemplu

$$(1 \ 2 \ 3 \ 4) = (2 \ 3 \ 4 \ 1) = (3 \ 4 \ 1 \ 2) = (4 \ 1 \ 2 \ 3)$$

În concluzie numărul permutărilor care au tipul (k_1, k_2, \dots, k_n) este

$$\frac{n!}{k_1! k_2! \dots k_n!}$$

Corespunzător partițiilor (5), (2, 3), (1, 4), (1, 2, 2), (1, 1, 3), (1, 1, 1, 2), (1, 1, 1, 1, 1) ale lui 5 avem, pentru permutările lui S_5 , următoarele tipuri de descompunere: (5, 0, 0, 0, 0), (1, 2, 0, 0, 0), (3, 1, 0, 0, 0), (0, 1, 1, 0, 0), (2, 0, 1, 0, 0), (1, 0, 0, 1, 0), (0, 0, 0, 0, 1), cărora le corespund clase de conjugare:

C_1 — formată numai din permutarea identică: $|C_1| = 1$;

C_2 — formată din toate produsele de două transpoziții disjuncte: $|C_2| = \frac{5!}{2! 2^2} = 15$;

C_3 — formată din toate transpozițiile: $|C_3| = \frac{5!}{3! 2} = 10$;

C_4 — formată din produsele de două cicluri disjuncte, unul de lungime 2 și unul de lungime 3: $|C_4| = \frac{5!}{2 \cdot 3} = 20$;

C_5 — formată din toate ciclurile de lungime 3: $|C_5| = \frac{5!}{2! \cdot 3} = 20$;

C_6 — formată din toate ciclurile de lungime 4: $|C_6| = \frac{5!}{4} = 30$;

C_7 — formată din toate ciclurile de lungime 5: $|C_7| = \frac{5!}{5} = 24$.

Rezultă că ecuația claselor pentru grupul simetric S_5 este:

$$120 = 1 + 15 + 10 + 20 + 20 + 30 + 24.$$

Propoziția 5.31. Fie C o clasă de conjugare a grupului simetric S_n , corespunzătoare tipului de descompunere (k_1, k_2, \dots, k_n) .

a) Avem $C \subset A_n$ sau $C \subset S_n - A_n$ după cum $\sum_{i=1}^n (i-1)k_i$ este un număr par sau impar.

b) Presupunem că $C \subset A_n$. Atunci C nu este o clasă de conjugare a grupului altern A_n dacă și numai dacă $k_i \leq 1$ pentru orice $i \in \{1, 2, \dots, n\}$ și $k_i = 0$ pentru orice i par, $i \in \{1, 2, \dots, n\}$ în care caz $C = C_1 \cup C_2$, unde

C_1 și C_2 sunt clase de conjugare ale lui A_n , având $|C_1| = |C_2| = \frac{1}{2} |C|$.

Demonstrație. a) Este evident deoarece signatura unei permutări $\sigma \in S_n$ nu depinde decât de tipul său de descompunere și anume, o permutare $\sigma \in C$ este pară dacă și numai dacă $\sum_{i=1}^n (i-1)k_i$ este număr par.

b) Fie $\sigma \in C$ și fie $H = C_{S_n}(\sigma)$. Evident avem $A_n \cap H = C_{A_n}(\sigma)$. Fie $C_1 = {}^{A_n}\sigma$, clasa de conjugare a lui σ în A_n . Avem

$$\begin{aligned} |C_1| &= |A_n : A_n \cap H| = \frac{|S_n : A_n \cap H|}{|S_n : A_n|} = \frac{|S_n : H| |H : A_n \cap H|}{2} = \\ &= \frac{|C| |H : A_n \cap H|}{2}. \end{aligned}$$

Deoarece $A_n \leq H A_n \leq S_n$ și $|S_n : A_n| = 2$, avem $H A_n = A_n$ sau $H A_n = S_n$ și deoarece $H/A_n \cap H \cong H A_n / A_n$ rezultă $|H : A_n \cap H| = |H A_n : A_n| = 1$ sau 2, după cum $H \leq A_n$ sau $H \not\leq A_n$.

În cazul cînd $H \leq A_n$, rezultă $|C_1| = \frac{|C|}{2}$. Alegînd o permutare $\tau \in C - C_1$ și notînd clasa sa de conjugare în A_n cu C_2 rezultă analog $|C_2| = \frac{|C|}{2}$. Clasele C_1 și C_2 fiind disjuncte avem $|C_1 \cup C_2| = |C_1| + |C_2| = |C|$, deci $C_1 \cup C_2 = C$. În cazul cînd $H \neq A_n$ avem $|C_1| = |C|$, deci $C = C_1$.

Rămîne să arătăm că $H \leq A_n$ dacă și numai dacă $k_i \leq 1$ pentru orice $i \in \{1, 2, \dots, n\}$ și $k_i = 0$ pentru orice i par, $i \in \{1, 2, \dots, n\}$ sau, echivalent, în descompunerea în cicluri disjuncte a lui $\sigma : \sigma = 0_1 0_2 \dots 0_p$, apar numai cicluri 0_i de lungime impară și nu există două dintre ciclurile $0_1, 0_2, \dots, 0_p$ care să aibă aceeași lungime.

Presupunem mai întii că în descompunerea în cicluri disjuncte a lui σ apar numai cicluri de lungime impară l_i , $i \in \{1, 2, \dots, p\}$ și ori- care două din aceste cicluri au lungimi distințe. Atunci $|S_n : H| = \frac{n!}{l_1 l_2 \dots l_p}$, deci $|H| = l_1 l_2 \dots l_p$ ceea ce arată că $|H|$ este impar. Dar atunci nu putem avea $H \not\leq A_n$ deoarece în acest caz $|H : A_n \cap H| = 2$, deci $|H| = 2 |A_n \cap H|$ este număr par. Prin urmare $H \leq A_n$.

Reciproc, să presupunem că $H \leq A_n$. Presupunem că descompunerea în cicluri disjuncte a lui σ este $\sigma = 0_1 0_2 \dots 0_p$, fiecare ciclu 0_i avind lungimea l_i . Cum orice două cicluri disjuncte permutează între ele, avem $0_i \sigma = \sigma 0_i$; deci $0_i \in H \leq A_n$ pentru orice $i \in \{1, 2, \dots, p\}$. Deoarece $\text{sgn}(0_i) = (-1)^{l_i} - 1$, rezultă că l_i este impar pentru toți $i \in \{1, 2, \dots, p\}$. Rămîne să arătăm că l_1, l_2, \dots, l_p sunt distințe două cîte două. Presupunem, prin absurd, că avem, de exemplu, $l_1 = l_2 = 2m + 1$. Putem presupune evident că

$$0_1 = (1, 2, \dots, 2m+1), \quad 0_2 = (2m+2, \dots, 4m+2)$$

și fie $0 = (1, 2m+2)(2, 2m+3)\dots(2m+1, 4m+2)$. Atunci $0 \cdot 0_1 = 0 \cdot 0_2 \theta^{-1} = \theta_2$ și $0 \cdot 0_2 = 0 \cdot 0_1 \theta^{-1} = \theta_1$. În plus 0 comută cu ciclurile $0_3, \dots, 0_p$ ceea ce arată că $0 \sigma = \sigma 0$ și deci $0 \in H \leq A_n$. Dar $\text{sgn}(0) = (-1)^{2m+1} = -1$, și nu putem avea $0 \in A_n$. Contradicția obținută arată că l_1, l_2, \dots, l_p sunt distințe două cîte două.

Grupul altern A_4 . Avem $|A_4| = 12$ și dintre clasele de conjugare ale lui S_4 sunt incluse în A_4 numai:

- clasa de conjugare corespunzătoare tipului $(4, 0, 0, 0)$: $C_1 = \{1\}$;
- clasa de conjugare corespunzătoare tipului $(0, 2, 0, 0)$: $C_2 = \{(1\ 2)(3\ 4), (13)(24), (14)(23)\}$;

— clasa de conjugare corespunzătoare tipului $(1, 0, 1, 0)$: $C_4 = \{(123), (132), (124), (142), (134), (143), (234), (243)\}$.

Conform propoziției precedente, C_1 și C_2 sunt clase de conjugare în A_4 în timp ce C_4 este reuniunea disjunctă a două clase de conjugare în A_4 : $C_4 = C'_4 \cup C''_4$ cu $|C'_4| = |C''_4| = \frac{|C_4|}{2} = 4$. Rezultă că ecuația claselor pentru grupul altern A_4 este

$$12 = 1 + 3 + 4 + 4.$$

Vom determina acum toate subgrupurile normale ale lui A_4 . Pentru aceasta observăm că, în general, un subgrup H al unui grup G este normal dacă și numai dacă pentru orice $\sigma \in H$ avem $\sigma\tau \in H$ astfel că un subgrup H este normal dacă și numai dacă este o reuniune de clase de conjugare. În plus, un subgrup H conține obligatoriu clasa de conjugare a elementului unitate $C_1 = \{1\}$, iar ordinul $|H|$ divide $|G|$.

Ecuația claselor pentru grupul A_4 arată că toate reuniunile de clase de conjugare care conțin elementul unitate au cardinalele:

$$1, 1+3, 1+4, 1+3+4, 1+3+4+4$$

și singura reuniune de acest fel care poate fi un subgrup propriu și netrivial H este cea care are $1+3=4$ elemente, respectiv $H = C_1 \cup C_2$. Făcind tablă de înmulțire a elementelor din $H = C_1 \cup C_2 = \{1, (12)(34), (13)(24), (14)(23)\}$ se constată că H este un subgrup al lui A_4 . În concluzie H este unicul subgrup normal propriu și netrivial al lui A_4 . De obicei acest subgrup se notează cu B_4 .

În particular rezultă că A_4 nu are subgrupuri de ordinul 6. Într-adevăr, un subgrup de ordinul 6 al lui A_4 ar avea indicele 2 deci ar fi normal, or singurul subgrup normal propriu și netrivial al lui A_4 are ordinul 4. Astfel, reciprocă teoremei lui Lagrange: dacă G este un grup finit și d este un divizor al ordinului lui G , atunci există un subgrup H al lui G de ordin d nu este în general adevărată. Pe de altă parte, există evident și grupuri G care satisfac reciprocă teoremei lui Lagrange.

Grupul altern A_5 . Avem $|A_5| = 60$ și dintre clasele de conjugare ale lui S_5 sunt incluse în A_5 numai:

clasa de conjugare corespunzătoare tipului $(5, 0, 0, 0, 0)$: C_1 cu $|C_1| = 1$;

clasa de conjugare corespunzătoare tipului $(1, 2, 0, 0, 0)$: C_2 cu $|C_2| = 15$;

clasa de conjugare corespunzătoare tipului $(2, 0, 1, 0, 0)$: C_5 cu $|C_5| = 20$;

clasa de conjugare corespunzătoare tipului $(0, 0, 0, 0, 1)$: C_7 cu $|C_7| = 24$.

Conform propoziției 5.31, C_1 , C_2 și C_5 sunt clase de conjugare în A_5 în timp ce C_7 este reuniunea a două clase de conjugare ale lui A_5 : $C_7 = C'_7 \cup C''_7$ cu $|C'_7| = |C''_7| = \frac{|C_7|}{2} = 12$. Prin urmare ecuația claselor pentru grupul altern A_5 este

$$60 = 1 + 15 + 20 + 12 + 12.$$

Reuniunile de clase de conjugare ale lui A_5 care conțin elementul unitate au deci cardinalele:

$$\begin{aligned} 1, 1+15=16, 1+20=21, 1+12=13; \\ 1+15+20=36, 1+15+12=28; 1+20+12=33; \\ 1+12+12=25; \\ 1+15+20+12=48, 1+15+12+12=40, 1+20+12+ \\ +12=55, 1+15+20+12+12=60. \end{aligned}$$

Deoarece, în afară de primul și ultimul dintre aceste numere, nici unul nu divide pe $60 = |A_5|$, rezultă că A_5 nu are nici un subgrup normal propriu și netrivial. Prin urmare A_5 este un grup simplu.

Propoziția 5.32. *Grupul altern A_n este grup simplu pentru orice $n \geq 5$.*

Demonstrație. Vom face demonstrația prin inducție după n . Pentru $n=5$ afirmația este adevărată în virtutea celor de mai sus. Presupunem $n > 5$ și că A_{n-1} este grup simplu. Considerăm acțiunea canonică a lui A_n pe multimea $\{1, 2, \dots, n\}$ și pentru orice $i \in \{1, 2, \dots, n\}$, fie $H_i := \text{Stab}_{A_n}(i)$. Dacă $i, j \in \{1, 2, \dots, n\}$, $i \neq j$, putem alege o permutare $\sigma \in A_n$ (de exemplu un ciclu de lungime 3 de forma $\sigma = (i, j, k)$), astfel încât $\sigma(i) = j$. Atunci avem $\sigma H_i \sigma^{-1} = H_j$. În particular, vom avea $H_i \cong H_n$ pentru orice $i \in \{1, 2, \dots, n\}$ și evident avem $H_n \cong A_{n-1}$ astfel că, pentru orice $i \in \{1, 2, \dots, n\}$, H_i este grup simplu. Vom presupune prin reducere la absurd că A_n are un subgrup normal K propriu și netrivial. Atunci, pentru orice $i \in \{1, 2, \dots, n\}$, avem $K \cap H_i \trianglelefteq H_i$, deci $K \cap H_i = 1$ sau $K \cap H_i = H_i$. Presupunem că există un $j \in \{1, 2, \dots, n\}$ astfel încât $K \cap H_j = H_j$, adică $H_j \trianglelefteq K$. După cum am văzut, pentru orice $i \in \{1, 2, \dots, n\}$, există o permutare $\sigma \in A_n$ cu $H_i = \sigma H_j \sigma^{-1}$, și rezultă $H_i = \sigma H_j \sigma^{-1} \trianglelefteq \sigma K \sigma^{-1} = K$. Acum fie $\sigma \in A_n$. Dacă $\sigma(1) = 1$, atunci $\sigma \in H_1 \trianglelefteq K$. Presupunem că $\sigma(1) = j \neq 1$ și alegem un $i \in \{1, 2, \dots, n\}$ cu $1 \neq i \neq j$. Avem $(j1i) \in A_n$, $((j1i)\sigma)(1) = 1$, deci $(j1i)\sigma \in H_1 \trianglelefteq K$. Deoarece $n > 5$, există un $l \in \{1, 2, \dots, n\}$ astfel încât $(j1i)^{-1} = (lji) \in K$, $\trianglelefteq K$ și rezultă astfel $\sigma = (j1i)^{-1}(lji)\sigma \in K$. Prin urmare, dacă există un $j \in \{1, 2, \dots, n\}$ astfel încât $H_j \trianglelefteq K$, atunci $H_i \trianglelefteq K$ pentru orice $i \in \{1, 2, \dots, n\}$ de unde rezultă $A_n = K$, o contradicție.

Deci $H_i \cap K = 1$ pentru orice $i \in \{1, 2, \dots, n\}$. Atunci alegem o permutare $\sigma \in K$, $\sigma \neq 1$. Deoarece $\sigma \notin H_i \cap K$ avem $\sigma(i) \neq i$ pentru orice $i \in \{1, 2, \dots, n\}$. Alegem un $a \in \{1, 2, \dots, n\}$ și fie $\sigma a = b$. Stîm că $b \neq a$ și putem alege $c \in \{1, 2, \dots, n\}$, cu $b \neq c \neq a$ și în plus $c \neq \sigma^{-1}a$. Luăm

$\sigma \tau = d$ și vom avea $d \notin \{a, b, c\}$. Deoarece $n \geq 6$ putem alege $e, f \in \{1, 2, \dots, n\}$ cu $e \neq f$ și $e, f \notin \{a, b, c, d\}$. Acum fie $\tau = (ab)(cdef)$. Atunci

$$(\tau \sigma \tau^{-1})b = a, (\tau \sigma \tau^{-1})d = e$$

și, în plus, $\tau \sigma \tau^{-1} \in K$, deoarece K este normal. Prin urmare $(\tau \sigma \tau^{-1})\sigma \in K$ și avem $(\tau \sigma \tau^{-1})\sigma e = (\tau \sigma \tau^{-1})d = e$ deci $(\tau \sigma \tau^{-1})\sigma \neq 1$ și

$$(\tau \sigma \tau^{-1})\sigma a = (\tau \sigma \tau^{-1})b = a,$$

ceea ce este o contradicție. Prin urmare A_n nu are subgrupuri normale proprii și netriviale, adică A_n este grup simplu.

Propoziția 5.33. Pentru orice $n \geq 3$ și orice subgrup H al lui A_n cu $|A_n : H| = n$ avem $H \cong A_{n-1}$.

Demonstrație. Pentru $n=3$, avem $|H|=1$, deci $H \cong A_2$. Pentru $n=4$ avem $|H|=2$, deci $H \cong A_3$. Presupunem acum $n \geq 5$. Conform propoziției precedente, în acest caz, A_n este grup simplu. Considerăm acțiunea lui A_n pe mulțimea $X = (A_n/H)$, prin multiplicare la dreapta. Deoarece A_n este grup simplu, această acțiune este fidelă astfel că reprezentarea prin permutări asociată $\phi: A_n \rightarrow S(X)$ este un morfism injectiv. Deoarece $|X| = |A_n : H| = n$, există o aplicație bijecțivă $\mu: X \rightarrow \{1, 2, \dots, n\}$. Atunci, aplicația $\psi: S(X) \rightarrow S_n$ definită prin $\psi(\sigma) = \mu \circ \sigma \circ \mu^{-1}$, $\sigma \in S(X)$ este un izomorfism de grupuri. Componerea $\psi \circ \phi: A_n \rightarrow S_n$ este deci un morfism injectiv și notăm cu K imaginea acestui morfism. Atunci aplicația $\theta: A_n \rightarrow K$ indușă de $\psi \circ \phi$ este un izomorfism. În plus, avem, pentru orice $x \in X$,

$$\begin{aligned} 0(\sigma)\mu(x) &= (\psi \circ \phi)(\sigma)\mu(x) = (\mu \circ \phi(\sigma) \circ \mu^{-1} \circ \mu)(x) = \\ &= (\mu \circ \phi(\sigma))(x) = \mu(\phi(\sigma)(x)) = \mu(\sigma x). \end{aligned}$$

Fie $x \in X$, astfel că $\mu(x) = n$ și fie $\text{Stab}_{A_n}(x)$ stabilizatorul lui x relativ la acțiunea lui A_n pe X prin multiplicare la dreapta și $\text{Stab}_K(n)$, stabilizatorul lui n relativ la acțiunea canonica a lui K pe $\{1, 2, \dots, n\}$. Avem:

$$\begin{aligned} \sigma \in \text{Stab}_{A_n}(x) &\Leftrightarrow \sigma x = x \Leftrightarrow \mu(\sigma x) = \mu(x) \\ &\Leftrightarrow \theta(\sigma)\mu(x) = \mu(x) \Leftrightarrow \theta(\sigma) \in \text{Stab}_K(n) \end{aligned}$$

ceea ce arată că θ induce un izomorfism

$$\text{Stab}_{A_n}(x) \cong \text{Stab}_K(n).$$

Elementul $x \in X = (A_n/H)$, este de forma $x = \sigma H$, $\sigma \in A_n$ și avem

$$\tau \in \text{Stab}_{A_n}(x) \Leftrightarrow \tau \sigma H = \sigma H \Leftrightarrow \tau \in \sigma H \sigma^{-1}$$

astfel că $\text{Stab}_{A_n}(x) = \sigma H \sigma^{-1}$ și deoarece evident avem $H \cong \sigma H \sigma^{-1}$ rezultă

$$H \cong \text{Stab}_K(n). \text{ Deoarece } K \cong A_n, \text{ avem } |S_n : K| = \frac{|S_n|}{|A_n|} = 2 \text{ deci } K \trianglelefteq S_n.$$

Aveam $A_n \leq A_n K \leq S_n$, deci $A_n K = S_n$ sau $A_n K = A_n$. Dacă $A_n K = S_n$, $A_n \cap K$ este un subgrup normal propriu al lui A_n , deci $A_n \cap K = 1$. În plus

$$S_n/K \cong A_n K / K \cong A_n / A_n \cap K \cong A_n$$

de unde rezultă

$$2 = |A_n| = \frac{n!}{2},$$

adică $n! = 4$, ceea ce evident nu se poate. Prin urmare, avem $A_n K = A_n$, deci $K \leq A_n$, $K = A_n$. Rezultă $H \cong \text{Stab}_{A_n}(n) \cong A_{n-1}$.

§ 6. p -GRUPURI ȘI TEOREMELE LUI SYLOW

Definiția 6.1. Dat un număr prim p , un grup finit G se numește p -grup, dacă ordinul G este o putere a lui p . În virtutea teoremei lui Cauchy (vezi 5.3), un grup finit G este p -grup dacă și numai dacă orice element $x \in G$ are ca ordin o putere a lui p . Această observație permite generalizarea noțiunii de p -grup și la cazul grupurilor infinite: un grup oarecare G se numește p -grup dacă orice element $x \in G$ are ordinul o putere a lui p . Un subgrup H al unui grup G se numește p -subgrup al lui G dacă H este p -grup.

Studiul p -grupurilor finite se bazează în esență pe considerarea unor acțiuni, iar rezultatele ce se obțin sint de mare importanță în studiul grupurilor în general.

Propoziția 6.2. Pentru orice p -grup finit G care acionează pe o mulțime finită M avem

$$\text{Fix}_G(X) \equiv |M| \pmod{p}.$$

Demonstrație. Considerăm ecuația claselor pentru acțiunea dată:

$$|M| = \text{Fix}_G(X) + \sum_{\substack{\text{orbită} \\ \text{netrivială}}} |G : \text{Stab}_G(x)|.$$

Deoarece pentru fiecare orbită netrivială gx , avem $1 \neq |G : \text{Stab}_G(x)|$ și cum ordinul lui G este o putere a lui p , rezultă că $p \mid |G : \text{Stab}_G(x)|$ deci că p divide suma care apare în membrul drept al egalității de mai sus, adică

$$|M| \equiv |\text{Fix}_G(M)| \pmod{p}.$$

Propoziția 6.3. Fie G un grup, H și K subgrupuri ale lui G și presupunem că H este de indice finit în G , să zicem $|G : H| = n$ iar K

este un p -grup finit, unde p este un număr prim care nu divide pe n . Atunci există un element $g \in G$, astfel încât $K \leq gHg^{-1}$.

Demonstrație. Considerăm acțiunea lui G pe mulțimea $M = (G/H)$, prin multiplicare la dreapta și apoi restricția acestei acțiuni la K . În virtutea propoziției precedente avem

$$\text{Fix}_K(M) \equiv |M| = |G:H| = n \pmod{p},$$

astfel că, deoarece $p \nmid n$, avem $\text{Fix}_K(M) \neq \emptyset$. Există deci un element $gH \in M$, astfel ca $xgH = gH$ pentru orice $x \in K$. Dar

$$xgH = gH \Leftrightarrow xg \in gH \Leftrightarrow x \in gHg^{-1},$$

astfel că $K \leq gHg^{-1}$.

Propoziția 6.4. Fie G un grup finit și H un p -subgrup al lui G astfel încât $p \mid |G:H|$. Atunci $p \mid |N_G(H):H|$.

Demonstrație. Considerăm acțiunea lui G pe mulțimea $M = (G/H)$, prin multiplicare la dreapta și apoi restricția acestei acțiuni la H . Conform propoziției 6.2, avem $|\text{Fix}_H(M)| \equiv |G:H| \pmod{p}$, astfel că avem $p \mid |\text{Fix}_H(M)|$. Pentru un element $gh \in M$ avem $gH \in \text{Fix}_H(M)$ dacă și numai dacă $xgH = gH$ pentru orice $x \in H$. Deoarece

$$xgH = gH \Leftrightarrow x \Leftrightarrow gHg^{-1}$$

rezultă că

$$gH \in \text{Fix}_H(M) \Leftrightarrow H \leq gHg^{-1} \Leftrightarrow H = gHg^{-1} \Leftrightarrow g \in N_G(H);$$

ceea ce arată că

$$\text{Fix}_H(M) = N_G(H)/H \subset (G/H)_s = M.$$

Prin urmare

$$p \mid |N_G(H)/H| = |N_G(H):H|.$$

Corolarul 6.5. Fie G un p -grup finit și H un subgrup al lui G . Atunci, dacă $H < G$, avem $H < N_G(H)$.

Demonstrație. Deoarece $|G:H| \neq 1$ și $|G:H||G|$, avem $p \mid |G:H|$ astfel că putem aplica propoziția precedentă. Conform acestei propoziții rezultă $p \mid |N_G(H):H|$, deci $|N_G(H):H| \neq 1$, adică $H < N_G(H)$.

Propoziția 6.6. Fie G un grup finit, H un subgrup normal al lui G și K un p -subgrup al lui G . Atunci, dacă $|H| \equiv 1 \pmod{p}$, avem $H \cap C_G(K) \neq 1$.

Demonstrație. Deoarece H este normal în G , G acționează pe mulțimea elementelor lui H prin conjugare. Restricția acestei acțiuni la K este o acțiune a lui K pe H , pentru care avem

$$h \in \text{Fix}_K(H) \Leftrightarrow khk^{-1} = h \text{ pentru orice } k \in K$$

$\Leftrightarrow kh = hk$ pentru orice $k \in K \Leftrightarrow h \in H \cap C_G(K)$,

astfel că

$$\text{Fix}_k(H) = H \cap C_G(K).$$

Deoarece K este p -grup, rezultă din 6.2

$$|H \cap C_G(K)| \not\equiv |H| \pmod{p}$$

și deoarece prin ipoteză $|H| \not\equiv 1 \pmod{p}$, obținem $|H \cap C_G(K)| \not\equiv 1 \pmod{p}$ și, în particular $H \cap C_G(K) \neq 1$.

Corolarul 6.7. Fie G un p -grup și H un subgrup normal netrivial al lui G . Atunci intersecția $H \cap Z(G)$ este netrivială: $H \cap Z(G) \neq 1$.

Demonstrație. Luăm în propoziția precedentă $K = G$ și rezultatul este imediat.

Definiția 6.8. Fie un grup finit și p un număr prim. Presupunem că $|G| = p^m r$ și $p \nmid r$. Atunci un subgrup al lui G de ordin p^n se numește p -subgrup Sylow al lui G . Existența p -subgrupurilor Sylow ale unui grup G pentru orice număr prim p și proprietățile acestor p -subgrupuri sint de importanță fundamentală în teoria grupurilor.

Propoziția 6.9. (Prima teoremă a lui Sylow.) Fie G un grup finit și p un număr prim. Atunci există un p -subgrup Sylow al lui G .

Demonstrație. Printre p -subgrupurile lui G , alegem unul H de ordin maxim și fie $|H| = p^m$. Evident H este un p -subgrup Sylow al lui G dacă și numai dacă $p \nmid |G : H|$. Presupunem, prin absurd, că $p \mid |G : H|$. Atunci, conform propoziției 6.4, avem și $p \nmid |N_G(H) : H|$. În plus, putem forma grupul factor $N_G(H)/H$ și ordinul acestui grup este divizibil cu p . Conform teoremei lui Cauchy, grupul $N_G(H)/H$ are un element de ordin p și acesta generează evident un subgrup de ordin p . Prin urmare, $N_G(H)/H$ are un subgrup de ordin p , și acesta este de forma K/H , unde $H \leq K \leq N_G(H)$. Avem $|K| = |H| \cdot |K/H| = = p^m p = p^{m+1}$, și aceasta contrazice alegerea lui H ca p -subgrup al lui G de ordin maxim.

Allă demonstrație a teoremei lui Sylow. Vom demonstra acum prima teoremă a lui Sylow fără a folosi teorema lui Cauchy. Pentru aceasta trebuie $|G| = p^m r$, cu $p \nmid r$ și fie X mulțimea tuturor submulțimilor U ale lui G care au p^m elemente. Numărul acestor submulțimi U este

$$X = C_{p^m r}^m = \frac{p^m r}{p^m} \cdot \frac{p^m r - 1}{p^m - 1} \cdot \frac{p^m r - 2}{p^m - 2} \cdots \frac{p^m r - p^m + 1}{1}$$

(unde C_n^k înseamnă numărul combinațiilor de n obiecte luate cîte k)

Dacă într-unul din factorii produsului de mai sus, să zicem $\frac{p^m r - j}{p^m - j}$.

$j \in \{0, 1, \dots, p_m - 1\}$, facem toate simplificările posibile cu divizorii comuni ai numărătorului și numitorului, numărătorul astfel obținut nu se divide cu p . Aceasta este clar pentru $j=0$:

$$\frac{p^m r}{p^n} = \frac{r}{1} \text{ și } p \nmid r;$$

dacă $j > 0$, luăm $j=p^n s$ cu $p \nmid s$ și avem

$$\frac{p^m r - j}{p^m - j} = \frac{p_m r - p^n s}{p_m - p^n s} = \frac{p^{m-n} r - s}{p^{m-n} - s}$$

și deoarece $n < m$, avem $p \nmid (p^{m-n} r - s)$. Deoarece p este prim, rezultă că p nu divide produsul numărătorilor obținuți după aceste simplificări și, în concluzie, $p \nmid |X|$. Deoarece pentru un $g \in G$ și $U \subseteq X$ avem $|gU| = |U| = p^m$, putem considera aplicația

$$\alpha: G \times X \rightarrow X$$

definită prin $\alpha(g, U) = gU$ și această aplicație este evident o acțiune. Deoarece X este o mulțime finită, acțiunea noastră are un număr finit de orbite, să zicem X_1, X_2, \dots, X_r , și avem $|X| = |X_1| + |X_2| + \dots + |X_r|$. Deoarece $p \nmid |X|$, există o asemenea orbită, să zicem X_1 , cu $p \nmid |X_1|$. Alegem un element $V \in X_1$ și fie $H = \text{Stab}_G(V) = \{g \in G \mid gV = V\}$. Atunci H este un subgrup al lui G și vom demonstra că H este un p -subgrup Sylow. Avem (vezi 5.8), $|X_1| = |G : H|$, deci $p^m r = |G| = |H||X_1|$ și, deoarece $p \nmid |X_1|$, rezultă $p^m \mid |H|$. Pentru orice $h \in H$ avem $hV = V$, astfel că alegind un element $x_1 \in V$, putem defini aplicația $\phi: H \rightarrow V$ prin $\phi(h) = hx_1$, $h \in H$. Aplicația ϕ este evident injectivă și prin urmare $|H| \leq |V| = p^m$. De aici și din faptul că $p^m \mid |H|$, rezultă $|H| = p^m$.

Propoziția 6.10. (A doua teoremă a lui Sylow.) *Fie G un grup finit, p un număr prim, K un p -subgrup al lui G și H un p -subgrup Sylow al lui G . Atunci, există un $g \in G$, astfel încât $K \leq gHg^{-1}$. În plus, p -subgrupurile Sylow ale lui G formează o clasă de conjugare de subgrupuri.*

Demonstrație. Prima parte a teoremei rezultă evident din propoziția 6.3. Pentru a doua parte, observăm că, pentru orice element $g \in G$, avem $|gHg^{-1}| = |H|$, astfel că gHg^{-1} este și el un p -subgrup Sylow pentru orice $g \in G$. Reciproc, dacă K este un p -subgrup Sylow, avem $K \leq gHg^{-1}$, pentru un $g \in G$ și deoarece $|K| = |H| = |gHg^{-1}|$, rezultă $K = gHg^{-1}$.

Propoziția 6.11. (A treia teoremă a lui Sylow.) *Fie G un grup finit, p un număr prim, H un p -subgrup Sylow al lui G și n_p numărul p -subgrupurilor Sylow ale lui G . Atunci*

$$n_p = |G : N_G(H)|, \quad n_p \mid |G : H| \text{ și } n_p \equiv 1 \pmod{p}.$$

Demonstrație. Fie S_p mulțimea p -subgrupurilor Sylow ale lui G . Conform lui 6.10, S_p este orbita lui H relativ la acțiunea prin conju-gare a lui G pe mulțimea submulțimilor lui G motiv pentru care

$$n_p = |S_p| = |G : N_G(H)|.$$

Deoarece

$$|G : H| = |G : N_G(H)| \cdot |N_G(H) : H| = n_p \cdot |N_G(H) : H|,$$

avem $n_p \mid |G : H|$. Putem defini aplicația $\varphi : H \times S_p \rightarrow S_p$, prin $\varphi(g, K) = gKg^{-1}$, $K \in S_p$, și această aplicație este evident o acțiune a lui H pe mulțimea S_p . Conform lui 6.2 avem

$$|\text{Fix}_H(S_p)| \equiv S_p (\text{mod } p).$$

Pentru un $K \in S_p$ avem

$$K \in \text{Fix}_H(S_p) \Leftrightarrow gKg^{-1} = K \quad \forall g \in H \Leftrightarrow H \leq N_G(K);$$

în această situație H și K sunt p -subgrupuri Sylow ale lui $N_G(K)$ și conform lui 6.10, avem $H = gKg^{-1}$ pentru un $g \in N_G(K)$ adică $H = K$. Prin urmare $\text{Fix}_H(S_p) = \{H\}$ și congruența de mai sus devine $n_p \equiv 1 (\text{mod } p)$.

Observație. A doua demonstrație a teoremei lui Sylow nu folosește teorema lui Cauchy ca prima demonstrație. Mai mult, putem deduce teorema lui Cauchy din prima teoremă a lui Sylow, astfel:

Fie G un grup finit, p un număr prim și $p \mid |G|$. Din prima teoremă a lui Sylow există un p -subgrup Sylow H al lui G și, deoarece $p \mid |G|$, avem $|H| > 1$, deci există un element $x \in H$, $x \neq 1$. Deoarece ordinul lui x divide $|H|$, ordinul lui x este o putere a lui p : $o(x) = p^e$. Atunci $x^{p^e} = 1$ și $x^{p^e-1} \neq 1$. Atunci, pentru $y = x^{p^e-1}$, avem $y^p = x^{p^e} = 1$ și $y \neq 1$, ceea ce arată că $o(y) = p$.

Propoziția 6.12. (Lema lui Frattini.) *Fie G un grup oarecare, K un subgrup normal finit al lui G și H un p -subgrup Sylow al lui K , unde p este un număr prim. Atunci $G = N_G(H)K$.*

Demonstrație. Pentru orice element $g \in G$, avem

$$gHg^{-1} \leq gKg^{-1} = K$$

și deoarece $|gHg^{-1}| = |H|$, gHg^{-1} este un p -subgrup Sylow al lui K ca și H . Prin teorema a doua a lui Sylow, există un element $k \in K$ astfel încât $gHg^{-1} = kHk^{-1}$ ceea ce implică $(k^{-1}g)H(h^{-1}g) = H$, adică $k^{-1}g \in N_G(H)$ sau $g \in N_G(H)k \subset N_G(H)K$. Aceasta arată că $G = N_G(H)K$.

Corolarul 6.13. *Fie G un grup finit, p un număr prim și H un p -subgrup Sylow al lui G . Atunci, pentru orice subgrup K al lui G cu $N_G(H) \leq K$, avem $N_G(K) = K$.*

Demonstrație. Avem $H \leq N_G(H) \leq K$, ceea ce arată că H este și un p -subgrup Sylow al lui K . Luăm $L = N_G(K)$ și aplicăm lema lui Frattini grupului L . Rezultă $L = N_L(H)K$. Dar $N_L(H) \leq N_G(H) \leq K$, astfel că $L = N_L(H)K \leq KK = K$, deci $L = K$, adică $N_G(K) = K$.

Exemple și unele aplicații ale teoremelor lui Sylow. Teoremele lui Sylow au aplicații numeroase și importante în teoria grupurilor. Exemplele și aplicațiile pe care le vom indica mai jos sănătoase sunt dintre cele mai concrete, ele ilustrând insă foarte bine importanța teoremelor lui Sylow și modul în care se folosesc ele. O modalitate de utilizare constă în a folosi teoremele lui Sylow pentru a identifica un subgrup normal propriu și netrivial al unui grup G : Fie p un divizor al lui $|G|$ și H un p -subgrup Sylow al lui G . Deoarece $p \mid |G|$, avem $|H| > 1$, iar dacă G nu este p -grup avem $H < G$ deci H este un subgrup propriu și netrivial. Fie n_p numărul p -subgrupurilor Sylow ale lui G . Dacă arătăm, folosind teorema a treia a lui Sylow sau alte mijloace, că $n_p = 1$, atunci din teorema a doua a lui Sylow rezultă că H este un subgrup normal al lui G .

Subgrupurile Sylow ale lui S_4 . Avem

$$S_4 = 4! = 24 = 2^3 \cdot 3.$$

Prin urmare 2-subgrupurile Sylow ale lui S_4 sunt exact subgrupurile de ordinul 8, iar 3-subgrupurile Sylow sunt exact subgrupurile de ordinul 3. Subgrupurile de ordinul 3 ale lui S_4 se descoperă imediat: ele sunt generate de elemente de ordinul 3, iar elementele de ordinul 3 în S_4 sunt exact ciclurile de lungime 3. Găsim $n_3 = 4$ și 3-subgrupurile Sylow ale lui S_4 sunt: $\{1, (123), (132)\}$, $\{1, (124), (142)\}$, $\{1, (134), (143)\}$, $\{1, (234), (243)\}$. Pentru a descrie 2-subgrupurile Sylow ale lui S_4 , observăm că dacă luăm $\rho = (1 \ 2 \ 3 \ 4)$ și $\epsilon = (1 \ 2)(3 \ 4)$, avem $\rho^4 = 1$, $\epsilon^2 = 1$, $\epsilon\rho = \rho^3\epsilon = (2 \ 4)$.

Rezultă că

$$H = \langle \rho, \epsilon \rangle = \{1, \rho, \rho^2, \rho^3, \epsilon, \rho\epsilon, \rho^2\epsilon, \rho^3\epsilon\}$$

este un subgrup de ordinul 8 al lui S_4 , izomorf cu grupul diedral D_4 . Orice 2-subgrup Sylow al lui S_4 este conjugat cu H , deci, de asemenea, izomorf cu D_4 . În virtutea celei de-a treia teoreme a lui Sylow, numărul n_2 al 2-subgrupurilor Sylow satisfacă condiția $n_2 \mid 3$, deci $n_2 = 1$ sau $n_2 = 3$. În cazul $n_2 = 1$, H ar fi normal în S_4 , ceea ce nu este adevărat. Într-adevăr, avem:

$$H = \{1, (1234), (1 \ 3)(2 \ 4), (1 \ 4 \ 3 \ 2), (1 \ 2)(3 \ 4), (1 \ 3), (2 \ 4)\}$$

deci, de exemplu, $(2 \ 4) \in H$ și

$$(1 \ 4)(2 \ 4)(1 \ 4)^{-1} = (1 \ 2) \notin H.$$

Prin urmare avem $n_2=3$, iar cele 3 subgrupuri ale lui S_4 de ordinul 8 sunt H

$$(1\ 4)H(1\ 4)^{-1} = \{1, (1423), (12)(34), (1324), (13)(24), (34), (12)\}$$

și

$$(12)H(12)^{-1} = \{1, (1342), (14)(23), (1243), (12)(34), (23), (14)\}.$$

Subgrupurile Sylow ale lui D_n , n impar. Avem

$$D_n = \langle \rho, \varepsilon \rangle, \text{ unde } \rho^n = 1, \varepsilon^2 = 1, \varepsilon\rho = \rho^{n-1}\varepsilon = \rho^{-1}\varepsilon.$$

Deoarece $|D_n| = 2n$, avem $o(\rho) = n$, deci $H = \langle \rho \rangle$ este un subgrup al lui D_n de ordin n . Orice element din $D_n - H$ este de forma $\rho^k\varepsilon$ cu $k \in \{0, 1, \dots, n-1\}$ și se verifică imediat (eventual prin inducție după k) că $\varepsilon\rho^k = \rho^{n-k}\varepsilon$ pentru orice număr natural k . Prin urmare

$$(\rho^k\varepsilon)^2 = \rho^k(\varepsilon\rho^k)\varepsilon = \rho^k\rho^{-k}\varepsilon^2 = 1,$$

astfel că orice element din $D_n - H$ are ordinul 2. În cazul cind n este impar, 2-subgrupurile Sylow ale lui D_n au ordinul 2 și deci sunt tot atitea 2-subgrupuri Sylow în D_n ; cîte elemente de ordinul 2 are D_n , iar aceste elemente de ordinul 2 din D_n sunt exact elementele de forma $\rho^k\varepsilon$, $k \in \{0, 1, \dots, n-1\}$. Într-adevăr, H fiind un grup de ordin n și n fiind impar, H nu are elemente de ordinul 2. Prin urmare $n_2 = n$ și 2-subgrupurile Sylow ale lui D_n sunt:

$$\{1, \rho^k\varepsilon\}, k \in \{0, 1, \dots, n-1\}.$$

Acum fie p un număr prim impar și presupunem că $p \mid |D_n| = 2n$. Atunci $p \mid n$ și dacă P este un p -subgrup Sylow al lui D_n , P nu conține elemente de ordinul 2. Rezultă $P \trianglelefteq H$.

Prin urmare, $n_p = 1$ și un p -subgrup Sylow al lui D_n este ciclic. Astfel, toate subgrupurile Sylow ale lui D_n , n impar, sunt ciclice.

Grupuri de ordin pq . Fie p și q numere prime distințe și fie G un grup de ordin pq . Fie P un p -subgrup Sylow al lui G și Q un q -subgrup Sylow al lui G . Avem $|P| = p$ și $|Q| = q$, astfel că P și Q sunt grupuri ciclice, să zicem $P = \langle x \rangle$ și $Q = \langle y \rangle$, unde $o(x) = p$, $o(y) = q$. Fie n_p numărul p -subgrupurilor Sylow ale lui G . Avem $n_p \mid q$ și $n_p \equiv 1 \pmod{p}$; rezultă $n_p = 1$ sau $n_p = q$, iar egalitatea $n_p = q$ poate avea loc numai în cazul cind $q \equiv 1 \pmod{p}$. Analog $n_q = 1$ sau $n_q = p$, iar egalitatea $n_q = p$ poate avea loc numai în cazul cind $p \equiv 1 \pmod{q}$. Deoarece $p \neq q$, nu putem avea simultan și $q \equiv 1 \pmod{p}$ și $p \equiv 1 \pmod{q}$. Prin urmare $n_p = 1$ sau $n_q = 1$, ceea ce arată că $P \trianglelefteq G$ sau $Q \trianglelefteq G$. Aceasta arată că G nu este grup simplu.

În plus, în cazul $p \not\equiv 1 \pmod{q}$ și $q \not\equiv 1 \pmod{p}$ avem $n_p = 1$ și $n_q = 1$, deci $P \trianglelefteq G$ și $Q \trianglelefteq G$. Atunci

$$x \in P, x^{-1} \in P, yx^{-1}y^{-1} \in P,$$

deci

$$xyx^{-1}y^{-1} = x(yx^{-1}y^{-1}) \in P.$$

Analog

$$xyx^{-1}y^{-1} = (xyx^{-1})y^{-1} \in Q$$

astfel că

$$xyx^{-1}y^{-1} \in P \cap Q = 1, \text{ deci } xy = yx.$$

Fie n un număr întreg și presupunem $(xy)^n = 1$. Din legea de comutativitate generalizată rezultă

$$1 = (xy)^n = x^n y^n.$$

deci $x^n = y^{-n} \in P \cap Q = 1$, deci $x^n = y^n = 1$.

Aceasta demonstrează că $p|n$, $q|n$, deci $pq|n$ și astfel $o(xy) = pq = |G|$. Prin urmare $G = \langle xy \rangle$ și G este ciclic. Astfel, orice grup de ordin pq , unde p și q sunt numere prime, $p \not\equiv 1 \pmod{q}$ și $q \not\equiv 1 \pmod{p}$ este ciclic. De exemplu orice grup de ordin 15, 33, 35 etc. este ciclic.

Grupuri de ordin p^2q . Fie p și q numere prime distințte și G un grup de ordin p^2q . Fie P un p -subgrup Sylow al lui G și Q un q -subgrup Sylow al lui G . Avem $|P| = p^2$ și $|Q| = q$. Fie n_p numărul p -subgrupurilor Sylow ale lui G . Să presupunem că $n_p > 1$ și $n_q > 1$. Deoarece $n_p | q$ și q este număr prim, rezultă $n_p = q$ și deoarece $q = n_p \equiv 1 \pmod{p}$, rezultă $q > p$. Deoarece $n_p | p^2$, avem $n_p = p$ sau $n_p = p^2$ și deoarece $n_q \equiv 1 \pmod{q}$ și $q > p$, nu putem avea $n_q = p$. Prin urmare, $n_q = p^2$. Orice element de ordinul q al lui G generează un subgrup de ordinul q al lui G , deci un q -subgrup Sylow al lui G și orice două asemenea subgrupuri au intersecția trivială de unde rezultă că numărul elementelor de ordin q ale lui G este

$$n_q(q-1) = p^2(q-1)$$

iar numărul elementelor lui G care nu sunt de ordin q este

$$p^2q - p^2(q-1) = p^2.$$

Deoarece $|P| = p^2$, orice element din P nu este de ordin q , de unde rezultă că P coincide cu mulțimea tuturor elementelor lui G , care nu au ordinul q . Acest lucru se va întâmpla de fapt pentru orice p -subgrup Sylow al lui G , astfel că rezultă $n_p = 1$, o contradicție. Prin urmare $n_p = 1$ sau $n_q = 1$, adică $P \trianglelefteq G$ sau $Q \trianglelefteq G$. Astfel, orice grup de ordin p^2q nu este grup simplu.

Presupunem acum că $p^2 \not\equiv 1 \pmod{q}$ și $q \not\equiv 1 \pmod{p}$. Conform celor de mai sus vom avea $n_p=1$ și $n_q=1$, deci $P \trianglelefteq G$ și $Q \trianglelefteq G$. Avem $|P|=p^2$, $|Q|=q$ și $|P \cap Q|$ divide atât pe $|P|=p^2$ cit și pe $|Q|=q$, astfel că $|P \cap Q|=1$, $P \cap Q=1$. Avem

$$|PQ| = \frac{|P||Q|}{|P \cap Q|} = p^2q,$$

astfel că $G=PQ$. Fie acum $x \in P$ și $y \in Q$. Atunci $xyx^{-1}y^{-1} \in P \cap Q=1$, astfel $xy=yx$. De aici rezultă că G este abelian. Într-adevăr, pentru orice două elemente $z_1, z_2 \in G$ avem $z_i=x_iy_i$, $x_i \in P$, $y_i \in Q$. Atunci, deoarece P și Q sint abeliene,

$$\begin{aligned} z_1z_2 &= (x_1y_1)(x_2y_2) = x_1(y_1x_2)y_2 = x_1(x_2y_1)y_2 = \\ &= (x_1x_2)(y_1y_2) = (x_2x_1)(y_2y_1) = x_2(x_1y_2)y_1 = \\ &= x_2(y_2x_1)y_1 = (x_2y_2)(x_1y_1) = z_2z_1. \end{aligned}$$

Prin urmare, dacă $|G|=p^2q$ și $p^2 \not\equiv 1 \pmod{q}$, $q \not\equiv 1 \pmod{p}$, atunci G este abelian. Astfel, orice grup de ordin 45, 99, 175 etc., este grup abelian.

Grupuri de ordin 255. Vom demonstra acum că orice grup de ordin 255 este ciclic. Fie G un astfel de grup. Deoarece $|G|=255=3 \cdot 5 \cdot 17$, un 17-subgrup Sylow H al lui G are ordinul 17. În plus, dacă n_{17} este numărul 17-subgrupurilor Sylow ale lui G , avem $n_{17} | 3 \cdot 5 = 15$ și $n_{17} \equiv 1 \pmod{17}$. Evident rezultă $n_{17}=1$, astfel că $H \trianglelefteq G$. Grupul factor G/H va avea ordinul $|G/H| = \frac{255}{17} = 15$. Grupul H este ciclic deoarece

ordinul său este un număr prim, iar G/H este de asemenea ciclic. Să considerăm elementele $a, b \in G$ astfel ca $H=\langle a \rangle$ și $G/H=\langle bH \rangle$. Fie $n=o(b)$. Deoarece $b^n=1$, avem $(bH)^n=1$ și cum $o(bH)=15$, rezultă $15 | n$. În plus $n || |G|=255=15 \cdot 17$, astfel că $n=15$ sau $n=255$. Dacă $n=255$, avem $G=\langle b \rangle$ și G este ciclic. În continuare vom presupune $o(b)=15$. Avem $a \in H \trianglelefteq G$, deci $bab^{-1} \in H=\langle a \rangle$, astfel că $bab^{-1}=a^r$, unde r este un număr întreg și $0 \leq r < o(a)=17$. Presupunând că are loc egalitatea $b^mab^{-m}=a^{rm}$ pentru un $m \in \mathbb{Z}$ rezultă

$$\begin{aligned} b^{m+1}ab^{-(m+1)} &= b(b^mab^{-m})b^{-1} = ba^rb^{-1} = \\ &= (bab^{-1})^r = (a^r)^r = a^{r^m}. \end{aligned}$$

Aceasta arată că $b^mab^{-m}=a^{rm}$ pentru orice număr natural m . Deoarece $o(b)=15$ avem $a^{15}=b^{15}ab^{-15}=a$, astfel că $r^{15} \equiv 1 \pmod{17}$. Deoarece $r^{16} \equiv 1 \pmod{17}$, rezultă $r \equiv 1 \pmod{17}$, deci $r=1$. Am demonstrat astfel că $bab^{-1}=a$, deci $ab=ba$. De aici rezultă ușor că $o(ab)=o(a)o(b)=15 \cdot 17=255$, deci $G=\langle ab \rangle$.

Grupuri simple de ordin ≤ 100 . Grupurile finite simple și abeliene sunt grupuri ciclice de ordin p , unde p este un număr prim. În continuare ne propunem să arătăm că orice grup finit simplu și neabelian, de ordin ≤ 100 , este izomorf cu grupul altern A_5 . Primul pas al demonstrației constă în a arăta că dacă G este un grup simplu neabelian de ordin n și $n \leq 100$, atunci $n = 60 = |A_5|$.

Pentru aceasta trebuie să vedem că anumite numere întregi positive n nu pot fi ordinul unui grup simplu neabelian. Relativ la această problemă există în teoria grupurilor două teoreme celebre:

Teorema lui Burnside. *Orice grup finit simplu neabelian are cel puțin trei divizori primi distincți;*

Teorema lui Feit-Thomson. *Orice grup finit simplu neabelian are ordinul par.*

Teorema lui Burnside a fost demonstrată la începutul acestui secol într-un mod relativ simplu dar folosind tehnică reprezentărilor de grupuri. Ulterior s-au obținut și demonstrații care nu utilizează reprezentările de grupuri, dar respectivele demonstrații sunt deja foarte complicate. Teorema lui Feit-Thomson a fost demonstrată în 1963, folosind o mulțime de tehnici de teoria grupurilor, care de care mai sofisticată.

În demonstrațiile ce urmează, noi nu vom folosi aceste două teoreme celebre. Vom folosi teoremele lui Sylow și, printre altele, următoarele rezultate care sunt evidente din paginile anterioare. (În ceea ce urmează, p, q, r sunt numere prime nu neapărat distincte):

1. Orice grup finit de ordin p^n nu este grup simplu neabelian.

Aceasta rezultă din faptul că dacă G este un grup de ordin p^n și $n \geq 1$, atunci $Z(G) \neq 1$ (vezi de exemplu 6.6). Deoarece $Z(G) \trianglelefteq G$, avem $Z(G) = G$ și atunci G este abelian, sau $Z(G) < G$ și atunci $Z(G)$ este un subgrup normal propriu și netrivial al lui G , deci G nu este grup simplu.

2. Orice grup finit de ordin pq nu este grup simplu.

3. Orice grup finit de ordin p^2q nu este grup simplu.

În aceeași direcție avem și

Propoziția 6.14. *Orice grup de ordin pqr nu este grup simplu.*

Demonstrație. În vîrfultea lui 3 de mai sus putem presupune că p, q, r sunt distințe două și fie $p > q > r$. Presupunem, priu absurd, că G este un grup simplu de ordin pqr . Atunci, notind cu n_p, n_q, n_r numărul p, q, r -subgrupurilor Sylow ale lui G , avem $n_p > 1, n_q > 1, n_r > 1$. Deoarece p -subgrupurile Sylow ale lui G au ordinul p , numărul elementelor lui G de ordin p este $n_p(p-1)$. Analog, numărul elementelor G de ordin q este $n_q(q-1)$ iar numărul elementelor de ordin r este $n_r(r-1)$. Prin urmare

$$pqr = |G| \geq 1 + n_p(p-1) + n_q(q-1) + n_r(r-1).$$

Avem $n_p|qr$, deci $n_p=q$, $n_p=r$ sau $n_p=qr$. În plus $n_p \equiv 1 \pmod{p}$, deci $n_p > p$ și deoarece $p > q > r$, avem $n_p=qr$. Avem $n_q|pr$ și $n_q \equiv 1 \pmod{q}$ și rezultă că mai sus că $n_q=p$ sau $n_q=pr$ și, în ambele cazuri, avem $n_q \geq p$. De asemenea $n_r|pq$, deci $n_r=p$, $n_r=q$ sau $n_r=pq$ și în toate situațiile posibile avem $n_r \geq q$. Rezultă

$$pqr \geq 1 + n_p(p-1) + n_q(q-1) + n_r(r-1) \geq$$

$$\geq 1 + qr(p-1) + p(q-1) + q(r-1) = pqr + pq - p - q + 1,$$

sau

$$0 \geq pq - p - q + 1 = (p-1)(q-1),$$

ceea ce evident nu se poate.

Îșiând toate numerele naturale n cuprinse între 1 și 100 și descompunindu-le în factori primi, vedem că dacă G este un grup finit simplu neabelian de ordin n , atunci, conform rezultatelor 1–3 și propoziției 6.14, nu putem avea decât următoarele posibilități pentru n : $24=2^3 \cdot 3$, $36=2^2 \cdot 3^2$, $40=2^3 \cdot 5$, $48=2^4 \cdot 3$, $54=2 \cdot 3^3$, $56=2^3 \cdot 7$, $60=2^2 \cdot 3 \cdot 5$, $72=2^3 \cdot 3^2$, $80=2^4 \cdot 5$, $84=2^2 \cdot 3 \cdot 7$, $88=2^3 \cdot 11$, $90=2 \cdot 3^2 \cdot 5$, $96=2^5 \cdot 3$ și $100=2^2 \cdot 5^2$.

Unele din aceste posibilități se pot elimina folosind următoarea:

Propoziția 6.15. Fie G un grup finit simplu neabelian și H un subgrup propriu al lui G . Atunci $|G:H| \geq 5$.

Demonstrație. Fie $n=|G:H|$ și fie H_G interiorul normal lui H în G . Avem $H_G \leq H \leq G$ și $H_G \trianglelefteq G$ astfel că, deoarece G este un grup simplu avem $H_G=1$. În plus, grupul factor G/H_G se poate scufunda în grupul simetric S_n astfel că, deoarece $H_G=1$, G se poate scufunda în grupul simetric S_n . Vom demonstra că grupul simetric S_n nu are subgrupuri simple neabeliene pentru $n \in \{1, 2, 3, 4\}$. Aceasta este clar pentru $n=1$ și $n=2$ deoarece în aceste cazuri S_n este abelian. Pentru $n=3$, avem $|S_3|=6$. S_3 nu este simplu deoarece $A_3 \trianglelefteq S_3$ și subgrupurile proprii ale lui S_3 , având ordinele 1, 2 sau 3 sunt abeliene. Pentru $n=4$, avem $|S_4|=24=2^3 \cdot 3 \cdot S_4$ nu este simplu deoarece $A_4 \trianglelefteq S_4$. Un subgrup simplu și neabelian H al lui S_4 nu poate avea ordinul egal cu 2 sau cu 3 deci acest ordin se divide și cu 2 și cu 3 și vom avea $|H|=2 \cdot 3$ sau $|H|=2^2 \cdot 3$. Ambele aceste posibilități sunt însă deja excluse.

Cazurile care se pot elimina pe baza propoziției 6.15. Fie G un grup finit simplu neabelian de ordin n , unde n este unul din numerele listate mai sus. Dacă $n=24=2^3 \cdot 3$, $n=48=2^4 \cdot 3$, $n=96=2^5 \cdot 3$, considerăm un 2-subgrup Sylow H al lui G și avem $|G:H|=3 < 5$, ceea ce contrazice propoziția 6.15. În acă $n=36=2^2 \cdot 3^2$, $n=54=2 \cdot 3^3$, considerăm un 3-subgrup Sylow H al lui G și avem $|G:H|=4$ în primul caz și $|G:H|=2$ în al doilea caz, ambele situații contrazicind propoziția 6.15. De asemenea cind $n=100=2^2 \cdot 5^2$ și H este un 5-subgrup Sylow al lui G , avem $|G:H|=4$, contrar lui 6.15.

În cazurile $n=40=2^3 \cdot 5$, $n=56=2^3 \cdot 7$, $n=72=2^5 \cdot 3^2$, $n=88=2^4 \cdot 11$, considerăm un p -subgrup Sylow H al lui G , unde p este respectiv 5, 7, 3, 11 și notăm cu n_p numărul p -subgrupurilor Sylow ale lui G . În toate aceste cazuri, $n_p | 2^3 = 8$ și, în plus, $n_p > 1$. Deoarece $n_p = |G : N_G(H)|$ și $N_G(H)$ este un subgrup propriu al lui G avem, în virtutea lui 6.15, $n_p \geq 5$, astfel că $n_p = 8$. Acest lucru nu se poate întâmpla în cazurile $p=5, 3, 11$ deoarece $n_p \equiv 1 \pmod{p}$. Rămîne $p=7$ deci $n=2^3 \cdot 7 = 56$. În acest caz deoarece 7-subgrupurile Sylow ale lui G au ordinul 7, numărul elementelor de ordinul 7 ale lui G este $n_7(7-1) = 8 \cdot 6 = 48$, astfel că numărul elementelor lui G care nu sunt de ordinul 7 este $56 - 48 = 8$. Orice 2-subgrup Sylow al lui G are ordinul 8 și deci coincide cu multimea celor 8 elemente care nu au ordinul 7. Prin urmare, $n_2 = 1$ și un 2-subgrup Sylow al lui G este normal în G , ceea ce contrazice faptul că G este grup simplu.

Cazurile care nu se pot elimina pe baza propoziției 6.15 sunt $n=60=2^2 \cdot 3 \cdot 5$, $n=80=2^4 \cdot 5$, $n=84=2^2 \cdot 3 \cdot 7$ și $n=90=2 \cdot 3^2 \cdot 5$.

Cazul $n=84=2^2 \cdot 3 \cdot 7$. Fie G un grup simplu de ordin 84, H un 7-subgrup Sylow al lui G și n_7 numărul 7-subgrupurilor Sylow ale lui G . Avem $n_7 | 12$ și $n_7 \equiv 1 \pmod{7}$; dar divizorii proprii 2, 3, 4, 6, 12 ai lui 12 nu sunt $\equiv 1 \pmod{7}$, astfel că $n_7 = 1$, deci $H \trianglelefteq G$, ceea ce contrazice faptul că G este grup simplu.

Cazul $n=80=2^4 \cdot 5$. Fie p un număr prim și m, r numere întregi astfel ca $m > 0$, $r > 1$ și $p \nmid r$. Fie G un grup simplu de ordin $p^m r$, H un p -subgrup Sylow al lui G și H_G inimă lui H în G . Deoarece $|G : H| = r$, grupul factor G/H_G se poate scufunda în grupul simetric S_r . Deoarece G este grup simplu, avem $H_G = 1$, astfel că G se poate scufunda în S_r . Prin urmare $p^m r = |G| = |S_r| = r!$, astfel că $p^m | (r-1)!$.

În particular cînd $p=r$ și $r=5$, ar trebui să avem $2^m | 4! = 24$ ceea ce implică $m \leq 3$. În concluzie nu există grupuri simple de ordin $2^m 5$ cu $m \geq 4$ și, în particular, nu există grupuri simple de ordin $80=2^4 \cdot 5$.

Cazul $n=90=2 \cdot 3^2 \cdot 5$. Fie $n=2r$, unde r este un număr întreg impar și fie G un grup simplu de ordin n . Există un element $t \in G$ de ordinul 2. Considerăm acțiunea lui G pe el însuși prin multiplicare la dreapta și reprezentarea prin permutări $\varphi: G \rightarrow S(G)$ asociată acestei acțiuni. Dacă $G = \{x_1, x_2, \dots, x_n\}$, atunci permutarea

$$\tau = \varphi(t) = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ tx_1 & tx_2 & \dots & tx_n \end{pmatrix} \in S(G) \cong S_n$$

are ordinul 2 ca și t , deoarece φ este un morfism de grupuri injectiv. Rezultă că τ este un produs de transpoziții disjuncte două cîte două și deoarece nu putem avea $tx=x$ pentru vreun $x \in G$, rezultă că τ este un produs de r transpoziții. Prin urmare $\text{sgn}(\tau) = (-1)^r = -1$, astfel că $\tau \notin A_n$. Prin urmare grupul $H = \varphi(G)$ nu este inclus în grupul altern A_n .

Deoarece φ este un morfism de grupuri injectiv, H este un grup simplu, ca și G . Deoarece $A_n \trianglelefteq S_n$, avem $A_n \cap H \trianglelefteq H$, deci $A_n \cap H = 1$. Atunci $H \cong H/A_n \cap H \cong HA_n/A_n \cong S_n/A_n$ și deoarece $|S_n/A_n| = 2$, rezultă $|H| = 2$, deci $n = |G| = |H| = 2$, adică $r = 1$. Prin urmare nu există grupuri simple de ordin $n = 2r$, unde r este un număr întreg impar > 1 și, în particular, nu există grupuri simple de ordin $n = 90$.

Cazul $n = 60$. Grupul altern A_5 este un grup simplu de ordin 60. Vom demonstra că orice grup simplu de ordin 60 este izomorf cu A_5 . Fie G un grup simplu de ordin $60 = 2^2 \cdot 3 \cdot 5$. Fie P un 5-subgrup Sylow al lui G , $H = N_G(P)$ și n_5 numărul 5-subgrupurilor Sylow ale lui G . Avem $n_5 = |G : H|$, $n_5 | 2^2 \cdot 3 = 12$ și $n_5 \equiv 1 \pmod{5}$; în plus $n_5 > 1$ deoarece G este grup simplu. Rezultă $n_5 = 6$, deci $|G : H| = 6$. Considerind interiorul normal H_G al lui H în G , avem $H_G = 1$ și $G \cong G/H_G$ se poate scufunda în S_6 . Prin urmare G este izomorf cu un subgrup K al lui S_6 . Deoarece $K \cap A_6 \trianglelefteq K$, avem $K \cap A_6 = 1$, caz în care rezultă $|K| = 2$, ceea ce nu este cazul, sau $K \cap A_6 = K$ caz în care avem $K \leq A_6$. Deoarece $|A_6| = \frac{6!}{2} = \frac{5!}{2}$, $|K| = |G| = 60 = \frac{5!}{2}$, rezultă $|A_6 : K| = 5$ și, conform propoziției 5.33, rezultă $K \cong A_5$, deci $G \cong K \cong A_5$.

Propoziția 6.16. Fie G un p -grup finit și $|G| = p^m$. Atunci, există subgrupurile normale G_0, G_1, \dots, G_m ale lui G , astfel ca

$$1 = G_0 < G_1 < \dots < G_{m-1} = G$$

și $|G_i| = p^i$ pentru orice $i \in \{0, 1, \dots, m\}$.

Demonstrație. Vom face inducție după m . Afirmația din enunț este trivială pentru $m \leq 1$, astfel că vom presupune $m > 1$ și că această afirmație este adeverată pentru grupuri de ordin p^{m-1} . Deoarece $Z(G) \neq 1$, există un element $x \in Z(G)$, $x \neq 1$, și avem $o(x) = p^n$ pentru un număr întreg $n > 0$. Atunci $(x^{p^{n-1}})^p = 1$ și $x^{p^{n-1}} \neq 1$, astfel că $o(x^{p^{n-1}}) = p$ și $G_1 = \langle x^{p^{n-1}} \rangle$ este un subgrup de ordin p al lui G . Deoarece $G_1 \leq Z(G)$, avem $G_1 \trianglelefteq G$ și grupul factor $\bar{G} = G/G_1$ are ordinul p^{m-1} . În virtutea ipotezei de inducție, grupul \bar{G} are subgrupurile normale $\bar{G}_0, \bar{G}_1, \dots, \bar{G}_{m-1}$, astfel ca

$$1 = \bar{G}_0 < \bar{G}_1 < \dots < \bar{G}_{m-1} = \bar{G}$$

și $|\bar{G}_i| = p^i$ pentru orice $i \in \{1, \dots, m-1\}$. Conform teoremei de corespondență, fiecare G_i este de forma $\bar{G}_i = G_{i+1}/G_1$, unde G_{i+1} este un subgrup normal al lui G și $G_1 \leq G_{i+1}$. În plus, $p^i = |G_i| = \frac{|G_{i+1}|}{|G_1|} = \frac{|G_{i+1}|}{p}$, deci $|G_{i+1}| = p^{i+1}$. Cu aceasta propoziția este demonstrată.

Observație. Teoremele lui Sylow nu pot da informații despre structura unui p -grup finit, dar ele arată că se pot obține informații despre

structura unui grup finit oarecare cunoscind structura p -subgrupurilor sale Sylow. Din acest motiv determinarea structurii p -grupurilor finite capătă importanță deosebită în teoria grupurilor, iar propoziția 6.16 este un pas important în această direcție. Ca o consecință a sa avem:

Corolarul 6.17. Fie G un grup finit, p un număr prim și presupunem că $p^n \mid |G|$. Atunci există un subgrup H al lui G de ordin p^n .

Demonstrație. Presupunem că $|G| = p^m r$, unde $p \nmid r$. Deoarece $p^n \mid |G|$, avem $n \leq m$. Prima teoremă a lui Sylow arată că există un subgrup P al lui G de ordin p^n , iar propoziția 6.16, arată că există un subgrup H al lui P de ordin p^n . Atunci H este și un subgrup al lui G de ordin p^n .

Definiție 6.18. Un grup G se numește *abelian elementar* dacă este abelian și există un număr prim p astfel ca $x^p = 1$ pentru orice $x \in G$. Spunem de asemenea că G este un p -grup abelian elementar, un astfel de grup G fiind evident un p -grup.

O submulțime X a unui grup G se numește *sistem de generatori minimal* al lui G dacă $\langle X \rangle = G$ și pentru orice submulțime proprie Y a lui X , $\langle Y \rangle$ este un subgrup propriu al lui G . În general, un grup G nu are neapărat un sistem de generatori minimal. Un grup finit G are însă evident un sistem de generatori minimal.

Propoziția 6.19. Fie G un p -grup abelian elementar finit și fie $\{x_1, x_2, \dots, x_n\}$ un sistem de generatori minimal al lui G . Atunci, orice element $x \in G$ se scrie în mod unic sub forma:

$$x = x_1^{r_1} x_2^{r_2} \dots x_n^{r_n}$$

unde, pentru fiecare $i \in \{1, 2, \dots, n\}$, $r_i \in \mathbb{Z}$ și $0 \leq r_i < p$. În particular, G are p^n elemente.

Demonstrație. Deoarece $\{x_1, x_2, \dots, x_n\}$ este un sistem de generatori al lui G , pentru orice element $x \in G$ avem

$$x = x_1^{a_1} x_2^{a_2} \dots x_n^{a_n}$$

cu $a_i \in \mathbb{Z}$, $i \in \{1, 2, \dots, n\}$. Împărțind fiecare a_i , $i \in \{1, 2, \dots, n\}$ la p avem $a_i = pb_i + r_i$ cu $0 \leq r_i < p$. Atunci

$$x_i^{a_i} = (x_i^p)^b x_i^{r_i} = x_i^{r_i}$$

astfel că $x = x_1^{r_1} x_2^{r_2} \dots x_n^{r_n}$. Pentru a demonstra unicitatea, să presupunem mai întâi că avem

$$x_1^{s_1} x_2^{s_2} \dots x_n^{s_n} = 1 \text{ cu } |s_i| < p, i \in \{1, 2, \dots, n\}.$$

Dacă $s_1 \neq 0$, avem $p \nmid s_1$, deci $(p, s_1) = 1$ și există numere întregi a și b cu $pa + s_1 b = 1$. Atunci

$$x_1 = x_1^{pa+s_1b} = (x_1^p)^a(x_1^{s_1})^b = (x_1^{s_1})^b = (x_2^{-r_1}, \dots, x_n^{-r_n})^b = x_2^{-sr_1b} \dots x_n^{-sr_nb} \in \langle x_2, \dots, x_n \rangle$$

Rezultă $G = \langle x_1, x_2, \dots, x_n \rangle \subset \langle x_2, \dots, x_n \rangle$. Aceasta însă contrazice minimalitatea sistemului de generatori $\{x_1, x_2, \dots, x_n\}$. Prin urmare avem $s_1=0$. Analog rezultă $s_2 = \dots = s_n = 0$. Acum să presupunem că

$$x_1^{r_1}x_2^{r_2} \dots x_n^{r_n} = x_1^{r'_1}x_2^{r'_2} \dots x_n^{r'_n}, \text{ unde } 0 \leq r_i, r'_i < p.$$

Atunci

$$x_1^{r_1-r'_1}x_2^{r_2-r'_2} \dots x_n^{r_n-r'_n} = 1$$

și, pentru fiecare $i \in \{1, 2, \dots, n\}$, $|r_i - r'_i| < p$, astfel că, conform celor de mai sus, $r_i = r'_i$.

Definiția 6.20. Un subgrup M al unui grup G se numește *subgrup maximal* al lui G dacă M este element maximal în mulțimea subgrupurilor proprii ale lui G ordonată prin incluziune. Notăm cu $F(G)$ intersecția tuturor subgrupurilor maximale ale lui G . Subgrupul $F(G)$ se numește *subgrupul Frattini* al grupului G .

Lema 6.21. Pentru orice grup G , subgrupul Frattini $F(G)$ este un subgrup characteristic al lui G . În particular, avem $F(G) \trianglelefteq G$.

Demonstrație. Fie $\sigma \in \text{Aut}(G)$ și M un subgrup maximal al lui G . Atunci $\sigma(M)$ este de asemenea un subgrup maximal al lui G . Într-adevăr, M fiind un subgrup propriu există un $x \in G$, $x \notin M$, și atunci $\sigma(x) \notin \sigma(M)$, deci $\sigma(M)$ este un subgrup propriu al lui G ; și, pentru orice subgrup H al lui G , avem:

$$\sigma(M) \subseteq H \Leftrightarrow M \subseteq \sigma^{-1}(H) \Leftrightarrow M = \sigma^{-1}(H) \text{ sau}$$

$$\sigma^{-1}(H) = G \Leftrightarrow \sigma(M) = H \text{ sau } H = G.$$

astfel că $\sigma(M)$ este un subgrup maximal al lui G . Dacă \mathcal{M} este mulțimea tuturor subgrupurilor maximale ale lui G , avem $F(G) = \bigcap_{M \in \mathcal{M}} M$, deci

$$\sigma(F(G)) = \bigcap_{M \in \mathcal{M}} \sigma(M) \subset F(G)$$

Analog vom avea $\sigma^{-1}(F(G)) \subset F(G)$, deci $\sigma(F(G)) = F(G)$.

Propoziția 6.22. Fie G un p -grup finit. Atunci, grupul factor $G/F(G)$ este p -grup abelian elementar.

Demonstrație. Fie M un subgrup maximal al lui G . Deoarece $M < G$, avem, conform corolarului $M < N_G(M)$ și, deoarece M este maximal, avem $N_G(M) = G$, deci $M \trianglelefteq G$. Grupul factor G/M este atunci un p -grup finit care nu are nici un subgrup propriu, de unde rezultă că $|G/M| = p$.

și G/M este ciclic, deci abelian. Pentru orice element $x \in G$, vom avea, în grupul factor G/M , $(xM)^p = 1$, deci $x^p \in M$. De asemenea, pentru orice două elemente $x, y \in G$, în grupul factor G/M avem $(xM)(yM) = (yM)(xM)$, deci $(xy)M = (yx)M$, $xyx^{-1}y^{-1} \in M$. Aceasta se întimplă pentru orice subgrup maximal M al lui G . Prin urmare, notind $F = F(G)$, avem $x^p \in F$ și $xyx^{-1}y^{-1} \in F$ pentru orice $x, y \in G$, ceea ce arată că $(xF)(yF) = (yF)(xF)$, deci G/F este abelian și $(xF)^p = 1$, deci G/F este abelian elementar.

Propoziția 6.23. Fie G un p -grup finit $F = F(G)$ și presupunem că $|G/F| = p^d$. Fie x_1, x_2, \dots, x_n elemente din G și pentru fiecare $i \in \{1, 2, \dots, n\}$, notăm $v_i = x_i F$. Atunci

i) $\langle x_1, x_2, \dots, x_n \rangle = G$ dacă și numai dacă $\langle v_1, v_2, \dots, v_n \rangle = G/F$ și, în acest caz, $n \geq d$;

ii) $\{x_1, x_2, \dots, x_n\}$ este un sistem de generatori minimal pentru G dacă și numai dacă $n = d$.

In particular, orice două sisteme de generatori minimale ale lui G au același număr de elemente.

Demonstrație. i) Dacă $\langle x_1, x_2, \dots, x_n \rangle = G$, rezultă în mod evident $\langle v_1, v_2, \dots, v_n \rangle = G/F$. Reciproc, presupunem că $\langle v_1, v_2, \dots, v_n \rangle = G/F$. Dacă $\langle x_1, x_2, \dots, x_n \rangle < G$, există un subgrup maximal M al lui G astfel ca $\langle x_1, x_2, \dots, x_n \rangle \leq M$; deoarece $F \leq M$ va rezulta $\langle v_1, v_2, \dots, v_n \rangle \leq M/F < G/F$, ceea ce contrazice faptul că $\langle v_1, v_2, \dots, v_n \rangle = G/F$. Prin urmare $\langle x_1, x_2, \dots, x_n \rangle = G$. Deoarece $\{v_1, v_2, \dots, v_n\}$ este un sistem de generatori al lui G/F există o submulțime a lui $\{v_1, v_2, \dots, v_n\}$ care este sistem de generatori minimal al lui G/F , și aceasta, conform lui 6.19, are exact d -elemente.

ii) În virtutea lui i), $\{x_1, x_2, \dots, x_n\}$ este sistem de generatori minimal pentru G dacă și numai dacă $\{v_1, v_2, \dots, v_n\}$ este sistem de generatori minimal pentru G/F , iar, conform lui 6.19, $\{v_1, v_2, \dots, v_n\}$ este sistem de generatori minimal pentru G/F dacă și numai dacă $n = d$.

§ 7. GRUPURI REZOLUBILE ȘI NILPOTENTE

Definiția 7.1. O serie $H = \{H_0, H_1, \dots, H_n\}$ a grupului G (vezi §3) se numește *serie normală* a lui G dacă toți termenii săi H_i , $i \in \{0, 1, \dots, n\}$, sunt subgrupuri normale ale lui G . În acest caz, factorul H_{i-1}/H_i al seriei H este un subgrup normal al lui G/H_i . Spunem că seria normală H este o *serie principală* a grupului G dacă pentru orice $i \in \{1, 2, \dots, n\}$, H_{i-1}/H_i este un subgrup normal minimal al grupului G/H_i .

Se poate vedea imediat că demonstrația făcută în lema 3.25 este valabilă dacă înlocuim cuvîntul serie de compozitie a lui G cu serie principală a lui G și, în particular, rezultă că teorema Jordan-Hölder rămîne adevarată pentru serii principale: orice două serii principale ale unui grup G sunt echivalente. Din teorema Jordan-Hölder rezultă că

lungimea unei serii principale a grupului G depinde numai de grupul G o vom numi lungimea principală a lui G și de asemenea că factorii unei serii principale a grupului G sunt unic determinați pînă la un izomorfism de grupul G și îi vom numi factorii principali ai lui G .

Evident, nu putem vorbi despre lungimea principală a lui G sau despre factorii principali ai lui G decît dacă grupul G are cel puțin o serie principală. Se poate vedea imediat că orice grup finit are cel puțin o serie principală.

Definiția 7.2. Reamintim (vezi § 3) că un subgrup H al lui G se numește *caracteristic* în G dacă pentru orice automorfism $\sigma \in \text{Aut}(G)$ avem $\sigma(H) = H$. Evident, subgrupurile caracteristice ale lui G sunt normale în G .

Un grup G se numește *caracteristic simplu* dacă $G \neq 1$ și 1 și G sunt singurele sale subgrupuri caracteristice.

Evident, grupurile simple sunt în mod automat caracteristic simple.

Propoziția 7.3. *Orice factor principal al unui grup G este grup caracteristic simplu.*

Demonstrație. Un factor principal al lui G este de forma H/K , unde H și K sunt subgrupuri normale ale lui G , $K \trianglelefteq H$, iar H/K este subgrup normal minimal al lui G/K . Evident, putem presupune $K=1$, astfel că H este un subgrup normal minimal al lui G . Atunci pentru orice subgrup caracteristic H' al lui H , avem, conform propoziției 3.2, H' normal în G și, deoarece H este normal minimal în G , rezultă $H'=1$ sau $H'=H$, astfel că H este caracteristic simplu.

Propoziția 7.4. *Un grup abelian finit, netrivial G , este caracteristic simplu dacă și numai dacă G este abelian elementar.*

Demonstrație. Presupunem că G este caracteristic simplu și fie p un divizor prim al ordinului lui G . Luăm

$$H = \{x \in G \mid x^p = 1\}.$$

Deoarece G este abelian, avem

$$x, y \in H \Rightarrow (xy)^p = x^p y^p = 1 \Rightarrow xy \in H,$$

ceea ce arată că H este un subgrup al lui G . În plus, în virtutea teoremei lui Cauchy, există un element $x \in G$ de ordin p ; atunci $1 \neq x \in H$, astfel că H este un subgrup netrivial al lui G . De asemenea, H este caracteristic în G deoarece pentru $\sigma \in \text{Aut}(G)$ avem:

$$x \in H \Rightarrow x^p = 1 \Rightarrow \sigma(x)^p = \sigma(x^p) = \sigma(1) = 1 \Rightarrow \sigma(x) \in H.$$

Rezultă $H=G$, deci $x^p=1$ pentru orice $x \in G$. Reciproc, presupunem că G este abelian elementar și fie p un număr prim astfel ca $x^p=1$ pentru orice $x \in G$. Să presupunem că $|G|=p^d$ și considerăm un element oarecare $x_1 \in G$, $x_1 \neq 1$. Alegem apoi un element $x_2 \in G$, $x_2 \notin \langle x_1 \rangle$, un

element $x_3 \in G$, $x_3 \notin \langle x_1, x_2 \rangle$ etc. Deoarece G este finit, există un număr natural $n \geq 1$, astfel ca $\langle x_1, x_2, \dots, x_n \rangle = G$ și, în plus, $x_{i+1} \notin \langle x_1, x_2, \dots, x_i \rangle$ pentru orice $i \in \{1, 2, \dots, n-1\}$. Atunci $\{x_1, x_2, \dots, x_n\}$ este un sistem de generatori minimal al lui G . Într-adevăr, avem $x_n \notin \langle x_1, \dots, x_{n-1} \rangle$ și putem demonstra că $x_1 \notin \langle x_2, \dots, x_n \rangle$, $x_2 \notin \langle x_1, x_3, \dots, x_n \rangle$ etc. De exemplu, dacă presupunem $x_1 \in \langle x_2, \dots, x_n \rangle$ avem $x_1 = x_2^{a_2} \dots x_n^{a_n}$ unde $a_2, \dots, a_n \in \mathbb{Z}$. Dacă $p \mid a_n$, atunci $x_n^{a_n} = 1$, astfel că putem presupune $x_1 = x_2^{a_2} \dots x_k^{a_k}$, $k \leq n$ și $p \nmid a_k$. Atunci $x_k^{a_k} \in \langle x_1, x_2, \dots, x_{k-1} \rangle$ și, deoarece $p \nmid a_k$, $\langle x_k \rangle = \langle x_k^{a_k} \rangle \leq \langle x_1, x_2, \dots, x_{k-1} \rangle$, deci $x_k \in \langle x_1, x_2, \dots, x_{k-1} \rangle$, ceea ce contrazice alegerea lui x_k . Deoarece $\{x_1, x_2, \dots, x_n\}$ este sistem de generatori minimal, rezultă $n=d$. Acum presupunem că H este un subgrup al lui G , propriu și netrivial. Alegem un element $x_1 \in H$, $x_1 \neq 1$ și un element $y_1 \in G$, $y_1 \notin H$. Conform celor de mai sus, există elemente $x_2, \dots, x_d, y_2, \dots, y_d$ în G astfel că $\{x_1, x_2, \dots, x_d\}$ și $\{y_1, y_2, \dots, y_d\}$ să fie sisteme de generatori minime pentru G . În virtutea propoziției 6.19, putem defini aplicația $\sigma: G \rightarrow G$ prin

$$\sigma(x_1^{r_1} x_2^{r_2} \dots x_d^{r_d}) = y_1^{r_1} y_2^{r_2} \dots y_d^{r_d}$$

pentru orice $r_1, r_2, \dots, r_d \in \mathbb{Z}$ cu $0 \leq r_i < p$, $i \in \{1, 2, \dots, d\}$. În plus este clar că σ este un automorfism al lui G . Deoarece $x_1 \in H$ și $\sigma(x_1) = y_1 \notin H$, rezultă că H nu este subgrup caracteristic în G . Prin urmare grupul G este caracteristic simplu.

Definiția 7.5. O serie $\mathbf{H} = \{H_0, H_1, \dots, H_n\}$ a unui grup G se numește serie centrală dacă \mathbf{H} este o serie normală și, pentru orice $i \in \{1, 2, \dots, n\}$, avem $H_{i-1}/H_i \leq Z(G/H_i)$. Grupul G se numește nilpotent dacă G are cel puțin o serie centrală.

O serie $\mathbf{H} = \{H_0, H_1, \dots, H_n\}$ a grupului G se numește abeliană dacă toți factorii săi H_{i-1}/H_i , $i \in \{1, 2, \dots, n\}$, sunt grupuri abeliene. Grupul G se numește rezolubil dacă G are cel puțin o serie abeliană.

Observații și exemple. Deoarece, evident, orice serie centrală este abeliană, rezultă că orice grup nilpotent este rezolubil.

Orice serie a unui grup abelian G , de exemplu seria $\{G, 1\}$, este evident centrală, astfel că orice grup abelian este nilpotent.

Dacă G este un grup simplu, singura serie a lui G este $\{G, 1\}$ și aceasta nu este abeliană dacă G nu este abelian. Prin urmare grupurile simple neabeliene nu sunt grupuri rezolubile.

Dacă pentru un grup netrivial G avem $Z(G) = 1$, atunci pentru o serie centrală $\mathbf{H} = \{H_0, H_1, \dots, H_n\}$ a lui G va trebui să avem $H_n = 1$, $H_{n-1} \leq Z(G) = 1$, $H_{n-2} \leq Z(G) = 1$, astfel că G nu este grup nilpotent. Se poate verifica ușor că $Z(S_3) = 1$. Prin urmare grupul simetric S_3 nu este nilpotent.

Grupul S_3 este însă rezolubil deoarece seria $1 \trianglelefteq A_3 \trianglelefteq S_3$ a lui S_3 este evident abeliană.

Definiția 7.6. Fie G un grup. Se numește *comutatorul elementelor* g_1 și g_2 din G elementul

$$[g_1, g_2] = g_1 g_2 g_1^{-1} g_2^{-1}.$$

Dacă H și K sunt două subgrupuri ale lui G , se numește comutatorul lui H și K subgrupul $[H, K]$ al lui G generat de toți comutatorii $[h, k]$, $h \in H$, $k \in K$.

Deoarece avem

$$[h, k]^{-1} = (h k h^{-1} k^{-1})^{-1} = khk^{-1}h^{-1} = [k, h]$$

comutatorul $[H, K]$ coincide cu mulțimea tuturor produselor de comutatori de elemente din H și K sau din K și H .

În particular, subgrupul $[G, G]$ coincide cu mulțimea tuturor produselor de comutatori de elemente din G . Subgrupul $[G, G]$ se notează adesea cu G' și se numește *subgrupul derivat* (sau *subgrupul comutator*) al lui G .

Propoziția 7.7. *Subgrupul derivat G' al lui G este caracteristic în G și, pentru orice subgrup normal H al lui G , avem G/H abelian $\Leftrightarrow G' \leqslant H$.*

Demonstrație. Fie $\sigma \in \text{Aut}(G)$. Pentru orice două elemente $g_1, g_2 \in G$ avem

$$\begin{aligned} \sigma([g_1, g_2]) &= \sigma(g_1 g_2 g_1^{-1} g_2^{-1}) = \\ &= \sigma(g_1) \sigma(g_2) \sigma(g_1)^{-1} \sigma(g_2)^{-1} = [\sigma(g_1), \sigma(g_2)] \in G'. \end{aligned}$$

Deoarece orice element din G' este un produs de comutatori, avem $\sigma(G') \leqslant G'$ astfel că G' este caracteristic în G . Acum fie H un subgrup normal al lui G . Pentru orice două elemente $x, y \in G$ avem, în grupul factor G/H

$$\begin{aligned} (xH)(yH) &= (yH)(xH) \Leftrightarrow (xy)H = (yx)H \\ &\Leftrightarrow (xy)(yx)^{-1} \in H \Leftrightarrow [x, y] \in H \end{aligned}$$

astfel că G/H este abelian dacă și numai dacă $[x, y] \in H$ pentru orice $x, y \in G$, adică dacă și numai dacă $G' \leqslant H$.

Propoziția 7.8. O serie:

$$1 = H_n \trianglelefteq H_{n-1} \trianglelefteq \dots \trianglelefteq H_1 \trianglelefteq H_0 = G$$

a grupului G este serie centrală dacă și numai dacă pentru orice $i \in \{1, 2, \dots, n\}$ avem:

$$[H_{i-1}, G] \leqslant H_i.$$

Demonstrație. Presupunem că seria dată este centrală, astfel că pentru orice $i \in \{1, 2, \dots, n\}$ avem $H_i \trianglelefteq G$ și $H_{i-1}/H_i \leqslant Z(G/H_i)$. Atunci pentru orice $x \in H_{i-1}$ și $y \in G$, avem

$$(xH_i)(yH_i) = (yH_i)(xH_i).$$

adică $(xy)H_i = (yx)H_i$, ceea ce evident implică $[x, y] \in H_i$, deci $[H_{i-1}, G] \leqslant H_i$. Reciproc presupunem $[H_{i-1}, G] \leqslant H_i$ pentru orice $i \in \{1, 2, \dots, n\}$. Atunci, pentru orice $x \in H_{i-1}$ și $y \in G$, avem

$$x(yxy^{-1})^{-1} = [x, y] \in H_i.$$

În particular, pentru orice $x \in H_i \leqslant H_{i-1}$, avem $x(yxy^{-1})^{-1} \in H_i$, de unde rezultă $(yxy^{-1})^{-1} \in H_i$, deci $yxy^{-1} \in H_i$. Aceasta arată că $H_i \trianglelefteq G$. În plus, pentru $x \in H_{i-1}$ și $y \in G$

$$xyx^{-1}y^{-1} = [x, y] \in H_i$$

de unde rezultă

$$(xH_i)(yH_i) = (yH_i)(xH_i),$$

astfel că $H_{i-1}/H_i \leqslant Z(G/H_i)$.

Propoziția 7.9. Fie G un grup, $H \leqslant G$ și $K \trianglelefteq G$.

- i) Dacă G este nilpotent, atunci H și G/K sunt nilpotente.
- ii) Dacă G este rezolubil, atunci H și G/K sunt rezolubile.

Demonstrație. Fie

$$(1) \quad 1 = H_n \trianglelefteq H_{n-1} \trianglelefteq \dots \trianglelefteq H_1 \trianglelefteq H_0 = G$$

o serie a grupului G . Atunci

$$(2) \quad 1 = H_n \cap H \trianglelefteq H_{n-1} \cap H \trianglelefteq \dots \trianglelefteq H_1 \cap H \trianglelefteq H_0 \cap H = H$$

și

$$(3) \quad 1 = K/K = H_nK/K \trianglelefteq H_{n-1}K/K \trianglelefteq \dots \trianglelefteq H_1K/K \trianglelefteq H_0K/K = G/K$$

sunt serii ale lui H și respectiv G/K . Presupunem că G este nilpotent și că (1) este o serie centrală. Atunci, pentru orice $i \in \{1, 2, \dots, n\}$, avem, conform lui 7.8,

$$[H_{i-1}, G] \leqslant H_i$$

de unde rezultă evident:

$$[H_{i-1} \cap H, H] \leqslant [H_{i-1}, G] \cap H \leqslant H_i \cap H$$

și

$$[H_{i-1}K/K, G/K] \leqslant [H_{i-1}, G]K/K \leqslant H_iK/K.$$

În virtutea propoziției 7.8, serile (2) și (3) sunt centrale deci H și G/K sunt nilpotente. Presupunem acum că G este rezolubil și că seria (1) este o serie abeliană. În virtutea teoremulor de izomorfism avem:

$$\begin{aligned} H_{i-1} \cap K/H_i \cap K &= H_{i-1} \cap K/(H_{i-1} \cap K) \cap H_i \cong \\ &\cong (H_{i-1} \cap K)/H_i \leqslant H_{i-1}/H_i \end{aligned}$$

și deoarece H_{t-1}/H_t este abelian, rezultă $H_{t-1} \cap K/H_t \cap K$ abelian pentru orice $i \in \{1, 2, \dots, n\}$, astfel că seria (2) este abeliană și H este rezolubil. De asemenea avem:

$$\begin{aligned}(H_{t-1}K/K)/(H_tK/K) &\simeq H_{t-1}K/H_tK = H_{t-1}(H_tK)/H_tK \simeq \\ &\simeq H_{t-1}/H_{t-1} \cap H_tK \simeq (H_{t-1}/H_t)/(H_{t-1} \cap H_tK/H_t)\end{aligned}$$

și, deoarece H_{t-1}/H_t este abelian, rezultă $(H_{t-1}K/K)(H_tK/K)$ abelian pentru orice $i \in \{1, 2, \dots, n\}$, astfel că seria (3) este abeliană și G/K este rezolubil.

