CURS I

NOŢIUNI PRELIMINARE

§ 1. MULŢIMI

Prin *mulţime* înţelegem o colecţie de obiecte care se numesc elementele mulţimii. Vom nota cu litere mari mulţimile, iar cu litere mici elementele lor. Dacă A este o mulţime şi x un element al său, vom scrie $x \in A$ şi vom citi „x aparţine lui A". Dacă x nu se găseşte în A, atunci vom scrie $x \notin A$ şi vom citi „x nu aparţine lui A".

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

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

ii) Specificând o proprietate pe care o au elementele sale şi nu le au alte elemente. Mai precis, dată o proprietate se poate vorbi de mulţimea acelor obiecte pentru care proprietatea respectivă are loc. Mulţimile definite în acest mod se vor nota prin A = {x | P(x)}, adică mulţimea acelor obiecte x pentru care are loc P(x).

De exemplu, să considerăm proprietatea "a fi număr natural par": în acest caz mulţimea A va fi mulţimea numerelor naturale pare.

Pentru câteva mulţimi care vor fi des utilizate avem notaţii speciale: cu **N** vom nota mulţimea numerelor naturale, adică **N** = {0, 1, 2, 3, ...}. Cu $\mathbf{N}^*$ vom nota mulţimea numerelor naturale nenule, adică $\mathbf{N}^*$ = {1, 2, 3, ...}. Cu **Z** vom nota mulţimea numerelor întregi, cu **Q** mulţimea numerelor raţionale, cu **R** mulţimea numerelor reale, iar cu **C** mulţimea numerelor complexe.

În teoria mulţimilor se admite existenţa unei mulţimi care nu are nici un element. Aceasta se numeşte *mulţimea vidă* şi se notează cu simbolul $\varnothing$.

Dacă A şi B sunt două mulţimi, vom spune că A este o *submulţime* a lui B (sau A este *conţinută*, respectiv *inclusă* în B) şi vom scrie $A \subseteq B$ dacă orice element al mulţimii A este şi element al mulţimii B. Simbolic scriem astfel: $\forall x,\ x \in A \Rightarrow x \in B$. Dacă incluziunea este strictă, adică există elemente în B care nu sunt în A, scriem $A \subset B$.

Mulţimea vidă este submulţime a oricărei mulţimi. Între mulţimile de numere considerate mai înainte avem incluziunile: $\mathbf{N}^* \subset \mathbf{N} \subset \mathbf{Z} \subset \mathbf{Q} \subset \mathbf{R} \subset \mathbf{C}$.

Două mulţimi A şi B sunt *egale* dacă au aceleaşi elemente, adică $A = B \Leftrightarrow A \subseteq B$ şi $B \subseteq A$ („$\Leftrightarrow$" înseamnă "dacă şi numai dacă").

Relaţia de incluziune (resp. relaţia de egalitate) între mulţimi are proprietăţile următoare:

a) este reflexivă, adică $A \subseteq A$ (resp. A = A);

b) este antisimetrică, adică din $A \subseteq B$ şi $B \subseteq A$ rezultă A = B (resp. este simetrică adică $A = B \Rightarrow B = A$);

c) este tranzitivă, adică $A \subseteq B$ şi $B \subseteq C \Rightarrow A \subseteq C$ (resp. $A = B$ şi $B = C \Rightarrow A = C$).

Cu mulţimi se fac următoarele operaţii:

• *intersecţia* a două mulţimi A şi B înseamnă mulţimea

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

• *reuniunea* mulţimilor A şi B înseamnă mulţimea

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

În cazul când $A \cap B = \varnothing$ spunem că mulţimile A şi B sunt *disjuncte*.