Propoziția 7.10. Fie G un grup și K un subgrup normal al lui G . Dacă K și G/K sunt grupuri rezolubile, atunci și G este rezolubil.

Demonstrație. Grupurile K și G/K fiind rezolubile, există serile abeliene

$$1 = K_m \trianglelefteq K_{m-1} \trianglelefteq \dots \trianglelefteq K_1 \trianglelefteq K_0 = K$$

$$1 = G/K = G_n/K \trianglelefteq G_{n-1}/K \trianglelefteq \dots \trianglelefteq G_1/K \trianglelefteq G_0/K = G/K$$

ale lui K și respectiv G/K . Atunci, evident

$$1 = K_m \trianglelefteq K_{m-1} \trianglelefteq \dots \trianglelefteq K_1 = K_0 = G_n \trianglelefteq G_{n-1} \trianglelefteq \dots \trianglelefteq G_1 \trianglelefteq G_0 = G$$

este o serie a lui G și deoarece

$$G_{t-1}/G_t \simeq (G_{t-1}/K)/(G_t/K)$$

pentru orice $i \in \{1, 2, \dots, n\}$, această serie este abeliană. Rezultă că G este rezolubil.

Corolarul 7.11. Fie G un grup și H, K subgrupuri normale ale lui G , rezolubile. Atunci HK este un subgrup normal al lui G rezolubil.

Demonstrație. Cunoaștem că $HK \trianglelefteq G$. Avem $HK/K \simeq H/H \cap K$ și deoarece H este rezolubil, propoziția 7.9 arată că $H/H \cap K$ este rezolubil deci și HK/K este rezolubil. Avem $K \trianglelefteq HK$ iar K și HK/K sunt grupuri rezolubile astfel că din propoziția 7.10 rezultă HK rezolubil.

Observație. Propoziția 7.10 nu rămâne adeverată pentru grupuri nilpotente. De exemplu, grupul simetric S_3 nu este nilpotent dar avem $A_3 \trianglelefteq S_3$, A_3 și S_3/A_3 nilpotente. Cu toate acestea enunțul corolarului 7.11 este adeverat pentru grupuri nilpotente. Însă demonstrația acestui fapt este mult mai complicată.

Definiția 7.12. Fie G un grup. Definim recursiv, pentru fiecare număr natural n , subgrupurile $G^{(n)}$ ale lui G astfel

$$G^{(0)} = G \text{ și } G^{(n+1)} = [G^{(n)}, G^{(n)}] = (G^{(n)})'.$$

În particular, $G^{(1)} = G'$ este subgrupul derivat al lui G .

Propoziția 7.13. Fie G un grup. Sunt adevărate următoarele afirmații:

(i) G este rezolubil dacă și numai dacă există un număr natural n astfel ca $G^{(n)}=1$.

(ii) Presupunem că G este rezolubil și fie n cel mai mic număr natural astfel ca $G^{(n)}=1$.

Atunci, pentru orice serie abeliană,

$$G = H_0 \triangleright H \triangleright \dots \triangleright H_r = 1,$$

avem $H_i \geq G^{(i)}$ pentru orice $i \in \{1, 2, \dots, r\}$ și în particular $r \geq n$.

Demonstrație. Dacă $G^{(n)}=1$ pentru un număr natural n , atunci

$$G = G^{(0)} \geq G^{(1)} \geq \dots \geq G^{(n)} = G,$$

este o serie abeliană a lui G în virtutea propoziției 7.7, astfel că G este rezolubil. Reciproc, presupunem că G este rezolubil și fie

$$G = H_0 \triangleright H_1 \triangleright \dots \triangleright H_r = 1$$

o serie abeliană a lui G . Avem $H_0 = G \geq G = G^{(0)}$ și dacă presupunem $H_i \geq G^{(i)}$, avem, deoarece H_i/H_{i+1} este abelian, $H_{i+1} \geq (H_i)' \geq (G^{(i)})' = G^{(i+1)}$, astfel că $H_i \geq G^{(i)}$ pentru orice $i \in \{0, 1, \dots, r\}$.

În particular, $1 = H_r \geq G^{(r)}$, deci $G^{(r)} = 1$. Cu aceasta, propoziția este demonstrată.

Definiția 7.14. Fie G un grup rezolubil și n cel mai mic număr natural astfel ca $G^{(n)}=1$. Numărul natural n se numește *lungimea derivată* a lui G , iar seria

$$G = G^{(0)} \triangleright G^{(1)} \triangleright \dots \triangleright G^{(n)} = 1$$

se numește *seria derivată* a lui G .

Se poate demonstra că pentru orice număr natural n există grupuri de lungime derivată egală cu n . Propoziția 7.13 arată că seria derivată a unui grup rezolubil G are cea mai rapidă descreștere printre toate seriile abeliene ale lui G . De asemenea se vede că deși grupurile rezolvabile au fost definite ca fiind grupuri ce au cel puțin o serie abeliană, ele au chiar o serie normală abeliană. Grupurile rezolvabile de lungime derivată egală cu 1 sunt exact grupurile abeliene netriviale.

Definiția 7.15. Fie G un grup. Definim recursiv, pentru fiecare număr natural n , subgrupurile $\Gamma_n(G)$ și $Z_n(G)$ ale lui G , astfel:

$$\Gamma_0(G) = G \text{ și } Z_0(G) = 1, \text{ iar } \Gamma_{n+1}(G) = [\Gamma_n(G), G] \text{ și}$$

$$Z_{n+1}(G)/Z_n(G) = Z(G/Z_n(G)).$$

Propoziția 7.16. Fie G un grup. Următoarele afirmații sunt echivalente:

a) G este nilpotent.

b) Există un număr natural n astfel ca $\Gamma_n(G) = 1$.

c) Există un număr natural n astfel ca $Z_n(G) = G$.
În plus, presupunem că G este nilpotent și fie

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \dots \trianglelefteq H_r = G$$

o serie centrală a lui G . Atunci

$$\Gamma_{r-i}(G) \leq H_i \leq Z_i(G)$$

pentru orice $i \in \{0, 1, \dots, r\}$ și cel mai mic număr natural c astfel încât $\Gamma_c(G) = 1$ este egal cu cel mai mic număr natural c astfel încât $Z_c(G) = G$.

Demonstrație. Presupunem că $\Gamma_n(G) = 1$ pentru un număr natural n . Atunci

$$(1) \quad G = \Gamma_0(G) \geq \Gamma_1(G) \geq \dots \geq \Gamma_n(G) = 1$$

este o serie centrală a lui G . Într-adevăr, $\Gamma_0(G) = G$ este caracteristic în G și dacă presupunem $\Gamma_i(G)$ caracteristic în G , avem, pentru $x \in \Gamma_i(G)$, $y \in G$, $\sigma \in \text{Aut}(G)$,

$$xyx^{-1}y^{-1} = x(yxy^{-1})^{-1} \in \Gamma_i(G),$$

deci

$$\Gamma_{i+1}(G) = [\Gamma_i(G), G] \leq \Gamma_i(G)$$

și

$$\begin{aligned} \sigma(xyx^{-1}y^{-1}) &= \sigma(x)\sigma(y)\sigma(x)^{-1}\sigma(y)^{-1} = \\ &= [\sigma(x), \sigma(y)] \text{ cu } \sigma(x) \in \Gamma_i(G), \end{aligned}$$

ceea ce arată că $\Gamma_{i+1}(G)$ este caracteristic în G .

Astfel pentru orice număr natural i , avem $\Gamma_{i+1}(G) \leq \Gamma_i(G)$ și $\Gamma_i(G)$ este caracteristic în G ; în particular, $\Gamma_i(G)$ este normal în G și (1) este o serie normală a lui G . Pentru $x \in \Gamma_{i+1}(G)$, $y \in G$ avem $xyx^{-1}y^{-1} \in \Gamma_{i+1}(G) \leq \Gamma_i(G)$, ceea ce arată că $xy\Gamma_i(G) = yx\Gamma_i(G)$, deci $\Gamma_{i+1}(G)/\Gamma_i(G) \leq Z(G/\Gamma_i(G))$ și (1) este o serie centrală. Astfel G este un grup nilpotent. Presupunem acum că $Z_n(G) = G$ pentru un număr natural n . Atunci

$$1 = Z_0(G) \trianglelefteq Z_1(G) \trianglelefteq \dots \trianglelefteq Z_n(G) = G$$

este o serie centrală a lui G . Aceasta este evident prin însăși definiția subgrupurilor $Z_n(G)$, astfel că și în acest caz grupul G este nilpotent.

Presupunem în final că G este nilpotent și fie

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \dots \trianglelefteq H_r = G$$

o serie centrală a lui G . Avem $H_0 = 1 \leq Z_0(G)$ și, dacă presupunem $H_i \leq Z_i(G)$, vom avea pentru $x \in H_{i+1}$, $y \in G$, $[x, y] = xyx^{-1}y^{-1} \in H_i$, deoarece $H_{i+1}/H_i \leq Z(G/H_i)$ deci $[x, y] \in Z_i(G)$. ceea ce arată că

$$H_{i+1}Z_i(G)/Z_i(G) \leq Z(G/Z_i(G)) = Z_{i+1}(G)/Z_i(G)$$

și prin urmare

$$H_{t+1} \leq H_t Z_t(G) \leq Z_{t+1}(G).$$

Astfel $H_i \trianglelefteq Z_t(G)$ pentru orice $i \in \{0, 1, \dots, r\}$. În particular, avem $G = H_r \trianglelefteq Z_r(G)$, deci $Z_r(G) = G$. Avem $\Gamma_0(G) = G \leq H_r$, și dacă presupunem $\Gamma_j(G) \leq H_{r-j}$, atunci aplicând propoziția 7.8 rezultă:

$$\Gamma_{j+1}(G) = [\Gamma_j(G), G] \leq [H_{r-j}, G] \leq H_{r-(j+1)}.$$

Prin urmare $\Gamma_j(G) \leq H_{r-j}$, pentru orice $j \in \{0, 1, \dots, r\}$. În particular $\Gamma_r(G) \leq H_0 = 1$, deci, $\Gamma_r(G) = 1$. Acum fie că cel mai mic număr întreg astfel ca $Z_c(G) = G$. Aplicând incluziunile obținute mai sus seriei centrale

$$1 = Z_0(G) \trianglelefteq Z_1(G) \trianglelefteq \dots \trianglelefteq Z_c(G) = G,$$

obținem $\Gamma_j(G) \leq Z_{c-j}(G)$ pentru orice $j \in \{0, 1, \dots, c\}$, astfel că $\Gamma_c(G) = 1$. Ultima aserțiune a propoziției noastre va fi demonstrată dacă arătăm că pentru $c > 1$ avem $\Gamma_{c-1}(G) \neq 1$. Dacă presupunem prin absurd că $\Gamma_{c-1}(G) = 1$, aplicând incluziunile de mai sus seriei centrale

$$G = \Gamma_0(G) \trianglerighteq \Gamma_1(G) \trianglerighteq \dots \trianglerighteq \Gamma_{c-1}(G) = 1$$

obținem $\Gamma_{c-(j+1)}(G) \leq Z_j(G)$ și, în particular, $G = \Gamma_0(G) \leq Z_{c-1}(G)$, deci $G = Z_{c-1}(G)$ contrar alegerei lui c.

Definiția 7.17. Fie G un grup nilpotent și c cel mai mic număr natural astfel ca $\Gamma_c(G) = 1$; sau, echivalent, $Z_c(G) = G$. Atunci c se numește *clasa de nilpotență* a lui G . Seria

$$G = \Gamma_0(G) \trianglerighteq \Gamma_1(G) \trianglerighteq \dots \trianglerighteq \Gamma_c(G) = 1,$$

se numește *seria centrală inferioară* a lui G iar seria

$$1 = Z_0(G) \trianglelefteq Z_1(G) \trianglelefteq \dots \trianglelefteq Z_c(G) = G$$

se numește *seria centrală superioară* a lui G .

Propoziția 7.16 arată că seria centrală inferioară a lui G are cea mai rapidă descreștere printre toate seriile centrale ale lui G iar seria centrală superioară are cea mai rapidă creștere. Grupurile nilpotente de clasă 1 sunt exact grupurile abeliene netriviale.

P opoziția 7.18. i). Orice p -grup G este nilpotent și dacă $|G| = p^n$ cu $n \geq 2$, atunci clasa de nilpotență a lui G este cel mult $n - 1$.

ii) Grupul *diedral* D_m , unde $m = 2^n$, $n \geq 2$, este nilpotent și are clasa de nilpotență egală cu n .

Demonstrație. i) Conform propoziției 5.24, avem $Z_1(G) = Z(G) \neq 1$, astfel că $|Z_1(G)| = p^{n_1}$ cu $0 < n_1 < n$. Dacă $Z_1(G) \neq G$, avem $Z_2(G)/Z_1(G) = Z(G/Z_1(G)) \neq 1$, astfel că $Z_2(G) = p^{n_2}$ cu $0 < n_1 < n_2 \leq n$. În general dacă $Z_{t-1}(G) \neq G$, avem $Z_t(G)/Z_{t-1}(G) = Z(G/Z_{t-1}(G)) \neq 1$, astfel că $|Z_t(G)| = p^n$

cu $0 < n_1 < \dots < n_{t-1} < n_t \leq n$. Evident va exista un număr natural k astfel încât $0 < n_1 < \dots < n_k = n$ și în această situație G este nilpotent de clasă k . Evident avem $k \leq n$. Presupunem $n \geq 2$ și $k = n$; atunci $n_i = i$, astfel că $|Z_i(G)| = p^i$ pentru orice $i \in \{1, 2, \dots, n\}$. Deoarece $|G/Z_{n-2}(G)| = p^2$, $G/Z_{n-2}(G)$ este grup abelian (vezi corolarul 5.25), astfel că $Z_{n-1}(G)/Z_{n-2}(G) = Z(G/Z_{n-2}(G)) = G/Z_{n-2}(G)$, adică $Z_{n-1}(G) = G$, ceea ce evident nu se poate. Prin urmare G este nilpotent de clasă $k \leq n - 1$.

ii) Deoarece $|D_m| = 2m = 2^{s+1}$, D_m este nilpotent de clasă cel mult n . Acum, în general, să presupunem că m este par. Avem $G = D_m = \langle \rho, \epsilon \rangle$ cu $\rho^m = 1$, $\epsilon^2 = 1$, $\epsilon\rho = \rho^{-1}\epsilon = \rho^{m-1}\epsilon$. Rezultă $\epsilon\rho^i = \rho^{m-i}\epsilon$ pentru orice număr natural i și, în particular, $\epsilon\rho^{\frac{m}{2}} = \rho^{\frac{m-m}{2}}\epsilon = \rho^{\frac{m}{2}}\epsilon$, ceea ce arată că $\rho^{\frac{m}{2}} \in Z(G)$. Evident avem $Z(G) = G$ pentru $m = 2$ și $Z(G) = \{1, \rho^{\frac{m}{2}}\}$, deci $|Z(G)| = 2$, pentru $m > 2$. Pentru $m > 2$, dacă notăm $\tilde{G} = G/Z(G)$, avem $\tilde{G} = \langle \tilde{\rho}, \tilde{\epsilon} \rangle$ unde $\tilde{\rho} = \rho Z(G)$, $\tilde{\epsilon} = \epsilon Z(G)$, $\tilde{\rho}^{\frac{m}{2}} = 1$, $\tilde{\epsilon}^2 = 1$, $\tilde{\epsilon}\tilde{\rho} = \tilde{\rho}^{-1}\tilde{\epsilon}$; deoarece $|\tilde{G}| = 2 \cdot \frac{m}{2}$, avem $\tilde{G} \cong D_{\frac{m}{2}}$. Acum, să revenim la cazul din enunț, anume $m = 2^n$, cu $n \geq 2$. Avem $|Z_1(G)| = 2$ și deoarece $G/Z_1(G) \cong D_{2^{n-1}}$, $|Z_2(G)/Z_1(G)| = |Z(G/Z_1(G))| = 4$ sau 2 după cum $n - 1 = 1$ sau $n - 1 \geq 2$, deci $|Z_2(G)| = 8$ sau 4, după cum $n - 1 = 1$ sau $n - 1 \geq 2$. În general $G/Z_i(G) \cong D_{2^{n-i}}$ deci $|Z_{i+1}(G)/Z_i(G)| = |Z(G/Z_i(G))| = 4$ sau 2 după cum $n - i = 1$ sau $n - i \geq 2$ deci $|Z_{i+1}(G)| = 4 |Z_i(G)| = 2^{i+2}$ sau $|Z_{i+1}(G)| = 2 |Z_i(G)| = 2^{i+1}$ după cum $n - i = 1$ sau $n - i \geq 2$. În particular, avem $|Z_{n-1}(G)| = 2^{n-1}$ și $|Z_n(G)| = 2^{n+1}$, deci $Z_{n-1}(G) \neq G$ și $Z_n(G) = G$. Aceasta arată că clasa de nilpotență a lui D_{2^n} este egală cu n .

Propoziția 7.19. Fie G un grup finit. Următoarele afirmații sunt echivalente:

- a) G este rezolubil;
- b) Orice factor de compozиie al lui G are ordinul prim;
- c) Orice factor principal al lui G este abelian elementar.

Demonstrație. Presupunem că G este rezolubil. Un factor de compozиie al lui G este de forma H/J , unde $J \trianglelefteq H \trianglelefteq G$; în plus H/J este grup simplu. În virtutea propoziției 7.9, H/J este grup rezolubil. Deoarece grupurile simple neabeliene nu sunt rezolubile, rezultă că H/J este grup simplu abelian, deci ordinul lui H/J este un număr prim. Fie acum n lungimea derivată a lui G și considerăm seria derivată:

$$1 = G^{(n)} \trianglelefteq G^{(n-1)} \trianglelefteq \dots \trianglelefteq G^{(1)} \trianglelefteq G.$$

Aceasta este o serie normală a lui G și, deoarece G este finit, există o serie principală \mathbf{H} a lui G :

$$1 = H_m \trianglelefteq H_{m-1} \trianglelefteq \dots \trianglelefteq H_1 \trianglelefteq G$$

astfel încit toți termenii seriei derivate să fie termeni ai seriei **H**. Deoarece seria derivată are toți factorii grupuri abeliene, rezultă că seria **H** are toți factorii grupuri abeliene. Orice factor principal al grupului *G* este izomorf cu un factor al seriei **H**, deci este grup abelian, și deci, în virtutea propozițiilor 7.3 și 7.4, el este grup abelian elementar. Reciproc, să presupunem că factorii de compoziție ai grupului *G* au ordinul prim; în particular ei sunt grupuri abeliene astfel că orice serie de compoziție a lui *G* este abeliană, deci *G* este rezolubil. Analog dacă factorii principali ai lui *G* sunt grupuri abeliene elementare, orice serie principală a lui *G* este abeliană și *G* este rezolubil.

Observație. Propoziția 7.19 arată că un grup finit rezolubil are o serie cu toți factorii ciclici. Acest lucru nu este adevărat în general pentru grupuri rezolubile infinite. De asemenea nu este adevărat în general că un grup finit rezolubil are o serie normală cu toți factorii ciclici.

Definiția 7.20. Un subgrup *H* al unui grup *G* se numește *subnormal* în *G* dacă există un număr natural *n* și subgrupurile *H*₀, *H*₁, ..., *H*_{*n*} ale lui *G* astfel că:

$$H = H_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \dots \trianglelefteq H_{n-1} \trianglelefteq H_n = G.$$

Propoziția 7.21. Orice subgrup al unui grup nilpotent *G* este subnormal în *G*.

Demonstrație. Fie *c* clasa de nilpotență a lui *G* și, pentru fiecare *i* ∈ {0, 1, ..., *c*}, fie *Z*_{*i*} = *Z*_{*i*}(*G*), astfel că

$$1 = Z_0 \trianglelefteq Z_1 \trianglelefteq \dots \trianglelefteq Z_c = G.$$

Atunci

$$H = HZ_0 \leqslant HZ_1 \leqslant \dots \leqslant HZ_c = G.$$

Pe baza faptului că *Z*_{*i*+1}/*Z*_{*i*} = *Z*(*G*/*Z*_{*i*}) rezultă *HZ*_{*i*} ⊲ *HZ*_{*i*+1} pentru orice *i* ∈ {0, 1, ..., *c*-1}. Într-adevăr, pentru *h*, *h'* ∈ *H*, *z*_{*i*} ∈ *Z*_{*i*}, *z*_{*i*+1} ∈ *Z*_{*i*+1}, avem

$$(h'z_{i+1})(hz_i)(h'z_{i+1})^{-1} = h'z_{i+1}(hz_i)z_{i+1}h'^{-1}$$

dar

$$z_{i+1}(hz_i)z_{i+1}(hz_i)^{-1} \in Z_i,$$

deci

$$z_{i+1}(hz_i)z_{i+1} = z'_i(hz_i) \text{ cu } z'_i \in Z_i.$$

Prin urmare $(h'z_{i+1})(hz_i)(h'z_{i+1})^{-1} = h'z'_i(hz_i)h'^{-1} \in HZ_i$.

Propoziția 7.22. Fie *H* și *K* subgrupuri ale unui grup *G* și considerăm aplicația $f: H \times K \rightarrow G$ definită prin $f(h, k) = hk$. Atunci:

- i) f este aplicație surjectivă dacă și numai dacă $HK=G$.
- ii) f este aplicație injectivă dacă și numai dacă $H \cap K=1$.
- iii) f este morfism de grupuri dacă și numai dacă pentru orice $h \in H$, $k \in K$, avem $hk=f(h, k)$.

Demonstrație. i) Rezultă imediat din faptul că

$$\{f(h, k) \mid h \in H, k \in K\} = HK.$$

ii) Dacă f este aplicație injectivă și $x \in H \cap K$, avem $f(x, 1)=x=f(1, x)$ astfel că $(x, 1)=(1, x)$, deci $x=1$. Reciproc, dacă $H \cap K=1$ și $f(h, k)=f(h', k')$, rezultă $hk=h'k'$, deci $h^{-1}h=k'k^{-1} \in H \cap K=1$, adică $h=h'$, $k=k'$, deci $(h, k)=(h', k')$.

iii) Dacă f este morfism de grupuri pentru $h \in H$, $k \in K$, avem: $hk=f(h, 1)f(1, k)=f((h, 1)(1, k))=f(h, k)=f((1, k)(h, 1))=f(1, k)f(h, 1)=kh$. Reciproc, dacă $hk=kh$ pentru orice $h \in H$, $k \in K$, avem pentru $h, h' \in H$ și $k, k' \in K$:

$$\begin{aligned} f((h, k)(h', k')) &= f(hh', kk') = (hh')(kk') = \\ &= h(h'k)k' = h(kh')k' = (hk)(h'k') = f(h, k)f(h', k'), \end{aligned}$$

deci f este morfism de grupuri.

Definiția 7.23. Fie H și K subgrupuri ale unui grup G . Dacă aplicația $f: H \times K \rightarrow G$, definită prin $f(h, k)=hk$, este un izomorfism de grupuri, spunem că G este produsul direct al subgrupurilor H și K și scriem $G=H \times K$.

Propoziția 7.22 arată că egalitatea $G=H \times K$ este echivalentă cu $HK=G$, $H \cap K=1$ și $hk=kh$ pentru orice $h \in H$, $k \in K$. Produsul direct obișnuit $H \times K$ este egal cu produsul direct al subgrupurilor H' și K' : $H \times K=H' \times K'$, unde $H'=\{(h, 1) \mid h \in H\} \leqslant H \times K$ și $K'=\{(1, k) \mid k \in K\} \leqslant H \times K$ sunt subgrupuri ale lui $H \times K$ izomorfe cu H și respectiv cu K .

Definiția se poate generaliza pentru un număr oarecare H_1, H_2, \dots, H_n de subgrupuri ale lui G . Grupul G este produsul direct al subgrupurilor H_1, H_2, \dots, H_n dacă aplicația $f: H_1 \times H_2 \times \dots \times H_n \rightarrow G$ definită prin $f(h_1, h_2, \dots, h_n)=h_1h_2 \dots h_n$ este un izomorfism de grupuri și, în acest caz, scriem $G=H_1 \times H_2 \times \dots \times H_n$. Propoziția 7.22 se poate generaliza imediat, și anume $G=H_1 \times \dots \times H_n$ dacă și numai dacă $H_1H_2 \dots H_n=G$, $H_i \cap \prod_{j \neq i} H_j=1$ pentru orice $j \in \{1, 2, \dots, n\}$ (unde $\prod_{j \neq i} H_j=H_1 \dots H_{i-1}H_{i+1} \dots H_n$) și $h_ih_j=h_jh_i$ pentru orice $i, j \in \{1, 2, \dots, n\}$ și $i \neq j$.

Propoziția 7.24. Fie H și K subgrupuri ale unui grup G . Avem $G=H \times K$ dacă și numai dacă $HK=G$, $H \cap K=1$ iar H și K sunt subgrupuri normale ale lui G .

Demonstratie. Presupunem $G = H \times K$, astfel că $HK = G$ și $H \cap K = 1$. Să demonstrăm că H este normal în G . Pentru $h \in H$ și $g = h'k' \in HK = G$, $h' \in H$, $k' \in K$ avem $h'h = hk'$ deci

$$ghg^{-1} = (h'k') h(h'k')^{-1} = h'k' \cdot hk'^{-1}k'^{-1} = h'hk'k'^{-1} = h'hh'^{-1} \in H$$

ceea ce arată că $H \trianglelefteq G$. Analog avem $K \trianglelefteq G$. Reciproc, să presupunem că $HK = G$, $H \cap K = 1$, $H \trianglelefteq G$ și $K \trianglelefteq G$. Pentru $h \in H$, $k \in K$, avem $hkh^{-1} \in K$, deci $hkh^{-1}k^{-1} \in K$ și $kh^{-1}k^{-1} \in H$ deci $hkh^{-1}k^{-1} \in H$; astfel $hkh^{-1}k^{-1} \in H \cap K = 1$, adică $hk = kh$.

Observație. Propoziția 7.24 se poate generaliza imediat la un număr oricare de subgrupuri. Dacă H_1, H_2, \dots, H_n sunt subgrupuri ale unui grup G , avem $G = H_1 \times H_2 \times \dots \times H_n$ dacă și numai dacă $H_1 H_2 \dots H_n = G$, $H_i \prod H_j = 1$, pentru orice $i \in \{1, 2, \dots, n\}$ și $H_i \trianglelefteq G$ pentru orice $i \in \{1, 2, \dots, n\}$.

Propoziția 7.25. Dacă H și K sunt subgrupuri nilpotente ale unui grup G și $G = H \times K$, atunci G este nilpotent. Mai general, dacă H_1, H_2, \dots, H_n sunt subgrupuri nilpotente ale lui G și $G = H_1 \times H_2 \times \dots \times H_n$, atunci G este nilpotent.

Demonstratie. Este suficient să presupunem H și K nilpotente și $G = H \times K$. Considerăm seriile centrale

$$1 = H_0 \trianglelefteq H_1 \trianglelefteq \dots \trianglelefteq H_m = H$$

$$1 = K_0 \trianglelefteq K_1 \trianglelefteq \dots \trianglelefteq K_n = K$$

ale lui H și K respectiv, putem presupune, fără a restrînge generalitatea, că $m = n$. Deoarece evident

$$[H_i \times K_i, G] = [H_i, H] \times [K_i, K]$$

deducem din propoziția 7.8,

$$[H_i \times K_i, G] \leq H_{i-1} \times K_{i-1}$$

pentru orice $i \in \{1, 2, \dots, n\}$ ceea ce, conform tot propoziției 7.8, arată că

$$1 = H_0 \times K_0 \trianglelefteq H_1 \times K_1 \trianglelefteq \dots \trianglelefteq H_n \times K_n = H \times K = G$$

este o serie centrală a lui G . Afirmația în cazul general rezultă imediat din faptul că

$$H_1 \times H_2 \times \dots \times H_n \simeq (H_1 \times \dots \times H_{n-1}) \times H_n,$$

prin inducție după n .

Propoziția 7.26. Fie G un grup finit.

Următoarele afirmații sunt echivalente;

a) G este nilpotent;

- b) Orice subgrup al lui G este subnormal;
c) Pentru orice subgrup propriu H al lui G avem $H \triangleleft N_G(H)$;
d) Orice subgrup maxim al lui G este normal;
e) $G' \leq F(G)$, unde $F(G)$ este subgrupul Frattini al lui G ;
f) Orice subgrup Sylow al lui G este normal;
g) G este izomorf cu un produs direct de grupuri finite de ordin putere de prim.

Demonstrație. a) \Rightarrow b) rezultă din propoziția 7.21.

b) \Rightarrow c) Fie $H \triangleleft G$. Deoarece H este subnormal există un subgrup H_1 al lui G astfel ca $H \triangleleft H_1$. Atunci $H \triangleleft H_1 \trianglelefteq N_G(H)$.

c) \Rightarrow d) Fie M un subgrup maximal al lui G . Deoarece $M \trianglelefteq G$ avem $M < N_G(M) \trianglelefteq G$ și din maximalitatea lui M rezultă $N_G(M) = G$, deci $M \trianglelefteq G$.

d) \Rightarrow e) Fie M un subgrup maximal al lui G . Atunci $M \trianglelefteq G$ și grupul factor G/M este ciclic de ordin prim. În particular, G/M este abelian astfel că prin propoziția 7.7 avem $G' \leq M$. Prin urmare $G' \leq F(G)$ ($F(G)$ este, prin definiție, intersecția tuturor subgrupurilor maximale ale lui G).

e) \Rightarrow d). Fie M un subgrup maximal al lui G . Atunci $G' \leq F(G) \leq M$, astfel că M/G' este subgrup al grupului abelian G/G' ; rezultă $M/G' \trianglelefteq G/G'$, deci $M \trianglelefteq G$.

d) \Rightarrow f). Fie P un p -subgrup Sylow al lui G . Presupunem că $N_G(P) < G$. Atunci, există un subgrup maximal M al lui G astfel ca $N_G(P) \trianglelefteq M$. Atunci, în virtutea lui 6.13 avem $N_G(M) = M$, ceea ce contrazice faptul că $M \trianglelefteq G$. Prin urmare, $N_G(P) = G$, deci $P \trianglelefteq G$.

f) \Rightarrow g). Fie p_1, p_2, \dots, p_s mulțimea divizorilor primi ai lui $|G|$. Pentru fiecare $i \in \{1, 2, \dots, s\}$ fie P_i un p_i -subgrup Sylow al lui G . Avem $P_i \trianglelefteq G$, $|P_i| = p_i^{n_i}$ și $|G| = p_1^{n_1} p_2^{n_2} \dots p_s^{n_s}$. Pentru fiecare $m \in \{1, 2, \dots, s\}$ notăm $I_m = P_1 P_2 \dots P_m \trianglelefteq G$. Vom demonstra prin inducție după m că $|I_m| = p_1^{n_1} p_2^{n_2} \dots p_m^{n_m}$. Pentru $m=1$ avem $I_1 = P_1$, deci $|I_1| = p_1^{n_1}$. Presupunem $m > 1$ și că $|I_{m-1}| = p_1^{n_1} \dots p_{m-1}^{n_{m-1}}$. În virtutea teoremei lui Lagrange avem $P_m \cap I_{m-1} = 1$, și, deoarece $I_m = I_{m-1} P_m$, avem

$$|I_m| = |I_{m-1} P_m| = \frac{|I_{m-1}| \cdot |P_m|}{|I_{m-1} \cap P_m|} = p_1^{n_1} p_2^{n_2} \dots p_m^{n_m}.$$

În particular $|I_s| = p_1^{n_1} p_2^{n_2} \dots p_s^{n_s} = |G|$, deci $I_s = G$. Deoarece $I_{m-1} \cap P_m = 1$ pentru orice $m \in \{2, \dots, s\}$, rezultă, conform observației de la propoziția 7.24, că

$$G = P_1 \times P_2 \times \dots \times P_s.$$

g) \Rightarrow f). Rezultă din propoziția 7.18, aplicând propoziția 7.25.

EXERCITII

1. Să se demonstreze că orice grup infinit G are o infinitate de subgrupuri.

Indicație. Dacă există un element $x \in G$ de ordin infinit, atunci $\langle x \rangle$ are o infinitate de subgrupuri; dacă orice element $x \in G$ are ordin finit, atunci reuniunea $\langle x_1 \rangle \cup \langle x_2 \rangle \cup \dots \cup \langle x_n \rangle$ este mulțime finită pentru orice n elemente $x_1, x_2, \dots, x_n \in G$.

2. Fie G un grup și $K \leq H \leq G$. Să se demonstreze că $|G: K|$ este finit dacă și numai dacă $|G: H|$ și $|H: K|$ sunt finite și în această situație avem:

$$|G: K| = |G: H| |H: K|.$$

Să se deducă teorema lui Lagrange ca un caz particular al afirmației de mai sus.

3. Fie A, B, C subgrupuri ale unui grup G . Presupunind că indicii care apar în membrul drept al inegalităților de mai jos sunt finiți, să se demonstreze că și cei care apar în membrul stîng sunt finiți și să se demonstreze respectivele inegalități:

- (i) dacă $A \leq B$, atunci $|C \cap B : C \cap A| \leq |B : A|$;
- (ii) $|G : A \cap B| \leq |G : A| |G : B|$;
- (iii) $|A \vee B : B| \leq |A : A \cap B|$.

Indicații. (i) Se demonstrează că asocierea

$$(C \cap A)x \sim \rightarrow Ax, \quad x \in C \cap B$$

definește o aplicație injectivă $(C \cap B / C \cap A)_d \rightarrow (B/A)_d$.

(ii) Se demonstrează că $|B : A \cap B| \leq |G : A|$ pe baza lui (i) și apoi, înmulțim ambii membri ai acestei inegalități cu $|G : B|$.

(iii) Se folosește (i) și faptul că $(A \vee B) \cap A = A$.

4. Fie A și B subgrupuri ale unui grup G și presupunem că $|G : A|$ și $|G : B|$ sunt finite și prime între ele. Să se demonstreze că avem

$$|G : A \cap B| = |G : A| |G : B| \text{ și } G = AB.$$

Indicații. $|G : A \cap B|$ este finit, conform exercițiului 3 (ii) și conform exercițiului 2 avem:

$$|G : A \cap B| = |G : A| |A : A \cap B| = |G : B| |B : A \cap B|.$$

Cind G este finit, egalitatea $|G : A \cap B| = |G : A| |G : B|$ devine

$$\frac{|G|}{|A \cap B|} = \frac{|G|}{|A|} \frac{|G|}{|B|} \text{ de unde rezultă } G = AB. \text{ Cind } G \text{ este infinit se}$$

consideră interiorul normal H_G , unde $H = A \cap B$ și se aplică rezultatul, deja obținut în cazul finit, grupului finit G/H_G .

5. Fie \mathbf{R}_+^* subgrupul lui \mathbf{R}^* format din numerele reale pozitive și \mathbf{Q}_+^* subgrupul lui \mathbf{Q}^* format din numerele raționale pozitive. Să se demonstreze că $\mathbf{R}_+^* \cong \mathbf{R}$ și $\mathbf{Q}_+^* \not\cong \mathbf{Q}$.

Indicații. Se consideră funcția logaritm $\ln: \mathbf{R}_+^* \rightarrow \mathbf{R}$; dacă $\varphi: \mathbf{Q}_+^* \rightarrow \mathbf{Q}$ este un morfism de grupuri și $r = \frac{1}{2} \varphi(2)$, să arată că $r \notin \text{Im } \varphi$.

6. Fie G un grup și $x, y \in G$ astfel încât $G = \langle x, y \rangle$ și $xyx^{-1} = y^k$ pentru un număr întreg k . Să se demonstreze că dacă x este de ordin finit, atunci y este de ordin finit, G este de ordin finit și $|G| \leqslant o(x)o(y)$.

7. Fie G un grup astfel ca, pentru orice $g \in G$, avem $g^2 = 1$. Să se demonstreze că:

(i) G este abelian;

(ii) există o submulțime B a lui G astfel ca pentru orice element $x \in G$ există un unic număr natural n și elementele $b_1, b_2, \dots, b_n \in B$ unic determinate de x (abstracție făcând de ordinea lor) astfel ca $x = b_1 b_2 \dots b_n$.

Indicație. În cazul cînd G este finit, B este un sistem de generatori minimal al lui G ; în cazul cînd G este numărabil, B se poate construi recursiv; în cazul cînd G este nenumărabil, B se poate construi, de asemenea, recursiv, dar pe baza inducției transfinite; se poate face apel și la existența bazei unui spațiu vectorial.

8. Fie G un grup oarecare. Să se demonstreze că $|\text{Aut}(G)| = 1$ dacă și numai dacă $|G| \leqslant 2$.

Indicație. Presupunind că $\text{Aut}(G) = 1$ și considerind automorfismele interioare ale lui G rezultă că G este abelian; în această situație aplicația $\tau: G \rightarrow G$ cu $\tau(x) = x^{-1}$ este un automorfism și rezultă $g^2 = 1$ pentru orice $g \in G$. Considerind acum o submulțime B a lui G ca la exercițiul 7, avem $\text{Aut}(G) \cong S(B)$ și rezultă $|B| \leqslant 1$, deci $|G| \leqslant 2$.

9. Fie G un grup finit netrivial. Un automorfism $\alpha \in \text{Aut}(G)$ se numește automorfism fără puncte fixe dacă

$$\alpha(x) = x \Rightarrow x = 1.$$

Să se demonstreze că:

(i) dacă α este un automorfism a lui G fără puncte fixe, atunci

$$\{\alpha(g)g^{-1} \mid g \in G\} = G;$$

(ii) există un automorfism $\alpha \in \text{Aut}(G)$ cu $o(\alpha) = 2$ și fără puncte fixe dacă și numai dacă G este abelian și de ordin impar.

Indicații. (i) Se demonstrează că aplicația $g \sim \rightarrow \alpha(g)g^{-1}$ este injectivă; (ii) dacă α este un automorfism al lui G de ordinul 2 și fără puncte fixe se demonstrează pe baza lui (i) că $\alpha(x)=x^{-1}$ pentru orice $x \in G$.

10. Să se demonstreze că:

- i) un grup oarecare G nu poate fi reuniunea a două subgrupuri proprii.
- ii) grupul diedral D_4 este reuniunea a trei subgrupuri proprii.

11. Considerăm permutările $\sigma, \tau \in S(\mathbb{R})$ (\mathbb{R} mulțimea numărelor reale) definite prin $\sigma(x)=2x$ și $\tau(x)=x+1$, $x \in \mathbb{R}$). Fie $G=\langle\sigma, \tau\rangle \leqslant S(\mathbb{R})$ și, pentru fiecare număr natural n , fie $H_n=\langle\tau^n\sigma\tau^n\rangle \leqslant G$.

Să se demonstreze că $H=\bigcup_{n=0}^{\infty} H_n$ este un subgrup al lui G și că H nu este finit generat (deși G este finit generat).

Indicație. Se arată că $H_n \subset H_{n+1}$ pentru orice număr natural n .

12. Fie G un grup finit simplu și H un subgrup al lui G cu $|G:H|=p$, p număr prim. Să se demonstreze că p este cel mai mare divizor prim al lui $|G|$ și că p^2 nu divide $|G|$.

Indicație. Considerind interiorul normal H_G al lui H în G , se demonstrează că G poate fi scufundat în S_p .

13. Să se demonstreze că pentru orice subgrup propriu H al grupului aditiv \mathbb{Q} , grupul factor \mathbb{Q}/H este infinit și nu este ciclic.

Indicații. Dacă $|G:H|=n$ rezultă $\mathbb{Q}=\frac{1}{n}H$, de unde $H=\mathbb{Q}$; dacă \mathbb{Q}/H este ciclic, rezultă $\mathbb{Q}/H \cong \mathbb{Z}$; alegind un element $x=\frac{m}{n} \in H$,

dacă \mathbb{Q}/H este ciclic, rezultă $\mathbb{Q}/H \cong \mathbb{Z}_n$; alegind un element $x=\frac{1}{n} \in H$, $m \neq 0$, $n > 0$, se demonstrează că $H \cap \frac{1}{n}\mathbb{Z}=0$ sau $H \leqslant \frac{1}{n}\mathbb{Z}$, ambele posibilități fiind contradictorii.

14. Să se demonstreze că pentru orice subgrup propriu H al grupului aditiv \mathbb{Q} avem $H + \mathbb{Z} \neq \mathbb{Q}$.

Indicație. Avem $H \neq 0$, de unde rezultă $H \cap \mathbb{Z} \neq 0$, deci $H \cap \mathbb{Z} = n\mathbb{Z}$, cu n număr întreg pozitiv. Se aplică la două teoremă de izomorfism pentru a deduce $\mathbb{Q}/H \cong \mathbb{Z}_n$, ceea ce contrazice exercițiul 13.

15. Fie X o mulțime nevidă și pentru fiecare $\sigma \in S(X)$, fie

$$s(\sigma)=\{x \in X \mid \sigma(x) \neq x\};$$

$\tilde{S}(X)=\{\sigma \in S(X) \mid s(\sigma) \text{ mulțime finită}\}$.

i) Să se demonstreze că $\tilde{S}(X) \leq S(X)$.

ii) Dacă X este mulțime infinită să se demonstreze că $S(X)$ este un grup infinit în care orice element este de ordin finit și că grupul factor $S(X)/\bar{S}(X)$ este infinit.

16. Să se demonstreze că dacă G este un grup finit general, atunci pentru orice număr întreg pozitiv n există cel mult un număr finit de subgrupuri ale lui G de indice n .

Indicație. Dacă H este un subgrup al lui G de indice n , atunci grupul factor G/H_σ , unde H_σ este interiorul normal al lui H în G , poate fi scufundat în S_n .

17. Fie G un grup. Să se demonstreze că dacă $Z(G)=1$, atunci

$$Z(\text{Aut}(G))=1.$$

18. Fie G un grup. Să se demonstreze că dacă $G'=G$, atunci

$$Z(G/Z(G))=1.$$

Indicație. Pentru fiecare $z \in G$ se consideră aplicația $\theta_z: G \rightarrow G$ cu $\theta_z(x)=[z, x]$ și se demonstrează că θ_z este un morfism de grupuri cu $\text{Im } \theta_z \leq Z_1(G)$ și $G' \leq \text{Ker } \theta_z$.

19. Fie G un grup finit, G' subgrupul derivat al lui G și $x \in G$. Să se arate că:

$$|G/G'| \leq |C_G(x)|.$$

Indicație. Pentru fiecare element y conjugat cu x , avem $yx^{-1} \in G'$ și rezultă $|G'| \geq |G: C_G(x)|$.

20. Fie G un grup finit neabelian și $k(G)$ numărul claselor de conjugare ale lui G . Să se demonstreze că:

i) $k(G) > |Z(G)| + 1$;

ii) dacă $|G| = p^3$, unde p este un număr prim, atunci $k(G) = p^2 + p - 1$.

Indicații. i) Evident $k(G) \geq |Z(G)| + 1$. Presupunând $k(G) = |Z(G)| + 1$, ecuația claselor pentru grupul G capătă forma $|G| = |Z(G)| + |G: C_G(x)|$ pentru un element $x \in G$ necentral și, această relație conduce la o contradicție.

ii) Se demonstrează că $|Z(G)| = p$ și apoi că pentru orice element $x \in G$, necentral, $|C_G(x)| = p^2$.

21. Fie G un grup finit, $k(G)$ numărul claselor de conjugare ale lui G , $H \trianglelefteq G$, j numărul claselor de conjugare ale lui G incluse în H . Să se demonstreze că:

(i) $k(G/H) \leq k(G) - j + 1$;

(ii) dacă G este neabelian și $G/Z(G)$ este abelian, atunci $k(G) \geq |G|Z(G)| + |Z(G)| - 1$.

Indicație. i) Se construiește o aplicație canonica surjectivă de la mulțimea claselor de conjugare ale lui G care nu sunt incluse în H (mulțime care are $k(G) - j$ elemente) pe mulțimea claselor de conjugare netriviale ale lui G/H (care are $k(G/H) - 1$ elemente).

ii) Se demonstrează că luând în (i) $H = Z(G)$, avem $j = |Z(G)|$.

22. Fie G un grup finit și $k(G)$ numărul claselor de conjugare ale lui G . Să se arate că:

$$(i) k(G) = 2 \Leftrightarrow G \cong \mathbb{Z}_2$$

$$(ii) k(G) = 3 \Leftrightarrow G \cong \mathbb{Z}_3 \text{ sau } G \cong S_3.$$

Indicație. Dacă G este neabelian și $k(G) = 3$, ecuația claselor pentru grupul G devine

$$|G| = 1 + |G : C_G(x)| + |G : C_G(y)|$$

pentru $1 \neq x, y \in G$, x și y neconjugate în G , de unde deducem $1 = \frac{1}{l} + \frac{1}{m} + \frac{1}{n}$, $l = |G|$, $m = |C_G(x)|$, $n = |C_G(y)|$.

Să demonstrează că această egalitate implică $l = 6$, deci $G \cong S_3$.

23. Să se demonstreze că nu există grupuri simple de ordin 1000.

Indicație. Se arată că dacă G este un grup de ordin 1000, atunci $n_5 = 1$.

24. Să se demonstreze că nu există grupuri simple de ordin 300.

Indicație. Se arată că dacă G este un grup simplu de ordin 300, atunci $n_5 = 6$ astfel că dacă P este un 5-subgrup Sylow al lui G și $H = N_G(P)$, avem $|G : H| = 6$. Considerind interiorul normal H_G al lui H în G se deduce că G poate fi scufundat în S_6 , o contradicție.

25. Să se demonstreze că nu există grupuri simple de ordin 132.

Indicație. Se arată că dacă G este un grup simplu de ordin 132, atunci $n_{11} = 12$ și $n_3 = 4$ sau $n_3 = 22$. În cazul $n_3 = 4$, se arată exact ca la exercițiul precedent că G poate fi scufundat în S_4 , o contradicție. În cazul $n_3 = 22$, obținem că G are $n_3(3-1) = 44$ elemente de ordinul 3 și $n_{11}(11-1) = 120$ elemente de ordinul 11, ceea ce evident nu se poate.

26. Să se demonstreze că nu există grupuri simple de ordin 144.

Indicație. Se arată că dacă G este un grup simplu de ordin 144, atunci $n_3 = 16$; H_1 și H_2 fiind două 3-subgrupuri Sylow ale lui G distincte, se arată că $H_1 \vee H_2 = G$ și $H_1 \cap H_2 = 1$; se deduce că G are exact

$n_3(3^2 - 1) = 128$ elemente netriviale al căror ordin este o putere a lui 3 de unde rezultă $n_2 = 1$, o contradicție.

27. Fie n un număr întreg pozitiv par. Să se demonstreze că orice grup de ordinul n este nilpotent dacă și numai dacă n este o putere a lui 2.

Indicație. Dacă $n=2m$, se demonstrează că $Z(D_n)=1$ dacă m este impar și $D_n/Z(D_n) \cong D_m$ dacă m este par).

28. Fie G un grup nilpotent de clasă n . Să se demonstreze că orice subgrup și orice grup factor al lui G are clasa de nilpotență mai mică sau egală cu n . În cazul cînd $G=H \times K$, unde H este nilpotent de clasă m și K nilpotent de clasă n , să se demonstreze că G este nilpotent de clasă $\max(m, n)$.

29. Să se demonstreze că un grup rezolubil G are o serie de compozitie dacă și numai dacă G este finit.

30. Să se demonstreze că un grup finit G de ordin ≤ 100 este rezolvabil dacă și numai dacă $G \cong A_5$.

Indicatie. A_5 este singurul grup simplu neabelian de ordin ≤ 100 .

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*.

Exemple. 1) Mulțimile Z , Q , R cu operațiile obișnuite de adunare și înmulțire formează inele comutative și unitare.

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

3) Mulțimea $C([0, 1], R) = \{f : [0, 1] \rightarrow R \mid f \text{ continuă}\}$ cu adunarea și înmulțirea funcțiilor, $f+g$ și fg , definite în mod ușual: $(f+g)(x) = f(x)+g(x)$ 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 $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \dots, \widehat{\overline{n-1}}\}$ 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 $m, n \in \mathbb{Z}$ 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) $a0 = 0a = 0$, oricare ar fi $a \in R$;

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

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

$(a_1 + a_2 + \dots + a_n)b = a_1b + a_2b + \dots + a_nb$, 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 ambele 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,

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

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

Așind 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 *integrug*. Dacă, în plus, inelul este și comutativ, va fi numit *domeniu de integritate*.

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

Intr-adevăr, dacă R este inel integrug și $ab=a$, $a \neq 0$, 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 $ab=a$, $a \neq 0$, avem $ab=a$ și deci $b=0$. La fel, din $ba=0$, $a \neq 0$, rezultă că $b=0$ și deci R este integrug.

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, $U(\mathbb{Z}) = \{-1, 1\}$, $U(\mathbb{Q}) = \mathbb{Q} \setminus \{0\}$, $U(\mathbb{R}) = \mathbb{R} \setminus \{0\}$, $U(\mathbb{Z}_n) = \{\hat{a} \in \mathbb{Z}_n \mid (a, n) = 1\}$ (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 $xy \in S$.

Demonstrație. Condițiile 1° și 2° arată că operațiile de pe R induc pe S operații algebrice. Multimea 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 subinetele ale sale.

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

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

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

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

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

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

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

Propoziția 1.5. Fie R un inel și $\{S_\alpha\}_{\alpha \in A}$ o familie de subinete 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 \mathbb{Z} este un subinel al lui \mathbb{Q} însă nu este ideal deoarece, de exemplu,

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

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

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

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

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

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 $x \in R$, atunci $x = x \cdot 1 = x(vu) = (xv)u$ și cum u aparține idealului la stînga I , rezultă $x \in I$. Deci $I = R$. 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, bilaterale).

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 întii 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 $I \supseteq I'$. Pe de altă parte, deoarece $I \supseteq E$, 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

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

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

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

$$1) p\mathbb{Z} + q\mathbb{Z} = d\mathbb{Z},$$

$$2) p\mathbb{Z} \cap q\mathbb{Z} = m\mathbb{Z}.$$

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

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

Astfel am arătat că $p\mathbb{Z} \cap q\mathbb{Z} \subset m\mathbb{Z}$ și deci egalitatea 2).

Vom construi în continuare un important inel necomutativ.

Definiția 1.13. Fie R un inel comutativ și unitar iar m și n numere naturale nenule. 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.

În mod analog, elementele (scrise de obicei pe verticală)

$$\begin{matrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{nj} \end{matrix}, \quad 1 \leq j \leq n,$$

formează coloana de rang j a matricei A .

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

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

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 formă unui astfel de tablou 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 A .

Definiția 1.14. 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 $A = (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$

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

Adunarea matricelor are următoarele proprietăți:

- 1) Adunarea matricelor este asociativă.
- 2) Adunarea matricelor este comutativă.
- 3) Matricea 0 de tip (m, n) , care are toate componentele egale cu zero este elementul nul, adică

$$A + 0 = 0 + A = A, \text{ oricare ar fi } A \in \mathcal{M}(m, n, R).$$

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 opusa matricei A , adică

$$A + (-A) = (-A) + A = 0.$$

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 $A + B =$

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

Mentionăm, 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.

Definiția 1.16. 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 al matricei A este egal cu numărul de linii al 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 componentelete de pe coloana j ale matricei B .

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

$$C = AB.$$

Înmulțirea matricelor are o serie de 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.

Intr-adevăr, să 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 $BC=F=(f_{jl})_{\substack{1 \leq j \leq n \\ 1 \leq l \leq q}}$ și $A(BC)=AF=G=(g_{il})_{\substack{1 \leq i \leq m \\ 1 \leq l \leq q}}$.

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

2º 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 $F=(f_{jl})_{\substack{1 \leq j \leq n \\ 1 \leq l \leq q}}$ este o matrice de tipul (n, p) , atunci

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

Intr-adevăr, 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 orice $1 \leq i \leq m$, $1 \leq k \leq p$, adică $M=N$ sau

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

Analog se demonstrează egalitatea a două.

3º 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 $A \in \mathcal{M}(m, m, R)$ este o matrice de tipul (m, n) , atunci este clar că

$$I_m A = A \text{ și } A I_n = A.$$

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

Propoziția 1.17. *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 demonstate mai înainte, este clar 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

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

iar

$$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix},$$

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 nenuli. De exemplu,

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

iar

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

Definiția 1.18. Fie $A = (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ o matrice de tip (m, n) peste inelul R . Matricea $'A = (\bar{a}_{kl})_{\substack{1 \leq k \leq n \\ 1 \leq l \leq m}}$ de tip (n, m) , unde $\bar{a}_{kl} = a_{lk}$, oricare ar fi $1 \leq k \leq n$, $1 \leq l \leq m$, se numește *transpusa* matricei A .

Deci liniile, respectiv coloanele matricei transpușe $'A$ sunt coloanele, respectiv liniile matricei A .

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

Următoarele proprietăți se verifică fără dificultate:

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

$$'(A+B) = 'A + 'B.$$

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

$$'(AB) = 'B'A.$$

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 $A + B = (c_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$. Avem $'(A+B) = ('c_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}}$, unde $'c_{ki} = c_{ni} = a_{ik} + b_{ik} = 'a_{ki} + 'b_{ki}$. Deci

$$'(A+B) = ('c_{ki})_{\substack{1 \leq k \leq n \\ 1 \leq i \leq m}} = ('a_{ki} + 'b_{ki})_{\substack{1 \leq k \leq n \\ 1 \leq i \leq m}} = ('a_{ki})_{\substack{1 \leq k \leq n \\ 1 \leq i \leq m}} + ('b_{ki})_{\substack{1 \leq k \leq n \\ 1 \leq i \leq m}} = 'A + 'B.$$

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

Am observat că inelul $\mathcal{M}_n(R)$ pentru $n \geq 2$ nu este comutativ. Să justificăm prin exemple că există ideale la stânga 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 stânga 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 stânga.

§ 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.

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

Intr-adevăr, de la grupuri rezultă că gof este morfism al grupurilor additive subiacente inelelor R și R'' .

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

$$(gof)(ab)=g(f(ab))=g(f(a)f(b))=g(f(a))g(f(b))=((gof)(a))((gof)(b)).$$

2º 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 demonstreăm că, dacă $g: R' \rightarrow R$ este o funcție

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

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

Pe de altă parte,

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

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

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

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

Mai mult, după definiție p este morfism surjectiv.

4) Fie R inel comutativ și unitar și $\mathcal{M}_n(R)$ inelul matricelor pătratice 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 ușile, în afară de cele de pe diagonală principală care sunt egale cu a .

Aveam 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 morfism 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 imaginea 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 familiei 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 iar înmulțirea satisfac următoarele condiții:

1º este asociativă,

2º este distributivă față de adunare.

Să verificăm, de exemplu, una din egalitățile care ne dau 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 $\mathbf{Z}_m = \{\hat{0}, \hat{1}, \dots, \hat{m-1}\}$, $\mathbf{Z}_n = \{\bar{0}, \bar{1}, \dots, \bar{n-1}\}$, $\mathbf{Z}_{mn} = \{\overline{\bar{0}}, \overline{\bar{1}}, \dots, \overline{\bar{mn-1}}\}$ 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 $\varphi(\bar{a}) = (\hat{a}; \bar{a})$.

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

Dacă $\bar{a} = \bar{a}'$, 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 $\varphi(\bar{a}) = \varphi(\bar{a}')$. Deci φ este bine definită. Funcția φ este un morfism de inele.

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

Fie acum $\varphi(\bar{a}) = \varphi(\bar{a}')$. 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 $a = a'$ 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 precedentă 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

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

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

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

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

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

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

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

Demonstrație. Din cele de mai sus rezultă că $\varphi(n) = \varphi(p_1^{m_1}) \varphi(p_2^{m_2}) \dots \dots \varphi(p_k^{m_k})$. Pentru un număr p^k cu p prim avem că $\varphi(p^k) = p^k - p^{k-1}$.

Intr-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 sint p^{k-1} astfel de numere și deci $\varphi(p^k) = p^k - p^{k-1}$. Atunci

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

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

§ 3. INEL FACTOR, TEOREME DE IZOMORFISM PENTRU INELE

Fie R un inel și $I \subset R$ un ideal bilateral al său. Dacă vom considera grupul aditiv subiacent lui R , atunci I este un subgrup al acestui grup abelian. De la grupuri avem următoarea relație de congruență definită pe R în raport cu subgrupul I . Dacă $a, b \in R$, atunci $a \equiv b \pmod{I}$ dacă și numai dacă $a - b \in I$. Aceasta este o relație de echivalență pe R , iar clasa de echivalență a lui $a \in R$ modulo I este $\hat{a} = a + I = \{a + x \mid x \in I\}$. Este cunoscut că multimea factor R/I pe care este definită operația algebrică de adunare, $\hat{a} + \hat{b} = \hat{a+b}$, oricare ar fi $\hat{a}, \hat{b} \in R/I$, este un grup abelian.

Pe grupul abelian R/I definim o nouă operație algebrică, înmulțirea, dată prin

$$\hat{ab} = \widehat{ab}.$$

Să demonstrăm că această operație este bine definită, adică nu depinde de alegerea reprezentanților.

Într-adevăr, dacă $\hat{a} = \hat{a}'$, $\hat{b} = \hat{b}'$, atunci $a - a' \in I$, $b - b' \in I$ și deci $a - a' = x$, $b - b' = y$ cu $x, y \in I$. Prin urmare, $a = a' + x$, $b = b' + y$ și avem

$$ab = (a' + x)(b' + y) = a'b' + a'y + xb' + xy.$$

Cum I este ideal bilateral, rezultă că $a'x + xb' + xy \in I$ și deci $ab - a'b' \in I$, adică

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

Propoziția 3.1. *Mulțimea factor R/I împreună cu operațiile de adunare și înmulțire, definite mai înainte, formează un inel. Mai mult, funcția surjectivă $p: R \rightarrow R/I$, $p(x) = \hat{x}$ este un morfism de inele.*

Demonstrație. După cum am menționat, R/I față de adunare este un grup abelian. În plus, înmulțirea are proprietățile:

$$1^\circ (\hat{ab})\hat{c} = \hat{a}(\hat{b}\hat{c}) \text{ (asociativitatea)},$$

$$2^\circ \hat{a}(\hat{b} + \hat{c}) = \hat{ab} + \hat{ac},$$

$(\hat{a} + \hat{b})\hat{c} = \hat{ac} + \hat{bc}$ (distributivitatea față de adunare),
oricare ar fi $\hat{a}, \hat{b}, \hat{c} \in R/I$.

Verificarea acestora se face ușor, prin calcul, bazîndu-ne pe proprietățile analoage ale operațiilor din inelul R .

De exemplu, $(\hat{ab})\hat{c} = \widehat{abc} = (\widehat{ab})\hat{c} = \widehat{abc} = \hat{a}(\hat{b}\hat{c})$.

Funcția $p: R \rightarrow R/I$ este un morfism de grupuri și, în plus,

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

adică p este morfism de inele.

Inelul R/I se numește *inelul factor* al inelului R în raport cu idealul bilateral I .

Observăm că dacă R este inel unitar, atunci inelul factor R/I este de asemenea unitar. Elementul unitate este $\hat{1}$, deoarece oricare ar fi $\hat{a} \in R/I$ avem

$$\hat{a}|\hat{1} = \hat{a}\hat{1} = \hat{a} \text{ și } \hat{1}\hat{a} = \hat{1}\hat{a} = \hat{a}.$$

În acest caz $p(1)=1$ și deci p este morfism unitar de inele.

Dacă R este comutativ, atunci și inelul factor R/I este comutativ, deoarece oricare ar fi $\hat{a}, \hat{b} \in R/I$ avem

$$\hat{a}\hat{b} = \hat{b}\hat{a} = \hat{b}\hat{a}.$$

Exemplu. Dacă \mathbb{Z} este inelul numerelor întregi și I este un ideal al său, atunci există $n \geq 0$ astfel încât $I = n\mathbb{Z}$. Este clar că, relația de congruență modulo idealul $n\mathbb{Z}$ este tocmai congruență modulo n . Mai mult, inelul factor $\mathbb{Z}/n\mathbb{Z}$ pentru $n\mathbb{Z} \neq 0$ este inelul claselor de resturi modulo n , iar pentru $n\mathbb{Z} = 0$, adică $n=0$, inelul factor $\mathbb{Z}/0\mathbb{Z}$ se identifică cu inelul \mathbb{Z} . Pentru $n=1$, inelul $\mathbb{Z}/1\mathbb{Z}$ este inelul nul.

Dacă R este inel, I un ideal bilateral și $p: R \rightarrow R/I$ morfismul canonice, atunci $\text{Ker } p = p^{-1}(\{0\}) = I$. Reciproc, am văzut că nucleul oricărui morfism de inele este ideal bilateral.

Prin urmare, o submulțime nevidă a unui inel R este ideal bilateral al lui R dacă și numai dacă este nucleul unui anumit morfism de inele definit pe R .

Dăm acum *teorema fundamentală de izomorfism* pentru inele.

Teorema 3.2. Fie $f: R \rightarrow S$ un morfism de inele. Atunci $\text{Ker } f$ este un ideal bilateral al lui R și există un unic izomorfism de inele

$$\varphi: R/\text{Ker } f \simeq \text{Im } f$$

astfel încât $f = \varphi \circ q$, unde q este morfismul canonice de la R la $R/\text{Ker } f$.

Demonstrație. Considerind structurile de grup aditiv subiacente inelelor din enunțul teoremei, f fiind în particular morfism de grupuri, din teorema fundamentală de izomorfism pentru grupuri (vezi cap. I, teorema 3.5.1) rezultă că funcția $\varphi: R/\text{Ker } f \rightarrow \text{Im } f$, definită prin $\varphi(\hat{a}) = f(a)$ este un izomorfism între grupurile aditive ale celor două inele. Mai mult, φ este unic cu proprietatea că $f = \varphi \circ q$. Pentru a termina demonstrația să arătăm că φ este chiar morfism de inele. Într-adevăr, dacă

$$\hat{a}, \hat{b} \in R/\text{Ker } f, \text{ atunci } \varphi(\hat{a}\hat{b}) = \varphi(\hat{a}\hat{b}) = f(ab) = f(a)f(b) = \varphi(\hat{a})\varphi(\hat{b}).$$

Propoziția 3.3. Fie $f: R \rightarrow S$ un morfism surjectiv de inele. Atunci aplicația

$$R' \rightarrow f(R')$$

stabilește o bijecție între mulțimea subinelelor respectiv idealelor la stânga (la dreapta, bilaterale) ale lui R care conțin $\text{Ker } f$ și mulțimea tuturor subinelelor respectiv idealelor la stânga (la dreapta, bilaterale) ale lui S , inversă acesteia fiind data de $S' \rightarrow f^{-1}(S')$.

Demonstrație. Dacă considerăm structurile de grup aditiv subiacente inelelor R și S , f fiind în particular morfism de grupuri, este cunoscut (vezi cap. I, prop. 2.8) că aplicația $R' \rightarrow f(R')$ stabilăse o bijecție între mulțimea

subgrupurilor grupului aditiv al lui R care conțin $\text{Ker } f$ și multimea tuturor subgrupurilor grupului aditiv al lui S , inversa acesteia fiind dată de $S' \rightarrow f^{-1}(S')$. După propoziția 2.3 rezultă că $R' \subset R$ este subinel (respectiv ideal la stînga, la dreapta, bilateral) dacă și numai dacă $f(R')$ este subinel (respectiv ideal la stînga, la dreapta, bilateral).

Avînd în vedere rezultatele menționate, afirmația propoziției este clară.

Dăm în continuare un rezultat important cunoscut sub numele de *teorema I-a de izomorfism pentru inele*.

Teorema 3.4. *Fie $f: R \rightarrow S$ un morfism surjectiv de inele. Dacă I este un ideal bilateral al lui R , atunci $f(I)$ este ideal bilateral al lui S și există un izomorfism de inele.*

$$\varphi: R/I \xrightarrow{\sim} S/f(I).$$

Demonstrație. Din propoziția 2.3, rezultă că, dacă I este ideal bilateral în R , atunci $f(I)$ este de asemenea ideal bilateral în S și deci putem vorbi de inelele factor R/I și $S/f(I)$. Dacă vom considera structurile de grup subiacente inelelor din enunț, din teorema I-a de izomorfism pentru grupuri, există un izomorfism $\varphi: R/I \rightarrow S/f(I)$ de grupuri additive dat de $\varphi(\hat{a}) = \overline{f(a)}$, unde prin \hat{a} și $\overline{f(a)}$ am notat, respectiv, clasele elementelor $a \in R$ și $f(a) \in S$ în inelele factor R/I și $S/f(I)$. Mai mult, dacă $\hat{a}, \hat{b} \in R/I$, atunci $\varphi(\hat{a}\hat{b}) = \varphi(\hat{a}\hat{b}) = \overline{f(ab)} = \overline{f(a)f(b)} = \overline{f(a)}\overline{f(b)} = \varphi(\hat{a})\varphi(\hat{b})$. Deci φ este un izomorfism de inele.

Aplicație. Am văzut în §2 că idealele inelului claselor de resturi modulo n sunt principale. Să dăm o descriere mai precisă a acestora. Dacă $p: \mathbf{Z} \rightarrow \mathbf{Z}_n$ este morfismul canonice din propoziția 3.3 rezultă o bijecție între idealele inelului \mathbf{Z}_n și cele ale inelului \mathbf{Z} care conțin $n\mathbf{Z}$, dată de $I \mapsto p(I)$ și a cărei inversă este $J \mapsto p^{-1}(J)$. Dar $p^{-1}(J) = m\mathbf{Z}$ și $m\mathbf{Z} \supset \text{Ker } p$. Avem $m\mathbf{Z} \supset n\mathbf{Z}$ dacă și numai dacă $m \mid n$. Cum $J = p(I)$, rezultă $J = m\mathbf{Z}/n\mathbf{Z}$. Deci idealele inelului \mathbf{Z}_n sunt de forma $m\mathbf{Z}/n\mathbf{Z}$ cu $m \mid n$, acesta fiind idealul principal generat de \hat{m} , adică (\hat{m}) . Conform teoremei 3.4 există un izomorfism de inele

$$\varphi: \mathbf{Z}/I \xrightarrow{\sim} \mathbf{Z}_n/p(I),$$

de unde $\mathbf{Z}_m \cong \mathbf{Z}_n/(\hat{m})$. Deci inelele factor ale inelului \mathbf{Z}_n sunt izomorfe cu inelele \mathbf{Z}_m , unde $m \mid n$.

Vom da acum *teorema a-II-a de izomorfism* pentru inele.

Teorema 3.5. *Fie R un inel, S un subinel și I un ideal bilateral al lui R . Atunci $S+I = \{a+x \mid a \in S, x \in I\}$ este un subinel al lui R care conține I , $S \cap I$ este ideal bilateral al lui S și există un izomorfism de inele*

$$\varphi: (S+I)/I \xrightarrow{\sim} S/S \cap I.$$

Demonstrație. Se verifică ușor prin calcul că $S+I$ este subinel al lui R . Deoarece $I \subset S+I$ este ideal bilateral al lui R , este evident că I este ideal bilateral al lui $S+I$. Cum I este ideal bilateral al lui R , rezultă imediat că $S \cap I$ este ideal bilateral al lui S . Definim $\psi: S \rightarrow R/I$, prin $\psi(a) = \bar{a}$. Avem că $\text{Im } \psi = S+I/I$, iar $\text{Ker } \psi = S \cap I$, ceea ce se vede ușor.

Din teorema fundamentală de izomorfism, rezultă un izomorfism de inele:

$$\varphi: S/\text{Ker } \psi \xrightarrow{\sim} \text{Im } \psi.$$

Cum $\text{Im } \psi = S+I/I$, atunci φ este izomorfismul căutat.

§ 4. CORP, SUBCORP, MORFISME DE CORPURI. EXEMPLE

Definiția 4.1. 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 $(K, +)$ al corpului și grupul multiplicativ (K^*, \cdot) al elementelor nenule ale corpului K . Aceste două structuri se numesc grupurile subiacente ale corpului.

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

2) Fie n un număr natural. Atunci inelul \mathbb{Z}_n este corp dacă și numai dacă n este prim.

Intr-adevăr, dacă n este prim și $\hat{a} \in \mathbb{Z}_n$, $\hat{a} \neq \hat{0}$, atunci $(\hat{a}, n) = 1$ și deci \hat{a} este element inversabil în \mathbb{Z}_n . Reciproc, dacă \mathbb{Z}_n este corp, să presupunem prin absurd că n nu este prim, adică $n = kl$, unde $1 < k, l < n$. Atunci avem $\hat{k} \neq \hat{0}$, $\hat{l} \neq \hat{0}$ și $\hat{k}\hat{l} = \hat{0}$.

Înmulțind ultima egalitate cu \hat{k}^{-1} rezultă $\hat{l} = \hat{0}$, contradicție.

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

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

și

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

două operații algebrice în raport cu care, după cum se verifică ușor, $\mathbb{Q}(\sqrt{2})$ devine un corp comutativ.

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

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

4) Orice inel integrul finit este corp.

Intr-adevăr, fie R un astfel de inel și $a \in R$, $a \neq 0$. Definim funcția $\varphi_a: R \rightarrow R$ prin $\varphi_a(x) = ax$. Dacă $\varphi_a(x) = \varphi_a(y)$, atunci $ax = ay$ sau $a(x-y) = 0$ și deci $x-y=0$ adică $x=y$. Rezultă φ_a injectivă și cum R este finit, va fi și surjectivă. Deci există $b \in R$ astfel încât $1 = \varphi_a(b) = ab$. La fel, considerind funcția $\psi_a: R \rightarrow R$, definită prin $\psi_a(x) = xa$, obținem că există $c \in R$ astfel încât $1 = \psi_a(c) = ca$. Deci $ab = 1$ și $ca = 1$ de unde $b = 1 \cdot b = (ca)b = c(ab) = c \cdot 1 = c$, adică a este inversabil. Deci R este corp.

Propoziția 4.2. Un inel unitar nenul R este corp dacă și numai dacă $\{0\}$ și R sunt singurele ideale la stînga și la dreapta ale lui R .

Demonstrație. Din propoziția 1.7 rezultă că într-un corp, $\{0\}$ și R sunt singurele ideale la stînga și ideale la dreapta. Reciproc, dacă presupunem că singurele ideale la stînga și ideale la dreapta ale lui R sunt $\{0\}$ și R , atunci fie $a \in R$, $a \neq 0$.

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

Deoarece orice element nenul al unui corp este inversabil, din §1 rezultă că orice corp nu are divizori ai lui zero nenuli.

Definiția 4.3. Fie K un corp. O submulțime nevidă F a lui K se numește subcorp al lui K dacă operațiile algebrice de pe K înduc 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 .

Propoziția 4.4. 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 1.4.

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

Exemplu. 1) Fie K un corp. Atunci K este evident subcorp al lui K .

2) $Q \subset R$ este un subcorp cu adunarea și înmulțirea numerelor.

3) $Q(\sqrt{2})$, construit mai înainte este în mod clar un subcorp al corpului R al numerelor reale.

4) Z_p și Q nu au alte subcorpuri în afară de ele însuși.

Intr-adevăr, dacă $F \subset Z_p$ este un subcorp al lui Z_p , atunci F este un subinel al lui Z_p . Știm că subinelele și idealele lui Z_p coincid, iar cum Z_p este corp singurele sale ideale sunt $\{0\}$ și Z_p . Deci singurul subcorp al lui Z_p este el însuși.

Fie acum $F \subset Q$ un subcorp al lui Q . Cum $1 \in F$ rezultă că oricare ar fi $n \in \mathbb{N}$, nenul, avem $n = \underbrace{1+1+\dots+1}_n \in F$. Dar $0 \in F$ implică $0-n \in F$

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

Definiția 4.5. Fie K și K' două coruri. Se numește *morfism* de coruri de la K la K' o funcție $f: K \rightarrow K'$, astfel încât să fie satisfăcute următoarele condiții:

$$1) f(x+y) = f(x) + f(y), \text{ oricare ar fi } x, y \in K,$$

$$2) f(xy) = f(x)f(y), \text{ oricare ar fi } x, y \in K,$$

$$3) f(1) = 1.$$

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

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

Propoziția 4.6. Orice morfism de coruri este injectiv.

Demonstrație. Intr-adevăr, fie $f: K \rightarrow K'$ morfism de coruri și $x, y \in K$ astfel încât $x \neq y$. Atunci $x-y \neq 0$ și deci există $z \in K$, astfel încât $(x-y)z = 1$, de unde $f((x-y)z) = f(1)$ sau $f(x-y)f(z) = 1$. Prin urmare, $f(x-y) \neq 0$ adică $f(x) - f(y) \neq 0$ sau $f(x) \neq f(y)$.

Fie K un corp și $\{F_\alpha\}_{\alpha \in A}$ o familie nevidă de subcorpuri ale sale. De la inele știm că $\bigcap_{\alpha \in A} F_\alpha$ este un subinel al lui K . Mai mult, dacă $y \in \bigcap_{\alpha \in A} F_\alpha$, $y \neq 0$, atunci $y \in F_\alpha$, $y \neq 0$, oricare ar fi $\alpha \in A$ și cum fiecare F_α este corp rezultă că $y^{-1} \in F_\alpha$, oricare ar fi $\alpha \in A$. Deci $y^{-1} \in \bigcap_{\alpha \in A} F_\alpha$.

Am obținut astfel că intersecția unei familii oarecare nevide de subcorpuri ale unui corp K este de asemenea un subcorp al lui K .

Dacă considerăm intersecția tuturor subcorpurilor unui corp, se obține un subcorp al său, care nu are alte subcorpuri în afară de el însuși.

Definiția 4.7. Un corp care nu are alte subcorpuri în afară de el însuși se numește *corp prim*.

Din cele precedente rezultă că orice corp conține ca subcorp al său un anumit corp prim.

Exemplul de mai înainte arată că corurile Z_p , p prim, și Q sunt prime.

Propoziția 4.8. Orice corp prim este izomorf sau cu corpul \mathbb{Q} al numerelor raționale sau cu un anumit corp \mathbb{Z}_p , p prim.

Demonstrație. Fie P un corp prim și funcția

$$\varphi: \mathbb{Z} \rightarrow P, \text{ definită prin } \varphi(n) = n1_P,$$

unde 1_P este elementul unitate al corpului P .

Funcția φ este morfism de inele. Într-adevăr,

$$\varphi(m+n) = (m+n)1_P = m1_P + n1_P = \varphi(m) + \varphi(n)$$

și

$$\varphi(mn) = (mn)1_P = (m1_P)(n1_P) = \varphi(m)\varphi(n), \text{ oricare ar fi } m, n \in \mathbb{Z}.$$

Atunci $\text{Ker } \varphi$ este un ideal al inelului \mathbb{Z} și deci există $n \geq 0$ astfel încât $\text{Ker } \varphi = n\mathbb{Z}$. Sunt numai două posibilități pe care le vom considera pe rînd.

1º $\text{Ker } \varphi = \{0\}$. Atunci φ este morfism injectiv de la \mathbb{Z} în P , și să considerăm subcorpul $\bar{P} = \left\{ \frac{m1_P}{n1_P} \mid m, n \in \mathbb{Z}, n \neq 0 \right\}$ al lui P .

Este clar că funcția $\bar{\varphi}: \mathbb{Z} \rightarrow \bar{P}$, dată prin $\bar{\varphi}\left(\frac{m}{n}\right) = \frac{m1_P}{n1_P}$ dă un izomorfism între corporile \mathbb{Q} și \bar{P} . Cum \bar{P} este prim rezultă că $\bar{P} = P$ și deci \mathbb{Q} este izomorf cu P .

2º $\text{Ker } \varphi \neq \{0\}$. Atunci $\text{Ker } \varphi = n\mathbb{Z}$, $n \neq 0$, și din teorema fundamentală de izomorfism la inele avem

$$\mathbb{Z}/\text{Ker } \varphi \simeq \text{Im } \varphi \text{ sau } \mathbb{Z}_n \simeq \text{Im } \varphi.$$

Dar $\text{Im } \varphi$ fiind subinel al corpului P , care este domeniu de integritate, va fi la rîndul său domeniu de integritate și deci \mathbb{Z}_n este domeniu de integritate. Atunci \mathbb{Z}_n este corp și deci $\text{Im } \varphi$ va fi un subcorp al lui P . Cum P este prim, rezultă $\text{Im } \varphi = P$ și deci \mathbb{Z}_n este izomorf cu P iar n este un număr prim.

Definiția 4.9. Un corp comutativ K ce conține un subcorp prim izomorf cu \mathbb{Q} se spune că este de caracteristică zero și scriem $\text{car } K=0$. Dacă subcorpul prim al lui K este izomorf cu \mathbb{Z}_p , p prim, spunem că, corpul K este de caracteristică p și scriem $\text{car } K=p$.

După propoziția 4.8 observăm că, un corp K este de caracteristică zero, dacă $m1_K \neq 0$ oricare ar fi m număr întreg pozitiv. De asemenea, caracteristica p a unui corp K este cel mai mic număr întreg pozitiv astfel încât $p1_K=0$.

Cu alte cuvinte, dacă luăm grupul aditiv $(K, +)$ subiacent corpului K , atunci K este de caracteristică zero dacă $\text{ord}(1)$ este infinit și este de caracteristică p dacă $\text{ord}(1)=p$.

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

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

2) Dacă p este un număr prim, \mathbb{Z}_p și orice altă extindere a sa au caracteristica p .

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

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

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

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

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 \hat{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 $\alpha = (\hat{0}, \hat{1})$ și atunci înțînd cont de cele precedente, elementele corpului K sunt:

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

$$(\hat{1}, \hat{1}) = (\hat{1}, \hat{0}) + (\hat{0}, \hat{1}) = \hat{1} + \alpha.$$

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

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

Propoziția 4.10. Fie K un corp comutativ cu car $K = p$, $p \neq 0$. Atunci avem:

- 1) $px = 0$,
- 2) $(xy)^p = x^p y^p$,
- 3) $(x \pm y)^p = x^p \pm y^p$ (semnele se corespund); oricare ar fi $x, y \in K$.

Demonstrație. 1) Avem $px = p(1x) = (p1)x = 0x = 0$.

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

Observăm că relațiile 2) și 3) ale propoziției precedente, arată că funcția

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

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

Vom construi în continuare două exemple importante de corpuri: corpul numerelor complexe și corpul cuaternionilor.

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 $(a, b), (a', b') \in \mathbb{R} \times \mathbb{R}$, este un grup abelian.

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

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

Avem că $\mathbb{R} \times \mathbb{R}$ 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 este: asociativă, distributivă față de adunare, comutativă. Elementul neutru la înmulțire este $(1, 0)$ și, mai mult, orice element nenul este inversabil.

Verificarea acestor proprietăți se face direct prin calcul, folosind proprietățile analoage ale operațiilor cu numere reale.

Să arătăm doar existența inversului oricărui element nenul. Într-adevăr, 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 obține $ax - by = 1$ și $bx + ay = 0$ de unde

$$x = \frac{a}{a^2 + b^2} \text{ și } y = \frac{-b}{a^2 + b^2}.$$

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

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

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

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

Este clar că φ este un morfism de coruri și deci injectiv. Pe baza acestuia rezultă că \mathbf{R} este izomorf cu $\text{Im } \varphi$, adică cu subcorful $C' = \{(a, 0) \mid a \in \mathbf{R}\}$ al corpului \mathbf{C} . Astfel putem identifica corpul \mathbf{R} al numerelor reale cu subcorful C' de numere complexe și numărul real a cu numărul complex $(a, 0)$. Așadar, în loc de elementul $(a, 0)$ din \mathbf{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 \mathbf{C} . Atunci $\alpha = (a, 0) + (0, b) = (a, 0) + (b, 0)(0, 1) = a + bi$.

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

Vom indica acum un corp izomorf cu corpul \mathbf{C} al numerelor complexe. Astfel putem concepe o altă construcție a acestui corp.

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

Se verifică fără dificultate că adunarea și înmulțirea obișnuită a matricelor conferă acestei mulțimi o structură de corp comutativ.

Funcția $\psi: \mathbf{C} \rightarrow \mathbf{K}$, definită prin

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

ne dă un izomorfism între cele două coruri.

Lăsăm pe seama cititorului demonstrația afirmațiilor precedente.

2) *Corpul cuaternionilor*. Fie inelul $\mathcal{M}_2(\mathbf{C})$ al matricelor pătratice de ordin 2 peste corpul \mathbf{C} și $H \subset \mathcal{M}_2(\mathbf{C})$, unde

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

Avem că H este un subinel al lui $\mathcal{M}_2(\mathbf{C})$.

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

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

$$\text{Avem } \begin{pmatrix} \alpha - \gamma & \beta - \delta \\ -\beta - \delta & \alpha - \gamma \end{pmatrix} \in H, \text{ și } \begin{pmatrix} \alpha - \gamma & \beta - \delta \\ -\beta - \delta & \alpha - \gamma \end{pmatrix} + \begin{pmatrix} \alpha - \gamma & \beta - \delta \\ -\beta - \delta & \alpha - \gamma \end{pmatrix} = \begin{pmatrix} 2(\alpha - \gamma) & 2(\beta - \delta) \\ -2(\beta - \delta) & 2(\alpha - \gamma) \end{pmatrix} = \begin{pmatrix} \alpha - \gamma & \beta - \delta \\ -\beta - \delta & \alpha - \gamma \end{pmatrix}.$$

$$2^{\circ} \quad \begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix} \begin{pmatrix} \gamma & \delta \\ -\delta & \gamma \end{pmatrix} = \begin{pmatrix} \alpha\gamma - \beta\delta & \alpha\delta + \beta\gamma \\ -\beta\gamma - \alpha\delta & -\beta\delta + \alpha\gamma \end{pmatrix} =$$

$$\text{Avem } \begin{pmatrix} \alpha\gamma - \beta\delta & \alpha\delta + \beta\gamma \\ -\beta\gamma - \alpha\delta & -\beta\delta + \alpha\gamma \end{pmatrix} \in H, \text{ și } \begin{pmatrix} \alpha\gamma - \beta\delta & \alpha\delta + \beta\gamma \\ -\beta\gamma - \alpha\delta & -\beta\delta + \alpha\gamma \end{pmatrix} + \begin{pmatrix} \alpha\gamma - \beta\delta & \alpha\delta + \beta\gamma \\ -\beta\gamma - \alpha\delta & -\beta\delta + \alpha\gamma \end{pmatrix} = \begin{pmatrix} 2(\alpha\gamma - \beta\delta) & 2(\alpha\delta + \beta\gamma) \\ -2(\beta\gamma - \alpha\delta) & 2(-\beta\delta + \alpha\gamma) \end{pmatrix} = \begin{pmatrix} \alpha\gamma - \beta\delta & \alpha\delta + \beta\gamma \\ -\beta\gamma - \alpha\delta & -\beta\delta + \alpha\gamma \end{pmatrix}.$$

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

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

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

Mai mult, vom arăta că H este corp. Într-adevăr, dacă $h = \begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix} \neq \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, atunci numărul real $\Delta = |\alpha|^2 + |\beta|^2$ este nenul. Inversul lui h este $h^{-1} = \begin{pmatrix} \bar{\alpha} & -\bar{\beta} \\ \bar{\beta} & \bar{\alpha} \end{pmatrix}$ după cum se vede ușor.

Deci H este un corp numit *corpul cuaternionilor*. Elementele sale le vom numi *cuaternioni*.

Definim funcția

$\varphi: \mathbb{R} \rightarrow H$, prin $\varphi(a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$, care este evident un morfism de coruri, deci injectiv.

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

Dată 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

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

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 §8, în cazul corporilor comutative acest lucru nu este posibil.

Aplicație. Să determinăm mulțimea soluțiilor ecuației $x^2 + 1 = 0$ în corpul cuaternionilor.

Să presupunem că $h = a + bi + cj + dk$ este o soluție a acestei ecuații. Atunci $h \neq 0$ și $h^2 + 1 = 0$. Înmulțind această egalitate cu cuaternionul $\bar{h} = a - bi - cj - dk$ obținem $\bar{h}h^2 + \bar{h} = 0$. Dacă $\Delta = a^2 + b^2 + c^2 + d^2$, avem $\bar{h}h = \Delta$ și deci $\Delta h + \bar{h} = 0$. De aici obținem $\Delta a + a = 0$, $\Delta b - b = 0$, $\Delta c - c = 0$, $\Delta d - d = 0$, de unde $a = 0$. Deoarece $h \neq 0$, neapărat unul dintre b, c, d este nenul și obținem $\Delta = 1$. Astfel mulțimea cuaternionilor $h = bi + cj + dk$, unde $b^2 + c^2 + d^2 = 1$ constituie mulțimea soluțiilor ecuației.

§ 5. IDEALE PRIME ȘI MAXIMALE

În acest paragraf inelele considerate vor fi comutative și unitare.

Definiția 5.1. Fie R un inel comutativ și unitar. Un ideal p al lui R se numește ideal **prim** dacă $p \neq A$ și dacă oricare ar fi $a, b \in R$ astfel încât $ab \in p$, rezultă că $a \in p$ sau $b \in p$.

Exemplu. 1) Dacă R este un inel, atunci idealul (0) este prim dacă și numai dacă R este domeniu de integritate.

Într-adevăr, dacă (0) este ideal prim și $a, b \in R$ astfel încât $ab = 0$, atunci $ab \in (0)$, de unde $a \in (0)$ sau $b \in (0)$, adică $a = 0$ sau $b = 0$. Reciproc, dacă R este domeniu de integritate rezultă evident din definiție că (0) este ideal prim.

2) Pentru inelul \mathbb{Z} al numerelor întregi, idealele prime sunt: (0) și $p\mathbb{Z}$ cu p număr prim.

Cum \mathbb{Z} este domeniu de integritate, (0) este ideal prim. Dacă p este număr prim, atunci idealul $p\mathbb{Z}$ este prim. Într-adevăr, $p\mathbb{Z} \neq \mathbb{Z}$ și

dacă $m, n \in \mathbb{Z}$ încit $mn \in p\mathbb{Z}$, atunci $p | mn$ și cum p este prim avem $p | m$ sau $p | n$ și deci $m \in p\mathbb{Z}$ sau $n \in p\mathbb{Z}$.

Reciproc, dacă $p\mathbb{Z}$ este ideal prim, atunci neapărat p este număr prim. Într-adevăr, avem $p \neq \pm 1$ și dacă $p | mn$, unde $m, n \in \mathbb{Z}$ atunci $mn \in p\mathbb{Z}$, de unde $m \in p\mathbb{Z}$ sau $n \in p\mathbb{Z}$, adică $p | m$ sau $p | n$.

Propoziția 5.2. Dacă R este un inel, atunci un ideal al său \underline{p} este prim dacă și numai dacă R/\underline{p} este domeniu de integritate.

Demonstrație. Dacă \underline{p} este ideal prim, atunci $\underline{p} \neq R$ și deci R/\underline{p} este inel nenul. Cum R este comutativ și unitar, inelul R/\underline{p} este de asemenea comutativ și unitar. Fie acum $\hat{a}, \hat{b} \in R/\underline{p}$ astfel încât $\hat{a}\hat{b} = \hat{0}$. Atunci $\hat{a}\hat{b} = \hat{0}$ adică $ab \in \underline{p}$ și cum \underline{p} este prim, rezultă $a \in \underline{p}$ sau $b \in \underline{p}$, adică $\hat{a} = \hat{0}$ sau $\hat{b} = \hat{0}$.

Reciproc, dacă R/\underline{p} este domeniu de integritate, atunci R/\underline{p} este nenul și deci $\underline{p} \neq R$. Dacă $a, b \in R$ astfel încât $ab \in \underline{p}$, atunci $\hat{a}\hat{b} = \hat{0}$ sau $\hat{a}\hat{b} = \hat{0}$ și cum R/\underline{p} este domeniu de integritate, rezultă $\hat{a} = \hat{0}$ sau $\hat{b} = \hat{0}$, adică $a \in \underline{p}$ sau $b \in \underline{p}$.

Propoziția 5.3. Fie $f: R \rightarrow R'$ un morfism unitar de inele. Atunci:

1) Dacă \underline{p}' este ideal prim în R' , atunci $f^{-1}(\underline{p}')$ este ideal prim în R .

2) Dacă, în plus, f este surjectiv și \underline{p} este ideal prim în R astfel încât $\underline{p} \supseteq \text{Ker } f$, atunci $f(\underline{p})$ este ideal prim în R' .

Demonstrație. 1) Fie \underline{p}' un ideal prim în R' și cum $\text{Im } f$ este subinel unitar al lui R' , din teorema a II-a de izomorfism rezultă că $\underline{p}' \cap \text{Im } f$ este ideal al lui R' , care evident este diferit de R' .

În plus, avem un izomorfism unitar

$$\text{Im } f + \underline{p}'/\underline{p}' \xrightarrow{\sim} \text{Im } f/\underline{p}' \cap \text{Im } f.$$

Dar $\text{Im } f + \underline{p}'/\underline{p}'$ fiind un subinel nenul al domeniului de integritate R'/\underline{p}' , rezultă că este, la rîndul său, un domeniu de integritate și, deci, $\text{Im } f/\text{Im } f \cap \underline{p}'$, este domeniu de integritate. Prin urmare $\text{Im } f \cap \underline{p}'$ este ideal prim în $\text{Im } f$. Din propoziția 3.3 avem că $I = f^{-1}(\text{Im } f \cap \underline{p}')$ este ideal al lui R și, mai mult, din teorema a II-a de izomorfism există un izomorfism de inele

$$R/I \xrightarrow{\sim} \text{Im } f/\underline{p}' \cap \text{Im } f.$$

Obținem astfel că R/I este domeniu de integritate, adică I este ideal prim al lui R . Dar, după cum se verifică ușor, $I = f^{-1}(\underline{p}')$ și deci $f^{-1}(\underline{p}')$ este ideal prim al lui R .

2) Din teorema I-a de izomorfism avem

$$R/\underline{p} \xrightarrow{\sim} R'/f(\underline{p}).$$

Cum R/\underline{p} este domeniu de integritate rezultă că $R'/f(\underline{p})$ este domeniu de integritate, adică $f(\underline{p})$ este ideal prim al lui R' .

Aplicație. Avind în vedere descrierea idealelor inelului \mathbf{Z}_n , dată în §3, ca și propoziția precedentă, rezultă că idealele prime ale lui \mathbf{Z}_n sunt de forma $p\mathbf{Z}/n\mathbf{Z}$ cu $p \mid n$, număr prim, adică sunt idealele principale (\hat{p}), cu $p \mid n$ număr prim.

Definiția 5.4. Fie R un inel comutativ și unitar. Un ideal \underline{m} al lui R se numește ideal maximal dacă $\underline{m} \neq R$ și dacă oricare ar fi idealul I al lui R astfel încât $\underline{m} \subset I \subset R$, rezultă că $I = \underline{m}$ sau $I = R$.

Exemplu. 1) În orice corp K idealul (0) este maximal.

Mai mult, dacă R este inel comutativ și unitar, nenul, astfel încât (0) este ideal maximal, atunci neapărat R este corp.

Într-adevăr, în acest caz R are doar două ideale (0) și R și după cum știm este un corp.

2) Pentru inelul \mathbf{Z} idealele maximale sunt: $p\mathbf{Z}$ cu p număr prim.

Într-adevăr, dacă p este număr prim, atunci $p\mathbf{Z} \neq \mathbf{Z}$ și dacă $I = n\mathbf{Z}$ este un ideal oarecare al lui \mathbf{Z} astfel încât $p\mathbf{Z} \subset n\mathbf{Z} \subset \mathbf{Z}$, rezultă $n \mid p$ de unde $n = \pm 1$ sau $n = \pm p$. Prin urmare $I = p\mathbf{Z}$ sau $I = \mathbf{Z}$. Reciproc, dacă $p\mathbf{Z}$ este ideal maximal, atunci $p\mathbf{Z} \neq \mathbf{Z}$ și deci $p \neq \pm 1$. Dacă $n \in \mathbf{Z}$ astfel încât $n \mid p$, atunci $p\mathbf{Z} \subset n\mathbf{Z} \subset \mathbf{Z}$ și cum $p\mathbf{Z}$ este maximal rezultă $n\mathbf{Z} = p\mathbf{Z}$ sau $n\mathbf{Z} = \mathbf{Z}$. De aici obținem că $p \mid n$ sau n inversabil, și deci $n = \pm p$ sau $n = \pm 1$.

Propoziția 5.5. Fie R un inel și $\underline{m} \neq R$ un ideal al său. Atunci următoarele afirmații sunt echivalente:

- 1) \underline{m} este maximal;
- 2) oricare ar fi $a \in R \setminus \underline{m}$, rezultă că $\underline{m} + (a) = R$;
- 3) R/\underline{m} este corp.

Demonstrație. 1) \Rightarrow 2). Fie \underline{m} un ideal maximal și $a \notin \underline{m}$. Atunci $\underline{m} + (a)$ este un ideal al lui R , care conține idealul \underline{m} . Mai mult, deoarece $a \notin \underline{m}$ și $a = 0 + 1a \in \underline{m} + (a)$ rezultă că $\underline{m} \neq \underline{m} + (a)$ și deci $\underline{m} + (a) = R$.

2) \Rightarrow 3) Fie $\hat{a} \in R/\underline{m}$, $\hat{a} \neq \hat{0}$. Atunci $a \notin \underline{m}$ și din $\underline{m} + (a) = R$ avem $\hat{1} \in \underline{m} + (a)$, adică $\hat{1} = x + \alpha a$ cu $x \in \underline{m}$ și $\alpha \in R$. Deci $\hat{1} = x + \alpha a = \hat{x} + \hat{\alpha} \hat{a} = \hat{0} + \hat{\alpha} \hat{a} = \hat{\alpha} \hat{a}$, adică a este element inversabil. Prin urmare R/\underline{m} este corp.

3) \Rightarrow 1) Fie morfismul canonic $p: R \rightarrow R/\underline{m}$ cu $\text{Ker } p = \underline{m}$. Dar R/\underline{m} fiind corp, atunci are numai două ideale și anume (0) și R/\underline{m} . Pe baza propoziției 3.3, rezultă evident că singurul ideal care conține \underline{m} este R însuși, adică \underline{m} este ideal maximal în R .

Corolarul 5.6. Dacă R este un inel comutativ și unitar, atunci orice ideal maximal în R este ideal prim în R .

Demonstrație. Dacă $\mathfrak{m} \subset R$ este ideal maximal, atunci R/\mathfrak{m} este corp și deci domeniu de integritate, adică \mathfrak{m} este ideal prim.

Observație. Reciproca corolarului precedent nu este în general adevărată. De exemplu, (0) este ideal prim în \mathbb{Z} , dar nu este maximal deoarece este cuprins în orice alt ideal al lui \mathbb{Z} .

Propoziția 5.7. Fie $f: R \rightarrow R'$ un morfism unitar surjectiv de inele. Atunci

1) Dacă \mathfrak{m}' este ideal maximal în R' , rezultă că $f^{-1}(\mathfrak{m}')$ este ideal maximal în R .

2) Dacă \mathfrak{m} este un ideal maximal în R astfel încât $\mathfrak{m} = \text{Ker } f$, rezultă că $f(\mathfrak{m})$ este ideal maximal în R' .

Demonstrație. Se poate proceda la fel ca la propoziția 5.3 și de aceea omitem demonstrația.

Aplicație. Un raționament analog celui folosit la descrierea idealelor prime ale inelului \mathbb{Z}_n ne va arăta că idealele maximale ale lui \mathbb{Z}_n sunt idealele principale (p) , cu $p \mid n$ număr prim, adică coincid cu idealele prime ale sale.

Vom da acum un rezultat important cunoscut sub numele de *lema lui Krull*.

Teorema 5.8. Fie R un inel comutativ și unitar. Atunci orice ideal al său $I \neq R$ este conținut într-un ideal maximal.

Demonstrație. Să considerăm mulțimea

$$\mathcal{P} = \{J \mid J \text{ ideal al lui } R, I \subset J \neq R\}.$$

Această mulțime este parțial ordonată prin inclusiune. Ea este inductiv ordonată. Într-adevăr, deoarece I este în \mathcal{P} , rezultă că \mathcal{P} este nevidă. Fie acum $\{I_\alpha\}_{\alpha \in A}$ o submulțime nevidă total ordonată a lui \mathcal{P} . Atunci $I = \bigcup_{\alpha \in A} I_\alpha$ este majorant al acesteia care aparține lui \mathcal{P} . Să arătăm mai întâi că I este un ideal. Dacă $x, y \in I$, atunci există $\alpha, \beta \in A$ astfel încât $x \in I_\alpha$ și $y \in I_\beta$. Familia $\{I_\alpha\}_{\alpha \in A}$ fiind total ordonată, să presupunem de exemplu că $I_\alpha \subset I_\beta$. Atunci $x, y \in I_\beta$ și cum I_β este ideal avem $x - y \in I_\beta$, de unde $x - y \in I$. Dacă $a \in R$ și $x \in I$, atunci există $\alpha \in A$ astfel încât $x \in I_\alpha$. Prin urmare $ax \in I_\alpha$, de unde $ax \in I$. Să arătăm acum că $I \neq R$. Presupunând prin absurd că $I = R$, rezultă $1 \in I$. Există deci $\alpha \in A$ astfel încât $1 \in I_\alpha$, adică $I_\alpha = R$, contradicție. Am demonstrat astfel că I este un majorant din \mathcal{P} al submulțimii total ordonate $\{I_\alpha\}_{\alpha \in A}$ a lui \mathcal{P} . Deci \mathcal{P} este inductiv ordonată. Conform lemei lui Zorn, \mathcal{P} are cel puțin un element maximal \mathfrak{m} . Atunci \mathfrak{m} este un ideal maximal al lui R care conține idealul I .

Corolarul 5.9. Orice element neinversabil al unui inel comutativ și unitar R aparține unui ideal maximal al lui R .

Demonstrație. Dacă $a \in R$ este neinversabil, atunci $(a) \neq R$ și conform lemei lui Krull există un ideal maximal \underline{m} astfel încât $(a) \subset \underline{m}$.

Corolarul 5.10. Orice inel comutativ și unitar are cel puțin un ideal maximal.

Demonstrație. Rezultă din lema lui Krull dacă luăm $I=(0)$.

Definiția 5.11. Un inel comutativ și unitar care are un singur ideal maximal se numește inel local.

De exemplu, orice corp comutativ este inel local. În paragrafele următoare vom întilni și alte exemple de inele locale.

Propoziția 5.12. Dacă R este un inel, următoarele afirmații sunt echivalente:

- 1) R este inel local.
- 2) Dacă $a, b \in R$ și $a+b=1$, atunci a sau b este inversabil.
- 3) Mulțimea elementelor neinversabile ale lui R formează un ideal.

Demonstrație. 1) \Rightarrow 2) Fie \underline{m} idealul maximal al lui R și $a, b \in R$ astfel încât $a+b=1$. Să presupunem, de exemplu, că a este neinversabil. Atunci avem că $(a) \neq R$ și conform lemei lui Krull, $(a) \subset \underline{m}$, adică $a \in \underline{m}$. Cum $\underline{m} \neq R$ rezultă $1 \notin \underline{m}$ adică $a+b \notin \underline{m}$ și deci $b \notin \underline{m}$. Conform corolarului 5.9, b este neapărat inversabil, adică $b \in U(R)$.

2) \Rightarrow 3) Trebuie să arătăm că $R \setminus U(R)$ formează un ideal. Fie $x, y \in R \setminus U(R)$ și să presupunem prin absurd că $x-y \in U(R)$. Atunci există $c \in R$ astfel încât $c(x-y)=1$ sau $cx+(-cy)=1$. Din 2) rezultă $cx \in U(R)$ sau $-cy \in U(R)$, de unde $x \in U(R)$ sau $y \in U(R)$, contradicție. Deci neapărat $x-y \in R \setminus U(R)$. Dacă $a \in R$ și $x \in R \setminus U(R)$, atunci este clar că $ax \in R \setminus U(R)$. Prin urmare, $R \setminus U(R)$ este un ideal al lui R .

3) \Rightarrow 1). Să presupunem că $R \setminus U(R)$ formează un ideal și fie \underline{m} un ideal maximal al lui R . Avem că $1 \in U(R)$ și deci $R \setminus U(R) \neq R$. Deoarece $\underline{m} \neq R$, orice element al lui \underline{m} este neinversabil și avem $\underline{m} \subset R \setminus U(R) \neq R$. Prin urmare $\underline{m}=R \setminus U(R)$ și deci $R \setminus U(R)$ este singurul ideal maximal al lui R , adică R este inel local.

§ 6. INELE DE FRACTII

În acest paragraf inelele considerate vor fi comutative și unitare.

Fie R un inel comutativ și unitar. O submulțime nevidă S a lui R care satisfac condițiile:

1° oricare ar fi $a, b \in S$, atunci $ab \in S$,

2° $0 \notin S$ și $1 \in S$,

se numește sistem multiplicativ (închis) al lui R .

Exemplu. 1) Dacă R este un inel, atunci $\{1\}$ este sistem multiplicativ al lui R .

2) Dacă R este inel și $a \in R$ un element oarecare, atunci mulțimea $S = \{a^n \mid n \in \mathbb{N}\}$ este un sistem multiplicativ al lui R .

3) Dacă R este inel, atunci mulțimea $U(R)$ a elementelor inversabile din R este sistem multiplicativ al lui R .

4) Dacă R este inel, atunci mulțimea S a nondivizorilor lui zero din R este sistem multiplicativ al lui R .

5) Dacă R este inel iar p este un ideal prim al lui R , atunci $S = R \setminus p$ este un sistem multiplicativ al lui R .

Având un inel R și $S \subset R$ un sistem multiplicativ al său, vom construi un inel care să satisfacă anumite condiții.

Propoziția 6.1. Fie R un inel comutativ și unitar iar S un sistem multiplicativ al lui R . Atunci există un inel comutativ și unitar $S^{-1}R$ și un morfism unitar de inele $i^S: R \rightarrow S^{-1}R$ astfel încât pentru orice $s \in S$, elementul $i^S(s)$ este inversabil în $S^{-1}R$ și, în plus, orice element din $S^{-1}R$ este de forma $i^S(a) i^S(s)^{-1}$, cu $a \in R$ și $s \in S$.

Demonstrație. Să considerăm produsul cartezian

$$R \times S = \{(a, s) \mid a \in R, s \in S\}.$$

Pe această mulțime definim o relație binară, notată „~”, în modul următor:

$(a, s) \sim (b, t)$ dacă și numai dacă există $r \in S$ astfel încât $r(at - bs) = 0$.

Relația „~” este o relație de echivalență.

1º Dacă $(a, s) \in R \times S$, atunci $(a, s) \sim (a, s)$ deoarece $1(as - as) = 0$. Deci relația este reflexivă.

2º Fie $(a, s), (b, t) \in R \times S$ astfel încit $(a, s) \sim (b, t)$. Atunci există $r \in S$ astfel încât $r(at - bs) = 0$. Atunci $r(bs - at) = -r(at - bs) = 0$ adică $(b, t) \sim (a, s)$. Deci relația este tranzitivă.

3º Fie $(a, s), (b, t), (c, u) \in R \times S$ astfel încit $(a, s) \sim (b, t)$ și $(b, t) \sim (c, u)$. Atunci există $r, v \in S$ astfel încit $r(at - bs) = 0$ și $v(bu - ct) = 0$. Deci $vur(at - bs) = 0$, $rsv(bu - ct) = 0$ și adunind aceste egalități obținem $vrt(au - cs) = 0$. Deoarece $vrt \in S$ rezultă $(a, s) \sim (c, u)$ și deci relația este tranzitivă.

Să notăm cu $S^{-1}R$ mulțimea factor $R \times S / \sim$, iar clasa de echivalență a perechii (a, s) o vom nota cu $\frac{a}{s}$. Deci

$$S^{-1}R = \left\{ \frac{a}{s} \mid a \in R, s \in S \right\}.$$

Pe mulțimea $S^{-1}R$ definim două operații algebrice, adunarea și înmulțirea, în modul următor:

$$\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st},$$

$$\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st},$$

oricare ar fi $\frac{a}{s}, \frac{b}{t} \in S^{-1}R$.

Observăm că, deoarece $s, t \in S$, atunci $st \in S$ și deci membrii drepti ai relațiilor precedente au sens. Să arătăm că operațiile algebrice sunt bine definite. Într-adevăr, dacă $\frac{a}{s} = \frac{a'}{s'}, \frac{b}{t} = \frac{b'}{t'}$, atunci $(a, s) \sim (a', s')$, $(b, t) \sim (b', t')$ și deci există $u, v \in S$ astfel încât $u(as' - a's) = 0$, $v(bt' - b't) = 0$. Prin urmare $vt'u(as' - a's) = 0$, $us'v(bt' - b't) = 0$ și adunând aceste egalități obținem $uv((at+bs)s't' - (a't'+b's')st) = 0$. Deoarece $uv \in S$, rezultă

$$(at+bs, st) \sim (a't'+b's', s't')$$

și deci

$$\frac{at+bs}{st} = \frac{a't'+b's'}{s't'}$$

ceea ce arată că adunarea este bine definită.

Analog, se arată că produsul este bine definit.

Mulțimea $S^{-1}R$ împreună cu operațiile algebrice definite mai înainte formează un inel comutativ și unitar.

Să arătăm, de exemplu, asociativitatea adunării.

Dacă $\frac{a}{s}, \frac{b}{t}, \frac{c}{u} \in S^{-1}R$, atunci

$$\left(\frac{a}{s} + \frac{b}{t} \right) + \frac{c}{u} = \frac{at+bs}{st} + \frac{c}{u} = \frac{(at+bs)u + c(st)}{(st)u} = \frac{atu + bsu + cst}{stu}.$$

Pe de altă parte,

$$\frac{a}{s} + \left(\frac{b}{t} + \frac{c}{u} \right) = \frac{a}{s} + \frac{bu+ct}{tu} = \frac{a(tu) + (bu+ct)s}{s(tu)} = \frac{atu + bus + cts}{stu}.$$

Deci

$$\left(\frac{a}{s} + \frac{b}{t} \right) + \frac{c}{u} = \frac{a}{s} + \left(\frac{b}{t} + \frac{c}{u} \right).$$

Remarcăm că elementul 0 al lui $S^{-1}R$ este $\frac{0}{1} = \frac{0}{s}$, oricare ar fi

$s \in S$. Elementul opus al lui $\frac{a}{s}$ este $\frac{-a}{s}$, iar elementul unitate 1 al lui $S^{-1}R$ este $\frac{1}{1} = \frac{s}{s}$, oricare ar fi $s \in S$.

Definim $i^S: R \rightarrow S^{-1}R$ prin $i^S(a) = \frac{a}{1}$. Funcția i^S este un morfism unitar de inele. Într-adevăr,

$$i^S(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = i^S(a) + i^S(b),$$

$$i^S(ab) = \frac{ab}{1} = \frac{a}{1} \frac{b}{1} = i^S(a)i^S(b),$$

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

$$\text{În plus, } i^S(1) = \frac{1}{1} = 1.$$

Dacă $s \in S$, atunci $i^S(s) = \frac{s}{1}$ este inversabil, inversul său fiind $\frac{1}{s}$,

$$\text{deoarece } \frac{s}{1} \frac{1}{s} = \frac{s}{s} = \frac{1}{1} = 1.$$

Dacă $\frac{a}{s}$ este un element oarecare din $S^{-1}R$, atunci $\frac{a}{s} = \frac{a}{1} \frac{1}{s} = i^S(a)i^S(s)^{-1}$.

Definiția 6.2. Fiind dat inelul comutativ și unitar R , iar $S \subset R$ un sistem multiplicativ al său, atunci inelul $S^{-1}R$ se numește *inelul de fracții al lui R , în raport cu S* , sau *cu numitorii în S* și se mai notează R_S .

Morfismul de inele $i^S: R \rightarrow S^{-1}R$ se numește *morfismul canonic*.

Exemplu. Fie R un inel și $S \subset R$ un sistem multiplicativ al său, care nu conține divizori ai lui zero. Dacă $(a, s), (b, t) \in R \times S$, atunci $(a, s) \sim (b, t)$ dacă și numai dacă există $r \in S$ astfel încât $r(at - bs) = 0$. Cum r nu este divizor al lui zero, avem că $r(at - bs) = 0$ dacă și numai dacă $at - bs = 0$, adică $at = bs$. Prin urmare, în acest caz, $(a, s) \sim (b, t)$ dacă și numai dacă $at = bs$.

Mai mult, morfismul canonic $i^S: R \rightarrow S^{-1}R$ este injectiv. Într-adevăr, dacă $i^S(a) = 0$, atunci $\frac{a}{1} = 0$, adică $a = 0$.

În cazul particular în care S este mulțimea tuturor nondivizorilor lui zero din R , atunci inelul $S^{-1}R$ se numește *inelul total de fracții al inelului R* .

2) Dacă R este un domeniu de integritate, atunci $S=R \setminus \{0\}$ este mulțimea tuturor nondivizorilor lui zero din R . În acest caz, inelul (total) de fracții $S^{-1}R$ este un corp, pe care-l vom nota $K(R)$ sau, mai simplu, K , dacă nu este pericol de confuzie.

Într-adevăr, dacă $\frac{a}{s} \neq 0$, atunci $a \neq 0$, adică $a \in S$. Deci are sens

$$\frac{s}{a} \text{ și } \frac{a}{s} \cdot \frac{s}{a} = \frac{as}{sa} = \frac{1}{1} = 1.$$

Prin urmare, elementul $\frac{a}{s}$ este inversabil, inversul său fiind $\frac{s}{a}$.

Acest corp se numește *corpul de fracții al domeniului de integritate R* .

În particular, dacă $A=\mathbb{Z}$, atunci corpul de fracții al domeniului de integritate \mathbb{Z} este corpul \mathbb{Q} al numerelor raționale.

Vom da în continuare o proprietate importantă a inelelor de fracții, numită *proprietatea de universalitate*.

Teorema 6.3. *Fie R un inel comutativ și unitar și S un sistem multiplicativ al lui R . Atunci inelul de fracții $S^{-1}R$ împreună cu morfismul canonic $i^S: R \rightarrow S^{-1}R$ au următoarea proprietate (de universalitate):*

(PU) *Oricare ar fi inelul comutativ și unitar T și morfismul unitar de inele $\varphi: R \rightarrow T$ astfel încât $\varphi(s)$ este inversabil pentru orice $s \in S$, există un morfism unitar de inele $\psi: S^{-1}R \rightarrow T$, unic determinat, astfel încât diagrama*

$$\begin{array}{ccc} R & \xrightarrow{i^S} & S^{-1}R \\ \varphi \searrow & & \swarrow \psi \\ & T & \end{array}$$

să fie comutativă, adică $\psi \circ i^S = \varphi$.

Demonstrație. Definim $\psi: S^{-1}R \rightarrow T$ prin $\psi\left(\frac{a}{s}\right) = \varphi(a)\varphi(s)^{-1}$. Să arătăm că ψ este într-adevăr o funcție, adică nu depinde de alegerea reprezentanților. Dacă $\frac{a}{s} = \frac{a'}{s'}$, atunci există $r \in S$ astfel încât $r(as' - a's) = 0$. Deci $\varphi(r(as' - a's)) = \varphi(0)$ sau $\varphi(r)(\varphi(a)\varphi(s') - \varphi(a')\varphi(s)) = 0$ și prin înmulțirea ambilor membri cu $\varphi(r)^{-1}\varphi(s')^{-1}\varphi(s)^{-1}$, obținem $\varphi(a)\varphi(s)^{-1} = \varphi(a')\varphi(s')^{-1}$. Deci $\psi\left(\frac{a}{s}\right) = \psi\left(\frac{a'}{s'}\right)$, adică ψ este corect definită. Funcția

ψ este un morfism unitar de inele. Într-adevăr, dacă $\frac{a}{s}, \frac{b}{t} \in S^{-1}R$, atunci $\psi\left(\frac{a}{s} + \frac{b}{t}\right) = \psi\left(\frac{at+bs}{st}\right) = \varphi(at+bs)\varphi(st)^{-1} = (\varphi(a)\varphi(t) + \varphi(b)\varphi(s))\varphi(s)^{-1}\varphi(t)^{-1} = \varphi(a)\varphi(s)^{-1} + \varphi(b)\varphi(t)^{-1} = \psi\left(\frac{a}{s}\right) + \psi\left(\frac{b}{t}\right)$.

Analog, avem $\psi\left(\frac{a}{s} \cdot \frac{b}{t}\right) = \psi\left(\frac{a}{s}\right)\psi\left(\frac{b}{t}\right)$.

De asemenea, $\psi(1) = \psi\left(\frac{1}{1}\right) = \varphi(1)\varphi(1)^{-1} = 1$.

Dacă $a \in R$, atunci $(\psi \circ i^S)(a) = \psi(i^S(a)) = \psi\left(\frac{a}{1}\right) = \varphi(a)\varphi(1)^{-1} = \varphi(a)$ și deci $\psi \circ i^S = \varphi$.

Să demonstrăm acum unicitatea. Dacă $\psi': S^{-1}A \rightarrow T$ este un morfism de inele astfel încât $\psi' \circ i^S = \varphi$, atunci, oricare ar fi $\frac{a}{s} \in S^{-1}R$,

$\psi'\left(\frac{a}{s}\right) = \psi'\left(\frac{a}{1} \cdot \frac{1}{s}\right) = \psi'(i^S(a)i^S(s)^{-1}) = \psi'(i^S(a))(\psi'(i^S(s)))^{-1} = \varphi(a)\varphi(s)^{-1} = \psi\left(\frac{a}{s}\right)$. Deci $\psi' = \psi$.

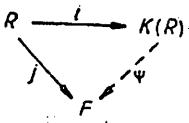
Am observat mai înainte că pentru un domeniu de integritate R , inelul de fracții al său în raport cu sistemul multiplicativ $S = R \setminus \{0\}$ este un corp, pe care l-am notat cu $K(R)$. Mai mult, morfismul canonic $i: R \rightarrow K(R)$ este injectiv. Astfel obținem un izomorfism al lui R cu $\text{Im } i = \left\{ \frac{a}{1} \mid a \in R \right\}$, care este un subinel al lui $K(R)$, dat prin $a \mapsto \frac{a}{1}$.

Acest izomorfism ne permite identificarea lui R cu imaginea sa în $K(R)$ și a lui a din R cu $\frac{a}{1}$ din $K(R)$. Putem considera deci că R este un subinel al lui $K(R)$.

Următorul rezultat ne va arăta că printre corpurile care conțin pe R ca subinel, corpul $K(R)$ are o proprietate de minimalitate.

Propoziția 6.4. *Fie R un domeniu de integritate și $K(R)$ corpul său de fracții. Dacă R este subinel unitar al unui corp comutativ F , atunci $K(R)$ este izomorf cu un subcorp al acestuia.*

Demonstrație. Condițiile teoremei 6.2 fiind evident satisfăcute, obținem diagrama comutativă



unde i este morfismul canonic, j este morfismul de incluziune iar morfismul ψ este definit prin

$$\psi\left(\frac{a}{s}\right) = j(a)j(s)^{-1} = as^{-1},$$

oricare ar fi $\frac{a}{s} \in K(R)$. Cum ψ este morfism de corpuri, rezultă injectivitatea sa și deci corpul $K(R)$ este izomorf cu $\text{Im } \psi$ care este un subcorp al lui F .

Observații. Dacă R este un inel și S un sistem multiplicativ al său, să considerăm morfismul canonic $i^S: R \rightarrow S^{-1}R$.

Este clar că avem

$$\text{Ker } i^S = \{a \in R \mid \text{există } s \in S \text{ astfel încât } sa = 0\}.$$

Observăm că morfismul canonic este injectiv dacă și numai dacă S nu conține divizori ai lui zero.

Exemplu. Fie R un inel comutativ și unitar, p un ideal prim al său și sistemul multiplicativ $S = R \setminus p$ al lui R . Inelul de fracții $S^{-1}R$ al lui R în raport cu S se mai notează cu R_p . Inelul R_p este local.

Intr-adevăr, fie $\frac{a}{s}, \frac{b}{t} \in R_p$ astfel încât $\frac{a}{s} + \frac{b}{t} = 1$. Atunci $\frac{at+bs}{st} = 1$, adică există $u \in S$ astfel încât $u(at+bs-st)=0$, de unde $ust = uat+ubs$. Deoarece $ust \in S$ avem că $ust \notin p$ și deci $uat+ubs \notin p$, de unde rezultă că $uat \notin p$ sau $ubs \notin p$.

Prin urmare $a \notin p$ sau $b \notin p$. Dacă presupunem că $a \notin p$, atunci $a \in S$ și deci există $\frac{s}{a}$ care este inversul elementului $\frac{a}{s}$. Astfel am arătat că $\frac{a}{s}$ este inversabil. Dacă $b \notin p$, atunci rezultă că mai înainte că $\frac{b}{s}$ este element inversabil în R_p .

După propoziția 5.12 obținem că R_p este inel local. Inelul R_p se mai numește localizatul lui R în idealul prim p . Idealul său maximal este

$$pR_p = \left\{ \frac{x}{s} \mid x \in p \text{ și } s \notin p \right\}.$$

§ 7. INELE DE POLINOAME

Fie R un inel comutativ și unitar. Vom da mai întii o construcție a inelului serilor formale peste R . Fie R^N mulțimea funcțiilor de la N în R . Dacă scriem o astfel de funcție prin mulțimea ordonată a valorilor sale, atunci R^N este mulțimea sirurilor

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

pentru orice $i \in N$.

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.

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

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

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

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

Înmulțirea pe R^N este asociativă, comutativă și are element unicitate

$$(1, 0, 0, \dots).$$

Să demonstrăm asociativitatea înmulțirii.

Fie $f, g, h \in R^N$, unde

$$f = (a_0, a_1, a_2, \dots), \quad g = (b_0, b_1, b_2, \dots), \quad h = (c_0, c_1, c_2, \dots)$$

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 $e_m = \sum_{k+l=m} d_k c_l$.

Avem

$$\begin{aligned} e_m &= \sum_{k+l=m} d_k c_l = \sum_{k+l=m} \left(\sum_{i+j=k} a_i b_j \right) c_l = \\ &= \sum_{\substack{k+l=m \\ i+j=k}} a_i b_j c_l = \sum_{i+j+l=m} a_i b_j c_l. \end{aligned}$$

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

iar $f(gh) = (e'_0, e'_1, e'_2, \dots)$, unde $e'_m = \sum_{i+k=m} a_i d'_k$, avem

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

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 inelului R^N construit mai înainte se numesc *serii formale* cu coeficienți în R .

Fie funcția $u: R \rightarrow R^N$ definită prin

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

Avem că u este un morfism injectiv de inele.

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

$$u(a+b) = (a+b, 0, 0, \dots) = (a, 0, 0, \dots) + (b, 0, 0, \dots) = u(a) + u(b)$$

$$\text{și } u(ab) = (ab, 0, 0, \dots) = (a, 0, 0, \dots)(b, 0, 0, \dots) = u(a)u(b).$$

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

Morfismul u dă un izomorfism al lui R pe subinelul $R' = \{(a, 0, 0, \dots) | a \in R\}$ 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 seria formală $(0, 1, 0, \dots)$ care se numește *nedeterminata X*.

Înmulțirea seriilor formale ne dă $X^2 = (0, 0, 1, 0, \dots)$ și, mai general, pentru orice număr natural i

$$X^i = \underbrace{(0, 0, \dots, 0)}_{i \text{ ori}}, \quad 1, 0, \dots).$$

Fie $f = (a_0, a_1, a_2, \dots, a_n, \dots)$ o serie formală din R^N .

Folosind adunarea și înmulțirea definite pe R^N se obține

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

Mai mult, după cele precedente putem scrie

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

obținând astfel scrierea obișnuită a unei serii formale.

Inelul R^N se numește *inelul seriilor formale în nedeterminata X* cu coeficienți în inelul R și se notează prin $R[[X]]$. Inelul $R[[X]]$ se mai numește și *inelul seriilor formale într-o nedeterminată*.

O serie formală în nedeterminata X o vom scrie, condensat,

$$f = \sum_{i \geq 0} a_i X^i,$$

aceasta fiind pur și simplu o notație, fără sens de adunare.

O serie formală din $R[[X]]$ care are doar un număr finit de coeficienți nenuli se numește *polinom* cu coeficienți în R . Notăm cu $R[X]$ mulțimea polinoamelor peste R .

Dacă f este un polinom cu coeficienți în R , $f = \sum_{i \geq 0} a_i X^i$, există un număr natural m astfel încât $a_i = 0$, pentru orice $i > m$.

Dacă $f = \sum_{i \geq 0} a_i X^i$ este un polinom nenul din $R[X]$, atunci $n = \max \{i \mid a_i \neq 0\}$ se numește *gradul* polinomului f , și se notează cu $\text{grad}(f)$. 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 $n = \text{grad}(f)$, f nenul, atunci a_0, a_1, \dots, a_n se numesc coeficienții polinomului f , care se va scrie

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

Propoziția 7.1. *Mulțimea $R[X]$ a polinoamelor împreună cu adunarea și înmulțirea seriilor formale, formează un inel.*

Demonstrație. Este clar că dacă f și g sunt polinoame din $R[X]$, atunci $f - g$ și fg sunt de asemenea polinoame din $R[X]$. Prin urmare $R[X]$ este un subinel al inelului seriilor formale și deci la rîndul său este un inel.

Acest inel se numește *inelul polinoamelor în nedeterminata X*, cu coeficienți în inelul R sau *inelul polinoamelor într-o nedeterminată*.

Propoziția 7.2. *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 coeficienții dominanti ai lui f și g nu sunt divizori ai 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 făcute:

$-\infty < n$, $-\infty + n = -\infty$, 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 $f = \sum_{i=0}^m a_i X^i$, $a_m \neq 0$, $g = \sum_{i=1}^n b_i X^i$, $b_n \neq 0$, astfel încât a_m și b_n să

nu fie divizori ai 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

Corolarul 7.3. *Dacă R este domeniu de integritate și f, g polinoame din $R[X]$, atunci*

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

Observație. Dacă R nu este domeniu de integritate, inegalitatea 2) poate fi strictă. De exemplu, fie polinoamele $f = \hat{1} + \hat{2}X$ și $g = \hat{2}X^2$ din inelul $\mathbb{Z}_4[X]$. 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.

Propoziția 7.4. *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, după corolarul 7.3 este clar că $R[X]$ este domeniu de integritate. Din punctul precedent rezultă că $U(R) \subset U(R[X])$. Pentru a demonstra inclusiunea 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 $f = a_0 \in U(R)$.

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 $(\hat{1} + \hat{2}X)(\hat{1} + \hat{2}X) = \hat{1}$.

Observații. Fie $R[[X]]$ inelul seriilor formale de o nedeterminată și $f = \sum_{i \geq 0} a_i X^i$ un element al său. Dacă $f \neq 0$, atunci $k = \min \{i \mid a_i \neq 0\}$ se numește *ordinul* seriei formale f și se notează $\text{ord}(f)$. Pentru seria formală nulă convenim să considerăm ordinul său ca fiind $+\infty$. Dacă $f \neq 0$ și $\text{ord}(f) = k$, atunci

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

Au loc următoarele proprietăți, analoage celor de la polinoame.

- 1) Dacă R este un inel și f, g serii formale din $R[[X]]$, atunci $\text{ord}(f+g) \geq \min(\text{ord}(f), \text{ord}(g))$; $\text{ord}(fg) \geq \text{ord}(f) + \text{ord}(g)$.

În plus, dacă R este domeniu de integritate, a doua dintre aceste inegalități devine egalitate.

2) Dacă R este domeniu de integritate, atunci $R[[X]]$ este domeniu de integritate.

3) Dacă $f = \sum_{i \geq 0} a_i X^i$ aparține lui $R[[X]]$, R inel comutativ, atunci f este inversabilă în $R[[X]]$ dacă și numai dacă a_0 este inversabil în R .

Demonstrația proprietăților 1) și 2) se face cu ușurință. Vom demonstra 3). Fie $f = \sum_{i \geq 0} a_i X^i$ inversabilă în $R[[X]]$. Atunci există $g = \sum_{i \geq 0} b_i X^i$ astfel încât $fg = 1$, de unde rezultă $a_0 b_0 = 1$. Reciproc, dacă $f = \sum_{i \geq 0} a_i X^i$ este o serie formală cu a_0 inversabil în R , atunci vom construi o serie formală $h = \sum_{i \geq 0} c_i X^i$ astfel încât $fh = 1$. Această relație ne va conduce la un sistem (infinit) de ecuații cu necunoscutele $\{c_i\}_{i \geq 0}$, a cărui rezolvare se face pas cu pas. Obținem următorul sistem de ecuații:

$$a_0 c_0 = 1, \quad a_0 c_1 + a_1 c_0 = 0, \quad \dots, \quad \sum_{i+j=k} a_i c_j = 0, \quad \dots .$$

Soluția sistemului se obține raționind inductiv. Avem $c_0 = a_0^{-1}$, $c_1 = -a_0^2 a_1$, $c_2 = a_1^2 a_0^{-3} - a_2 a_0^{-2}$. În general, dacă cunoaștem $c_0, c_1, c_2, \dots, c_{k-1}$, atunci c_k se obține din relația $a_k c_0 + a_{k-1} c_1 + \dots + a_0 c_k = 0$ prin înmulțire cu a_0^{-1} .

De exemplu,

$$(1+X)^{-1} = \sum_{i \geq 0} (-1)^i X^i.$$

În particular, pentru inelul $K[[X]]$ al seriilor formale cu coeficienți într-un corp comutativ, un element $f = \sum_{i=0}^{\infty} a_i X^i$ este inversabil în $K[[X]]$ dacă și numai dacă $a_0 \neq 0$.

Prin urmare, mulțimea elementelor neinversabile din $K[[X]]$, adică a seriilor formale fără termen liber, formează un ideal. Deci $K[[X]]$ este un inel local.

Dacă R este un inel comutativ și unitar, $R[X]$ inelul polinoamelor în nedeterminată X cu coeficienți în R , avem morfismul unitar de inele

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

numit *morfismul canonice* de la R la $R[X]$.

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

Teorema 7.5. Fie R un inel comutativ și unitar, $R[X]$ inelul polinoamelor de o nedeterminată cu coeficienți în R , $u: R \rightarrow R[X]$ morfismul canonice. 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

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

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

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

$$\varphi(f+g) = \varphi\left(\sum_{i=0}^n (a_i + b_i) X^i\right) = \sum_{i=0}^n v(a_i + b_i)x^i =$$

$$\begin{aligned}
 &= \sum_{t=0}^n (v(a_t) + v(b_t))x^t = \sum_{t=0}^n v(a_t)x^t + \sum_{t=0}^n v(b_t)x^t = \\
 &= \sum_{t=0}^n v(a_t)x^t + \sum_{t=0}^n v(b_t)x^t = \varphi(f) + \varphi(g).
 \end{aligned}$$

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

$$v(c_k) = \sum_{i+j=k} v(a_i)v(b_j).$$

Tinind seamă de acest lucru se verifică imediat că $v(fg) = v(f)v(g)$. Deci φ este morfism de inele. Mai mult, $\varphi(X) = \varphi(1X) = v(1)x = 1x = x$.

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 încit $\bar{\varphi}(X) = x$ și $\bar{\varphi} \circ u = v$. Atunci, pentru $f = \sum_{t=0}^m a_t X^t$, avem

$$\begin{aligned}
 \bar{\varphi}(f) &= \bar{\varphi}\left(\sum_{t=0}^m a_t X^t\right) = \sum_{t=0}^m \bar{\varphi}(a_t) \bar{\varphi}(X^t) = \sum_{t=0}^m \bar{\varphi}(u(a_t)) (\bar{\varphi}(X))^t = \\
 &= \sum_{t=0}^m v(a_t) x^t = \varphi(f)
 \end{aligned}$$

și deci $\bar{\varphi} = \varphi$. Astfel am demonstrat unicitatea lui φ .

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

$$\varphi(f) = \varphi\left(\sum_{t=0}^m a_t X^t\right) = \sum_{t=0}^m a_t x^t.$$

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

Fiind dat un polinom arbitrar f 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 fiecărui polinom f din $R[X]$ și fiecărui șir S care conține pe R ca subinel să corespundă o funcție definită pe S cu valori în S .

Orice 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*.

Având în vedere cele precedente, pot fi funcții polinomiale \tilde{f} care să fie constante, chiar cind $f \notin R$. Dar numai acele polinoame care sunt în R se numesc constante.

Observație. Dacă R este un inel și f, g sint polinoame din $R[X]$, atunci este evident că funcțiile polinomiale \tilde{f} și \tilde{g} sint egale. Există însă și polinoame diferite care să aibă funcțiile polinomiale egale. De exemplu, să considerăm $f = X + 1$ și $g = X^2 + 1$ polinoame din $Z_2[X]$, și fie, $\tilde{f}: Z_2 \rightarrow Z_2$, $\tilde{g}: Z_2 \rightarrow Z_2$ funcțiile polinomiale asociate lui f și g . Avem $\tilde{f}(0) = \tilde{g}(0) = 1$ și $\tilde{f}(1) = \tilde{g}(1) = 0$. Deci $\tilde{f} = \tilde{g}$ dar, evident, $f \neq g$.

Am construit mai înainte inelul polinoamelor într-o nedeterminată cu coeficienți într-un inel R . În continuare vom defini, prin inducție matematică, *inelul polinoamelor într-un număr finit de nedeterminante*.

Dacă R este un inel, atunci inelul polinoamelor în nedeterminatele X_1, X_2, \dots, X_n cu coeficienți în inelul R , notat prin $R[X_1, X_2, \dots, X_n]$, se definește inductiv astfel: $R[X_1]$ este inelul polinoamelor în nedeterminata X_1 cu coeficienți în inelul R , $R[X_1, X_2]$ este inelul polinoamelor în nedeterminata X_2 cu coeficienți în inelul $R[X_1]$ și, în general, $R[X_1, X_2, \dots, X_n]$ este inelul polinoamelor în nedeterminata X_n cu coeficienți în inelul $R[X_1, X_2, \dots, X_{n-1}]$.

Deci $R[X_1]$ l-am construit și atunci

$$R[X_1, X_2] = R[X_1][X_2], \dots, R[X_1, X_2, \dots, X_n] = R[X_1, X_2, \dots, X_{n-1}][X_n].$$

Analog, plecind de la $R[[X_1]]$, se definește inductiv inelul $R[[X_1, X_2, \dots, X_n]]$ al seriilor formale în nedeterminatele X_1, X_2, \dots, X_n .

Dacă f este un polinom din inelul $R[X_1, X_2, \dots, X_n]$, atunci el este un polinom în nedeterminata X_n cu coeficienți în $R[X_1, X_2, \dots, X_{n-1}]$ și deci

$$f = f_0 + f_1 X_n + \dots + f_{k_n} X_n^{k_n}, \text{ unde } f_i \in R[X_1, X_2, \dots, X_{n-1}],$$

pentru orice $i = 0, 1, \dots, k_n$. Este clar că, din aproape în aproape, f se scrie ca o sumă finită de forma

$$\sum a_{i_1 i_2 \dots i_n} X_1^{i_1} X_2^{i_2} \dots X_n^{i_n},$$

în care elementele $a_{i_1 i_2 \dots i_n}$ din R se numesc *coeficienții* polinomului f .

Propoziția 7.6. Orice polinom f din inelul $R[X_1, X_2, \dots, X_n]$ are o scriere unică sub forma

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

Demonstrație. Am observat mai înainte că polinomul f se scrie sub forma indicată. Să arătăm că o astfel de scriere este unică, ceea ce este echivalent cu faptul că dacă $f=0$, atunci toți coeficienții polinomului f sunt nuli.

Demonstrația o facem prin inducție matematică după numărul n de nedeterminate.

Pentru $n=1$, afirmația este clară deoarece avem de-a face cu polinoame într-o nedeterminată. Fie acum $f \in R[X_1, X_2, \dots, X_n]$. Avem $f=f_0+f_1X_n+\dots+f_{k_n}X_n^{k_n}$, unde $f_i \in R[X_1, X_2, \dots, X_{n-1}]$ pentru orice $i=0, 1, \dots, k_n$. Atunci fiecare f_i are o scriere unică

$$f_i = \sum_{i_1, i_2, \dots, i_{n-1}=0}^{k_1, k_2, \dots, k_{n-1}} a_{i_1 i_2 \dots i_{n-1}} X_1^{i_1} X_2^{i_2} \dots X_{n-1}^{i_{n-1}},$$

și deci

$$f_i X_n^i = \sum_{i_1, i_2, \dots, i_{n-1}=0}^{k_1, k_2, \dots, k_{n-1}} a_{i_1 i_2 \dots i_{n-1}} X_1^{i_1} X_2^{i_2} \dots X_{n-1}^{i_{n-1}} X_n^i,$$

pentru orice $i=0, 1, \dots, k_n$.

Observăm că, orice coeficient $a_{i_1 i_2 \dots i_n}$ apare drept coeficient al unuia dintre polinoamele f_i , $0 \leq i \leq k_n$. Atunci dacă $f=0$, ținând seama că f este polinom în nedeterminata X_n cu coeficienții $f_0, f_1 \dots, f_{k_n}$, rezultă $f_0=f_1=\dots=f_{k_n}=0$.

Dar oricare f_i este polinom în $n-1$ nedeterminate și deci conform presupunerii inductive rezultă că toți coeficienții acestora sunt nuli. Deoarece orice coeficient $a_{i_1 i_2 \dots i_n}$ al polinomului f este coeficient al unuia dintre polinoamele f_i , rezultă că toți coeficienții polinomului f sunt nuli, adică unicitatea scrierii lui f sub forma indicată.

Dacă f este un polinom din inelul $R[X_1, X_2, \dots, X_n]$, gradul lui f relativ la nedeterminata X_i , $i=1, 2, \dots, n$, este cel mai mare exponent la care figurează X_i în expresia lui f . Cind acesta este zero înseamnă că nedeterminata X_i nu apare în expresia lui f . Un polinom de forma $aX_1^{i_1} X_2^{i_2} \dots X_n^{i_n}$, $a \neq 0$, se numește monom, iar prin gradul său înțelegem suma $i_1+i_2+\dots+i_n$ și scriem

$$\text{grad}(a X_1^{i_1} X_2^{i_2} \dots X_n^{i_n}) = i_1 + i_2 + \dots + i_n.$$

Fie acum

$$f = \sum_{t_1, t_2, \dots, t_n=0}^{k_1, k_2, \dots, k_n} a_{t_1 t_2 \dots t_n} X_1^{t_1} X_2^{t_2} \dots X_n^{t_n},$$

un polinom scris ca sumă de monoame, scrierea fiind unică. Aceste monoame se numesc *termenii* polinomului. Gradul polinomului f , notat prin $\text{grad}(f)$, se definește astfel:

$$\text{grad}(f) = \begin{cases} -\infty, & \text{dacă } f=0, \\ \text{maximul gradelor termenilor săi,} & \text{dacă } f \neq 0. \end{cases}$$

Observăm că în scrierea lui f pot să apară termeni diferenți care să aibă același grad.

Dacă toți termenii unui polinom f din $R[X_1, X_2, \dots, X_n]$ au același grad, atunci f se numește *polinom omogen* sau *formă*. Fiind date două polinoame omogene, atunci fg este sau polinomul nul sau un polinom omogen nenul de grad egal cu $\text{grad}(f)+\text{grad}(g)$.

Polinomul $f \neq 0$ de grad n , se scrie în mod unic sub forma

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

unde fiecare f_i este sau nul sau un polinom omogen de grad i și $f_n \neq 0$. Polinoamele f_i , $0 \leq i \leq n$, se numesc *componentele omogene* ale polinomului f .

Propoziția 7.7. Fie R un inel și f, g polinoame din $R[X_1, X_2, \dots, X_n]$. Atunci

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

3) Dacă în plus R este domeniu de integritate, atunci $R[X_1, X_2, \dots, X_n]$ este de asemenea domeniu de integritate, și la pct. 2) avem egalitate.

Demonstrație. Afirmațiile 1) și 2) sunt clare dacă avem în vedere scrierea polinoamelor f și g ca sumă de polinoame omogene. Vom detalia demonstrația afirmației 3), care o vom face prin inducție după n . Într-adevăr, pentru $n=1$ s-a arătat în corolarul 7.3. Dacă presupunem acum că $R[X_1, X_2, \dots, X_{n-1}]$ este domeniu de integritate, atunci aşa va fi și $R[X_1, X_2, \dots, X_n]$, deoarece

$$R[X_1, X_2, \dots, X_n] = R[X_1, X_2, \dots, X_{n-1}] [X_n].$$

Fie acum f și g polinoame nenule de grad p și q respectiv. Scriem $f = f_0 + f_1 + \dots + f_p$, $g = g_0 + g_1 + \dots + g_q$, cu $f_p \neq 0$ și $g_q \neq 0$, iar f_i și g_i sint

sau egale cu zero, sau polinoame omogene de grad i și j respectiv. Avem

$$fg = \sum_{k=0}^{p+q} h_k, \quad h_k = \sum f_i g_j.$$

Deoarece $R[X_1, X_2, \dots, X_n]$ este domeniu de integritate, atunci $h_{p+q} = f_p g_q$, de unde relația

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

Funcția $u: R \rightarrow R[X_1, X_2, \dots, X_n]$, definită prin $u(a) = a$, este un morfism unitar de inele, pe care-l vom numi *morfismul canonic* de la R la $R[X_1, X_2, \dots, X_n]$.

Vom da acum proprietatea de universalitate a inelelor de polinoame în n nedeterminate, analoagă celei pentru cazul unei singure nedeterminate dată în teorema 7.5.

Teorema 7.8. Fie R un inel comutativ și unitar, inelul polinoamelor $R[X_1, X_2, \dots, X_n]$ și $u: R \rightarrow R[X_1, X_2, \dots, X_n]$ morfismul canonic. Atunci oricare ar fi inelul comutativ și unitar S , morfismul unitar de inele $v: R \rightarrow S$ și $x_1, x_2, \dots, x_n \in S$, există un unic morfism de inele $\varphi: R[X_1, X_2, \dots, X_n] \rightarrow S$ astfel încât $u(X_i) = x_i$, $1 \leq i \leq n$, și diagrama

$$\begin{array}{ccc} R & \xrightarrow{u} & R[X_1, X_2, \dots, X_n] \\ & \searrow v & \swarrow \varphi \\ & S & \end{array}$$

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

Demonstratie. Se demonstrează prin inducție după n .

Pentru $n=1$ rezultă din teorema 7.5. Presupunând afirmația adevarată pentru $n-1$, există o diagramă comutativă de forma

$$\begin{array}{ccc} R & \xrightarrow{u'} & R[X_1, X_2, \dots, X_{n-1}] \\ & \searrow v & \swarrow \varphi' \\ & S & \end{array}$$

unde u' este morfismul canonic, iar φ' este unicul morfism de inele, astfel încât $\varphi'(X_i) = x_i$, $1 \leq i \leq n-1$, și $\varphi' \circ u' = v$. Cum $R[X_1, X_2, \dots, X_n] = R[X_1, X_2, \dots, X_{n-1}][X_n]$ din teorema 7.5, avem diagrama comutativă

$$\begin{array}{ccc} R[X_1, X_2, \dots, X_{n-1}] & \xrightarrow{u''} & R[X_1, X_2, \dots, X_{n-1}][X_n] \\ & \searrow \varphi & \swarrow \varphi \\ & S & \end{array}$$

unde u'' este morfismul canonic, iar φ este unicul morfism de inele, astfel încât $\varphi(X_n) = x_n$ și $\varphi \circ u'' = \varphi'$. Deoarece $u = u'' \circ u'$ este morfismul canonic de la R la $R[X_1, X_2, \dots, X_n]$, avem că $\varphi \circ u = \varphi \circ (u'' \circ u') = = (\varphi \circ u'') \circ u' = \varphi' \circ u' = v$, adică diagrama

$$\begin{array}{ccc} R & \xrightarrow{u} & R[X_1, X_2, \dots, X_n] \\ & \searrow v & \swarrow \varphi \\ & S & \end{array}$$

este comutativă. Mai mult, pentru $1 \leq i \leq n-1$, $\varphi(X_i) = \varphi'(u(X_i)) = = \varphi'(X_i) = x_i$. Deci $\varphi(X_i) = x_i$ pentru orice $1 \leq i \leq n$. Avind în vedere că φ' este unic iar $\varphi' = \varphi \circ u''$ rezultă imediat unicitatea morfismului φ .

Dacă R și R' sunt inele comutative și unitare, iar $\psi: R \rightarrow R'$ este un morfism unitar de inele, atunci există un morfism unitar de inele $\tilde{\psi}: R[X_1, X_2, \dots, X_n] \rightarrow R'[X_1, X_2, \dots, X_n]$ definit în modul următor:

Dacă

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

atunci

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

Mai mult, fie R , R' domenii de integritate și inelele $R[X_1, X_2, \dots, X_n]$, $R'[X_1, X_2, \dots, X_n]$, care sunt de asemenea domenii de integritate. Dacă $R(X_1, X_2, \dots, X_n)$ respectiv $R'(X_1, X_2, \dots, X_n)$ sunt corpurile de fractii ale lui $R[X_1, X_2, \dots, X_n]$ și $R'[X_1, X_2, \dots, X_n]$, morfismul $\tilde{\psi}: R[X_1, X_2, \dots, X_n] \rightarrow R'[X_1, X_2, \dots, X_n]$ induce un morfism de corpuri

$$\bar{\psi}: R(X_1, X_2, \dots, X_n) \rightarrow R'(X_1, X_2, \dots, X_n) \text{ definit prin } \bar{\psi}\left(\frac{f}{g}\right) = \frac{\tilde{\psi}(f)}{\tilde{\psi}(g)}.$$

Fie acum S un inel, $R \subset S$ un subinel al său și $v: R \rightarrow S$ inclusiunea, astfel încât $v(a) = a$. Teorema precedentă aplicată în acest caz ne dă pentru oricare n elemente $x_1, x_2, \dots, x_n \in S$ un morfism de inele $\varphi: R[X_1, X_2, \dots, X_n] \rightarrow S$, astfel încât

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

$$= \sum_{i_1, i_2, \dots, i_n=0}^{k_1, k_2, \dots, k_n} a_{i_1, i_2, \dots, i_n} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n} = f(x_1, x_2, \dots, x_n).$$

Spunem că și în cazul unei singure nedeterminate că $f(x_1, x_2, \dots, x_n)$ este valoarea polinomului f în (x_1, x_2, \dots, x_n) . Avem că

$$\text{Im } \varphi = \{f(x_1, x_2, \dots, x_n) \mid f(X_1, X_2, \dots, X_n) \in R[X_1, X_2, \dots, X_n]\}$$

este un subinel al lui S , pe care îl vom nota cu $R[x_1, x_2, \dots, x_n]$. Se spune că $R[x_1, x_2, \dots, x_n]$ este inelul obținut prin adjuncționarea la R a elementelor x_1, x_2, \dots, x_n din S .

§ 8. PROPRIETĂȚI ALE RĂDĂCINILOR UNUI POLINOM. DERIVATA UNUI POLINOM

În acest paragraf R va fi un domeniu de integritate. Atunci $R[X]$ va fi de asemenea un domeniu de integritate.

Fie f, g două polinoame din $R[X]$. Spunem că f divide g și scriem $f \mid g$ dacă există $h \in R[X]$ astfel încât $g=fh$. În caz contrar, spunem că f nu divide g și scriem $f \nmid g$.

Observăm că orice polinom divide polinomul nul, iar polinomul nul divide numai pe el însuși.

În §7 am definit noțiunea de rădăcină a unui polinom și anume, $x \in R$ este o rădăcină a polinomului f dacă $f(x)=0$.

Propoziția 8.1. (Teorema lui Bézout). Fie R domeniu de integritate și f un polinom din $R[X]$. Atunci $x \in R$ este o rădăcină a lui f dacă și numai dacă $X-x$ divide f .

Demonstrație. Fie $f \in R[X]$, $f=a_0+a_1X+\dots+a_nX^n$, $a_n \neq 0$, astfel încât $f(x)=0$. Atunci $f(X)=f(X)-0=f(X)-f(0)=a_0+a_1X+\dots+a_nX^n-(a_0+a_1x+\dots+a_nx^n)=a_1(X-x)+\dots+a_n(X^n-x^n)$.

Deoarece $X-x$ divide X^k-x^k pentru orice $1 \leq k \leq n$, rezultă că $X-x$ divide f . Reciproc, dacă $X-x$ divide f , atunci $f=(X-x)h$ cu $h \in R[X]$. Deci $f(x)=(x-x)h(x)=0$, adică x este o rădăcină a lui f .

Definiția 8.2. Spunem că elementul x din domeniul de integritate R este rădăcină multiplă de ordin i sau rădăcină de ordin de multiplicitate i a polinomului f din $R[X]$, dacă $(X-x)^i \mid f$ iar $(X-x)^{i+1} \nmid f$.

Este clar, după teorema lui Bézout, că x din R este rădăcină multiplă de ordin i a lui f dacă și numai dacă există un polinom g din $R[X]$ astfel încât

$$f=(X-x)^ig \text{ eu } g(x) \neq 0.$$

Propoziția 8.3. Fie R domeniu de integritate, iar f și g polinoame din $R[X]$. Dacă $x \in R$ este rădăcină multiplă de ordin i a lui f și respectiv rădăcină multiplă de ordin j a lui g , atunci x este rădăcină multiplă de ordin $i+j$ a produsului fg .

Demonstrație. Avem $f=(X-x)^i f_1$ cu $f_1(x) \neq 0$ și $g=(X-x)^j g_1$ cu $g_1(x) \neq 0$. Atunci $fg=(X-x)^{i+j} f_1 g_1$ și cum R este domeniu de integritate $f_1(x)g_1(x) \neq 0$. Deci x este rădăcină de ordin de multiplicitate $i+j$ a lui fg .

Propoziția 8.4. Fie R un domeniu de integritate și f un polinom nenul din $R[X]$. Dacă elementele x_1, x_2, \dots, x_k din R sunt rădăcini distincte ale lui f , de ordine de multiplicitate i_1, i_2, \dots, i_k , atunci f se scrie sub forma

$$f=(X-x_1)^{i_1}(X-x_2)^{i_2} \dots (X-x_k)^{i_k} g,$$

unde $g \in R[X]$.

Demonstrație. Procedăm prin inducție după k . Pentru $k=1$, propoziția rezultă din definiția 8.2. Presupunem că propoziția este adevărată pentru $k-1$ și să arătăm că ea este adevărată pentru k .

Există deci $f_1 \in R[X]$ astfel încit

$$f=(X-x_1)^{i_1}(X-x_2)^{i_2} \dots (X-x_{k-1})^{i_{k-1}} g_1.$$

Atunci $f(x_k)=(x_k-x_1)^{i_1}(x_k-x_2)^{i_2} \dots (x_k-x_{k-1})^{i_{k-1}} g_1(x_k)=0$ și cum $x_k \neq x_i$, pentru orice $1 \leq i \leq k-1$, rezultă $g_1(x_k)=0$.

Notind $h=(X-x_1)^{i_1}(X-x_2)^{i_2} \dots (X-x_{k-1})^{i_{k-1}}$ avem $f=hg_1$ cu $h(x_k) \neq 0$ și deoarece x_k este rădăcină a lui f de ordin de multiplicitate i_k este clar că x_k este rădăcină a lui g_1 de același ordin de multiplicitate. Într-adevăr, $g_1=(X-x_k)g_2$ și $f=(X-x_k)^{i_k} f_1$ cu $f_1(x_k) \neq 0$. Atunci $(X-x_k)^{i_k} f_1=(X-x_k)g_2 h$, de unde $(X-x_k)^{i_k-1} f_1=g_2 h$ și deci $0=g_2(x_k)h(x_k)$.

Cum $h(x_k) \neq 0$, atunci $g_2(x_k)=0$, adică $g_2=(X-x_k)g_3$. Avem deci $g_1=(X-x_k)^2 g_3$ și continuăm proceseul de atâtea ori cît este ordinul de multiplicitate al rădăcinii x_k a lui f .

Obținem deci $g_1=(X-x_k)^{i_k} g$ și deci

$$f=(X-x_1)^{i_1}(X-x_2)^{i_2} \dots (X-x_{k-1})^{i_{k-1}}(X-x_k)^{i_k} g.$$

Observație. Cind numărăm rădăcinile unui polinom și nu specificăm că sunt distincte, considerăm fiecare rădăcină de atâtea ori cît este ordinul său de multiplicitate.

Din cele de mai înainte rezultă

Corolarul 8.5. Dacă R este un domeniu de integritate și f un polinom din $R[X]$ cu grad $(f)=n > 0$, atunci f are cel mult n rădăcini.

Observație. Dacă R nu este domeniu de integritate, afirmația din corolarul precedent nu este neapărat adevărată.

Fie inelul $R=\mathbb{Z} \times \mathbb{Z}$ care nu este domeniu de integritate. De exemplu, $(0, 1)(1, 0)=(0, 0)$ și deci R are divizori ai lui zero. Să considerăm polinomul $f=(1, 0)X$ din $R[X]$ al cărui grad este 1. Orice element $(0, n)$ din R este rădăcină a lui f deoarece $f(0, n)=(1, 0)(0, n)=(0, 0)$ și deci f are o infinitate de rădăcini.

Propoziția 8.6. (Relațiile lui Viète). Fie R un domeniu de integrare și

$$f = a_0 + a_1 X + \dots + a_n X^n, \quad a_n \neq 0,$$

un polinom nenul din $R[X]$. Dacă x_1, x_2, \dots, x_n sunt rădăcinile lui f în R , atunci

$$f = a_n(X - x_1)(X - x_2) \dots (X - x_n),$$

și

$$-a_{n-1} = a_n(x_1 + x_2 + \dots + x_n),$$

$$a_{n-2} = a_n(x_1 x_2 + x_1 x_3 + \dots + x_1 x_n + \dots + x_{n-1} x_n),$$

$$\dots (-1)^k a_k = a_n(x_1 x_2 \dots x_k + x_1 x_2 \dots x_{k-1} x_{k+1} + \dots + x_{n-k+1} x_{n-k+2} \dots x_n),$$

$$\dots (-1)^n a_0 = a_n(x_1 x_2 \dots x_n).$$

Demonstrație. După propoziția 8.4 putem scrie $f = (X - x_1)(X - x_2) \dots (X - x_n)g$ cu $g \in R[X]$. Identificind coeficientul lui X^n din ambii membri, avem $g = a_n$. Deci

$$\begin{aligned} f &= a_n(X - x_1)(X - x_2) \dots (X - x_n) = a_n X^n - a_n(x_1 + x_2 + \dots + x_n) X^{n-1} + \\ &\quad + a_n(x_1 x_2 + x_1 x_3 + \dots + x_1 x_n + \dots + x_{n-1} x_n) X^{n-2} + \dots \\ &\quad \dots + (-1)^k a_n(x_1 x_2 \dots x_k + x_1 x_2 \dots x_{k-1} x_{k+1} + \dots + \\ &\quad + x_{n-k-1} x_{n-k+2} \dots x_n) X^{n-k} + \dots + (-1)^n a_n x_1 x_2 \dots x_n, \end{aligned}$$

de unde, prin identificarea coeficienților în cele două scrierile ale lui f se obțin relațiile cerute.

Relațiile din propoziția precedentă se numesc *relațiile dintre rădăcinile și coeficienții unui polinom sau relațiile lui Viète*.

Corolarul 8.7. (Teorema lui Wilson). Dacă $p \geq 2$ este un număr natural prim, atunci

$$(p-1)! + 1 \equiv 0 \pmod{n}.$$

Demonstrație. Fie corpul \mathbf{Z}_p al claselor de resturi modulo p și polinomul $f = X^{p-1} - 1$ din $\mathbf{Z}_p[X]$. Grupul $U(\mathbf{Z}_p)$ al elementelor inversabile din \mathbf{Z}_p are ordinul $p-1$. Rezultă că oricare ar fi $\hat{x} \neq \hat{0}$ din \mathbf{Z}_p avem $\hat{x}^{p-1} = \hat{1}$ și deci rădăcinile polinomului f sunt $\hat{1}, \hat{2}, \dots, \hat{p-1}$. Folosind propoziția precedentă, rezultă

$$\hat{1} \cdot \hat{2} \cdots \hat{p-1} = (-1)^{p-1}(-\hat{1}).$$

Cum p este prim, dacă $p \geq 3$, atunci p este impar și deci $(-1)^{p-1} = 1$, iar dacă $p=2$, atunci

$$(-1)^{2-1}(-\hat{1})=(-1)(-\hat{1})=\hat{1}=-\hat{1}.$$

Prin urmare, $\widehat{(p-1)!} = -\hat{1}$, adică $\widehat{(p-1)!+1} = \hat{0}$, de unde

$$(p-1)!+1 \equiv 0 \pmod{p}$$

Observație. Este adevărată și reciproca teoremei lui Wilson, mai precis, dacă $p \geq 2$ este un număr natural astfel încât

$$(p-1)!+1 \equiv 0 \pmod{p},$$

atunci p este număr prim.

Într-adevăr, fie q cu $0 < q < p$ un divizor natural al lui p . Deoarece $p \mid (p-1)!+1$, rezultă $q \mid (p-1)!+1$. Cum $q \mid (p-1)!$ avem $q \mid 1$ și deci $q=1$.

Ne propunem în continuare să dăm un criteriu important pentru studiul rădăcinilor multiple ale unui polinom cu coeficienți într-un corp comutativ.

Să considerăm K un corp comutativ și $K[X]$ inelul polinoamelor în nedeterminata X cu coeficienți în K . Fie funcția

$$d: K[X] \rightarrow K[X],$$

definită astfel:

Dacă $a \in K$, atunci $d(a)=0$, iar dacă $f = \sum_{i=0}^n a_i X^i$ este un polinom al cărui grad este ≥ 1 , atunci

$$d(f) = \sum_{i=0}^n i a_i X^{i-1}.$$

După definiția funcției d , avem $d(X^i) = iX^{i-1}$, pentru $i \geq 1$ și deci

$$\begin{aligned} d(X^{i+j}) &= (i+j)X^{i+j-1} = X^i(jX^{j-1}) + (iX^{i-1})X^j = \\ &= X^i d(X^j) + d(X^i)X^j. \end{aligned}$$

Această funcție o vom numi *derivare* iar dacă f este un polinom, $d(f)$ se numește *derivată* lui f și o vom nota prin $f'(1)$. Prin recurență definim $f^{(n)} = d^n(f) = d(d^{n-1}(f))$ pentru orice număr natural $n \geq 1$ și o vom numi *derivată de ordin n* a lui f . Pentru $n=0$, notăm

$$f^{(0)} = d^0(f) = f.$$

Tinând seamă de cele precedente, rezultă proprietățile următoare:

$$1^\circ \quad d(fg) = fd(g) + d(f)g.$$

$$2^{\circ} \quad d(f+g)=d(f)+d(g),$$

$$3^{\circ} \quad d(af)=ad(f),$$

oricare ar fi $f, g \in K[X]$ și $a \in K$.

Verificarea acestor proprietăți se face cu ușurință prin calcul.

Lema 8.8. Fie K un corp comutativ, f un polinom nenul de grad n din $K[X]$. Dacă $x \in K$, atunci f se poate scrie sub forma

$$f = \sum_{i=0}^n b_i (X-x)^i,$$

unde $b_i \in K$, oricare ar fi $i=0, 1, \dots, n$.

Mai mult, dacă car $K=0$, atunci această scriere este unică.

Demonstrație. Pentru a demonstra existența unei astfel de scrieri, procedăm prin inducție după $n=\text{grad } f$. Pentru $n=1$, fie $f=a_0+a_1X$, $a_1 \neq 0$. Avem $f=(a_0+a_1x)+a_1(X-x)$ și deci luăm $b_0=a_0+a_1x \in K$ și $b_1=a_1 \in K$. Să presupunem acum că afirmația este adeverată pentru polinoame de grad egal cu $n-1$ și să demonstrăm pentru polinomul f de grad n . Fie polinomul $h(X)=f(X)-f(x)$. Avem $h(x)=f(x)-f(x)=0$ și deci $X-x \mid h(X)$. Atunci există polinomul g astfel încât

$$h(X)=(X-x)g(X),$$

de unde

$$f(X)-f(x)=(X-x)g(X).$$

Deci

$$f=(X-x)g+b_0, \text{ unde } b_0=f(x) \in K.$$

Deoarece grad $g=n-1$, din ipoteza inductivă g se scrie sub forma

$$g = \sum_{j=0}^{n-1} c_j (X-x)^j,$$

și deci

$$f=(X-x) \sum_{j=0}^{n-1} c_j (X-x)^j + b_0 = b_0 + \sum_{j=0}^{n-1} c_j (X-x)^{j+1}.$$

Punând $j+1=i$ și $c_j=b_{i+1}$, obținem

$$f=b_0 + \sum_{i=1}^n b_i (X-x)^i = \sum_{i=0}^n b_i (X-x)^i.$$

Din formula care ne dă scrierea lui f obținem prin derivare, membru cu membru, că

$$f^{(k)}(x)=k! b_k, \text{ pentru } 1 \leq k \leq n.$$

În cazul în care $\text{car } K=0$, rezultă de aici că toți coeficienții b_k , $0 \leq k \leq n$, sunt unic determinați.

Teorema 8.9. Fie K un corp, f un polinom nenul din $K[X]$, $r \geq 1$ un număr natural și x un element din K . Atunci

1) Dacă $x \in K$ este o rădăcină multiplă de ordin r a lui f , rezultă $f(x)=f^{(1)}(x)=\dots=f^{(r-1)}(x)=0$.

2) Dacă $\text{car } K=0$ și $f(x)=f^{(1)}(x)=\dots=f^{(r-1)}(x)=0$, iar $f^{(r)}(x) \neq 0$, rezultă că x este rădăcină multiplă de ordin r a lui f .

Demonstrație. Dacă $\text{grad}(f)=n$, atunci după lema precedentă f se scrie sub forma

$$f = \sum_{i=0}^n b_i(X-x)^i.$$

1) Dacă x este rădăcină multiplă de ordin r , din formula precedentă, care dă expresia lui f , rezultă $b_0=0$ și prin derivarea acesteia membru cu membru obținem succesiv $b_1=0, \dots, b_{r-1}=0$. Deci $b_i=0$ oricare ar fi $i=0, 1, \dots, r-1$ și cum $f^{(i)}(x)=i!b_i$, pentru orice $1 \leq i \leq n$, rezultă $f^{(i)}(x)=0$, pentru orice $i=0, 1, \dots, r-1$.

2) Corpul K avind caracteristica zero și cum $f^{(i)}(x)=0$, pentru orice $0 \leq i \leq r-1$, după lema precedentă rezultă $b_i=0$, pentru orice $0 \leq i \leq r-1$. Deci $(X-x)^r$ divide f și deoarece $f^{(r)}(x) \neq 0$ avem că $(X-x)^{r+1}$ nu divide f . Prin urmare x este rădăcină multiplă de ordin r a lui f .

Observație. Afirmația 2) a teoremei precedente nu este neapărat adevărată pentru un corp de caracteristică $\neq 0$. Într-adevăr, fie corpul Z_p cu car $Z_p=p$ și polinomul $f=X^p$ din $Z_p[X]$. Avem că $\hat{0}$ este rădăcină a lui f de ordin de multiplicitate p , dar $f^{(i)}(\hat{0})=\hat{0}$ oricare ar fi $i>0$ număr natural.

§ 9. { 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 permuteare 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

$$f = \sum_{t_1, t_2, \dots, t_n=0}^{k_1, k_2, \dots, k_n} a_{t_1 t_2 \dots t_n} X_1^{t_1} X_2^{t_2} \dots X_n^{t_n},$$

atunci

$$\sigma^*(f) = \sum_{t_1, t_2, \dots, t_n=0}^{k_1, k_2, \dots, k_n} a_{t_1 t_2 \dots t_n} X_{\sigma(1)}^{t_1} X_{\sigma(2)}^{t_2} \dots X_{\sigma(n)}^{t_n}.$$

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

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

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 $(\sigma^{-1})^*$.

Definiția 9.1. 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 rămâne 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 $R[X_1, X_2, \dots, X_n]$.

Propoziția 9.2. *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 rindul 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 .

Lema 9.3. Fie f un polinom din $R[X_1, X_2, \dots, X_n]$ de grad m și f_i , $0 \leq i \leq m$, componentele 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 oricare. 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.

Propoziția 9.4. Polinoamele $s_1, s_2, s_3, \dots, s_n$ din $R[X_1, X_2, \dots, X_n]$, definite prin

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

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

$$s_3 = X_1 X_2 X_3 + X_1 X_2 X_4 + \dots + X_{n-2} X_{n-1} X_n = \sum_{1 \leq i < j < k \leq n} X_i X_j X_k,$$

$$\dots$$

$$s_n = X_1 X_2 \dots X_n.$$

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 $g(X) = X^n - s_1 X^{n-1} + s_2 X^{n-2} - \dots + (-1)^n s_n$.

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,

$$\sigma^{**}(g(X)) = \sigma^{**}(X^n - s_1 X^{n-1} + s_2 X^{n-2} - \dots + (-1)^n s_n) =$$

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

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 .

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

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

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

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

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:

$$M_1 = a X_1^{i_1} X_2^{i_2} \dots X_n^{i_n}, \quad a \neq 0 \quad \text{și} \quad M_2 = b X_1^{j_1} X_2^{j_2} \dots X_n^{j_n}, \quad b \neq 0.$$

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

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. Aceasta se numește termenul *principal* al polinomului.

Lema 9.5. 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 încit $M_1 > M_2$. Atunci :

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

2) Dacă $N_2 = X_1^{l_1} X_2^{l_2} \dots X_n^{l_n}$ este un alt monom astfel încit $N_1 > N_2$, 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 încit $i_1 = j_1, \dots, i_{s-1} = j_{s-1}, i_s > j_s$, 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 $M_1N_1 > M_1N_2 > M_2N_2$.

Propoziția 9.6. 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 $aX_1^{k_1}X_2^{k_2}\dots X_n^{k_n}$ respectiv $bX_1^{l_1}X_2^{l_2}\dots X_n^{l_n}$ termenii principali ai celor două polinoame, astfel încit $ab \neq 0$. Din lema precedentă rezultă că $abX_1^{k_1+l_1}X_2^{k_2+l_2}\dots X_n^{k_n+l_n}$ este termenul principal al produsului celor două polinoame.

Lema 9.7. 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

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

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

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 $X_1^{s_1}X_2^{s_2}\dots X_n^{s_n}$, pentru care $s_1 \geq s_2 \geq \dots \geq s_n$ și $X_1^{k_1}X_2^{k_2}\dots X_n^{k_n} > X_1^{s_1}X_2^{s_2}\dots X_n^{s_n}$. Într-adevăr, avem $r_1 \geq s_1$ și deci există doar un număr finit de numere s_1 , iar pentru fiecare s_1 dat există cel mult s_1^{n-1} sisteme (s_2, s_3, \dots, s_n) pentru care $s_1 \geq s_2 \geq \dots \geq s_n$.

Teorema 9.8. (Teorema fundamentală a polinoamelor simetrice). Fiecare polinom simetric f din $R[X_1, X_2, \dots, X_n]$ se poate exprima în mod unic ca 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 $f \in R[X_1, X_2, \dots, X_n]$ un polinom simetric de grad n . Conform lemei 9.3, f se scrie în mod unic ca sumă de polinoame omogene simetrice.

Putem presupune, fără a restringe generalitatea, că f este polinom simetric omogen. Fie $\text{grad}(f)=m$, 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 $X_1X_2\dots X_i$ și atunci, după propoziția 9.6, 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

$$f_1 = f - as_1^{k_1-k_2} s_2^{k_2-k_3} \dots s_{n-1}^{k_{n-1}-k_n} s_n^{k_n}$$

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

$$f_2 = f_1 - bs_1^{t_1-t_2} s_2^{t_2-t_3} \dots s_{n-1}^{t_{n-1}-t_n} s_n^{t_n}.$$

Termenul principal al lui f_2 este mai mic decât al lui f și putem continua procedeul. Înținând seama de observația precedentă, procedeul se va sfîrși după un număr finit de pași. Astfel se ajunge la o expresie a lui f în funcție de 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

$$h(s_1, s_2, \dots, s_n) = \sum a_{t_1 t_2 \dots t_n} s_1^{t_1} s_2^{t_2} \dots s_n^{t_n} = 0$$

și să arătăm că toți coeficienții $a_{t_1 t_2 \dots t_n}$ 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 $X_1^{k_1} X_2^{k_2} \dots$

$\dots X_n^{k_n}$, 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 diferiți. 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 distințe 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.

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

$$f = (X_1 - X_2)^2 (X_1 - X_3)^2 (X_2 - X_3)^2$$

cu coeficienți reali.

Termenul principal al polinomului f este $X_1^4 X_2^2$. Atunci exponentii termenilor principali ai polinoamelor care vor rămaîne după eliminarea succesivă a termenilor principali, ca-n procedeul descris în demonstrația teoremei 9.8, vor fi $(4, 2, 0)$, $(4, 1, 1)$, $(3, 3, 0)$, $(3, 2, 1)$ 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 din valori numerice nedeterminate 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	0
2	-1	-1	0	-3	2	0
1	-2	-2	-3	0	4	0
1	-1	-1	-1	-1	1	0

Obținem astfel sistemul de ecuații

$$0 = 4 + b, \quad 0 = -27b + 4d, \quad 0 = -108a + 16d, \quad 0 = 1 - a - b + c + d,$$

de unde $a = -4, b = -4, c = 18, d = -27$.

Prin urmare,

$$(X_1 - X_2)^2 (X_1 - X_3)^2 (X_2 - X_3)^2 = s_1^2 s_2^2 - 4s_1^3 s_3 - 4s_2^3 + 18s_1 s_2 s_3 - 27s_3^2.$$

Fie K un corp comutativ și $K[X_1, X_2, \dots, X_n]$ domeniul de integritate al polinoamelor de n nedeterminate. Să considerăm $K(X_1, X_2, \dots, X_n)$ corpul fracțiilor raționale și $\sigma \in S_n$. Morfismul pe care l-am definit mai înainte

$$\sigma^*: K[X_1, X_2, \dots, X_n] \rightarrow K[X_1, X_2, \dots, X_n]$$

are proprietatea că oricare ar fi $g \in K[X_1, X_2, \dots, X_n], g \neq 0$, $\sigma^*(g)$ este element inversabil în $K(X_1, X_2, \dots, X_n)$. Conform proprietății de universalitate a inelelor de fracții, există un morfism

$$\bar{\sigma}: K(X_1, X_2, \dots, X_n) \rightarrow K(X_1, X_2, \dots, X_n),$$

astfel încit $\bar{\sigma}(f) = \sigma^*(f)$ oricare ar fi polinomul f din $K[X_1, X_2, \dots, X_n]$. Avem că

$$\bar{\sigma}\left(\frac{f}{g}\right) = \frac{\sigma^*(f)}{\sigma^*(g)}.$$

Mai mult, $\bar{\sigma}$ este un izomorfism de coruri.

Definiția 9.9. O fracție rațională $\frac{f}{g}$ din $K(X_1, X_2, \dots, X_n)$ se numește simetrică, dacă, pentru orice $\sigma \in S_n$, avem că $\bar{\sigma}\left(\frac{f}{g}\right) = \frac{f}{g}$.

Mulțimea fracțiilor raționale simetrice este în mod clar un subcorp al corpului $K(X_1, X_2, \dots, X_n)$.

Propoziția 9.10. Dacă K este un corp comutativ, atunci pentru orice fracție rațională simetrică F din $K(X_1, X_2, \dots, X_n)$ există o fracție rațională F' din $K(X_1, X_2, \dots, X_n)$ unic determinată astfel încât $F = F'(s_1, s_2, \dots, s_n)$.

Demonstrație. Fie $F = \frac{f}{g}$, $g \neq 0$, o fracție rațională simetrică. Polinomul $\prod_{\sigma \in S_n} \sigma^*(g) = g \prod_{\sigma \in S_n} \sigma^*(g)$, $\sigma \neq e$, fiind permutarea identică, este nenul și, mai mult, este chiar simetric. Deci dacă F este o fracție rațională simetrică, există f, g polinoame simetrice astfel încât $F = \frac{f}{g}$. După teorema fundamentală a polinoamelor simetrice, există f', g' din $K[X_1, X_2, \dots, X_n]$ astfel încât $f = f'(s_1, s_2, \dots, s_n)$ și $g = g'(s_1, s_2, \dots, s_n)$ și deci $F = F'(s_1, s_2, \dots, s_n)$.

Pentru a demonstra unicitatea, fie $F \in K(X_1, X_2, \dots, X_n)$ cu $F''(s_1, s_2, \dots, s_n) = F$. Atunci, dacă $F'' = \frac{f''}{g''}$, $g'' \neq 0$, din relația

$$\frac{f''(s_1, s_2, \dots, s_n)}{g''(s_1, s_2, \dots, s_n)} = \frac{f'(s_1, s_2, \dots, s_n)}{g'(s_1, s_2, \dots, s_n)}$$

rezultă

$$f''(s_1, s_2, \dots, s_n)g'(s_1, s_2, \dots, s_n) - f'(s_1, s_2, \dots, s_n)g''(s_1, s_2, \dots, s_n) = 0.$$

Conform unicității din teorema fundamentală a polinoamelor simetrice, rezultă $f''g' - f'g'' = 0$, adică

$$F'' = \frac{f''}{g''} = \frac{f}{g} = F'.$$

§ 10. TEOREMA FUNDAMENTALĂ A ALGEBREI

Fie $K \subset L$ corpuri comutative astfel încât K să fie un subcorp al lui L . Spunem că L este o extindere a lui K .

De exemplu, corpul \mathbb{C} al numerelor complexe este o extindere a corpului \mathbb{R} al numerelor reale.

Propoziția 10.1. Fie K un corp comutativ și f un polinom 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 (propoziția 7.4). Atunci idealul (f) este diferit de $K[X]$ și conform lemei lui Krull (teorema 5.8) există un ideal maximal m al lui $K[X]$ care conține (f) . Fie

$$K \xrightarrow{i} K[X] \xrightarrow{p} K[X]/\mathfrak{m}$$

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 $g \in K[X]$. Idealul \mathfrak{m} fiind maximal, avem că inelul factor $K[X]/\mathfrak{m}$ este un corp pe care-l notăm cu F . Componerea $\varphi = poi$, $\varphi: K \rightarrow F$ este un morfism de coruri și deci injectiv. Fie $f = a_0 + a_1X + \dots + a_nX^n$ din $K[X]$ și 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

$$\begin{aligned} f^\varphi(a) &= \varphi(a_0) + \varphi(a_1)a + \dots + \varphi(a_n)a^n = \\ &= \varphi(a_0) + \varphi(a_1)\hat{X} + \dots + \varphi(a_n)\hat{X}^n = \hat{a} + \hat{a}_1\hat{X} + \dots + \hat{a}_n\hat{X}^n = \\ &= \overbrace{a_0 + a_1X + \dots + a_nX^n}^{\hat{f}} = \hat{f} = \hat{0}. \end{aligned}$$

Deci $f^\varphi(a) = \hat{0}$, 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 coruri, 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 coruri. 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

$$\begin{aligned} x \oplus y &= \theta^{-1}(\theta(x) + \theta(y)) = \theta^{-1}(\varphi(x) + \varphi(y)) = \theta^{-1}(\varphi(x+y)) = \\ &= \theta^{-1}(\theta(x+y)) = x+y \end{aligned}$$

și, analog, $x \odot y = xy$.

Astfel, operațiile algebrice ale corpului K sunt induse de cele de pe corpul L și 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 $f^{\theta}(a) = 0$ adică $\varphi(a_0) + \varphi(a_1)a + \dots + \varphi(a_n)a^n = 0$, rezultă $\theta^{-1}(\varphi(a_0) + \varphi(a_1)a + \dots + \varphi(a_n)a^n) = \theta^{-1}(0)$. Coeficienții polinomului f fiind din K , avem în continuare

$$\theta^{-1}(0(a_0)) + \theta^{-1}(\theta(a_1))\theta^{-1}(a) + \dots + \theta^{-1}(\theta(a_n))\theta^{-1}(a^n) = 0$$

sau $a_0 + a_1x + \dots + a_nx^n = 0$, adică $f(x) = 0$.

Corolarul 10.2. Fie K un corp comutativ și f 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 rădăcina în K . Presupunem că afirmația este adeverată 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 inducțive 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 .

Lema 10.3. 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 încit $g = h(s_1, s_2, \dots, s_n)$. 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

$$g(x_1, x_2, \dots, x_n) = h(s_1(x_1, x_2, \dots, x_n), s_2(x_1, x_2, \dots, x_n), \dots, \dots, s_n(x_1, x_2, \dots, x_n)) \text{ este un element din } K.$$

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

Teorema 10.4. Orice polinom de grad $n \geq 1$ cu coeficienți complecsi are cel puțin o rădăcină complexă.

Demonstrație. Mai întii, observăm că orice polinom f cu coeficienți reali de grad impar are cel puțin o rădăcină reală. Într-adevăr, funcția polinomială $\tilde{f}: \mathbb{R} \rightarrow \mathbb{R}$ asociată lui f este continuă și pentru

$a \in R$ suficient de mare avem $f(a) f(-a) < 0$. Atunci, după o proprietate fundamentală a funcțiilor continue, rezultă că există $x \in R$ astfel încit $f(x)=0$ 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 $R[X]$ cu grad $(f)=n>1$ și să considerăm k natural, astfel încit 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 10.2 există o extindere L a corpului 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

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

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 $\text{grad}(h_a) = \binom{n}{2}$. Deoarece $n = 2^k q$ și 2 nu divide q , rezultă $\binom{n}{2} = \frac{n(n-1)}{2} =$

$= 2^{k-1}q(2^kq-1)$ 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 10.3, 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 inductivă rezultă că h_a are cel puțin o rădăcină complexă. Există deci o pereche (i, j) cu $1 \leq i < j \leq n$, astfel încit z_{ij}^a să aparțină lui C . Făcind pe a să parcurgă multimea (infinită) R a numerelor reale și cum multimea perechilor (i, j) , $1 \leq i < j \leq n$, este finită, rezultă că există $a, b \in R$, $a \neq b$, astfel încit z_{ij}^a și z_{ij}^b să aparțină lui 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} este un polinom cu coeficienți reali. Într-adevăr, dacă $b_k = \sum_{i+j=k} a_i \bar{a}_j$, $0 \leq k \leq 2n$, este un coeficient oarecare al lui \tilde{f} , atunci evident $\tilde{b}_k = b_k$ și deci b_k este număr real. Prin urmare există numărul complex x , astfel încât $(\tilde{f})(x) = 0$. Deci $0 = (\tilde{f})(x) = f(x)\bar{f}(x)$, de unde $f(x) = 0$ sau $\bar{f}(x) = 0$. Dacă $f(x) = 0$, atunci x este o rădăcină complexă a lui f . Dacă $\bar{f}(x) = 0$ este clar că $f(\bar{x}) = 0$ și deci \bar{x} este o rădăcină complexă a lui f .

Definiția 10.4. Fie K un corp comutativ și f din $K[X]$ un polinom de grad ≥ 1 . Polinomul f se numește *ireducibil* dacă nu poate fi scris ca produsul a două polinoame din $K[X]$, ambele cu gradul strict mai mic decit gradul lui f .

Ca aplicații la teorema fundamentală a algebrei să descriem polinoamele ireductibile din $C[X]$ și $R[X]$.

1) Din teorema fundamentală a algebrei și teorema lui Bézout, rezultă că un polinom cu coeficienți complecsi este ireducibil în $C[X]$ dacă, și numai dacă, este de gradul întii.

2) Dacă f este un polinom cu coeficienți reali,

$$f = a_0 + a_1 X + \dots + a_n X^n, \quad a_n \neq 0$$

și x este o rădăcină complexă a sa, avem $f(x) = 0$.

Atunci

$$\begin{aligned} 0 &= \overline{f(x)} = \overline{a_0 + a_1 x + \dots + a_n x^n} = \bar{a}_0 + \bar{a}_1 \bar{x} + \dots + \bar{a}_n \bar{x}^n = \\ &= a_0 + a_1 \bar{x} + \dots + a_n \bar{x}^n, \end{aligned}$$

adică \bar{x} este de asemenea o rădăcină a polinomului f din $R[X]$. 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 $x = a - bi$ 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, avind discriminantul $4a^2 - 4(a^2 + b^2) = -4b^2 < 0$. De aici rezultă imediat că un polinom cu coeficienți reali este ireducibil în $R[X]$ dacă și numai dacă este de gradul întii sau de gradul al doilea cu discriminantul negativ.

EXERCITII

1. Fie R un inel. Pe mulțimea $S = \mathbb{Z} \times R$ definim operațiile

$$(m, a) + (n, b) = (m+n, a+b),$$

$$(m, a)(n, b) = (mn, mb+na+ab).$$

Să se arate că, în acest mod, S devine un inel unitar, iar R este izomorf cu un subinel al acestuia.

Indicație. Elementul unitate al lui S este $(1, 0)$. Funcția $f: R \rightarrow S$, $f(a) = (0, a)$ ne dă izomorfismul cerut.

2. Să se arate că mulțimea

$$F = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$$

împreună cu adunarea și înmulțirea numerelor reale este un corp comutativ.

Indicație. Rezultă imediat că F este un subinel al lui \mathbb{R} . Pentru a demonstra că orice element nenul din F este inversabil în F , se arată mai întâi că $a + b\sqrt[3]{2} + c\sqrt[3]{4} = 0$ dacă și numai dacă $a = b = c = 0$.

3. Să se arate că, într-un inel unitar, axioma de comutativitate a operației de adunare este o consecință a celorlalte axiome ale definiției inclusiv.

Indicație. Se folosește egalitatea

$$(1+1)(a+b) = (1+1)a + (1+1)b.$$

4. Fie R un inel unitar și $a, b \in R$. Să se arate că $1-ab$ este inversabil dacă și numai dacă $1-ba$ este inversabil.

Indicație. Dacă $u \in R$ este inversul lui $1-ab$, atunci inversul lui $1-ba$ este $1+buu$.

5. Fie R un inel unitar și $a, b \in R$ astfel încât $a, b, ab-1$ sint inversabile. Să se arate că elementele $a-b^{-1}$ și $(a-b^{-1})^{-1}-a^{-1}$ sint inversabile și, în plus, are loc egalitatea

$$((a-b^{-1})^{-1}-a^{-1})^{-1} = aba-a.$$

6. Să se arate că există o bijecție între mulțimea $I_b(R)$ a idealelor bilaterale ale unui inel unitar R și mulțimea $I_b(M_n(R))$ a idealelor bilaterale ale inelului $M_n(R)$.