Operaţiile de intersecţie şi reuniune au următoarele proprietăţi:

$$A \cup \varnothing = A;\ A \cap \varnothing = \varnothing$$

$$A \cup B = B \cup A;\ A \cap B = B \cap A \text{ (comutativitate)}$$

$$A \cup (B \cup C) = (A \cup B) \cup C;\ A \cap (B \cap C) = (A \cap B) \cap C \text{ (asociativitate)}$$

$$A \cup A = A;\ A \cap A = A \text{ (idempotenţă)}$$

$A \subseteq B$ dacă şi numai dacă $A \cup B = B$; $A \subseteq B$ dacă şi numai dacă $A \cap B = A$

Operaţiile de intersecţie şi reuniune satisfac egalităţile:

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

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

numite *distributivitatea intersecţiei (resp. reuniunii) faţă de reuniune (resp. intersecţie).*

Prin *diferenţa* mulţimilor B şi A înţelegem mulţimea

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

Să observăm că $A \subseteq B$ dacă şi numai dacă $A \setminus B = \varnothing$.

Dacă A este o submulţime a lui B, atunci diferenţa $B \setminus A$ se numeşte *complementara* mulţimii A în B şi se notează cu $C_B A$. De exemplu $C_B\varnothing = B$, iar $C_B B = \varnothing$. De asemenea, $A \cup C_B A = B$, iar $A \cap C_B A = \varnothing$, adică A şi $C_B A$ sunt disjuncte.

Dacă A şi A' sunt două submulţimi ale mulţimii B au loc egalităţile:

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

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

numite *formulele lui De Morgan.*

Relaţia de incluziune ne permite să definim *mulţimea părţilor* unei mulţimi T notată cu $\mathscr{P}(T)$, adică $\mathscr{P}(T)$ are ca elemente toate submulţimile mulţimii T.

Fie A şi B două mulţimi arbitrare. Dacă $a \in A$ şi $b \in B$, atunci putem forma *perechea ordonată* (a, b), adică perechea formată din elementele a şi 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) şi (a_2, b_2) sunt egale dacă şi numai dacă $a_1 = a_2$ şi $b_1 = b_2$. Prin *produsul cartezian* al mulţimilor A şi B înţelegem mulţimea

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

Când $A = B$, notăm $A^2 = A \times A$.

Se observă că dacă $A = \emptyset$ sau $B = \emptyset$, atunci $A \times B = \emptyset$. În plus, dacă A are *m* elemente iar B are *n* elemente, atunci mulţimea $A \times B$ are *mn* elemente.

§ 2. FUNCŢII

Fiind date mulţimile A şi B, prin *funcţie* (sau *aplicaţie*) definită pe mulţimea A cu valori în mulţimea B se înţelege o „lege" f în baza căreia oricărui element $a \in A$ i se asociază un unic element, notat f(a), din B.

Mulţimea A se numeşte *domeniul de definiţie* al funcţiei f, iar mulţimea B se numeşte *domeniul valorilor* funcţiei f (sau *codomeniul* funcţiei f).

O funcţie f este determinată atunci când se dă domeniul de definiţie, codomeniul său şi modul cum acţionează f. O funcţie f definită pe mulţimea A cu valori în B se notează $f : A \to B$.

Fie $f : A \to B$ o funcţie. Prin *graficul* lui f se înţelege mulţimea $G_f = \{(a, b) \mid a \in A, b \in B \text{ şi } b = f(a)\}$. Evident $G_f \subseteq A \times B$. Dacă ştim graficul unei funcţii, atunci putem identifica domeniul, codomeniul şi „legea" funcţiei. De aceea este mult mai riguros să definim o funcţie ca un triplet (A, B, G) format din trei mulţimi A, B şi $G \subseteq A \times B$ cu proprietatea că $\forall a \in A\ \exists!\ b \in B$ astfel încât $(a, b) \in G$.

Dacă A şi B sunt două mulţimi oarecare, vom nota cu $B^A = \{f : A \to B \mid f \text{ funcţie}\}$, adică mulţimea tuturor funcţiilor definite pe A cu valori în B.

Dacă A este o mulţime oarecare, funcţia $1_A : A \to A$, unde $1_A(a) = a$ oricare ar fi $a \in A$ se numeşte *funcţia identică* a mulţimii A.

Dacă $A \subseteq B$, atunci funcţia $i : A \to B$, unde $i(a) = a$ oricare ar fi $a \in A$ se numeşte *funcţia incluziune* a submulţimii A a lui B.