Indicație. Definim $f: I_b(R) \rightarrow I_b(M_n(R))$ prin

$$f(I) = \{(a_{ij})_{1 \leq i, j \leq n} \mid a_{ij} \in I, \text{ oricare } i, j\}.$$

Avem că $f(I) \in I_b(M_n(R))$ și, evident, f este injectivă. Dacă acum $U \subseteq I_b(M_n(R))$ definim pentru orice (t, s) , $1 \leq t, s \leq n$,

$U_{t,s} = \{x \in R \mid \text{există } (a_{ij})_{1 \leq i,j \leq n} \text{ din } U \text{ astfel încit } x = a_{ts}\}.$

Se arată că $U_{t,s}$ sunt ideale bilaterale ale lui R care coincid între ele.
Dacă $I = U_{t,s}$, atunci $f(I) = U$ și deci f este surjectivă.

7. Dacă R este un inel, fie

$$Z(R) = \{x \in R \mid xa = ax, \text{ oricare ar fi } a \in R\}.$$

Să se arate că

i) $Z(R)$ este un subinel al lui R ;

ii) Dacă $a^2 - a \in Z(R)$, oricare ar fi $a \in R$, atunci R este comutativ.

Indicație. ii) Dacă $a, b \in R$, elementele $a^2 - a, b^2 - b, (a+b)^2 - (a+b) \in Z(R)$ și rezultă că $ab + ba \in Z(R)$. Apoi, se vede că $a^2 \in Z(R)$ și deci $a = a^2 - (a^2 - a) \in Z(R)$ pentru orice a .

8. Fie K un corp comutativ. Să se arate că grupurile $(K, +)$ și (K^*, \cdot) subiacente corpului K nu sunt izomorfe.

Indicație. Să presupunem prin absurd că $f: (K, +) \rightarrow (K^*, \cdot)$ este un izomorfism de grupuri. Atunci $f(0) = 1$ și există $x \in K, x \neq 0$ cu $f(x) = -1$. Rezultă, apoi, $f(-x) = -1$ și din injectivitatea lui f , $x = -x$, adică $2x = 0$, de unde $2 \cdot 1_K = 0$ și deci $2y = 0$, oricare $y \in K$. Rezultă apoi, imediat, că $f(1) = 1$ și din injectivitate avem $1 = 0$, contradicție.

9. Să se determine numărul structurilor de inel, neizomorfe, care pot fi definite pe o mulțime cu un număr prim de elemente.

Indicație. Există două astfel de structuri neizomorfe. Avem inelul nul în care produsul oricărui două elemente este nul și inelul \mathbf{Z}_p .

10. Să se arate că nu se poate defini nici o structură de inel unitar pe grupul aditiv $(\mathbb{Q}/\mathbb{Z}, +)$.

11. Să se descrie idealele inelului $K[[X]]$ al seriilor formale peste corpul comutativ K .

Indicație. Este clar că (0) și $(X^n), n \in \mathbb{N}$, sunt ideale ale lui $K[[X]]$. Se arată că acestea sunt singurele ideale ale sale. Dacă $I \neq (0)$ este un ideal, atunci fie $\text{ord}(I) = \min \{\text{ord}(f) \mid f \in I\}$. Se demonstrează că $I = (X^{\text{ord}(I)})$.

12. Să se descrie morfismele de inele de la \mathbf{Z} la \mathbf{Z}_n .

Indicație. Dacă $f: \mathbf{Z} \rightarrow \mathbf{Z}_n$ este un morfism de inele, atunci elementul $\hat{a} = f(1)$ are proprietatea $\hat{a}^2 = \hat{a}$ (adică este un element idempotent al lui \mathbf{Z}_n). Se obține o bijecție dată de $f \mapsto f(1)$ între morfismele de inele de la \mathbf{Z} la \mathbf{Z}_n și elementele idempotente din \mathbf{Z}_n .

13. Să se descrie morfismele de inele de la \mathbf{Z}_m la \mathbf{Z}_n .

Indicație. Se stabilește o bijecție între morfismele de inele de la \mathbf{Z}_m la \mathbf{Z}_n și elementele idempotente \hat{a} din \mathbf{Z}_n pentru care $m\hat{a} = \hat{0}$.

14. Să se determine automorfismele corpului \mathbf{R} al numerelor reale.

Indicație. Fie $f: \mathbb{R} \rightarrow \mathbb{R}$ un automorfism. Se arată mai întâi că $f(q) = q$, oricare ar fi $q \in \mathbb{Q}$. Apoi se arată că f este o funcție strict crescătoare. Fie $x \in R$ și să presupunem că $f(x) \neq x$, adică $f(x) < x$ sau $f(x) > x$. Dacă, de exemplu, $f(x) < x$, fie $q \in \mathbb{Q}$ astfel încât $f(x) < q < x$. Cum f este strict crescătoare obținem o contradicție. La fel, se procedează dacă $f(x) > x$. Deci oricare ar fi $x \in R$ avem $f(x) = x$ și prin urmare $f = 1_R$.

15. Fie K și K' două corpuri comutative și $f: K \rightarrow K'$ o funcție astfel încât $f(1) = 1$. Să se arate că f este morfism de corpuri dacă și numai dacă

$$\text{i)} f(x+y) = f(x) + f(y), \text{ oricare ar fi } x, y \in K;$$

$$\text{ii)} f(x^{-1}) = (f(x))^{-1}, \text{ oricare ar fi } x \in K, x \neq 0.$$

Indicație. Se folosește identitatea $(x+y)^2 = x^2 + xy + yx + y^2$ și exercițiul 4.

16. Să se arate că inelele de matrice $M_{mn}(R)$ și $M_m(M_n(R))$ sunt izomorfe.

17. Să se determine numărul structurilor de inel unitar care pot fi definite pe grupul aditiv $(\mathbb{Z}_n, +)$ și să se arate că oricare două astfel de inele sunt izomorfe.

Indicație. Dacă R este un astfel de inel, iar e este elementul unitate al său, se arată că $\text{ord}(e) = n$ și deci orice element din R se scrie sub forma ke , cu $0 \leq k < n$, iar $ne = \hat{0}$. Asocierea $\hat{k} \rightarrow ke$ dă un izomorfism de inele $\mathbb{Z}_n \simeq R$. Cum pentru fiecare alegere a lui e de ordin n există un astfel de izomorfism, rezultă că sunt $\varphi(n)$ structuri de inel unitar pe $(\mathbb{Z}_n, +)$.

18. Fie K mulțimea matricelor A de forma

$$\begin{pmatrix} a & b & c & d \\ -b & a-d & c & \\ -c & d & a-b & \\ -d & -c & b & a \end{pmatrix}$$

unde $a, b, c, d \in \mathbb{R}$. Să se arate că mulțimea K împreună cu operațiile de adunare și înmulțire obișnuite ale matricelor formează un corp necomutativ, izomorf cu corpul cuaternionilor.

Indicație. Se folosește faptul că $AA^t = (a^2 + b^2 + c^2 + d^2)I_4$, de unde $\det A = -(a^2 + b^2 + c^2 + d^2)^2$. Dacă $A \neq 0$, atunci $\det A \neq 0$ și matricea A este inversabilă. Izomorfismul cu corpul cuaternionilor este dat de asocierea $a+bi+cj+dk \rightarrow A$.

19. Fie R un inel comutativ și unitar. Un element $a \in R$ se numește *nilpotent* dacă există $n \in \mathbb{N}$ astfel încât $a^n = 0$. Să se arate că suma dintre un element inversabil și un element nilpotent este element inversabil în R .

Indicație. Dacă $x \in R$, $x^n=0$, avem

$(1-x)(1+x+x^2+\dots+x^{n-1})=1-x^n=1$. De aici rezultă imediat afirmația din enunț.

20. Fie R un inel comutativ și unitar, iar $N(R)$ mulțimea tuturor elementelor nilpotente ale sale. Să se arate că $N(R)$ este un ideal care coincide cu intersecția tuturor idealelor prime ale lui R . ($N(R)$) se numește *nilradicalul* lui R .

Indicație. Dacă $x, y \in N(R)$, atunci $x^m=0$, $y^n=0$ cu m, n , naturale. Atunci $(x+y)^{m+n-1}=0$ și deci $x+y \in N(R)$. Fie acum $N'(R)$ intersecția idealelor prime din R . Dacă $a \in R$ este nilpotent, este clar că $a \in N'(R)$. Reciproc, să presupunem că a nu este nilpotent și să notăm cu $\mathcal{J} = \{I \subset R \mid I \text{ ideal astfel încit } a^n \notin I, \text{ oricare ar fi } n\}$. Se arată că \mathcal{J} este o mulțime inductiv ordonată. Dacă p este un element maximal al său, acesta va fi un ideal prim al lui R , care nu conține a și deci $a \notin N'(R)$.

21. Dacă R este un inel comutativ și unitar, iar $J(R)$ este intersecția tuturor idealelor maximale ale sale, să se arate că $x \in J(R)$ dacă și numai dacă $1-xy$ este inversabil în R pentru orice $y \in R$. ($J(R)$ se numește *radicalul Jacobson* al lui R).

Indicație. Se folosește corolarul 5.8 din cap. III.

22. Fie R un inel comutativ și unitar și I_1, I_2, \dots, I_n ideale ale sale. Definim morfismul de inele $\varphi: R \rightarrow \prod_{k=1}^n R/I_k$, prin $\varphi(a) = (a+I_1, a+I_2, \dots, a+I_n)$. Să se arate că:

i) φ este surjectiv dacă și numai dacă $I_1+I_2=\dots+I_n=R$, pentru orice $k \neq l$.

ii) φ este injectiv dacă și numai dacă $\bigcap_{k=1}^n I_k=(0)$.

Indicație. i) Există $a \in R$ astfel încât $\varphi(a)=(1, 0, \dots, 0)$, adică $a \equiv 1 \pmod{I_1}$ și $a \equiv 0 \pmod{I_2}$. Deci $1=(1-a)+a \in I_1+I_2$, adică $I_1+I_2=R$. Invers, vom arăta, de exemplu, că există $a \in R$ încât $\varphi(a)=(-1, 0, \dots, 0)$. Avem $u_k+v_l=1$, $u_k \in I_k$ și $v_l \in I_l$, pentru orice $k \neq l$.

Atunci $a=\prod_{l=1}^n v_l$ are proprietatea cerută.

ii) Este clar deoarece $\text{Ker } \varphi = \bigcap_{k=1}^n I_k$.

23. Să se arate că orice subinel unitar al lui \mathbb{Q} este un inel de fracții al lui \mathbb{Z} în raport cu un anumit sistem multiplicativ al său.

Indicație. Dacă R este un subinel al lui \mathbb{Q} , fie $S = \{s \in \mathbb{Z} \setminus \{0\} \mid s^{-1} \in R\}$. Se arată că S este un sistem multiplicativ și $S^{-1}\mathbb{Z} = R$.

24. Fie R un inel comutativ și unitar, S un sistem multiplicativ, iar $i^S: R \rightarrow S^{-1}R$ morfismul canonic. Dacă $I \subset R$ este un ideal notăm cu $S^{-1}I$ idealul lui $S^{-1}R$ generat de $i^S(I)$. Să se arate că

$$\text{i) } S^{-1}I = \left\{ \frac{x}{s} \mid x \in I, s \in S \right\};$$

ii) Există o bijecție dată de $p \mapsto S^{-1}p$ între mulțimea idealelor prime ale lui R care nu se intersectează cu S și mulțimea idealelor prime ale lui $S^{-1}R$.

Indicație. ii) Dacă p' este ideal prim în $S^{-1}R$, atunci $(i^S)^{-1}(p')$ este ideal prim în R . Invers, dacă p este ideal prim în R , atunci R/p este domeniu de integritate. Notind prin \tilde{S} imaginea lui S în A/p , avem că $S^{-1}R/S^{-1}p \cong \tilde{S}^{-1}(R/p)$, ultimul inel fiind sau nul sau domeniu de integritate.

25. Fie R un inel comutativ și unitar. Să se arate că un polinom $f = \sum_{i=0}^n a_i X^i$ din $R[X]$ este inversabil în $R[X]$ dacă și numai dacă a_0 este inversabil în R și a_1, a_2, \dots, a_n sint elemente nilpotente.

Indicație. Pentru o implicație se aplică exercițiul 19. Reciproc, fie f inversabil și $g = b_0 + b_1X + \dots + b_nX^n$ încit $fg = 1$. Deducem $a_0b_0 = 1$, $a_nb_m = 0$, $a_nb_{m-1} + a_{n-1}b_m = 0$ etc. Deci a_0 este inversabil și raționind inducțiv, avem $a_n^{k+1}b_{m-k} = 0$ pentru orice $k = 0, 1, \dots, m$. Obținem $a_n^{m+1}b_0 = 0$ și deci a_n este nilpotent. Avem că $f_1 = f - a_nX^n$ este de asemenea inversabil și raționind ca mai înainte rezultă că a_{n-1} este nilpotent s.a.m.d.

26. Fie R un inel comutativ și $f \in R[X]$. Să se arate că f este divizor al lui zero în $R[X]$ dacă și numai dacă există $a \in R$, $a \neq 0$, astfel încit $af = 0$.

Indicație. Dacă $f = a_0 + a_1X + \dots + a_nX^n$ este divizor al lui zero în $R[X]$, fie $g = b_0 + b_1X + \dots + b_mX^m$ un polinom de grad minim încit $gf = 0$. Atunci $a_nb_m = 0$ și deoarece a_ng este un polinom de grad $< m$, astfel încit $(a_ng)f = 0$, rezultă că $a_ng = 0$. Succesiv se arată că $a_{n-k}g = 0$ pentru $0 \leq k \leq n$ și deci $a_ib_j = 0$ pentru orice i, j . Cum $g \neq 0$ există $b_k \neq 0$, și avem $b_kf = 0$.

27. Fie R un domeniu de integritate și $R[X]$ inelul polinoamelor într-o nedeterminată peste R . Să se arate că o funcție $\varphi: R[X] \rightarrow R[X]$ este un automorfism al lui $R[X]$ care invariază elementele din R dacă și numai dacă există $a, b \in R$, a inversabil, astfel încit $\varphi(f(X)) = f(aX + b)$, oricare ar fi $f(X) \in R[X]$.

Indicație. Dacă a este inversabil, să considerăm morfismul $\psi: R[X] \rightarrow R[X]$, dat prin $\psi(f(X)) = f(a^{-1}X - a^{-1}b)$. Morfismul ψ este inversul lui ϕ . Reciproc, fie $u: R[X] \rightarrow R[X]$ un automorfism cu $u(a) = a$, oricare ar fi $a \in R$ și v inversul. Dacă $u(X) = a_0 + a_1X + \dots + a_nX^n$ și $v(x) = b_0 + b_1X + \dots + b_mX^m$, din $(uv)(X) = X$ se obține $mn = 1$, de unde $m = n = 1$ §.a.m.d.

28. Fie d un număr întreg nenul liber de pătrate și mulțimile $Z[\sqrt{d}] = \{m + n\sqrt{d} \mid m, n \in Z\}$,

$$M(d) = \left\{ \begin{pmatrix} m & n \\ dn & m \end{pmatrix} \mid m, n \in Z \right\}.$$

Să se arate că $Z[\sqrt{d}]$ și $M(d)$ sunt subinele ale lui C și respectiv $M_2(Z)$ și, în plus, $Z[\sqrt{d}]$ și $M(d)$ sunt inele izomorse. Mai mult, să se arate că inelul factor $Z[X]/(X^2 - d)$ este izomorf cu fiecare dintre acestea.

Indicație. Izomorfismul $Z[\sqrt{d}] \rightarrow M(d)$ este dat de $m + n\sqrt{d} \rightarrow \begin{pmatrix} m & n \\ dn & m \end{pmatrix}$.

Fie acum $\phi: Z[X] \rightarrow Z[\sqrt{d}]$ morfismul de inele dat prin $\phi(X) = \sqrt{d}$. Avem că $\ker \phi = (X^2 - d)$ și se aplică teorema fundamentală de izomorfism.

29. Fie R un inel comutativ și unitar, $a \in R$ un nondivizor al lui zero și sistemul multiplicativ $S = \{a^n\}_{n \geq 0}$. Să se arate că inelele $S^{-1}R$ și $R[X]/(aX - 1)$ sunt izomorfe.

Indicație. Fie morfismul de inele $\phi: R[X] \rightarrow S^{-1}R$ dat prin $\phi(X) = a^{-1}$. Se arată că $\ker \phi = (aX - 1)$ și apoi se aplică teorema fundamentală de izomorfism.

30. Să se exprime ca polinom de polinoame simetrice fundamentale, polinomul simetric $f = (-X_1 + X_2 + X_3 + \dots + X_n)(X_1 - X_2 + X_3 + \dots + X_n) \dots (X_1 + X_2 + X_3 + \dots - X_n)$ cu coeficienți reali.

Indicație. Se procedează după algoritmul dat în demonstrația teoremei fundamentale a polinoamelor simetrice. Se obține

$$f = -s_1^n + 4s_1^{n-2}s_2 - 8s_1^{n-3}s_3 + \dots + (-2)^ns_n.$$

Capitolul IV

PROPRIETĂȚI ARITMETICE ALE INELELOR

§ 1. DIVIZIBILITATEA ÎN INELE

Pe parcursul întregului capitol, R va desemna un inel comutativ cu unitate și care este domeniu de integritate.

Vom nota cu $U(R)$ mulțimea elementelor inversabile din R ; $U(R)$ ca operația de înmulțire este un grup abelian numit grupul *unităților* lui R . Vom nota cu $R^* = R - \{0\}$.

Exemple. i) $U(\mathbb{Z}) = \{-1, 1\}$.

ii) Dacă K este un corp, atunci $U(K) = K^*$, și invers, dacă $U(K) = K^*$ atunci K este corp.

iii) Dacă R este domeniu de integritate, atunci $U(R[X]) = U(R)$. Intr-adevăr, dacă $f = a_0 + a_1X + \dots + a_nX^n$ este un element din $U(R[X])$, atunci există $g = b_0 + b_1X + \dots + b_mX^m$ un polinom astfel încât $fg = 1$. Evident că această egalitate implică în mod necesar $n = m = 0$ și $a_0b_0 = 1$, adică $f = a_0$ este un element inversabil în R .

Fie R un domeniu de integritate; spunem că un element $a \in R$ divide elementul $b \in R$ (sau că a este un divizor al lui b sau b este un multiplu al lui a) și scriem $a | b$ dacă există $c \in R$ astfel încât $b = ac$. Cind a nu este un divizor al lui b , notăm $a \nmid b$.

Notăm cu Ra sau cu (a) idealul principal generat de $a \in R$, adică $Ra = \{\lambda a \mid \lambda \in R\}$.

Vom da cele mai simple proprietăți ale relației de divizibilitate.

Propoziția 1.1. Relația de divizibilitate are următoarele proprietăți:

- 1) $a | b \Leftrightarrow Rb \subset Ra$.
- 2) $a | a$ oricare ar fi $a \in R$.
- 3) Dacă $a | b$ și $b | c$, atunci $a | c$.
- 4) Dacă $a | b_i$, $i = 1, \dots, n$, atunci $a | c_1b_1 + \dots + c_nb_n$ oricare ar fi $c_1, c_2, \dots, c_n \in R$.
- 5) $a | b$ și $b | a \Leftrightarrow \exists u \in U(R)$ astfel încât $b = ua$.

Demonstrație. 1) Presupunem că $a | b$, deci există $c \in R$ astfel încât $b = ac$. Dacă $x \in Rb$, atunci există $\lambda \in R$ astfel încât $x = \lambda b$. Cum $b = ac$, atunci $x = (\lambda c)a$ și deci $x \in Ra$, adică $Rb \subset Ra$.

Invers, presupunem că $Rb \subset Ra$. Cum $b \in Rb$, atunci $b \in Ra$ și deci există $c \in R$ astfel încât $b = ac$, adică $a | b$.

2) Relația $a | a$ rezultă din faptul că $a = 1 \cdot a$.

3) Dacă $a | b$ și $b | c$, atunci există elementele $\lambda, \mu \in R$ astfel încât $b = \lambda a$ și $c = \mu b$. Deci $c = \mu(\lambda a) = (\mu\lambda)a$ adică $a | c$.

4) Cum $a | b_i$ oricare ar fi $i = 1, \dots, n$, există $\lambda_i \in R$ astfel încât $b_i = \lambda_i a$, $i = 1, \dots, n$. Deci $c_1 b_1 + \dots + c_n b_n = c_1 \lambda_1 a + \dots + c_n \lambda_n a = (c_1 \lambda_1 + \dots + c_n \lambda_n)a$ și deci $a | c_1 b_1 + \dots + c_n b_n$.

5) Presupunem că $a | b$ și $b | a$. Înseamnă că există $u, v \in R$ astfel încât $b = ua$ și $a = bv$. Dacă $a = 0$ obținem $b = 0$ și putem lua $u = 1$. Dacă $b = 0$ obținem $a = 0$ și în mod similar putem lua $u = 1$. Dacă $a, b \neq 0$, atunci din relațiile de mai sus obținem $a = (uv)a$ și cum $a \neq 0$ rezultă $uv = 1$ adică $u \in U(R)$.

Invers, dacă $b = ua$, unde $u \in U(R)$, atunci $a | b$. Cum $a = u^{-1}b$, atunci avem și $b | a$.

Observație. Proprietățile 2) și 3) arată că relația de divizibilitate pe R este o relație binară *reflexivă* și *tranzitivă*. Relația de divizibilitate nu este reflexivă așa cum se vede din relațiile $2 | 4$ dar $4 \not| 2$ în inelul Z .

Relația de divizibilitate nu este nici antisimetrică așa cum se vede din exemplul: $2 | -2$ și $-2 | 2$ dar $2 \neq -2$.

Proprietatea 5) din propoziția 1.1 permite să definim o altă relație binară pe mulțimea R : dacă $a, b \in R$ spunem că a și b sunt *asociate* în divizibilitate și notăm $a \sim b$ dacă $a | b$ și $b | a$.

Propoziția 1.2. *Relația “ \sim ” are următoarele proprietăți:*

1) $a \sim b \Leftrightarrow Ra = Rb$

2) \sim este o relație de echivalență pe R .

3) $a \sim 1 \Leftrightarrow a \in U(R) \Leftrightarrow Ra = R$.

Demonstrație. 1) Rezultă din afirmația 1) din Propoziția 1.1.

2) Rezultă din 1) deoarece relația de egalitate pe mulțimea idealelor principale este o relație de echivalență.

3) Dacă $a \sim 1$, atunci $a | 1$ și deci există $b \in R$ astfel încât $1 = ab$ și deci $a \in U(R)$.

Invers, dacă $a \in U(R)$, atunci există $b \in R$ astfel încât $1 = ab$ și $a | 1$. Cum evident $1 | a$, atunci $a \sim 1$.

Echivalența $a \in U(R) \Leftrightarrow Ra = R$ este evidentă.

C.m.m.d.c. și c.m.m.m.c. A DOUĂ ELEMENTE

Definiția 1.3. Fie $a, b \in R$. Un element $d \in R$ se numește un cel mai mare divizor comun (prescurtat c.m.m.d.c.) al elementelor a și b dacă are următoarele proprietăți:

i) $d | a$ și $d | b$, adică d este un divizor comun al elementelor a și b .

ii) Dacă $d' | a$ și $d' | b$, atunci $d' | d$.

Este clar că dacă d_1, d_2 au proprietățile i) și ii), atunci $d_1 \nmid d_2$, și invers, dacă d are proprietățile i) și ii), atunci orice element asociat în diviziabilitate cu d are aceleași proprietăți.

În concluzie, orice două elemente d_1 și d_2 care sunt fiecare un cel mai mare divizor comun al elementelor a și b se găsesc în aceeași clasă de echivalență relativ la relația „ \sim ”.

Din aceste motive vom nota cu (a, b) sau c.m.m.d.c.(a, b) orice element care este un cel mai mare divizor comun, adică nu vom face nici o distincție între elementele asociate.

Două elemente a și b din R se numesc prime între ele dacă $(a, b) = 1$. Cu această convenție putem da proprietățile cele mai importante ale c.m.m.d.c. a două elemente:

Propoziția 1.4. Fie R un domeniu de integritate cu proprietatea că pentru orice două elemente există un c.m.m.d.c. Atunci următoarele afirmații sunt adevărate:

$$1) (a, b) = a \Leftrightarrow a \mid b.$$

$$2) (a, 0) = a.$$

3) Dacă $(a, b) = d$, unde $a \neq 0$ și $b \neq 0$, și scriem $a = da'$ și $b = db'$, atunci $(a', b') = 1$.

$$4) (ac, bc) = c(a, b).$$

$$5) (a, (b, c)) = ((a, b), c).$$

Demonstrație. 1) și 2) sunt evidente.

3) Fie $d' = (a', b')$. Cum $d' \mid a'$ și $d' \mid b'$, atunci evident $d'd \mid a$ și $d'd \mid b$ și deci $d'd \mid d$. Cum $d \neq 0$, atunci $d' \mid 1$, adică $d' \nmid 1$ ceea ce arată că $(a', b') = 1$.

4) Fie $d = (a, b)$ și $d' = (ac, bc)$. Evident putem presupune că $d \neq 0$ și $c \neq 0$. Cum $d = (a, b)$, atunci $a = da'$ și $b = db'$ și deci $ac = (dc)a'$ și $bc = (dc)b'$ ceea ce implică $dc \mid d'$, adică $d' = (dc)d''$. Deoarece $d' = (ac, bc)$ obținem că $ac = d'\lambda$ și $bc = d'\mu$ de unde rezultă că $ac = dc d''\lambda$ și $bc = dc d''\mu$ sau $dca' = dc d''\lambda$ și $dc b' = dc d''\mu$. Cum $dc \neq 0$, atunci $a' = d''\lambda$ și $b' = d''\mu$ ceea ce implică $d'' \mid a'$ și $d'' \mid b'$. Cum $(a', b') = 1$, atunci $d'' \mid 1$ adică d'' este inversabil și deci $d' \nmid dc$, ceea ce trebuie demonstrat. Afirmația 5) rezultă din definiția 1.3.

Proprietatea 5) din propoziția 1.4 ne permite să extindem noțiunea c.m.m.d.c. la un număr finit de elemente: dacă $a_1, a_2, \dots, a_n \in R$, atunci definim c.m.m.d.c. $(a_1, a_2, \dots, a_n) = \text{c.m.m.d.c.}(\dots, \text{c.m.m.d.c.}(a_1, a_2, \dots), a_n)$ pe care îl vom nota mai simplu (a_1, a_2, \dots, a_n) .

Alături de c.m.m.d.c. apare conceptul de cel mai mic multiplu comun (prescurtat c.m.m.m.c.)

Definiția 1.5. Fie $a, b \in R$. Un element $m \in R$ se numește un c.m.m.m.c. al elementelor a și b dacă are următoarele proprietăți:

i) $a \mid m$ și $b \mid m$, adică m este un multiplu comun al elementelor a și b .

ii) Dacă $a \mid m'$ și $b \mid m'$, atunci $m \mid m'$.

Din definiția 1.5 rezultă imediat că c.m.m.m.c. a două elemente (dacă există) este unic, abstracție făcind de o multiplicare cu un element inversabil. Din aceste motive vom nota cu $[a, b]$ sau c.m.m.m.c. (a, b) , orice element care este un cel mai mic multiplu comun.

Teorema 1.6. Fie R un domeniu de integritate. Următoarele afirmații sunt echivalente:

1) Pentru orice două elemente există un c.m.m.d.c.

2) Pentru orice două elemente există un c.m.m.m.c.

3) Intersecția oricărora două ideale principale este un ideal principal.

In plus, dacă este verificată una din condițiile echivalente de mai sus, atunci pentru orice $a, b \in R$ avem egalitatea

$$(a, b)[a, b] = ab.$$

Demonstrație. Să arătăm mai întâi $2 \Leftrightarrow 3$). Este ușor de văzut că dacă $m = [a, b]$, atunci $Rm \subset Ra$ și $Rm \subset Rb$ adică $Rm \subset Ra \cap Rb$. Dacă $m' \in Ra \cap Rb$, atunci $a \mid m'$ și $b \mid m'$ și deci $m \mid m'$ adică $m' \in Rm$ și deci avem și inclusiunea $Ra \cap Rb \subset Rm$ și deci $Rm = Ra \cap Rb$.

Invers, se arată ușor că dacă $Rm = Ra \cap Rb$, atunci $m = [a, b]$.

1) $\Rightarrow 2$). Fie $a, b \in R$; dacă $a=0$ sau $b=0$, atunci $[a, b]=0$. Deci presupunem că $a \neq 0$ și $b \neq 0$ și fie $d = (a, b)$. Înseamnă că $a = da'$ și $b = db'$, unde $(a', b') = 1$. Să notăm cu $m = \frac{d}{d} = a'b = ab'$ și să dovedim că

$m = [a, b]$. Se vede că $a \mid m$ și $b \mid m$. Fie acum $m' \in R$ astfel încât $a \mid m'$ și $b \mid m'$; deci există $\lambda, \mu \in R$ astfel încât $m' = a\lambda = b\mu$. Deci $da'\lambda = db'\mu$ și cum $d \neq 0$ rezultă că $a'\lambda = b'\mu$. Cum $(a', b') = 1$, atunci din propoziția 1.4 rezultă că $\lambda = (a'\lambda, b'\lambda) = (b'\mu, b'\lambda)$ și deci $b' \mid \lambda$ adică $\lambda = b'\lambda_1$. Deci $m' = a\lambda = ab'\lambda_1 = m\lambda_1$ adică $m \mid m'$.

2) $\Rightarrow 1$). Evident că putem presupune $a \neq 0$ și $b \neq 0$ și fie $m = [a, b]$. Atunci există $a', b' \in R$ astfel încât $m = aa' = bb'$. Deoarece $a \mid ab$ și $b \mid ab$, atunci $m \mid ab$ și deci există $d \in R$ astfel încât $ab = md$. Să dovedim că $d = (a, b)$. Deoarece $ab = aa'd = bb'd$, obținem prin simplificare că $b = a'd$ și $a = b'd$ și deci $d \mid a$ și $d \mid b$. Fie $d' \mid a$ și $d' \mid b$. Deci $a = d'a_1$ și $b = d'b_1$. Punem $m' = d'a_1b_1 = ab_1 = ba_1$. Deci $a \mid m'$ și $b \mid m'$ de unde rezultă că $m \mid m'$ adică $m' = mc$ și deci $d'm' = d'mc$. Cum $d'm' = d^2a_1b_1 = (d'a_1)(d'b_1) = ab$, obținem că $ab = d'mc$ sau $md = d'mc$ și prin simplificare rezultă că $d = d'c$ adică $d' \mid d$.

ELEMENTE PRIME ȘI ELEMENTE IRREDUCTIBILE ÎNTR-UN INEL

Definiție 1.7. Fie R un domeniu de integritate. Un element $p \in R$ se numește prim dacă

i) $p \neq 0$ și $p \notin U(R)$.

ii) $p \mid ab \Rightarrow p \mid a$ sau $p \mid b$.

Un element q din R se numește ireductibil dacă:

i) $q \neq 0$ și $q \notin U(R)$.

ii) Dacă $q = ab \Rightarrow a$ sau b este inversabil.

Este evident că un element asociat cu un element prim (resp. ireductibil) este prim (resp. ireductibil).

Următoarea teoremă caracterizează elementele prime și ireductibile într-un inel oarecare.

Teorema 1.8. Fie p și q două elemente nenule dintr-un domeniu de integritate R .

1) p este un element prim \Leftrightarrow idealul principal (p) este prim.

2) q este un element ireductibil \Leftrightarrow idealul (q) este maximal în mulțimea tuturor idealelor principale și proprii ale lui R .

3) Orice element prim este ireductibil.

4) Dacă inelul R are proprietatea că pentru orice două elemente există un c.m.m.d.c., atunci orice element ireductibil este prim.

Demonstrație. 1) Presupunem că p este element prim în R și fie $a, b \in R$ astfel încât $ab \in (p)$. Deci există $\lambda \in R$ cu $ab = p\lambda$, adică $p \mid ab$. Deci $p \mid a$ sau $p \mid b$, de unde rezultă că $a \in (p)$ sau $b \in (p)$ și prin urmare idealul (p) este prim.

Invers, presupunem că (p) este un ideal prim și presupunem că $p \nmid ab$. Atunci $ab \in (p)$ și deci $a \in (p)$ sau $b \in (p)$ adică $p \mid a$ sau $p \mid b$. Deci p este un element prim în R .

2) Presupunem că q este ireductibil și fie $a \in R$ astfel încât $(q) \subset (a) \neq R$. Atunci $a \nmid q$, și deci există $b \in R$ astfel încât $q = ab$. Cum a nu este inversabil, deoarece $(a) \neq R$, rezultă că b este inversabil și deci $q \mid a$, adică $(a) \subset (q)$ și deci $(a) = (q)$.

Pentru implicația inversă se parcurge raționamentul de mai sus în sens invers.

3) Fie $p = ab$, unde p este un element prim; atunci $p \mid ab$ și deci $p \mid a$ sau $p \mid b$. Dacă $p \mid a$, atunci $a = pa'$ și prin urmare $p = pa'b$ de unde rezultă că $a'b = 1$ adică b este inversabil. Analog se arată că dacă $p \mid b$ rezultă că a este inversabil. Deci p este ireductibil.

4) Presupunem că q este ireductibil și că $q \mid ab$. Fie $d = (q, a)$. Cum $d \mid q$ rezultă că d este inversabil sau d este asociat în divizibilitate cu q . În cazul că d este inversabil, atunci $1 = (q, a)$ și deci $b = -(qb, ab)$ și cum $q \mid ab$ rezultă că $q \mid b$. Dacă q este asociat în divizibilitate cu d , atunci $q \mid d$ și cum $d \mid a$ rezultă că $q \mid a$. În concluzie q este element prim în R .

Observație. Într-un domeniu de integritate oarecare noțiunile de element prim și element ireductibil sunt în general distincte, aşa cum rezultă din exemplul următor:

Considerăm multimea $R = \mathbb{Z}[i\sqrt{5}] = \{a+ib\sqrt{5} \mid a, b \in \mathbb{Z}\}$ care este un subinel al corpului C . Considerăm funcția $\varphi: \mathbb{Z}[i\sqrt{5}] \rightarrow \mathbb{N}$, $\varphi(a+ib\sqrt{5}) = a^2 + 5b^2$. Este ușor de văzut că dacă $z, z' \in \mathbb{Z}[i\sqrt{5}]$, atunci $\varphi(z \cdot z') = \varphi(z) \cdot \varphi(z')$. Rezultă ușor că $z \in U(\mathbb{Z}[i\sqrt{5}]) \Leftrightarrow \varphi(z) = 1 \Leftrightarrow z = \pm 1$.

Cum $\mathbb{Z} \subset \mathbb{Z}[i\sqrt{5}]$, avem în $\mathbb{Z}[i\sqrt{5}]$ descompunerea $6 = 2 \cdot 3 = (1+i\sqrt{5})(1-i\sqrt{5})$. Se verifică ușor, folosind funcția φ , că elementele $2, 3, 1+i\sqrt{5}$ și $1-i\sqrt{5}$ sunt ireductibile dar nu sunt prime în $\mathbb{Z}[i\sqrt{5}]$.

Intr-adevăr, să arătăm că 3 este ireductibil. Fie $3 = z_1 z_2$, unde $z_1 = a_1 + ib_1\sqrt{5}$ și $z_2 = a_2 + ib_2\sqrt{5}$. Din $\varphi(3) = \varphi(z_1 z_2) = \varphi(z_1) \cdot \varphi(z_2)$ obținem că $9 = (a_1^2 + 5b_1^2)(a_2^2 + 5b_2^2)$ și deci $a_1^2 + 5b_1^2 = 1, 3$ sau 9 . Egalitatea $a_1^2 + 5b_1^2 = 0$ implică $a_1 = \pm 1$ și $b_1 = 0$, adică z_1 este inversabil. Egalitatea $a_1^2 + 5b_1^2 = 3$ este imposibilă iar egalitatea $a_1^2 + 5b_1^2 = 9$ implica $\varphi(z_2) = 1$ adică z_2 este inversabil. Deci 3 este ireductibil în $\mathbb{Z}[i\sqrt{5}]$. Similar se arată că $2, 1+i\sqrt{5}, 1-i\sqrt{5}$ sunt ireductibile în $\mathbb{Z}[i\sqrt{5}]$.

Dacă 3 ar fi prim, atunci cum $3 \mid (1+i\sqrt{5})(1-i\sqrt{5})$ obținem că $3 \mid 1+i\sqrt{5}$ sau $3 \mid 1-i\sqrt{5}$ adică $1+i\sqrt{5} = 3(a+ib\sqrt{5})$ sau $1-i\sqrt{5} = -3(a-ib\sqrt{5})$ cu $a, b \in \mathbb{Z}$. Deci $3a = 1$, contradicție.

§ 2. INELE FACTORIALE

Propoziția 2.1. Fie R un domeniu de integritate. Dacă p_1, \dots, p_n sunt elemente prime iar q_1, \dots, q_m sunt elemente ireducibile astfel încât

$$p_1 \cdots p_n = q_1 \cdots q_m,$$

atunci $m=n$ și există o permutare $\sigma \in S_n$ astfel încât p_i și $q_{\sigma(i)}$ sunt asociate, oricare ar fi $i=1, \dots, n$.

Demonstrație. Vom proceda prin inducție după n .

Dacă $n=1$, din egalitatea $p_1 = q_1 \cdots q_m$ și din faptul că p_1 este ireductibil rezultă că $m=1$ și deci $p_1 = q_1$.

Presupunem că $n > 1$. Cum $p_1/q_1 \dots q_m$ și p_1 este prim, există q_k astfel încit p_1/q_k . Cum q_k este ireductibil, rezultă că q_k și p_1 sunt asociate. Renumerotând elementele q_1, \dots, q_m putem presupune că p_1 și q_1 sunt asociate. Deci $q_1 = p_1 u$, unde $u \in U(R)$. Înlocuind pe q_1 în egalitatea din enunț obținem $p_1 \cdots p_n = p_1 \cdot u q_2 \cdots q_m$. Simplificând cu p_1 obținem egalitatea $p_2 \cdots p_n = (u q_2) \cdots q_m$. Cum $u q_2$ este ireductibil, putem aplica ipoteza de inducție. Deci $n-1=m-1$, adică $m=n$ și abstracție făcând de o renumerotare a elementelor $u q_2, \dots, q_m$ avem că $p_2 \not\sim u q_2$, $p_i \not\sim q_i$ oricare ar fi $i > 2$. Cum u este inversabil, avem $p_2 \not\sim q_2$. Deci $p_i \not\sim q_i$ oricare ar fi $i \geq 1$.

Propoziția 2.2. Fie R un domeniu de integritate și $a, b \in R$. Dacă elementul ab este un produs de elemente prime, atunci alături de a și b este un produs de elemente prime (sau inversabile).

Demonstrație. Presupunem că $ab = p_1 \dots p_n$, unde p_1, \dots, p_n sunt elemente prime. Vom proceda prin inducție după n . Dacă $n=1$, atunci $ab = p_1$. Cum p_1 este ireductibil, atunci a este asociat în divizibilitate cu p_1 și b este inversabil sau b este asociat în divizibilitate cu p_1 și b este inversabil. În primul caz a este prim; în cel de-al doilea caz b este prim. Presupunem că $n > 1$. Cum $p_1 \mid ab$ rezultă că $p_1 \mid a$ sau $p_1 \mid b$. Să presupunem că $p_1 \mid a$; atunci $a = p_1 c$ și înlocuind obținem că $p_1 bc = p_1 \dots p_n$, sau, simplificind cu p_1 , rezultă că $bc = p_2 \dots p_n$. Aplicând ipoteza de inducție rezultă că b și c sunt produse de elemente prime (sau inversabile) și deci a este un produs de elemente prime.

Definiția 2.3. Un domeniu de integritate R se numește *factorial* dacă orice element nenul și neinversabil al lui R este produs de elemente prime ale lui R .

Deoarece relația de asociere este o relație de echivalență pe mulțimea R , putem vorbi de un sistem de reprezentanți de elemente prime pe care îl vom nota cu $P = (p_i)_{i \in I}$. Deci $(p_i)_{i \in I}$ sunt proprietăți:

i) Dacă $i, j \in I$, $i \neq j$, atunci elementele p_i și p_j nu sunt asociate în divizibilitate.

ii) Dacă p este un element prim al lui R , există un $i \in I$ astfel încât $p \sim p_i$ (p_i este unic).

De exemplu, în inelul \mathbb{Z} , un sistem de reprezentanți de elemente prime poate fi luat mulțimea $P = \{2, 3, 5, 7, 11, \dots\}$.

Un alt sistem de reprezentanți de elemente prime este și mulțimea $P' = \{-2, -3, -5, -7, -11, \dots\}$.

Dacă inelul R este factorial iar $(p_i)_{i \in I}$ este un sistem de reprezentanți de elemente prime, atunci este evident că orice $a \in R$, $a \neq 0$, se poate scrie sub forma

$$(1) \quad a = u \prod_{i \in I} p_i^{m_i},$$

unde $u \in U(R)$, $m_i \geq 0$, și numai un număr finit dintre numerele $(m_i)_{i \in I}$ sunt nenule. Mai mult, conform propoziției 2.1, scrierea lui a sub forma (1) este unică, în sensul că numerele m_i sunt unic determinate.

Propoziția 2.4. Fie R un inel factorial. Dacă $a, b \in R$ sunt două elemente nenule scrise sub forma (1), adică

$$a = u \prod_{i \in I} p_i^{m_i}, \quad b = v \prod_{i \in I} p_i^{n_i},$$

atunci elementul $d = \prod_{i \in I} p_i^{\min(m_i, n_i)}$ (resp. $m = \prod_{i \in I} p_i^{\max(m_i, n_i)}$) este c.m.m.d.c. (resp. c.m.m.m.c.) al elementelor a și b .

Demonstrație. Se vede imediat că $d \mid a$ și $d \mid b$. Fie $d' \in R$ astfel încât $d' \mid a$ și $d' \mid b$. Deoarece R este factorial, putem scrie $d' = w \prod_{i \in I} p_i^{s_i}$,

unde $w \in U(R)$, $s_i \geq 0$; și numai un număr finit dintre numerele $(s_i)_{i \in I}$ sunt nenule.

Utilizând propoziția 2.1, din faptul că $d' \mid a$ rezultă că $s_i \leq m_i$ oricare ar fi $i \in I$. Analog din $d' \mid b$ rezultă că $s_i \leq n_i$, $\forall i \in I$, și deci $s_i \leq \min(m_i, n_i)$, $\forall i \in I$, ceea ce implică $d' \mid d$.

Similar se demonstrează că m este un c.m.m.m.c. al elementelor a și b . În continuare vom da caracterizarea inelelor factoriale.

Teorema 2.5. Fie R un domeniu de integritate. Următoarele afirmații sunt echivalente:

1) R este factorial.

2) Orice element nenul și neinversabil al lui R se scrie în mod unic ca un produs de elemente ireductibile.

3) Orice element nenul și neinversabil este un produs de elemente ireductibile și orice element ireductibil este prim.

4) Orice element nenul și neinversabil este un produs de elemente ireductibile și pentru orice două elemente există un c.m.m.d.c. (sau un c.m.m.m.c.).

5) Orice ideal prim nenul al lui R conține un element prim.

6) a) Orice lanț ascendent de ideale principale este staționar, adică dacă $Ra_1 \subseteq Ra_2 \subseteq \dots \subseteq Ra_n \subseteq \dots$ este un lanț ascendent de ideale principale, există un n astfel încât $Ra_n = Ra_{n+1} = \dots$

b) Intersecția a două ideale principale este un ideal principal.

Demonstrație. 1) \Rightarrow 2). Rezultă din propoziția 2.1.

2) \Rightarrow 3). Trebuie să dovedim că dacă q este ireductibil, atunci q este prim. Presupunem că $q \mid ab$, adică $ab = qc$. Dar $a = q_1 \dots q_s$, $b = q'_1 \dots q'_r$, $c = q''_1 \dots q''_t$, unde $q_1, \dots, q_s, q'_1, \dots, q'_r, q''_1, \dots, q''_t$ sunt elemente ireductibile. Din egalitatea $q_1 \dots q_s q'_1 \dots q'_r = q''_1 \dots q''_t$ și din faptul că scrierea unui element ca produs de elemente ireductibile este unică, rezultă că există q_k sau q'_l astfel încât $q \nmid q_k$ sau $q \nmid q'_l$ și deci $q \mid a$ sau $q \mid b$. Deci q este prim.

3) \Rightarrow 1). Este evidentă.

1) \Rightarrow 4). Rezultă din propoziția 2.4 iar 4) \Rightarrow 3) rezultă din teorema 1.8.

1) \Rightarrow 5). Dacă p este un ideal prim nenul al lui R , există $a \in p$, $a \neq 0$. Cum a este neinversabil, atunci $a = p_1 \dots p_n$, unde p_1, \dots, p_n sunt elemente prime. Cum $p_1 \dots p_n \in p$ rezultă că există $1 \leq k \leq n$ astfel încât $p_k \in p$.

5) \Rightarrow 1). Notăm $S = \{a \in R \mid a \neq 0, a \notin U(R)\}$ și a este un produs de elemente prime}. Este clar că S este un sistem multiplicativ închis. Pentru a încheia demonstrația este suficient să arătăm că dacă $a \in R$, $a \neq 0$, și $a \notin S$, atunci $a \in S$. Prin reducere la absurd presupunem că $a \notin S$. Din propoziția 2.2 rezultă că $(a) \cap S = \emptyset$. Înseamnă că aplicând lema lui Zorn, există un ideal p maximal cu proprietatea $p \cap S =$

$\Rightarrow \emptyset$ și $(a) \subset p$. Să dovedim că p este ideal prim. Fie, pentru aceasta, $\lambda, \mu \in R$ astfel încât $\lambda\mu \in p$. Dacă $\lambda \in p$ și $\mu \notin p$, atunci $\lambda \in S$ și $\mu \in S$ (deoarece în cazul că $\lambda \notin S$ rezultă că avem $p \subseteq p + (\lambda)$ și deci $(p + (\lambda)) \cap S \neq \emptyset$). Rezultă că există $s_1 \in S$ de forma $s_1 = a_1 + \lambda\lambda'$ cu $a_1 \in p$. Similar, din faptul că $(p + (\mu)) \cap S \neq \emptyset$, există $s_2 \in S$ astfel încât $s_2 = a_2 + \mu\mu'$ cu $a_2 \in p$. Atunci $s_1s_2 = (a_1 + \lambda\lambda')(a_2 + \mu\mu')$ de unde rezultă că $s_1s_2 \in p$, contradicție.

Cum $\lambda, \mu \in S$, rezultă că λ și μ sunt produse de elemente prime și deci $\lambda\mu$ este un produs de elemente prime, adică $p \cap S \neq \emptyset$, contradicție.

1) \Rightarrow 6). Considerăm sirul ascendent de ideale

$$Ra_1 \subset Ra_2 \subset \dots \subset Ra_n \subset \dots$$

Atunci rezultă că $a_n | a_1$ oricare ar fi n . Cum inelul R este factorial, atunci a_1 este un produs finit de elemente. Deci a_1 are un număr finit de divizori și prin urmare există un n_0 astfel încât oricare ar fi $n \geq n_0$, a_n și a_{n+1} sunt asociate în divizibilitate și deci $Ra_n = Ra_{n+1}$, oricare ar fi $n \geq n_0$.

6) \Rightarrow 1). Înind cont de teorema 1.6, este suficient să dovedim că orice element din R nenul și neinversabil este un produs finit de elemente ireductibile. Prin reducere la absurd vom presupune că afirmația nu este adevărată și fie a un element de acest fel. Vom nota cu $X = \{a \in R \mid a \neq 0, a \notin U(R)\} \text{ și } a \text{ nu este un produs finit de elemente ireductibile}\}$. Deci $X \neq \emptyset$. Dacă $a \in X$, atunci în particular a nu este ireductibil; deci există $a_1, b_1 \in R$ astfel încât $a = a_1b_1$ și $a_1, b_1 \notin U(R)$. Evident că unul dintre elementele a_1, b_1 nu aparține mulțimii X . Să presupunem că $a_1 \notin X$. În particular, a_1 nu este ireductibil. Dacă există $a_2, b_2 \notin U(R)$ astfel încât $a_1 = a_2b_2$. Unul dintre elementele a_2, b_2 nu aparține mulțimii X ; deci putem presupune că $a_2 \notin X$. Continuând procedeul găsim sirurile de elemente: $(a_n)_{n \geq 1}$ și $(b_n)_{n \geq 1}$ astfel încât $a_n = a_{n+1}b_{n+1}$, unde $a_n, b_n \notin U(R)$ și $a = a_1b_1$. Deoarece $b_n \notin U(R)$, atunci sirul de ideale $Ra_1 \subset Ra_2 \subset Ra_3 \subset \dots$ este strict crescător, deci o contradicție.

§ 3. FACTORIALITATEA INELELOR DE FRACȚII

Fie R un domeniu de integritate și $S \subset R$ un sistem multiplicativ închis al lui R ; vom nota cu $S^{-1}R$ inelul de fracții asociat. Evident că $S^{-1}R$ este conținut în corpul de fracții al lui R .

Propoziția 3.1. Dacă R este un inel factorial, atunci $S^{-1}R$ este un inel factorial.

Demonstrație. Fie $p \in R$ un element prim astfel încât p nu divide nici un element al mulțimii S ; atunci p este un element prim și în inelul

$S^{-1}R$. Într-adevăr, p este nenul și neinversabil în $S^{-1}R$ deoarece p nu divide nici un element al lui S . Presupunem că $p \mid \frac{a}{s} \cdot \frac{b}{t}$ unde $a, b \in R$ și $s, t \in S$. Deci $\frac{a}{s} \cdot \frac{b}{t} = \frac{p}{s} \cdot \frac{c}{r}$, unde $r \in S$. Există $u, v \in S$ astfel încât $uab = pcv$. Cum p este prim, atunci $p \mid u$ sau $p \mid a$ sau $p \mid b$. Cum situația $p \mid u$ este imposibilă, atunci avem $p \mid a$ sau $p \mid b$ și deci $p \mid \frac{a}{s}$ sau $p \mid \frac{b}{s}$ în inelul $S^{-1}R$.

Fie acum $\alpha = \frac{a}{s}$ un element oarecare din inelul $S^{-1}R$. Cum R este

factorial, atunci $a = p_1 \dots p_n$, unde p_1, \dots, p_n sunt elemente prime. Fie dintre acestea p_{r+1}, \dots, p_n elementele prime care divid cel puțin un element din S . Rezultă că în inelul $S^{-1}R$ avem:

$$\alpha = \frac{a}{s} = \frac{p_1}{1} \dots \frac{p_r}{1} \frac{p_{r+1}}{1} \dots \frac{p_n}{1} s^{-1} = \frac{p_1}{1} \dots \frac{p_r}{1} u$$

unde am notat cu $u = \frac{p_{r+1} \dots p_n}{s}$ care este un element inversabil în $S^{-1}R$.

Deci α este în $S^{-1}R$ egal cu produsul a r elemente prime.

Fie R un domeniu de integritate oarecare și $(p_i)_{i \in I}$ o mulțime nevidă de elemente prime ale lui R . Vom nota cu S sistemul multiplicativ generat de această mulțime, adică un element din S este un produs finit din elementele $(p_i)_{i \in I}$ și un element inversabil al lui R . Următoarea teoremă constituie o reciprocă a propoziției 3.1.

Teorema 3.2. Fie R un domeniu de integritate cu proprietatea că orice lanț ascendent de ideale principale este staționar. Fie $(p_i)_{i \in I}$ o mulțime de elemente prime și S sistemul multiplicativ inchis generat de această mulțime. Dacă inelul $S^{-1}R$ este factorial, atunci R este factorial.

Demonstrație. Conform teoremei 2.5, este suficient să dovedim că orice ideal prim nenul \underline{p} al lui R conține un element prim. Dacă $\underline{p} \cap S \neq \emptyset$, atunci este evident că \underline{p} conține un element prim din mulțimea $(p_i)_{i \in I}$. Presupunem deci că $\underline{p} \cap S = \emptyset$. Vom nota $S^{-1}\underline{p} = \left\{ \frac{a}{s} \mid a \in \underline{p}, s \in S \right\}$

care este un ideal prim al inelului $S^{-1}R$. Cum $S^{-1}R$ este inel factorial, atunci $S^{-1}\underline{p}$ conține un element prim; fie acesta $\frac{q}{s}$, unde $q \in \underline{p}$. Cum s este inversabil, atunci $S^{-1}\underline{p}$ conține elementul $\frac{q}{1}$. Putem alege elementul q astfel încât să nu fie divizibil cu nici un element p_i .

Într-adevăr, dacă q este divizibil cu p_i , atunci $q = p_i q'$ și cum $p_i \notin p$, rezultă $q' \in p$ și în plus $\frac{q}{1} \in p$ și $\frac{q'}{1}$ sunt asociate în divizibilitate în inelul

$S^{-1}R$, deoarece p_i este inversabil în $S^{-1}R$. Deci putem înlocui pe $\frac{q}{1}$

cu $\frac{q'}{1}$. Continuind procedeul de dividere cu elemente p_j , deoarece inelul R satisfacă condiția lanțurilor ascendențe pentru ideale principale, după un număr finit de pași găsim un element $\frac{q_0}{1}$ cu $q_0 \in p$ astfel încât

$\frac{q}{1}$ și $\frac{q_0}{1}$ sunt asociate în divizibilitate și q_0 nu se mai divide cu nici un element $p_i (i \in I)$.

Să dovedim acum că q este un element prim. Fie $q \mid ab$ în R . Atunci $\frac{q}{1} \mid \frac{a}{1} \cdot \frac{b}{1}$ în $S^{-1}R$ și cum $\frac{q}{1}$ este element prim în $S^{-1}R$, obținem că $\frac{q}{1} \mid \frac{a}{1}$ sau $\frac{q}{1} \mid \frac{b}{1}$. Presupunem că $\frac{q}{1} \mid \frac{a}{1}$. Deci $\frac{a}{1} = \frac{q}{1} \cdot \frac{c}{s}$ și deci $a = qc$ în R , unde $s \in S$. Fie $s = p_{t_1} \dots p_{t_s}$; atunci avem $p_{t_1} \dots p_{t_s} a = qc$. Cum q nu se divide cu nici un p_i rezultă că $p_{t_1} \dots p_{t_s}$ divide pe c și deci $c = p_{t_1} \dots p_{t_s} c'$. Înlocuind și făcând simplificările obținem că $a = qc'$, adică $q \mid a$ și deci q este un element prim în R .

§ 4. INELE PRINCIPALE ȘI INELE EUCLIDIENE

Un inel se numește principal dacă este un domeniu de integritate și orice ideal al său este principal.

Teorema 4.1. *Dacă R este un inel principal, atunci R este factorial.*

Demonstrație. Conform teoremei 2.5, afirmația 6), este suficient să dovedim că orice lanț ascendent de ideale este staționar.

Fie pentru aceasta lanțul ascendent de ideale:

$$I_1 \subset I_2 \subset \dots \subset I_n \subset \dots$$

Vom nota $I = \bigcup_{n=1}^{\infty} I_n$. Este evident că I este un ideal. Cum inelul R este principal, atunci există $a \in R$ astfel încât $I = Ra$. Cum $a \in I$, atunci $a \in \bigcup_{n=1}^{\infty} I_n$ și deci există un $r \geq 1$ astfel încât $a \in I_r$. Deci $Ra \subset I_r$, adică $I \subset I_r$ și, în particular, $I_k \subset I_r$, oricare ar fi $k \geq 1$. În particular, dacă $k \geq r$, obținem $I_k \subset I_r \subset I_k$ și deci $I_r = I_k$. Deci $I_r = I_{r+1} = \dots$.

Teorema 4.2. Fie R un inel principal și $a, b \in R$. Dacă d este un c.m.m.d.c. al elementelor a și b , atunci există $\lambda, \mu \in R$ astfel încât

$$d = \lambda a + \mu b.$$

În particular, elementele a și b sunt prime între ele dacă și numai dacă există $\lambda, \mu \in R$ astfel încât $1 = \lambda a + \mu b$.

Demonstrație. Considerăm idealul $Ra + Rb$ care fiind principal, există $d \in R$ astfel încât $Ra + Rb = Rd$. Cum $d \in Rd$, atunci există $\lambda, \mu \in R$ astfel încât $d = \lambda a + \mu b$. Cum $Ra \subset Ra + Rb$, atunci $Ra \subset Rd$ și deci $d \mid a$. Analog avem și relația $d \mid b$.

Fie $d' \in R$ astfel încât $d' \mid a$ și $d' \mid b$; atunci $d' \mid \lambda a + \mu b$, adică $d' \mid d$. Deci d este un c.m.m.d.c.. Cum orice alt c.m.m.d.c. al elementelor a și b este asociat cu d , atunci rezultă imediat prima afirmație din teorema 4.2.

A doua afirmație rezultă imediat din prima folosind definiția elementelor prime între ele.

În continuare vom introduce noțiunea de inel euclidian.

Definiția 4.3. Se numește inel euclidian un domeniu de integritate R pentru care există o funcție $\varphi: R - \{0\} \rightarrow \mathbb{N}$ având proprietatea următoare: oricare ar fi $a, b \in R$, $b \neq 0$, există $q, r \in R$ astfel încât

$$(1) \quad a = bq + r, \text{ unde } r = 0 \text{ sau } \varphi(r) < \varphi(b)$$

Egalitatea din (1) se numește formula împărțirii cu rest în inelul euclidian R . Elementele q și r se numesc cîțul, respectiv restul împărțirii.

Legătura între inele eucliadiene și inele principale este dată de următoarea teoremă:

Teorema 4.4. Dacă R este un inel euclidian, atunci R este un inel principal. În particular orice inel euclidian este factorial.

Demonstrație. Fie I un ideal al lui R . Dacă $I = (0)$, atunci I este un ideal principal. Deci putem presupune că $I \neq (0)$. Vom nota cu $A = \{\varphi(a) \mid a \in I, a \neq 0\}$. Cum $A \neq \emptyset$ și $A \subset \mathbb{N}$, există un cel mai mic element al lui A ; fie acesta n_0 . Atunci există $a_0 \in I$ astfel încât $n_0 = \varphi(a_0)$. Vom dovedi că $I = Ra_0$. Cum $a_0 \in I$, este evidentă inclusiunea $Ra_0 \subset I$. Invers, fie $x \in I$. Cum $a_0 \neq 0$, atunci există $q, r \in R$ astfel încât $x = a_0q + r$, unde $r = 0$ sau $\varphi(r) < \varphi(a_0)$.

Dacă $r \neq 0$, atunci $r = x - a_0q \in I$ și deci $\varphi(r) \in A$. Cum $\varphi(r) < \varphi(a_0) = n_0$, obținem o contradicție. Deci trebuie ca $r = 0$ și deci $x = a_0q$, adică $x \in Ra_0$. Prin urmare are loc egalitatea $I = Ra_0$.

Observație. Reciproca teoremei 4.4 nu este adeverată. Există inele principale care nu sunt eucliadiene. De exemplu inelul $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right] = \left\{ a+b\left(\frac{1+i\sqrt{19}}{2}\right) \mid a, b \in \mathbb{Z} \right\}$ este un inel principal dar nu este euclidian.

În cazul cînd inelul R este euclidian se poate determină c.m.m.d.c a două elemente prin aplicarea de un număr finit de ori a formulei împărțirii cu rest. Mai exact, fie $a, b \in R$. Dacă $b=0$, atunci $(a, 0)=a$. Deci presupunem că $b \neq 0$. Aplicînd formula împărțirii cu rest avem egalitatea

$$(E_1) \quad a=bq_1+r_1 \text{ cu } r_1=0 \text{ sau } \varphi(r_1)<\varphi(b).$$

Dacă $r_1 \neq 0$, aplicăm din nou formula împărțirii cu rest și găsim elementele q_2, r_2 astfel încît

$$(E_2) \quad b=r_1q_2+r_2 \text{ cu } r_2=0 \text{ sau } \varphi(r_2)<\varphi(r_1).$$

Repetînd acest procedeu obținem elementele $q_3, q_4, \dots, q_n, \dots$ și $r_3, r_4, \dots, r_n, \dots$ din R astfel încît

$$(E_3) \quad r_1=r_2q_3+r_3 \text{ cu } r_3=0 \text{ sau } \varphi(r_3)<\varphi(r_2)$$

.....

$$(E_n) \quad r_{n-2}=r_{n-1}q_n+r_n \text{ cu } r_n=0 \text{ sau } \varphi(r_n)<\varphi(r_{n-1})$$

$$(E_{n+1}) \quad r_{n-1}=r_nq_{n+1}+r_{n+1} \text{ cu } r_{n+1}=0 \text{ sau } \varphi(r_{n+1})<\varphi(r_n).$$

Cum $\varphi(r_1)>\varphi(r_2)>\dots>\varphi(r_n)>\varphi(r_{n+1})>\dots$ și cum N este bine ordonată există un număr natural n astfel încît $r_n \neq 0$ și $r_{n+1}=0$.

Vom arăta că r_n este un c.m.m.d.c. al elementelor a și b . Cum $r_{n-1}=r_nq_{n+1}$, rezultă că $r_n|r_{n-1}$. Dar deoarece $r_{n-2}=r_{n-1}q_n+r_n$, rezultă că $r_n|r_{n-2}$. În continuare folosim egalitatea $r_{n-3}=r_{n-2}q_{n-1}+r_{n-1}$ și înînind cont că $r_n|r_{n-2}$ și $r_n|r_{n-1}$ rezultă că $r_n|r_{n-3}$. Din aproape în aproape, înînind cont de egalitățile (E_n) rezultă că r_n divide elementele $r_{n-1}, r_{n-2}, \dots, r_2, r_1$.

Din egalitatea (E_2) rezultă că $r_n|b$ iar din egalitatea (E_1) obținem că $r_n|a$. Deci r_n este un divizor comun al elementelor a și b . Fie d' un divizor comun al elementelor a și b . Din (E_1) obținem că $r_1=a-bq_1$ și deci $d'|r_1$. Din egalitatea (E_2) obținem $r_2=b-r_1q_2$. Cum $d'|r_1$ și $d'|b$, atunci $d'|r_2$.

Acum, folosind egalitățile $(E_3), \dots, (E_n), \dots$ obținem că d' divide elementele $r_3, r_4, \dots, r_{n-1}, r_n$.

Așadar r_n (*ultimul rest nenul*) este un c.m.m.d.c. al elementelor a și b .

Sirul de egalități $(E_1), (E_2), \dots, (E_n)$, poartă denumirea de algoritmul lui Euclid.

§ 5. EXEMPLE DE INELLE EUCLIDIENE

5.1 Inelul $(\mathbb{Z}, +, \cdot)$ este un inel euclidian.

Intr-adevăr, în acest inel are loc formula împărțirii cu rest: dacă $a, b \in \mathbb{Z}$ cu $b \neq 0$, există $q, r \in \mathbb{Z}$ unic determinate cu proprietatea

$$(1) \quad a=bq+r, \text{ unde } 0 \leq r < |b|.$$

Evident că dacă considerăm funcția

$$\varphi: \mathbf{Z} - \{0\} \rightarrow \mathbf{N}, \quad \varphi(n) = |n| = \begin{cases} n, & \text{dacă } n \geq 0 \\ -n, & \text{dacă } n < 0 \end{cases}$$

această funcție satisfacă proprietatea (1) din definiția 4.3.

Observație. Formula (1) se poate pune sub forma următoare: dacă $a, b \in \mathbf{Z}$ cu $b \neq 0$, există $q_0, r_0 \in \mathbf{Z}$ astfel încât

$$(2) \quad a = b q_0 + r_0, \quad \text{unde } |r_0| \leq \frac{b}{2}$$

În general numerele q_0 și r_0 nu sunt unic determinate.

5.2. Fie K un corp comutativ. Inelul de polinoame într-o singură variabilă $K[X]$ este un inel euclidian. Într-adevăr, fie $f, g \in K[X]$ cu $g \neq 0$. Vom dovedi că există două polinoame $q, r \in K[X]$ astfel încât

$$(3) \quad f = gq + r, \quad \text{unde } \text{grad } r < \text{grad } g$$

Într-adevăr, fie $f = a_0 + a_1 X + \dots + a_n X^n$ și $g = b_0 + b_1 X + \dots + b_m X^m$, unde $b_m \neq 0$ și $m \geq 0$. Vom demonstra că există formula (3) prin inducție după $\text{grad } f = n$.

Dacă $n < \text{grad } g$, atunci punem $q=0$ și $r=f$.

Dacă $n \geq \text{grad } g$ considerăm polinomul $f' = f - b_m^{-1} a_n X^{n-m} g$. Se observă imediat că $\text{grad } f' < n$ și conform ipotezei de inducție există polinoamele q', r' astfel încât

$$f' = gq' + r' \quad \text{unde } \text{grad } r' < \text{grad } g$$

sau $f = b_m^{-1} a_n X^{n-m} g = gq' + r'$ de unde $f = g(q' + b_m^{-1} a_n X^{n-m}) + r'$. Notând $q = q' + b_m^{-1} a_n X^{n-m}$ și $r = r'$ obținem $f = gq + r$, unde $\text{grad } r < \text{grad } g$. Formula (3) ne sugerează să considerăm funcția

$$\varphi: K[X] - \{0\} \rightarrow \mathbf{N}, \quad \varphi(f) = \text{grad } f$$

care se vede imediat că satisfacă proprietatea (1) din definiția 4.3.

5.3. Fie K un corp comutativ. Inelul de serii formale într-o singură variabilă $K[[X]]$ este un inel euclidian.

Într-adevăr, dacă $f = a_0 + a_1 X + \dots + a_n X^n + \dots$ este o serie formală, atunci f este un element inversabil în $K[[X]]$ dacă și numai dacă $a_0 \neq 0$. Rezultă că orice $f \in K[[X]]$, $f \neq 0$, este de forma $f = X^n u$, unde u este element inversabil în $K[[X]]$ iar n este unic determinat.

În particular, rezultă că dacă $f, g \in K[[X]]$, atunci avem $f \mid g$ sau $g \mid f$. Definim funcția $\varphi: K[[x]] - \{0\} \rightarrow \mathbf{N}$, $\varphi(f) = n$, unde $n \in \mathbf{N}$, cu proprietatea că $f = X^n u$, unde u este element inversabil din $K[[X]]$. Este evident că φ satisfacă proprietatea (1) din definiția 4.3.

5.4. Fie $a, b \in \mathbb{Z}$ și fie 0 o rădăcină a ecuației

$$(4) \quad x^2 + ax + b = 0$$

Vom nota $\mathbb{Z}[\theta] = \{m+n\theta \mid m, n \in \mathbb{Z}\}$. $\mathbb{Z}[\theta]$ are următoarele proprietăți:

i) $\mathbb{Z}[\theta]$ este subinel al lui \mathbb{C} și $\mathbb{Z} \subset \mathbb{Z}[\theta]$.

Într-adevăr, dacă $m \in \mathbb{Z}$, atunci putem scrie $m = m + 0 \cdot 0$ și deci $m \in \mathbb{Z}[\theta]$. Deci $\mathbb{Z} \subset \mathbb{Z}[\theta]$. Dacă $z_1, z_2 \in \mathbb{Z}[\theta]$, atunci există numerele întregi m_1, n_1 astfel încât $z_1 = m_1 + n_1\theta$ și există numerele întregi $m_2, n_2 \in \mathbb{Z}$ astfel încât $z_2 = m_2 + n_2\theta$. Dar cum $z_1 + z_2 = (m_1 + m_2) + (n_1 + n_2)\theta$ rezultă că $z_1 + z_2 \in \mathbb{Z}[\theta]$. Pe de altă parte, $z_1 z_2 = (m_1 + n_1\theta)(m_2 + n_2\theta) = m_1 m_2 + (m_1 n_2 + n_1 m_2)\theta + n_1 n_2\theta^2$. Dar cum $\theta^2 + a\theta + b = 0$, avem $\theta^2 = -a\theta - b$ și deci $z_1 z_2 = m_1 m_2 + (m_1 m_2 + n_1 n_2)\theta + n_1 n_2(-a\theta - b) = (m_1 m_2 - b n_1 n_2) + (m_1 n_2 + n_1 m_2 - a n_1 n_2)\theta$ ceea ce ne arată că $z_1 z_2 \in \mathbb{Z}[\theta]$.

În concluzie $\mathbb{Z}[\theta]$ este un subinel al lui \mathbb{C} .

Cazuri particulare. Dacă $a=0$, $b=1$, atunci ecuația (4) devine $x^2 + 1 = 0$ și $0 = i$ este rădăcină a acestei ecuații. În acest caz avem inelul $\mathbb{Z}[i] = \{m+ni \mid m, n \in \mathbb{Z}\}$. Inelul $\mathbb{Z}[i]$ se numește inelul întregilor lui Gauss.

Dacă $a=0$ și $b=-2$, atunci ecuația (4) devine $x^2 - 2 = 0$ și $\theta = \sqrt{2}$ este o rădăcină a acestei ecuații. În acest caz obținem inelul

$$\mathbb{Z}[\sqrt{2}] = \{m+n\sqrt{2} \mid m, n \in \mathbb{Z}\}.$$

ii) Dacă $0'$ este celalaltă rădăcină a ecuației (4), avem $\mathbb{Z}[\theta] = \mathbb{Z}[\theta']$. Într-adevăr, cum $\theta + \theta' = -a \in \mathbb{Z}$, rezultă că $\theta' = -a - \theta$ și deci din afirmația i) avem $\theta' \in \mathbb{Z}[\theta]$ și deci $\mathbb{Z}[\theta'] \subset \mathbb{Z}[\theta]$. În mod analog din $\theta = -a - \theta'$ obținem și inclusiunea $\mathbb{Z}[\theta] \subset \mathbb{Z}[\theta']$ și deci $\mathbb{Z}[\theta] = \mathbb{Z}[\theta']$.

iii) Notăm $d = a^2 - 4b$; deci $\theta = \frac{-a \pm \sqrt{a^2 - 4b}}{2}$. Dacă $d \geq 0$ și

d este un pătrat perfect, atunci $\theta \in \mathbb{Z}$.

Într-adevăr, dacă a este par, atunci $a^2 - 4b$ este număr întreg par și deci $\sqrt{a^2 - 4b}$ este par, ceea ce ne arată că $-a \pm \sqrt{a^2 - 4b}$ este număr par. Dacă a este impar, atunci $a^2 - 4b$ este impar și deci $\sqrt{a^2 - 4b}$ este impar ceea ce ne arată că $-a \pm \sqrt{a^2 - 4b}$ este par.

În concluzie $\theta \in \mathbb{Z}$ și deci $\mathbb{Z}[\theta] = \mathbb{Z}$.

iv) Vom studia în continuare cazul cind $d < 0$ sau $d > 0$ și d nu este pătrat perfect.

Să presupunem că

$$\theta = \frac{-a + \sqrt{a^2 - 4b}}{2} = \frac{-a + \sqrt{d}}{2}.$$

Atunci $\mathbf{Z}[\theta] = \{m+n\theta \mid m, n \in \mathbf{Z}\} = \{(m - \frac{a}{2}n) + \sqrt{d}\frac{n}{2} \mid m, n \in \mathbf{Z}\}$.

Dacă $z \in \mathbf{Z}[\theta]$, atunci z este de forma $z = (m - \frac{a}{2}n) + \sqrt{d}\frac{n}{2}$, unde $m, n \in \mathbf{Z}$. Se observă că avem $z=0$ dacă și numai dacă $m=n=0$.

Intr-adevăr, $z=0$ implică $(m - \frac{a}{2}n) + \sqrt{d}\frac{n}{2} = 0$. Cum \sqrt{d} este număr complex (cind $d < 0$) sau irațional (cind $d > 0$ și d nu este patrat perfect), atunci $m - \frac{a}{2}n = 0$ și $\frac{n}{2} = 0$ și deci $n=0$ și $m=0$. Notăm prin

$$z = (m - \frac{a}{2}n) + \sqrt{d}\frac{n}{2}.$$

Cum $z+z=2m-an \in \mathbf{Z}$, atunci $\bar{z} \in \mathbf{Z}[\theta]$. Numărul \bar{z} il vom numi conjugatul lui z în inelul $\mathbf{Z}[\theta]$. Se observă că dacă θ' este cealaltă rădăcină a ecuației (4), atunci dacă $z=m+n\theta$, avem $\bar{z}=m+n\theta'$.

Dacă $z_1, z_2 \in \mathbf{Z}[\theta]$, atunci au loc egalitățile:

$$(5) \quad \begin{aligned} \overline{z_1+z_2} &= \bar{z}_1 + \bar{z}_2, \\ \overline{z_1 z_2} &= \bar{z}_1 \cdot \bar{z}_2. \end{aligned}$$

Intr-adevăr, $z_1 = m_1 + n_1\theta$, $z_2 = m_2 + n_2\theta$, unde $m_1, n_1, m_2, n_2 \in \mathbf{Z}$. Deci $\bar{z}_1 = m_1 + n_1\theta'$ și $\bar{z}_2 = m_2 + n_2\theta'$. Vom verifica a doua egalitate din (5) deoarece prima este evidentă.

Avem

$$\text{și deci } z_1 z_2 = (m_1 m_2 - b n_1 n_2) + (m_1 n_2 + n_1 m_2 - a n_1 n_2) \theta$$

$$\bar{z}_1 \bar{z}_2 = (m_1 m_2 - b n_1 n_2) + (m_1 n_2 + n_1 m_2 - a n_1 n_2) \theta'.$$

Pe de altă parte, cum $\bar{z}_1 = m_1 + n_1\theta'$ și $\bar{z}_2 = m_2 + n_2\theta'$, avem

$$\bar{z}_1 \bar{z}_2 = (m_1 + n_1\theta')(m_2 + n_2\theta') = m_1 m_2 + (m_1 n_2 + n_1 m_2)\theta' + n_1 n_2 \theta'^2.$$

Cum $\theta'^2 + a\theta' + b = 0$, avem $\theta'^2 = -a\theta' - b$ și deci

$$\bar{z}_1 \bar{z}_2 = (m_1 m_2 - b n_1 n_2) + (m_1 n_2 + n_1 m_2 - a n_1 n_2) \theta'$$

și deci $\overline{z_1 z_2} = \bar{z}_1 \bar{z}_2$.

v) Definim funcția:

$$N: \mathbf{Z}[\theta] \rightarrow \mathbf{Z}$$

$$N(z) = z \cdot \bar{z}, \text{ unde } z \in \mathbf{Z}[\theta].$$

Dacă $z = m + n\theta = (m - \frac{a}{2}n) + \sqrt{d}\frac{n}{2}$, atunci

$$N(z) = [(m - \frac{a}{2}n) + \sqrt{d}\frac{n}{2}] \left[(m - \frac{a}{2}n) - \sqrt{d}\frac{n}{2} \right] = m^2 - amn + bn^2.$$

Numărul întreg $N(z)$ îl vom numi norma lui z .

Funcția N are următoarele proprietăți:

a) N este multiplicativă, adică

$$N(z_1 z_2) = N(z_1)N(z_2), \text{ oricare ar fi } z_1, z_2 \in \mathbb{Z}[\theta].$$

Intr-adevăr, $N(z_1 z_2) = z_1 z_2 \overline{z_1 z_2} = z_1 z_2 \bar{z}_1 \bar{z}_2 = (z_1 \bar{z}_1)(z_2 \bar{z}_2) = N(z_1)N(z_2).$

b) Dacă $z \in [0]$, atunci $N(z) = 0 \Leftrightarrow z = 0$.

Este clar că dacă $z = 0$, atunci $N(z) = 0$.

Invers, dacă presupunem $N(z) = 0$ și $z = m + n\theta$, cum $N(z) = m^2 - amn + bn^2$, obținem $m^2 - amn + bn^2 = 0$. Dacă $n \neq 0$, atunci avem $\left(\frac{m}{n}\right)^2 - a\left(\frac{m}{n}\right) + b = 0$ și deci

$$\frac{m}{n} = \frac{a \pm \sqrt{a^2 - 4b}}{2} = \frac{a \pm \sqrt{d}}{2}.$$

Cum $\frac{m}{n} \in \mathbb{Q}$, rezultă că $\sqrt{d} \in \mathbb{Q}$, contradicție. Deci $n = 0$ și atunci avem $m^2 = 0$, adică și $m = 0$, de unde $z = 0$.

c) $z \in U(\mathbb{Z}[\theta])$ (adică z este inversabil în inelul $\mathbb{Z}[\theta]$) $\Leftrightarrow N(z) = \pm 1$. Într-adevăr, dacă $z \in U(\mathbb{Z}[\theta])$, există $z' \in U(\mathbb{Z}[\theta])$ astfel încât $zz' = 1$. Cum N este multiplicativă, avem $N(zz') = N(1) = 1$ sau $N(z)N(z') = 1$. Cum $N(z) \in \mathbb{Z}$, atunci $N(z) = \pm 1$.

Invers, dacă $N(z) = \pm 1$, atunci $N(z) = z \cdot \bar{z} = \pm 1$. Dacă $z \cdot \bar{z} = 1$, atunci inversul lui z este \bar{z} .

vi) Definim funcția $\varphi: \mathbb{Z}[\theta] \rightarrow \mathbb{N}$, $\varphi(z) = |N(z)| = |m^2 - amn + bn^2|$. Din proprietățile a) b), c) ale funcției N obținem că φ are proprietățile:

a') φ este multiplicativă: $\varphi(zz') = \varphi(z) \cdot \varphi(z')$.

b') $\varphi(z) = 0 \Leftrightarrow z = 0$.

c') $z \in \mathbb{Z}[\theta]$ este inversabil $\Leftrightarrow \varphi(z) = 1$.

De exemplu în cazul inelului întregilor lui Gauss $\mathbb{Z}[i]$, funcția φ este următoarea:

$$\varphi: \mathbb{Z}[i] \rightarrow \mathbb{N}, \varphi(m+ni) = m^2 + n^2.$$

În continuare vom studia posibilitățile inelului $Z[\theta]$ de a fi euclidian relativ la funcția φ .

Fie $z, z' \in Z[\theta]$ cu $z' \neq 0$. Avem $\frac{z}{z'} = \frac{z\bar{z}'}{z'\bar{z}'} = \frac{z_1}{N(z_1)}$, unde am notat $z_1 = z\bar{z}'$.

Cum $z_1 \in Z[\theta]$, atunci $z_1 = m + n\theta$, unde $m, n \in Z$. Cum $z' \neq 0$, atunci din proprietatea b) avem $N(z') \neq 0$.

Apliind formula împărțirii cu rest sub forma care este dată în egalitatea (3), obținem: există $q_1, r_1 \in Z$ astfel încit:

$$(6) \quad m = N(z')q_1 + r_1 \text{ cu } |r_1| \leq \frac{1}{2} |N(z')|$$

există $q_2, r_2 \in Z$ astfel încit

$$(7) \quad n = N(z')q_2 + r_2 \text{ cu } |r_2| \leq \frac{1}{2} |N(z')|$$

$$\text{Atunci } \frac{z}{z'} = \frac{m+n}{N(z')} = \frac{N(z')q_1 + r_1 + N(z')q_2\theta + r_2\theta}{N(z')} = (q_1 + q_2\theta) + \frac{r_1 + r_2\theta}{N(z')}.$$

Notăm $Q = q_1 + q_2\theta$ și $R = \frac{z'(r_1 + r_2\theta)}{N(z')}$. Atunci este clar că

$$(8) \quad Q \in Z[\theta] \text{ și } z = z'\theta + R$$

Cum $z, z' \in Z[\theta]$ și cum $R = z - z'\theta$, obținem că și $R \in Z[\theta]$. Pe de altă parte, cum $RN(z') = z'(r_1 + r_2\theta)$, aplicind funcția φ , obținem

$$\varphi(R)\varphi(N(z')) = \varphi(z')\varphi(r_1 + r_2\theta)$$

sau

$$\varphi(R)N(z')^2 = |N(z')| \varphi(r_1 + r_2\theta)$$

de unde prin simplificare cu $|N(z')|$ obținem

$$\varphi(R) = \frac{(r_1 + r_2\theta)}{\varphi(z')}.$$

Dar cum

$$\varphi(r_1 + r_2\theta) = |r_1^2 - ar_1r_2 + br_2^2| \leq |r_1^2| + |a| \cdot |r_1| |r_2| + |b| |r_2|^2,$$

folosind inegalitățile din (6) și (7), obținem că

$$\begin{aligned} \varphi(r_1 + r_2\theta) &\leq \frac{1}{4}\varphi(z')^2 + \left|\frac{a}{4}\right| \varphi(z')^2 + \frac{|b|}{4} \varphi(z')^2 = \\ &= \varphi(z')^2 \left(\frac{1}{4} + \frac{|a|}{4} + \frac{|b|}{4} \right). \end{aligned}$$

Dec

$$(9) \quad \varphi(R) \leq \varphi(z') \left(\frac{1}{4} + \frac{|a|}{4} + \frac{|b|}{4} \right)$$

Dacă $|a| + |b| < 3$, atunci din (9) deducem că

$$(10) \quad \varphi(R) < \varphi(z')$$

Să vedem cînd este verificată egalitatea

$$(11) \quad |a| + |b| < 3.$$

Dacă $a=0$, atunci din (11) rezultă $|b|=1$ sau $|b|=2$. Adică $b=-\pm 1$ sau $b=\pm 2$. Pentru $a=0$ și $b=1$ ecuația (4) devine $x^2+1=0$ și deci $\theta=i$. În acest caz obținem inelul întregilor lui Gauss $Z[i]$. Pentru $a=0$ și $b=-1$ ecuația (4) devine $x^2-1=0$ și deci $\theta=1$. În acest caz obținem inelul $Z[\theta]=Z$.

Pentru $a=0$ și $b=2$ ecuația (4) devine $x^2+2=0$ și deci $\theta=i\sqrt{2}$.

În acest caz obținem inelul $Z[i\sqrt{2}] = \{m+n\sqrt{2} \mid m, n \in Z\}$. Pentru $a=0$ și $b=-2$ ecuația (4) devine $x^2-2=0$ și deci $\theta=2$. În acest caz obținem inelul $Z[\sqrt{2}] = \{m+n\sqrt{2} \mid m, n \in Z\}$. Dacă $|a|=1$, atunci din (11) rezultă că $|b|=0$ sau $|b|=1$. În cazul $|a|=1$ și $|b|=0$, ecuația (4) devine $x^2+x=0$, adică $\theta=0$ sau $\theta=1$. În acest caz obținem $Z[\theta]=Z$.

În cazul $|a|=1$ și $|b|=1$, ecuația (4) ia una din următoarele forme:

$$x^2+x+1=0; \quad x^2-x+1=0; \quad x^2+x-1=0 \quad \text{și} \quad x^2-x-1=0.$$

În cazul $x^2-x+1=0$ obținem $\theta = \frac{1+i\sqrt{3}}{2}$ și deci avem inelul

$$Z\left[\frac{1+i\sqrt{3}}{2}\right] = \left\{ \frac{m+i\sqrt{3}}{2} \mid m, n \in Z \right\}.$$

În cazul $x^2+x+1=0$ obținem același inel.)

În cazul cînd $x^2-x-1=0$ obținem $\theta = \frac{1+\sqrt{5}}{2}$ și deci avem inelul

$$Z\left[\frac{1+\sqrt{5}}{2}\right] = \left\{ m + \frac{1+\sqrt{5}}{2}n \mid m, n \in Z \right\}.$$

În cazul cînd $x^2+x-1=0$ obținem același inel.)

În concluzie, ținând cont de cele de mai sus și de relațiile (9) și (10) avem următorul rezultat:

Teorema 5.5. Inelele următoare:

$\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{2}]$, $\mathbb{Z}[i\sqrt{2}]$, $\mathbb{Z}\left[\frac{1+i\sqrt{3}}{2}\right]$, $\mathbb{Z}\left[\frac{1+\sqrt{5}}{2}\right]$ sunt inele euclidiene.

În continuare vom da o demonstrație geometrică a faptului că inelul întregilor lui Gauss $\mathbb{Z}[i]$ este inel euclidian relativ la funcția $\varphi: \mathbb{Z}[i] \rightarrow \mathbb{N}$, $\varphi(m+ni)=m^2+n^2$ ($\varphi(m+ni)$ este pătratul modulului numărului complex $m+ni$).

Folosim reprezentarea geometrică a numerelor complexe în plan. Numărului complex $z=a+ib$, $a, b \in \mathbb{R}$ î se asociază în plan punctul M de coordonate (a, b) .

Numerele complexe din mulțimea $\mathbb{Z}[i]$ sunt reprezentate în plan prin puncte ale căror coordonate sunt numere întregi. În felul acesta obținem o rețea în plan (fig. 1).

Fie $z, z' \in \mathbb{Z}[i]$ cu $z' \neq 0$. Fie M punctul din plan asociat numărului complex $\frac{z}{z'}$. Există un pătrat $ABCD$ din rețea în care se găsește punctul M . Presupunem că A este virful cel mai apropiat de M . Dacă $A(a, b)$, atunci $a, b \in \mathbb{Z}$ și A este asociat numărului complex $q=a+ib$.

Pe de altă parte, cum latura pătratului $ABCD$ este unitate și cum A a fost ales cel mai apropiat de M , obținem că distanța MA este mai mică decât jumătate din diagonala pătratului $ABCD$. Deci

$$|MA| \leq \sqrt{\frac{2}{2}} < 1.$$

Dar $|MA|$ este egal cu modulul numărului complex $\frac{z}{z'} - q$. Deci avem

$$(12) \quad \left| \frac{z}{z'} - q \right| < 1$$

Notăm cu $r = z - q \cdot z'$. Avem atunci din (12) că $|z - qz'| < |z'|$ sau $|r| < |z'|$ sau $|r|^2 < |z'|^2$ și deci $\varphi(r) < \varphi(z')$.

În concluzie avem

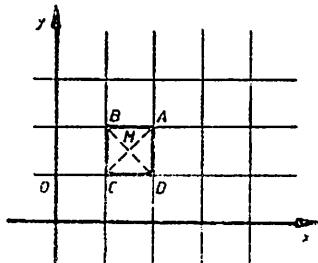


Fig. 1

(13)

$$z = qz' + r \text{ cu } \phi(r) < \phi(z')$$

ceea ce arată și pe această cale că $\mathbb{Z}[\mathrm{i}]$ este euclidian.

Din această demonstrație rezultă imediat că restul și cîtul împărțirii în (13) nu sunt unic determinate.

Intr-adevăr, dacă M este în centrul pătratului $ABCD$, atunci putem alege cîtul q al împărțirii în egalitatea (13) numărul complex $q = a + bi$ cu $a, b \in \mathbb{Z}$ pentru care (a, b) să fie coordonatele oricărui din vîrfurile pătratului $ABCD$.

Exemplu. Să considerăm în $\mathbb{Z}[\mathrm{i}]$ numerele $z = 6\mathrm{i}$ și $z' = 2 + 2\mathrm{i}$.

A vom $\frac{z}{z'} = \frac{6\mathrm{i}}{2+2\mathrm{i}} = \frac{3}{2} + \frac{3}{2}\mathrm{i}$. În figura 2 punctul M , care este reprezentarea geometrică a numărului complex $\frac{z}{z'} = \frac{3}{2} + \frac{3}{2}\mathrm{i}$, cade în centrul pătratului $ABCD$. Deci putem alege cîturile:

$$q_1 = 1 + \mathrm{i} \text{ sau } q_2 = 2 + \mathrm{i}, \text{ sau } q_3 = 2 + 2\mathrm{i} \text{ sau } q_4 = 1 + 2\mathrm{i}.$$

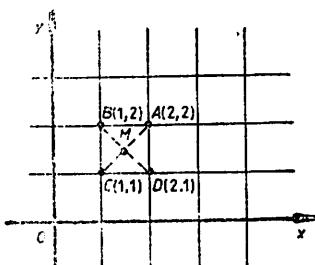


Fig. 2

A vom egalăriile:

$$z = z'q_1 + r_1 \text{ unde } r_1 = 2\mathrm{i}$$

$$z = z'q_2 + r_2, \text{ unde } r_2 = -2$$

$$z = z'q_3 + r_3, \text{ unde } r_3 = -2\mathrm{i}$$

$$z = z'q_4 + r_4, \text{ unde } r_4 = 2.$$

Se observă ușor că în toate cele patru cazuri avem

$$\phi(r_i) < \phi(z') \quad (1 \leq i \leq 4).$$

§ 6. FACTORIALITATEA INELELOR DE POLINOAME

În acest paragraf vom proba următoarea teoremă:

Teorema 6.1. Fie R un inel factorial. Atunci inelul de polinoame $R[X]$ este factorial.

Pentru demonstrația acestei teoreme avem nevoie de o serie de rezultate preliminare.

Lema 1. Fie $a \in R$ și $f = a_0 + a_1X + \dots + a_nX^n \in R[X]$. Dacă a divide f , atunci $a | a_i$ oricare ar fi $i = 0, 1, \dots, n$.

Demonstrație. Cum $a | f$, există $g = b_0 + b_1X + \dots + b_mX^m$ astfel încît $f = a \cdot g = ab_0 + ab_1X + \dots + ab_mX^m$. Evident că dacă $f = 0$, atunci

$a_i=0$ și deci $a \mid a_i$, oricare ar fi i . Putem presupune că $f \neq 0$ și în acest caz avem $m=n$ și $a_i=ab_i$, adică $a \mid a_i$.

Lema 2. Fie R un domeniu de integritate. Dacă $p \in R$ este un element prim în R , atunci p este element prim în $R[X]$.

Demonstrație. Fie $f, g \in R[X]$ astfel încât $p \mid fg$.

Presupunem că $f=a_0+a_1X+\dots+a_nX^n$ și $g=b_0+b_1X+\dots+b_mX^m$ și că $p \nmid f$ și $p \nmid g$. Conform lemei 1, din $p \nmid f$ rezultă că există un a_k astfel încât $p \nmid a_k$. Alegem pe k cel mai mic număr cu această proprietate. Deci $p \nmid a_0, \dots, p \nmid a_{k-1}$ și $p \nmid a_k$. Analog, din $p \nmid g$, există un l astfel încât $p \nmid b_0, \dots, p \nmid b_{l-1}$ dar $p \nmid b_l$.

Coefficientul lui X^{k+l} din produsul fg este elementul

$$c_{k+l} = \sum_{i+j=k+l} a_i b_j = a_0 b_{k+l} + a_1 b_{k+l-1} + \dots + a_{k-1} b_{l+1} + a_k b_l + a_{k+1} b_{l-1} + \dots + a_{k+l} b_0.$$

Deoarece $p \mid a_i b_j$ cu $i \neq k$ și $j \neq l$ și $p \nmid a_k b_l$, rezultă că $p \nmid c_{k+l}$ și deci $p \nmid fg$, contradicție. Deci trebuie ca $p \mid f$ sau $p \mid g$. Presupunem acum că inelul R este factorial și fie $f=a_0+a_1X+\dots+a_nX^n$ un polinom din $R[X]$. Vom nota cu $c(f)$ c.m.m.d.c. al elementelor a_0, a_1, \dots, a_n .

$c(f)$ se numește *cofactorul* polinomului f .

Dacă $c(f)=1$, atunci polinomul f se numește *primativ*.

Se observă că putem scrie $f=c(f)f'$, unde f' este un polinom primativ.

Lema 3. (Gauss). Dacă R este un inel factorial și $f, g \in R[X]$, atunci $c(fg)=c(f)c(g)$.

Demonstrație. Cum $f=c(f)f'$ și $g=c(g)g'$, unde f' și g' sunt polinoame primitive, obținem $fg=c(f)c(g)f'g'$ și deci $c(fg)=c(f)c(g)c(f'g')$. Deci trebuie probat că $c(f'g')=1$. Presupunem că $c(f'g') \neq 1$. Deci există $p \in R$ element prim astfel încât $p \mid c(f'g')$. Deci $p \mid f'g'$ și conform lemei 2 rezultă că $p \mid f'$ sau $p \mid g'$; conform lemei 1 rezultă că $p \mid c(f')$ sau $p \mid c(g')$, contradicție deoarece polinoamele f' și g' sunt primitive.

Lema 4. Fie R un inel factorial și $f, g \in R[X]$, unde g este un polinom primativ. Dacă $a \in R$, $a \neq 0$ și $g \mid af$, atunci $g \mid f$.

Demonstrație. Avem $af=gh$, unde $h \in R[X]$. Din lema 3 obținem $ac(f)=c(g)c(h)=c(h)$. Cum $h=c(h)h'$, atunci obținem $af=gac(f)h'$ și simplificând cu a , avem $f=c(f)gh'$ și deci $g \mid f$.

Vom nota cu K corpul de fracții al domeniului de integritate R .

Lema 5. Fie R un inel factorial cu corpul de fracții K și fie $f, g \in R[X]$ două polinoame primitive. Atunci f și g sunt asociate în $R[X]$ dacă și numai dacă sunt asociate în inelul $K[X]$.

Demonstrație. Evident că dacă f și g sunt asociate în $R[X]$, sunt asociate și în inelul $K[X]$.

Invers, presupunem că f și g sunt asociate în $K[X]$. Deci există $u \in K[X]$ element inversabil astfel încât $g = fu$. Cum $u \in K$, atunci putem scrie $u = \frac{a}{b}$ cu $a, b \in R$ și $a \neq 0, b \neq 0$. Deci $bg = af$. Aplicind lema 4, obținem că $f \mid g$ și $g \mid f$, adică f și g sunt asociate în divizibilitate în inelul $R[X]$.

Lema 6. Fie R un inel factorial și K corpul său de fracții. Fie $f \in R[X]$ un polinom primativ cu grad $f \geq 1$. Atunci f este ireductibil în $R[X] \Leftrightarrow f$ este ireductibil în $K[X]$.

Demonstrație. Presupunem că f este ireductibil în $R[X]$ și fie $f = gh$, unde $g \in K[X]$, $h \in K[X]$ și grad $g \geq 1$, grad $h \geq 1$. Evident că putem scrie $g = \frac{a}{b} g_1$, unde $a, b \in R$, $(a, b) = 1$ și $g_1 \in R[X]$. Analog,

$h = \frac{c}{d} h_1$, unde $c, d \in R$ cu $(c, d) = 1$ și $h_1 \in R[X]$. În plus grad $g = \text{grad } g_1$,

și grad $h = \text{grad } h_1$. Deci $f = \frac{ac}{bd} g_1 h_1$. Cum $g_1 = c(g_1)g_1'$ și $h_1 = c(h_1)h_1'$, unde g_1 și h_1 sunt polinoame primitive, obținem că $f = ug_1'h_1'$, unde u este un element inversabil din K . Deci f și $g_1'h_1'$ sunt asociate în $K[X]$. Conform lemei 5 rezultă că f și $g_1'h_1'$ sunt asociate în $R[X]$, adică $f = vg_1'h_1'$, unde $v \in U(R)$. Cum grad $g_1' \geq 1$ și grad $h_1' \geq 1$, rezultă că f nu este ireductibil în $R[X]$, contradicție. Invers, presupunem că f este ireductibil în $K[X]$ și presupunem că $f = gh$ cu $g, h \in R[X]$. Cum f este ireductibil în $K[X]$ rezultă că g este inversabil sau h este inversabil în $K[X]$. Dacă g este inversabil în $K[X]$, rezultă că $g \in K$, adică $g = a \in R$. Prin urmare $f = ah$. Cum f este primativ, rezultă că a este inversabil în R . Deci f este ireductibil în $R[X]$.

Demonstrația teoremei 6.1. Fie $f \in R[X]$. Putem scrie $f = c(f)f_0$, unde f_0 este un polinom primativ. Cum $f_0 \in K[X]$ iar $K[X]$ este un inel factorial (fiind euclidian), rezultă că $f_0 = f_1 f_2 \dots f_n$, unde $f_1, f_2, \dots, f_n \in K[X]$ și sunt polinoame ireductibile. Putem scrie evident pentru f_n , $f_n = \frac{a_n}{b_n} g_n$, unde $a_n, b_n \in R$ și $g_n \in R[X]$ este un polinom primativ. Conform lemei 6, rezultă că g_n este ireductibil în $R[X]$. Rezultă că f_0 se scrie sub forma $f_0 = \frac{a}{b} g_1 g_2 \dots g_n$, unde $a, b \in R$. Cum f_0 este primativ și produsul $g_1 g_2 \dots g_n$ este un polinom primativ, din lema 5 rezultă că $f_0 = ug_1 g_2 \dots g_n$, unde $u \in U(R)$. Cum $c(f)$ este un produs finit de elemente prime în R care sunt prime și în $R[X]$ (conform lemei 2) rezultă că f este un produs finit de elemente ireductibile în $R[X]$. Vom demonstra acum unicitatea scrierii lui f ca produs de elemente ireductibile în $R[X]$.

Intr-adevăr, să presupunem că avem egalitatea

$$f = f_1 f_2 \dots f_s = g_1 g_2 \dots g_n,$$

unde $f_i, g_i \in R[X]$ sunt elemente ireductibile în $R[X]$. Dacă $\text{grad } f_i \geq 1$, atunci evident $c(f_i) = 1$. Deci putem scrie

$$f = f_1 f_2 \dots f_s f_{s+1} \dots f_m = g_1 g_2 \dots g_r g_{r+1} \dots g_m,$$

unde $f_1, \dots, f_s, g_1, \dots, g_r \in R$ iar $f_{s+1}, \dots, f_m, g_{r+1}, \dots, g_m$ sunt polinoame de grad ≥ 1 . Aplicind lema lui Gauss obținem că $f_1 f_2 \dots f_s$ și $g_1 g_2 \dots g_r$ sunt asociate în divizibilitate în R . Cum R este factorial rezultă că $r = s$ și abstracție făcând de o renumerotare avem $g_i \sim f_i$, oricare ar fi $1 \leq i \leq s$. Din egalitatea de mai sus rezultă că

$$f_{s+1} \dots f_m = g_{s+1} \dots g_m.$$

Din lema 6, această egalitate găndită în inelul $K[X]$, implică $m = n$ și $g_k \sim f_k$ în $K[X]$, oricare ar fi $k = s + 1, \dots, n$.

Aplicind din nou lema 5, obținem că $g_k \sim f_k$ în $R[X]$, oricare ar fi $k = s + 1, \dots, n$. Cu aceasta am demonstrat și unicitatea lui f ca produs de elemente ireductibile în $R[X]$.

Corolar 6.2. *Dacă R este un inel factorial, atunci inelul de polinoame în n variabile $R[X_1, \dots, X_n]$ este factorial.*

Demonstrație. Se procedează prin inducție după n . Dacă $n = 1$, atunci se aplică teorema 6.1. Presupunem afirmația adevărată pentru $n - 1$. Deci inelul $R[X_1, \dots, X_{n-1}]$ este factorial. Cum $R[X_1, \dots, X_n] = R[X_1, \dots, X_{n-1}][X_n]$, aplicând din nou teorema 6.1, obținem afirmația noastră.

Corolarul 6.3. *Fie K un corp; atunci inelul de polinoame în n variabile $K[X_1, \dots, X_n]$ este factorial.*

Corolarul 6.4. *Inelul $Z[X_1, \dots, X_n]$ este factorial.*

Observație. Deoarece inelul $Z[X]$ este factorial și nu este inel principal (idealul $(2, X)$ de exemplu nu este principal), atunci avem incluziunile stricte:

$\{\text{Inelele euclidiene}\} \subsetneq \{\text{Inelele principale}\} \subsetneq \{\text{Inelele factoriale}\}$.

Apendice. A doua demonstrație pentru teorema 6.1.

Considerăm în inelul $R[X]$ mulțimea $(p_i)_{i \in I}$ a tuturor elementelor prime din R . Sistemul multiplicativ S generat de această mulțime este mulțimea tuturor elementelor nenule ale lui R . Atunci inelul de fracții $S^{-1}R[X]$ este exact inelul $K[X]$, unde K este corpul de fracții al lui R . Cum $K[X]$ este un inel euclidian, deci factorial, conform teoremei 3.2 este suficient să dovedim că orice lanț ascendent de ideale principale ale lui $R[X]$ este staționar. Fie, deci, lanțul ascendent de ideale principale ale lui $R[X]$:

$$(f_1) \subset (f_2) \subset \dots \subset (f_n) \subset \dots$$

unde $f_i \in R[X]$. Rezultă că avem relațiile:

$$f_{n+1} \mid f_n, \text{ oricare ar fi } n \geq 1.$$

Scriind $f_n = c(f_n)f'_n$, unde f'_n este un polinom primativ, din relația $f_{n+1} \mid f_n$ rezultă, conform lemei 1, că $c(f_{n+1}) \mid c(f_n)$ și conform lemei 4 obținem că $f'_{n+1} \mid f'_n$. În particular rezultă că avem sirul ascendent de ideale principale în R

$$(c(f_1)) \subset (c(f_2)) \subset \dots \subset (c(f_n)) \subset \dots$$

și siru descendente de numere naturale

$$(\text{grad } f'_1 \geq \text{grad } f'_2 \geq \dots \geq \text{grad } f_n \geq \dots)$$

Cum inelul R este factorial și cum multimea \mathbb{N} a numerelor naturale este bine ordonată există un $s \in \mathbb{N}$ astfel încit să avem

$$(c(f_s)) = (c(f_{s+1})) = \dots$$

și

$$\text{grad } f'_s = \text{grad } f'_{s+1} = \dots$$

Evident că avem $c(f_k) \sim c(f_{k+1})$, oricare ar fi $k \geq s$. Cum $f'_{s+1} \mid f'_s$, f'_s , f'_{s+1} sunt primitive și au același grad, rezultă că f'_s și f'_{s+1} sunt asociate în divizibilitate. Deci f_k și f_{k+1} sunt asociate în divizibilitate, oricare ar fi $k \geq s$, adică $(f_s) = (f_{s+1}) = \dots$.

§ 7. FACTORIALITATEA INELELOR DE SERII FORMALE

În acest paragraf ne propunem să demonstrăm următorul rezultat:

Teorema 7.1. *Dacă inelul R este principal, atunci inelul de serii formale într-o variabilă $R[[X]]$ este factorial.*

Demonstrație. Notăm cu $\varphi: R[[X]] \rightarrow R$ aplicația care asociază unei serii formale $f = a_0 + a_1X + \dots$ termenul a_0 , adică $\varphi(f) = a_0$. Se vede imediat că φ este un omomorfism surjectiv de inele. Pentru a arăta că $R[[X]]$ este un inel factorial este suficient să dovedim, conform teoremei 2.5, afirmația 5), că dacă p este un ideal prim al lui $R[[X]]$, atunci p conține un element prim. Dacă $X \in p$, atunci cum X este un element prim în $R[[X]]$, p conține un element prim.

Presupunem că $X \notin p$ și vom arăta în acest caz că p este un ideal principal. Într-adevăr, notăm cu $p^* = \varphi(p)$ care este un ideal al inelului R . Cum R este un inel principal, atunci există $a \in R$ astfel încit $p^* = Ra$. Există $f \in p$ astfel încit $a = \varphi(f)$. Deci f este de forma $f = a + a_1X + \dots + a_nX^n$.

Vom arăta că $p = R[[X]] \cdot f$. Cum $f \in p$, este evidentă incluziunea $R[[X]] \cdot f \subseteq p$.

Fie $g = b_0 + b_1X + \dots + b_nX^n + \dots$ un element oarecare din p . Cum $b_0 = \varphi(g)$, atunci $b_0 \in p^*$ și deci există $\lambda_0 \in R$ astfel încât $b_0 = \lambda_0a$. Dar atunci $g - \lambda_0f$ se scrie sub forma Xg_1 și cum $Xg_1 \in p$ dar $X \notin p$, rezultă că $g_1 \in p$. Înseamnă că există un $\lambda_1 \in R$ astfel încât $g_1 - \lambda_1f$ este de forma $\bar{X}g_2$.

Deci $g - \lambda_0f = Xg_1$ și $g_1 - \lambda_1f = Xg_2$ de unde obținem că

$$g = \lambda_0f + X(\lambda_1f + Xg_2) = (\lambda_0 + \lambda_1X)f + X^2g_2.$$

Continuind procedeul cu $g_2 \in p$, găsim $\lambda_2 \in R$ astfel încât

$g_2 - \lambda_2f$ este de forma Xg_3 și deci

$$g = (\lambda_0 + \lambda_1X + \lambda_2X^2)f + X^3g_3.$$

Recursiv găsim elementele $\lambda_1, \lambda_2, \dots, \lambda_n, \dots$ astfel încât dacă notăm cu $h = \lambda_0 + \lambda_1X + \dots + \lambda_nX^n + \dots$ avem egalitatea $g = hf$, adică $g \in R[[X]] \cdot f$ și deci p este un ideal principal generat de f . Cum p este un ideal prim, atunci f este un element prim în $R[[X]]$. Deci orice ideal prim al inelui $R[[X]]$ conține un element prim.

Corolarul 7.2. Dacă K este un corp, atunci inelul de serii formale în două variabile $K[[X, Y]]$ este un inel factorial.

Demonstrație. Avem $K[[X, Y]] = K[[X]][[Y]]$ și cum $K[[X]]$ este un inel euclidian (deci factorial), aplicând Teorema 7.1, rezultă afirmația din corolarul 7.2.

Observație. Un rezultat similar teoremei 6.1 nu are loc pentru inelele de serii formale, adică dacă R este un inel factorial, atunci inelul de serii formale $R[[X]]$ nu este în general un inel factorial. Evident, sunt cunoscute rezultate mult mai generale decit corolarul 7.2, ca, de exemplu: dacă K este un corp, atunci inelul de serii formale în n variabile $K[[X_1, \dots, X_n]]$ este un inel factorial.

§ 8. CRITERII DE IREDUCTIBILITATE PENTRU POLINOAME

Teorema 8.1. Fie R un inel factorial și $f = a_0 + a_1X + \dots + a_nX^n$ un polinom cu coeficienți în R . Presupunem că există un element prim $p \in R$ și un k , $0 \leq k \leq n$, cu proprietățile:

- i) $p \mid a_0, p \mid a_1, \dots, p \mid a_{k-1}$.
- ii) $p \nmid a_k$.
- iii) $p^2 \nmid a_0$.

Atunci f are, în descompunerea sa în factori ireductibili, un polinom de grad $\geq k$.

Demonstrație. Deoarece inelul $R[X]$ este factorial, atunci $f = -f_1 f_2 \dots f_t$, unde f_i sunt polinoame ireductibile. Trebuie să dovedim că unul dintre aceste polinoame are gradul $\geq k$. Prin reducere la absurd presupunem că $\text{grad } f_i < k$, oricare ar fi $i = 1, \dots, t$.

Considerăm inelul $R/(p)$ care este un domeniu de integritate deoarece (p) este un ideal prim și vom nota cu $\bar{\varphi}: R \rightarrow R/(p)$ surjecția canonica, adică $\bar{\varphi}(a) = \bar{a}$ (clasa elementului a).

φ induce morfismul de inele

$$\bar{\varphi}: R[X] \rightarrow R/(p)[X], \quad \bar{\varphi}(f) = \bar{a}_0 + \bar{a}_1 X + \dots + \bar{a}_n X^n.$$

Cum $\bar{\varphi}$ este un morfism de inele, rezultă că avem

$$\bar{\varphi}(f) = \bar{\varphi}(f_1) \bar{\varphi}(f_2) \dots \bar{\varphi}(f_t)$$

Cum $p | a_0, p | a_1, \dots, p | a_{k-1}$, rezultă că $\bar{a}_0 = \bar{a}_1 = \dots = \bar{a}_{k-1} = 0$ și deci $\bar{\varphi}(f) = \bar{a}_k X^k + \dots + \bar{a}_n X^n$ și deci $X^k | \bar{\varphi}(f)$, adică $X^k | \bar{\varphi}(f_1) \dots \bar{\varphi}(f_t)$. Cum X este un element prim în inelul $R/(p)[X]$ rezultă că X divide în particular unul dintre factorii $\bar{\varphi}(f_1), \dots, \bar{\varphi}(f_t)$. Să presupunem că $X | \bar{\varphi}(f_1)$. În acest caz rezultă că $X^k | \bar{\varphi}(f_1)$ deoarece dacă am avea $X | \bar{\varphi}(f_2)$ de exemplu, atunci notind cu a_{0i} termenul liber al polinomului f_i ($1 \leq i \leq t$) rezultă că $a_{0i} = a_{01} a_{02} \dots a_{0t}$. Pe de altă parte, din faptul că $X | \bar{\varphi}(f_1)$ și $X | \bar{\varphi}(f_2)$ rezultă că $\bar{a}_{01} = \bar{a}_{02} = 0$, adică $p | a_{01}$ și $p | a_{02}$ adică $p^2 | a_{01} a_{02} \dots a_{0t}$, adică $p^2 | a_0$, contradicție. Deci neapărat avem $X^k | \bar{\varphi}(f_1)$ și atunci $\text{grad } \bar{\varphi}(f_1) \geq k$. Cum am presupus $\text{grad } \bar{\varphi}(f_1) < k$, trebuie că $\bar{\varphi}(f_1) = 0$, dar atunci avem $\bar{\varphi}(f) = 0$ și deci $\bar{a}_k = 0$, adică $p | a_k$, ceea ce constituie o contradicție. În concluzie există un i , $1 \leq i \leq t$, astfel încât $\text{grad } f_i \geq k$.

Corolarul 8.2. (Criteriul de ireductibilitate al lui Eisenstein). Fie R un inel factorial, $f = a_0 + a_1 X + \dots + a_n X^n$ un polinom cu coeficienți în R . Presupunem că există un element prim $p \in R$ cu proprietățile

- i) $p | a_0, p | a_1, \dots, p | a_{n-1}$.
- ii) $p \nmid a_n$.
- iii) $p^2 \nmid a_0$.

Atunci f este ireductibil în $K[X]$, unde K este corpul de fracții al lui R .

Demonstrație. Aplicind teorema 8.1, polinomul f are un factor ireductibil de gradul n . Deci putem scrie că $f = ag$, unde $a \in R$. Cum g este ireductibil în $R[X]$, atunci conform lemei 6 din § 6 rezultă că g este ireductibil în $K[X]$ și deci f este ireductibil în $K[X]$.

Exemplu. 1. Fie polinomul

$$f = X^5 + 15X^4 + 20X^3 - 40X + 35.$$

Acest polinom este ireductibil în $\mathbb{Q}[X]$ deoarece luind numărul prim $p=5$, sint îndeplinite condițiile din corolarul 8.2.

2. Fie polinomul X^n+2 . Acest polinom este ireductibil conform criteriului lui Eisenstein. Acest exemplu ne arată că pentru orice număr natural n , există un polinom ireductibil în $\mathbb{Q}[X]$ având gradul n .

3. Fie p un număr prim. Polinomul

$f=X^{p-1}+X^{p-2}+\dots+X+1$ este ireductibil în $\mathbb{Q}[X]$. Sub această formă nu putem aplica criteriul lui Eisenstein pentru a arăta că f este ireductibil în $\mathbb{Q}[X]$. Dar se vede imediat că f este ireductibil dacă polinomul $g=f(X+1)$ este ireductibil. Cum $f(X)=\frac{X^p-1}{X-1}$, obținem că

$$\begin{aligned} g(X) &= \frac{(X+1)^p-1}{X} = X^p + C_p^1 X^{p-1} + C_p^2 X^{p-2} + \dots + C_p^{p-1} = \\ &= X^p + C_p^1 X^{p-1} + C_p^2 X^{p-2} + \dots + C_p^{p-2} X + p. \end{aligned}$$

Deoarece p este prim, avem că $p \mid C_p^k$, oricare ar fi $1 \leq k \leq p-1$ și deci, conform criteriului lui Eisenstein, $g(X)$ este un polinom ireductibil.

4. Polinomul $f=X^{2^n}+1$ este ireductibil în $\mathbb{Q}[X]$. Dar sub această formă nu putem să aplicăm criteriul lui Eisenstein. Vom arăta în schimb că polinomul

$$g(X)=f(X+1)=(X+1)^{2^n}+1$$

este ireductibil. Într-adevăr, avem $g(X)=X^{2^n}+\sum_{1 \leq k \leq 2^n-1} C_{2^n}^k X^k+2$.

Vom dovedi că $2 \mid C_{2^n}^k$ oricare ar fi $1 \leq k \leq 2^n-1$.

$$\text{Avem că } C_{2^n}^k = \frac{2^n(2^n-1)(2^n-2)\dots(2^n-k+1)}{k!}.$$

Fie $1 \leq k' < k$; putem scrie atunci $k'=2^p r$, unde $p < n$ și r este număr impar. Deoarece

$$\frac{2^n-k'}{k'} = \frac{2^p(2^{n-p}-r)}{2^p r} = \frac{2^{n-p}-2}{r}, \text{ atunci } \frac{2^n-k'}{k'} \text{ este egal cu cîtul a două numere impare. Deci produsul } \frac{(2^n-1)(2^n-2)\dots(2^n-(k-1))}{1 \cdot 2 \dots (k-1)} \text{ este cîtul a două numere impare. Cum } k < 2^n, \text{ atunci în cîtul } \frac{2^n}{k} \text{ apare cel puțin un factor egal cu 2. Deci } 2 \mid C_{2^n}^k.$$

Luind numărul prim $p=2$ și aplicînd criteriul lui Eisenstein, obținem că polinomul $g(X)$ este ireductibil. Aceasta arată că $f(X)=X^{2^n}+1$ este un polinom ireductibil în $\mathbb{Q}[X]$.

5. Să arătăm că polinomul $f=X^{p^n}+p-1$, unde p este un număr prim, este ireductibil.

Vom proceda ca în cazul precedent. Pentru a arăta că $f(X)$ este ireductibil este suficient să dovedim că polinomul $g(X)=f(X+1)$ este ireductibil. Într-adevăr, avem

$$g(X)=(X+1)^{p^n}+p-1=X^{p^n}+\sum_{1 \leq k \leq p^n-1} C_{p^n}^k X^k + 1 + p - 1 = X^{p^n} + \sum_{1 \leq k \leq p^n-1} C_{p^n}^k X^k + p.$$

Vom dovedi că $p \mid C_{p^n}^k$ oricare ar fi $1 \leq k \leq p^n-1$.

$$\text{Dar } C_{p^n}^k = \frac{p^n(p^n-1)\dots(p^n-k+1)}{k!}.$$

Fie $1 \leq k' < k$; putem scrie atunci $k'=p^t r$, unde $t < n$ și $(p, r) = 1$. Deoarece

$$\frac{p^n-k'}{k'} = \frac{p^n(p^{n-t}-r)}{p^t r} = \frac{p^{n-t}-r}{r}$$

se observă că din condiția că $(p, r) = 1$ rezultă că în fracția $\frac{p^n-k'}{k'}$, după simplificare, numărătorul și numitorul nu se mai divid cu p . Deci fracția $\frac{(p^n-1)\dots(p^n-(k-1))}{1\cdot 2\dots(k-1)}$, după simplificare, este cîntul a două

numere naturale în care atît numărătorul cît și numitorul nu se mai divid cu p . Deoarece $k < p^n$, atunci putem scrie $k=p^s k_1$, unde $s < n$ și $(p, k_1) = 1$. Deci $\frac{p^n}{k} = \frac{p^{n-s}}{k_1}$. Deci numărul întreg $C_{p^n}^k$ este cîntul a două numere naturale în care numărătorul se divide cu p (de fapt cu p^{n-s}) și numitorul nu se divide cu p .

În concluzie $p \mid C_{p^n}^k$. Aplicînd criteriul lui Eisenstein pentru numărul prim p obținem că polinomul $g(X)$ este ireductibil și deci polinomul $f(X)=X^{p^n}+p-1$ este ireductibil în $\mathbb{Q}[X]$.

Observație. Am văzut că dacă $1 \leq k < p^n$ și $k=p^s k_1$, unde $s < n$ și $(p, k_1) = 1$, atunci în descompunerea în factori primi a lui $C_{p^n}^k$, numărul p apare la puterea p^{n-s} .

În particular, cînd $k=p^{n-1}$, atunci în descompunerea în factori primi a lui $C_{p^n}^{p^{n-1}}$ numărul p apare la puterea p^1 .

Deci rezultă că c.m.m.d.c. al numerelor $C_{p^n}^k$ ($1 \leq k \leq p^n-1$) este egal cu p .

Un alt criteriu de ireductibilitate simplu, dar util, este următorul :

Teorema 8.3. Fie R și S două inele factoriale; $\varphi: R \rightarrow S$ un morfism de inele cu $\varphi(1)=1$, $\bar{\varphi}: R[X] \rightarrow S[X]$ morfismul de inele ce extinde pe φ , adică dacă $f=a_0+a_1X+\dots+a_nX^n \in R[X]$, atunci

$$\bar{\varphi}(f) = \varphi(a_0) + \varphi(a_1)X + \dots + \varphi(a_n)X^n.$$

Presupunem că f este un polinom primitiv în $R[X]$ astfel încât grad $f=\text{grad } \bar{\varphi}(f)$ și $\bar{\varphi}(f)$ este ireductibil în $S[X]$; atunci f este ireductibil.

Demonstrație. Presupunem că f nu este ireductibil în $R[X]$. Atunci $f=gh$ cu $g, h \in R[X]$ și g și h nu sunt inversabile în $R[X]$. Cum f este primitiv, atunci trebuie că grad $g \geq 1$ și grad $h \geq 1$. Dar din egalitatea $f=gh$ rezultă că $\bar{\varphi}(f)=\bar{\varphi}(g)\bar{\varphi}(h)$ și cum grad $\bar{\varphi}(g) \leq \text{grad } g$ și grad $\bar{\varphi}(h) \leq \text{grad } h$ iar grad $\bar{\varphi}(f)=\text{grad } f$ rezultă că $\bar{\varphi}(g)=\text{grad } g \geq 1$ și grad $\bar{\varphi}(h)=\text{grad } h \geq 1$ ceea ce arată că $\bar{\varphi}(f)$ nu este ireductibil în $S[X]$.

Exemplu. Fie p un număr prim și $a \in \mathbb{Z}$ astfel încât $(a, p)=1$. Să arătăm că polinomul $X^p - X + a$ este ireductibil în $\mathbb{Z}[X]$.

Într-adevăr, să considerăm inelul $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ care este corp finit și fie $\varphi: \mathbb{Z} \rightarrow \mathbb{Z}_p$, surjecția canonică, adică $\varphi(x)=\hat{x}$. Conform teoremei 8.3, pentru a arăta că polinomul $f=X^p - X + a$ este ireductibil, este suficient să dovedim că polinomul $g=X^p - X + \hat{a} \in \mathbb{Z}_p[X]$ este ireductibil în $\mathbb{Z}_p[X]$.

Cum \mathbb{Z}_p este un corp, există o extindere K a lui \mathbb{Z}_p astfel încât g are toate cele p rădăcini în K . Fie $\alpha \in K$ o rădăcină a lui g . Vom dovedi că $\alpha, \alpha+1, \alpha+2, \dots, \alpha+p-1$ sunt toate rădăcinile lui g . Într-adevăr, fie $\beta=\alpha+k$, $0 \leq k \leq p-1$, una dintre aceste rădăcini. Cum corpul K are caracteristica p , avem că

$$\begin{aligned} g(\beta) &= \beta^p - \beta + \hat{a} = (\alpha+k)^p - (\alpha+k) + \hat{a} = \alpha^p + \hat{k}^p - \alpha - \hat{k} + \hat{a} = \\ &= (\alpha^p - \alpha + \hat{a}) + \hat{k}^p - \hat{k}. \end{aligned}$$

Cum $\alpha^p - \alpha + \hat{a} = 0$ și ținând cont de teorema lui Fermat, avem $\hat{k}^p - \hat{k} = 0$. Deci $g(\beta) = 0$.

Presupunem că g nu este ireductibil în $\mathbb{Z}_p[X]$; atunci există $g_1, g_2 \in \mathbb{Z}_p[X]$ astfel încât $g=g_1g_2$ și grad $g_1 \geq 1$ și grad $g_2 \geq 1$. Cum $g=(X-\alpha)(X-\alpha-\hat{1})(X-\alpha-\hat{2})\dots(X-\alpha-(p-1))$ rezultă că g_1 este de forma $g_1=(X-\alpha-\hat{k}_1)\dots(X-\alpha-\hat{k}_s)$, unde $\hat{k}_1, \dots, \hat{k}_s \in \mathbb{Z}_p$, iar $1 \leq s < p$. Cum $g_1 \in \mathbb{Z}_p[X]$, atunci coeficientul termenului de gradul X^{s-1} al lui g_1 este $(\alpha+\hat{k}_1)+\dots+(\alpha+\hat{k}_s)$ și aparține lui \mathbb{Z}_p . Deci $s\alpha \in \mathbb{Z}_p$, de unde rezultă că $\alpha \in \mathbb{Z}_p$. Cum $g(\alpha)=0$, atunci $\alpha^p - \alpha + \hat{a} = 0$ și cum $\alpha^p - \alpha = 0$, din teorema lui Fermat obținem că $\hat{a}=0$, adică $p \mid a$, contradicție. Deci polinomul g este ireductibil și conform teoremei 8.3 rezultă că f este ireductibil în $\mathbb{Z}[X]$.

EXERCITII

1. Fie $n \geq 3$ un număr natural impar astfel încât n nu este patrat perfect. Să se arate că inelul $\mathbb{Z}[i\sqrt{n}] = \{a+ib\sqrt{n} \mid a, b \in \mathbb{Z}\}$ nu este factorial.

Indicație. Avem $n+1 = (1+i\sqrt{n})(1-i\sqrt{n})$ și cum $n+1$ este par avem $n+1 = 2k$. Se arată că elementele $2, k, 1+i\sqrt{n}, 1-i\sqrt{n}$ sunt ireductibile în acest inel dar nu sunt prime.

2. Fie R un inel factorial care nu este corp. Să se arate că dacă grupul $U(R)$ este finit, atunci R conține o infinitate de elemente prime neasociate.

Indicație. Să presupunem că R are un număr finit de elemente prime p_1, \dots, p_n neasociate. Pentru orice $k \in N$ considerăm elementele $q_k = (p_1 \dots p_n)^k + 1$. Avem $q_k \neq q_l$ pentru $k \neq l$. Din ipoteză rezultă că există un $r \in N$ astfel încât q_r este neinversabil. Scriem $q_r = up_1^{\alpha_1} \dots p_n^{\alpha_n}$, unde $u \in U(R)$ și cel puțin un $\alpha_i > 0$. Rezultă că p_i este inversabil, contradicție.

3. Fie inelul $\mathbb{Z}[\theta] = \{m+n\theta \mid m, n \in \mathbb{Z}\}$, unde θ este o rădăcină a ecuației $x^2+ax+b=0$ ($a, b \in \mathbb{Z}$). Dacă $d=a^2-4b<0$ să se arate că $U(\mathbb{Z}[\theta])$ este un grup finit.

4. Să se arate că $U(\mathbb{Z}\sqrt{2})$ este un grup infinit.

5. Să se arate că inelele \mathbb{Z} , $\mathbb{Z}[i]$, $\mathbb{Z}[i\sqrt{2}]$, $\mathbb{Z}\left[\frac{1+\sqrt{3}}{2}\right]$ sunt infinite de elemente prime neasociate.

Indicație. Se aplică exercițiile 2) și 3).

6. Fie R un inel factorial și $a, b \in R$ două elemente prime între ele. Dacă m și n sunt două numere naturale să se arate că dacă

$$d=(m, n), \text{ atunci } (a^m - b^m, a^n - b^n) = a^d - b^d.$$

Indicație. Se vede imediat că $a^d - b^d \mid a^m - b^m$ și $a^d - b^d \mid a^n - b^n$. Dacă notăm cu $\delta = (a^m - b^m, a^n - b^n)$ rezultă că $a^d - b^d \mid \delta$. Invers pentru a arăta că $\delta \mid a^d - b^d$ se scrie algoritmul lui Euclid pentru numerele m și n

$$m = nq_1 + r_1 \text{ cu } 0 \leq r_1 < n$$

$$n = r_1q_2 + r_2 \text{ cu } 0 \leq r_2 < r_1$$

.....

$$r_{n-2} = r_{n-1}q_n + r_n \text{ cu } 0 \leq r_n < r_{n-1}$$

$$r_{n-1} = r_n q_{n+1}$$

Deci $d = r_n$.

Se arată că $\delta \mid a^{r_1} - b^{r_1}$ și din aproape în aproape obținem că $\delta \mid a^{r_n} - b^{r_n}$.

7. Să se arate că dacă m și n sunt două numere naturale cu $d = (m, n)$, atunci

$$2^d - 1 = (2^m - 1, 2^n - 1).$$

8. Să se arate că dacă m și n sunt două numere naturale cu $d = (m, n)$, atunci în inelul $R = K[X]$, unde K este un corp are loc relația

$$X^d - 1 = (X^m - 1, X^n - 1).$$

Indicație. Pentru 7) și 8) se aplică 6).

9. Fie $x, y \in \mathbb{R}$ cu $y \neq 0$. Să se arate că există $q, r \in \mathbb{R}$ unice cu proprietățile următoare:

$$x = yq + r, \text{ unde } q \in \mathbb{Z} \text{ și } 0 \leq r < |y|.$$

Indicație. Dacă $y > 0$, atunci $q = \left[\frac{x}{y} \right]$, adică partea întreagă a numărului $\frac{x}{y}$.

10. Fie K un corp de caracteristică $\neq 2$. Să se arate că în inelul $K[X, Y]$ polinomul $X^2 + Y^2 - 1$ este ireductibil.

Indicație. Considerăm polinomul $X^2 + Y^2 - 1$ ca polinom în X și cu coeficienți în $K[Y]$. Se observă că $Y - 1$ este element prim în $K[Y]$ și $Y - 1 \mid Y^2 - 1$. Cum $\text{char } K \neq 2$, atunci $(Y - 1)^2 \nmid Y^2 - 1$. În continuare se aplică criteriul lui Einstein.

11. Fie K un corp. Să se arate că polinoamele $X^2 - Y^2$, $X^2 - Y^2 Z$, $X^2 - Y Z^2$ sunt ireductibile în $K[X, Y, Z]$.

Indicație. Se aplică criteriul lui Eisenstein.

12. Fie polinomul omogen de gradul n ,

$$f(X, Y) = a_0 X^n + a_1 X^{n-1} Y + \dots + a_{n-1} X Y^{n-1} + a_n Y^n \in \mathbb{Q}[X, Y].$$

Să se arate că

- a) Orice factor ireductibil al lui $f(X, Y)$ este un polinom omogen
- b) $f(X, Y)$ este ireductibil dacă și numai dacă polinomul

$$f(X, 1) = a_0 X^n + a_1 X^{n-1} + \dots + a_n \in \mathbb{Q}[X]$$

este ireductibil.

Indicație. a) Se înlocuiește Y cu tX , unde $t \in \mathbb{Q}$.

13. Fie n^2 nedeterminatele X_{ij} . Să se arate că polinomul

$$\det(X_{ij})_{1 \leq i, j \leq n} = \sum_{\sigma \in S_n} \epsilon(\sigma) X_{1\sigma(1)} X_{2\sigma(2)} \dots X_{n\sigma(n)}$$

este ireductibil în $\mathbb{Z}[X_{ij}]_{1 \leq i, j \leq n}$.

14. Fie $\mathbb{Z}[i] = \{a+ib \mid a, b \in \mathbb{Z}\}$ inelul întregilor lui Gauss și $\varphi: \mathbb{Z}[i] \rightarrow \mathbb{N}$ funcția $\varphi(a+ib) = a^2 + b^2$.

Să se arate că:

- a) Orice element prim din $\mathbb{Z}[i]$ este un divizor al unui număr prim din \mathbb{Z} .

Indicație. Dacă $\pi \in \mathbb{Z}[i]$ este prim, atunci $\varphi(\pi) \in \mathbb{N}$. Fie $\varphi(\pi) = p_1 \dots p_s$, unde p_1, p_2, \dots, p_s sunt numere prime din \mathbb{Z} . Cum $\pi(\varphi) = \pi\pi$, atunci $\pi \mid p_1 \dots p_s$, și deci π divide un anume p_i .

- b) $1+i$ și $1-i$ sunt prime în $\mathbb{Z}[i]$

- c) Orice număr prim p de forma $4k+3$ este prim în $\mathbb{Z}[i]$.

Indicație. Presupunem că p nu este prim în $\mathbb{Z}[i]$, deci avem $p = z_1 z_2$, unde $z_1 = a_1 + b_1 i$ și $z_2 = a_2 + b_2 i$ nu sunt inversabile în $\mathbb{Z}[i]$.

Aveam $p^2 = \varphi(p) = \varphi(z_1)\varphi(z_2) = (a_1^2 + b_1^2)(a_2^2 + b_2^2)$ și deci $a_1^2 + b_1^2 = a_2^2 + b_2^2 = p$. Deci trebuie ca $a_1 = 2r$ sau $a_1 = 2r+1$ și $b_1 = 2s$ sau $b_1 = 2s+1$. În acest caz rezultă că p este de forma $4k+1$, contradicție.

- d) Orice număr prim p de forma $4k+1$ este produsul a două elemente prime din $\mathbb{Z}[i]$ care nu sunt asociate în divizibilitate. În plus, aceste elemente prime sunt conjugate unul celuilalt.

Indicație. Utilizând teorema lui Wilson: $(p-1)! + 1 \equiv 0 \pmod{p}$ și sirul de congruențe:

$$\begin{aligned} p-1 &\equiv -1 \pmod{p} \\ p-2 &\equiv -2 \pmod{p} \end{aligned}$$

$$\frac{p-1}{2} + 1 \equiv -\frac{p-1}{2} \pmod{p}$$

obținem că $1+x^2 \equiv 0 \pmod{p}$, unde $x = \left(\frac{p-1}{2}\right)!$. Deci $p \mid (1+ix)$

• $(1-ix)$. Dacă p ar fi prim în $\mathbb{Z}[i]$, atunci $p \mid 1+ix$ sau $p \mid 1-ix$ și fiecare duce la o contradicție. Deci p în $\mathbb{Z}[i]$ se scrie $p = \pi_1 \pi_2 \dots \pi_s$, unde $\pi_i \in \mathbb{Z}[i]$ sunt elemente prime iar $s \geq 2$. Cum $p^2 = \varphi(p) = \varphi(\pi_1) \dots \varphi(\pi_s)$, atunci trebuie ca $s \leq 2$, adică $s=2$. Deci $p = \pi_1 \pi_2$. Rezultă $\pi_2 = \pi_1$ și π_1 și π_2 nu sunt asociate în divizibilitate.

- e) Dacă notăm cu $P = \{1+i\} \cup \{\text{mulțimea numerelor naturale prime de forma } 4k+3\} \cup \{\text{mulțimea divizorilor primi în } \mathbb{Z}[i]\}$ ai numerelor naturale prime de forma $4k+1\}$ să se arate că orice element prim din $\mathbb{Z}[i]$ este asociat cu un element din mulțimea P .

- f) Să se arate că orice număr natural prim p de forma $4k+1$ este suma a două pătrate.

Indicație. $p = \pi_1\pi_2$, unde $\pi_1 = a + ib$ iar $\pi_2 = a - ib$. Deci $p = a^2 + b^2$.

15. Să se descompună în factori primi în inelul $\mathbb{Z}[i]$ numerele 200, 550, 600, 750.

16. Să se arate că mulțimea numerelor prime de forma $4k+3$ este infinită.

Indicație. Orice număr de forma $4k-1$ în descompunerea sa în factori primi conține un factor prim de forma $4l-1$. Presupunem că există un număr infinit de numere prime p_1, \dots, p_n de forma $4k-1$. Fie $N = 4p_1p_2\dots p_n - 1$. Există un număr prim p de forma $4l-1$ care divide pe N . În acest caz rezultă că $p \mid 1$.

17. Să se arate că mulțimea numerelor prime de forma $4k+1$ este infinită.

Indicație. Presupunem că această mulțime este finită și fie p_1, \dots, p_n aceste numere.

Fie $x = (p_1\dots p_n)^2 + 1$. Fie q un divizor prim al lui x . Dacă q este de forma $4k+3$, atunci q este prim în $\mathbb{Z}[i]$. Dacă notăm $a = p_1\dots p_n$, atunci $q \mid (1+ia)(1-ia)$ și deși $q \mid 1+ia$ sau $q \mid 1-ia$ care conduce la contradicție.

Deci q este neapărat de forma $4k+1$, adică $q \in \{p_1, \dots, p_n\}$.

Cum $q \mid x$ rezultă $q \mid 1$, contradicție.

18. Să se arate că există o infinitate de numere prime de forma $6k-1$, $k \in \mathbb{N}$.

Capitolul V

MODULE ȘI SPAȚII VECTORIALE

§ 1. MODUL. SUBMODUL. MORFISME DE MODULE

Definiția 1.1. Fie R un inel unitar și $(M, +)$ un grup abelian. Spunem că M este R -modul la stînga, sau modul la stînga peste R , dacă este definită o operație algebrică externă pe M , adică o funcție

$$f: R \times M \rightarrow M, f(a, x) = ax,$$

astfel încît să fie îndeplinite următoarele condiții:

- 1) $a(x+y) = ax+ay$,
- 2) $(a+b)x = ax+bx$,
- 3) $(ab)x = a(bx)$,
- 4) $1x = x$,

oricare ar fi $a, b \in R$ și $x, y \in M$.

În mod analog se definește noțiunea duală, cea de R -modul la dreapta. Mai precis, un grup abelian $(M, +)$ este R -modul la dreapta, sau modul la dreapta peste R , dacă este definită o operație algebrică externă pe M ,

$$g: M \times R \rightarrow M, g(x, a) = xa$$

astfel încît

- 1') $(x+y)a = xa + ya$,
- 2') $x(a+b) = xa + xb$,
- 3') $x(ab) = (xa)b$,
- 4') $x1 = x$,

oricare ar fi $a, b \in R$ și $x, y \in M$.

Grupul abelian M se numește grupul aditiv subiacent R -modulului la stînga, respectiv la dreapta M .

Dacă M este un R -modul la stînga sau la dreapta, elementele lui R se numesc scalari iar operația externă se numește înmulțire cu scalari. Faptul că M este un R -modul la stînga, respectiv la dreapta se mai notează și prin ${}_R M$, respectiv M_R .

Observație. Fie R un inel unitar, M un grup abelian și $\text{End } M$ inelul endomorfismelor lui M . Orice morfism unitar de inele $\varphi: R \rightarrow \text{End } M$ definește pe M o structură de R -modul la stînga, punind

$$ax = \varphi(a)(x), \text{ oricare ar fi } a \in R \text{ și } x \in M.$$

Se verifică cu ușurință că sunt îndeplinite condițiile 1)–4). De exemplu,

$$a(x+y) = \varphi(a)(x+y) = \varphi(a)(x) + \varphi(a)(y) = ax + ay.$$

Reciproc, fie M un R -modul la stînga. Dacă $a \in R$, atunci funcția $\varphi_a: M \rightarrow M$, $\varphi_a(x) = ax$, este un morfism de grupuri abeliene, iar $\varphi: R \rightarrow \text{End } M$, $\varphi(a) = \varphi_a$ este un morfism unitar de inele. Deoarece $\varphi(a)(x) = \varphi_a(x) = ax$, rezultă că R -modulul la stînga definit pe grupul aditiv subiacent lui M de către morfismul φ coincide cu R -modulul la stînga dat. Considerații analoage se pot face pentru R -modulele la dreapta.

Fie R un inel și R° inelul opus inelului R . Amintim că grupul aditiv subiacent lui R° coincide cu cel al lui R iar operația de înmulțire „*“ din R° este dată prin $a*b = ba$, unde ba este produsul elementelor b și a în inelul R .

Dacă M este un R -modul la stînga, definim pe M operația algebrică externă $h: M \times R^\circ \rightarrow M$, dată de $h(x, a) = ax$.

Să notăm $h(x, a) = x*a$. Atunci

$$x*(a*b) = (a*b)x = (ba)x = b(ax) = (ax)*b = (x*a)*b,$$

adică este verificată condiția 4') a modulelor la dreapta. Celelalte condiții sunt imediate. Deci orice R -modul la stînga M devine un R° -modul la dreapta pe care-l vom nota M° și-l vom numi opusul modulului M . Analog, orice R -modul la dreapta devine un R° -modul la stînga. În cazul comutativ inelele R și R° sunt aceleași și deci orice R -modul la stînga M este și R -modul la dreapta după legea $xa = ax$, pentru orice $x \in M$ și $a \in R$ și reciproc. Deci cele două concepte de R -modul la stînga și la dreapta coincid și de aceea în acest caz vom spune pur și simplu R -modul. Dacă inelul considerat este un corp K , atunci orice K -modul la stînga, respectiv la dreapta, se numește *spațiu vectorial* la stînga, respectiv la dreapta, peste corpul K sau *K -spațiu vectorial*.

În acest paragraf, dacă nu menționăm contrariul, prin R -modul vom înțelege un R -modul la stînga, noțiunile și rezultatele obținute transportindu-se direct și pentru R -module la dreapta.

Exemplu. 1) Un inel R poate fi conceput ca un R -modul la stînga, considerind grupul aditiv subiacent inelului R , împreună cu operația externă $R \times R \rightarrow R$, dată prin $(a, x) \rightarrow ax$, unde ax este produsul în R al elementelor a și x din inelul R .

În mod analog se poate defini pe R și o structură de R -modul la dreapta. Inelul R privit ca R -modul la stînga și la dreapta se notează respectiv cu R_s și R_d .

2) Fie G un grup abelian. Funcția $\mathbb{Z} \times G \rightarrow G$ dată prin $(n, x) \rightarrow nx$ este o operație algebrică externă pe G cu scalari din \mathbb{Z} , în raport cu care G devine un \mathbb{Z} -modul.

3) Fie R un inel comutativ unitar, $n \geq 1$ un număr natural și

$$R_n[X] = \{P \in R[X] \mid \text{grad } P \leq n\}.$$

Mulțimea $R_n[X]$, cu adunarea obișnuită a polinoamelor, are o structură de grup abelian.

Mai mult, dacă luăm ca operație externă, înmulțirea polinoamelor cu elemente din R prin înmulțirea tuturor coeficienților cu un astfel de element, obținem pe $R_n[X]$ o structură de R -modul.

La fel, mulțimea $R[X]$ a tuturor polinoamelor cu coeficienți în R are o structură de R -modul.

4). Fie R un inel unitar și $I \neq \emptyset$ o mulțime nevidă. Fie $R' = \{f \mid f: I \rightarrow R\}$. Pentru $a \in R$ și $f, g \in R'$ definim $f+g$ și af în modul următor:

$$(f+g)(i) = f(i) + g(i),$$

$$(af)(i) = af(i),$$

oricare ar fi $i \in I$. Cu adunarea și înmulțirea cu scalari definite mai înainte, R' devine un R -modul la stânga. Verificarea acestui fapt se face cu ușurință și de aceea o omitem. Menționăm doar că elementul neutru la adunare este funcția $0: I \rightarrow R$, $0(i) = 0$, oricare ar fi $i \in I$, iar opusul elementului $f \in R'$ este funcția $-f$, definită prin $(-f)(i) = -f(i)$, oricare ar fi $i \in I$.

În particular, fie m, n numere naturale ≥ 1 , $M = \{1, 2, \dots, m\}$, $N = \{1, 2, \dots, n\}$ iar $I = M \times N$. Dacă R este inel comutativ și unitar, atunci $R^{M \times N} = \mathcal{M}(m, n, R)$ are o structură de R -modul.

5) Dacă $[a, b]$ este un interval al mulțimii \mathbf{R} a numerelor reale, fie mulțimea

$$C([a, b], \mathbf{R}) = \{f: I \rightarrow \mathbf{R} \mid f \text{ continuă}\}.$$

Operațiile algebrice definite la exemplul 4) dau pe această mulțime operații algebrice în raport cu care aceasta devine un spațiu vectorial peste corpul \mathbf{R} al numerelor reale.

6) De asemenea, mulțimea

$$D([a, b], \mathbf{R}) = \{f: I \rightarrow \mathbf{R} \mid f \text{ derivabilă}\},$$

înzestrată cu operațiile de la exemplul precedent devine în mod clar un \mathbf{R} -spațiu vectorial.

Propoziția 1.2. Dacă M este un R -modul $a, b \in R$ și $x, y \in M$, atunci

- 1) $a0=0x=0$;
- 2) $(-a)x=-ax$, $a(-x)=-ax$, $(-a)(-x)=ax$;
- 3) $a(x-y)=ax-ay$;
- 4) $(a-b)x=ax-bx$;

5) Dacă, în plus, R este corp și $ax=0$, atunci $a=0$ sau $x=0$.

Demonstrație. 1) Avem $a0 = a(0+0) = a0 + a0$. Dacă adunăm la ambii membri ai egalității $a0 = a0 + a0$ elementul $-a0$ rezultă că $0 = a0$. La fel, $0x = (0+0)x = 0x + 0x$ și adunând la ambii membri ai egalității $0x = 0x + 0x$ pe $-0x$ rezultă că $0 = 0x$.

2) Avem $0 = 0x = (a + (-a))x = ax + (-a)x$. Relația $0 = ax + (-a)x$ arată că $(-a)x = -ax$. La fel, se demonstrează că $a(-x) = -ax$, iar ultima relație de la 2) rezultă imediat din primele două.

3) $a(x-y) = a(x+(-y)) = ax + a(-y) = ax - ay$.

4) Se demonstrează analog cu cea precedentă.

5) Fie $ax = 0$. Dacă $a \neq 0$ și cum R este corp, există $a^{-1} \in R$. Avem că $a^{-1}(ax) = a^{-1}0$ adică $(a^{-1}a)x = 0$ și deci $x = 0$.

Definiția 1.3. Fie M un R -modul la stînga. O submulțime nevidă $N \subset M$ se numește *submodul* al modului M dacă sunt îndeplinite condițiile:

1) oricare ar fi $x, y \in N$, atunci $x - y \in N$.

2) oricare ar fi $a \in R$ și $x \in N$, atunci $ax \in N$.

Prima condiție ne arată că N este subgrup al grupului aditiv M . Deci $0 \in N$ iar dacă $x \in N$, atunci $-x \in N$.

Fie N un submodul al R -modului M . Rezultă că operațiile algebrice definite pe M , induc pe N , luând restricțiile lor la $N \times N$ respectiv $R \times N$, două operații algebrice și anume adunarea și înmulțirea cu scalari:

$$N \times N \rightarrow N, (x, y) \rightarrow x - y,$$

$$R \times N \rightarrow N, (a, x) \rightarrow ax.$$

Mulțimea N împreună cu aceste operații algebrice constituie în mod clar un R -modul. Axiomele modului sunt evident îndeplinite deoarece ele sunt îndeplinite în cazul modului M .

Dacă R este un corp și deci M este un spațiu vectorial, un submodul al lui M se numește *subspațiu vectorial*.

Exemple. 1) Dacă M este un R -modul oarecare, atunci M și $\{0\}$ sunt submodule ale sale. Submodulul $\{0\}$ se va numi *submodulul nul* al lui M .

2) Dacă R este un inel, submodulele lui R , sunt idealele la stînga ale lui R , iar submodulele lui R_a sunt idealele la dreapta ale lui R .

3) Am văzut că orice grup abelian G are o structură de \mathbb{Z} -modul. Submodulele lui G privit ca \mathbb{Z} -modul coincid cu subgrupurile grupului G .

4) Dacă R este un inel comutativ și unitar, avem că $R[X]$ este un submodul al R -modului $R[X]$ (vezi ex. 3)).

5) Spațiul $D([0, 1], R)$ este un subspațiu vectorial al spațiului $C([0, 1], R)$ (vezi ex. 5)).

Propoziția 1.4. Fie M un R -modul și $\{N_\alpha\}_{\alpha \in A}$ o familie de submodule ale lui M . Atunci $\bigcap_{\alpha \in A} N_\alpha$ este un submodul al lui M .

Demonstrație. De la grupuri avem că $\bigcap_{\alpha \in A} N_\alpha$ este un subgrup al grupului abelian subiacent lui M . Dacă $a \in R$ și $x \in \bigcap_{\alpha \in A} N_\alpha$, atunci $a \in R$ și $x \in N_\alpha$, oricare ar fi $\alpha \in A$ și deci $ax \in N_\alpha$, oricare ar fi $\alpha \in A$, de unde $ax \in \bigcap_{\alpha \in A} N_\alpha$.

Definiția 1.5. Fie M un R -modul și S o submulțime a lui M . Intersecția tuturor submodulelor la stînga ale lui R care conțin mulțimea S se numește *submodulul la stînga generat de mulțimea S* . Se spune că S este un *sistem de generatori* ai acestui submodul. Submodulul generat de mulțimea vidă este submodulul nul.

Să notăm cu $\langle S \rangle$ submodulul generat de S .

Propoziția 1.6. Fie M un R -modul și S o submulțime nevidă a sa.

Atunci

$$\langle S \rangle = \left\{ \sum_{i=1}^n a_i x_i \mid a_i \in R, x_i \in S, n \in \mathbb{N} \right\}.$$

Demonstrație. Observăm mai întii că $N = \left\{ \sum_{i=1}^n a_i x_i \mid a_i \in R, x_i \in S, n \in \mathbb{N} \right\}$ este un submodul la stînga al lui M , care conține submulțimea S . Deci $N \supset \langle S \rangle$. Pe de altă parte, deoarece $S \subset \langle S \rangle$, atunci oricare ar fi $x \in N$, $x = \sum_{i=1}^n a_i x_i$, unde $a_i \in R$, $x_i \in S$, aparține lui $\langle S \rangle$. Deci $\langle S \rangle = N$ ceea ce trebuia demonstrat.

Observăm că $\langle S \rangle$ este cel mai mic submodul, în raport cu incluziunea, care conține mulțimea S .

Este clar că, dacă $x \in M$, atunci $\langle \{x\} \rangle = \{ax \mid a \in R\}$. Submodulul $\langle \{x\} \rangle$ se notează prin Rx și se numește *submodulul ciclic sau monogen* al lui M generat de x .

Definiția 1.7. Fie M un R -modul și $\{N_\alpha\}_{\alpha \in A}$ o familie de submodule ale sale. Submodulul generat de $\bigcup_{\alpha \in A} N_\alpha$ se numește *suma* familiei de submodule $\{N_\alpha\}_{\alpha \in A}$ și o vom nota cu $\sum_{\alpha \in A} N_\alpha$.

Avînd în vedere propoziția precedentă rezultă că

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

În particular, dacă N_1, N_2, \dots, N_k sunt submodule ale lui M , atunci

$$\sum_{i=1}^k N_i = \left\{ \sum_{i=1}^k x_i \mid x_i \in N_i, i = 1, 2, \dots, k \right\}.$$

Observăm că dacă S este o submulțime a R -modulului M , atunci

$$\langle S \rangle = \sum_{x \in S} Rx.$$

Definiția 1.8. Fie M și M' două R -module. Se numește *morfism* de R -module de la M la M' o funcție $f: M \rightarrow M'$ astfel încât să fie satisfăcute următoarele condiții:

- 1) $f(x+y)=f(x)+f(y)$, oricare ar fi $x, y \in M$.
- 2) $f(ax)=af(x)$, oricare ar fi $a \in R$ și $x \in M$.

Deoarece f este, în particular, morfism de la grupul aditiv $(M, +)$ la grupul aditiv $(M', +)$, știm că $f(0)=0$ și $f(-x)=-f(x)$, oricare ar fi $x \in M$.

Dacă R este corp și deci M și M' sunt spații vectoriale, morfismul $f: M \rightarrow M'$ se numește *morfism de spații vectoriale sau aplicație liniară* de la M la M' .

Observăm că pentru orice două R -module M și M' , funcția $\theta: M \rightarrow M'$, definită prin $\theta(x)=0$, este un morfism de R -module numit *morfismul nul*.

Proprietățile morfismelor de module se obțin fără dificultate din cele ale morfismelor de grupuri.

1º Dacă M, M', M'' sint R -module iar $f: M \rightarrow M'$, $g: M' \rightarrow M''$ sint morfisme, atunci $gof: M \rightarrow M''$ este un morfism de R -module.

Proprietatea analogă pentru grupuri arată că gof este morfism de grupuri de la M la M'' . În plus, oricare ar fi $a \in R$ și $x \in M$, avem $(gof)(ax)=g(f(ax))=g(af(x))=ag(f(x))=a(gof)(x)$.

2º Pentru orice R -modul M , funcția identică este un morfism de module, numit *morfismul identic* al lui M . Avem că oricare ar fi $f: M \rightarrow M'$ un morfism de module, atunci

$$f \circ 1_M = f \text{ și } 1_{M'} \circ f = f.$$

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

$$f \circ g = 1_{M'} \text{ și } g \circ f = 1_M.$$

Un morfism de module $f: M \rightarrow M'$ astfel încât funcția f este injectivă (respectiv surjectivă) se numește *monomorfism* (respectiv *epimorfism*).

Teorema 1.9. Un morfism de module $f: M \rightarrow M'$ este izomorfism dacă și numai dacă funcția f este bijectivă.

Demonstrație. Având în vedere rezultatul corespunzător de la grupuri este suficient să demonstrăm că, dacă $g: M' \rightarrow M$ este o funcție astfel încât $f \circ g = 1_{M'}$ și $g \circ f = 1_M$, atunci $g(ay) = ag(y)$, oricare ar fi $a \in R$ și $y \in M'$.

Într-adevăr, $a \cdot y = 1_{M'}(a \cdot y) = (f \circ g)(a \cdot y) = f(g(a \cdot y))$.

Pe de altă parte,

$$a \cdot y = a \cdot 1_{M'}(y) = a(f \circ g)(y) = a \cdot f(g(y)) = f(a \cdot g(y)).$$

Deci $f(g(a \cdot y)) = f(a \cdot g(y))$ și cum f este injectivă, rezultă $g(a \cdot y) = a \cdot g(y)$.

Exemplu. 1) Fie R un inel, $I \neq \emptyset$ o mulțime oarecare și să considerăm R -modulul R^I construit în ex. 4). Pentru fiecare $i \in I$, definim o funcție $\varphi^i: R^I \rightarrow R$, prin $\varphi^i(f) = f(i)$. Dacă $a \in R$ și $f, g \in R^I$, atunci

$$\varphi^i(f+g) = (f+g)(i) = f(i) + g(i) = \varphi^i(f) + \varphi^i(g)$$

și

$$\varphi^i(af) = (af)(i) = af(i) = a\varphi^i(f).$$

Deci φ^i , $i \in I$, este morfism de R -module.

2) Fie $\mathcal{M}_n(R)$ modulul peste R al matricelor pătratice cu n linii și n coloane (vezi ex. 4)). Considerând pe R structura de R -modul, definim funcția

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

ncit pentru $A = (a_{ij})_{1 \leq i, j \leq n}$, $\text{Tr}(A) = \sum_{i=1}^n a_{ii}$. Numim $\text{Tr}(A)$ urma matricei A . Funcția Tr este un morfism de R -module, după cum se verifică ușor.

3) Fie K un corp și $K[X]$ spațiul vectorial al polinoamelor în nedeterminata X . Funcția

$$d: K[X] \rightarrow K[X], \quad d(f) = f^{(1)},$$

unde $f^{(1)}$ este derivata lui f este un morfism de K -spații vectoriale (vezi cap. III, §8).

4) Să considerăm R -spațiul vectorial

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

(vezi ex. 5)). Fie funcția $I: C([0, 1], R) \rightarrow C([0, 1], R)$, definită astfel:

Dacă $f \in C([0, 1], R)$, atunci $I(f) \in C([0, 1], R)$, dată prin $I(f)(x) = \int_0^x f(t) dt$.

Funcția I este morfism de spații vectoriale. Într-adevăr, dacă $f, g \in C([0, 1], R)$, atunci oricare ar fi $x \in [0, 1]$, avem

$$I(f+g)(x) = \int_0^x (f+g)(t) dt = \int_0^x f(t) dt + \int_0^x g(t) dt =$$

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

Deci $I(f+g) = I(f) + I(g)$.

La fel, dacă $a \in R$ și $f \in C([0,1], R)$, avem

$$I(af) = aI(f).$$

Fie M și M' două R -module și $f: M \rightarrow M'$ un morfism de module. Este clar că dacă N este un submodul al lui M , atunci $f(N)$ este un submodul al lui M' . Reciproc, dacă N' este un submodul al lui M' , atunci $f^{-1}(N')$ este un submodul al lui M .

În particular,

$$\text{Ker } f = f^{-1}(\{0\}) = \{x \in M \mid f(x) = 0\} \text{ și } \text{Im } f = f(M)$$

sunt submodule în M și respectiv în M' .

Pentru R -modulele M și M' mulțimea

$$\text{Hom}_R(M, M') = \{f: M \rightarrow M' \mid f \text{ morfism}\}$$

devine un grup abelian, față de adunarea definită în modul următor.

Dacă $f, g \in \text{Hom}_R(M, M')$ sunt morfisme oarecare, definim funcția $f+g: M \rightarrow M'$ prin $(f+g)(x) = f(x) + g(x)$. Funcția $f+g$ este un morfism de R -module. Într-adevăr,

$$1^{\circ} (f+g)(x+y) = f(x+y) + g(x+y) = f(x) + f(y) + g(x) + g(y) = f(x) + g(x) + f(y) + g(y) = (f+g)(x) + (f+g)(y), \text{ oricare ar fi } x, y \in M.$$

$$2^{\circ} (f+g)(ax) = f(ax) + g(ax) = af(x) + ag(x) = a(f(x) + g(x)) = a(f+g)(x), \text{ oricare ar fi } a \in R \text{ și } x \in M.$$

Dacă R este un inel comutativ definim de asemenea o operație algebrică externă, mai precis înmulțirea cu scalari din R . Dacă $a \in R$ și $f \in \text{Hom}_R(M, M')$, atunci $af: M \rightarrow M'$ este funcția dată prin $(af)(x) = af(x)$. Se verifică ușor că af este morfism de R -module. De exemplu, dacă $b \in R$ și $x \in M$, atunci

$$(af)(bx) = af(bx) = a(bf(x)) = (ab)f(x) = (ba)f(x) = b(af(x)) = b(af)(x).$$

În raport cu adunarea și înmulțirea cu scalari definite mai înainte se verifică ușor că mulțimea $\text{Hom}_R(M, M')$ formează un R -modul. Lăsăm ca exercițiu verificarea axiomelor de modul. Menționăm doar că elementul neutru la adunare este morfismul nul, iar elementul opus morfismului $f: M \rightarrow M'$ este morfismul $-f: M \rightarrow M'$, definit prin $(-f)(x) = -f(x)$.

Definiția 1.10. Spunem că o mulțime nevidă A formează o *algebră peste inelul comutativ și unitar R* , dacă pe mulțimea A sunt definite două operații algebrice interne, adunarea și înmulțirea și o operație externă, înmulțirea cu scalari din R , astfel încât următoarele condiții să fie îndeplinite:

1) A este un inel unitar,

2) A este R -modul,

3) $a(xy) = (ax)y = x(ay)$, oricare ar fi $a \in R$, $x, y \in A$.

Dacă A și B sunt algebrelle peste inelul R , funcția $f: A \rightarrow B$ este un morfism de algebrelle dacă f este în același timp morfism de inele și de R -module.

Observație. Dacă R este inel comutativ și unitar, atunci un inel unitar A este o R -algebră dacă există un morfism unitar de inele $\varphi: R \rightarrow A$, astfel încât $x\varphi(a) = \varphi(a)x$, oricare ar fi $a \in R$ și $x \in A$.

Atunci putem considera A ca un R -modul, definind operația externă $R \times A \rightarrow A$, prin $(a, x) \mapsto \varphi(a)x$.

Exemple. 1) Inelul R are în mod evident o structură de R -algebră.

2) Multimea $\mathcal{M}_n(R)$ a matricelor împreună cu adunarea și înmulțirea matricelor este un inel unitar.

Mai mult, dacă definim o operație algebraică externă

$$R \times \mathcal{M}_n(R) \rightarrow \mathcal{M}_n(R)$$

prin $(a, (a_{ij})_{1 \leq i, j \leq n}) \mapsto (aa_{ij})_{1 \leq i, j \leq n}$, obținem pe $\mathcal{M}_n(R)$ o structură de R -algebră.

3) Multimea $R[X]$ a polinoamelor într-o nedeterminată împreună cu adunarea și înmulțirea matricelor este inel unitar.

Dacă luăm ca operație algebraică externă, înmulțirea obișnuită a polinoamelor cu elemente din R (vezi ex. 3)), obținem pe $R[X]$ o structură de R -algebră.

Vom construi un alt exemplu de algebră peste un inel comutativ R .

Dacă M este un R -modul, multimea $\text{Hom}_R(M, M)$ o vom nota cu $\text{End}_R M$ și o vom numi multimea endomorfismelor modulului M . Deci

$$\text{End}_R M = \{f: M \rightarrow M \mid f \text{ morfism}\}.$$

Dacă $f, g \in \text{End}_R M$, compunerea gof este tot un morfism de la M la M . Definim operația de înmulțire a morfismelor prin operația de compunere.

Față de adunarea și înmulțirea morfismelor, multimea $\text{End}_R M$ devine un inel unitar, în general necomutativ, și dacă, în plus, considerăm și înmulțirea morfismelor cu scalari din R , $\text{End}_R M$ devine o R -algebră.

Verificarea condițiilor care trebuie indeplinite se face ușor și o omitem.

§ 2. MODUL FACTOR. TEOREME DE IZOMORFISM PENTRU MODULE

Fie R un inel unitar. Ca și în paragraful precedent R -modulele considerate vor fi R -module la stînga.

Fie M un R -modul și $N \subset M$ un submodul al său. Atunci N este un subgrup al grupului aditiv subiacent lui M și prin urmare putem considera grupul factor M/N . Amintim că relația de congruență definită pe M în raport cu subgrupul N este dată prin

$$x \sim y \pmod{N} \text{ dacă și numai dacă } x - y \in N.$$

Clasa de echivalență a lui $x \in M$ este $\hat{x} = x + N = \{x + z \mid z \in N\}$, iar operația algebrică prin care M/N devine grup abelian este dată de $\hat{x} + \hat{y} = \widehat{x+y}$, oricare ar fi $\hat{x}, \hat{y} \in M/N$.

Pe grupul aditiv M/N definim o operație externă, înmulțirea cu scalari din R , dată prin

$$a\hat{x} = \widehat{ax}, \text{ oricare ar fi } a \in R \text{ și } \hat{x} \in M/N.$$

Să demonstrăm că această operație este bine definită.

Într-adevăr, dacă $\hat{x} = \hat{x}'$, atunci $x - x' \in N$ și $a(x - x') \in N$ sau $ax - ax' \in N$, adică $ax \equiv ax' \pmod{N}$ și deci $\widehat{ax} = \widehat{ax'}$.

Propoziția 2.1. *Mulțimea factor M/N împreună cu operațiile de adunare și înmulțire cu scalari definite mai înainte formează un R -modul. Mai mult, funcția surjectivă $p: M \rightarrow M/N$, $p(x) = \hat{x}$ este un morfism de module.*

Demonstrație. Am menționat deja că M/N împreună cu adunarea este un grup abelian. În plus, înmulțirea cu scalari are proprietățile:

$$1^\circ \quad a(\hat{x} + \hat{y}) = a\hat{x} + a\hat{y},$$

$$2^\circ \quad (a+b)\hat{x} = a\hat{x} + b\hat{x},$$

$$3^\circ \quad (ab)\hat{x} = a(b\hat{x}),$$

$$4^\circ \quad 1\hat{x} = \hat{x},$$

oricare ar fi $a, b \in R$ și $\hat{x}, \hat{y} \in M/N$.

Verificarea acestora se face ușor, bazându-se pe proprietățile analoage ale operațiilor din R -modulul M .

De exemplu, $a(\hat{x} + \hat{y}) = a\widehat{x+y} = a(\widehat{x+y}) = a\widehat{x} + a\widehat{y} = \widehat{ax} + \widehat{ay} = a\hat{x} + a\hat{y}$.

Funcția $p: M \rightarrow M/N$ este un morfism de grupuri și, în plus,

$$p(ax) = \widehat{ax} = a\hat{x} = ap(x),$$

adică p este un morfism de module.

Modulul M/N se numește *modulul factor* al lui M prin submodulul N .

Dacă $N = M$, atunci M/N este modulul nul și reciproc.

Observăm că $\text{Ker } p = p^{-1}(\{\hat{0}\}) = N$. Reciproc, am văzut că nucleul oricărui morfism de module definit pe M este un submodul al lui M . Deci, o submulțime nevidă a unui R -modul M este un submodul al său dacă și numai dacă este nucleul unui anumit morfism de module definit pe M .

Pentru un morfism de module $f: M \rightarrow M'$, notăm coim $f = M/\text{Ker } f$ și coker $f = M'/\text{Im } f$.

Propoziția 2.2. Fie $f: M \rightarrow M'$ un morfism de R -module. Următoarele afirmații sunt echivalente:

1) f este monomorfism;

2) $\text{Ker } f = \{0\}$;

3) Oricare ar fi R -modulul P și morfismele $u: P \rightarrow M$ și $v: P \rightarrow M'$ astfel încât $f \circ u = f \circ v$, atunci $u = v$.

Demonstrație. Echivalența $1) \Leftrightarrow 2)$ se deduce din cea corespunzătoare de la grupuri.

$1) \Rightarrow 3)$ Dacă $u: P \rightarrow M$ și $v: P \rightarrow M'$ sunt morfisme astfel încât $f \circ u = f \circ v$, atunci oricare ar fi $x \in P$, $(f \circ u)(x) = (f \circ v)(x)$ sau $f(u(x)) = f(v(x))$. Cum f este funcție injectivă, atunci $u(x) = v(x)$, oricare ar fi $x \in P$, adică $u = v$.

$3) \Rightarrow 2)$. Să presupunem prin absurd că $\text{Ker } f \neq \{0\}$ și fie morfismele $\theta: \text{Ker } f \rightarrow M$, $\theta(\hat{x}) = 0$ și $i: \text{Ker } f \rightarrow M$, $i(\hat{x}) = \hat{x}$, adică morfismul nul și morfismul incluziune. Avem $f \circ \theta = f \circ i$. Într-adevăr, dacă $x \in \text{Ker } f$, $(f \circ \theta)(x) = f(\theta(x)) = f(0) = 0$ și $(f \circ i)(x) = f(i(x)) = f(x) = 0$. Deci $\theta = i$, ceea ce contrazice faptul că $\text{Ker } f \neq \{0\}$.

Propoziția 2.3. Fie $f: M \rightarrow M'$ un morfism de R -module. Următoarele afirmații sunt echivalente:

1) este epimorfism;

2) $\text{coker } f = \{\hat{0}\}$;

3) Oricare ar fi R -modulul Q și morfismele $u: M' \rightarrow Q$ și $v: M' \rightarrow Q$ astfel încât $u \circ f = v \circ f$, atunci $u = v$.

Demonstrație. $1) \Leftrightarrow 2)$ Această echivalență este evidentă.

$1) \Rightarrow 3)$. Fie $u: M' \rightarrow Q$ și $v: M' \rightarrow Q$ morfisme astfel încât $u \circ f = v \circ f$. Dacă $y \in M'$ este un element oarecare, există $x \in M$ astfel încât $f(x) = y$. Atunci $u(y) = u(f(x)) = (u \circ f)(x) = (v \circ f)(x) = v(f(x)) = v(y)$, de unde $u = v$.

$3) \Rightarrow 2)$. Să presupunem prin absurd că $\text{coker } f \neq \{\hat{0}\}$ și fie morfismele $\theta: M' \rightarrow \text{coker } f$, $\theta(\hat{y}) = \hat{0}$ și $p: M' \rightarrow \text{coker } f$, $p(y) = \hat{y}$. Avem $\theta \circ f = p \circ f$. Într-adevăr, dacă $x \in M'$ atunci $(\theta \circ f)(x) = \theta(f(x)) = \hat{0}$ și $(p \circ f)(x) = p(f(x)) = \hat{f}(x) = \hat{0}$. Deci $\theta = p$, ceea ce contrazice faptul că $\text{coker } f \neq \{\hat{0}\}$.

Rezultatele de la grupuri privind corespondența submodulelor prin morfisme de module ea și teoremele de izomorfism se transpun în mod cu totul analog la module. De aceea ne vom opri doar la unele dintre acestea.

Teorema 2.4. (Teorema fundamentală de izomorfism). *Fie $f: M \rightarrow N$ un morfism de R -module. Atunci există un unic izomorfism de R -module:*

$$\varphi: M/\text{Ker } f \xrightarrow{\sim} \text{Im } f$$

astfel încât $f = \varphi \circ q$, unde q este morfismul canonice de la M la $M/\text{Ker } f$.

Demonstrație. Considerind structurile de grup aditiv subiacente modulelor M și N , din teorema fundamentală de izomorfism pentru grupuri (vezi cap. I, teorema 3.5.1) rezultă că $\varphi: M/\text{Ker } f \rightarrow \text{Im } f$, $\varphi(\hat{x}) = f(x)$, este un izomorfism între grupurile abeliene subiacente. În plus, φ este unic cu proprietatea că $f = \varphi \circ q$. Dacă $a \in R$ și $\hat{x} \in M/\text{Ker } f$, atunci $\varphi(a\hat{x}) = \varphi(\hat{ax}) = f(ax) = af(x) = a\varphi(\hat{x})$ adică este morfism de R -module, și cu aceasta demonstrația este terminată.

Corolarul 2.5. (Teorema I-a de izomorfism). *Fie M un R -modul și N, P submodule ale sale astfel încât $N \subset P$. Atunci P/N este un submodul al lui M/N și există un izomorfism de module*

$$\varphi: \frac{M/N}{P/N} \xrightarrow{\sim} M/P.$$

Demonstrație. Considerind grupurile additive subiacente modulelor precedente, de la grupuri știm că funcția $\psi: M/N \rightarrow M/P$, $\psi(\hat{x}) = \hat{x}$, este un morfism surjectiv de grupuri și $\text{Ker } \psi = P/N$.

Mai mult, ψ este un morfism de module. Într-adevăr, dacă $a \in R$ și $\hat{x} \in M/N$, atunci $\psi(a\hat{x}) = \psi(\hat{ax}) = \overline{ax} = a\hat{x} = a\psi(\hat{x})$. Deci $\text{Ker } \psi = P/N$ este un submodul al lui M/N și cum ψ este surjectiv, adică $\text{Im } \psi = M/P$, totul rezultă din teorema precedentă.

Corolarul 2.6. (Teorema a II-a de izomorfism). *Dacă M este un R -modul, N și P submodule ale sale, atunci există un izomorfism de module*

$$\varphi: N + P/N \xrightarrow{\sim} P/N \cap P.$$

Demonstrație. Funcția $\psi: P \rightarrow N + P/N$, $\psi(x) = \hat{x}$, este un morfism de module. Mai mult, deoarece ψ este surjectiv, iar $\text{Ker } \psi = N \cap P$, totul rezultă din teorema fundamentală de izomorfism.

§ 3. MODULE LIBERE

În acest paragraf vom considera module la stînga peste un inel unitar R . Fie M un R -modul și $S \subset M$ o submulțime a sa. Spunem că S este o mulțime de generatori pentru M sau că S formează un sistem

de generatori al lui M dacă $\langle S \rangle = M$, unde prin $\langle S \rangle$ am notat submodulul lui M generat de S .

Orice modul M admite cel puțin un sistem de generatori, de exemplu $S = M$.

Dacă M admite o mulțime finită de generatori spunem că este *modul finit general sau de tip finit*.

Fie $\{x_1, x_2, \dots, x_n\}$ o mulțime de elemente ale unui R -modul M . Spunem că mulțimea $\{x_1, x_2, \dots, x_n\}$ este *liniar independentă* sau că formează un *sistem liniar independent* al lui M dacă din orice relație de forma

$$a_1x_1 + a_2x_2 + \dots + a_nx_n = 0, \text{ cu } a_i \in R,$$

rezultă că $a_i = 0$, oricare ar fi $i = 1, 2, \dots, n$.

În caz contrar, dacă există elementele $a_1, a_2, \dots, a_n \in R$, nu toate nule, astfel încât $a_1x_1 + a_2x_2 + \dots + a_nx_n = 0$ spunem că x_1, x_2, \dots, x_n este un *sistem liniar dependent* al lui M . O familie arbitrară $X = (x_i)_{i \in I}$ de elemente ale lui M spunem că este *liniar independentă* sau că formează un *sistem liniar independent* al lui M dacă orice parte finită a sa este liniar independentă. În caz contrar, dacă există cel puțin o parte finită a sa liniar dependentă spunem că familia X este *liniar dependentă* sau că formează un *sistem liniar dependent* al lui M .

Dacă $(x_i)_{i \in I}$ este o familie de elemente ale unui R -modul M , atunci mulțimea

$$\text{supp}(x_i)_{i \in I} = \{i \in I \mid x_i \neq 0\}$$

se numește *suportul* familiei $(x_i)_{i \in I}$.

Familia $(x_i)_{i \in I}$ se numește de *suport finit* dacă $\text{supp}(x_i)_{i \in I}$ este o mulțime finită și scriem $|\text{supp}(x_i)_{i \in I}| < \infty$.

Având în vedere cele precedente, familia $X = (x_i)_{i \in I}$ de elemente ale R -modulului M este liniar independentă dacă oricare ar fi familia $(a_i)_{i \in I}$ de elemente ale lui R , de suport finit, astfel încât $\sum_{i \in I} a_i x_i = 0$ rezultă $a_i = 0$, oricare ar fi $i \in I$.

Spunem că un element $x \in M$ este o *combinație liniară* cu coeficienți în R de familia $(x_i)_{i \in I}$ de elemente din M , dacă există o familie de suport finit $(a_i)_{i \in I}$ de elemente din R astfel încât $x = \sum_{i \in I} a_i x_i$.

Este clar că o familie $(x_i)_{i \in I}$ de elemente din M formează un sistem de generatori al lui M dacă oricare element din M este o combinație liniară cu coeficienți în R de această familie.

Definiția 3.1. O familie $B = (e_i)_{i \in I}$ de elemente ale unui R -modul M se numește *bază* dacă, B formează totodată un sistem de generatori și un sistem liniar independent al lui M . Un modul care admite cel puțin o bază se numește *modul liber*.

Exemplu. 1) Fie M un R -modul și X o familie de elemente din M care conține pe 0. Deoarece $1 \cdot 0 = 0$, rezultă că X formează un sistem liniar dependent al lui M .

2) Dacă V este un K -spațiu vectorial și $x \in V$, atunci $\{x\}$ este sistem liniar independent dacă și numai dacă $x \neq 0$.

Într-adevăr, dacă $\{x\}$ este sistem liniar independent din ex. 3) avem $x \neq 0$. Reciproc, fie $x \neq 0$ și $ax = 0$ cu $a \in K$. Dacă presupunem că $a \neq 0$, atunci există $a^{-1} \in K$ și $a^{-1}(ax) = a^{-1}0$, de unde $x = 0$, contradicție.

3) Fie grupul aditiv \mathbb{Z}_n al claselor de resturi modulo n cu structura de \mathbb{Z} -modul. Dacă $\hat{x} \in \mathbb{Z}_n$, atunci $n\hat{x} = \hat{0}$ și deci orice sistem de elemente al lui \mathbb{Z}_n este liniar dependent.

4) Dacă R este un inel unitar, atunci $\{1\}$ formează o bază a R -modulului R .

5) Fie R -modulul $R_n[X]$ al polinoamelor de grad $\leq n$, cu coeficienți în inelul R . Multimea polinoamelor: $1, X, X^2, \dots, X^n$ formează o bază a sa.

De asemenea, multimea: $1, X, X^2, \dots, X^n, \dots$ este o bază a R -modulului $R[X]$ al tuturor polinoamelor.

Considerăm R -modulul $R^I = \{f \mid f: I \rightarrow R\}$ (vezi ex. 4).

Dacă $f \in R^I$, atunci suportul lui f , pe care-l notăm $\text{supp}(f)$, este prin definiție $\text{supp}(f(i))_{i \in I}$. Deci

$$\text{supp}(f) = \{i \in I \mid f(i) \neq 0\}.$$

Spunem că f este *suport finit* dacă familia $(f(i))_{i \in I}$ este de suport finit și scriem $|\text{supp}(f)| < \infty$.

Observăm că, dacă $f, g \in R^I$ și $a \in R$, atunci

$$1^\circ \text{ supp}(f+g) \subset \text{supp}(f) \cup \text{supp}(g);$$

$$2^\circ \text{ supp}(af) \subset \text{supp}(f).$$

Într-adevăr, dacă $i \in \text{supp}(f+g)$, atunci $(f+g)(i) \neq 0$ sau $f(i) + g(i) \neq 0$, de unde $f(i) \neq 0$ sau $g(i) \neq 0$ și deci $i \in \text{supp}(f)$ sau $i \in \text{supp}(g)$. Prin urmare $i \in \text{supp}(f) \cup \text{supp}(g)$, adică proprietatea 1°. A doua proprietate este clară.

Propoziția 3.2. Fie R un inel unitar și $I \neq \emptyset$ o mulțime nevidă oarecare. Atunci există un R -modul liber având o bază indexată după mulțimea I .

Demonstrație. Considerăm $R^I = \{f \mid f: I \rightarrow R\}$ și fie $R^{(I)} = \{f \mid f: I \rightarrow R, |\text{supp}(f)| < \infty\}$. Înțînd seamă de proprietățile precedente 1° și 2°, rezultă că dacă $f, g \in R^{(I)}$ și $a \in R$, atunci $f+g, af \in R^{(I)}$. Prin urmare $R^{(I)}$ este un submodul al R -modulului R^I și deci este la rîndul său un R -modul. Pentru fiecare $i \in I$, fie $e_i \in R^{(I)}$, definită prin $e_i(j) =$

$$= \begin{cases} 1 & \text{dacă } j=i, \\ 0 & \text{dacă } j \neq i. \end{cases}$$

Vom arăta că $(e_i)_{i \in I}$ este o bază pentru $R^{(I)}$.

Dacă $f \in R^{(I)}$, atunci familia $(f(i))_{i \in I}$ este de suport finit și $f = \sum_{i \in I} f(i)e_i$. Într-adevăr, pentru orice $j \in I$, $(\sum_{i \in I} f(i)e_i)(j) = \sum_{i \in I} f(i)e_i(j) = f(j)$.

Avem că f este o combinație liniară cu coeficienți în R de familia $(e_i)_{i \in I}$ și deci $(e_i)_{i \in I}$ este un sistem de generatori al lui $R^{(I)}$. Fie acum $(a_i)_{i \in I}$ o familie de suport finit de elemente ale lui R , astfel încât $\sum_{i \in I} a_i e_i = 0$.

Atunci pentru orice $j \in I$ avem $(\sum_{i \in I} a_i e_i)(j) = 0(j)$ sau $\sum_{i \in I} a_i e_i(j) = 0$, de unde $a_j = 0$. Deci sistemul de generatori $(e_i)_{i \in I}$ este și liniar independent, adică este o bază a lui $R^{(I)}$. Această bază se numește *baza canonica* a lui $R^{(I)}$.

În particular, dacă I este o mulțime finită, atunci $R^{(I)} = R^I$. Pentru $N = \{1, 2, \dots, n\}$, unde $n \geq 1$ este un număr natural, obținem un R -modul pe care-l vom nota cu R^n . Avem că

$$R^n = \{(a_1, a_2, \dots, a_n) \mid a_i \in R, 1 \leq i \leq n\}$$

este un R -modul liber, o bază a sa fiind mulțimea $(e_i)_{1 \leq i \leq n}$, unde $e_i = (0, \dots, 0, 1, 0, \dots, 0)$ pentru orice $1 \leq i \leq n$.

⁽⁶⁾ Dacă $M = \{1, 2, \dots, m\}$ și $N = \{1, 2, \dots, n\}$, unde $m, n \geq 1$ sunt numere naturale, $R^{(M \times N)}$ este R -modulul $\mathcal{M}(m, n, R)$. Avem că $\mathcal{M}(m, n, R)$ este un R -modul liber, o bază a sa fiind mulțimea de matrice $(e_{ij})_{1 \leq i \leq m, 1 \leq j \leq n}$, unde e_{ij} este matricea care are 1 pe poziția (i, j) și 0 în rest.

Lema 3.3. Fie L un R -modul liber și $B = (e_i)_{i \in I}$ o familie de elemente ale lui L . Atunci B este o bază dacă și numai dacă

1) B este un sistem de generatori al lui L ;

2) Oricare $x \in L$ se scrie în mod unic ca o combinație liniară cu coeficienți în R de familia $(e_i)_{i \in I}$.

Demonstrație. Să presupunem mai întii că B este bază a lui L . Atunci B este sistem de generatori al lui L . Dacă $x \in L$, atunci există o familie $(a_i)_{i \in I}$ de elemente din R de suport finit astfel încât $x = \sum_{i \in I} a_i e_i$.

Mai mult, dacă $(b_i)_{i \in I}$ este o altă familie de suport finit astfel încât $x = \sum_{i \in I} b_i e_i$, atunci $\sum_{i \in I} a_i e_i = \sum_{i \in I} b_i e_i$ sau $\sum_{i \in I} (a_i - b_i) e_i = 0$. Deoarece $(e_i)_{i \in I}$ este un sistem liniar independent, atunci $a_i - b_i = 0$ și deci $a_i = b_i$, oricare ar fi $i \in I$.

Reciproc, dacă B verifică condițiile 1) și 2), rămîne să arătăm că B este un sistem liniar independent. Într-adevăr, fie $(a_i)_{i \in I}$ o familie de elemente din R de suport finit astfel încât $\sum_{i \in I} a_i e_i = 0$. Deoarece $\sum_{i \in I} 0 e_i = 0$, condiția 2) ne dă $a_i = 0$, oricare ar fi $i \in I$.

Vom da acum o proprietate importantă a modulelor libere numită *proprietatea de universalitate*.

Teorema 3.4. Fie L un R -modul liber de bază $B = (e_i)_{i \in I}$. Atunci oricare ar fi modulul M și oricare ar fi familia $(x_i)_{i \in I}$ de elemente din M , există un unic morfism de module $\varphi: L \rightarrow M$ astfel încât $\varphi(e_i) = x_i$ pentru orice $i \in I$. Mai mult, φ este injectivă (respectiv surjectivă, bijectivă) dacă și numai dacă $(x_i)_{i \in I}$ este un sistem liniar independent (respectiv sistem de generatori, bază).

Demonstrație. Dacă $x \in L$, există o unică familie $(a_i)_{i \in I}$ de elemente din R de suport finit astfel încât $x = \sum_{i \in I} a_i e_i$. Definim $\varphi(x) = \sum_{i \in I} a_i x_i$. Este clar că φ este bine definită și vom demonstra că φ este morfism de module. Dacă $x' \in L$, există o unică familie $(a'_i)_{i \in I}$ de elemente din R de suport finit astfel încât $x' = \sum_{i \in I} a'_i e_i$.