O funcţie $f : A \to B$ se numeşte *restricţie* a funcţiei $g : A' \to B$ dacă $A \subseteq A'$ şi $f(a) = g(a)$, oricare ar fi $a \in A$. (Să observăm că $f = g \circ i$, unde $i : A \to A'$ este funcţia incluziune.) f se notează cu $g_{|A}$. În această situaţie g se numeşte *extindere* a lui f.

O funcţie $f : A \to B$ se numeşte *corestricţie* a funcţiei $g : A \to B'$ dacă $\operatorname{Im} g \subseteq B \subseteq B'$ şi $f(a) = g(a)$, oricare ar fi $a \in A$.

Dacă A_1 şi A_2 sunt două mulţimi oarecare, definim o funcţie $p_1 : A_1 \times A_2 \to A_1$ prin $p_1((a_1, a_2)) = a_1$ oricare ar fi $(a_1, a_2) \in A_1 \times A_2$. Această funcţie se numeşte *proiecţia pe prima componentă*. Analog definim o funcţie $p_2 : A_1 \times A_2 \to A_2$ prin $p_2((a_1, a_2)) = a_2$ oricare ar fi $(a_1, a_2) \in A_1 \times A_2$ şi o numim *proiecţia pe a doua componentă*.

Dacă A_1, A_2, B_1, B_2 sunt mulţimi oarecare şi $f_1 : A_1 \to B_1$, $f_2 : A_2 \to B_2$ sunt două funcţii, atunci putem defini o funcţie $f_1 \times f_2 : A_1 \times A_2 \to B_1 \times B_2$ prin $(f_1 \times f_2)((a_1, a_2)) = (f_1(a_1), f_2(a_2))$ oricare ar fi $(a_1, a_2) \in A_1 \times A_2$. Această funcţie se numeşte *produsul cartezian* al lui f_1 cu f_2.

Dacă A şi T sunt două mulţimi şi $A \subseteq T$, definim o funcţie $\chi_A : T \to \{0, 1\}$ astfel: $\chi_A(t) = 1$ dacă $t \in A$, respectiv $\chi_A(t) = 0$ dacă $t \in T \setminus A$. Această funcţie se numeşte *funcţia caracteristică* a lui A.

Să observăm că dacă A şi A' sunt submulţimi ale lui T, atunci $A = A'$ dacă şi numai dacă $\chi_A = \chi_{A'}$.

Exerciţiu. Fie A şi A' submulţimi ale lui T. Arătaţi că:

1) $\chi_{A\cap A'} = \chi_A \chi_{A'}$.

2) $\chi_{A\cup A'} = \chi_A + \chi_{A'} - \chi_A \chi_{A'}$. În particular, dacă A şi A' sunt disjuncte avem $\chi_{A\cup A'} = \chi_A + \chi_{A'}$.

3) $\chi_{A\setminus A'} = \chi_A(1 - \chi_{A'})$.

Dacă $f : A \to B$ este o funcţie şi $A' \subseteq A$ este o submulţime a mulţimii A, notăm

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

numită *imaginea directă* a lui A' prin funcţia f şi este o submulţime a lui B. În cazul particular când $A' = A$, notăm $f(A) = \text{Im } f$ şi se numeşte *imaginea* funcţiei f.

Similar, dacă $B' \subseteq B$ este o submulţime a lui B, atunci notăm

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

Această submulţime se numeşte *imaginea inversă* a lui B' prin funcţia f şi este o submulţime a lui A.

Propoziţia 2.1. Considerăm o funcţie $f : A \to B$.

a) Dacă $M \subseteq N \subseteq A$, atunci $f(M) \subseteq f(N)$.

b) Dacă $M \subseteq A$ şi $N \subseteq A$, atunci $f(M \cup N) = f(M) \cup f(N)$.

c) Dacă $M \subseteq A$ şi $N \subseteq A$, atunci $f(M \cap N) \subseteq f(M) \cap f(N)$.

d) Dacă $M \subseteq A$, atunci $M \subseteq f^{-1}(f(M))$.

e) Dacă $P \subseteq Q \subseteq B$, atunci $f^{-1}(P) \subseteq f^{-1}(Q)$.

f) Dacă $P \subseteq B$ şi $Q \subseteq B$, atunci $f^{-1}(P \cup Q) = f^{-1}(P) \cup f^{-1}(Q)$.

g) Dacă $P \subseteq B$ şi $Q \subseteq B$, atunci $f^{-1}(P \cap Q) = f^{-1}(P) \cap f^{-1}(Q)$.

h) Dacă $P \subseteq B$, atunci $f(f^{-1}(P)) \subseteq P$.