Atunci $x + x' = \sum_{i \in I} (a_i + a'_i) e_i$ și deci

$$\varphi(x + x') = \sum_{i \in I} (a_i + a'_i) x_i = \sum_{i \in I} a_i x_i + \sum_{i \in I} a'_i x_i = \varphi(x) + \varphi(x').$$

Dacă $a \in R$, atunci $ax = \sum_{i \in I} (aa_i) e_i$ și deci $\varphi(ax) = \sum_{i \in I} (aa_i) x_i = a \sum_{i \in I} a_i x_i = a\varphi(x)$. Deci φ este morfism de R -module. Să demonstrează unicitatea lui φ . Într-adevăr, fie $\psi: L \rightarrow M$ un morfism de module astfel încât $\psi(e_i) = x_i$, pentru orice $i \in I$. Pentru $x \in L$, $x = \sum_{i \in I} a_i e_i$ avem $\psi(x) = \psi(\sum_{i \in I} a_i e_i) = \sum_{i \in I} a_i \psi(e_i) = \sum_{i \in I} a_i x_i = \varphi(\sum_{i \in I} a_i e_i) = \varphi(x)$ și deci $\psi = \varphi$.

Să presupunem acum că φ este injectivă și fie $(a_i)_{i \in I}$ o familie de elemente din R de suport finit astfel încât $\sum_{i \in I} a_i x_i = 0$. Deoarece $x_i = \varphi(e_i)$, pentru orice $i \in I$, avem $0 = \sum_{i \in I} a_i \varphi(e_i) = \varphi(\sum_{i \in I} a_i e_i)$ și cum φ este injectivă, obținem că $\sum_{i \in I} a_i e_i = 0$, de unde $a_i = 0$, pentru orice $i \in I$. Deci $(x_i)_{i \in I}$ este un sistem liniar independent. Reciproc, fie $x \in L$ astfel încât $\varphi(x) = 0$. Dacă $x = \sum_{i \in I} a_i e_i$, unde $(a_i)_{i \in I}$ este o familie de elemente din R de suport finit, atunci $\sum_{i \in I} a_i \varphi(e_i) = 0$, adică $\sum_{i \in I} a_i x_i = 0$. Deoarece $(x_i)_{i \in I}$ este un sistem de elemente din M liniar independent, atunci $a_i = 0$ pentru orice $i \in I$ și deci $x = 0$. Prin urmare φ este injectivă.

Fie acum φ surjectivă. Pentru $y \in M$ există $x \in L$ astfel încât $\varphi(x) = y$. Deoarece $x = \sum_{i \in I} a_i e_i$, unde $(a_i)_{i \in I}$ este o familie de suport finit de elemente din R , atunci

$$y = \varphi(x) = \varphi(\sum_{i \in I} a_i e_i) = \sum_{i \in I} a_i \varphi(e_i) = \sum_{i \in I} a_i x_i.$$

Prin urmare $(x_i)_{i \in I}$ este un sistem de generatori al lui M . Reciproc, fie $(x_i)_{i \in I}$ un sistem de generatori al lui M . Dacă $y \in M$, există o familie $(a_i)_{i \in I}$ de elemente din R de suport finit astfel încât $y = \sum_{i \in I} a_i x_i$. Atunci

$y = \sum_{i \in I} a_i \varphi(e_i) = \varphi(\sum_{i \in I} a_i e_i)$, unde $\sum_{i \in I} a_i e_i \in L$. Deci φ este surjectivă. Din cele precedente rezultă că φ este bijectivă dacă și numai dacă $(x_i)_{i \in I}$ este bază.

Corolarul 3.5. Fie M un R -modul. Atunci există un R -modul liber L și un submodul K al lui L astfel încât $M \cong L/K$.

Demonstrație. Fie $S = (x_i)_{i \in I}$ un sistem de generatori al lui M . Considerăm modulul liber $L = R^{(I)}$ și fie $(e_i)_{i \in I}$ baza sa canonică. Conform teoremei precedente există un unic morfism $\varphi: R^{(I)} \rightarrow M$, $\varphi(e_i) = x_i$ pentru orice $i \in I$, care este surjectiv, și din teorema fundamentală de izomorfism $M \cong L/K$, unde $K = \text{Ker } \varphi$.

Corolarul 3.6. Dacă L este un R -modul liber, există o mulțime I astfel încât $L \cong R^{(I)}$.

Demonstrație. Fie $(x_i)_{i \in I}$ o bază a R -modulului liber L . Dacă $R^{(I)}$ este modulul liber cu baza canonică $(e_i)_{i \in I}$, conform teoremei precedente există un unic morfism $\varphi: R^{(I)} \rightarrow L$, $\varphi(e_i) = x_i$ pentru orice $i \in I$, care în plus este un izomorfism.

În particular, dacă R -modulul liber L are o bază finită $\{e_1, e_2, \dots, e_n\}$, atunci L este izomorf cu R^n .

Corolarul 3.7. Fie L și L' două R -module libere, fiecare având cile o bază indexată după aceeași mulțime de indici I . Atunci $L \cong L'$.

Demonstrație. Avem că $L \cong R^{(I)}$ și $L' \cong R^{(I)}$, de unde $L \cong L'$.

Următorul rezultat ne va arăta că spațiile vectoriale peste un corp K sunt K -module libere.

Teorema 3.8. (Teorema bazei). Fie V un K -spațiu vectorial nenul, $X \subset V$ un sistem de vectori liniar independent și $S \subset V$ un sistem de generatori al lui V astfel încât $X \subset S$. Atunci există o bază B a lui V astfel încât $X \subset B \subset S$.

Demonstrație. Fie \mathcal{P} mulțimea tuturor sistemelor de vectori liniar independente incluse în S . Deoarece X aparține lui \mathcal{P} avem că $\mathcal{P} \neq \emptyset$. Arătăm că \mathcal{P} , ordonată cu inclusiunea, este inductivă. Într-adevăr, dacă $\{B_i\}_{i \in I}$ este o submulțime total ordonată a lui \mathcal{P} , să considerăm $E = \bigcup_{i \in I} B_i$. Evident avem că $X \subset E \subset S$. Vom demonstra că E este sistem liniar independent, adică orice submulțime finită a sa formează un sistem liniar independent. Să presupunem prin absurd că există $e_1, e_2, \dots, e_n \in E$ și $a_1, a_2, \dots, a_n \in R$, nu toți nuli, astfel încât $\sum_{i=1}^n a_i e_i = 0$. Dacă

$x_k \in B_{t_k}$, $1 \leq k \leq n$, deoarece $\{B_t\}_{t \in I}$ este total ordonată, există B_{t_r} , $1 \leq r \leq n$, astfel încit $B_{t_k} \subset B_{t_r}$, oricare ar fi $k=1, 2, \dots, n$. Deci $\{x_1, x_2, \dots, x_n\}$ este o submulțime a lui B_{t_r} care formează un sistem de vectori liniar dependent, ceea ce contrazice faptul că B_{t_r} este sistem liniar independent. Deci E aparține lui \mathcal{P} și cum $B_i \subset E$, oricare ar fi $i \in I$, rezultă că E este un majorant al familiei $\{B_i\}_{i \in I}$. După lema lui Zorn, \mathcal{P} are cel puțin un element maximal.

Dacă B este un astfel de element maximal vom arăta că B este o bază. Într-adevăr, deoarece B aparține lui \mathcal{P} , rezultă că formează un sistem liniar independent. Să arătăm că B este sistem de generatori. Fie $x \in S$ și să presupunem că $x \notin B$. Atunci $B \not\subseteq B \cup \{x\} \subset S$ și cum B este maximal rezultă că $B \cup \{x\}$ este un sistem liniar dependent. Deci există $x_1, x_2, \dots, x_n \in B$ și elementele a_1, a_2, \dots, a_n , $a \in K$, nu toate nule, astfel încit $a_1x_1 + a_2x_2 + \dots + a_nx_n + ax = 0$. Deoarece B este sistem liniar independent avem că $a \neq 0$ și deci $x = (-a^{-1}a_1)x_1 + (-a^{-1}a_2)x_2 + \dots + (-a^{-1}a_n)x_n$. Prin urmare, $x \in \langle B \rangle$ adică $S \subset \langle B \rangle$, de unde $V = \langle S \rangle \subset \langle B \rangle \subset V$. Deci $V = \langle B \rangle$ adică B este un sistem de generatori al lui V .

Corolarul 3.9. Fie V un K -spațiu vectorial nenul. Atunci orice sistem de vectori liniar independent $X \subset V$ poate fi completat pînă la o bază a lui V .

Demonstrație. Luăm în teorema precedentă $S = V$ și totul rezultă.

Corolarul 3.10. Fie V un K -spațiu vectorial nenul. Atunci, din orice sistem de generatori $S \subset V$, se poate extrage o bază.

Demonstrație. Fie $x \neq 0$, $x \in S$. Luăm în teorema precedentă $X = \{x\}$ și totul rezultă.

Aplicație. Fie K un corp comutativ cu un număr finit n de elemente. Atunci există p și k , p număr prim, astfel încit $n = p^k$.

Într-adevăr, fie $P \subset K$ subcorpul său prim. Cum K este finit rezultă că P este finit și deci există p număr prim, astfel încit $P \cong \mathbb{Z}_p$. În mod clar K este P -spațiu vectorial, înmulțirea cu scalari din P fiind dată de înmulțirea din K . Deci K are o bază, evident finită, $\{e_1, e_2, \dots, e_k\}$ și atunci $K \cong P^k$. Prin urmare $n = \text{card } K = \text{card } P^k = \text{card } \mathbb{Z}_p^k = p^k$.

§ 4. DIMENSIUNEA SPAȚIILOR VECTORIALE. RANGUL MODULELOR LIBERE

În acest paragraf corporile și inelele considerate sunt comutative.

Teorema 4.1. (Teorema schimbului). Fie V un K -spațiu vectorial, x_1, x_2, \dots, x_r un sistem liniar independent de vectori al lui V , iar y_1, y_2, \dots, y_n un sistem de generatori al lui V . Atunci :

1) $r \leq n$;

2) Există r vectori printre y_1, y_2, \dots, y_n , după o eventuală numărare, fie aceia y_1, y_2, \dots, y_r pe care înlocuindu-i cu x_1, x_2, \dots, x_r obținem că $x_1, x_2, \dots, x_r, y_{r+1}, \dots, y_n$ este de asemenea un sistem de generatori al lui V .

Demonstrație. Vom face demonstrația prin inducție după r . Fie $r=1$. Este evident că $1 \leq r$. Cum $V=\langle y_1, y_2, \dots, y_n \rangle$ și $x_1 \in V$, există $a_1, a_2, \dots, a_n \in K$ astfel încât $x_1 = a_1 y_1 + a_2 y_2 + \dots + a_n y_n$. Dar $x_1 \neq 0$ și deci cel puțin unul dintre coeficienții a_1, a_2, \dots, a_n este nenul. Prinț-o eventuală renumerotare a vectorilor y_1, y_2, \dots, y_n putem presupune că $a_1 \neq 0$. Atunci

$$y_1 = a_1^{-1} x_1 + (-a_1^{-1} a_2) y_2 + \dots + (-a_1^{-1} a_n) y_n$$

și deci $y_1 \in \langle x_1, y_2, \dots, y_n \rangle$. Dar evident $y_2, \dots, y_n \in \langle x_1, y_2, \dots, y_n \rangle$, de unde $\langle y_1, y_2, \dots, y_n \rangle \subset \langle x_1, y_2, \dots, y_n \rangle$ și deci $V=\langle x_1, y_2, \dots, y_n \rangle$, adică x_1, y_2, \dots, y_n este un sistem de generatori al lui V .

Să presupunem acum că teorema este adeverată pentru cazul cind avem de-a face cu un sistem liniar independent format din $r-1$ vectori și să demonstrăm pentru sistemele x_1, x_2, \dots, x_r și y_1, y_2, \dots, y_n .

Deoarece x_1, x_2, \dots, x_r este sistem liniar independent, atunci x_1, x_2, \dots, x_{r-1} formează un sistem liniar independent. Conform ipotezei inducțive avem $r-1 \leq n$ și după o eventuală renumerotare a vectorilor y_1, y_2, \dots, y_n avem $V=\langle x_1, \dots, x_{r-1}, y_r, \dots, y_n \rangle$.

Într-adevăr, dacă am avea $r-1=n$, atunci x_1, x_2, \dots, x_{r-1} constituie un sistem de generatori al lui V și deci există $a_1, a_2, \dots, a_{r-1} \in K$ astfel încât $x_r = a_1 x_1 + a_2 x_2 + \dots + a_{r-1} x_{r-1}$. Atunci $a_1 x_1 + \dots + a_{r-1} x_{r-1} + (-1)x_r = 0$, unde $-1 \neq 0$, ceea ce contrazice faptul că x_1, x_2, \dots, x_r este un sistem liniar independent.

Deci neapărat $r-1 < n$ și atunci $r < n$.

Deoarece $\langle x_1, x_2, \dots, x_{r-1}, y_r, \dots, y_n \rangle = V$, există $a_1, \dots, a_{r-1}, b_r, \dots, b_n$ astfel încât $x_r = a_1 x_1 + \dots + a_{r-1} x_{r-1} + b_r y_r + \dots + b_n y_n$. Cum x_1, x_2, \dots, x_r este un sistem liniar independent, atunci cel puțin unul dintre coeficienții b_r, \dots, b_n este nenul. După o eventuală renumerotare putem presupune că $b_r \neq 0$ și atunci

$$\begin{aligned} y_r = & (-b_r^{-1} a_1) x_1 + \dots + (-b_r^{-1} a_{r-1}) x_{r-1} + b_r^{-1} x_r + (b_r^{-1} b_{r+1}) y_{r+1} + \\ & + \dots + (-b_r^{-1} b_n) y_n. \end{aligned}$$

Deci $y_r \in \langle x_1, x_2, \dots, x_r, y_{r+1}, \dots, y_n \rangle$ și cum în mod clar $y_{r+1}, \dots, y_n \in \langle x_1, x_2, \dots, x_r, y_{r+1}, \dots, y_n \rangle$ rezultă $\langle x_1, x_2, \dots, x_{r-1}, y_r, \dots, y_n \rangle \subseteq \langle x_1, x_2, \dots, x_r, y_{r+1}, \dots, y_n \rangle$ de unde $V=\langle x_1, x_2, \dots, x_r, y_{r+1}, \dots, y_n \rangle$. Deci $x_1, x_2, \dots, x_r, y_{r+1}, \dots, y_n$ este un sistem de generatori al lui V .

Corolarul 4.2. Dacă V este un K -spațiu vectorial nenul finit generat, atunci V are cel puțin o bază finită. Mai mult, orice altă bază este finită și toate bazele au același număr de elemente.

Demonstrație. Spațiul vectorial V , fiind finit generat, are un sistem finit de generatori S . Deoarece din S se poate extrage cel puțin o bază, rezultă că V are o bază finită $\{e_1, e_2, \dots, e_m\}$. Din teorema schimbului avem că orice sistem liniar independent al lui V are cel mult n vectori și deci orice altă bază a lui V este finită. Dacă $\{f_1, f_2, \dots, f_n\}$ este o altă bază a lui V , conform teoremei schimbului rezultă $n \leq m$ și $m \leq n$, adică $n = m$.

Teorema 4.3. Fie V un K -spațiu vectorial. Dacă $(e_i)_{i \in I}$ și $(f_j)_{j \in J}$ sunt două baze ale lui V , atunci I și J au același cardinal.

Demonstrație. După cum am arătat, dacă una dintre mulțimile I sau J este finită, atunci și cealaltă este finită și cele două mulțimi au același număr de elemente. Fie deci I și J mulțimi infinite. Deoarece $(f_j)_{j \in J}$ este bază, atunci pentru orice $i \in I$, există o unică familie $(a_j^i)_{j \in J}$ al cărei suport $J_i = \{j \in J \mid a_j^i \neq 0\}$ este o mulțime finită astfel încât $e_i = \sum_{j \in J} a_j^i f_j = \sum_{j \in J_i} a_j^i f_j$. Vom demonstra că $J = \bigcup_{i \in I} J_i$. Incluziunea $\bigcup_{i \in I} J_i \subset J$ fiind evidentă, să presupunem prin absurd că există un element $j_0 \in J$ și $j_0 \notin \bigcup_{i \in I} J_i$. Deoarece $(e_i)_{i \in I}$ este bază, există o unică familie de suport finit $(b_i^{j_0})_{i \in I}$ astfel încât $f_{j_0} = \sum_{i \in I} b_i^{j_0} e_i$.

Dacă presupunem că suportul familiei $(b_i^{j_0})_{i \in I}$ este $\{i_1, i_2, \dots, i_s\}$, atunci

$$f_{j_0} = b_{i_1} e_{i_1} + b_{i_2} e_{i_2} + \dots + b_{i_s} e_{i_s}.$$

Deci

$$f_{j_0} = b_{i_1} \sum_{j \in J_{i_1}} a_j^{i_1} f_j + b_{i_2} \sum_{j \in J_{i_2}} a_j^{i_2} f_j + \dots + b_{i_s} \sum_{j \in J_{i_s}} a_j^{i_s} f_j,$$

și cum $j_0 \notin \bigcup_{k=1}^s J_{i_k}$ rezultă că familia $\{f_j\} \cup (f_j)_{j \in \bigcup_{k=1}^s J_{i_k}}$ formează un sistem

de vectori liniar independent, ceea ce contrazice faptul că $(f_j)_{j \in J}$ este bază. Deci $J = \bigcup_{i \in I} J_i$ și atunci $\text{card } J = \text{card } (\bigcup_{i \in I} J_i) \leq \sum_{i \in I} \text{card } J_i$. Deoarece

$\text{card } J_i < \aleph_0$, atunci $\text{card } J \leq \aleph_0 \text{ card } I = \text{card } I$. Avem deci $\text{card } J \leq \text{card } I$ și analog $\text{card } I \leq \text{card } J$, de unde $\text{card } I = \text{card } J$.

Dacă V este un K -spațiu vectorial, numim *dimensiunea* lui V și vom nota $\dim_K V$, cardinalul unei baze arbitrară a lui V . Cele precedente ne arată că acest cardinal este același oricare ar fi baza lui V . Dacă $\dim_K V$ este finit, atunci spunem că V este spațiu vectorial de *dimensiune finită*. În caz contrar, spunem că V este de *dimensiune infinită*. Vom conveni ca dimensiunea spațiului nul să fie 0.

Observație. Conform corolarului 3.7 două spații vectoriale care au aceeași dimensiune sunt izomorfe, iar reciproca acestei afirmații rezultă din teorema 3.4.

Lema 4.4. Fie V un K -spațiu vectorial de dimensiune finită și $U \subset V$ un subspațiu al său.

Atunci spațiile U și V/U sunt de asemenea de dimensiune finită, mai precis $\dim_K U$ și $\dim_K V/U$ sunt mai mici sau egale cu $\dim_K V$.

Demonstrație. Fie $\{e_1, e_2, \dots, e_n\}$ o bază a lui V și $\{f_i\}_{i \in I}$ o bază a lui U . Dacă I ar fi infinită, atunci există un sistem liniar independent format din $n+1$ vectori și după teorema schimbului $n+1 \leq n$, contradicție. Astfel I este finită și deci U este de dimensiune finită. Mai mult, este clar că $\dim_K U \leq \dim_K V$. Fie acum $p: V \rightarrow V/U$, $p(x) = \hat{x}$, morfismul canonic. Multimea $\{\hat{e}_1, \hat{e}_2, \dots, \hat{e}_n\}$ este un sistem de generatori al lui V/U . Într-adevăr, fie $\hat{x} \in V/U$ și cum $\{e_1, e_2, \dots, e_n\}$ este o bază a lui V ,

atunci $x = \sum_{i=1}^n a_i e_i$. De aici obținem $\hat{x} = \sum_{i=1}^n a_i \hat{e}_i$. Din teorema schimbului rezultă că V/U are o bază finită și evident $\dim_K V/U \leq \dim_K V$.

Teorema 4.5. Fie V și V' două K -spații vectoriale de dimensiune finită, iar $f: V \rightarrow V'$ un morfism de spații vectoriale. Atunci $\text{Ker } f$ și $\text{Im } f$ sunt spații de dimensiune finită și

$$\dim_K(\text{Ker } f) + \dim_K(\text{Im } f) = \dim_K V.$$

Demonstrație. Din lema 4.4 rezultă că $\text{Ker } f$ și $\text{Im } f$ sunt spații vectoriale de dimensiune finită. Fie $B' = \{e_1, e_2, \dots, e_r\}$ o bază a lui $\text{Ker } f$. Sistemul liniar independent de vectori e_1, e_2, \dots, e_r poate fi completat pînă la o bază $B = \{e_1, e_2, \dots, e_r, e_{r+1}, \dots, e_n\}$ a lui V .

Vom demonstra că $B'' = \{f(e_{r+1}), \dots, f(e_n)\}$ este o bază a lui $\text{Im } f$. Într-adevăr, dacă $y \in \text{Im } f$, există $x \in V$ astfel încît $y = f(x)$. Dar

$$x = \sum_{i=1}^n a_i e_i \text{ și deci}$$

$$y = f\left(\sum_{i=1}^n a_i e_i\right) = f\left(\sum_{i=1}^r a_i e_i\right) + f\left(\sum_{i=r+1}^n a_i e_i\right).$$

Cum $\sum_{i=1}^r a_i e_i \in \text{Ker } f$, rezultă

$$y = f\left(\sum_{i=r+1}^n a_i e_i\right) = \sum_{i=r+1}^n a_i f(e_i).$$

Astfel am obținut că B'' este sistem de generatori. Fie acum $b_{r+1}, \dots, b_n \in K$, astfel încît $b_{r+1}f(e_{r+1}) + \dots + b_n f(e_n) = 0$.

A v e m deci $f\left(\sum_{i=r+1}^n b_i e_i\right) = 0$ sau $\sum_{i=r+1}^n b_i e_i \in \text{Ker } f$.

A tunci $\sum_{i=r+1}^n b_i e_i = \sum_{i=1}^r a_i e_i$ sau $(-a_1)e_1 + \dots + (-a_r)e_r + b_{r+1}e_{r+1} + \dots + b_n e_n = 0$.

Cum B este bază rezultă $-a_1 = \dots = -a_r = b_{r+1} = \dots = b_n = 0$ și deci B'' este sistem liniar independent. Deci B'' este bază a lui $\text{Im } f$.

A v e m $\dim_K(\text{Ker } f) = r$, $\dim_K V = n$ și $\dim_K(\text{Im } f) = n - r$, $r + (n - r) = n$, adică relația din enunț.

Corolarul 4.6. Fie V un K -spațiu vectorial de dimensiune finită și U un subspațiu al său. Atunci U și V/U sunt spații de dimensiune finită și

$$\dim_K U + \dim_K V/U = \dim_K V.$$

Demonstrație. Din lema 4.4 avem că U și V/U au dimensiune finită. Totul rezultă din teorema precedentă aplicată spațiilor vectoriale U , V/U și morfismului canonic $p: V \rightarrow V/U$, $p(x) = \bar{x}$.

Corolarul 4.7. Fie V un K -spațiu vectorial de dimensiune finită, iar U și W subspacele sale.

A tunci

$$\dim_K U + \dim_K W = \dim_K(U \cap W) + \dim_K(U + W).$$

Demonstrație. Din teorema a II-a de izomorfism avem că $U + W/U \cong W/U \cap W$ și deci $\dim_K U + W/U = \dim_K W/U \cap W$. Aplicăm apoi corolarul precedent.

Observație. Relațiile din enunțul teoremei 4.5 și corolarelor 4.6 și 4.7 au loc și pentru spațiile vectoriale de dimensiune infinită. Demonstrația acestora în acest caz se face complet analog numai că intervin operații cu cardinale.

Teorema 4.8. Fie R un inel comutativ și L un R -modul liber. Dacă $(e_i)_{i \in I}$ și $(f_j)_{j \in J}$ sunt două baze ale lui L , atunci I și J au același cardinal.

Demonstrație. Conform lemei lui Krull, există un ideal maximal \mathfrak{m} al lui R și fie corpul $K = R/\mathfrak{m}$.

Mulțimea

$$\mathfrak{m}L = \left\{ \sum_{i=1}^n a_i x_i \mid n \in \mathbb{N}, a_i \in \mathfrak{m}, x_i \in L, 1 \leq i \leq n \right\}$$

este un submodul al lui L și fie $\tilde{L} = L/\mathfrak{m}L$. Pe grupul aditiv subiacent R -modulului \tilde{L} definim o structură de K -spațiu vectorial. Dacă $\tilde{a} \in K$ și $\tilde{x} \in \tilde{L}$, punem prin definiție $\tilde{a}\tilde{x} = \tilde{ax}$. Să arătăm că aceasta este corectă definită. Într-adevăr, dacă $a = a'$ și $x = x'$, atunci $a - a' \in \mathfrak{m}$ și $x - x' \in \mathfrak{m}L$,

de unde $a = a' + b$ și $x = x' + y$ cu $b \in \underline{m}$ și $y \in \underline{m}L$. Avem $ax = (a' + b)(x' + y) = a'x' + bx' + a'y + by$, și cum $bx' + a'y + by \in \underline{m}L$, atunci $ax - a'x' \in \underline{m}L$, adică $\bar{ax} = \bar{a}'\bar{x}'$. Împreună cu această operație algebrică externă grupul abelian \bar{L} devine un *K-spațiu vectorial*. Verificarea condițiilor este imediată. Demonstrăm că $\bar{B} = (\bar{e}_i)_{i \in I}$ este o bază a *K-spațiului* \bar{L} . Dacă $\bar{x} \in \bar{L}$, atunci $x \in L$ se scrie ca o sumă finită $x = \sum_i a_i e_i$ cu $a_i \in R$ și deci $\bar{x} = \sum_i \bar{a}_i \bar{e}_i$ suma fiind finită. Rezultă că \bar{B} este un sistem de generatori al lui \bar{L} . Fie acum $\sum_j \hat{b}_j \hat{e}_j = \bar{0}$, unde $(\hat{b}_j)_{j \in J}$ este o familie de suport finit de elemente din K . Atunci $\sum_j \hat{b}_j e_j = \bar{0}$ de unde $\sum_j b_j e_j \in \underline{m}L$. Deci $\sum_j b_j e_j = -\sum_k a_k x_k$, unde $a_k \in \underline{m}$, $x_k \in L$, suma după k fiind finită. Cum $(e_i)_{i \in I}$ este bază a lui L , atunci $x_k = \sum_t c_t^k e_t$, unde $c_t^k \in R$, suma fiind finită. Deci $\sum_j b_j e_j = \sum_k a_k (\sum_t c_t^k e_t) = \sum_t (\sum_k a_k c_t^k) e_t$, de unde $b_j = \sum_k a_k c_j^k$, suma fiind finită. Deoarece $a_k \in \underline{m}$, pentru orice k , rezultă $b_j \in \underline{m}$, pentru orice j , adică $\hat{b}_j = \hat{0}$ pentru orice j . Deci \bar{B} formează un sistem liniar independent. Prin urmare \bar{B} este o bază a *K-spațiului* vectorial \bar{L} . La fel, $\bar{F} = (\bar{f}_j)_{j \in J}$ este o altă bază a aceluiași spațiu vectorial și conform teoremei precedente $\text{card } I = \text{card } J$.

Dacă R este un inel comutativ spunem că un R -modul liber L are *rang infinit* dacă admite o bază infinită. Dacă L are o bază finită spunem că este de *rang finit* iar numărul de elemente al unei baze, și deci al oricărei baze, se numește *rangul* R -modulului L și-l notăm cu $\text{rang}_R L$.

În cazul în care R este corp și deci L este spațiu vectorial, atunci $\text{rang}_R L = \dim_R L$.

Același raționament folosit mai înainte pentru spații vectoriale, ne arată că două R -module libere sunt izomorfe dacă și numai dacă au același rang.

Exemplu. 1) Dacă R este un inel comutativ, $\text{rang}_R R^n = n$, $\text{rang}_R \mathcal{M}(m, n, R) = mn$. În general, $\text{rang}_R R^{(I)} = \text{card } I$.

2) Cu notațiile din paragraful precedent, R fiind un inel comutativ, avem $\text{rang}_R R[X] = n+1$, iar $\text{rang}_R R[X] = \aleph_0$.

În cazul în care R este corp, cardinalele de la ex. 1) și 2) reprezintă toamai dimensiunile spațiilor vectoriale respective.

§ 5. SCHIMBAREA COORDONATELOR. MATRICEA ASOCIAȚĂ UNUI MORFISM DE MODULE LIBERE DE RANG FINIT

În acest paragraf, R va fi un inel comutativ și unitar. Fie L un R -modul liber de rang finit și $B = \{e_1, e_2, \dots, e_n\}$ o bază a sa. Dacă $x \in L$, atunci $x = a_1 e_1 + a_2 e_2 + \dots + a_n e_n$, unde $a_i \in R$, $i = 1, 2, \dots, n$. Elementele

a_1, a_2, \dots, a_n se numesc *coordonatele* elementului x în raport cu baza $\{e_1, e_2, \dots, e_n\}$. Lema 3.3 arată că într-o bază dată fiecare vector are coordonatele sale determinate în mod unic.

Fie L este un R -modul liber de rang n și $B = \{e_1, e_2, \dots, e_n\}$, $B' = \{e'_1, e'_2, \dots, e'_n\}$ două baze ale sale. Fiecare element al bazei B' se exprimă ca o combinație liniară de elementele bazei B . Să presupunem că formulele prin care elementele e_i , $1 \leq i \leq n$, se exprimă cu ajutorul elementelor primei baze sint următoarele:

$$e'_1 = u_{11}e_1 + u_{21}e_2 + \dots + u_{n1}e_n,$$

$$e_2' = u_{12}e_1 + u_{22}e_2 + \dots + u_{n2}e_n,$$

$$e'_n = u_{1n}e_1 + u_{2n}e_2 + \dots + u_{nn}e_n.$$

Astfel, s-a pus în evidență o matrice

$$U = \begin{pmatrix} u_{11} & u_{12} & \dots & u_{1n} \\ u_{21} & u_{22} & \dots & u_{2n} \\ \dots & \dots & \dots & \dots \\ u_{n1} & u_{n2} & \dots & u_{nn} \end{pmatrix}$$

numită *matricea de trecere* de la baza B la baza B' .

Să considerăm un element $x \in L$, ale cărui coordonate în raport cu baza B sunt a_1, a_2, \dots, a_n , iar în raport cu baza B' sunt a'_1, a'_2, \dots, a'_n adică

$$x = a_1e_1 + a_2e_2 + \dots + a_ne_n \quad \text{si} \quad x = a'_1e'_1 + a'_2e'_2 + \dots + a'_ne'_n$$

Ne propunem să găsim legătura între coordonatele vectorului x în cele două baze, folosind matricea de trecere de la o bază la alta.

A vem

$$x = \sum_{i=1}^n a'_i e'_i = \sum_{i=1}^n a'_i \left(\sum_{j=1}^n u_{ji} e_j \right) = \sum_{j=1}^n \left(\sum_{i=1}^n a'_i u_{ji} \right) e_j.$$

Pe de altă parte, $x = \sum_{i=1}^n a_i e_i$ și cum coordonatele unui element x ,

într-o bază dată, sunt unic determinate, rezultă că $a_j = \sum_{i=1}^n a_i u_{ji}$, pentru orice $j = 1, 2, \dots, n$.

Să scriem desfășurat cele n relații precedente. Avem

$$\begin{aligned} a_1 &= u_{11}a'_1 + u_{12}a'_2 + \dots + u_{1n}a'_n, \\ a_2 &= u_{21}a'_1 + u_{22}a'_2 + \dots + u_{2n}a'_n, \\ &\dots \\ a_n &= u_{n1}a'_1 + u_{n2}a'_2 + \dots + u_{nn}a'_n. \end{aligned}$$

sau, scrise sub formă matriceală,

$$\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} = U \begin{pmatrix} a'_1 \\ a'_2 \\ \vdots \\ a'_n \end{pmatrix}.$$

Această ultimă relație se numește *formula transformării coordonatelor*.

Să considerăm acum în R -modulul liber L , trei baze $B = \{e_1, e_2, \dots, e_n\}$, $B' = \{e'_1, e'_2, \dots, e'_n\}$ și $B'' = \{e''_1, e''_2, \dots, e''_n\}$. Fie $U = (u_{ij})_{1 \leq i, j \leq n}$, $U' = (u'_{ij})_{1 \leq i, j \leq n}$ și $U'' = (u''_{ij})_{1 \leq i, j \leq n}$ respectiv, matricele de trecere de la baza B la baza B' , de la baza B' la baza B'' și de la B la baza B'' .

Lema 5.1. Cu notațiile precedente avem

$$U'' = UU'.$$

Demonstrație. Într-adevăr,

$$e'_i = \sum_{j=1}^n u_{ji}e_j, \quad e''_i = \sum_{j=1}^n u'_{ji}e'_j \text{ și } e''_i = \sum_{j=1}^n u''_{ji}e_j, \text{ pentru orice } 1 \leq i \leq n.$$

Atunci

$$e''_i = \sum_{j=1}^n u'_{ji}e'_j = \sum_{j=1}^n u'_{ji} \left(\sum_{k=1}^n u_{kj}e_k \right) = \sum_{k=1}^n \left(\sum_{j=1}^n u_{kj}u'_{ji} \right) e_k.$$

Pe de altă parte, $e''_i = \sum_{k=1}^n u''_{ki}e_k$ și cum coordonatele unui vector într-o bază sunt unic determinate, rezultă $u''_{ki} = \sum_{j=1}^n u_{kj}u'_{ji}$, pentru orice $1 \leq i, k \leq n$. Aceste relații exprimă faptul că $U'' = UU'$.

Propoziția 5.2. Fie L un R -modul liber de rang finit n și $B = \{e_1, e_2, \dots, e_n\}$, $B' = \{e'_1, e'_2, \dots, e'_n\}$ două baze ale sale. Atunci matricea de trecere de la baza B la baza B' este inversabilă.

Demonstrație. Fie U matricea de trecere de la baza B la baza B' , și V matricea de trecere de la baza B' la baza B . Deoarece matricea de trecere de la baza B la ea însăși este evident matricea unitate I_n , conform lemei precedente $UV = I_n$. Analog, avem $VU = I_n$ și deci U este matrice inversabilă.

Cum matricea U este inversabilă, formula transformării coordonatelor se mai poate scrie

$$\begin{pmatrix} a'_1 \\ a'_2 \\ \vdots \\ a'_n \end{pmatrix} = U^{-1} \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}.$$

Fie R un inel comutativ și unitar, L și L' două R -module libere de rang finit, $B = \{e_1, e_2, \dots, e_m\}$ o bază a lui L și $B' = \{e'_1, e'_2, \dots, e'_n\}$ o bază a lui L' . Dacă $f: L \rightarrow L'$ este un morfism de R -module, avem:

$$f(e_1) = a_{11}e'_1 + a_{21}e'_2 + \dots + a_{n1}e'_n,$$

$$f(e_2) = a_{12}e'_1 + a_{22}e'_2 + \dots + a_{n2}e'_n,$$

$$\dots$$

$$f(e_m) = a_{1m}e'_1 + a_{2m}e'_2 + \dots + a_{nm}e'_n.$$

Matricea

$$M_B^{B'}(f) = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nm} \end{pmatrix}$$

se numește *matricea asociată* morfismului f în bazele B și B' .

Lema 5.3. Dacă L și L' sunt R -module libere de rang finit, de baze respectiv $B = \{e_1, e_2, \dots, e_m\}$ și $B' = \{e'_1, e'_2, \dots, e'_n\}$, atunci, oricare ar fi $f, g \in \text{Hom}_R(M, M')$ și $a \in R$, avem:

$$1) M_B^{B'}(f+g) = M_B^{B'}(f) \oplus M_B^{B'}(g);$$

$$2) M_B^{B'}(af) = aM_B^{B'}(f).$$

Demonstrație. 1) Fie $M_B^{B'}(f) = (a_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}}$ și $M_B^{B'}(g) = (b_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}}$,

adică

$$f(e_j) = \sum_{i=1}^n a_{ij}e'_i \text{ și } g(e_j) = \sum_{i=1}^n b_{ij}e'_i, \quad j = 1, 2, \dots, m.$$

A vom

$$(f+g)(e_j) = f(e_j) + g(e_j) = \sum_{i=1}^n a_{ij}e'_i + \sum_{i=1}^n b_{ij}e'_i = \sum_{i=1}^n (a_{ij} + b_{ij})e'_i.$$

Deci

$$M_B^{B'}(f+g) = (a_{ij} + b_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} = (a_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} + (b_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} = M_B^{B'}(f) + M_B^{B'}(g).$$

2) Dacă $a \in R$, atunci

$$(af)(e_j) = af(e_j) = a \sum_{i=1}^n a_{ij} e'_i = \sum_{i=1}^n (aa_{ij}) e'_i$$

și deci

$$M_B^{B'}(af) = (aa_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} = a(a_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} = aM_B^{B'}(f).$$

Teorema 5.4. Fie L și L' două R -module libere de rang finit, de baze respectiv $B = \{e_1, e_2, \dots, e_m\}$ și $B' = \{e'_1, e'_2, \dots, e'_n\}$. Atunci există un izomorfism de R -module între $\text{Hom}_R(L, L')$ și $\mathcal{M}(n, m, R)$.

Demonstrație. Definim

$\varphi: \text{Hom}_R(L, L') \rightarrow \mathcal{M}(n, m, R)$ prin $\varphi(f) = M_B^{B'}(f)$. Din lema precedentă rezultă că φ este morfism de R -module.

Funcția φ este bijectivă. Într-adevăr, fie $f, g \in \text{Hom}_R(L, L')$ astfel încât $\varphi(f) = \varphi(g)$, adică $M_B^{B'}(f) = M_B^{B'}(g)$. Dacă presupunem că

$$M_B^{B'}(f) = (a_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}} \text{ și } M_B^{B'}(g) = (b_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}}, \text{ atunci}$$

$$f(e_j) = \sum_{i=1}^n a_{ij} e'_i = \sum_{i=1}^n b_{ij} e'_i = g(e_j),$$

oricare ar fi $j = 1, 2, \dots, m$. Conform teoremei 3.2 rezultă $f = g$ și deci φ este injectivă.

Funcția φ este și surjectivă. Într-adevăr, fie $M = (a_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}}$ o matrice din $\mathcal{M}(n, m, R)$ și să considerăm elementele x_1, x_2, \dots, x_m ale căror coordonate sint respectiv coloanele acestei matrice. Deci $x_j = \sum_{i=1}^n a_{ij} e_i$, oricare ar fi $j = 1, 2, \dots, m$.

Aplinind teorema 3.2 există un unic morfism $f \in \text{Hom}_R(L, L')$, cu proprietatea că $f(e_j) = x_j$, oricare ar fi $j = 1, 2, \dots, m$. Este clar că $M_B^{B'}(f) = M$, adică $\varphi(f) = M$.

Lema 5.5. Fie L, L', L'' module libere de rang finit peste inelul R , de baze respectiv $B = \{e_1, e_2, \dots, e_m\}$, $B' = \{e'_1, e'_2, \dots, e'_n\}$ și $B'' = \{e''_1, e''_2, \dots, e''_p\}$. Atunci oricare ar fi $f \in \text{Hom}_R(L, L')$ și $g \in \text{Hom}_R(L', L'')$ avem:

$$M_B^{B''}(g \circ f) = M_{B'}^{B''}(g) \cdot M_B^{B'}(f).$$

Demonstrație. Să presupunem că $M_B^{B'}(f) = (a_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}}$, $M_B^{B''}(g) = (b_{ij})_{\substack{1 \leq i \leq p \\ 1 \leq j \leq n}}$ și $M_{B'}^{B''}(g \circ f) = (c_{ij})_{\substack{1 \leq i \leq p \\ 1 \leq j \leq m}}$. Atunci $(g \circ f)(e_j) = \sum_{i=1}^p c_{ij} e'_i$, $1 \leq j \leq m$.

Pe de altă parte, $(g \circ f)(e_j) = g(f(e_j)) = g\left(\sum_{k=1}^n a_{kj} e'_k\right) = \sum_{k=1}^n a_{kj} g(e'_k) = \sum_{k=1}^n a_{kj} \left(\sum_{i=1}^p b_{ik} e''_i\right) = \sum_{i=1}^p \left(\sum_{k=1}^n b_{ik} a_{kj}\right) e''_i$.

Cum $B'' = \{e'_1, e'_2, \dots, e''_p\}$ este o bază, rezultă $c_{ij} = \sum_{k=1}^n b_{ik} a_{kj}$ oricare ar fi $1 \leq i \leq p$ și $1 \leq j \leq m$. Aceste relații arată tocmai că egalitatea din enunț este adevărată.

Fie acum un R -modul liber de rang finit L de bază $B = \{e_1, e_2, \dots, e_m\}$. Dacă $f \in \text{End}_R(L)$ să notăm cu $M_B(f)$ matricea $M_B^B(f)$ asociată morfismului f în baza B . În acest caz avem o funcție $\varphi: \text{End}_R(L) \rightarrow \mathcal{M}_m(R)$, dată prin $\varphi(f) = M_B(f)$.

Având în vedere teorema 5.4 și lema 5.5 rezultă că φ este un izomorfism de inele.

Astfel am obținut următorul corolar:

Corolarul 5.6. *Dacă L este un R -modul liber de rang finit, $B = \{e_1, e_2, \dots, e_m\}$ fiind o bază a sa, atunci există un izomorfism de R -algebrelor între $\text{End}_R(L)$ și $\mathcal{M}_m(R)$.*

Corolarul 5.7. *Fie L un R -modul liber de rang finit și $B = \{e_1, e_2, \dots, e_m\}$ o bază a sa. Atunci un endomorfism $f \in \text{End}_R(L)$ este inversabil (izomorfism) dacă și numai dacă matricea $M_B(f)$ este inversabilă.*

Fie L și L' două R -module de rang finit și $h: L \rightarrow L'$ un morfism. Să considerăm bazele $B = \{e_1, e_2, \dots, e_m\}$, $C = \{f_1, f_2, \dots, f_n\}$ ale lui L și $B' = \{e'_1, e'_2, \dots, e'_n\}$, $C' = \{f'_1, f'_2, \dots, f'_n\}$ ale lui L' . Notăm cu $U = (u_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}}$ și $V = (v_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}}$ matricea de trecere de la baza B la C și respectiv matricea de trecere de la baza B' la C' . Ne punem problema de a găsi legătura care există între matricea $M_B^{B'}(h)$ asociată morfismului h în bazele B și B' și matricea $M_C^{C'}(h)$ asociată morfismului h în bazele C și C' . Să presupunem că $M_B^{B'}(h) = (a_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}}$ și $M_C^{C'}(h) = (a'_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq m}}$. Cu notările precedente avem relațiile:

$$f_i = \sum_{j=1}^m u_{ij} e_j, \quad 1 \leq i \leq m; \quad f'_i = \sum_{j=1}^n v_{ji} e'_j, \quad 1 \leq i \leq n;$$

$$h(e_i) = \sum_{j=1}^n a_{ji} e_j, \quad 1 \leq i \leq m; \quad h(f_i) = \sum_{j=1}^n a'_{ji} f'_j, \quad 1 \leq i \leq m.$$

Pentru un vector f_j oarecare al bazei C , avem

$$h(f_j) = \sum_{k=1}^n a'_{kj} f_k' = \sum_{k=1}^n a'_{kj} \left(\sum_{i=1}^n v_{ik} e_i' \right) = \sum_{i=1}^n \left(\sum_{k=1}^n v_{ik} a'_{kj} \right) e_i'.$$

De asemenea,

$$\begin{aligned} h(f_j)) &= h\left(\sum_{k=1}^m u_{kj} e_k\right) = \sum_{k=1}^m u_{kj} h(e_k) = \\ &= \sum_{k=1}^m u_{kj} \left(\sum_{i=1}^n a_{ik} e_i' \right) = \sum_{i=1}^n \left(\sum_{k=1}^m u_{kj} a_{ik} \right) e_i'. \end{aligned}$$

Cum scrierea unui element într-o bază este unică, rezultă că $\sum_{k=1}^n v_{ik} a'_{kj} = \sum_{k=1}^m u_{kj} a_{ik}$, oricare ar fi $1 \leq i \leq n$ și $1 \leq j \leq m$.

Deci $VM_C^{C'}(h) = M_B^{B'}(h)U$. Conform propoziției 5.2, matricea de trecere de la o bază la alta este inversabilă și deci putem scrie

$$M_C^{C'}(h) = V^{-1} M_B^{B'}(h)U.$$

În particular, dacă $L=L'$, $B=C$ și $B'=C'$, atunci $U=V$ este matricea de trecere de la baza B la baza B' . Dacă $g: L \rightarrow L$ este un endomorfism al lui L , atunci formula de schimbare a matricei asociate lui g la schimbarea bazei este

$$M_{B'}(g) = U^{-1} M_B(g)U.$$

EXERCITII

1. Fie R un inel unitar și M un R -modul la stînga. Să se arate că grupul abelian $\text{Hom}_R(R, M)$ este izomorf cu grupul aditiv subiectiv modului M .

Indicație. Funcția $\phi: \text{Hom}_R(R, M) \rightarrow M$, definită prin $\phi(f) = -f(1)$ este izomorfism de grupuri abeliene.

2. Fie R un inel unitar. Un R -modul la stînga nenul M se numește *simplu* dacă (0) și M sunt singurele submodule ale lui M . Să se arate că, un R -modul M este simplu dacă și numai dacă $M \neq 0$ și M este generat de orice element nenul al său.

3. Să se arate că, dacă M și N sunt R -module simple, atunci orice morfism nenul de la M la N este un izomorfism. Să se deducă de aici că, dacă M este R -modul simplu, atunci $\text{End}_R(M)$ este corp.

4. Dacă M este un R -modul și $f \in \text{End}_R(M)$ astfel încît $f^2 = f$, să se arate că $M = \ker f + \text{Im } f$ și $\ker f \cap \text{Im } f = (0)$. Reciproc, dacă

P și Q sunt submodule ale lui M astfel încât $M=P+Q$ și $P \cap Q=(0)$, să se arate că există $f \in \text{End}_R(M)$, cu $f^2=f$, astfel încât $P=\text{Ker } f$ și $Q=\text{Im } f$.

Indicație. Dacă $x \in M$, atunci $x=(x-f(x))+f(x)$ și $x-f(x) \in \text{ker } f$, iar $f(x) \in \text{Im } f$. Reciproc, fie $i_Q: Q \rightarrow P+Q$, $i_Q(x)=x$ și $p_Q: P+Q \rightarrow Q$, $p_Q(x+y)=y$ (y este unic, deoarece $P \cap Q=(0)$). Atunci $f: P+Q \rightarrow P+Q$, unde $f=i_Q \circ p_Q$ are proprietățile cerute.

5. Fie M un R -modul finit generat, I un ideal al lui R și $f \in \text{End}_R(M)$, astfel încât $f(M) \subset IM$. Să se arate că există n , natural, și $a_i \in I$, $1 \leq i \leq n$, astfel încât $f^n+a_1f^{n-1}+\dots+a_{n-1}f+a_n=0$.

Indicație. Fie x_1, x_2, \dots, x_n generatorii lui M . Deoarece $f(M) \subset IM$ avem $f(x_i)=\sum_{j=1}^n a_{ij}x_j$, $1 \leq i \leq n$ și $a_{ij} \in I$. Deci $\sum_{j=1}^n (\delta_{ij}f-a_{ij})x_j=0$, de unde rezultă $\det(\delta_{ij}f-a_{ij})=0$, care reprezintă o relație de tipul cerut.

6. Fie M un R -modul finit generat și I un ideal al lui R , astfel încât $IM=M$. Să se arate că există $a \in R$, $a \equiv 1 \pmod{I}$ astfel încât $aM=0$.

Indicație. Pentru $f=1_M$ sătem în condițiile problemei precedente și deci $1_M^n+a_11_M^{n-1}+\dots+a_{n-1}1_M+a_n=0$, unde $a_i \in I$, $1 \leq i \leq n$. Luăm $a=1+a_1+\dots+a_n$.

7. Fie M un R -modul finit generat și I un ideal al lui R inclus în radicalul Jacobson $J(R)$. Să se arate că:

- i) Dacă $IM=0$, atunci $M=0$;
- ii) Dacă, în plus, N este un submodul al lui M , astfel încât $M=IM+N$, atunci $M=N$.

Indicație. i) Din exercițiul precedent avem $a \in R$ încât $aM=0$ și $a \equiv 1 \pmod{I}$. Cum $a-1 \in J(R)$, din exercițiul 21, cap. III, rezultă că a este inversabil. ii) Se aplică pct. i) modului M/N .

8. Fie V și V' două spații vectoriale peste un corp K , de aceeași dimensiune, iar $f: V \rightarrow V'$ un morfism. Următoarele afirmații sunt echivalente:

- iii) f este injectiv; ii) f este surjectiv; iii) f este izomorfism.

Indicație. i) \Rightarrow ii). Dacă $\{e_1, e_2, \dots, e_n\}$ este o bază a lui V , se arată că $\{f(e_1), f(e_2), \dots, f(e_n)\}$ este o bază a lui V' . ii) \Rightarrow iii). Dacă $\{e'_1, e'_2, \dots, e'_n\}$ este o bază a lui V' , fie vectorii $x_1, x_2, \dots, x_n \in V$ astfel încât $f(x_i)=e'_i$, $1 \leq i \leq n$. Morfismul $g: V' \rightarrow V$ astfel încât $g(e'_i)=x_i$, $1 \leq i \leq n$, are proprietatea că $f \circ g=1_{V'}$ și $g \circ f=1_V$.

9. Fie V un spațiu vectorial peste un corp K și $\{x_1, x_2, \dots, x_n\}$ o mulțime de vectori ai săi. Să se arate că $\{x_1, x_2, \dots, x_n\}$ formează

un sistem de vectori liniar independent dacă și numai dacă $Kx_i \cap \sum_{j \neq i} Kx_j = \{0\}$, oricare ar fi $i = 1, 2, \dots, n$.

10. Fie M un R -modul finit generat și $\varphi: M \rightarrow R^n$ un morfism surjectiv de module. Să se arate că $\text{Ker } \varphi$ este un submodul finit generat al lui M .

Indicație. Fie $\{e_1, e_2, \dots, e_n\}$ o bază a lui R^n și $x_i \in M$, astfel încât $\varphi(x_i) = e_i$, $i = 1, 2, \dots, n$. Se arată că $M = \text{Ker } \varphi + \sum_{i=1}^n Rx_i$ și $\text{Ker } \varphi \cap \sum_{i=1}^n Rx_i = \{0\}$. Se aplică apoi teorema a II-a de izomorfism pentru module.

11. Fie K un corp comutativ, V un K -spațiu vectorial de dimensiune n și $B = \{e_1, e_2, \dots, e_n\}$ o mulțime de elemente ale lui V . Următoarele afirmații sunt echivalente:

- i) B este o bază a lui V ;
- ii) B este un sistem liniar independent al lui V ;
- iii) B este un sistem de generatori al lui V .

Indicație. Demonstrația rezultă ușor, folosind teorema bazei și teorema schimbului.

12. Fie R un inel local și \underline{m} idealul său maximal. Să se arate că, dacă $\hat{x}_1, \hat{x}_2, \dots, \hat{x}_n$ formează o bază a R/\underline{m} -spațiului vectorial $M/\underline{m}M$, atunci x_1, x_2, \dots, x_n formează un sistem de generatori al lui M .

Indicație. Dacă $N = Rx_1 + Rx_2 + \dots + Rx_n$, se arată că $N = \underline{m}M + N$. Apoi se folosește exercițiul 7.

13. Fie V un K -spațiu vectorial. Să se arate că, dacă oricare ar fi morfismul $f \in \text{End}_K(V)$ există n , natural, și $a_i \in K$, $1 \leq i \leq n$, astfel încât $f^n + a_1f^{n-1} + \dots + a_{n-1}f + a_n = 0$, atunci V este de dimensiune finită.

Indicație. Dacă B este o bază infinită a lui V , fie $B' \subset B$, $B' = \{x_1, x_2, \dots, x_n, \dots\}$. Să considerăm morfismul $f: V \rightarrow V'$, astfel încât $f(x_i) = x_{i+1}$, pentru $x_i \in B'$ și $f(x) = 0$, pentru $x \in B \setminus B'$. Avem $f(x_1) = x_2$, $f^2(x_1) = x_3$, ..., $f^n(x_1) = x_{n+1}$, de unde $x_{n+1} + a_1x_n + \dots + a_nx_1 = 0$, contradicție.

14. Fie R un inel comutativ, M un R -modul și să considerăm R -modulul $M^* = \text{Hom}_R(M, R)$, numit *dualul* lui M . Dacă M este R -modul liber de rang n , atunci dualul său este R -modul liber de același rang.

Indicație. Dacă $\{e_1, e_2, \dots, e_n\}$ este o bază a lui M , atunci $\{e_1^*, e_2^*, \dots, e_n^*\}$, unde $e_i^*(e_j) = \delta_{ij}$ este o bază a lui M^* (δ_{ij} este simbolul lui Kronecker).

15. Fie R un inel unitar, L un R -modul liber și $(e_i)_{i \in I}, (f_j)_{j \in J}$ două baze ale lui L . Să se arate că, dacă una dintre multimiile I sau J este infinită, atunci și cealaltă este infinită și, mai mult, $\text{card } I = \text{card } J$.

Indicație. Demonstrația se face analog cu cea a teoremei 4.3.

16. Fie K un corp comutativ, K -spațiul vectorial $V = K^{(N)}$ și $R = \text{End}_K(V)$. Să se arate că R -modulul la stînga ${}_R R$ admite baze finite care să nu aibă același număr de elemente.

Indicație. Dacă $(e_n)_{n \in \mathbb{N}}$ este baza canonica a lui V , există morfismele $u, v \in R$ astfel încit, $u(e_{2n}) = e_n$ și $u(e_{2n+1}) = 0$, iar $v(e_{2n}) = 0$ și $v(e_{2n+1}) = e_n$. Se arată că $\{u, v\}$ este o bază a lui ${}_R R$, iar $\{1\}$ este evident o altă bază a sa.

17. Fie V un K -spațiu vectorial de dimensiune finită. Să se arate că oricare ar fi endomorfismul f al lui V , există n , natural, astfel încit $\text{Im } f^n = \text{Im } f^{n+1}$.

Indicație. Avem că sirul descreșător de subspații $V \supset \text{Im } f \supset \text{Im } f^2 \supset \dots \supset \text{Im } f^n \supset \dots$ este finit.

18. Fie $C_n[X]$ spațiul vectorial al polinoamelor de grad $\leq n$ cu coeficienți complecsi. Să se arate că, oricare ar fi $a \in \mathbb{C}$ polinoamele $1, X - a, (X - a)^2, \dots, (X - a)^n$ formează o bază a sa și să se determine coordonatele unui polinom oarecare în raport cu această bază.

Indicație. Se aplică lema 8.8 din cap. III.

19. În spațiul vectorial $C_n[X]$ considerăm bazele $B = \{1, X, X^2, \dots, X^n\}$, $B' = \{1, X - a, (X - a)^2, \dots, (X - a)^n\}$, $a \in \mathbb{C}$ (vezi exercițiul 18) și morfismul $d: C_n[X] \rightarrow C_n[X]$, $d(f) = f^{(1)}$, unde $f^{(1)}$ este derivata lui f . Să se scrie matricele asociate morfismului d în fiecare din cele două baze.

Indicație. Față de prima bază avem:

$$M_B(d) = \begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 2 & 2 & \dots & 0 \\ 0 & 0 & 0 & 3 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & 0 & \dots & n \\ 0 & 0 & 0 & 0 & \dots & 0 \end{pmatrix},$$

iar față de cea de-a doua bază avem $M_{B'}(d) = U^{-1}M_B(d)U$, unde

$$U = \begin{pmatrix} a & -a & a^2 & \dots & (-1)^n a^n \\ 0 & 1 & -2a & & \vdots \\ 0 & 0 & 1 & \ddots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix}.$$

20. Să se determine endomorfismele unui K -spațiu vectorial V de dimensiune finită ale căror matrice asociate în orice bază a lui V sunt egale.

Indicație. Fie $B = \{e_1, e_2, \dots, e_n\}$ și $B' = \{e'_1, e'_2, \dots, e'_n\}$ două baze, U matricea de trecere de la baza B la baza B' . Dacă $f: V \rightarrow V'$ este un endomorfism, atunci $M_{B'}(f) = U^{-1}M_B(f)U$ și cum $M_{B'}(f) = M_B(f)$, $UM_B(f) = M_B(f)U$. Mai mult, orice matrice inversabilă este o matrice de trecere de la baza B la o altă bază și deci $AM_B(f) = M_B(f)A$, ori care ar fi matricea inversabilă A . Particularizând matricele A , rezultă $a \in K$ astfel încât $f(x) = ax$, oricare ar fi $x \in V$.

Capitolul VI

DETERMINANȚI. SISTEME ȘI ECUAȚII LINIARE

§ 1. DETERMINANȚI DE ORDIN MIC

În acest paragraf vom defini determinanții de ordinul 2 și 3 pornind de la rezolvarea sistemelor de două ecuații liniare cu două necunoscute, respectiv a sistemelor de trei ecuații liniare cu trei necunoscute (pentru simplificare, cu elemente din corpul numerelor reale).

Fie, mai întii, un sistem de două ecuații liniare cu două necunoscute:

$$(1) \quad \begin{cases} a_{11}x_1 + a_{12}x_2 = b_1 \\ a_{21}x_1 + a_{22}x_2 = b_2 \end{cases}$$

Să notăm cu A matricea coeficienților sistemului (1), adică

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}.$$

A este o matrice pătratică de ordinul doi.

Rezolvarea sistemului (1) este bine cunoscută. Aplicind metoda reducerii obținem sistemul echivalent

$$\begin{cases} (a_{11}a_{22} - a_{12}a_{21})x_1 = b_1a_{22} - a_{12}b_2 \\ (a_{11}a_{22} - a_{12}a_{21})x_2 = b_2a_{11} - b_1a_{21} \end{cases}$$

Presupunem că $a_{11}a_{22} - a_{12}a_{21} \neq 0$; atunci soluția sistemului (1) este:

$$(2) \quad x_1 = \frac{b_1a_{22} - a_{12}b_2}{a_{11}a_{22} - a_{12}a_{21}}, \quad x_2 = \frac{b_2a_{11} - b_1a_{21}}{a_{11}a_{22} - a_{12}a_{21}}$$

Se observă că numitorul din egalitățile (2) se exprimă simplu: el este egal cu produsul elementelor de pe diagonala principală a matricei A din care se scade produsul elementelor de pe diagonala secundară a matricei A .

Acest număr îl notăm cu $\det A$ și îl numim *determinantul matricei A* , sau, încă, *determinant de ordinul doi* (deoarece matricea A este de ordinul doi). Acest număr se notează de obicei și astfel:

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}$$

deci avem egalitatea

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}.$$

Produsele $a_{11}a_{22}$, $a_{12}a_{21}$ se numesc termenii determinantului de ordinul doi.

Exemplu. Fie matricea $A = \begin{pmatrix} 2 & 1 \\ 3 & 6 \end{pmatrix}$. Avem $\det A = \begin{vmatrix} 2 & 1 \\ 3 & 6 \end{vmatrix} = 2 \cdot 6 - 3 \cdot 1 = 12 - 3 = 9$.

Să revenim la formulele (2) care dă soluțiile sistemului (1). Se observă că numărătorul formulei care dă valoarea lui x_1 este tot un determinant de ordinul doi, și anume determinantul matricei

$$A_1 = \begin{pmatrix} b_1 & a_{12} \\ b_2 & a_{22} \end{pmatrix}$$

Această matrice se obține din A înlocuindu-i prima coloană cu coloana formată din elementele b_1 și b_2 . Analog, numărătorul formulei care dă valoarea lui x_2 este un determinant de ordinul doi, și anume determinantul matricei

$$A_2 = \begin{pmatrix} a_{11} & b_1 \\ a_{21} & b_2 \end{pmatrix}$$

Deci formulele (2) se pot scrie sub forma

$$(3) \quad x_1 = \frac{\begin{vmatrix} b_1 & a_{12} \\ b_2 & a_{22} \end{vmatrix}}{\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}}, \quad x_2 = \frac{\begin{vmatrix} a_{11} & b_1 \\ a_{21} & b_2 \end{vmatrix}}{\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}}$$

Formulele (3) poartă denumirea de *formulele lui Cramer*.

Să considerăm acum un sistem de trei ecuații liniare cu trei necunoscute:

$$(4) \quad \begin{cases} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 = b_1 \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 = b_2 \\ a_{31}x_1 + a_{32}x_2 + a_{33}x_3 = b_3 \end{cases}$$

și să notăm cu A matricea coeficienților, adică:

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

Rezolvarea sistemului (4) o vom face prin metoda reducerii. Dacă înmulțim prima ecuație din (4) cu a_{23} și a doua cu $-a_{13}$ și le adunăm, obținem ecuația

$$(5) \quad (a_{11}a_{23} - a_{21}a_{13})x_1 + (a_{12}a_{23} - a_{22}a_{13})x_2 = b_1a_{23} - b_2a_{13}$$

Analog, înmulțind prima ecuație cu a_{33} și a treia cu $-a_{13}$ și apoi adunând, obținem ecuația:

$$(6) \quad (a_{11}a_{33} - a_{31}a_{13})x_1 + (a_{12}a_{33} - a_{32}a_{13})x_2 = b_1a_{33} - b_3a_{13}$$

Cu ecuațiile (5) și (6) formăm sistemul:

$$(7) \quad \begin{cases} (a_{11}a_{23} - a_{21}a_{13})x_1 + (a_{12}a_{23} - a_{22}a_{13})x_2 = b_1a_{23} - b_2a_{13} \\ (a_{11}a_{33} - a_{31}a_{13})x_1 + (a_{12}a_{33} - a_{32}a_{13})x_2 = b_1a_{33} - b_3a_{13} \end{cases}$$

care este un sistem de două ecuații cu două necunoscute. Dacă în sistemul (7) înmulțim prima ecuație cu $a_{12}a_{33} - a_{32}a_{13}$ și a doua cu $-(a_{12}a_{23} - a_{22}a_{13})$ și apoi le adunăm, obținem:

$$[(a_{11}a_{23} - a_{21}a_{13})(a_{12}a_{33} - a_{32}a_{13}) - (a_{12}a_{13} - a_{22}a_{13})(a_{11}a_{33} - a_{31}a_{13})]x_1 = \\ = (b_1a_{23} - b_2a_{13})(a_{12}a_{33} - a_{32}a_{13}) - (b_1a_{33} - b_3a_{13})(a_{12}a_{23} - a_{22}a_{13}).$$

Desfăcind parantezele, avem:

$$(8) \quad (a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32})x_1 = \\ = b_1a_{22}a_{33} + a_{12}a_{23}b_3 + a_{13}b_2a_{32} - a_{13}a_{22}b_3 - a_{12}b_2a_{33} - b_1a_{23}a_{32}$$

Numărul care este coeficientul lui x_1 în ecuația (8) îl notăm cu $\det A$ și îl numim *determinantul matricei A*, sau încă, *determinant de ordinul trei* (deoarece matricea A este o matrice de ordinul trei). Acest număr se notează de obicei și astfel:

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}$$

Deci avem egalitatea

$$(9) \quad \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - \\ - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32}$$

Din (9) se vede că formula care dă valoarea determinantului de ordinul trei are șase termeni, numiți termenii determinantului de ordinul trei.

Exemplu. Fie matricea $A = \begin{pmatrix} 1 & 2 & -1 \\ 3 & -1 & 0 \\ -2 & -4 & 5 \end{pmatrix}$. Aplicind formula

$$(9), \text{ avem: } \det A = 1 \cdot (-1) \cdot 5 + 2 \cdot 0 \cdot (-2) + 3 \cdot (-4) \cdot (-1) - (-1) \cdot (-1) \cdot (-2) - 2 \cdot 3 \cdot 5 - 1 \cdot 0 \cdot (-4) = -5 + 0 + 12 + 2 - 30 + 0 = -21.$$

Observăm că formula (9), care dă valoarea determinantului de ordinul trei, este greu de ținut minte. Pentru aceasta se stabilește o regulă simplă pentru calculul determinantului de ordinul trei. Se formează următorul tablou: se scriu mai întii liniile matricei A și apoi sub ele se scrie mai întii prima linie și apoi a doua linie a matricei A . În felul acesta se obține un tablou cu cinci linii:

$$\begin{array}{ccc|cc} a_{11} & a_{12} & a_{13} & & \\ a_{21} & a_{22} & a_{23} & & \\ a_{31} & a_{32} & a_{33} & & \\ \hline a_{11} & a_{12} & a_{13} & & \\ a_{21} & a_{22} & a_{23} & & \end{array}$$

Termenii cu semnul (+) în dezvoltarea determinantului de ordinul trei sunt cei care se obțin prin înmulțirea elementelor în sensul săgețiilor continue, adică: $a_{11}a_{22}a_{33}$, $a_{21}a_{32}a_{13}$, $a_{31}a_{12}a_{23}$, iar termenii cu semnul (-) sunt cei care se obțin prin înmulțirea elementelor în sensul săgețiilor punctate, adică: $a_{31}a_{22}a_{13}$, $a_{11}a_{32}a_{23}$, $a_{21}a_{12}a_{33}$. Regula expusă mai înainte, după care se face dezvoltarea determinantului de ordinul trei, se numește *regulă lui Sarrus*.

Exemplu. Să considerăm matricea $A = \begin{pmatrix} 1 & -2 & 3 \\ 1 & 0 & 2 \\ -4 & 1 & 3 \end{pmatrix}$. Formăm tabelul pentru aplicarea reguli lui Sarrus:

$$\begin{array}{ccc|cc} 1 & -2 & 3 & & \\ 1 & 0 & 2 & & \\ -4 & 1 & 3 & & \\ \hline 1 & -2 & 3 & & \\ 1 & 0 & 2 & & \\ 1 & 0 & 2 & & \end{array}$$

$$\text{Deci } \det A = 1 \cdot 0 \cdot 3 + 1 \cdot 1 \cdot 3 + (-4) \cdot (-2) \cdot 2 - (-4) \cdot 0 \cdot 3 - 1 \cdot 1 \cdot 2 - 1 \cdot (-2) \cdot 3 = 3 + 16 - 2 + 6 = 23.$$

Să ne reîntoarcem la ecuația (8) care dă valoarea lui x_1 . Se observă că membrul al doilea este tot un determinant de ordinul trei care

se obține din matricea A , matricea coeficienților, prin înlocuirea primei coloane cu coloana termenilor liberi din sistemul (4). Deci formula (8) se mai poate scrie astfel:

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}, \quad x_1 = \begin{vmatrix} b_1 & a_{12} & a_{13} \\ b_2 & a_{22} & a_{23} \\ b_3 & a_{32} & a_{33} \end{vmatrix}.$$

Procedind exact așa cum am făcut pentru obținerea ecuației (8), avem și ecuațiile care dă valorile lui x_2 și x_3 :

$$\begin{array}{l} \left| \begin{array}{ccc} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{array} \right|, \quad x_2 = \left| \begin{array}{ccc} a_{11} & b_1 & a_{13} \\ a_{21} & b_2 & a_{23} \\ a_{31} & b_3 & a_{33} \end{array} \right| \\ \left| \begin{array}{ccc} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{array} \right|, \quad x_3 = \left| \begin{array}{ccc} a_{11} & a_{12} & b_1 \\ a_{21} & a_{22} & b_2 \\ a_{31} & a_{32} & b_3 \end{array} \right| \end{array}$$

Dacă

$$\left| \begin{array}{ccc} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{array} \right| \neq 0$$

atunci valorile lui x_1 , x_2 și x_3 sunt:

$$(10) \quad x_1 = \frac{\left| \begin{array}{ccc} b_1 & a_{12} & a_{13} \\ b_2 & a_{22} & a_{23} \\ b_3 & a_{32} & a_{33} \end{array} \right|}{\left| \begin{array}{ccc} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{array} \right|}, \quad x_2 = \frac{\left| \begin{array}{ccc} a_{11} & b_1 & a_{13} \\ a_{21} & b_2 & a_{23} \\ a_{31} & b_3 & a_{33} \end{array} \right|}{\left| \begin{array}{ccc} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{array} \right|}, \quad x_3 = \frac{\left| \begin{array}{ccc} a_{11} & a_{12} & b_1 \\ a_{21} & a_{22} & b_2 \\ a_{31} & a_{32} & b_3 \end{array} \right|}{\left| \begin{array}{ccc} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{array} \right|}$$

Formulele (10) se numesc, de asemenea, *formulele lui Cramer* de rezolvare a sistemelor de trei ecuații liniare cu trei necunoscute.

§ 2. DEFINIȚIA DETERMINANȚILOR DE ORDINUL n

În cele ce urmează vom căuta să dăm definiția determinantului unei matrice pătratice de ordinul n în așa fel încit pentru $n=2$ și $n=3$ să obținem determinantul de ordinul 2 și 3.

În definirea determinantului de ordinul 2 și 3 am utilizat rezolvarea sistemelor de ecuații liniare. Acest procedeu este greu de folosit pentru cazul general, datorită calculelor laborioase care intervin. Noi vom utiliza altă metodă: analizând formulele care dă determinantul de ordinul 2 și 3 vom deduce o lege generală prin care vom defini determinantul de ordinul n . În capitolul următor vom arăta că formula

determinantului de ordinul n , aşa cum o dăm mai jos, ne va permite obținerea unor formule de tip Cramer pentru rezolvarea sistemelor de n ecuații liniare cu n necunoscute.

Să reamintim formulele determinanților de ordinul 2 și 3:

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}$$

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33} - a_{11}a_{23}a_{32} =$$

$$= a_{11} \begin{vmatrix} a_{23} & a_{33} \\ a_{32} & a_{33} \end{vmatrix} - a_{12} \begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix} + a_{13} \begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix}$$

Constatăm că termenii determinantelor de ordinul 2 și 3 sunt produse de elemente aparținând la linii și coloane distincte. În plus, orice astfel de produs (din elemente aparținând la linii și coloane distincte) este termen în formula determinantului respectiv.

Fie R un inel comutativ cu unitate. Să considerăm acum o matrice pătratică de ordinul n cu elemente din inelul R .

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}; A \in \mathcal{M}_n(R)$$

Vom forma toate produsele posibile de n elemente aparținând la linii și coloane distincte. Un astfel de produs este de forma:

$$(1) \quad a_{1i_1}a_{2i_2} \dots a_{ni_n}$$

unde i_1, i_2, \dots, i_n sunt toate elementele mulțimii $1, 2, \dots, n$, eventual în altă ordine. Înseamnă că putem considera permutarea de gradul n :

$$\sigma = \begin{pmatrix} 1 & 1 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{pmatrix}$$

și deci produsul (1) se scrie

$$a_{1i_1}a_{2i_2} \dots a_{ni_n} = a_{1\sigma(1)}a_{2\sigma(2)} \dots a_{n\sigma(n)}$$

Numărul total al produselor de forma (1) este egal cu numărul tuturor permutărilor de grad n , deci $n!$. Tinând cont de formulele determinantelor de ordinul 2 și 3, în mod natural formula determinantului de ordinul n trebuie să conțină toate produsele

$$a_{1\sigma(1)}a_{2\sigma(2)} \dots a_{n\sigma(n)},$$

unde σ parcurge toate permutările lui S_n . Mai rămâne de aflat semnul cu care apare produsul $a_{1\sigma(1)}a_{2\sigma(2)} \dots a_{n\sigma(n)}$. Să revenim din nou la for-

mulele determinanților de ordinul 2 și 3. Să luăm, de exemplu, din formula determinantului de ordinul trei termenii cu semnul (+): $a_{11}a_{22}a_{33}$, $a_{12}a_{23}a_{31}$, $a_{13}a_{21}a_{32}$. Se observă că permutările asociate acestor termeni:

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

sunt permutări pare, deci semnul lor este +1.

Dacă luăm acum termenii cu semnul (-): $a_{13}a_{22}a_{31}$, $a_{12}a_{21}a_{33}$, $a_{11}a_{23}a_{32}$, permutările asociate acestor termeni:

$$\sigma_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad \sigma_5 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad \sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

sunt permutări impare, deci au signatura (semnul) -1. Aceste observații ne sugerează că în definiția determinantului de ordinul n , produsul $a_{1\sigma(1)}a_{2\sigma(2)}\dots a_{n\sigma(n)}$ trebuie să aibă semnul (+) sau (-) după cum permutarea σ are signatura (semnul) +1 sau -1. Acum să întem să definim determinantul de ordinul n .

Definiția 2.1. Fie $A \in \mathcal{M}_n(R)$. Elementul din inelul R

$$\det A = \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \dots a_{n\sigma(n)},$$

unde S_n este mulțimea tuturor permutărilor de gradul n și $\varepsilon(\sigma)$ este signatura permutării σ , se numește determinantul matricei A , sau, mai simplu, determinant de ordinul n și se notează de obicei astfel:

$$\det A = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}$$

Produsul $a_{1\sigma(1)}a_{2\sigma(2)}\dots a_{n\sigma(n)}$ se numește termen al determinantului de ordinul n .

Se obișnuiește să se spună despre elementele, liniile și coloanele matricei A că sunt elementele, liniile și coloanele determinantului $\det A$. Uneori $\det A$ se mai notează prescurtat și $|A|$ sau $|a_{ij}|$.

$$\begin{matrix} 1 \leq i \leq n \\ 1 \leq j \leq n \end{matrix}$$

Observații. 1) Noțiunea de determinant al unei matrice are sens numai pentru matrice pătratice. Este deosebire între matrice și determinantul său: matricea este o funcție, iar determinantul matricei este un element al inelului R .

2) În formula determinantului unei matrice există $n!$ termeni dintre care $\frac{n!}{2}$ au semnul (+), iar $\frac{n!}{2}$ au semnul (-).

3) Definiția determinantului se aplică și matricelor de ordinul 1, cind $A = (a_{11})$. În acest caz $\det A = a_{11}$.

4) Așa cum a fost definit determinantul de ordinul n , pentru $n=2$ și $n=3$, obținem determinantul de ordinul 2, respectiv 3.

§.3. PROPRIETĂȚILE DETERMINANȚILOR

Formula determinantului de ordinul 2 este simplă; formula determinantului de ordinul trei este deja complicată. Aici avem avantajul că avem o regulă simplă, regula lui Sarrus, care ne permite să calculăm destul de ușor un determinant de ordinul 3. Dacă, în schimb, avem de calculat determinantă de ordin $n \geq 4$, formula prin căreia este definit determinantul de ordinul n , în general este aproape imposibil de aplicat datorită calculelor laborioase care apar. De exemplu, pentru un determinant de ordinul 4 avem $4! = 24$, termeni în formula sa, pentru $n=5$ avem $5! = 120$ termeni de calculat, iar pentru $n=10$ avem $10! = 3\,628\,800$ termeni de calculat. Din aceste motive se caută să se scoată în evidență o serie de proprietăți ale determinantelor de ordinul n , care simplifică de multe ori calculul determinantelor.

Proprietatea 1. Determinantul unei matrice coincide cu determinantul matricei transpuse. Adică dacă $A \in \mathcal{M}_n(R)$, atunci $\det A = \det {}^t A$.

Demonstrație. Fie $A = (a_{ij})$ și ${}^t A = ({}^t a_{ij})$ matricea transpusă a lui A .

Deci ${}^t a_{ij} = a_{ji}$, oricare ar fi $i = 1, 2, \dots, n$; $j = 1, 2, \dots, n$. Avem

$$(1) \quad \det A = \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \dots a_{n\sigma(n)}$$

$$(2) \quad \begin{aligned} \det {}^t A &= \sum_{\sigma \in S_n} \varepsilon(\sigma) {}^t a_{1\sigma(1)} {}^t a_{2\sigma(2)} \dots {}^t a_{n\sigma(n)} = \\ &= \sum_{\tau \in S_n} \varepsilon(\sigma) a_{\sigma(1)1} a_{\sigma(2)2} \dots a_{\sigma(n)n} \end{aligned}$$

Dacă notăm $\sigma(i) = k_i$, atunci $i = \sigma^{-1}(k_i)$ și deci produsul

$$\begin{aligned} \varepsilon(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \dots a_{n\sigma(n)} &= \varepsilon(\sigma) a_{\sigma^{-1}(k_1)k_1} a_{\sigma^{-1}(k_2)k_2} \dots a_{\sigma^{-1}(k_n)k_n} = \\ &= \varepsilon(\sigma^{-1}) a_{\sigma^{-1}(k_1)k_1} a_{\sigma^{-1}(k_2)k_2} \dots a_{\sigma^{-1}(k_n)k_n} \end{aligned}$$

deoarece $\varepsilon(\sigma) = \varepsilon(\sigma^{-1})$. Cum numerele k_1, k_2, \dots, k_n sunt numerele $1, 2, \dots, n$, eventual în altă ordine, iar înmulțirea numerelor este comutativă, atunci

$$\varepsilon(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \dots a_{n\sigma(n)} = \varepsilon(\sigma^{-1}) a_{\sigma^{-1}(1)1} a_{\sigma^{-1}(2)2} \dots a_{\sigma^{-1}(n)n}$$

și deci orice termen din suma (1) se regăsește ca termen în suma (2) și invers. Deci $\det A = \det {}^t A$.

Observații. 1) Proprietatea 1 se scrie și astfel:

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{21} & \dots & a_{n1} \\ a_{12} & a_{22} & \dots & a_{n2} \\ \dots & \dots & \dots & \dots \\ a_{1n} & a_{2n} & \dots & a_{nn} \end{vmatrix}$$

2) Proprietatea 1 arată că ori de câte ori avem o proprietate adevărată, referitoare la liniile unui determinant, aceeași proprietate este adevărată și pentru coloanele determinantului.

Proprietatea 2. Dacă toate elementele unei linii (sau coloane) dintr-o matrice sunt nule, atunci determinantul matricei este nul.

Demonstrație. Să presupunem că toate elementele de pe linia i sunt nule. Cum fiecare termen al determinantului este un produs de elemente, printre care se găsește și un element de pe linia i , atunci acest termen este zero. Deci determinantul este zero.

Exemplu. Fie matricea:

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

Deoarece linia a 3-a a matricei A are toate elementele nule, $\det A = 0$.

Proprietatea 3. Dacă într-o matrice schimbăm două linii (sau coloane) între ele obținem o matrice care are determinantul egal cu opusul determinantului matricei inițiale.

Demonstrație. Fie matricea:

$$A = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ a_{i1} & a_{i2} & \dots & a_{in} \\ \dots & \dots & \dots & \dots \\ a_{j1} & a_{j2} & \dots & a_{jn} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}$$

(i)

(j)

Prin schimbarea liniilor i și j între ele obținem matricea:

$$A' = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ a_{j1} & a_{j2} & \dots & a_{jn} \\ \dots & \dots & \dots & \dots \\ a_{i1} & a_{i2} & \dots & a_{in} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}$$

Avem

$$\det A' = \sum_{\sigma \in S_n} \epsilon(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \dots a_{j\sigma(i)} \dots a_{i\sigma(j)} \dots a_{n\sigma(n)}$$

Să considerăm transpoziția $\tau = (ij)$ deci $\tau(i)=j$, $\tau(j)=i$ și $\tau(k)=k$ dacă $k \neq i, j$. Atunci

$$\begin{aligned} \det A' &= \sum_{\sigma \in S_n} \epsilon(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \dots a_{j\sigma(i)} \dots a_{i\sigma(j)} \dots a_{n\sigma(n)} \\ &= \sum_{\sigma \in S_n} \epsilon(\sigma) a_{1(\sigma\tau)(1)} a_{2(\sigma\tau)(2)} \dots a_{j(\sigma\tau)(j)} \dots a_{i(\sigma\tau)(i)} \dots a_{n(\sigma\tau)(n)} \end{aligned}$$

Cum $\epsilon(\sigma\tau) = \epsilon(\sigma)\epsilon(\tau) = -\epsilon(\sigma)$, avem

$$\det A' = - \sum_{\sigma \in S_n} \epsilon(\sigma\tau) a_{1(\sigma\tau)(1)} \dots a_{i(\sigma\tau)(i)} \dots a_{j(\sigma\tau)(j)} \dots a_{n(\sigma\tau)(n)}$$

Cind σ parcurge toate permutările lui S_n și $\sigma\tau$ parcurge toate permutările lui S_n , deci dacă notăm $\sigma\tau=\sigma'$, avem

$$\det A' = - \sum_{\sigma' \in S_n} \epsilon(\sigma') a_{1\sigma'(1)} a_{2\sigma'(2)} \dots a_{n\sigma'(n)}$$

și deci $\det A' = -\det A$.

Exemplu. Fie matricea $A = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 4 \\ -1 & 0 & 5 \end{pmatrix}$. Dacă schimbăm liniile 1 și 2 între ele obținem matricea $A' = \begin{pmatrix} 2 & 1 & 4 \\ -1 & 2 & 3 \\ -1 & 0 & 5 \end{pmatrix}$. Conform proprietății 3, avem $\det A = -\det A'$, ceea ce se poate verifica și folosind regula lui Sarrus.

Proprietatea 4. *Dacă o matrice are două linii (sau coloane) identice atunci determinantul său este nul.*

Demonstrație. Fie $A = (a_{ij})$ o matrice pătratică de ordinul n în care liniile i și j sunt identice. Aceasta înseamnă că $a_{ik} = a_{jk}$ pentru orice $k = 1, 2, \dots, n$. Înseamnă că orice termen din dezvoltarea lui $\det A$ se regăsește în această dezvoltare cu semnul schimbat. Deci toți termenii din dezvoltarea lui $\det A$ se reduc 2 cîte 2 și prin urmare $\det A = 0$.

Exemplu. Fie matricea $A = \begin{pmatrix} 3 & -13 & -13 \\ -2 & 52 & 52 \\ 1 & 7 & 7 \end{pmatrix}$ care are două

coloane identice (coloana 2 și coloana 3). Deci conform proprietății 4 avem $\det A = 0$.

Proprietatea 5. Dacă toate elementele unei linii (sau coloane) ale unei matrice sunt înmulțite cu un element α obținem o matrice al cărui determinant este egal cu α înmulțit cu determinantul matricei inițiale.

Demonstrație. Fie matricea $A = (a_{ij})$ și fie $A' = (a'_{ij})$

$\sum_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}} \epsilon(\sigma) a'_{i\sigma(1)} a'_{2\sigma(2)} \dots a'_{i\sigma(i)} \dots a'_{n\sigma(n)}$

matricea care se obține din A prin înmulțirea liniei i cu elementul α . Deci avem $a'_{rj} = a_{rj}$ pentru $r \neq i$ și $j = 1, 2, \dots, n$ și $a'_{ij} = \alpha a_{ij}$ oricare ar fi $j = 1, 2, \dots, n$. Deci

$$\det A' = \sum_{\sigma \in S_n} \epsilon(\sigma) a'_{1\sigma(1)} a'_{2\sigma(2)} \dots a'_{i\sigma(i)} \dots a'_{n\sigma(n)} =$$

$$= \sum_{\sigma \in S_n} \epsilon(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \dots (\alpha a_{i\sigma(i)}) \dots a_{n\sigma(n)} =$$

$$= \alpha \sum_{\sigma \in S_n} \epsilon(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \dots a_{i\sigma(i)} \dots a_{n\sigma(n)} = \alpha \det A.$$

Deci $\det A' = \alpha \det A$.

Observație. Proprietatea 5 se transcrie și astfel (pentru linii):

$$\left| \begin{array}{cccc} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ \alpha a_{i1} & \alpha a_{i2} & \dots & \alpha a_{in} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{array} \right| = \alpha \left| \begin{array}{cccc} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{i1} & a_{i2} & \dots & a_{in} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{array} \right|$$

Exemplu. Fie matricea

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

Dacă înmulțim coloana 1 cu numărul $\alpha = -2$ obținem matricea

$$A' = \begin{pmatrix} -2 & 0 & 2 \\ -6 & 1 & -3 \\ -2 & -1 & 4 \end{pmatrix}$$

Aplicând proprietatea 5 avem $\det A' = -2 \cdot \det A$, lucru ce se poate verifica și direct aplicând regula lui Sarrus. Avem $\det A = -7$, $\det A' = 14$.

Proprietatea 6. Dacă elementele a două linii (sau coloane) ale unei matrice sunt proporționale, atunci determinantul matricei este nul.

Demonstrație. Fie matricea $A = (a_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$ în care liniile i și j sunt proporționale, adică există un element α astfel încât $a_{ji} = \alpha a_{ii}$ oricare ar fi $i = 1, 2, \dots, n$.

Aplicând proprietatea 5 rezultă că $\det A$ este produsul dintre elementul α și determinantul unei matrice care are două linii egale. Aplicând proprietatea 4 rezultă că $\det A$ este zero.

Exemplu. Fie matricea

$$A = \begin{pmatrix} 2 & 1 & 0 & 3 \\ -4 & 2 & -5 & 1 \\ 3 & 1 & 0 & -1 \\ -2 & 1 & -5 & 1 \\ & & 2 & 2 \end{pmatrix}.$$

Cum linia a 2-a și a 4-a a matricei A sunt proporționale, aplicind proprietatea 6, avem $\det A = 0$.

Proprietatea 7. Fie $A = (a_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$ o matrice pătratică de ordinul n . Presupunem că elementele liniei i sunt de forma $a_{ij} = a'_{ij} + a''_{ij}$, oricare ar fi $j = 1, 2, \dots, n$. Dacă A' (respectiv A'') este matricea care se obține din A înlocuind elementele de pe linia i cu elementele a'_{ij} (respectiv a''_{ij}), $j = 1, 2, \dots, n$, atunci

$$\det A = \det A' + \det A''.$$

Demonstrație. Avem:

$$\begin{aligned} \det A &= \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \dots a_{i\sigma(i)} \dots a_{n\sigma(n)} = \\ &= \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \dots (a'_{i\sigma(i)} + a''_{i\sigma(i)}) \dots a_{n\sigma(n)} = \\ &= \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \dots a'_{i\sigma(i)} \dots a_{n\sigma(n)} + \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{1\sigma(1)} \dots a''_{i\sigma(i)} \dots a_{n\sigma(n)} = \\ &= \det A' + \det A''. \end{aligned}$$

Observații. 1) Proprietatea 7 se transcrie și astfel:

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ a''_{11} + a'_{11}, a''_{12} + a'_{12}, \dots, a''_{1n} + a'_{1n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ a'_{11} & a'_{12} & \dots & a'_{1n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ a''_{11} & a''_{12} & \dots & a''_{1n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}$$

2) Folosind proprietatea 1 obținem pentru proprietatea 7 și varianta pe coloane, adică egalitatea:

$$\left| \begin{array}{cccc} a_{11} & a_{12} & \dots & a'_{1j} + a''_{1j} \dots a_{1n} \\ \dots & \dots & \dots & \dots \\ a_{21} & a_{22} & \dots & a'_{2j} + a''_{2j} \dots a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a'_{nj} + a''_{nj} \dots a_{nn} \end{array} \right| = \left| \begin{array}{cccc} a_{11} & a_{12} & \dots & a'_{1j} \dots a_{1n} \\ \dots & \dots & \dots & \dots \\ a_{21} & a_{22} & \dots & a'_{2j} \dots a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a'_{nj} \dots a_{nn} \end{array} \right| + \left| \begin{array}{cccc} a_{11} & a_{12} & \dots & a''_{1j} \dots a_{1n} \\ \dots & \dots & \dots & \dots \\ a_{21} & a_{22} & \dots & a''_{2j} \dots a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a''_{nj} \dots a_{nn} \end{array} \right|$$

Fie $A = (a_{ij})_{1 \leq i \leq n, 1 \leq j \leq n}$ o matrice pătratică. Vom spune că linia i a matricei A este o combinație liniară de celelalte linii, dacă există elementele α_j , $j = 1, 2, \dots, i-1, i+1, \dots, n$, astfel încât

$$a_{ij} = \alpha_1 a_{1j} + \alpha_2 a_{2j} + \dots + \alpha_{i-1} a_{i-1,j} + \alpha_{i+1} a_{i+1,j} + \dots + \alpha_n a_{nj}$$

oricare ar fi $j = 1, 2, \dots, n$. Asupra elementelor α_j nu se pune nici o condiție, în sensul că unele dintre ele pot fi și zero. Analog se poate defini ce înseamnă că o coloană j a matricei A este combinație liniară de celelalte coloane.

Exemplu. Fie matricea:

$$A = \begin{pmatrix} 2 & 1 & -1 \\ 3 & 3 & -5 \\ 1 & -1 & 3 \end{pmatrix}$$

Linia a 2-a a matricei A este combinație liniară de celelalte două linii. Într-adevăr, dacă considerăm numerele $\alpha_1=2$ și $\alpha_3=-1$ se observă că $3=2 \cdot 2 + (-1) \cdot 1$, $3=2 \cdot 1 + (-1) \cdot (-1)$, $-5=2 \cdot (-1) + (-1) \cdot 3$.

Proprietatea 8. Dacă o linie (sau coloană) a unei matrice pătratice este o combinație liniară de celelalte linii (sau coloane) atunci determinantul matricei este nul.

Demonstrație. Presupunem că linia i a matricei A este o combinație liniară de celelalte linii. Utilizând proprietatea 7, determinantul matricei A este o sumă de determinanți care au două linii proporționale, deci, după proprietatea 6, sunt zero toți acești determinanți. Prin urmare determinantul matricei A este zero.

Exemplu. Să considerăm din nou matricea de mai sus

$$A = \begin{pmatrix} 2 & 1 & -1 \\ 3 & 3 & -5 \\ 1 & -1 & 3 \end{pmatrix}$$

Cu linia a 2-a este o combinație liniară de celelalte două linii rezultă că $\det A = 0$.