Exerciţii.

1) Daţi exemple de funcţii $f : A \to B$ cu proprietatea că există $M \subseteq A$ şi $N \subseteq A$ astfel încât $f(M \cap N) \subset f(M) \cap f(N)$.

2) Daţi exemple de funcţii $f : A \to B$ cu proprietatea că există $M \subseteq A$ astfel încât $M \subset f^{-1}(f(M))$.

3) Daţi exemple de funcţii $f : A \to B$ cu proprietatea că există $P \subseteq B$ astfel încât $f(f^{-1}(P)) \subset P$.

O funcţie $f : A \to B$ se numeşte *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 $a = a'$.

Propoziţia 2.2. (i) O funcţie $f : A \to B$ este injectivă dacă şi numai dacă $\forall M \subseteq A$ şi $\forall N \subseteq A$, $f(M \cap N) = f(M) \cap f(N)$.

(ii) O funcţie $f : A \to B$ este injectivă dacă şi numai dacă $M = f^{-1}(f(M))$ $\forall M \subseteq A$

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

Propoziţia 2.3. O funcţie $f : A \to B$ este surjectivă dacă şi numai dacă $f(f^{-1}(P)) = P$, $\forall P \subseteq B$.

O funcţie care este injectivă şi surjectivă se numeşte *bijectivă*.

Fiind date funcţiile $f : A \to B$ şi $g : B \to C$, funcţia notată cu $g \circ f$, unde $g \circ f : A \to C$ şi $(g \circ f)(a) = g(f(a))$ oricare ar fi $a \in A$, se numeşte *compunerea* funcţiilor f şi g.

Dacă $f : A \to B$ este o funcţie, atunci sunt evidente egalităţile:

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

O proprietate importantă a compunerii funcţiilor este următoarea:

Teorema 2.4. Compunerea funcţiilor este asociativă, adică fiind date funcţiile $f : A \to B$, $g : B \to C$ şi $h : C \to D$ are loc egalitatea

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

Demonstraţie. Într-adevăr, se vede mai întâi că funcţiile $h \circ (g \circ f)$ şi $(h \circ g) \circ f$ au domeniul de definiţie A, iar codomeniul D. Fie acum $a \in A$. Avem

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

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

de unde rezultă că $h \circ (g \circ f) = (h \circ g) \circ f$.

Propoziţia 2.5. Fie funcţiile $f : A \to B$ şi $g : B \to C$.

a) Dacă f şi g sunt injective, atunci $g \circ f$ este injectivă.

b) Dacă $g \circ f$ este injectivă, atunci f este injectivă.

c) Dacă f şi g sunt surjective, atunci $g \circ f$ este surjectivă.

d) Dacă $g \circ f$ este surjectivă, atunci g este surjectivă.

e) Dacă f şi g sunt bijective, atunci $g \circ f$ este bijectivă.

f) Dacă $g \circ f$ este bijectivă, atunci f este injectivă, iar g este surjectivă.

Demonstraţie. a) Fie $a, a' \in A$ astfel încât $(g \circ f)(a) = (g \circ f)(a')$. Atunci avem că $g(f(a)) = g(f(a'))$ şi cum g este injectivă rezultă $f(a) = f(a')$, de unde obţinem că $a = a'$ deoarece f este injectivă.

b) Fie $a, a' \in A$ astfel încât $f(a) = f(a')$. Atunci avem că $g(f(a)) = g(f(a'))$, adică $(g \circ f)(a) = (g \circ f)(a')$, de unde obţinem că $a = a'$. Deci f este o funcţie injectivă.

c) Fie $c \in C$. Deoarece g este surjectivă există $b \in B$ astfel încât $g(b) = c$. Pe de altă parte există $a \in A$ cu $f(a) = b$, deoarece f este surjectivă. Rezultă că $(g \circ f)(a) = c$, deci $g \circ f$ este surjectivă.

d) Fie acum $c \in C$ şi $a \in A$ cu $(g \circ f)(a) = c$. Fie $b = f(a)$. Atunci $g(b) = c$, ceea ce ne arată că g este surjectivă.

e), f) Rezultă din precedentele.

Exerciţiu. Daţi exemplu de funcţii $f, g : \mathbf{N} \to \mathbf{N}$ cu proprietatea că $g \circ f = 1_{\mathbf{N}}$, dar g nu este injectivă, iar f nu este surjectivă.

O funcţie $f : A \to B$ se numeşte *inversabilă* dacă există o funcţie $g : B \to A$ astfel încât $g \circ f = 1_A$ şi $f \circ g = 1_B$.

Să presupunem acum că funcţia $f : A \to B$ este inversabilă. În acest caz funcţia $g : B \to A$ cu proprietăţile $g \circ f = 1_A$ şi $f \circ g = 1_B$ este unic determinată. Într-adevăr, să presupunem că mai există o funcţie $g' : B \to A$ astfel încât $g' \circ f = 1_A$ şi $f \circ g' = 1_B$. 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 $g = g'$. Funcţia g fiind unică se notează cu f^{-1} şi se numeşte *inversa* funcţiei f.

Teorema 2.6. 1) Dacă funcţia $f : A \to B$ este inversabilă, atunci inversa sa $f^{-1} : B \to A$ este inversabilă şi are loc egalitatea $(f^{-1})^{-1} = f$.

2) Dacă funcţiile $f : A \to B$ şi $g : B \to C$ sunt inversabile, atunci şi funcţia $g \circ f : A \to C$ este inversabilă şi are loc egalitatea

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

Demonstraţie. 1) Cum avem egalităţile $f \circ f^{-1} = 1_B$ şi $f^{-1} \circ f = 1_A$ rezultă că şi f^{-1} este inversabilă şi inversa sa este f, adică $(f^{-1})^{-1} = f$.

2) Avem

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

şi

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

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

Următoarea teoremă caracterizează funcţiile inversabile:

Teorema 2.7. Dacă $f : A \to B$ este o funcţie, atunci f este inversabilă dacă şi numai dacă f este bijectivă.

Demonstraţie. Presupunem că f este inversabilă. Atunci există o funcţie $g : B \to A$

astfel încât $g \circ f = 1_A$ şi $f \circ g = 1_B$. Din Propoziţia 2.5 b) rezultă că f este injectivă iar din Propoziţia 2.5 d) rezultă că f este surjectivă, 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 funcţia $g : B \to A$ astfel: $g(b) = a_b$. Se verifică imediat că $g \circ f = 1_A$ şi $f \circ g = 1_B$.

Un rezultat foarte util în cele ce vor urma este următorul:

Teorema 2.8. Fie A o mulţime finită şi $f : A \to A$ o funcţie. Următoarele afirmaţii sunt echivalente:
1) f este bijectivă;
2) f este injectivă;
3) f este surjectivă.

Demonstraţie. 1) $\Rightarrow$ 2) şi 1) $\Rightarrow$ 3) sunt evidente.

2) $\Rightarrow$ 1) Deoarece A este o mulţime finită, putem scrie că $A = \{a_1, a_2, \dots, a_n\}$. Cum f este injectivă, avem $f(A) = \{f(a_1), f(a_2), \dots, f(a_n)\}$, unde $f(a_i) \neq f(a_j)$, oricare ar fi $i \neq j$. Deci f(A) are n elemente. Din $f(A) \subseteq A$ rezultă că $f(A) = A$ şi deci f este şi surjectivă, adică bijectivă.

3) $\Rightarrow$ 1) Fie $b \in A$ şi notăm cu $f^{-1}(b) = \{a \in A \mid f(a) = b\}$. Evident că $f^{-1}(b)$ este o submulţime a lui A. Cum f este surjectivă, atunci $f^{-1}(b) \neq \emptyset$ oricare ar fi $b \in A$. Deoarece $A = \bigcup_{b \in A} f^{-1}(b)$ şi mulţimile $f^{-1}(b)$ sunt disjuncte două câte 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 decât mulţimea A. Aceasta ne arată că f este neapărat o funcţie injectivă.