Proprietatea 9. Dacă la o linie (sau coloană) a matricei A adunăm elementele altrei linii (sau coloane), înmulțite cu același element, atunci această matrice are același determinant ca și matricea A .

Demonstrație. Să presupunem că $A = (a_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$ și că la linia i adunăm elementele liniei j înmulțite cu elementul α . Obținem astfel o matrice A' care are aceleași linii ca matricea A , în afară de linia i , ale cărei elemente sunt

$$a_{ir} + \alpha a_{jr}, \quad r = 1, 2, \dots, n.$$

Folosind proprietatea 7, determinantul matricei A' este suma a doi determinanți dintre care unul este determinantul unei matrice care are două linii proporționale. Conform proprietății 6, acest al doilea determinant este nul. Prin urmare $\det A' = \det A$.

Observație. Proprietatea 9 se transcrie astfel (pentru linii):

$$\left| \begin{array}{cccc} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ a_{i1} + \alpha a_{j1} & a_{i2} + \alpha a_{j2} & \dots & a_{in} + \alpha a_{jn} \\ \dots & \dots & \dots & \dots \\ a_{j1} & a_{j2} & \dots & a_{jn} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{array} \right| = \left| \begin{array}{cccc} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ a_{i1} & a_{i2} & \dots & a_{in} \\ \dots & \dots & \dots & \dots \\ a_{j1} & a_{j2} & \dots & a_{jn} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{array} \right|$$

Observație. Se poate constata că proprietatea 8 extinde proprietatea 6 și că proprietățile 4 și 2 sunt cazuri particulare ale proprietății 6. Dar le-am dat datorită importanței lor și pentru o reținere mai bună.

§ 4. CALCULUL DETERMINANȚILOR

În cele ce urmează vom da un procedeu prin care calculul unui determinant de ordinul n se reduce la calculul unui anumit număr de determinanți de ordinul $n-1$.

Fie

$$d = \left| \begin{array}{cccc} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{array} \right|$$

un determinant de ordinul n . Determinantul de ordinul $n-1$ care se obține suprimind linia i și coloana j din determinantul d se numește *minorul elementului a_{ij}* și se notează cu d_{ij} . Elementul $\delta_{ij} = (-1)^{i+j} d_{ij}$ se numește *complementul algebric* al elementului a_{ij} în determinantul d . Evident, unui determinant de ordinul n îi se pot asocia n^2 minori de ordinul $n-1$ și respectiv n^2 complementi algebrici.

Exemplu. Fie determinantul de ordinul trei

$$d = \begin{vmatrix} 2 & 0 & 3 \\ 1 & 4 & -2 \\ 3 & 5 & -1 \end{vmatrix}.$$

Minori elementelor din d sunt în număr de 9. Aceștia sunt:

$$d_{11} = \begin{vmatrix} 4 & -2 \\ 5 & -1 \end{vmatrix} = -6; \quad d_{12} = \begin{vmatrix} 1 & -2 \\ 3 & -1 \end{vmatrix} = 5; \quad d_{13} = \begin{vmatrix} 1 & 4 \\ 3 & 5 \end{vmatrix} = -7$$

$$d_{21} = \begin{vmatrix} 0 & 3 \\ 5 & -1 \end{vmatrix} = -15; \quad d_{22} = \begin{vmatrix} 2 & 3 \\ 3 & -1 \end{vmatrix} = -11; \quad d_{23} = \begin{vmatrix} 2 & 0 \\ 3 & 5 \end{vmatrix} = 10$$

$$d_{31} = \begin{vmatrix} 0 & 3 \\ 4 & -2 \end{vmatrix} = -12; \quad d_{32} = \begin{vmatrix} 2 & 3 \\ 1 & -2 \end{vmatrix} = -7; \quad d_{33} = \begin{vmatrix} 2 & 0 \\ 1 & 4 \end{vmatrix} = 8.$$

Complementii algebrici ai elementelor din d sunt:

$$\delta_{11} = (-1)^{1+1} d_{11} = -6; \quad \delta_{12} = (-1)^{1+2} d_{12} = 5; \quad \delta_{13} = (-1)^{1+3} d_{13} = -7$$

$$\delta_{21} = (-1)^{2+1} d_{21} = 15; \quad \delta_{22} = (-1)^{2+2} d_{22} = -11; \quad \delta_{23} = (-1)^{2+3} d_{23} = -10$$

$$\delta_{31} = (-1)^{3+1} d_{31} = -12; \quad \delta_{32} = (-1)^{3+2} d_{32} = 7; \quad \delta_{33} = (-1)^{3+3} d_{33} = 8.$$

Teorema 4.1. Fie determinantul de ordinul n , $d = |a_{ij}|_{1 \leq i \leq n, 1 \leq j \leq n}$.

Atunci pentru orice $1 \leq i \leq n$, are loc egalitatea:

$$(1) \quad d = a_{1i}\delta_{1i} + a_{2i}\delta_{2i} + \dots + a_{ni}\delta_{ni}$$

Egalitatea (1) poartă denumirea de dezvoltarea determinantului după linia i .

Demonstrație. Vom nota cu S suma

$$(2) \quad S = a_{1i}\delta_{1i} + a_{2i}\delta_{2i} + \dots + a_{ni}\delta_{ni}.$$

Să considerăm termenul $a_{ij}\delta_{ij} = (-1)^{i+j} a_{ij}d_{ij}$ din suma (2). Să presupunem mai întâi că $i=j=1$. În acest caz un termen oarecare din dezvoltarea determinantului d_{11} de ordinul $n-1$ este de forma $a_{2k_1} \dots a_{nk_n}$, unde k_2, k_3, \dots, k_n sunt numerele $2, 3, \dots, n$ eventual ordine. Rezultă că termenul $a_{11}a_{2k_1}a_{3k_2} \dots a_{nk_n}$ este un termen al determinantului d . Semnul termenului $a_{2k_1}a_{3k_2} \dots a_{nk_n}$ provenit de dezvoltarea determinantului d_{11} este egal cu $(-1)^l$, unde l este de inversiuni ale permutării

$$\sigma = \begin{pmatrix} 2 & 3 \dots n \\ k_2 & k_3 \dots k_n \end{pmatrix}$$

Deci semnul termenului $a_{11}a_{2k_2}a_{3k_3} \dots a_{nk_n}$ provenit din produsul $a_{11}\delta_{11}$ este $(-1)^{1+1}(-1)^l = (-1)^l$.

Pe de altă parte semnul termenului $a_{11}a_{2k_2}a_{3k_3} \dots a_{nk_n}$ în dezvoltarea determinantului d este egal cu $(-1)^r$, unde r este numărul de inversiuni ale permutării

$$\tau = \begin{pmatrix} 1 & 2 & 3 \dots n \\ 1 & k_2 & k_3 \dots k_n \end{pmatrix}$$

Cum $k_2 > 1$, $k_3 > 1$, ..., $k_n > 1$, permutările σ și τ au același număr de inversiuni; deci $r = l$. Prin urmare termenul $a_{11}a_{2k_2}a_{3k_3} \dots a_{nk_n}$ provenit din produsul $a_{11}\delta_{11}$ are același semn cu cel provenit din dezvoltarea determinantului d .

Trecem la cazul general. Vom proceda în modul următor: vom schimba liniile și coloanele în aşa fel încit elementul a_{ij} să vină în locul elementului a_{11} și minorul d_{ij} să rămînă neschimbat. În acest fel linia i și coloana j devin linia 1 respectiv coloana 1; linia 1 devine linia 2, linia 2 devine linia 3, ..., linia $i-1$ devine linia i ; coloana 1 devine coloana 2, coloana 2 devine coloana 3, ..., coloana $j-1$ devine coloana j . Determinantul obținut prin aceste schimbări îl notăm cu d' . Aplicând proprietatea 3 a determinantelor, avem:

$$(3) \quad d = (-1)^{i+j}d'$$

În plus, $d'_{11} = d_{ij}$. Dacă $a_{1k_1}a_{2k_2} \dots a_{t-1k_{t-1}k_{t-1}}a_{t+1k_{t+1}} \dots a_{nk_n}$ este un termen oarecare din dezvoltarea determinantului d_{ij} , din egalitatea (3) și ținind seama de prima parte a demonstrației, rezultă că semnul termenului $(-1)^{t+j}a_{1k_1}a_{2k_2} \dots a_{t-1k_{t-1}}a_{tj}a_{t+1k_{t+1}} \dots a_{nk_n}$ provenit din produsul $a_{ij}d_{ij}$ este același cu cel dat de dezvoltarea determinantului d . În concluzie, fiecare termen din produsul $a_{ij}d_{ij}$ luat cu semnul său este un termen cu același semn, al determinantului d . Cum produsul $a_{ij}d_{ij}$ conține $(n-1)!$ termeni, atunci toți termenii care apar în suma (2) sunt în număr de $(n-1)!n = n!$. Deci în suma (2) se găsesc toți termenii (inclusiv semnul) determinantului d . Deci are loc egalitatea

Lema 4.2. Fie $d = |a_{ij}|_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$ un determinant de ordinul n .

$i \neq j$ are loc egalitatea

$$a_{i1}\delta_{j1} + a_{i2}\delta_{j2} + \dots + a_{in}\delta_{jn} = 0$$

Demonstrație. Considerăm determinantul

$$d' = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ a_{i1} & a_{i2} & \dots & a_{in} \\ \dots & \dots & \dots & \dots \\ a_{t1} & a_{t2} & \dots & a_{tn} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} \quad \begin{matrix} (i) \\ (j) \end{matrix}$$

care s-a obținut din d prin înlocuirea liniei j cu linia i . Cum d' are două linii egale, aplicând proprietatea 4 a determinanților, avem $d' = 0$. Dezvoltind determinantul d' după linia j (conform teoremei 1) obținem egalitatea căutată.

Din proprietatea 1 a determinanților și teorema 1 obținem

Teorema 4.3. Fie determinantul de ordinul n , $d = |a_{ij}|_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$.

Atunci pentru orice $1 \leq j \leq n$ are loc egalitatea:

$$(1') \quad d = a_{1j}\delta_{1j} + a_{2j}\delta_{2j} + \dots + a_{nj}\delta_{nj}$$

Egalitatea (1') poartă denumirea de dezvoltarea determinantului d după coloana j .

Corolarul 4.4. Fie $d = |a_{ij}|_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$ un determinant de ordinul n .

Pentru orice $i \neq j$ are loc egalitatea

$$a_{1j}\delta_{1i} + a_{2j}\delta_{2i} + \dots + a_{nj}\delta_{ni} = 0$$

Demonstrație. Se aplică proprietatea 1 a determinanților și consecința 1.

După cum se observă, teorema 4.1 și teorema 4.3 dau procedee prin care calculul unui determinant de ordinul n se reduce la calculul unui anumit număr de determinanțe de ordinul $n-1$. Pentru a simplifica calculele, în aplicații, vom face dezvoltarea unui determinant după acea linie sau coloană care are cel mai mare număr de elemente egale cu zero. Din aceste motive, la calculul unui determinant vom aplica sistematic cele 9 proprietăți ale determinanților pentru ca pe o anumită linie sau coloană să obținem cât mai multe elemente egale cu zero.

Exemplu. 1) Să calculăm determinantul de ordinul 4:

$$d = \begin{vmatrix} 1 & -1 & -2 & 3 \\ -2 & 1 & 0 & 5 \\ 4 & -3 & 1 & -6 \\ 2 & 1 & -1 & 0 \end{vmatrix}$$

Cum linia a 2-a conține un element nul, vom face dezvoltarea determinantului după linia a două:

$$d = (-1)^{2+1} \cdot (-2) \cdot \begin{vmatrix} -1 & -2 & 3 \\ -3 & 1 & -6 \\ 1 & -1 & 0 \end{vmatrix} + (-1)^{2+2} \cdot 1 \cdot \begin{vmatrix} 1 & -2 & 3 \\ 4 & 1 & -6 \\ 2 & -1 & 0 \end{vmatrix} + \\ + (-1)^{2+4} \cdot 5 \cdot \begin{vmatrix} 1 & -1 & -2 \\ 4 & -3 & 1 \\ 2 & 1 & -1 \end{vmatrix}.$$

Calculăm primul determinant de ordinul 3:

$$\begin{vmatrix} -1 & -2 & 3 \\ -3 & 1 & -6 \\ 1 & -1 & 0 \end{vmatrix} = \begin{vmatrix} -1 & -3 & 3 \\ -3 & -2 & -6 \\ 1 & 0 & 0 \end{vmatrix} = (-1)^{3+1} \cdot 1 \cdot \begin{vmatrix} -3 & 3 \\ -2 & -6 \end{vmatrix} = \\ = (-3) \cdot (-6) - (-2) \cdot 3 = 24$$

La calculul acestui determinant am procedat astfel: mai întii am adunat coloana 1 la coloana 2, apoi am dezvoltat determinantul după a 3-a linie:

$$\begin{vmatrix} 1 & -2 & 3 \\ 4 & 1 & -6 \\ 2 & -1 & 0 \end{vmatrix} = (-1)^{3+1} \cdot 2 \cdot \begin{vmatrix} -2 & 3 \\ 1 & -6 \end{vmatrix} + (-1)^{3+2} \cdot (-1) \cdot \begin{vmatrix} 1 & 3 \\ 4 & -6 \end{vmatrix} = \\ = 2 \cdot 9 + 1 \cdot (-18) = 0.$$

La calculul acestui determinant am făcut dezvoltarea determinantului după linia a 3-a:

$$\begin{vmatrix} 1 & -1 & -2 \\ 4 & -3 & 1 \\ 2 & +1 & -1 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 \\ 4 & 1 & 9 \\ 2 & 3 & 3 \end{vmatrix} = \begin{vmatrix} 1 & 9 \\ 3 & 3 \end{vmatrix} = -24.$$

La calculul acestui determinant am procedat astfel: mai întii am adunat coloana 1 la coloana 2, apoi am înmulțit coloana 1 cu 2 și am adunat-o la coloana 3. În final am dezvoltat determinantul după prima linie.

Deci valoarea determinantului d este:

$$d = 2 \cdot 24 + 1 \cdot 0 + 5 \cdot (-24) = 48 - 120 = -72.$$

2) Să calculăm determinantul de ordinul 4:

$$d = \begin{vmatrix} 1 & -2 & 5 & 9 \\ 4 & 1 & -3 & 0 \\ 12 & 0 & 7 & 8 \\ -5 & 1 & 2 & 0 \end{vmatrix}$$

Cum coloana a patra conține două elemente egale cu zero, vom face dezvoltarea după această coloană

$$d = (-1)^{1+4} \cdot 9 \begin{vmatrix} 4 & 1 & -3 \\ 12 & 0 & 7 \\ -5 & 1 & 2 \end{vmatrix} + (-1)^{3+4} \cdot 8 \begin{vmatrix} 1 & -2 & 5 \\ 4 & 1 & -3 \\ -5 & 1 & 2 \end{vmatrix}.$$

Calculăm primul determinant de ordinul 3:

$$\begin{vmatrix} 4 & 1 & -3 \\ 12 & 0 & 7 \\ -5 & 1 & 2 \end{vmatrix} = \begin{vmatrix} 4 & 1 & -3 \\ 12 & 1 & 7 \\ -9 & 0 & 5 \end{vmatrix} = - \begin{vmatrix} 12 & 7 \\ -9 & 5 \end{vmatrix} = -(60 + 63) = -123.$$

La calculul acestui determinant am procedat astfel: mai întii am înmulțit linia 1 cu (-1) și apoi am adunat-o la linia 3. În final am dezvoltat determinantul după coloana 2.

Calculăm al doilea determinant:

$$\begin{vmatrix} 1 & -2 & 5 \\ 4 & 1 & -3 \\ -5 & 1 & 2 \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 \\ 4 & 9 & -23 \\ -5 & -9 & 27 \end{vmatrix} = \begin{vmatrix} 9 & -23 \\ -9 & 27 \end{vmatrix} = 36.$$

La calculul acestui determinant am procedat astfel: mai întii am înmulțit coloana 1 cu 2 și am adunat-o la coloana 2; apoi am înmulțit coloana 1 cu -5 și am adunat-o la coloana 3. În final am făcut dezvoltarea determinantului după linia 1.

Valoarea determinantului d este:

$$d = (-1)^{1+4} \cdot 9 \cdot (-123) + (-1)^{3+4} \cdot 8 \cdot 36 = 1107 - 288 = 819.$$

5. FORMULA BINET-CAUCHY

DETERMINANTUL PRODUSULUI A DOUĂ MATRICE

Fie m și n două numere naturale nenule astfel încât $m \leq n$, iar R un inel comutativ. Ca de obicei, notăm prin $\mathcal{M}(m, n, R)$ (respectiv $\mathcal{M}(n, m, R)$) mulțimea matricelor cu m linii și n coloane (respectiv cu

n linii și m coloane) peste inelul R . Fie acum $A = (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} \in \mathcal{M}(m, n, R)$ (respectiv $B = (b_{kj})_{\substack{1 \leq k \leq m \\ 1 \leq j \leq n}} \in \mathcal{M}(n, m, R)$). Pentru orice $k_1, \dots, k_m \in \{1, \dots, n\}$ nu neapărat distinge notăm cu A_{k_1, \dots, k_m} (respectiv B^{k_1, \dots, k_m}) matricea pătrată de ordinul m avind m coloane (respectiv m linii), egale în ordine cu coloanele (respectiv liniile) de indici k_1, \dots, k_m ale matricei A (respectiv B). Să considerăm $k_1, \dots, k_m \in \{1, \dots, n\}$ cu $k_i \neq k_j$, pentru $i \neq j$ și fie j_1, \dots, j_m o rearanjare a elementelor k_1, \dots, k_m astfel încât $j_1 < j_2 < \dots < j_m$. Atunci există o unică permutare $\tau \in S_m$ astfel încât $k_i = j_{\tau(i)}$.

Din proprietățile determinanților rezultă că:

$$\det A_{k_1, \dots, k_m} = \varepsilon(\tau) \det A_{j_1, \dots, j_m} \text{ și}$$

$$\det B^{k_1, \dots, k_m} = \varepsilon(\tau) \det B^{j_1, \dots, j_m}$$

Pe de altă parte, din definiția determinantului avem că

$$\det A_{k_1, \dots, k_m} = \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{1k_{\sigma(1)}} a_{2k_{\sigma(2)}} \dots a_{mk_{\sigma(m)}} = \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{\sigma(1)k_1} a_{\sigma(2)k_2} \dots a_{\sigma(m)k_m}$$

O relație analoagă avem și pentru B^{k_1, \dots, k_m} , adică

$$\det B^{k_1, \dots, k_m} = \sum_{\sigma \in S_n} \varepsilon(\sigma) b_{k_{\sigma(1)}1} b_{k_{\sigma(2)}2} \dots b_{k_m \sigma(m)}$$

Cu notațiile introduse mai sus avem

Teorema 5.1. (Formula Binet-Cauchy). *Fie m, n numere naturale nenule cu $m \leq n$. Atunci pentru orice două matrice $A \in \mathcal{M}(m, n, R)$ și $B \in \mathcal{M}(n, m, R)$ are loc egalitatea:*

$$\det(AB) = \sum_{1 \leq j_1 < \dots < j_m \leq n} \det A_{j_1, \dots, j_m} \cdot \det B^{j_1, \dots, j_m}.$$

Demonstrație. Fie $C = AB \in \mathcal{M}(m, m, R)$, adică $C = (c_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq m}}$.

Aplicind definiția determinantului matricei C , avem:

$$\begin{aligned} \det C &= \sum_{\sigma \in S_m} \varepsilon(\sigma) c_{1\sigma(1)} c_{2\sigma(2)} \dots c_{m\sigma(m)} = \\ &= \sum_{\sigma \in S_m} \varepsilon(\sigma) \left(\sum_{k_1=1}^n a_{1k_1 \sigma(1)} b_{k_1 \sigma(1)} \right) \dots \left(\sum_{k_m=1}^n a_{mk_m} b_{k_m \sigma(m)} \right) = \sum_{k_1, \dots, k_m \in \{1, 2, \dots, n\}} a_{1k_1} \dots a_{mk_m} \cdot \\ &\quad \sum_{\sigma \in S_m} \varepsilon(\sigma) b_{k_1 \sigma(1)} \dots b_{k_m \sigma(m)} = \sum_{k_1, \dots, k_m \in \{1, \dots, n\}} a_{1k_1} \dots a_{mk_m} \cdot \det B^{k_1, \dots, k_m} = \\ &= \sum_{\substack{k_1, \dots, k_m \in \{1, \dots, n\} \\ k_i \neq k_j \text{ pt. } i \neq j}} a_{1k_1} \dots a_{mk_m} \cdot \det B^{k_1, \dots, k_m} \end{aligned}$$

Am folosit faptul că determinantul unei matrice cu două linii identice este nul.

Grupind termenii cu $\{k_1, \dots, k_m\} = \{j_1, \dots, j_m\}$ pentru $1 \leq j_1 < \dots < j_m \leq n$ arbitrar fixați, obținem:

$$\sum_{\substack{k_1, \dots, k_m \in \{1, \dots, n\} \\ k_i \neq k_j \text{ pt. } i \neq j}} a_{1k_1} \dots a_{mk_m} \det B^{k_1 \dots k_m} = \sum_{1 \leq j_1 < \dots < j_m \leq n} \det B^{j_1 \dots j_m}.$$

$$\cdot \sum_{\tau \in S_m} \varepsilon(\tau) a_{1j_{\tau(1)}} \dots a_{mj_{\tau(m)}} = \sum_{1 \leq j_1 < \dots < j_m \leq n} \det B^{j_1 \dots j_m} \cdot \det A_{j_1 \dots j_m}$$

$$\text{Deci } \det(AB) = \sum_{1 \leq j_1 < \dots < j_m \leq n} \det A_{j_1 \dots j_m} \cdot \det B^{j_1 \dots j_m}$$

ceea ce trebuia demonstrat.

Corolarul 5.2. Fie n un număr natural nenul. Atunci pentru orice două matrice $A, B \in \mathcal{M}_n(R)$ are loc egalitatea:

$$\det(AB) = \det(A) \det(B).$$

Demonstrație. Se obține imediat din formula Binet-Cauchy pentru $m=n$.

Corolarul 5.3. Fie R un inel comutativ și $a_1, a_2, \dots, a_n, b_1, b_2, \dots, b_n \in R$. Atunci are loc identitatea:

$$(a_1^2 + a_2^2 + \dots + a_n^2)(b_1^2 + b_2^2 + \dots + b_n^2) - (a_1b_1 + a_2b_2 + \dots + a_nb_n)^2 = \\ = \sum_{1 \leq i < j \leq n} (a_i b_j - b_i a_j)^2.$$

Demonstrație. Considerăm matricea $A = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ b_1 & b_2 & \dots & b_n \end{pmatrix}$

Dacă $B = A^t$ este transpusa matricei A , atunci:

$$A \cdot A^t = \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix}$$

unde

$$c_{11} = a_1^2 + \dots + a_n^2, \quad c_{22} = b_1^2 + \dots + b_n^2,$$

$$c_{12} = c_{21} = a_1b_1 + a_2b_2 + \dots + a_nb_n$$

deci

$$\det(A^t A) = c_{11}c_{22} - c_{12}c_{21} = (a_1^2 + a_2^2 + \dots + a_n^2)(b_1^2 + b_2^2 + \dots + b_n^2) - \\ - (a_1b_1 + \dots + a_nb_n)^2.$$

Dacă $1 \leq i < j \leq n$, atunci

$$A_{i,j} = \begin{pmatrix} a_i & a_j \\ b_i & b_j \end{pmatrix} \text{ și } B^{i,j} = \begin{pmatrix} a_i & b_i \\ a_j & b_j \end{pmatrix}$$

și deci $\det A_{i,j} = a_i b_j - a_j b_i$ și $\det B^{i,j} = a_i b_j - a_j b_i$.

Aplicînd acum formula Binet-Cauchy, obținem identitatea din corolarul 5.3.

Observație. Dacă $a_1, a_2, \dots, a_n; b_1, b_2, \dots, b_n$ sunt numere reale, din corolarul 5.3 obținem bine cunoscuta inegalitate a lui Cauchy-Bouniakovski:

$$\left(\sum_{i=1}^n a_i b_i \right)^2 \leq \sum_{i=1}^n a_i^2 \cdot \sum_{i=1}^n b_i^2$$

§ 6. DEFINIREA DETERMINANTULUI UNEI MATRICE PRIN INDUȚIE

Am văzut în §1 că formula determinanților de ordinul 2 și 3 are o formă simplă, adică

$$(1) \quad \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}$$

$$(2) \quad \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} = a_{11} \begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix} - a_{12} \begin{vmatrix} a_{21} & a_{23} \\ a_{31} & a_{33} \end{vmatrix} + a_{13} \begin{vmatrix} a_{21} & a_{22} \\ a_{31} & a_{32} \end{vmatrix}$$

Formula acestor determinanțăi, dar mai ales a celui de ordinul 3, ne sugerează că putem defini determinantul de ordinul n prin inducție și anume pentru $n=1$ și $n=2$ avem definit determinantul de ordinul 2 (respectiv 3) prin formulele (1) (și respectiv (2)). Presupunem că este definit determinantul pentru orice matrice de ordinul $n-1$. Atunci punem ca determinantul de ordinul n să fie egal cu

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} = a_{11}D_1 - a_{12}D_2 + a_{13}D_3 - \dots + (-1)^{n-1}a_{1n}D_n$$

unde D_k este determinantul matricei de ordinul $(n-1) \times (n-1)$

$$\begin{pmatrix} a_{21} & \dots & a_{2, k-1} & a_{2, k+1} & \dots & a_{2n} \\ \vdots & & \vdots & & \vdots & \\ a_{n1} & \dots & a_{n, k-1} & a_{n, k+1} & \dots & a_{nn} \end{pmatrix}$$

adică submatricea matricei inițiale din care am scos prima linie și coloana „ k ”.

Problema care se pune este de a arăta că modul în care am definit determinantul de ordinul n , coincide cu definiția determinantului dată în § 2.

Pentru aceasta este comod să introducem cîteva noțiuni preliminare.

Definiția 6.1. Fie R un inel comutativ, E și F două R -module.

O aplicație $\varphi: E^n \rightarrow F$ se numește multiliniară dacă pentru orice $i=1, \dots, n$ și pentru orice $\lambda, \mu \in R$, $x_1, \dots, x_i, x'_i, \dots, x_n \in E$ să avem

$$\varphi(x_1, \dots, \lambda x_i + \mu x'_i, \dots, x_n) = \lambda \varphi(x_1, \dots, x_i, \dots, x_n) + \mu \varphi(x_1, \dots, x'_i, \dots, x_n)$$

Dacă $F=R$, atunci φ se numește formă n -lineară pe E .

Dacă $n=2$, φ se numește aplicație biliniară (respectiv formă biliniară). Dacă în plus aplicația multiliniară φ are proprietatea că $\varphi(x_1, \dots, x_i, x_{i+1}, \dots, x_n) = 0$ ori de câte ori $x_i = x_{i+1}$, atunci φ se numește multiliniară și alternată.

În continuare vom da cele mai importante proprietăți ale aplicațiilor multiliniare și alternate:

Teorema 6.2. Fie $\varphi: E^n \rightarrow F$ o aplicație multiliniară și alternată. Atunci au loc următoarele afirmații:

$$1) \text{ Dacă } i < j, \text{ atunci } \varphi(x_1, \dots, x_i, \dots, x_j, \dots, x_n) = -\varphi(x_1, \dots, x_j, \dots, x_i, \dots, x_n)$$

$$2) \text{ Dacă } x_i = x_j \text{ (} i \neq j \text{), atunci } \varphi(x_1, \dots, x_n) = 0.$$

$$3) \text{ Dacă } a \in R, \text{ atunci } \varphi(x_1, \dots, x_i + ax_j, \dots, x_r, \dots, x_n) = \\ = \varphi(x_1, \dots, x_i, \dots, x_j, \dots, x_n).$$

$$4) \text{ Dacă } \sigma \in S_n, \text{ atunci}$$

$$\varphi(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = \varepsilon(\sigma) \varphi(x_1, \dots, x_n).$$

5) Fie matricea $A = (a_{ij})_{1 \leq i, j \leq n}$ și elementele $e_1, e_2, \dots, e_n \in E$. Dacă definim elementele

$$f_i = \sum_{j=1}^n a_{ij} e_j \text{ și } g_i = \sum_{j=1}^n a_{ji} e_j \text{ cu } i = 1, \dots, n, \text{ atunci } \varphi(f_1, f_2, \dots, f_n) = \\ = \varphi(g_1, g_2, \dots, g_n) = \det(A) \varphi(e_1, e_2, \dots, e_n).$$

Demonstrație. 1) Cum $i < j$, putem scrie $j = i + k$ cu $k \geq 1$. Vom face inducție după k . Dacă $k=1$, atunci $j=i+1$ și atunci

$$\varphi(x_1, \dots, x_i + x_{i+1}, x_i + x_{i+1}, \dots, x_n) = 0.$$

Cum φ este multiliniară obținem egalitatea

$$0 = \varphi(x_1, \dots, x_i, x_i, \dots, x_n) + \varphi(x_1, \dots, x_i, x_{i+1}, \dots, x_n) + \\ + \varphi(x_1, \dots, x_{i+1}, x_i, \dots, x_n) + \varphi(x_1, \dots, x_{i+1}, x_{i+1}, \dots, x_n)$$

și aplicând din nou faptul că φ este și alternată obținem

$$\varphi(x_1, \dots, x_i, x_{i+1}, \dots, x_n) + \varphi(x_1, \dots, x_{i+1}, x_i, \dots, x_n) = 0$$

dе unde

$$\varphi(x_1, \dots, x_i, x_{i+1}, \dots, x_n) = -\varphi(x_1, \dots, x_{i+1}, x_i, \dots, x_n).$$

Presupunem afirmația adevărată pentru $k-1$ și o demonstrăm pentru k .

Avem succesiv:

$$\begin{aligned} \varphi(x_1, \dots, x_i, \dots, x_j, \dots, x_n) &= -\varphi(x_1, \dots, x_i, \dots, x_j, x_{j-1}, \dots, x_n) = \\ &\equiv -(-\varphi(x_1, \dots, x_i, \dots, x_i, x_{j-1}, \dots, x_n)) = -(-(-\varphi(x_1, \dots, x_j, \dots, x_i, \dots, \\ &\dots, x_n))) = -\varphi(x_1, \dots, x_j, \dots, x_i, \dots, x_n). \end{aligned}$$

2) Presupunem $i < j$. Atunci aplicând proprietatea 1) avem

$$\varphi(x_1, \dots, x_i, \dots, x_j, \dots, x_n) = -\varphi(x_1, \dots, x_{j-1}, \dots, x_i, x_j, \dots, x_n) = 0.$$

3) Se aplică faptul că φ este multiliniară și 2).

4) Permutarea σ este un produs de transpoziții. Înind cont că $\epsilon(\sigma) = \epsilon(\tau_1) \dots \epsilon(\tau_k)$, atunci în mod evident ne putem reduce la cazul cind $k=1$, adică σ este o transpoziție.

Dar în acest caz afirmația noastră rezultă din 2).

5) Avem

$$\varphi(f_1, \dots, f_n) = \varphi\left(\sum_{j=1}^n a_{1j}e_j, \dots, \sum_{j=1}^n a_{nj}e_j\right) = \sum_{1 \leq i_1, \dots, i_n \leq n} a_{1i_1}a_{2i_2} \dots a_{ni_n} \varphi(e_{i_1}, \dots, e_{i_n}).$$

Considerăm funcția $\sigma: \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ astfel încit $\sigma(k) = i_k$. Atunci

$$\begin{aligned} \varphi(f_1, f_2, \dots, f_n) &= \sum_{\sigma: \{1, \dots, n\} \rightarrow \{1, \dots, n\}} a_{1\sigma(1)}a_{2\sigma(2)} \dots a_{n\sigma(n)} \cdot \varphi(e_{\sigma(1)}, \dots, e_{\sigma(n)}) = \\ &= \sum_{\sigma \in S_n} a_{1\sigma(1)} \dots a_{n\sigma(n)} \varphi(e_{\sigma(1)}, \dots, e_{\sigma(n)}) + \sum_{\substack{\sigma: \{1, \dots, n\} \rightarrow \{1, \dots, n\} \\ \sigma \text{ nu este injectivă}}} a_{1\sigma(1)} \dots a_{n\sigma(n)} \varphi(e_{\sigma(1)}, \dots, e_{\sigma(n)}). \end{aligned}$$

Dacă $\sigma: \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ este neinjectivă, există $k \neq l$ astfel încit $\sigma(k) = \sigma(l)$ și deci $e_{\sigma(k)} = e_{\sigma(l)}$.

Cum φ este alternată, atunci $\varphi(e_{\sigma(1)}, \dots, e_{\sigma(n)}) = 0$. Deci

$$\begin{aligned}\varphi(f_1, \dots, f_n) &= \sum_{\sigma \in S_n} a_{1\sigma(1)} \dots a_{n\sigma(n)} \varphi(e_{\sigma(1)}, \dots, e_{\sigma(n)}) = \\ &= \sum_{\sigma \in S_n} \varepsilon(\sigma) a_{1\sigma(1)} \dots a_{n\sigma(n)} \varphi(e_1, \dots, e_n) = \det A \cdot \varphi(e_1, \dots, e_n).\end{aligned}$$

Analog se arată egalitatea

$$\varphi(g_1, \dots, g_n) = \det(A) \varphi(e_1, \dots, e_n)$$

(aici se ține cont de proprietatea 1 a determinanților).

Fie R un inel comutativ. Notăm $E = M(n, 1, R)$ adică

$$E = \left\{ \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}, a_i \in R \right\}$$

Este evident că E este un R -modul liber cu baza

$$\xi^1 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \xi^2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \dots, \xi^n = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$$

Dacă $A = (a_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$ este o matrice pătratică de ordinul n , vom nota cu A^1, A^2, \dots, A^n coloanele acestei matrice. Evident, $A^1, \dots, A^n \in E$.

Corolarul 6.3. Fie φ o formă multiliniară și alternată $\varphi: E^n \rightarrow R$ astfel încât $\varphi(\xi^1, \dots, \xi^n) = 1$. Dacă $A = (a_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$ este o matrice pătratică de ordinul n , atunci

$$\varphi(A^1, \dots, A^n) = \det A.$$

Demonstrație. Cum $A^i = \sum_{j=1}^n a_{ij} \xi^j$, atunci din propoziția precedentă obținem că

$$\varphi(A^1, \dots, A^n) = \det A \varphi(\xi^1, \dots, \xi^n) = \det A.$$

Teorema 6.4. (Teorema fundamentală a teoriei determinanților).

Fie $E \in M(n, 1, R)$. Atunci există o unică formă multiliniară și alternată $\varphi_n: E^n \rightarrow R$ astfel încă $\varphi_n(\xi^1, \dots, \xi^n) = 1$.

Demonstrație. Fie $A^1, \dots, A^n \in E$. Putem forma matricea pătratică $A = (A^1, A^2, \dots, A^n)$ care are coloanele A^1, A^2, \dots, A^n . Dacă $\varphi_n, \varphi_n: E^n \rightarrow R$ sunt două forme multiliniare alternate cu proprietatea $\varphi_n(\xi^1, \dots, \xi^n) =$

$\Rightarrow \varphi'_n(\xi^1, \dots, \xi^n)$ avem din teorema 6.2 că $\varphi_n(A^1, \dots, A^n) = \varphi'_n(A^1, \dots, A^n) = \det A$ și deci $\varphi_n = \varphi'_n$.

În continuare vom arăta existența lui $\varphi_n: E^n \rightarrow R$. Procedăm prin inducție după n . Dacă $n=1$, atunci $E=\{(a), a \in R\}$, $\xi^1=1$ și punem $\varphi_1((a))=a$. Presupunem construită $\varphi_{n-1}: F^{n-1} \rightarrow R$, unde $F=M(n-1, 1, R)$ cu proprietatea din enunțul teoremei.

Fie acum $A^1, \dots, A^n \in E$ și $A=(A^1, \dots, A^n)$ matricea pătratică având coloanele A^1, \dots, A^n .

Presupunem că $A^i = \begin{pmatrix} a_{1i} \\ a_{2i} \\ \vdots \\ a_{ni} \end{pmatrix}$ unde $i=1, \dots, n$.

În acest caz $A=(a_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$. Dacă A_{ij} este matricea obținută din A eliminind linia i și coloana j , punem prin definiție:

$$\varphi_n(A^1, \dots, A^n) = \sum_{j=1}^n (-1)^{i+j} a_{ij} \varphi_{n-1}(A_{ij}^1, \dots, A_{ij}^{n-1}). \quad (3)$$

Se observă că

$$\varphi_n(\xi^1, \dots, \xi^n) = (-1)^{i+1} a_{ii} \varphi_{n-1}(A_{ii}^1, \dots, A_{ii}^{n-1}) = 1,$$

deoarece $a_{ii}=1$ și $\varphi_{n-1}(A_{ii}^1, \dots, A_{ii}^{n-1})=1$, conform ipotezei de inducție. Să dovedim că φ_n este multilineară. Mai întâi vom arăta că

$$\begin{aligned} \varphi_n(A^1, \dots, A^k + A'^k, \dots, A^n) &= \varphi_n(A^1, \dots, A^k, \dots, A_n) + \\ &\quad + \varphi_n(A^1, \dots, A'^k, \dots, A^n). \end{aligned}$$

Presupunem $A'^k = \begin{pmatrix} a'_{11} \\ \vdots \\ a'_{nn} \end{pmatrix}$ și să fie $A=(A^1, \dots, A^k, \dots, A^n)=(a_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$ și $A'=(A^1, \dots, A'^k, \dots, A^n)=(a'_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$, unde $a'_{ij}=a_{ij}$ pentru $j \neq k$.

Fie matricea $B=(B^1, \dots, B^k, \dots, B^n)=(b_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$, unde $B^i=A^i$ pentru $i \neq k$ și $B^k=A^k+A'^k$. Deci $b_{ij}=a_{ij}=a'_{ij}$ pentru $j \neq k$ și $b_{ik}=a_{ik}+a'_{ik}$.

Aveam

$$\begin{aligned} \varphi_n(A^1, \dots, A^k + A'^k, \dots, A^n) &= \sum_{i=1}^n (-1)^{i+k} b_{ik} \varphi_{n-1}(B_{ik}^1, \dots, B_{ik}^{n-1}) = \\ &= \sum_{\substack{i=1 \\ i \neq k}}^n (-1)^{i+k} b_{ik} \varphi_{n-1}(B_{ik}^1, \dots, B_{ik}^{n-1}) + (-1)^{i+k} b_{ik} \varphi_{n-1}(B_{ik}^1, \dots, B_{ik}^{n-1}) \end{aligned}$$

Dacă $j \neq k$, avem

$$\varphi_{n-1}(B_{ij}^1, \dots, B_{ij}^{n-1}) = \varphi_{n-1}(A_{ij}^1, \dots, A_{ij}^{n-1}) + \varphi_{n-1}(A_{ij}^1, \dots, A_{ij}^{n-1})$$

Dacă $j=k$, obținem

$$\varphi_{n-1}(B_{ii}^1, \dots, B_{ii}^{n-1}) = \varphi_{n-1}(A_{ii}^1, \dots, A_{ii}^{n-1}) = \varphi_{n-1}(A_{ii}^1, \dots, A_{ii}^{n-1}).$$

Deci

$$\begin{aligned} \varphi_n(A^1, \dots, A^k + A'^k, \dots, A^n) &= \sum_{\substack{j=1 \\ j \neq k}}^n (-1)^{t+j} a_{ij} \varphi_{n-1}(A_{ij}^1, \dots, A_{ij}^{n-1}) + \\ &+ \sum_{\substack{j=1 \\ j \neq k}}^n (-1)^{t+j} a'_{ij} \varphi_{n-1}(A_{ij}^1, A_{ij}^{n-1}) + (-1)^{t+k} a_{kk} \varphi_{n-1}(A_{kk}^1, \dots, A_{kk}^{n-1}) + \\ &+ (-1)^{t+k} a'_{kk} \varphi_{n-1}(A_{kk}^1, \dots, A_{kk}^{n-1}). \end{aligned}$$

Grupând convenabil obținem că

$$\varphi_n(A^1, \dots, A^k + A'^k, \dots, A^n) = \varphi_n(A^1, \dots, A^k, \dots, A^n) + \varphi^n A^1, \dots, A'^k, \dots, A^n)$$

În mod similar se arată că

$$\varphi_n(A^1, \dots, \lambda A^k, \dots, A^n) = \lambda \varphi_n(A^1, \dots, A^k, \dots, A^n).$$

Să dovedim că φ_n este alternată. Presupunem că $A^k = A'^{k+1}$. Deci $a_{ik} = a_{i(k+1)}$ oricare ar fi $i = 1, \dots, n$.

Aveam

$$\begin{aligned} \varphi_n(A^1, \dots, A^n) &= \sum_{j=1}^n (-1)^{t+j} a_{ij} \varphi_{n-1}(A_{ij}^1, \dots, A_{ij}^{n-1}) = \\ &= \sum_{\substack{j=1 \\ j \neq k, k+1}}^n (-1)^{t+j} a_{ij} \varphi_{n-1}(A_{ij}^1, \dots, A_{ij}^{n-1}) + (-1)^{t+k} a_{ik} \varphi_{n-1}(A_{ik}^1, \dots, A_{ik}^{n-1}) + \\ &\quad + (-1)^{t+k+1} a_{i(k+1)} \varphi_{n-1}(A_{i(k+1)}^1, \dots, A_{i(k+1)}^{n-1}) \end{aligned}$$

Deoarece $A^k = A'^{k+1}$ și $j \neq k, k+1$ avem $\varphi_{n-1}(A_{ij}^1, \dots, A_{ij}^{n-1}) = 0$

intrucât două componente consecutive din sirul $A_{ij}^1, \dots, A_{ij}^{n-1}$ sunt egale).

Pe de altă parte, se observă imediat că

$$\varphi_{n-1}(A_{ik}^1, \dots, A_{ik}^{n-1}) = \varphi_{n-1}(A_{ik+1}^1, \dots, A_{ik+1}^{n-1})$$

și deci

$$\varphi_n(A^1, \dots, A^n) = ((-1)^{t+k} a_{ik} + (-1)^{t+k+1} a_{i(k+1)}) \varphi_{n-1}(A_{ik}^1, \dots, A_{ik}^{n-1}) = 0$$

deoarece $a_{ik} = a_{i(k+1)}$ și $(-1)^{t+k+1} = -(-1)^{t+k}$.

Corolarul 6.5. Dacă $A = (a_{ij})_{1 \leq i, j \leq n}$ este o matrice pătratică de ordinul n , atunci

$$\det A = \sum_{j=1}^n (-1)^{i+j} a_{ij} \cdot \det (A_{ij}),$$

unde A_{ij} este matricea care se obține din A eliminând linia i și coloana j .

Demonstrație. Se ține cont de definiția lui φ_n și de corolarul 6.3.

Observații. 1) Pentru $i=1$ obținem dezvoltarea determinantului după prima linie așa cum am dat-o la începutul acestui paragraf.

2) Din teorema 6.4, ținând cont de proprietățile aplicațiilor multipliare și alternate, obținem toate proprietățile determinanților.

Folosind funcția φ_n ne propunem să demonstrăm și

Teorema 6.6. Fie $A, B \in \mathcal{M}(n, R)$. Atunci $\det (AB) = \det A \cdot \det B$.

Demonstrație. Fie $A = (a_{ij})_{1 \leq i, j \leq n}$, $B = (b_{ij})_{1 \leq i, j \leq n}$. Fie $e_i = \sum_{j=1}^n b_{ij} \xi^j$ și $f_i = \sum_{j=1}^n a_{ij} e_j$, $i = 1, \dots, n$. Deci $e_1, e_2, \dots, e_n; f_1, \dots, f_n \in E = \mathcal{M}(n, 1, R)$.

Se observă imediat că:

$$\begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix} = B \begin{pmatrix} \xi^1 \\ \vdots \\ \xi^n \end{pmatrix}; \quad \begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix} = A \begin{pmatrix} e_1 \\ \vdots \\ e_n \end{pmatrix}$$

Deci

$$\begin{pmatrix} f_1 \\ \vdots \\ f_n \end{pmatrix} = A \cdot (B \begin{pmatrix} \xi^1 \\ \vdots \\ \xi^n \end{pmatrix}) = (AB) \begin{pmatrix} \xi^1 \\ \vdots \\ \xi^n \end{pmatrix}.$$

Din teorema 6.2 avem

$$\varphi_n(f_1, \dots, f_n) = \det(AB) \varphi_n(\xi^1, \dots, \xi^n) = \det(AB).$$

Pe de altă parte,

$$\begin{aligned} \varphi_n(f_1, \dots, f_n) &= \det A \cdot \varphi_n(e_1, \dots, e_n) = \\ &= \det A (\det B \cdot \varphi_n(\xi^1, \dots, \xi^n)) = \det A \cdot \det B. \end{aligned}$$

Deci $\det(AB) = \det A \cdot \det B$.

§ 7. MATRICE INVERSABILE. INVERSA UNEI MATRICE. REGULA LUI CRAMER

Fie R un inel comutativ. Vom considera $\mathcal{M}(n, R)$ inelul matricelor pătratice de ordinul n . O matrice $A \in \mathcal{M}(n, R)$ se numește inversabilă

dacă este inversabilă ca element în inelul $\mathcal{M}(n, R)$, adică există o matrice $B \in \mathcal{M}(n, R)$ (care este unică) astfel încit $AB = BA = I_n$. Matricea B , dacă există, se notează cu A^{-1} și se numește inversa matricei A .

Teorema 7.1. Fie $A = (a_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}} \in \mathcal{M}(n, R)$. Atunci A este inversabilă dacă și numai dacă $\det(A)$ este un element inversabil în inelul R .

În acest caz $A^{-1} = (a_{ij}^*)_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$, unde $a_{ij}^* = (-1)^{i+j} d^{-1} d_{ji}$, unde $d = \det A$ și d_{ji} este minorul elementului a_{ji} .

Demonstrație. Presupunem că A este inversabilă. Există $B \in \mathcal{M}(n, R)$ astfel încit $AB = BA = I_n$. În acest caz avem $\det(AB) = \det I_n = 1$ sau $\det A \cdot \det B = 1$ ceea ce arată că $\det A$ este un element inversabil în R .

Invers, presupunem că $d = \det A$ este inversabil în R . Să notăm

$$A^* = (a_{ij}^*)_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}} \text{ și } AA^* = B = (b_{ij})_{1 \leq i, j \leq n}. \text{ Deci } b_{ij} = \sum_{k=1}^n a_{ik} a_{kj}^* =$$

$$= \sum_{k=1}^n a_{ik} (-1)^{k+j} d^{-1} d_{jk} = d^{-1} \sum_{k=1}^n (-1)^{k+j} a_{ik} d_{jk}.$$

Dacă $j = i$, atunci din teorema 4.1 obținem că $b_{ii} = dd^{-1} = 1$.

Dacă $j \neq i$, din corolarul 4.2 obținem că $b_{ij} = 0$. Deci $B = I_n$, adică $AA^* = I_n$. Analog se arată că $AA^* = I_n$.

Exemplu. Să se calculeze inversa matricei

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ -1 & 2 & 1 \end{pmatrix}, \det A = d = \begin{vmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ -1 & 2 & 1 \end{vmatrix} = -4 \neq 0.$$

$$A^{-1} = \begin{pmatrix} a_{11}^* & a_{12}^* & a_{13}^* \\ a_{21}^* & a_{22}^* & a_{23}^* \\ a_{31}^* & a_{32}^* & a_{33}^* \end{pmatrix},$$

unde

$$a_{11}^* = (-1)^{1+1} d^{-1} \cdot d_{11}, \quad d_{11} = \begin{vmatrix} 1 & 2 \\ 2 & 1 \end{vmatrix} = 1 - 4 = -3,$$

$$a_{12}^* = (-1)^{1+2} d^{-1} \cdot d_{21}, \quad d_{21} = \begin{vmatrix} 2 & 3 \\ 2 & 1 \end{vmatrix} = 2 - 6 = -4,$$

$$a_{13}^* = (-1)^{1+3} d^{-1} \cdot d_{31}, \quad d_{31} = \begin{vmatrix} 2 & 3 \\ 1 & 2 \end{vmatrix} = 4 - 3 = 1,$$

$$a_{21}^* = (-1)^{2+1} d^{-1} \cdot d_{12}, \quad d_{12} = \begin{vmatrix} 0 & 2 \\ -1 & 1 \end{vmatrix} = 2,$$

$$a_{22}^* = (-1)^{2+2} d^{-1} \cdot d_{22}, \quad d_{22} = \begin{vmatrix} 1 & 3 \\ -1 & 1 \end{vmatrix} = 1 + 3 = 4,$$

$$a_{23}^* = (-1)^{2+3} d^{-1} \cdot d_{32}, \quad d_{32} = \begin{vmatrix} 1 & 3 \\ 0 & 2 \end{vmatrix} = 2,$$

$$a_{31}^* = (-1)^{3+1} d^{-1} \cdot d_{13}, \quad d_{13} = \begin{vmatrix} 0 & 1 \\ -1 & 2 \end{vmatrix} = 1,$$

$$a_{32}^* = (-1)^{3+2} d^{-1} \cdot d_{23}, \quad d_{23} = \begin{vmatrix} 1 & 2 \\ -1 & 2 \end{vmatrix} = 2 + 2 = 4,$$

$$a_{33}^* = (-1)^{3+3} d^{-1} \cdot d_{33}, \quad d_{33} = \begin{vmatrix} 1 & 2 \\ 0 & 1 \end{vmatrix} = 1,$$

deci

$$a_{11}^* = \frac{3}{4}, \quad a_{12}^* = -\frac{4}{4} = -1, \quad a_{13}^* = -\frac{1}{4},$$

$$a_{21}^* = \frac{2}{4} = \frac{1}{2}, \quad a_{22}^* = -\frac{4}{4} = -1, \quad a_{23}^* = \frac{2}{4} = \frac{1}{2},$$

$$a_{31}^* = -\frac{1}{4}, \quad a_{32}^* = \frac{4}{4} = 1, \quad a_{33}^* = -\frac{1}{4}.$$

Deci

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

Corolarul 7.2. Fie K un corp și $A \in \mathcal{M}_n(K)$. Atunci A este inversabilă dacă și numai dacă $\det A \neq 0$.

Teorema 7.3. (Regula lui Cramer). *Fie un sistem de n ecuații liniare cu n necunoscute cu coeficienți într-un corp K :*

$$(1) \quad \left\{ \begin{array}{l} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = b_2 \\ \dots \\ a_{n1}x_1 + a_{n2}x_2 + \dots + a_{nn}x_n = b_n \end{array} \right.$$

Notăm cu $A = (a_{ij})_{1 \leq i, j \leq n}$ matricea coeficienților. Dacă $d = \det A \neq 0$, atunci sistemul (1) are o unică soluție dată de egalitățile: $x_1 = d_1 d^{-1}$, $x_2 = d_2 d^{-1}$, ..., $x_n = d_n d^{-1}$, unde

$$d_1 = \begin{vmatrix} b_1 & a_{12} & \dots & a_{1n} \\ b_2 & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ b_n & a_{n2} & \dots & a_{nn} \end{vmatrix}, \quad d_2 = \begin{vmatrix} a_{11} & b_1 & a_{13} & \dots & a_{1n} \\ a_{21} & b_2 & a_{23} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & b_n & a_{n3} & \dots & a_{nn} \end{vmatrix} \quad \text{s.a.m.d.}$$

Demonstrație. Sistemul (1) de ecuații îl punem sub forma matricială:

$$(2) \quad A \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}.$$

Dacă înmulțim la stanga cu A^{-1} egalitatea (2) și ținând cont de asociativitatea produsului de matrice, obținem:

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = A^{-1} \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_n \end{pmatrix}$$

Din teorema 7.1 avem că $A^{-1} = (a_{ij}^*)_{1 \leq i, j \leq n}$, unde $a_{ij}^* = d^{-1}(-1)^{i+j}d_{ji}$; deci avem

$$\begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} d^{-1} \sum_{j=1}^n (-1)^{1+j} d_{j1} b_j \\ d^{-1} \sum_{j=1}^n (-1)^{2+j} d_{j2} b_j \\ \vdots \\ d^{-1} \sum_{j=1}^n (-1)^{n+j} d_{jn} b_j \end{pmatrix} = \begin{pmatrix} d^{-1} d_1 \\ d^{-1} d_2 \\ \vdots \\ d^{-1} d_n \end{pmatrix}$$

și deci $x_1 = d^{-1}d_1$, $x_2 = d^{-1}d_2$, ..., $x_n = d^{-1}d_n$.

§ 8. RANGUL UNEI MATRICE

În cele ce urmează matricele considerate sunt cu elemente dintr-un corp K (comutativ).

Fie $A = (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} \in \mathcal{M}(m, n, K)$.

Dacă considerăm sirurile de numere $1 \leq i_1 < i_2 < \dots < i_p \leq m$ și $1 \leq j_1 < j_2 < \dots < j_q \leq n$, putem construi o submatrice a matricei A , de tipul $p \times q$, astfel:

$$\begin{pmatrix} a_{i_1, j_1} & a_{i_1, j_2} \dots a_{i_1, j_q} \\ \vdots & \vdots \\ a_{i_p, j_1} & a_{i_p, j_2} \dots a_{i_p, j_q} \end{pmatrix}$$

adică este o matrice constituată din toate elementele matricei A care se găsesc la intersecția liniilor i_1, \dots, i_p cu coloanele j_1, \dots, j_q .

Se observă că în acest fel putem construi $C_m^p \times C_n^q$ submatrici de tipul $p \times q$, ale matricei A .

Vom numi *minor de ordinul p* ($p \geq 1$) al matricei A , determinantul unei submatrici de tipul $p \times p$ al lui A .

Definiția 8.1. Fie $A \in \mathcal{M}(m, n, K)$ o matrice nenulă cu m linii și n coloane. Se numește *rangul matricei A* un număr natural $r > 0$ având următoarele proprietăți:

1. Există un minor de ordinul r al lui A , nenul.
2. Orice minor de ordin $>r$ este egal cu zero.

Numărul r se notează astfel $r = \text{rang } A$.

Dacă $A=0$, atunci punem prin definiție rang $A=0$.

Vom da acum cîteva proprietăți simple ale rangului unei matrice $A \in \mathcal{M}(m, n, K)$ care rezultă imediat din definiția 8.1 și din proprietățile determinanților.

- 1) $0 \leq \text{rang } A \leq \min(m, n)$.
- 2) $\text{rang } A = \text{rang } {}^t A$.
- 3) Rangul unei matrici nu se schimbă dacă permuteam liniile (respectiv coloanele) între ele.
- 4) Rangul unei matrici nu se schimbă dacă înmulțim o linie (sau coloană) cu un element nenul din corpul K .
- 5) $r = \text{rang } A$ dacă și numai dacă există un minor de ordinul r nenul al lui A și orice minor de ordinul $r+1$ al lui A este nul.

Pentru verificarea afirmației 5) trebuie să arătăm că orice minor al lui A de ordin $s > r$ este nul. Într-adevăr, dacă $s = r+1$, afirmația rezultă din ipoteză. Dacă $s = r+2$ se ține cont că orice determinant de ordinul $r+2$ dezvoltat după o linie este o combinație liniară de s deter-

minanți de ordinul $r+1$ și deci acest minor este nul. În continuare se procedează prin recurență după s .

Alte proprietăți ale rangului unei matrici vor rezulta din teorema lui Kronecker pe care o vom prezenta în continuare.

Fie $A = (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} \in \mathcal{M}(m, n, K)$.

Vom nota cu A_1, \dots, A_m (respectiv A^1, \dots, A^n) liniile (respectiv coloanele) matricei A .

Dacă $E = \mathcal{M}(m, 1, K)$ și $F = \mathcal{M}(1, n, K)$ este binecunoscut că E și F sunt K -spații vectoriale în care $\dim_K E = m$ și $\dim_K F = n$.

Se observă că $A_1, \dots, A_m \in E$ iar $A^1, \dots, A^n \in F$ și deci are sens să vorbim de subspațiul vectorial al lui F generat de elementele A_1, \dots, A_m notat $\langle A_1, \dots, A_m \rangle$ precum și de subspațiul vectorial al lui E generat de elementele A^1, \dots, A^n notat $\langle A^1, \dots, A^n \rangle$.

Cu aceste notări putem enunța:

Teorema 8.2. (Kronecker). $\text{rang } A = \dim_K \langle A^1, \dots, A^n \rangle = \dim_K \langle A_1, \dots, A_m \rangle$ sau altfel spus $\text{rang } A$ este egal cu numărul maxim de coloane (respectiv liniile) care sunt liniar independente.

Demonstrație. Fie $r = \text{rang } A$. Putem presupune că $A \neq 0$ (deoarece cazul $A=0$ este evident). Dacă $A \neq 0$, atunci $r \neq 0$ și atunci există un minor de ordinul r nenul.

Deoarece rangul unei matrici nu se schimbă dacă permuteam liniile (respectiv coloanele) între ele, putem presupune că submatricea lui A :

$$M = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1r} \\ \dots & \dots & \dots & \dots \\ a_{r1} & a_{r2} & \dots & a_{rr} \end{pmatrix} \text{ are } \det M \neq 0$$

Pentru a arăta egalitatea $r = \dim_K \langle A^1, \dots, A^n \rangle$ vom proba că A^1, \dots, A^r sunt liniar independente și este un sistem de generatori pentru subspațiul $\langle A^1, \dots, A^n \rangle$.

Fie egalitatea $\alpha_1 A^1 + \alpha_2 A^2 + \dots + \alpha_r A^r = 0$. Rezultă clar că $\alpha_1 M^1 + \alpha_2 M^2 + \dots + \alpha_r M^r = 0$. Deoarece $\det M \neq 0$, putem aplica regula lui Cramer și rezultă că $\alpha_1 = \alpha_2 = \dots = \alpha_r = 0$.

Să dovedim că A^1, \dots, A^r este un sistem de generatori pentru subspațiul $\langle A^1, \dots, A^n \rangle$. Este suficient să dovedim că orice A^t , cu $t > r$, este o combinație liniară de A^1, \dots, A^r .

Considerăm matricea pătratică de ordinul $r+1$

$$B = \begin{vmatrix} a_{11} & \dots & a_{1r} & a_{1,t} \\ a_{21} & \dots & a_{2r} & a_{2,t} \\ \dots & \dots & \dots & \dots \\ a_{r1} & \dots & a_{rr} & a_{r,t} \\ a_{s1} & \dots & a_{sr} & a_{s,t} \end{vmatrix}, \text{ unde } i \text{ este arbitrar}$$

Dacă $i < r$ avem $\det B = 0$ deoarece B are 2 linii egale; dacă $i > r$ avem $\det B = 0$ deoarece $r = \text{rang } A$, deci oricum ar fi i avem $\det B = 0$.

Pentru simplificare notăm cu d complementul algebric al lui a_{ij} în matricea B , cu d_k ($1 \leq k \leq r$) complementul algebric al lui a_{ik} . Dezvoltând $\det B$ după ultima linie avem $a_{11}d_1 + a_{12}d_2 + \dots + a_{1r}d_r + a_{rr}d = 0$.

Cum $d \neq 0$, atunci $a_{rr} = -d^{-1}d_1a_{11} - d^{-1}d_2a_{12} - \dots - d^{-1}d_ra_{1r}$ și deci $A' = -d^{-1}d_1A^1 - \dots - d^{-1}d_rA^r$, unde d_1, d_2, \dots, d_r nu depind de i . Deci A^1, \dots, A^r este un sistem de generatori pentru subspațiul $\langle A^1, \dots, A^r \rangle$.

Analog se arată egalitatea $\text{rang } A = \dim_K \langle A_1, \dots, A_m \rangle$.

Din teorema lui Kronecker rezultă următoarele proprietăți ale rangului unei matrici, care se adaugă la cele 5 proprietăți deja puse după definiția 8.1.

6) Rangul unei matrici A nu se schimbă dacă:

— la o linie (respectiv coloană) adunăm o altă linie (respectiv coloană) înmulțită cu un element din corpul K .

Într-adevăr, dacă A' este matricea care se obține din A adunând la o linie o altă linie înmulțită cu un element, atunci este evident că subspațiul generat de liniile lui A este egal cu subspațiul generat de liniile lui A' .

Analog se demonstrează afirmația pentru coloane.

Corolar 8.3. Determinantul unei matrici pătratice este nul dacă și numai dacă una dintre liniile (respectiv coloanele) sale este o combinație liniară de celelalte liniii (respectiv coloane).

Theorema lui Kronecker ne permite să calculăm rangul unei matrici în mod iterativ.

Fiind dată o matrice nenulă, aceasta are neapărat un minor de ordinul întâi nenul (putem lua orice element nenul al matricei).

Dacă am găsit un minor de ordinul k nenul, îl bordăm pe rînd cu elementele corespunzătoare ale uneia dintre liniile și uneia dintre coloanele rămasă obținind astfel toți minorii de ordinul $k+1$ care-l conțin. Dacă toți acești minori sunt nuli, rangul matricei este $r=k$.

Dacă însă cel puțin unul dintre aceștia (de ordinul $k+1$) este nenul, atunci reținem unul dintre ei și continuăm procedeul.

Numărul minorilor de ordinul $r+1$ care trebuie considerați este $(m-r)(n-r)$ (în loc de $C_m^{r+1} C_n^{r+1}$) reducindu-se în mod substanțial numărul lor.

Exemplu. Să calculăm rangul matricei

$$A = \begin{pmatrix} 3 & 2 & 1 & 4 \\ 3 & -1 & 1 & -3 \\ 3 & 5 & 1 & 11 \end{pmatrix}$$

Se observă că minorul $\begin{vmatrix} 3 & 2 \\ 3 & -1 \end{vmatrix} = -9$ este nenul.

Dacă bordăm acest minor obținem 2 minori de ordinul 3.

$$\begin{vmatrix} 3 & 2 & 1 \\ 3 & -1 & 1 \\ 3 & 5 & 1 \end{vmatrix} = 0 \text{ și } \begin{vmatrix} 3 & 2 & 4 \\ 3 & -1 & -3 \\ 3 & 5 & 11 \end{vmatrix} = 0.$$

Cum acești 2 minori de ordinul 3 sunt nuli, din teorema lui Kronecker rezultă că $\text{rang } A = 2$.

§ 9. TRANSFORMĂRI ELEMENTARE DE MATRICI

Fie K un corp și $A, B \in \mathcal{M}(m, n, K)$ două matrici de tipul $m \times n$ cu elemente din corpul K . Vom nota ca de obicei cu A_1, \dots, A_m (respectiv B_1, \dots, B_m) liniile matricei A (respectiv ale matricei B).

a) Spunem că matricea B se obține pe linii din A printr-o transformare elementară de tipul (I) dacă B se obține din A prin permutarea a două linii între ele, celelalte linii rămânind neschimbate, adică $B_s = A_t$, $B_t = A_s$, pentru o anumită pereche de indici $s \neq t$ și $B_i = A_i$ pentru $i \neq s, t$.

b) Spunem că matricea B se obține pe linii din A printr-o transformare elementară de tipul (II) dacă B se obține din A prin adunarea la o anumită linie a lui A a altrei linii înmulțită cu un element λ din K , celelalte linii rămânind neschimbate, adică $B_i = A_i$ pentru $i \neq s$ și $B_s = A_s + \lambda \cdot A_i$, $s \neq i$ și $\lambda \in K$.

Matricele A și B se zic echivalente pe linii și notăm $A \xrightarrow{I} B$ dacă B se obține din A printr-un număr finit de transformări elementare de tipul (I) sau (II). În mod similar se definește ce înseamnă că matricea B se obține pe coloane din A printr-o transformare elementară de tipul (I) sau (II), precum și ce înseamnă că A și B sunt echivalente pe coloane, relație ce o notăm $A \xrightarrow{c} B$.

Matricele A și B se zic echivalente, și notăm acest fapt prin $A \sim B$, dacă B se obține din A printr-un număr finit de transformări elementare de tipul (I) sau (II) aplicate pe linii sau pe coloane (nu contează ordinea). Este ușor de văzut că relațiile binare „ \xrightarrow{I} ”, „ \xrightarrow{c} ” și „ \sim ” sunt relații de echivalență pe mulțimea $\mathcal{M}(m, n, K)$.

Propoziția 9.1. Fie $A, B \in \mathcal{M}(m, n, K)$. Dacă $A \xrightarrow{I} B$ (resp $A \xrightarrow{c} B$, resp. $A \sim B$) atunci $\text{rang } A = \text{rang } B$.

Demonstrație. Rezultă imediat din faptul că rangul unei matrici nu se schimbă dacă permuteam două linii (sau coloane) sau dacă la o linie (coloană) adunăm o altă linie (coloană) înmulțită cu un element din corpul K .

O matrice $A = (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ se numește triunghiulară superior dacă are forma

$$A = \begin{pmatrix} 0 \dots a_{1k_1} & \dots & a_{1n} \\ 0 \dots 0 & a_{2k_2} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ 0 \dots 0 \dots 0 & a_{rk_r} & \dots & a_{rn} \\ 0 & \dots & \dots & 0 \end{pmatrix}$$

unde $a_{1k_1}, a_{2k_2}, \dots, a_{rk_r}$ sunt nenule iar $1 \leq k_1 < k_2 < \dots < k_r$ și $1 \leq r \leq m$.

Deoarece $a_{1k_1}, a_{2k_2}, \dots, a_{rk_r} \neq 0$, atunci se vede ușor că rang $B = r$ și deci r este unic determinat.

Similar se definește că o matrice A este triunghiulară inferior.

Se vede imediat că A este o matrice triunghiulară superior dacă și numai dacă matricea transpusă $'A$ este triunghiulară inferior.

Matricea A se numește diagonală, dacă $a_{ij} = 0$ oricare ar fi $i \neq j$.

Teorema 9.2. Fie $A = (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} \in \mathcal{M}(m, n, K)$. Atunci

i) Există o matrice $B \in \mathcal{M}(m, n, K)$ triunghiulară superior astfel încât $A \sim B$.

ii) Există o matrice $C \in \mathcal{M}(m, n, K)$ triunghiulară inferior astfel încât $A \sim C$.

iii) Există o matrice diagonală $D \in \mathcal{M}(m, n, K)$ astfel încât $A \sim D$.

Demonstrație. i) Fie k_1 , prima coloană nenulă a matricei A . Deci există un $1 \leq i \leq m$ astfel încât $a_{ik_1} \neq 0$. Dacă $a_{ik_1} \neq 0$, punem $b_{1k_1} = -a_{ik_1}$. Dacă $a_{ik_1} = 0$, atunci permutează prima linie cu linia „ i ”, celelalte răminând neschimbate și punem $b_{1k_1} = a_{ik_1}$. După această transformare elementară avem o nouă matrice B_1 echivalentă pe linii cu matricea A . Fie o linie j din matricea B_1 cu $j \neq 1$, i . Această linie este egală cu linia j din matricea A deci este egală cu

$$A_j = (0 \dots 0 \ a_{jk_1} \ \dots \ a_{jn}).$$

Dacă înmulțim prima linie a matricei B_1 cu $b_{1k_1}^{-1} a_{jk_1}$ și o scădem din linia j a lui B_1 obținem o nouă linie în care elementul din poziția (j, k_1) este nul. Făcind aceeași operație cu toate liniile j ale lui B_1 , unde $j \neq i, 1$, obținem o matrice A' de forma

$$A' = \begin{pmatrix} 0 \dots 0 & a'_{1k_1} & \dots & a'_{1n} \\ 0 \dots 0 & 0 & a'_{2k_2} & \dots & a'_{2n} \\ 0 \dots 0 & 0 & a'_{mk_m} & \dots & a'_{mn} \end{pmatrix}$$

unde prima linie a lui A' este prima linie a lui B_1 , $k_1 < k_2$ și cel puțin un element din $a'_{2k_1}, \dots, a'_{mk_1}$ este nenul. Deci, în particular, $a'_{1k_1} = -b_{1k_1}$. Evident, $A \sim A'$. În continuare considerăm submatricea lui A' din care eliminăm prima linie și continuăm procedeul anterior cu această submatrix.

Înseamnă că există k_2 cu $k_1 < k_2$ și o matrice de forma:

$$A'' = \begin{pmatrix} 0 \dots 0 & a''_{1k_1} & \dots & a''_{1n} \\ 0 \dots 0 & 0 & a''_{2k_1} & \dots & a''_{2n} \\ 0 \dots 0 & 0 & 0 & a''_{3k_1} & \dots & a''_{3n} \\ 0 \dots 0 & 0 & 0 & a''_{mk_1} & \dots & a''_{mn} \end{pmatrix},$$

unde prima linie și a doua a matricei A'' coincide cu prima (respectiv a doua) linie a matricei A' și cel puțin un element din elementele $a''_{3k_1}, \dots, a''_{mk_1}$ este nenul. Evident că $A'' \sim A'$ și deci prin tranzitivitatea relației „ \sim ” rezultă $A \sim A'$.

Continuând procedeul după un număr finit de pași obținem o matrice B triunghiulară superior astfel încât $A \sim B$.

ii) Raționamentul este identic cu cel de la punctul i) numai că se operează pe coloane.

iii) Dacă $A=0$, nu avem ce demonstra. Presupunem $A \neq 0$. Există un $a_{ij} \neq 0$. Dacă $a_{11}=0$, atunci permutând prima linie cu linia i și apoi prima coloană cu coloana j aducem pe a_{11} în locul a_{11} și obținem o matrice echivalentă cu A . Deci putem presupune că $a_{11} \neq 0$. Scăzind din fiecare linie $j \neq 1$ prima linie înmulțită cu $a_{11}^{-1}a_{j1}$ obținem o matrice echivalentă cu A având toate elementele de pe prima coloană egale cu zero, mai puțin primul element.

Acum scăzind din fiecare coloană $A^k = \begin{pmatrix} a_{1k} \\ a_{2k} \\ \vdots \\ a_{mk} \end{pmatrix}$ ($k \neq 1$) prima coloană

înmulțită cu $a_{11}^{-1}a_{1k}$ obținem o matrice echivalentă cu cea inițială având toate elementele de pe prima linie egale cu zero, mai puțin primul element. Deci obținem o matrice $A' \in \mathcal{M}(m, n, K)$ echivalentă cu A și având forma următoare

$$A' = \begin{pmatrix} a'_{11} & 0 & \dots & 0 \\ 0 & a'_{22} & a'_{33} & \dots & a'_{2n} \\ 0 & a'_{m2} & \dots & a'_{mn} \end{pmatrix}$$

În continuare reluăm raționamentul cu submatricea

$$B = \begin{pmatrix} a'_{22} & a'_{23} & \dots & a'_{2n} \\ a'_{m2} & \dots & \dots & a'_{mn} \end{pmatrix}$$

care este o matrice de tipul $(m-1) \times (n-1)$. După un număr finit de pași obținem o matrice diagonală $D \in \mathcal{M}(m, n, K)$ astfel încât $A \sim D$.

Propoziția precedentă ne ajută să calculăm rangul unei matrici reducind matricea inițială prin transformări elementare la o matrice diagonală.

În practică pentru calculul rangului unei matrici se folosește și un al treilea tip de transformări elementare.

c) Spunem că o matrice B se obține pe linii (coloane) din A prin transformări elementare de tipul (III) dacă B se obține din A prin înmulțirea unei anumite linii (coloane) cu un element nenul din K , celelalte linii rămânind neschimbate.

Din proprietățile rangului unei matrici se vede că $\text{rang } A = \text{rang } B$.

Folosind și transformările elementare de tipul (III) și ținând cont de teorema 9.2 afirmația (iii), obținem:

Dată o matrice $A \in \mathcal{M}(m, n, K)$, există o matrice diagonală de forma

$$D = \begin{pmatrix} 1 & & & 0 \\ & 1 & & \\ & & 1 & \\ & & & \ddots \\ 0 & & & & 1 & 0 \end{pmatrix}$$

unde primele r elemente de pe diagonala principală sunt 1 iar restul 0, și astfel încât D se obține din A prin transformări liniare de tipul (I), (II) și (III). În acest caz rezultă $\text{rang } A = r$.

Exemplu. Fie matricea

$$A = \begin{pmatrix} 0 & 1 & -2 & -3 & -5 \\ 6 & -1 & 1 & 2 & 3 \\ -2 & 4 & 3 & 2 & 1 \\ -3 & 0 & 2 & 1 & 2 \end{pmatrix}$$

APLICIND TRANSFORMĂRI ELEMENTARE DE TIPUL (I), (II) SAU (III) OBȚINEM SUCCESIV:

$$A = \begin{pmatrix} 0 & 1 & -2 & -3 & -5 \\ 6 & -1 & 1 & 2 & 3 \\ -2 & 4 & 3 & 2 & 1 \\ -3 & 0 & 2 & 1 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & -2 & -3 & -5 \\ -1 & 6 & 1 & 2 & 3 \\ 4 & -2 & 3 & 2 & 1 \\ 0 & -3 & 2 & 1 & 2 \end{pmatrix} \sim$$

$$\begin{aligned}
& \sim \left(\begin{array}{ccccc} 1 & 0 & -2 & -3 & -5 \\ 0 & 6 & -1 & -1 & -2 \\ 0 & -2 & 11 & 14 & 21 \\ 0 & -3 & 2 & 1 & 2 \end{array} \right) \sim \left(\begin{array}{ccccc} 1 & 0 & 0 & 0 & 0 \\ 0 & 6 & -1 & -1 & -2 \\ 0 & -2 & 11 & 14 & 21 \\ 0 & -3 & 2 & 1 & 2 \end{array} \right) \sim \\
& \sim \left(\begin{array}{ccccc} 1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 6 & -1 & -2 \\ 0 & 11 & -2 & 14 & 21 \\ 0 & 2 & -3 & 1 & 2 \end{array} \right) \sim \left(\begin{array}{ccccc} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 6 & -1 & -2 \\ 0 & -11 & -2 & 14 & 21 \\ 0 & -2 & -3 & 1 & 2 \end{array} \right) \sim \\
& \sim \left(\begin{array}{ccccc} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 6 & -1 & -2 \\ 0 & 0 & 64 & 3 & -1 \\ 0 & 0 & 9 & -1 & -2 \end{array} \right) \sim \left(\begin{array}{ccccc} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 64 & 3 & -1 \\ 0 & 0 & 9 & -1 & -2 \end{array} \right) \sim \\
& \sim \left(\begin{array}{ccccc} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 3 & 64 \\ 0 & 0 & -2 & -1 & 9 \end{array} \right) \sim \left(\begin{array}{ccccc} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 3 & 64 \\ 0 & 0 & 2 & -1 & 9 \end{array} \right) \sim \\
& \sim \left(\begin{array}{ccccc} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 3 & 64 \\ 0 & 0 & 0 & -7 & -117 \end{array} \right) \sim \left(\begin{array}{ccccc} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & -7 & -117 \end{array} \right) \sim \\
& \sim \left(\begin{array}{ccccc} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & -117 \end{array} \right) \sim \left(\begin{array}{ccccc} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{array} \right)
\end{aligned}$$

Deci rang $A = 4$.

§ 10. SISTEME DE ECUAȚII LINIARE

În tot acest capitol K va desemna un corp comutativ. Fie sistemul de m ecuații cu n necunoscute

$$(1) \quad (S) = \begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = b_2 \\ \dots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = b_m \end{cases}$$

unde $a_{ij}, b_i \in K$, oricare ar fi $i=1, \dots, m$ și $j=1, \dots, n$. Dacă $b_1 = b_2 = \dots = b_n = 0$ sistemul (1) se numește *omogen*.

Sistemul (S) se numește *compatibil* dacă are cel puțin o soluție. Este evident că orice sistem omogen este compatibil deoarece admite soluția banală $x_1 = x_2 = \dots = x_n = 0$.

Sistemul (1) se scrie concentrat sub forma:

$$(1') \quad \sum_{j=1}^n a_{ij}x_j = b_i, \quad i=1, \dots, m$$

Vom nota cu $A = (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ matricea coeficienților sistemului (S), numită matricea sistemului iar cu A^e matricea care se obține din A adăugîndu-i încă o coloană și anume coloana $B = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$, adică

$$A^e = \begin{pmatrix} a_{11} \dots a_{1n} & b_1 \\ a_{21} \dots a_{2n} & b_2 \\ \vdots & \vdots \\ a_{m1} \dots a_{mn} & b_m \end{pmatrix}$$

Matricea A^e se numește *matricea extinsă* a sistemului (S).

Dacă notăm cu $X = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ matricea nedeterminatelor, sistemul (S) se scrie sub formă matriceală astfel:

$$(3) \quad AX = B$$

sau dacă notăm cu A^1, \dots, A^n coloanele matricei A , atunci (S) se scrie și astfel:

$$(4) \quad \sum_{i=1}^n x_i A^i = B.$$

Teorema 10.1. (Kronecker-Capelli). Sistemul (S) este compatibil dacă și numai dacă $\text{rang } A = \text{rang } A^e$.

Demonstrație. Presupunem că sistemul (S) este compatibil, atunci există o soluție $(\alpha_1, \dots, \alpha_n)$ a sa. Folosind scrierea (4) a sistemului (S) avem că

$$B = \sum_{i=1}^n \alpha_i A^i \text{ și deci } B \in \langle A^1, \dots, A^n \rangle$$

de unde $\langle A^1, \dots, A^n, B \rangle = \langle A^1, \dots, A^n \rangle$, ceea ce implică

$$\dim_K \langle A^1, \dots, A^n \rangle = \dim_K \langle A^1, \dots, A^n, B \rangle.$$

Din teorema lui Kronecker rezultă că $\text{rang } A = \text{rang } A^e$.

Invers, dacă $\text{rang } A = \text{rang } A^*$, cum $\langle A^1, \dots, A^n \rangle$ este un subspațiu al spațiului vectorial $\langle A^1, \dots, A^n, B \rangle$, rezultă că aceste două spații vectoriale coincid, adică $\langle A^1, \dots, A^n \rangle = \langle A^1, \dots, A^n, B \rangle$. Deci, $B \in \langle A^1, \dots, A^n \rangle$, adică există $\alpha_1, \dots, \alpha_n \in K$ astfel încât $B = \alpha_1 A^1 + \alpha_2 A^2 + \dots + \alpha_n A^n$. Aceasta ne arată că sistemul $\alpha_1, \dots, \alpha_n$ este o soluție a sistemului (S) .

În continuare, pentru simplificare, vom introduce cîteva notății:

$$K^n = \{(\alpha_1, \dots, \alpha_n) \mid \alpha_i \in K\} = \mathcal{M}(1, n, K).$$

$${}^n K = \left\{ \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \mid \alpha_i \in K \right\} = \mathcal{M}(n, 1, K).$$

Dacă $A = (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ este o matrice de tipul $m \times n$, putem să definim aplicația:

$$u: {}^n K \rightarrow {}^m K, \quad u(x) = Ax, \quad \text{unde } x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$$

este un element oarecare din ${}^n K$.

Este evident că u este o aplicație liniară de spații vectoriale.

Dacă notăm cu $b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \in {}^m K$, atunci mulțimea soluțiilor sistemului (S) este egală cu

$$u^{-1}(\{b\}) = \{\alpha \in {}^n K \mid u(\alpha) = b\}.$$

Se observă imediat că $\text{Im } u = \langle A^1, \dots, A^n \rangle$, adică subspațiu generat de coloanele A^1, \dots, A^n ale matricei A .

Presupunem că sistemul (S) este omogen. În acest caz $b=0$ și deci mulțimea soluțiilor lui (S) este egală cu nucleul morfismului u , $\text{Ker } u$ care este un subspațiu vectorial al lui ${}^n K$.

Cum $\text{Im } u \subseteq {}^m K / \text{Ker } u$, atunci avem egalitatea:

$\dim_K \text{Im } u = \dim_K {}^m K - \dim_K \text{Ker } u = n - \dim_K \text{Ker } u$ și deci $\dim_K \text{Ker } u = n - \text{rang } A$.

Deci putem enunța următorul rezultat:

Teorema 10.2. Dacă sistemul (S) este omogen, atunci mulțimea soluțiilor lui (S) este un subspațiu vectorial la lui ${}^n K$ de dimensiune egală cu $n - \text{rang } A$.

Din această teoremă rezultă imediat:

Corolarul 10.3. Dacă (S) este un sistem omogen, atunci (S) are numai soluția hanală $(0, 0 \dots 0)$, dacă și numai dacă $n = \text{rang } A$.

Cum mulțimea soluțiilor unui sistem omogen formează un spațiu vectorial, are sens să vorbim de o bază a sa, care se va numi *un sistem fundamental de soluții* al sistemului omogen dat.

Evident că un sistem omogen poate avea mai multe sisteme fundamentale de soluții. Din teorema 10.2 rezultă că orice sistem fundamental de soluții are $n = \text{rang } A$ elemente.

Presupunem acum că sistemul (S) este oarecare. Am văzut că mulțimea soluțiilor acestui sistem este egală cu $u^{-1}(\{b\})$. Presupunem că (S) este compatibil și presupunem că $x_0 = \begin{pmatrix} x_1^0 \\ \vdots \\ x_n^0 \end{pmatrix}$ este o soluție particulară a lui (S) .

Vom nota cu $x_0 + \text{Ker } u = \{x_0 + \alpha \mid \text{unde } \alpha \in \text{Ker } u\}$, unde, aşa cum am văzut, $\text{Ker } u$ este mulțimea soluțiilor sistemului omogen asociat lui (S) .

Teorema 10.4. Cu notațiile de mai sus, dacă sistemul (S) este compatibil, atunci mulțimea soluțiilor sale este egală cu $x_0 +$ mulțimea soluțiilor sistemului omogen asociat, unde x_0 este o soluție particulară a lui (S) .

Demonstrație. Fie α o soluție a sistemului omogen asociat lui (S) . Avem $u(\alpha) = 0$. Cum $u(x_0) = b$, atunci $u(x_0 + \alpha) = u(x_0) + u(\alpha) = b$ și deci $x_0 + \alpha$ este o soluție a lui (S) . Invers, fie y_0 o soluție oarecare a lui (S) . Cum $u(x_0) = b$ și $u(y_0) = b$, obținem că $u(x_0) = u(y_0)$ și deci $u(y_0 - x_0) = 0$, de unde $\alpha = y_0 - x_0 \in \text{Ker } u$ este o soluție a sistemului omogen asociat lui (S) . Dar $y_0 = x_0 + \alpha$, ceea ce încheia demonstrația.

Corolarul 10.5. Dacă sistemul (S) este compatibil, atunci el are o unică soluție dacă și numai dacă $n = \text{rang } A$.

Corolarul 10.6. Presupunem că $m = n$. Atunci sistemul (S) are o soluție unică dacă și numai dacă $\det A \neq 0$. (În acest caz soluția se obține cu regula lui Cramer).

Teorema Kronecker-Capelli ne permite să decidem dacă sistemul (S) este compatibil sau nu, dar nu ne dă un mijloc practic de aflare a tuturor soluțiilor sistemului dat. De această problemă ne vom ocupa în continuare. Fie deci sistemul (S) compatibil.

Să presupunem că $\text{rang } A = \text{rang } A^c = r$. Cum $\text{rang } A = r$, matricea A conține un minor de ordinul r nenul și toți minorii de ordinul $>r$ sunt zero. Făcind o eventuală renumerotare a ecuațiilor și a nedeterminatelor din sistemul (S) , putem presupune că acest minor nenul de ordinul r este determinantul matricei

$$P = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1r} \\ a_{21} & a_{22} & \dots & a_{2r} \\ \vdots & \vdots & \ddots & \vdots \\ a_{r1} & a_{r2} & \dots & a_{rr} \end{pmatrix}$$

În acest caz $\det P$ se va numi *minor principal* al sistemului (S) . Asociem sistemului (S) sistemul

$$(S') = \begin{cases} a_{11}x_1 + \dots + a_{1n}x_n = b_1 \\ a_{21}x_1 + \dots + a_{2n}x_n = b_2 \\ \dots \\ a_{r1}x_1 + \dots + a_{rn}x_n = b_r \end{cases}$$

care are r ecuații și n nedeterminate.

Teorema 10.7. *Mulțimea soluțiilor sistemului (S) este egală cu mulțimea soluțiilor sistemului (S') .*

Demonstrație. Este evident că orice soluție a lui (S) este o soluție și a lui (S') . Invers, fie $(\alpha_1, \dots, \alpha_n)$ o soluție a lui (S') . Cum rang $A' = r$, atunci din teorema lui Kronecker și din faptul că $\det P \neq 0$, primele r linii ale matricei A' formează o bază pentru spațiul generat de toate liniile lui A' . Deci orice altă linie a lui A' este o combinație liniară de primele r linii ale lui A' . Acest fapt ne arată imediat că $(\alpha_1, \dots, \alpha_n)$ anulează orice ecuație a sistemului (S) .

Introducem următoarele notății.

$X^P = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_r \end{pmatrix}$; x_1, \dots, x_r se vor numi *nedeterminate principale*.

$X^s = \begin{pmatrix} x_{r+1} \\ \vdots \\ x_n \end{pmatrix}$; și x_{r+1}, \dots, x_n se vor numi *nedeterminate secundare*.

De asemenea, vom considera și matricele

$$\mathcal{J} = \begin{pmatrix} a_{1r+1} & \dots & a_{1n} \\ a_{2r+1} & \dots & a_{2n} \\ \dots & \dots & \dots \\ a_{rr+1} & \dots & a_{rn} \end{pmatrix}, \quad B' = \begin{pmatrix} b_1 \\ \vdots \\ b_r \end{pmatrix}$$

Cu aceste notății sistemul (S') se scrie sub forma matriceală astfel:

$$PX^P + \mathcal{J}X^s = B'$$

Cum P este inversabilă, obținem imediat că

$$(4) \quad X^P = P^{-1}B' - (P^{-1}\mathcal{J})X^s$$

care constituie formula de rezolvare a unui sistem compatibil (S) .

În cazul cînd (S) este omogen avem $B' = 0$ și (4) se scrie sub forma

$$(5) \quad X^P = -(P^{-1}\mathcal{J})X^s,$$

care constituie formula de rezolvare a unui sistem omogen.

Formula (5) ne permite să obținem un sistem fundamental de soluții pentru un sistem omogen în felul următor: Dăm pentru nede-

eterminatele secundare următoarele valori: $x_{r+1}=1$, $x_{r+2}=\dots=x_n=0$ și din (5) obținem în mod unic valorile $x_1=\lambda_1^1$, ..., $x_r=\lambda_r^1$ și deci obținem pentru sistemul omogen dat soluția

$$\alpha_1=(\lambda_1^1, \lambda_2^1, \dots, \lambda_r^1, 1, 0, \dots, 0).$$

Acum dăm pentru nedeterminatele secundare valorile:

$x_{r+1}=0$, $x_{r+2}=1$, $x_{r+3}=\dots=x_n=0$ și din (5) obținem în mod unic valorile $x_1=\lambda_1^2$, ..., $x_r=\lambda_r^2$ și deci obținem pentru sistemul omogen dat soluția:

$$\alpha_2=(\lambda_1^2, \dots, \lambda_r^2, 0, 1, 0, 0, \dots, 0).$$

Continuind proceful în final dăm nedeterminatelor secundare valorile: $x_{r+1}=\dots=x_{n-1}=0$, $x_n=1$. Din formula (5) obținem în mod unic valorile $x_1=\lambda_1^{n-r}$, $x_2=\lambda_2^{n-r}$, ..., $x_r=\lambda_r^{n-r}$ și deci obținem pentru sistemul omogen dat soluția

$$\alpha_{n-r}=(\lambda_1^{n-r}, \dots, \lambda_r^{n-r}, 0, 0, \dots, 1).$$

Cu aceste notații putem enunța rezultatul următor:

Teorema 10.8. Dacă sistemul (S) este omogen, atunci $\alpha_1, \dots, \alpha_{n-r}$ formează un sistem fundamental de soluții pentru (S) .

Deci mulțimea soluțiilor sistemului (S) este mulțimea:

$$\{\lambda_1\alpha_1+\dots+\lambda_{n-r}\alpha_{n-r} \mid \lambda_1, \dots, \lambda_{n-r} \in K\}.$$

Demonstrație. Se vede ușor că $\alpha_1, \dots, \alpha_{n-r}$ sunt liniar independente peste K . Cum sunt în număr de $n-r$, rezultă că $\alpha_1, \alpha_2, \dots, \alpha_{n-r}$ formează o bază pentru spațiul vectorial al tuturor soluțiilor sistemului (S) și deci $\alpha_1, \dots, \alpha_{n-r}$ este un sistem fundamental de soluții.

Combinind teorema 10.4 și teorema 10.8 obținem:

Teorema 10.9. Fie (S) un sistem compatibil de ecuații liniare. Dacă $\alpha_1, \dots, \alpha_{n-r}$ este un sistem fundamental de soluții pentru sistemul omogen asociat, iar x_0 este o soluție particulară a sistemului (S) , atunci orice soluție a lui (S) este de forma

$$x_0+\lambda_1\alpha_1+\dots+\lambda_{n-r}\alpha_{n-r}, \text{ unde } \lambda_1, \dots, \lambda_{n-r} \in K.$$

Mai mult, o soluție particulară x_0 a lui (S) se obține dând valorile $x_{r+1}=\dots=x_n=0$ și din formula (4) obținem valorile pentru nedeterminatele principale date de egalitatea:

$$X^0 = P^{-1}B' \text{ unde } X^0 = \begin{pmatrix} x_1^0 \\ x_2^0 \\ \vdots \\ x_r^0 \end{pmatrix}$$

Exemplu

$$S: \begin{cases} x_1 + x_2 + x_3 - 2x_4 = 5 \\ 2x_1 + x_2 - 2x_3 + x_4 = 1 \\ 2x_1 - 3x_2 + x_3 + 2x_4 = 3 \end{cases}$$

A vom: $A = \begin{pmatrix} 1 & 1 & 1 & -2 \\ 2 & 1 & -2 & 1 \\ 2 & -3 & 1 & 2 \end{pmatrix}$

$$A^e = \begin{pmatrix} 1 & 1 & 1 & -2 & 5 \\ 2 & 1 & -2 & 1 & 1 \\ 2 & -3 & 1 & 2 & 3 \end{pmatrix}$$

$$P = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 1 & -2 \\ 2 & -3 & 1 \end{pmatrix}, \det P = -19 \neq 0, \text{ deci rang } A = 3.$$

Notăm $X^P = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$, $X^S = (x_4)$, $\mathcal{S} = \begin{pmatrix} -2 \\ 1 \\ 2 \end{pmatrix}$, $B' = \begin{pmatrix} 5 \\ 1 \\ 3 \end{pmatrix}$, $B = \begin{pmatrix} 5 \\ 1 \\ 3 \end{pmatrix}$

Înlocuim în formula $X^P = P^{-1}B' - (P^{-1}\mathcal{S})X^S$ și obținem:

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 2 & 1 & -2 \\ 2 & -3 & 1 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 5 \\ 1 \\ 3 \end{pmatrix} - \begin{pmatrix} 1 & 1 & -1 \\ 2 & 1 & -2 \\ 2 & -3 & 1 \end{pmatrix}^{-1} \begin{pmatrix} -2 \\ 1 \\ 2 \end{pmatrix}. (x_4)$$

Prin calcule se obține:

$$\begin{pmatrix} 1 & 1 & -1 \\ 2 & 1 & -2 \\ 2 & -3 & 1 \end{pmatrix}^{-1} = \begin{vmatrix} \frac{5}{19} & \frac{4}{19} & \frac{3}{19} \\ \frac{6}{19} & \frac{1}{19} & -\frac{4}{19} \\ \frac{8}{19} & -\frac{5}{19} & \frac{1}{19} \end{vmatrix}$$

Deci:

$$\begin{aligned} \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} &= \begin{pmatrix} \frac{5}{19} & \frac{4}{19} & \frac{3}{19} \\ \frac{6}{19} & \frac{1}{19} & -\frac{4}{19} \\ \frac{8}{19} & -\frac{5}{19} & \frac{1}{19} \end{pmatrix} \cdot \begin{pmatrix} 5 \\ 1 \\ 3 \end{pmatrix} - \begin{pmatrix} \frac{5}{19} & \frac{4}{19} & \frac{3}{19} \\ \frac{6}{19} & \frac{1}{19} & -\frac{4}{19} \\ \frac{8}{19} & -\frac{5}{19} & \frac{1}{19} \end{pmatrix} \cdot \begin{pmatrix} -2 \\ 1 \\ 2 \end{pmatrix}. (x_4) = \\ &= \begin{pmatrix} 2 \\ 1 \\ 2 \end{pmatrix} - \begin{pmatrix} 0 \\ -1 \\ -1 \end{pmatrix} (x_4) = \begin{pmatrix} 2 \\ 1+x_4 \\ 2+x_4 \end{pmatrix} \end{aligned}$$

Deci:

$$\begin{aligned}x_1 &= 2, \\x_2 &= 1+x_4, \\x_3 &= 2+x_4.\end{aligned}$$

Dăm lui x_4 valoarea $\lambda \in R$ și obținem soluția

$$\begin{aligned}x_1 &= 2 \\x_2 &= 1+\lambda \\x_3 &= 2+\lambda \\x_4 &= \lambda, \quad \lambda \in R.\end{aligned}$$

§ 11. METODA LUI GAUSS DE REZOLVARE A UNUI SISTEM DE ECUAȚII LINIARE

În continuare vom prezenta o nouă metodă de rezolvare a sistemelor de ecuații liniare, numită metoda lui Gauss sau metoda *eliminării successive*.

Considerăm sistemul (S) de m ecuații liniare cu n necunoscute.

$$(S) = \left\{ \begin{array}{l} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = b_1, \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = b_2, \\ \dots \\ a_{m1}x_1 + a_{m2}x_2 + \dots + a_{mn}x_n = b_m. \end{array} \right.$$

Așa cum știm vom nota cu A (resp. A') matricea sistemului (respectiv matricea extinsă a lui (S)).

Evident că fiecare coloană a matricei A o putem presupune nenulă, deoarece în caz contrar sistemul (S) s-ar înlătura cu un sistem având un număr mai mic de necunoscute.

Fie și un alt sistem (S') având m ecuații liniare și n necunoscute:

$$(S') = \left\{ \begin{array}{l} a'_{11}x_1 + a'_{12}x_2 + \dots + a'_{1n}x_n = b'_1 \\ \dots \\ a'_{m1}x_1 + a'_{m2}x_2 + \dots + a'_{mn}x_n = b'_m \end{array} \right.$$

cu A' (resp. A'^*) notăm matricea sistemului (respectiv matricea extinsă).

i) Vom spune că sistemul (S') se obține din (S) printr-o transformare elementară de tipul (I) dacă ecuațiile lui (S') se obțin din aceleia ale lui (S) printr-o permutare a două ecuații ale lui (S) , celelalte rămânind neschimbate.

ii) Spunem că sistemul (S') se obține din sistemul (S) printr-o transformare elementară de tipul (II) dacă toate ecuațiile lui (S') sunt identice cu ale lui (S) cu excepția ecuației „ i ” care se obține din ecuația „ i ” a lui (S) adunată cu ecuația „ k ” a lui (S) multiplicată cu un element $\lambda \in K$.

Vom spune că sistemele (S) și (S') sunt echivalente și notăm prin $(S) \sim (S')$ dacă sistemul (S') se obține din (S) printr-un număr finit de transformări elementare de tipul (I) și (II).

Este evident că relația „ \sim ” este o relație de echivalență pe mulțimea sistemelor de m ecuații liniare cu n necunoscute.

Se vede imediat că $(S) \sim (S')$ dacă și numai dacă $A' \sim A^e$, adică matricele extinse asociate sunt echivalente pe linii.

Teorema 11.1. Fie (S) și (S') două sisteme de m ecuații liniare cu n necunoscute. Dacă $(S) \sim (S')$, atunci (S) și (S') au aceleași soluții.

Demonstrație. Ne putem reduce la cazul cind (S') se obține din (S) printr-o transformare elementară de tipul (I) sau (II). În acest caz se vede imediat că orice soluție a lui (S) este o soluție și a lui (S') .

Cum evident (S) se obține la rîndul său din (S') printr-o transformare liniară de tipul (I) sau (II), atunci și orice soluție a lui (S') este o soluție a lui (S) .

Teorema 11.2. Orice sistem de ecuații (S) este echivalent cu un sistem (\tilde{S}) de forma următoare:

$$(\tilde{S}) = \left\{ \begin{array}{l} \tilde{a}_{11}x_1 + \dots + \tilde{a}_{1n}x_n = \tilde{b}_1 \\ \tilde{a}_{2k_2}x_{k_2} + \dots + \tilde{a}_{2n}x_n = \tilde{b}_2 \\ \tilde{a}_{3k_3}x_{k_3} + \dots + \tilde{a}_{3n}x_n = \tilde{b}_3 \\ \dots \\ \tilde{a}_{rk_r}x_{k_r} + \dots + \tilde{a}_{rn}x_n = \tilde{b}_r \\ 0 = \tilde{b}_{r+1} \\ \dots \\ 0 = \tilde{b}_m \end{array} \right.$$

unde $\tilde{a}_{11}, \tilde{a}_{2k_2}, \tilde{a}_{3k_3}, \dots, \tilde{a}_{rk_r}$ sunt nenule și $1 < k_2 < k_3 < \dots < k_r$.

Sistemul (\tilde{S}) se numește formă trapezoidală a sistemului (S) .

Demonstrație. Vom urma pas cu pas demonstrația de aducere a unei matrice la o matrice triunghiulară superior printr-un număr finit de transformări liniare (teorema 9.2). Cum prima coloană a matricei A este nenulă, există un $a_{11} \neq 0$. Dacă $a_{11} = 0$, atunci permutăm ecuațiile 1 și i între ele și obținem un sistem echivalent cu primul în care coeficientul lui x_1 din prima ecuație este nul. Dacă $a_{11} \neq 0$, atunci nu facem nici o permutare de ecuații.

Acum din ecuația j , $a_{j1}x_1 + \dots + a_{jn}x_n = b_j$, unde $j > 1$ scădem prima ecuație înmulțită cu elementul $a_{11}^{-1} a_{j1}$. Repetând raționamentul pentru orice ecuație j cu $j > 1$ obținem următorul sistem:

$$(S_1) = \begin{cases} a'_{11}x_1 + \dots + a'_{1n}x_n = b'_1 \\ a'_{2k_2}x_{k_2} + \dots + a'_{2n}x_n = b'_2 \\ \dots \dots \dots \\ a'_{mk_2}x_{k_2} + \dots + a'_{mn}x_n = b'_m \end{cases}$$

unde $a'_{11} \neq 0$ și $k_2 > 1$ și unui dintre elementele $a'_{2k_2}, \dots, a'_{mk_2}$ este nenul.

Evident că $(S_1) \sim (S)$.

În continuare aplicăm procedeul de mai sus la sistemul de $m-1$ ecuații obținut din (S_1) eliminând prima ecuație.

Obținem astfel un sistem de ecuații liniare.

$$(S_2) = \begin{cases} a''_{11}x_1 + \dots + a''_{1n}x_n = b''_1 \\ a''_{2k_2}x_{k_2} + \dots + a''_{2n}x_n = b''_2 \\ a''_{3k_3}x_{k_3} + \dots + a''_{3n}x_n = b''_3 \\ \dots \dots \dots \\ a''_{mk_3}x_{k_3} + \dots + a''_{mn}x_n = b''_m \end{cases}$$

unde prima ecuație este de fapt identică cu prima ecuație a lui (S_1) iar $1 < k_2 < k_3$ și cel puțin unul dintre elementele $a''_{3k_3}, \dots, a''_{mk_3}$ este nenul.

Evident $(S_2) \sim (S_1)$ și deci $(S_2) \sim (S)$. Continuind în felul acesta procedeul de mai sus după un număr finit de pași ajungem la forma trapezoidală a sistemului (S) .

Concluzii. 1) În forma trapezoidală (\bar{S}) a sistemului (S) numărul r este egal cu rangul matricii A , deoarece matricea \bar{A} a sistemului (\bar{S}) se obține din matricea lui (S) prin transformări elementare și deci rang $A = \text{rang } \bar{A}$.

Cum se vede ușor că $r = \text{rang } \bar{A}$, atunci $r = \text{rang } A$.

2) Sistemul (S) este compatibil dacă și numai dacă în forma sa trapezoidală (S) nu apar ecuații de forma $0 = b_i$ cu $b_i \neq 0$. În particular, dacă rang $A = m$, atunci sistemul (S) este compatibil.

Acum dacă sistemul (S) este compatibil, rezolvarea se face în felul următor: vom numi necunoscutele x_1, x_{k_2}, \dots, x_r , nedeterminate principale, iar restul de $n-r$ necunoscute le vom numi nedeterminate secundare. În continuare, vom da valori arbitrale nedeterminatelor secundare și începând cu ultima ecuație

$$\bar{a}_{rk_r}x_{k_r} + \dots + \bar{a}_{rk_n}x_n = \bar{b}_r$$

din sistemul (S) determinăm mai întâi pe x_{k_r} ; apoi luând penultima ecuație determinăm pe $x_{k_{r-1}}$ și continuând astfel în final determinăm pe x_1 .

Exemplu. Să aplicăm metoda lui Gauss sistemului:

$$\left\{ \begin{array}{l} 2x_1 - x_2 + x_3 - x_4 = 1 \\ 2x_1 - x_2 - 3x_4 = 2 \\ 3x_1 - x_3 - x_3 + x_4 = -3 \\ 2x_1 + 2x_2 - 2x_3 + 5x_4 = -6 \end{array} \right.$$

Împărțim prima ecuație cu 2 și obținem:

$$x_1 - \frac{1}{2}x_2 + \frac{1}{2}x_3 - \frac{1}{2}x_4 = \frac{1}{2}$$

După aceea, înmulțim această ecuație cu -2 și o adunăm la a 2-a, apoi o înmulțim cu -3 și o adunăm la a treia și în final o înmulțim cu -2 și o adunăm la a patra. Obținem:

$$\left\{ \begin{array}{l} -x_3 - 2x_4 = 1 \\ \frac{3}{2}x_2 - \frac{5}{2}x_3 + \frac{5}{2}x_4 = -\frac{9}{2} \\ 3x_2 - 3x_3 + 6x_4 = -7 \end{array} \right.$$

Permutăm liniile 1 și 2 între ele:

$$\left\{ \begin{array}{l} \frac{3}{2}x_2 - \frac{5}{2}x_3 + \frac{5}{2}x_4 = -\frac{9}{2} \\ -x_3 - 2x_4 = 1 \\ 3x_2 - 3x_3 + 6x_4 = -7 \end{array} \right.$$

Împărțim prima ecuație cu $\frac{3}{2}$:

$$x_2 - \frac{5}{3}x_3 + \frac{5}{3}x_4 = -3.$$

Înmulțim această ecuație cu -3 și o adunăm la a 3-a. Sistemul devine:

$$\left\{ \begin{array}{l} -x_3 - 2x_4 = 1 \\ 2x_3 + x_4 = 2 \end{array} \right.$$

Împărțim prima ecuație cu -1.

$$x_3 + 2x_4 = -1$$

Obținem:

$$-3x_4 = 4$$

$$x_4 = -\frac{4}{3}$$

Deci

$$\left\{ \begin{array}{l} x_1 - \frac{1}{2}x_2 + \frac{1}{2}x_3 - \frac{1}{2}x_4 = \frac{1}{2} \\ x_2 - \frac{5}{3}x_3 + \frac{5}{3}x_4 = -3 \\ x_3 + 2x_4 = -1 \\ x_4 = -\frac{4}{3} \end{array} \right.$$

Vom avea soluțiile:

$$x_4 = -\frac{4}{3}$$

$$x_3 = -2x_4 - 1 = -\frac{5}{3}$$

$$x_2 = -3 - \frac{5}{3}x_4 + \frac{5}{3}x_3 = 2$$

$$x_1 = \frac{1}{2}x_2 - \frac{1}{2}x_3 + \frac{1}{2}x_4 + \frac{1}{2} = 0.$$

§ 12. FORMULA DE INVERSIUNE MÖBIUS. APLICAȚII

Fie (P, \leq) o mulțime finită și nevidă, înzestrată cu o relație de ordine parțială. Definim funcția:

$$\zeta: P \times P \rightarrow \mathbb{Z} \text{ astfel: } \zeta(x, y) = \begin{cases} 1, & \text{dacă } x \leq y, \\ 0, & \text{în caz contrar.} \end{cases}$$

Important în cele ce urmează este următoarea propoziție:

Propoziția 12.1. Există o numerotare $P = \{x_1, x_2, \dots, x_n\}$ a mulțimii P astfel încât, dacă $x_i < x_j$, să implice $i < j$.

Demonstrație. Numerotarea mulțimii P o facem astfel: alegem x_1 din P astfel încât să fie element minimal; alegem x_2 astfel încât să fie element minimal $P \setminus \{x_1\}$; alegem x_3 să fie element minimal în $P \setminus \{x_1, x_2\}, \dots$; alegem x_i să fie element minimal în mulțimea $P \setminus \{x_1, x_2, \dots, x_{i-1}\}$ s.a.m.d. Presupunem prin absurd că din $x_i < x_j$, implică $j < i$. Rezultă că $x_i, x_j \in P \setminus \{x_1, x_2, \dots, x_{i-1}\}$ și cum x_i este element minimal în $P \setminus \{x_1, \dots, x_{i-1}\}$, obținem o contradicție.

Observație. 1) În general mulțimea P se poate numera în mai multe feluri având proprietatea din enunțul propoziției 12.1, depinzind de numărul de elemente minime care le conțin.

2) Dacă (P, \leq) este total ordonată, este evident că P are o singură numerotare cu proprietatea de mai sus.

Presupunem că P are numerotarea $P = \{x_1, \dots, x_m\}$ cu condiția că $x_i \leq x_j$, implică $i < j$. Funcției $\zeta: P \times P \rightarrow \mathbb{Z}$ ii asociem matricea $A = (\zeta_{ij})_{1 \leq i, j \leq n}$, unde $\zeta_{ij} = \zeta(x_i, x_j)$. Este evident că $A \in \mathcal{M}(n, \mathbb{Z})$ și are forma

$$A = \begin{pmatrix} 1 & \zeta_{12} & \dots & \zeta_{1n} \\ 0 & 1 & \zeta_{23} & \dots & \zeta_{2n} \\ & & \ddots & & \\ 0 & \dots & & & 1 \end{pmatrix} \text{ unde } \zeta_{ii} = 1 \text{ oricare ar fi } i = 1, \dots, n$$

$$\zeta_{ij} = 0 \text{ dacă } i > j \text{ și}$$

Cum $\det A = 1$, atunci A este inversabilă în $\mathcal{M}(n, \mathbb{Z})$.

Vom nota cu $B = (\mu_{ij})_{1 \leq i, j \leq n}$ inversa sa.

Este ușor de văzut din calculul inversei unei matrici că avem $\mu_{ii} = 1$ dacă $1 \leq i \leq n$ și $\mu_{ij} = 0$ dacă $i > j$.

Matricei B ii asociem funcția:

$$\mu: P \times P \rightarrow \mathbb{Z}, \mu(x_i, x_j) = \mu_{ij}.$$

Din egalitatea $AB = I_n$ obținem egalitățile:

$$\sum_{k=1}^n \zeta_{ik} \mu_{kj} = \delta_{ij} \text{ sau } \sum_{k=1}^n \zeta(x_i, x_k) \mu(x_k, x_j) = \delta_{ij}$$

oricare ar fi $i, j = 1, \dots, n$.

Deoarece $\zeta(x_i, x_k) = 0$ dacă $x_i \not\leq x_k$, $\zeta(x_i, x_k) = 1$ dacă $x_i \leq x_k$ obținem egalitatea

$$\sum_{x_i \leq x_k} \mu(x_i, x_j) = \delta_{ij}.$$

Cum din $x_j < x_k$ rezultă $j < k$ și în acest caz avem $\mu(x_k, x_j) = 0$, atunci egalitatea de mai sus devine

$$(*) \quad \sum_{\substack{x_i \leq x_k \\ x_j \leq x_k}} \mu(x_i, x_j) = \delta_{ij}$$

Să dovedim mai întii că dacă $x_i \not\leq x_j$, atunci $\mu(x_i, x_j) = 0$.

Prin reducere la absurd, presupunem că $\mu(x_i, x_j) \neq 0$.

Considerăm mulțimea $P_j = \{x_i \in P \mid x_i \not\leq x_j \text{ și } \mu(x_i, x_j) \neq 0\}$ și fie un x_{i_0} element maximal în P_j , P_j fiind finită. Înseamnă că dacă $x_{i_0} < x_k$ și $x_k \not\leq x_j$, atunci $\mu(x_k, x_j) = 0$.

Egalitatea (*) scrisă pentru x_{i_0} și x_j se reduce la $\mu(x_{i_0}, x_j) = \delta_{i_0, j} = 0$ (deoarece $i_0 \neq j$), contradicție.

Dacă avem $x_i \leq x_j$, și ținând cont de rezultatul pe care l-am demonstrat, egalitatea (*) se scrie

$$\sum_{x_i \leq x_k \leq x_j} \mu(x_k, x_j) = \delta_{ij}$$

sau renunțind la numerotarea mulțimii P obținem că $\mu(x, y) = 0$ dacă $x \not\leq y$ și în cazul că $x \leq y$ avem

$$(1) \quad \sum_{z \leq z < y} \mu(z, y) = \delta(x, y) = \begin{cases} 1 & \text{dacă } x=y \\ 0 & \text{dacă } x \neq y \end{cases}$$

Analog, din egalitatea $B \cdot A = I_n$ obținem egalitatea:

$$(2) \quad \sum_{x \leq z \leq y} \mu(x, z) = \delta(x, y).$$

Caracterizarea funcției μ este dată de următoarea teoremă:

Teorema 12.2. *Fiind dată (P, \leq) o mulțime finită parțial ordonată, există o unică funcție $\mu: P \times P \rightarrow \mathbb{Z}$ cu proprietățile:*

i) $\mu(x, y) = 0$ dacă $x \not\leq y$.

ii) $\mu(x, x) = 1$

iii) Oricare ar fi $x < y$, $\mu(x, y) = - \sum_{z \leq z < y} \mu(x, z) = - \sum_{z \leq z \leq y} \mu(z, y)$.

Demonstrație. Existența funcției μ cu proprietățile i), ii), iii) rezultă din egalitățile (1) și (2).

Să dovedim unicitatea lui μ . Presupunem că mai există o funcție $\mu': P \times P \rightarrow \mathbb{Z}$ cu proprietățile i), ii) și iii).

Dacă $x \not\leq y$, atunci din condiția i) rezultă că $\mu(x, y) = \mu'(x, y) = 0$. Presupunem deci că $x \leq y$ și considerăm intervalul:

$$[x, y] = \{z \in P \mid x \leq z \leq y\}$$

Să notăm cu r numărul de elemente din mulțimea $[x, y]$. Vom dovedi prin inducție după r egalitatea $\mu(x, y) = \mu'(x, y)$.

Dacă $r=1$, atunci $x=y$ și deci din condiția ii) rezultă că $\mu'(x, y) = \mu(x, y) = 1$.

Presupunem $r>1$; deci $x < y$. Relația iii) implică

$$\sum_{z \leq z \leq y} \mu(x, z) = \sum_{z \leq z < y} \mu'(x, z) = \delta(x, y) = 0$$

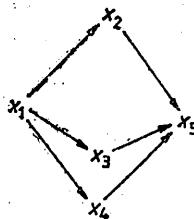
sau

$$\mu(x, y) + \sum_{z \leq z < y} \mu(x, z) = \mu'(x, y) + \sum_{z \leq z < y} \mu'(x, z).$$

Pe baza ipotezei de inducție avem $\mu(x, z) = \mu'(x, z)$ pentru orice z cu $x \leq z < y$ și deci din ultima egalitate obținem $\mu(x, y) = \mu'(x, y)$.

Funcția μ ce verifică condițiile i), ii), iii) din teorema 12.2 se numește *funcția Möbius asociată mulțimii parțial ordonate P* iar relațiile i), ii), și iii) se numesc *relațiile de recurență* ce definesc funcția μ .

Exemplu. I) Fie (P, \leq) multimea ordonată formată din 5 elemente iar relația de ordine „ \leq ” este dată de sensul săgeților din următoarea diagramă



Să determinăm funcția Möbius asociată mulțimii (P, \leq) . Avem deci $\mu(x_i, x_j) = 0$ dacă $x_i \not\leq x_j$; $\mu(x_i, x_i) = 1$, oricare ar fi $i = 1, 2, 3, 4, 5$.

Cum $\mu(x_1, x_1) + \mu(x_1, x_2) = 0$ obținem $\mu(x_1, x_2) = -1$.

Analog obținem $\mu(x_1, x_3) = \mu(x_1, x_4) = \mu(x_2, x_5) = \mu(x_3, x_5) = \mu(x_4, x_5) = -1$.

Din egalitatea $\sum_{x_1 \leq z \leq x_5} \mu(x, z) = 0$ rezultă $\mu(x_1, x_1) + \mu(x_1, x_2) + \mu(x_1, x_3) + \mu(x_1, x_4) + \mu(x_1, x_5) = 0$ și deci $\mu(x_1, x_5) = 2$.

II) Fie $P = \{0, 1, \dots, n\}$ cu relația de ordine obișnuită. Funcția Möbius asociată este următoarea:

$$\mu(i, i) = 1 \text{ oricare ar fi } i \in P.$$

$$\mu(i, i+1) = 1 \text{ deoarece } \mu(i, i) + \mu(i, i+1) = 0$$

și

$$\mu(i, j) = 0 \text{ oricare ar fi } j \neq i, i+1.$$

Intr-adevăr, dacă $j < i$, atunci $\mu(i, j) = 0$; dacă $i < j$ și $j \neq i+1$, atunci $i < i+1 < j$. Să luăm cazul $j = i+2$, atunci din egalitatea $\sum_{i \leq k \leq j} \mu(i, k) = 0$ obținem $\mu(i, i) + \mu(i, i+1) + \mu(i, i+2) = 0$ de unde rezultă că $\mu(i, i+2) = 0$.

Analog, se arată că $\mu(i, i+3) = \dots = \mu(i, n) = 0$.

$$\text{Deci avem } \mu(i, j) = \begin{cases} 1 & \text{dacă } j = i \\ -1 & \text{dacă } j = i+1 \\ 0 & \text{în rest} \end{cases}$$

III) Dacă (P, \leq) este o mulțime finită total ordonată, atunci, exact ca în exemplul II, rezultă că funcția Möbius asociată este dată de egalitățile:

$$\mu(x, y) = \begin{cases} 1 & \text{dacă } x = y \\ -1 & \text{dacă } x < y \text{ și între } x \text{ și } y \text{ nu mai există nici un element} \\ 0 & \text{în rest.} \end{cases}$$

IV) Fie X o mulțime finită și $P = \mathcal{P}(X)$ mulțimea părților lui X cu relația de ordine inclusiunea. Vom arăta că funcția Möbius asociată este dată de egalitățile:

$$\mu(U, V) = \begin{cases} (-1)^{|V-U|} & \text{dacă } U \subseteq V \\ 0 & \text{dacă } U \not\subseteq V. \end{cases}$$

Intr-adevăr, presupunem $U \subset V$ și $m = |V - U|$ dacă $m \neq 0$; atunci $U = V$ și $\mu(U, U) = 1$. Presupunem afirmația adevărată pentru toate valorile mai mici ca m și o demonstrăm pentru m .

Cum $\sum_{U \subseteq W \subseteq V} \mu(U, W) = 0$, această egalitate se mai scrie și astfel:

$$\mu(U, U) + \sum_{\substack{U \subseteq W \subseteq V \\ |W-U|=1}} \mu(U, W) + \sum_{\substack{U \subseteq W \subseteq V \\ |W-U|=2}} \mu(U, W) + \dots + \sum_{\substack{U \subseteq W \subseteq V \\ |W-U|=m-1}} \mu(U, W) + \mu(U, V) = 0.$$

Folosind ipoteza de inducție și faptul că există C_m^k submulțimi W cu proprietatea că $U \subset W \subset V$ și cu $|W - U| = k$:

$$1 + C_m^1(-1)^1 + C_m^2(-1)^2 + \dots + C_m^{m-1}(-1)^{m-1} + \mu(U, V) = 0.$$

Cum $1 - C_m^1 + C_m^2 - C_m^3 + \dots + (-1)^m C_m^m = 0$ obținem că $\mu(U, V) = (-1)^m$.

V) Fie (P_1, \leq) și (P_2, \leq) două mulțimi parțial ordonate. Considerăm mulțimea $P = P_1 \times P_2$ cu relația de ordine $(x_1, x_2) \leq (y_1, y_2) \Leftrightarrow x_1 \leq y_1$ și $x_2 \leq y_2$.

Fie $\mu_1: P_1 \times P_2 \rightarrow Z$, $\mu_2: P_2 \times P_1 \rightarrow Z$ și $\mu: P \times P \rightarrow Z$ funcțiile Möbius asociate mulțimilor P_1 , P_2 și respectiv P .

Vom arăta că

$$\mu((x_1, x_2), (y_1, y_2)) = \mu_1(x_1, y_1) \cdot \mu_2(x_2, y_2).$$

Intr-adevăr, fie funcția $\mu': P \times P \rightarrow Z$ definită prin egalitatea $\mu'((x_1, x_2), (y_1, y_2)) = \mu_1(x_1, y_1) \cdot \mu_2(x_2, y_2)$.

Dacă $(x_1, x_2) \nleq (y_1, y_2)$, atunci $x_1 \nleq y_1$ sau $x_2 \nleq y_2$ și atunci $\mu_1(x_1, y_1) = 0$ sau $\mu_2(x_2, y_2) = 0$ adică $\mu'((x_1, x_2), (y_1, y_2)) = 0$.

Presupunem că $(x_1, x_2) \leq (y_1, y_2)$ și calculăm

$$\sum_{(x_1, x_2) \leq (y_1, y_2) \leq (z_1, z_2)} \mu'((x_1, x_2), (y_1, y_2)) = \sum_{\substack{x_1 \leq y_1 \leq z_1 \\ x_2 \leq y_2 \leq z_2}} \mu_1(x_1, y_1) \cdot \mu_2(x_2, y_2) = \sum_{x_1 \leq y_1 \leq z_1} \sum_{x_2 \leq y_2 \leq z_2} \mu_1(x_1, y_1) \cdot \mu_2(x_2, y_2).$$

$$\mu_1(x_1, y) \cdot \mu_2(x_2, z) = \sum_{x_1 \leq y \leq v_1} \mu_1(x_1, y) \cdot \sum_{x_2 \leq z \leq v_2} \mu_2(x_2, z) = \delta(x_1, y_1) \cdot \delta(x_2, y_2) = \\ = \delta((x_1, x_2), (y_1, y_2)).$$

Din teorema 12.2 rezultă că $\mu' = \mu$.

VI) Fie $n > 0$ un număr natural. Considerăm D_n mulțimea divizorilor lui n , deci $D_n = \{d \in N / d|n\}$.

Pe D_n considerăm relația de ordine divizibilitatea, adică dacă $d, d' \in D_n$, atunci $d \leq d' \Leftrightarrow d|d'$.

Putem scrie $n = p_1^{m_1} \cdot p_2^{m_2} \cdots p_r^{m_r}$, unde p_1, \dots, p_r sunt numere prime distincte și $m_i \geq 1$. Considerăm mulțimile $P_i = \{0, 1, \dots, m_i\}$.

Rezultă că D_n este izomorfă ca latice cu mulțimea ordonată $P_1 \times P_2 \times \cdots \times P_r$. Acest izomorfism este definit astfel: dacă $d \in D_n$, $d = p_1^{k_1} \cdots p_r^{k_r}$, $0 \leq k_i \leq m_i$, atunci definim $\phi: D_n \rightarrow P_1 \times P_2 \times \cdots \times P_r$ astfel: $\phi(d) = (k_1, \dots, k_r)$. Se vede imediat că ϕ este o bijecție. Rezultă că funcția Möbius a lui D_n este egală cu funcția Möbius a mulțimii $P_1 \times \cdots \times P_r$.

Tinind cont de V) și II) obținem că: dacă $a = p_1^{k_1} \cdots p_r^{k_r}$ și $b = p_1^{l_1} \cdots p_r^{l_r}$ și $a | b$, atunci $k_i \leq l_i$ și $\mu(a, b) = \prod_{i=1}^r \mu_i(k_i, l_i)$.

Cum $\mu_i(k_i, l_i) = -1$ dacă $l_i = k_i + 1$, $\mu_i(k_i, l_i) = 1$ dacă $l_i = k_i$ și $\mu_i(k_i, l_i) = 0$ în rest obținem că:

$$\mu(a, b) = \begin{cases} (-1)^s & \text{dacă } b | a \text{ este produsul a } s \text{ numere prime distincte} \\ 0 & \text{dacă } b | a \text{ conține un factor patratnic} \\ 0 & \text{dacă } a \text{ nu divide } b. \end{cases}$$

Utilizând funcția lui Möbius asociată mulțimii D_n putem defini următoarea funcție:

$$\bar{\mu}: N^* \rightarrow Z, \text{ unde } N^* = \{1, 2, \dots, n, \dots\}$$

$$\bar{\mu}(n) = \mu(1, n) = \begin{cases} (-1)^s & \text{dacă } n \text{ este produs de } s \text{ numere prime distincte} \\ 0 & \text{în cazul cînd } n \text{ are un factor patratnic.} \end{cases}$$

Se verifică ușor că funcția $\bar{\mu}$ este multiplicativă, în sensul că dacă $m, n \in N^*$ astfel încit $(m, n) = 1$, atunci $\bar{\mu}(m, n) = \bar{\mu}(m) \cdot \bar{\mu}(n)$.

În plus, dacă $n > 1$, avem

$$\sum_{d|n} \bar{\mu}(d) = 0.$$

Într-adevăr, dacă $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$, unde p_1, \dots, p_s sunt numere distincte iar $k_i \geq 1$, atunci notind $n_0 = p_1 p_2 \cdots p_s$, avem

$$\sum_{d|n} \bar{\mu}(d) = \sum_{d|n_0} \bar{\mu}(d) = \sum_{r=0}^s C_r (-1)^r = (1 - 1)^s = 0$$

VII) Fie K un corp finit avind q elemente (corpul K este comutativ) și V un K -spațiu vectorial de dimensiune n . Deoarece $V \cong K^n$, atunci V are q^n -elemente.

Vom nota cu $L(V)$ laticea tuturor subspațiilor vectoriale ale lui V . Deoarece corpul K este finit, atunci $L(V)$ este o latice finită. Dacă $0 \leq k \leq n$ este un număr natural vom nota $\binom{n}{k}_q$ numărul de subspații vectoriale ale lui V care au dimensiunea egală cu k . Numerele $\binom{n}{k}_q$, unde $k=0, 1, \dots, n$ se numesc *coeficienții lui Gauss sau numerele lui Gauss* asociati spațiului vectorial V . Cum avem un singur subspațiu de dimensiune zero și anume subspațiul vectorial nul al lui V , atunci $\binom{n}{0}_q = 1$.

Următoarea teoremă ne precizează mai bine care sunt numerele $\binom{n}{k}_q$.

Teorema 12.3. Cu notațiile de mai sus avem relațiile

$$i) \quad \binom{n}{k}_q = \frac{(q^n - 1)(q^{n-1} - 1) \dots (q^{n-k+1} - 1)}{(q^k - 1)(q^{k-1} - 1) \dots (q - 1)}$$

$$ii) \quad \binom{n}{k}_q = \binom{n}{n-k}_q \quad (\forall) k = 0, 1, \dots, n$$

$$iii) \quad \binom{n}{k}_q = q^k \binom{n-1}{k}_q + \binom{n-1}{k-1}_q.$$

IV. Are loc identitatea polinomială (identitatea lui Cauchy)

$$iv) \quad y^n = 1 + \sum_{k=0}^{n-1} \binom{n}{k}_q (y-1)(y-q)\dots(y-q^{n-k-1})$$

Demonstrație. i) Vom nota $U_{n,k}$ numărul de sisteme ordonate avind k vectori liniar independenți. Ca prim element al unui astfel de sistem putem considera pe oricare din cei $q^n - 1$ vectori diferenți de 0. Orice vector $v \neq 0$ generează un subspațiu unidimensional conținând q vectori. Deci sunt $q^n - q$ vectori liniar independenți față de V și oricare dintre ei poate fi luat ca cea de-a doua componentă.

Fie w una dintre acestea. Perechea $\{v, w\}$ generează un subspațiu bidimensional conținând q^2 vectori. Deci există $q^n - q^2$ vectori liniar independenți față de $\{v, w\}$ și oricare ar fi dintre ei poate fi luat ca cea de-a treia componentă. Continuând astfel rezultă că $U_{n,1} = (q^n - 1)(q^n - q) \dots (q^n - q^{k-1})$.

Fiecare k sistem de vectori liniar independenți generează un subspațiu k -dimensional. Pe de altă parte, orice subspațiu k -dimensional conține $U_{k,k}$ baze ordonate care îl generează. Deci

$$\binom{n}{k}_q = \frac{\bigcup_{n,k}}{\bigcup_{k,k}} = \frac{(q^n - 1)(q^n - q) \dots (q^n - q^{k-1})}{(q^k - 1)(q^k - q) \dots (q^k - q^{k-1})}$$

și relația i) se obține reducind în mod convenabil puterile lui q .

Egalitatea i) se mai poate scrie și astfel:

$$(*) \binom{n}{k}_q = \frac{\prod_{t=1}^n (q^t - 1)}{\prod_{t=1}^k (q^t - 1) \prod_{t=1}^{n-k} (q^t - 1)}$$

ceea ce ne arată că $\binom{n}{k}_q = \binom{n}{n-k}_q$, adică ii).

Afirmarea iii) rezultă direct prin calcul folosind egalitatea (*) de mai sus.

Pentru a demonstra afirmația IV) vom nota cu V_n un spațiu vectorial de dimensiune n peste corpul K iar cu V un K -spațiu vectorial având y vectori. Este evident că avem y^n omomorfisme definite pe V_n și cu valori în V . Fie $f: V_n \rightarrow V$ un omomorfism. Avem $\text{Im } f \simeq V_n / \text{Ker } f$, unde $\text{Ker } f$ este un subspațiu vectorial al lui V_n . Fie acum W un subspațiu vectorial al lui V_n de dimensiune k ($0 \leq k \leq n$).

Fie $e_1, e_2, \dots, e_{n-k}, e_{n-k+1}, \dots, e_n$ o bază a lui V_n astfel încât e_{n-k+1}, \dots, e_n constituie o bază pentru W . Atunci o aplicație liniară $f: V_n \rightarrow V$ are $\text{Ker } f = W$ dacă și numai dacă ea aplică vectorii e_{n-k+1}, \dots, e_n în zero iar vectorii e_1, e_2, \dots, e_{n-k} intr-o mulțime liniar independentă de vectori din V . Deoarece $f(e_1)$ poate fi oricare din cei $y-1$ vectori nenuli; $f(e_2)$ poate fi oricare din cei $y-q$ vectori care nu aparțin subspațiului generat de $f(e_1)$; $f(e_3)$ poate fi oricare din cei $y-q^2$ vectori care nu aparțin subspațiului generat de $f(e_1)$ și $f(e_2)$. Găsim astfel $(y-1)(y-q)\dots(y-q^{n-k-1})$ aplicații liniare $f: V_n \rightarrow V$ cu proprietatea că $\text{Ker } f = W$. Cum în V_n există $\binom{n}{k}_q$ subspații vectoriale de dimensiune k și cum pentru $k=n$ avem o singură aplicație liniară definită pe V_n și cu valori în V și anume aplicația nulă, rezultă imediat egalitatea IV) cind y este dimensiunea unui spațiu vectorial arbitrar. Cum această egalitate are loc pentru o infinitate de valori, atunci egalitatea IV) este valabilă pentru $y \in \mathbb{R}$.

Remarcă. Se observă imediat că

$$\lim_{q \rightarrow 1} \left(\frac{n}{k} \right)_q = \left(\frac{n}{k} \right) = C_n^k$$

Ne propunem acum să calculăm funcția Möbius a lăicei $L(V)$. Fie $X, Y \subseteq L(V)$ astfel încit $X \subset Y$. Cum intervalul $[X, Y] = \{Z \in L(V) \mid X \subset Z \subset Y\}$ este izomorf cu lăicea subspațiilor $L(Y/X)$ a spațiului vectorial Y/X și folosind formulele de recurență rezultă că $\mu(X, Y)$ depinde numai de

$$m = \dim_K(Y/X) = \dim_K Y - \dim_K X.$$

Din aceste motive mai notăm $\mu(X, Y) = \mu(m)$.

Teorema 12.4. Cu notatiile de mai sus avem că

$$\mu(X, Y) = (-1)^m \cdot q \frac{m(m-1)}{2}.$$

Demonstratie. Din cele de mai sus ne putem reduce la cazul cînd $X = (0)$ și $Y = V$, adică să arătăm că $\mu(n) = (-1)^n \cdot q \frac{n(n-1)}{2}$.

Procedăm prin inducție după n . Dacă $n = 0$ afirmația este evidentă.

Presupunem afirmația adevărată pentru toate numerele naturale strict mai mici ca n .

Din formulele de recurență avem egalitatea $\sum_{W \in L(V)} \mu(0, W) = 0$ de unde obținem

$$\begin{aligned} \mu(0, 0) + \sum_{\substack{W \in L(V) \\ \dim W=1}} \mu(0, W) + \sum_{\substack{W \in L(V) \\ \dim W=2}} \mu(0, W) + \dots + \sum_{\substack{W \in L(V) \\ \dim W=n-1}} \mu(0, W) + \\ + \mu(0, V) = 0 \end{aligned}$$

sau folosind coeficienții lui Gauss obținem:

$$1 + \binom{n}{1}_q \mu(1) + \binom{n}{2}_q \mu(2) + \dots + \binom{n}{n-1}_q \mu(n-1) + \mu(n) = 0.$$

Din ipoteza de inducție avem că $\mu(m) = (-1)^m q \frac{m(m-1)}{2}$ oricare ar fi $m < n$. Deci

$$\begin{aligned} 1 + \binom{n}{1}_q (-1)^1 q^0 + \binom{n}{2}_q (-1)^2 q^1 + \binom{n}{3}_q (-1)^3 q^3 + \dots + \\ + \binom{n}{n-1}_q (-1)^{n-1} q^{\frac{(n-1)(n-2)}{2}} + \mu(n) = 0 \end{aligned}$$

Din teorema 12.3 egalitatea iv) rezultă că $\mu(n)$ trebuie să fie egal cu $(-1)^n \cdot q^{\frac{n(n-1)}{2}}$.

Algebra de incidență asociată unei mulțimi finite parțial ordonate.
 Fie (P, \leq) o mulțime finită parțial ordonată și K un corp de caracteristică zero (de exemplu corpul Q al numerelor raționale). Definim

$$A_k(P) = \{f: P^2 \rightarrow K \mid x \leq y \Rightarrow f(x, y) = 0\}.$$

Când nu este nici o problemă de confuzie notăm mai simplu $A(P) = A_k(P)$. Mulțimea $A_k(P)$ devine un K -spațiu vectorial unde pentru $f, g \in A_k(P)$ și $r \in K$ avem operațiile:

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

$$(rf)(x, y) = rf(x, y).$$

Definim *convoluția* $f*g$ a lui $f, g \in A_k(P)$ prin $(f*g)(x, y) = \sum_{z \leq z \leq y} f(x, z)g(z, y)$ în cazul $x \leq y$, și $(f*g)(x, y) = 0$ dacă $x \not\leq y$.

Teorema 12.5. *Mulțimea $A_k(P)$ cu operațiile de adunare, înmulțire cu scalari și convoluția este o algebră numită algebra de incidență asociată mulțimii (P, \leq) . Elementele din $A_k(P)$ se vor numi funcții de incidență.*

Demonstrație. Să verificăm mai întii asociativitatea operației de convoluție: dacă $f, g, h \in A_k(P)$ avem pentru

$$\begin{aligned} x \leq y: & (f*(g*h))(x, y) = \sum_{z \leq z \leq y} f(x, z)(g*h)(z, y) = \\ & = \sum_{x \leq z \leq y} f(x, z) \left(\sum_{z \leq w \leq y} g(z, w)h(w, y) \right) = \sum_{x \leq w \leq y} \left(\sum_{x \leq z \leq w} f(x, z)g(z, w) \right) h(w, y) = \\ & = \sum_{x \leq w \leq y} (f*g)(x, w)h(w, y) = ((f*g)*h)(x, y) \text{ și deci } f*(g*h) = (f*g)*h. \end{aligned}$$

Se observă imediat că funcția lui Kronecker

$$\delta: P^2 \rightarrow K, \quad \delta(x, y) = \begin{cases} 1 & \text{dacă } x = y, \text{ aparține} \\ 0 & \text{dacă } x \neq y \end{cases}$$

mulțimii $A_k(P)$ și este element neutru față de operația de convoluție.

Celelalte axiome se verifică imediat.

Corolarul 12.6. Un element $f \in A_k(P)$ este inversabil dacă și numai dacă $f(x, x) \neq 0$ pentru orice $x \in P$.

Demonstrație. Dacă f este inversabil, există $g \in A_k(P)$ astfel încât $f * g = g * f = \delta$.

Atunci pentru orice $x \in P$ avem $1 = (f * g)(x, x) = f(x, x) \cdot g(x, x)$ și deci $f(x, x) \neq 0$.

Invers, presupunem că $f(x, x) \neq 0$ pentru orice $x \in P$. Vom defini recursiv funcția f^{-1} :

$$f^{-1}(x, x) = f(x, x)^{-1} \text{ oricare ar fi } x \in P, \text{ dacă } x < y, \text{ punem } f^{-1}(x, y) =$$

$$= f(y, y)^{-1} \left(\sum_{z \leqslant z < y} f^{-1}(x, z) f(z, y) \right)$$

iar dacă $x \not\leqslant y$ punem $f^{-1}(x, y) = 0$. Să dovedim că $f * f^{-1} = f^{-1} * f = \delta$.

Evident, presupunem că $x \leqslant y$ și vom proceda prin inducție după numărul m de elemente din intervalul $[x, y]$. Dacă $m = 1$, atunci $(f * f^{-1})(x, x) = f(x, x) \cdot f(x, x)^{-1} = 1$.

Presupunem deci că $m > 1$; avem în acest caz:

$$\begin{aligned} (f * f^{-1})(x, y) &= \sum_{x \leqslant z < y} f(x, z) f^{-1}(z, y) = \sum_{x \leqslant z < y} f(x, z) \cdot f(z, y) + \\ &+ f(x, y) \cdot f^{-1}(y, y) = f(y, y)^{-1} \sum_{x \leqslant z < y} f(x, z) \left(- \sum_{z \leqslant u < y} f^{-1}(z, u) f(u, y) \right) + \\ &+ f(x, y) \cdot f^{-1}(y, y) = f(y, y)^{-1} \sum_{x \leqslant u < y} f(u, y) \left(- \sum_{z \leqslant z \leqslant u} f(x, z) f^{-1}(z, u) \right) + \\ &+ (f(x, y) f^{-1}(y, y)) = -f(y, y)^{-1} \sum_{x \leqslant u < y} f(u, y) (f * f)^{-1}(x, u) + \\ &+ f(x, y) f^{-1}(y, y) = -f(y, y)^{-1} \sum_{x \leqslant u < y} f(u, y) \delta(x, u) + f(x, y) \cdot f^{-1}(y, y) = \\ &= -f(y, y)^{-1} f(x, y) + f(x, y) f^{-1}(y, y) = 0. \end{aligned}$$

Deci $f * f^{-1} = \delta$. Analog se arată și egalitatea $f^{-1} * f = \delta$.

Exemple de funcții de incidență. i) Funcția lui Kronecker (sau funcția Delta)

$$\delta(x, y) = \begin{cases} 1 & \text{dacă } x = y \\ 0 & \text{dacă } x \neq y \end{cases}$$

Am văzut că δ este elementul unitate în algebra $A_k(P)$.

ii) Funcția Zeta

$$\zeta(x, y) = \begin{cases} 1 & \text{dacă } x \leqslant y \\ 0 & \text{dacă } x \not\leqslant y. \end{cases}$$

iii) Funcția Lambda

$$\lambda(x, y) = \begin{cases} 1 & \text{dacă } x = y \text{ sau } x < y \\ 0 & \text{în caz contrar.} \end{cases}$$

iv) Funcția Lanț $\eta = \zeta - \delta$.

v) Funcția Acoperire $K = \lambda - \delta$.

vi) Funcția Möbius $\mu = \zeta^{x-1}$.

Are sens să vorbim de funcția Möbius deoarece ζ este un element inversabil în $A_K(P)$. Din demonstrația coloralului 12.6 funcția μ are proprietățile:

$$1) \mu(x, x) = 1; \quad 2) \text{ dacă } x < y, \quad \mu(x, y) = - \sum_{x \leq z < y} \mu(x, z) = - \sum_{x < z \leq y} \mu(z, y);$$

3) dacă $x \not\leq y$ $\mu(x, y) = 0$ și astfel regăsim relațiile de recurență din teorema 12.2.

Inversiunea Möbius. Aplicații. Fie din nou (P, \leq) o mulțime finită parțial ordonată și G un grup abelian. Fie $f: P \rightarrow G$ o aplicație oarecare.

Definim funcțiile:

$$g: P \rightarrow G, \quad g(x) = \sum_{y \leq x} f(y)$$

$$h: P \rightarrow G, \quad h(x) = \sum_{y \leq x} f(y).$$

Am văzut că putem numerota mulțimea P astfel: $P = \{x_1, \dots, x_n\}$, cu condiția că $x_i < x_j \Rightarrow i < j\}$. Folosind funcția Zeta $\zeta: P^2 \rightarrow \mathbb{Z}$, $\zeta(x, y) =$

$$= \begin{cases} 1 & \text{dacă } x \leq y \\ 0 & \text{dacă } x \not\leq y \end{cases}, \quad \text{atunci putem scrie}$$

$$g(x) = \sum_{y \in P} \zeta(x, y) f(y) \text{ sau } g(x) = \sum_{j=1}^n \zeta(x_i, y_i) f(x_i)$$

iar $i = 1, 2, \dots, n$. Aceste egalități le putem scrie sub forma matriceală

$$\begin{pmatrix} g(x_1) \\ g(x_2) \\ \vdots \\ g(x_n) \end{pmatrix} = A \begin{pmatrix} f(x_1) \\ f(x_2) \\ \vdots \\ f(x_n) \end{pmatrix}.$$

Înmulțind această egalitate cu $A^{-1} = B$ obținem

$$\begin{pmatrix} f(x_1) \\ \vdots \\ f(x_n) \end{pmatrix} = B \begin{pmatrix} g(x_1) \\ \vdots \\ g(x_n) \end{pmatrix}$$

de unde rezultă că $f(x_i) = \sum_{j=1}^n \mu(x_i, x_j) g(x_j)$ sau renunțind la numera-tarea lui A avem:

$$f(x) = \sum_{y \in P} \mu(x, y) g(y) = \sum_{x \leq y} \mu(x, y) g(y).$$

Un rezultat analog obținem pentru funcția h :

$$f(x) = \sum_{y \leq x} \mu(x, y) \cdot h(y).$$

Deci avem următorul rezultat.

Teorema 12.7. Fie $f, g, h: P \rightarrow G$. Atunci au loc relațiile:

$$\text{i)} \quad g(x) = \sum_{z \leq y} f(z) \Leftrightarrow f(x) = \sum_{z \leq y} \mu(x, z) g(z)$$

$$\text{ii)} \quad h(x) = \sum_{y \leq x} f(y) \Leftrightarrow f(x) = \sum_{y \leq x} \mu(x, y) \cdot h(y).$$

Acstea egalități se numesc inversiunile Möbius.

Aplicații. I) Considerăm mulțimea $P = \{0 < 1 < \dots < n\}$. Reamintim că funcția Möbius asociată mulțimii P este:

$$\mu(i, j) = \begin{cases} 1 & \text{dacă } i=j \\ -1 & \text{dacă } j=i+1 \\ 0 & \text{în caz contrar.} \end{cases}$$

Atunci pentru orice $f, g, h: P \rightarrow G$ avem relațiile:

$$g(m) = \sum_{i=m}^n f(i) \Leftrightarrow f(m) = g(m) - g(m+1)$$

$$h(m) = \sum_{i=0}^m f(i) \Leftrightarrow f(m) = g(m) - g(m-1).$$

II. Fie X o mulțime finită și $P = \mathcal{P}(X)$ cu relația de ordine incluziunea. Am văzut că funcția Möbius asociată lui $\mathcal{P}(X)$ este:

$$\mu(A, B) = (-1)^{|B-A|} \text{ pentru } A \subset B$$

Deci pentru orice $f, g, h: \mathcal{P}(X) \rightarrow G$ au loc relațiile:

$$g(A) = \sum_{A \subset B} f(B) \Leftrightarrow f(A) = \sum_{A \subset B} (-1)^{|B-A|} g(B)$$

$$h(A) = \sum_{B \subset A} f(B) \Leftrightarrow f(A) = \sum_{B \subset A} (-1)^{|A-B|} h(B).$$

III. Fie A_1, \dots, A_t submulțimi ale unei mulțimi finite A . Fie $T = \{1, 2, \dots, t\}$; dacă $I \subset T$ este o submulțime a lui T , vom nota $f(I)$ numărul de elemente din A care se găsesc în mulțimile A_i cu $i \in I$ și nu se găsesc în celelalte.

Deci

$$f(I) = |\bigcap_{i \in I} A_i \cap (A - \bigcup_{i \in T \setminus I} A_i)|.$$

Obținem astfel o funcție $f: \mathcal{P}(A) \rightarrow \mathbb{Z}$.

Este clar că funcția $g: \mathcal{P}(A) \rightarrow \mathbb{Z}$, unde $g(I) = \sum_{J \subset I \subset T} f(J) = |\bigcap_{i \in I} A_i|$

Aplicând exemplul precedent obținem că:

$$f(I) = \sum_{J \subset I} (-1)^{|J|-|I|} |\bigcap_{j \in J} A_j|.$$

Pentru $I = \emptyset$ obținem egalitatea

$$\begin{aligned} |A - \bigcup_{i=1}^t A_i| &= |A| - \sum_{i=1}^t |A_i| + \sum_{i < j}^t |A_i \cap A_j| - \dots \\ &\quad + (-1)^t |A_1 \cap \dots \cap A_t|. \end{aligned} \quad (*)$$

Am ținut cont că $\bigcap_{i \in I} A_i = A$ cind $I = \emptyset$) care ne implică egalitatea, numită principiul incluziunii-excluziunii:

$$|\bigcup_{i=1}^t A_i| = \sum_{i=1}^t |A_i| - \sum_{i < j}^t |A_i \cap A_j| \pm \dots \pm (-1)^t |A_1 \cap \dots \cap A_t|.$$

Este binecunoscut că această ultimă egalitate se demonstrează ușor prin inducție după t .

Tinând cont de egalitatea $(*)$ putem determina numărul de elemente din A care se găsesc în exact p mulțimi A_i . Acest număr este egal cu

$$\begin{aligned} \sum_{I \subset T, |I|=p} f(I) &= \sum_{|I|=p} \sum_{J \subset I} (-1)^{|J|-p} |\bigcap_{j \in J} A_j| = \sum_{I \subset T, |I|=p} \sum_{J \subset I} (-1)^{|J|-p} |\bigcap_{j \in J} A_j| = \\ &= \sum_{k=p}^t (-1)^{k-p} \cdot C_p^k \sum_{|I|=k} |\bigcap_{j \in I} A_j|. \end{aligned}$$

Deci am obținut următorul rezultat.

Teorema 12.8. Fie A o mulțime finită, A_1, \dots, A_t submulțimi ale lui A și $T = \{1, \dots, t\}$. Atunci numărul de elementelor din A care se găsesc în exact p submulțimi A_i este

$$c_p = \sum_{k=p}^t (-1)^{k-p} C_p^k \sum_{|I|=k} |\bigcap_{j \in I} A_j|.$$

Să aplicăm această egalitate la următoarea problemă: Fie S_n grupul permutărilor de gradul n . Vom nota cu $e_p(n)$ numărul permutărilor care au p puncte fixe. Ne propunem să determinăm acest număr. Pentru aceasta vom nota cu $A_i = \{\sigma \in S_n \mid \sigma(i) = i\}$, unde $i = 1, \dots, n$. Este evident că $|\bigcap_{i \in I} A_i| = (n - |I|)!$ unde $I \subset \{1, \dots, n\}$.

Aplicând teorema 12.8 obținem:

$$e_p(n) = \sum_{k=p}^n (-1)^{k-p} C_k^p C_n^k (n-k)! = \frac{n!}{p!} \sum_{k=p}^n \frac{(-1)^{k-p}}{(k-p)!} = \frac{n!}{p!} \sum_{k=0}^{n-p} \frac{(-1)^k}{k!}.$$

Dacă $p=0$, obținem numărul d_n al tuturor permutărilor de gradul n care nu au nici un punct fix.

$$\text{Deci } d_n = n! \sum_{k=0}^n \frac{(-1)^k}{k!}$$

$$\text{Să observăm că } \frac{d_n}{n!} \rightarrow \frac{1}{e} \text{ cind } n \rightarrow \infty.$$

IV. (*Funcția lui Euler*). Fie $n \geq 1$ un număr natural. Vom nota cu $\varphi(n)$ numărul de numere naturale prime cu n și mai mici ca n ; $\varphi(n)$ se numește *indicatorul lui Euler* al numărului n , iar funcția φ se numește *funcția lui Euler*.

Presupunem că $n = p_1^{k_1} \dots p_t^{k_t}$, unde p_1, \dots, p_t sunt numere prime distincte și $k_i \geq 1$. Fie $A = \{1, \dots, n\}$ $A_i = \{k \in A \mid p_i \mid k\}$ pentru $i = 1, \dots, t$ și $T = \{1, \dots, t\}$. Este clară egalitatea:

$$|\bigcap_{i \in I} A_i| = \frac{n}{\prod_{i \in I} p_i}, \text{ unde } I \subset T.$$

Aplicând teorema 12.8 avem

$$\varphi(n) = \varphi_0 = n - \sum_{i=1}^t \frac{n}{p_i} + \sum_{i < j} \frac{n}{p_i p_j} + \dots + (-1)^t \frac{n}{p_1 \dots p_t} = n \cdot \prod_{i=1}^t \left(1 - \frac{1}{p_i}\right).$$

Se vede ușor că din ultima egalitate obținem

$$\varphi(n) = \sum_{d|n} \mu(d, n) d,$$

unde μ este funcția Möbius asociată mulțimii, $D_n = \{d \mid d \text{ divide } n\}$ unde relația de ordine este divizibilitatea.

Dar această ultimă egalitate este echivalentă cu egalitatea $n = \sum_{d|n} \varphi(d)$, conform teoremei 12.7.

V) Polinomul cromatic asociat unei hărți (Problema celor patru culori). Numim hartă împărțirea planului în regiuni (numite ţări) prin arce. Două ţări sunt vecine dacă au frontieră în comun un arc. Fie k culorile fixate. Se numește colorare proprie a hărții dacă oricare două ţări vecine nu sunt colorate cu aceeași culoare (folosindu-ne de cele k culori).

Fie Γ o hartă. Ne propunem să determinăm numărul de colorări proprii ale acestei hărți folosindu-ne de cele k culori. Acest număr il notăm $f_k(\Gamma)$. Dacă $k=4$, problema celor 4 culori spune că orice hartă se poate colora propriu cu cele 4 culori, adică $f_4(\Gamma) \neq 0$ oricare ar fi harta.

Această problemă a fost enunțată pentru prima dată în anul 1850, de către De Morgan.

Δ este o subhartă a lui Γ , $\Delta \subseteq \Gamma$, dacă se obține din Γ ștergind anumite frontiere.

Notăm $S_\Gamma = \{\Delta : \Delta \text{ subhartă a lui } \Gamma\}$.

(S_Γ, \leq) este o mulțime parțial ordonată.

Dacă $\Delta \in S_\Gamma$, considerăm $f_k(\Delta) = \text{numărul de colorări proprii ale hărții } \Delta$, folosind cele k culori.

Dacă $\Delta \in S_\Gamma$, definim $g_k(\Delta) = \text{numărul tuturor colorărilor lui } \Delta$ (nu neapărat proprii) este clar că $g_k(\Delta) = k^{c(\Delta)}$, unde $C(\Delta) = \text{numărul de ţări care aparțin hărții}$.

Avem $\sum_{E \in \Delta} f_k(E) = g_k(\Delta)$, deci

$$f(\Delta) = \sum_{E \in \Delta} \mu(E, \Delta), \quad g(E) = \sum_{E \in \Delta} \mu(E, \Delta) k^{c(E)}.$$

Dacă $\Delta = \Gamma$, avem

$$f(\Gamma) = \sum_{\Delta \subseteq \Gamma} \mu(\Delta, \Gamma) k^{c(\Delta)},$$

formulă care se numește polinomul cromatic asociat hărții.

VI) Numărul de polinoame ireductibile de gradul n ($n \geq 1$) peste un corp finit.

Fie K un corp finit având q elemente, adică $|K| = q$.

Vom nota cu $X_{n,q}$ mulțimea polinoamelor ireductibile monice de gradul n din inelul $K[X]$ (un polinom se zice monic dacă coeficientul termenului de grad maxim este 1) și cu $N_{n,q} = |X_{n,q}|$. Ne propunem să determinăm acest număr. Pentru aceasta avem nevoie de o serie de rezultate preliminarii.

a) Fie $p = \text{char } K$; deci $p \geq 2$ și p este un număr prim. Vom nota cu P subcorpul prim al lui K . Deci $P \cong Z_p$ și deci $|P| = p$.

Fie $K \subset E$ o extindere a lui K ; evident E este un K spațiu vectorial; vom nota cu $[E : K]$ dimensiunea lui E considerat ca K spațiu vectorial. Dacă $[E : K] = m < \infty$; atunci spunem că E este o extindere finită.

În acest caz, deoarece $E \cong K^m$, atunci $|E| = q^m$. În particular, dacă $[K : P] = n$ rezultă că $|K| = p^n$ adică $q = p^n$.

b) Multimea K este egală cu multimea rădăcinilor polinomului $X^q - X \in P[X]$.

Intr-adevăr, fie $\alpha \in K$. Dacă $\alpha = 0$, atunci 0 este evident o rădăcină a polinomului $X^q - X$.

Dacă $\alpha \neq 0$, atunci $\alpha \in K^* = K - \{0\}$. Cum K^* este un grup față de operația de înmulțire și $|K^*| = q - 1$, atunci conform teoremei lui Lagrange rezultă că $\alpha^{q-1} = 1$, de unde rezultă că $\alpha^q = \alpha$ ceea ce ne arată că α este o rădăcină a polinomului $X^q - X$. Cum $X^q - X$ are cel mult q rădăcini, rezultă că K este egală cu multimea rădăcinilor polinomului $X^q - X$.

c) Fie $f = a_0 + a_1X + \dots + a_{n-1}X^{n-1} + X^n$ un polinom ireductibil monic din inelul $K[X]$. Cum X_{p^n} este o mulțime finită este bine cunoscut că există o extindere $K \subset L$ care conține toate rădăcinile polinoamelor din mulțimea X_{p^n} . Fie $\alpha \in L$ o rădăcină a lui f . Vom nota cu

$$E = K[\alpha] = \{b_0 + b_1\alpha + \dots + b_{n-1}\alpha^{n-1} \mid b_0, b_1, \dots, b_{n-1} \in K\}.$$

Deoarece $\alpha^n + a_{n-1}\alpha^{n-1} + \dots + a_0 = 0$, atunci este ușor de văzut că E este un subinel al corpului L .

Pe de altă parte, elementele $1, \alpha, \dots, \alpha^{n-1}$ sunt liniar independente peste K .

Intr-adevăr, dacă avem o egalitate de forma

$$\lambda_0 + \lambda_1\alpha + \dots + \lambda_{n-1}\alpha^{n-1} = 0, \quad \lambda_i \in K,$$

atunci notind cu $g(X)$ polinomul $g(X) = \lambda_0 + \lambda_1X + \dots + \lambda_{n-1}X^{n-1} \in K[X]$ avem că $g(\alpha) = 0$.

Dacă polinomul $g(X)$ nu este zero, atunci rezultă că f și g sunt prime între ele și deci există polinoamele $f_1, g_1 \in K[X]$ astfel, încât $1 = f_1f + gg_1$ de unde înlocuind pe X cu α obținem $1 = 0$, contradicție.

Deci $g(X) = 0$ și prin urmare $\lambda_0 = \lambda_1 = \lambda_2 = \dots = \lambda_{n-1} = 0$. Prin urmare $E = K[\alpha]$ este un K -spațiu vectorial având o bază egală cu $\{1, \alpha, \dots, \alpha^{n-1}\}$.

Intr-adevăr, rezultă că E este un inel finit. Cum E este un subinel al unui corp rezultă că E este un corp. Deci E este o extindere finită cu $[E : K] = n$.

d) Cu notatiile de la pct. c) E conține toate rădăcinile polinoamelor care aparțin mulțimii X_{p^n} .

Intr-adevăr, cum $[E : K] = n$, atunci $E \cong K^n$ ca un K -spațiu vectorial și deci $|E| = q^n$. Conform pct. b), E este egală cu mulțimea rădăcinilor polinomului $X^{q^n} - X$. Cum f este un polinom redusibil iar $f(x) = 0$, atunci f divide polinomul $X^{q^n} - X$ și deci toate rădăcinile

lui f sint conținute în multimea rădăcinilor polinomului $X^{q^n} - X$ și deci E conține toate rădăcinile lui f .

Dacă $g \in X_{n,q}$ este un alt polinom, atunci un raționament similar celui dinainte, ne arată că rădăcinile lui g se găsesc în multimea E .

În plus, dacă $g \neq f$, atunci multimea rădăcinilor lui f este disjunctă de multimea rădăcinilor lui g , deoarece dacă f și g au o rădăcină comună, cum f și g sunt ireductibile, rezultă $f \mid g$ și $g \mid f$ adică $f = g$.

e) Fie $\beta \in E$ un element oarecare. Atunci există un $m \mid n$ și un $h \in X_{m,q}$ astfel încit β este o rădăcină a polinomului h .

Într-adevăr, cum $[E : K] < \infty$, atunci sistemul de elemente $1, \beta, \beta^2, \dots, \beta^k, \dots$ este liniar dependent peste corpul K , înseamnă că există elementele $b_0, b_1, \dots, b_s \in K$ nu toate nule astfel încit $b_0 + b_1\beta + \dots + b_s\beta^s = 0$. Dacă notăm cu $g(X)$ polinomul $g(X) = b_0 + b_1X + \dots + b_sX^s$, atunci $g(\beta) = 0$. Vom nota cu $h(X)$ un polinom monic nenul de gradul cel mai mic astfel încit $h(\beta) = 0$. Este ușor de văzut că $h(X)$ este ireductibil. Să notăm cu $m = \text{grad } h$. Cum $h(\beta) = 0$, atunci corpul $F = K[\beta]$ este o extindere finită a lui K astfel încit $[F : K] = m$. Pe de altă parte, avem $K \subset F \subset E$. Cum $|E|$ este o putere a lui $|F|$ rezultă în particular că $m \mid n$. Din afirmația e) rezultă, că $E = \bigcup_{h \in X_{m,q}} \{\text{rădăcinile polinomului } h\}$. Cum multimile care apar în această reuniune sint disjuncte două cîte două și cum un polinom $h \in X_{m,q}$ are m rădăcini, atunci obținem egalitatea

$$|E| = \sum_{m \mid n} m |X_{m,q}| \text{ sau } q^n = \sum_{m \mid n} m N_{m,q}.$$

Folosind formula de inversiune a lui Möbius obținem că

$$N_{n,q} = \frac{1}{n} \sum_{d \mid n} \mu\left(\frac{n}{d}\right) q^d$$

care ne dă numărul polinoamelor monice ireductibile de gradul n peste corpul finit K avînd q elemente.

De exemplu, dacă $K = \mathbb{Z}_2$ avem $q = 2$ și avem $N_{1,2} = 2$;

$$N_{2,2} = \frac{1}{2} (2^2 - 2) = 1; \quad N_{3,2} = \frac{1}{3} (2^3 - 2) = 2;$$

$$N_{4,2} = \frac{1}{4} (2^4 - 2^2) = 3; \quad N_{5,2} = \frac{1}{5} (2^5 - 2) = 6;$$

$$N_{6,2} = \frac{1}{6} (2^6 - 2^3 - 2^2 + 2) = 9.$$

Dacă $K = \mathbb{Z}_3$ avem $q = 3$ și deci $N_{1,3} = 3$;

$$N_{2,3} = \frac{1}{2} (3^2 - 3) = 3; \quad N_{3,3} = \frac{1}{3} (3^3 - 3) = 12;$$

$$N_{4,3} = \frac{1}{4} (3^4 - 3^2) = 18; \quad N_{5,3} = \frac{1}{5} (3^5 - 3) = 48;$$

$$N_{6,3} = \frac{1}{6} (3^6 - 3^3 - 3^2 + 3) = 232.$$

EXERCITII

1. Notăm cu \mathbb{C}^N mulțimea sirurilor de numere complexe
 $x = (\alpha_1, \alpha_2, \dots, \alpha_n, \dots)$

Să se arate

- a) \mathbb{C}^N este un \mathbb{C} -spațiu vectorial față de operațiile

$$\lambda x = (\lambda \alpha_1, \lambda \alpha_2, \dots, \lambda \alpha_n, \dots), \quad \lambda \in \mathbb{C}$$

dacă $y = (\beta_1, \beta_2, \dots, \beta_n, \dots)$, atunci

$$x + y = (\alpha_1 + \beta_1, \alpha_2 + \beta_2, \dots, \alpha_n + \beta_n, \dots)$$

- b) Fie $p, q \in \mathbb{C}$ cu $q \neq 0$. Să se arate că mulțimea sirurilor $x = (\alpha_1, \alpha_2, \dots, \alpha_n, \dots)$ care verifică proprietatea

$$\alpha_n = p\alpha_{n-1} + q\alpha_{n-2}, \quad n = 3, 4, \dots \quad (*)$$

este un spațiu vectorial V al lui \mathbb{C}^N de dimensiune 2.

- c) Fie ecuația algebrică (numită ecuația caracteristică)

$$\lambda^2 - p\lambda - q = 0.$$

Dacă rădăcinile λ_1, λ_2 ale ecuației caracteristice sunt distințte, să se arate că sirurile

$$e_1 = (\lambda_1, \lambda_1^2, \lambda_1^3, \dots, \lambda_1^n, \dots)$$

$$e_2 = (\lambda_2, \lambda_2^2, \lambda_2^3, \dots, \lambda_2^n, \dots)$$

constituie o bază pentru V .

- d) Dacă rădăcinile ecuației caracteristice sunt egale $\lambda_1 = \lambda_2 = \lambda$, să se arate că sirurile

$$e_1 = (\lambda, \lambda^2, \lambda^3, \dots, \lambda^n, \dots)$$

$$e_2 = (1, 2\lambda, 3\lambda^2, \dots, n\lambda^{n-1}, \dots)$$

constituie o bază pentru V .

e) Să se determine α_n în funcție de x_1, x_2 și n , unde α_n verifică relația de recurență (*).

2. Să se determine în funcție de n sirurile $x_1, x_2, \dots, x_n, \dots$, unde $x_n = x_{n-1} + x_{n-2}$ oricare ar fi $n \geq 3$ iar $x_1 = x_2 = 1$ (sirul numerelor lui Fibonacci).

3. Să se calculeze determinantul de ordinul n având forma următoare

$$D_n = \begin{vmatrix} a & b & 0 & \dots & 0 & 0 \\ c & a & b & 0 & \dots & 0 & 0 \\ 0 & c & a & b & \dots & 0 & 0 \\ \vdots & & & & & & \\ 0 & 0 & 0 & \dots & c & a & b \\ 0 & 0 & 0 & \dots & c & a & \end{vmatrix}$$

(D_n se numește determinant tridiagonal).

Indicație. Dezvoltând după ultima linie avem relația de recurență

$$D_n = aD_{n-1} - bcD_{n-2}, \quad n = 3, 4, \dots$$

4. Să se calculeze determinanții

$$\text{a)} \begin{vmatrix} 0 & 1 & 0 & 0 & \dots & 0 & 0 \\ 1 & 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & 1 & \dots & 0 & 0 \\ \dots & & & & & & \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & 0 & 0 & \dots & 1 & 0 \end{vmatrix}; \quad \text{b)} \begin{vmatrix} 0 & 1 & 0 & 0 & \dots & 0 & 0 \\ -1 & 0 & 1 & 0 & \dots & 0 & 0 \\ 0 & -1 & 0 & 1 & \dots & 0 & 0 \\ \dots & & & & & & \\ 0 & 0 & 0 & 0 & \dots & 0 & 1 \\ 0 & 0 & 0 & 0 & \dots & -1 & 0 \end{vmatrix}$$

$$\text{c)} \begin{vmatrix} 2 & 1 & 0 & 0 & \dots & 0 & 0 \\ 1 & 2 & 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & 2 & 1 & \dots & 0 & 0 \\ \dots & & & & & & \\ 0 & 0 & 0 & 0 & \dots & 2 & 1 \\ 0 & 0 & 0 & 0 & \dots & 1 & 2 \end{vmatrix}$$

Indicație. a) Aplicind 3) avem relația de recurență $D_n = -D_{n-2}$ dacă $n \geq 3$ (avem $D_1 = 0$ și $D_2 = -1$). Ecuția caracteristică este $\lambda^2 + 1 = 0$ având rădăcinile $\lambda_1 = i$ și $\lambda_2 = -i$. Deci $D_n = c_1 \lambda_1^n + c_2 \lambda_2^n$. Cum $c_1 \lambda_1 + c_2 \lambda_2 = 0$ și $c_1 \lambda_1^2 + c_2 \lambda_2^2 = -1$ obținem $c_1 = c_2 = \frac{1}{2}$. Deci $D_n = \frac{1}{2} (i^n + (-i)^n)$ $\Rightarrow D_n = 0$, n impar și $D_n = (-1)^k$ dacă $n = 2k$.

Observație. Acest determinant rezultă ușor și altfel din relația de recurență $D_n = -D_{n-2}$.
Pentru b) și c) se procedează identic.

5. Să se determine semnul următorilor termeni din dezvoltarea determinantului:

a) $a_{14}a_{23}a_{31}a_{42}$; b) $a_{16}a_{25}a_{32}a_{43}a_{54}a_{61}$; c) $a_{71}a_{17}a_{36}a_{54}a_{43}a_{27}a_{62}$.

6. Să se determine i și j astfel încât termenul $a_{12}a_{21}a_{36}a_{41}a_{52}a_{61}$ să intre cu semnul $(-)$ în dezvoltarea determinantului de ordinul 6.

7. Folosind definiția determinantului să se calculeze

$$\left| \begin{array}{ccccc} a_{11} & 0 & 0 & \dots & 0 \\ a_{21} & a_{22} & 0 & \dots & 0 \\ a_{31} & a_{32} & a_{33} & \dots & 0 \\ \vdots & & & & \ddots \\ a_{n1} & a_{n2} & a_{n3} & \dots & a_{nn} \end{array} \right| \quad \text{și} \quad \left| \begin{array}{ccccc} 0 & \dots & 0 & 0 & a_{1n} \\ 0 & \dots & 0 & a_{2n-1} & a_{2n} \\ 0 & \dots & a_{3n-2} & a_{3n-1} & a_{3n} \\ \ddots & & & & \ddots \\ a_{n1} & a_{n2} & \dots & \dots & a_{nn} \end{array} \right|$$

8. Să se arate prin inducție că

$$\left| \begin{array}{cccc} 1 & 1 & \dots & 1 \\ a_1 & a_2 & \dots & a_n \\ a_1^2 & a_2^2 & \dots & a_n^2 \\ \vdots & & & \ddots \\ a_1^{n-1} & a_2^{n-1} & \dots & a_n^{n-1} \end{array} \right| = \prod_{1 \leq i < j \leq n} (a_j - a_i).$$

9. Dacă A este o matrice de tipul $m \times n$ ($m \geq n$), atunci

$$\det(^t A A) = \sum_M M^2,$$

unde M parcurge toți minorii de ordinul n ai lui A (care sunt în număr de C_m^n).

10. Fie R un inel comutativ, $A \in \mathcal{M}_n(R)$; $B \in \mathcal{M}_n(R)$ și $C \in \mathcal{M}(m, n, R)$. Să se arate că

$$\det \begin{pmatrix} A & C \\ 0 & B \end{pmatrix} = \det(A) \cdot \det(B).$$

11. O matrice $A = (a_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$ se numește antisimetrică dacă $a_{ij} = -a_{ji}$, oricare ar fi i și j .

Să se arate că dacă n este impar, atunci $\det A = 0$.

12. Fie $A = (a_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$ o matrice cu elemente numere complexe.

Dacă $a_{ij} = \bar{a}_{ji}$, oricare ar fi i și j , atunci $\det A$ este un număr real.

Indicație. Dacă $B = (b_{ij})_{\substack{1 \leq i \leq n \\ 1 \leq j \leq n}}$, unde $b_{ij} = \bar{a}_{ij}$, atunci folosind

definiția determinantului avem că $\det B = \overline{\det A}$. Luind $B = ^t A$ obținem $\det(^t A) = \det A$ de unde $\det(A) = \overline{\det(A)}$ și deci $\det A \in \mathbb{R}$.

13. Fie A_n matricea pătratică de ordinul n ale cărei elemente sunt toate egale cu 1. Să se arate că:

a) $A_n^2 = nA_n$; b) $I_n - A_n$ este inversabilă și avem

$$(I_n - A_n)^{-1} = I_n - \frac{1}{n-1} A_n.$$

14. Fie $A \in \mathcal{M}(m, n, k)$ de rang 1 (k este un corp).

Să se arate că:

a) Există elementele b_1, b_2, \dots, b_m și c_1, c_2, \dots, c_n astfel încit oricare ar fi i, j să avem $a_{ij} = b_i c_j$.

b) Matricea A se poate scrie ca produsul XY a două matrici X, Y , unde $X \in \mathcal{M}(m, 1, k)$ iar $Y \in \mathcal{M}(1, n, k)$.

15. Fie $A \in \mathcal{M}_n(\mathbb{C})$ cu rang $A=1$. Să se arate că:

a) există un număr α astfel încât $A^2 = \alpha A$;

b) dacă $\alpha \neq -1$, atunci matricea $I_n + A$ este inversabilă și avem:

$$(I_n + A)^{-1} = I_n - \frac{1}{n+1} A.$$

16. Să se calculeze rangul următoarelor matrici:

$$\begin{pmatrix} -1 & 5 & 2 & 3 & 5 \\ 6 & -12 & 3 & -7 & -8 \\ -3 & 7 & 9 & 4 & 15 \\ -3 & 2 & 0 & 1 & 4 \end{pmatrix}; \quad \begin{pmatrix} 3 & 0 & -4 & -5 & 3 & -4 \\ 0 & -1 & 0 & 4 & 3 & 0 \\ 1 & 2 & 0 & -3 & 0 & 0 \\ 0 & -3 & 0 & 2 & 0 & 4 \\ 0 & 4 & 2 & -1 & 0 & 0 \end{pmatrix}$$

17. Fie $A \in \mathcal{M}(m, n, k)$ și $B \in \mathcal{M}(n, p, k)$, unde k este un corp. Să se arate că

$$\text{rang}(AB) \leq \min(\text{rang } A, \text{ rang } B).$$

Indicație. Coloanele lui AB sunt combinații liniare de coloanele lui A iar liniile lui AB sunt combinații liniare de liniile lui B .

18. Fie $A \in \mathcal{M}(m, n, k)$ și $B \in \mathcal{M}(n, m, k)$, unde $m > n$. Să se arate că $\det(AB) = 0$.

Indicație. Se aplică 17).

19. Fie $A \in \mathcal{M}(m, n, k)$ cu $m > n$. Să se arate că $\det(A^t A) = 0$.

20. Se numește matrice de permutări o matrice P cu proprietatea că pentru fiecare linie și fiecare coloană se află 1, restul elementelor fiind zero.

Să se arate că P este un produs de matrici elementare de tipul I). Să se arate că $\det P = \pm 1$.

21. Să se rezolve sistemul de ecuații liniare

a)
$$\begin{cases} x_1 + 4x_2 + 2x_3 - 3x_5 = 0 \\ 2x_1 + 9x_2 + 5x_3 + 2x_4 + x_5 = 0 \\ x_1 + 3x_2 + x_3 - 2x_4 - 9x_5 = 0 \end{cases}$$

b)
$$\begin{cases} -2x_1 + x_2 + x_3 + x_4 + x_5 = 0 \\ x_1 - 2x_2 + x_3 + x_4 + x_5 = 0 \\ 4x_1 + x_2 - 5x_3 - 5x_4 - 5x_5 = 0 \\ x_1 + x_2 + 2x_3 + x_4 + x_5 = 0 \\ x_1 + x_2 + 2x_3 + x_4 + x_5 = 0 \end{cases}$$

c)
$$\begin{cases} (3 - 2\lambda)x_1 + (2 - \lambda)x_2 + x_3 = \lambda \\ (2 - \lambda)x_1 + (2 - \lambda)x_2 + x_3 = 1 \\ x_1 + x_2 + (2 - \lambda)x_3 = 1. \end{cases}$$

22. Fie $A = (a_{ij})_{1 \leq i,j \leq n}$ o matrice pătratică de ordinul n unde $a_{ij} \in \mathbb{R}$ și $|a_{ij}| \leq 1$. Să se arate că maximul valorilor absolute ale determinanților matricelor A de forma de mai sus este realizat cind $a_{ij} \in \{-1, 1\}$ oricare ar fi $i, j = 1, 2, \dots, n$.

Indicație. Fie $A = (a_{ij})_{1 \leq i,j \leq n}$ o matrice pentru care $|\det A|$ este maxim. Presupunem că există un element a_{ij} astfel încât $|a_{ij}| < 1$. Notăm cu $d = \det A$ și d_{ij} complementul algebric al elementului a_{ij} .

Presupunem că $d \geq 0$; dacă $d_{ij} > 0$, atunci determinantul crește dacă înlocuim pe a_{ij} cu $+1$; dacă $d_{ij} < 0$, atunci determinantul crește dacă înlocuim pe a_{ij} cu -1 . Dacă $d < 0$, atunci determinantul crește dacă înlocuim pe $a_{ij} = -\text{sgn}(d_{ij})$. Dacă $d_{ij} = 0$, valoarea determinantului nu se modifică dacă înlocuim a_{ij} cu ± 1 . Deci pentru orice matrice $A = (a_{ij})_{1 \leq i,j \leq n}$ care are un element $-1 < a_{ij} < 1$, găsim o matrice B în care elementele sale sunt ± 1 astfel încit $|\det A| < |\det B|$.

23. Fie $A = (a_{ij})_{1 \leq i,j \leq n}$ o matrice pătratică de ordinul n astfel încât $a_{ij} \in \{-1, 1\}$ oricare ar fi $i, j = 1, 2, \dots, n$. Să se arate că $\det A \in \mathbb{Z}$ și 2^{n-1} divide $\det A$.

Indicație. Adunând prima linie la toate celelalte linii obținem o matrice care are pe liniile $2, 3, \dots, n$ elementele 0, $+2$, -2 . În continuare se aplică proprietățile determinanților.

24. Să se calculeze valoarea maximă (resp. minimă) a determinanților de ordinul 3 și 4 ale cărui elemente sunt -1 și $+1$.

Indicație. Fie $A = (a_{ij})_{1 \leq i, j \leq 3}$ cu $a_{ij} \in \{-1, 1\}$. Folosind dezvoltarea după linii, rezultă că maximul poate fi cel mult $+6$.

Din exercițiul 23 rezultă că 4 divide $\det A$. Deci $\det A$ poate fi $-4, 0, +4$. Se arată ușor că există o matrice pentru care $\det A = +4$; de exemplu,

$$A = \begin{pmatrix} -1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

Deci maximul este $+4$ (resp. minimul este -4).

Cind determinanții sunt de ordinul 4, se aplică prima parte a acestui exercițiu și exercițiul 23. Se găsește că maximul este $+16$ iar minimul este -16 .

25. Fie V și V' , două K -spații vectoriale de dimensiune finită peste corpul K , $\dim_K V = m$, $\dim_K V' = n$. Fie $u: V \rightarrow V'$ o aplicație liniară. Definim *rangul* aplicației u ca fiind $\dim_K \text{Im } u$ și vom nota cu rang $u = \dim_K \text{Im } u$. Să se arate că:

a) Dacă $u: V \rightarrow V'$ și $v: V' \rightarrow V''$ sunt aplicații liniare, atunci rang $(v \circ u) \leq \min(\text{rang } u, \text{rang } v)$.

b) Dacă $u, v: V \rightarrow V'$ sunt aplicații liniare, atunci rang $(u+v) \leq \text{rang } u + \text{rang } v$.

c) Fie e_1, e_2, \dots, e_m o bază a lui V iar f_1, f_2, \dots, f_n o bază a lui V' . Notăm cu A matricea asociată lui u relativ la cele două baze, adică $A = (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$, unde $u(e_i) = \sum_{j=1}^n a_{ij} f_j$, $i = 1, \dots, m$. Să se arate că rang $u = \text{rang } A$.

d) Să se dea o nouă demonstrație exercițiului 17.

Indicație. a) Avem $\text{Im}(v \circ u) \subseteq \text{Im } v$ și deci rang $(v \circ u) \leq \text{rang } v$. Cum $\text{Im } (v \circ u)$ este izomorf cu un spațiu cît al lui $\text{Im } u$ rezultă că $\dim_K \text{Im}(v \circ u) \leq \dim_K \text{Im } u$ și deci rang $(v \circ u) \leq \text{rang } u$.

b) $\text{Im}(u+v) \subset \text{Im } u + \text{Im } v$.

c). Avem că $\text{Im } u$ este generat de $u(e_1), \dots, u(e_m)$. Dacă $r = \text{rang } u$, atunci există r vectori liniar independenti dintre cei $u(e_1), \dots, u(e_m)$. Fie aceştia $u(e_1), \dots, u(e_r)$. Deci $u(e_1), \dots, u(e_r)$ constituie o bază pentru $\text{Im } u$.

În continuare folosind teorema lui Kronecker se arată $r = \text{rang } A$.
d) se aplică a).

26. Fie X o mulțime finită avind n elemente. Să se determine funcția Möbius a mulțimii ordonate $(\mathcal{P}(X), \subseteq)$ folosind izomorfismul de latice dat de:

$$\varphi: \mathcal{P}(X) \rightarrow \{0, 1\}$$

$$\varphi(A)(x) = \begin{cases} 1 & \text{dacă } x \in A \\ 0 & \text{dacă } x \notin A. \end{cases}$$

B I B L I O G R A F I E

1. Aigner, M., *Combinatorial Theory*, Springer-Verlag, Berlin, Heidelberg, New York-1979.
2. Atiyah, M., Mac Donald I., *Introduction to commutative algebra*, Addison Wesley Publishing Company, 1969.
3. Becheanu, Mircea, Viraciu, C., *Probleme de teoria grupurilor*, Tipografia Universității din București, 1982.
4. Bourbaki, N., *Algèbre*, chap. 1-9, Act. Sci. Ind. Hermann, Paris.
5. Bourbaki, N., *Algèbre commutative*, chap. 1-7, Act. Sci. Ind. Hermann, Paris.
6. Fadeev, D.K., Sominiski, I., *Sbornik zadaci po visšej algebre*, Fizmatgiz, Moskva, 1961.
7. Gallură, Gh., *Algebra*, Editura didactică și pedagogică, București 1972.
8. Hungerford, T., *Algebra*, Graduate Texts in Mathematics Springer Verlag, New York Heidelberg, Berlin.
9. Ikramov, H.D., *Zadacnik po lineinoi algebre*, Moskva, 1975.
10. Ion, D. Ion, Năstăsescu, C., Niță, C., *Complemente de algebră*, Editura didactică și pedagogică, București, 1984.
11. Ion, D. Ion, Niță, C., *Elemente de aritmetică cu aplicații în tehnici de calcul*, Editura didactică și pedagogică, București, 1978.
12. Ion, D. Ion, Niță C., Popescu, D., Radu, N., *Probleme de algebră*, Editura didactică și pedagogică; București, 1981.
13. Ion, D. Ion, Radu, N., *Algebră*, Editura didactică și pedagogică, București, 1981.
14. Jacobson, N., *Basic Algebra*, J. Freeman, San Francisco, 1965.
15. Kaplansky, I., *Commutative Rings*, Boston, Allyn and Bacon Inc., 1970.
16. Kostrikin, A.I., *Vvedenie v algebrę*, Moskva, 1977.
17. Kuroš, A.G., *Iecții po obycei algebre*, Moskva, 1962.
18. Kuroš, A.G., *Teoriia grupp*, Moskva, 1967.
19. Lang, S., *Algebra*, Addison-Wiley Publishing Company, 1965.
20. Năstăsescu, C., *Introducere în teoria mulțimilor*, Editura didactică și pedagogică, București, 1974.
21. Năstăsescu, C., *Inele, module, categorii*, Editura Academiei, București, 1970.
22. Năstăsescu, C., *Teoria dimensiunii în algebră necomutativă*, Editura Academiei, București, 1983.
23. Năstăsescu, C., Niță, C., *Teoria calitativă a ecuațiilor algebrice*, Editura tehnică, București, 1979.

24. Năstăsescu, C., Niță, C., Brandiburu, M., Joița D., *Exerciții și probleme de algebră (pentru clasele IX–XII)*, Editura didactică și pedagogică, București, 1981.
25. Năstăsescu, C., Niță, C., Vraciu, C., *Aritmetică și Algebră*, Tipografia Universității din București, 1986.
26. Niță, C., Spircu, T., *Probleme de structuri algebrice*, Editura tehnica, București, 1974.
27. Popescu, N., *Categorii abeliene*, Editura Academiei, București, 1971.
28. Popescu, D., Vraciu, C., *Elemente de teoria grupurilor finite*, Editura științifică și enciclopedică, București, 1985.
29. Purdea, I., Pic, Gh., *Tratat de algebră modernă*, I., Editura Academiei, București, 1977.
30. Radu, N. și colab., *Algebră pentru perfecționarea profesorilor*, Editura didactică și pedagogică, București, 1983.
31. Rose, A course on Group Theory, Cambridge, Londra, 1978.
32. Suzuki, M., Structure of a Group and the Structure of its Lattice of Subgroup, Berlin, Heidelberg, Springer Verlag, 1967.
33. Zariski, O., Samuel P., *Commutative Algebra*, vol. I, II, Princeton, 1958, 1960.

Redactor: PETRE MOCANU
Teknoredactor: MAGDALENA IACOB

Bun de tipar: 29.VII.1986

Format: 16/61 × 86; Coli de tipar: 22
C.Z. pentru biblioteci mari și mici: 512



**Intreprinderea poligrafică Brașov,
Str. Zizinului nr. 110
Comanda 1177
Republie Socialistă România**