§ 3. PRODUSUL CARTEZIAN AL UNEI FAMILII DE MULŢIMI

Fie $I \neq \emptyset$ şi A o mulţime oarecare. O funcţie $\varphi: I \to A$ se mai numeşte *familie de elemente* din A indexată după I. Se notează

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

Dacă $I = \{1, 2, \dots, n\}$, atunci folosim notaţia $(a_i)_{i \in I} = (a_1, a_2, \dots, a_n)$ şi $(a_1, a_2, \dots, a_n)$ se mai numeşte *n-uplu*.

Dacă elementele lui A sunt mulţimi (sau submulţimi ale unei mulţimi T) obţinem noţiunea de *familie de mulţimi* (respectiv *familie de submulţimi* a lui T).

Fie $(A_i)_{i \in I}$ o familie de mulţimi. Atunci mulţimile

$$\bigcup_{i \in I} A_i = \{x \mid \exists\, i \in I, x \in A_i\}, \text{ respectiv } \bigcap_{i \in I} A_i = \{x \mid \forall\, i \in I, x \in A_i\}$$

se numesc *reuniunea*, respectiv *intersecţia* familiei $(A_i)_{i \in I}$.

Avem egalităţile:

$$A \cap (\cup_{i\in I} A_i) = \cup_{i\in I} (A \cap A_i)$$

$$A \cup (\cap_{i\in I} A_i) = \cap_{i\in I} (A \cup A_i)$$

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

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

se numeşte *produsul cartezian* sau *produsul 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 decât mulţimea $A^I = \{\varphi : I \to A\}$, adică mulţimea funcţiilor definite pe I cu valori în A. Dacă $I = \{1, 2, \dots, n\}$, atunci notăm $\prod_{i\in I} A_i$ cu $A_1 \times A_2 \times \dots \times A_n$. 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 $n = 2$ obţinem produsul cartezian a două mulţimi 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 $j \in I$. Funcţia $p_j : \prod_{i\in I} A_i \to A_j$, definită prin egalitatea $p_j(\varphi) = \varphi(j) \in A_j$, unde $\varphi \in \prod_{i\in I} A_i$ (sau $p_j((a_i)_{i\in I}) = a_j$) se numeşte *j-proiecţia canonică* a produsului cartezian pe mulţimea A_j. Aceasta este în mod evident o funcţie surjectivă.

Fie $(A_i)_{i\in I}$, $(B_i)_{i\in I}$ două familii de mulţimi şi $f_i : A_i \to B_i$ o familie de funcţii. Definim o funcţie $\prod_{i\in I} f_i : \prod_{i\in I} A_i \to \prod_{i\in I} B_i$ prin $(\prod_{i\in I} f_i)((a_i)_{i\in I}) = (f_i(a_i))_{i\in I}$. Această funcţie se numeşte *produsul cartezian* al familiei de funcţii $(f_i)_{i\in I}$.

În teoria mulţimilor se admite următoarea axiomă:

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

$$\prod_{i\in I} A_i \neq \varnothing.$$

Echivalentă cu axioma alegerii este următoarea afirmaţie: dacă $\boldsymbol{S}$ este o colecţie nevidă de mulţimi nevide disjuncte două câte două, atunci există o mulţime A, numită *mulţime selectivă*, astfel încât $A \cap X$ este formată dintr-un singur element oricare ar fi $X \in \boldsymbol{S}$.

CURS II

§ 4. RELAŢII DE ECHIVALENŢĂ

Fie A şi B două mulţimi. O submulţime $\rho \subseteq A \times B$ se numeşte *relaţie binară* între A şi B. Dacă $(a, b) \in \rho$, unde $a \in A$ şi $b \in B$, spunem că *a este în relaţia* ρ *cu b* şi notăm $a \rho b$. Când scriem $a \not\rho b$ înseamnă că elementele $a \in A$ şi $b \in B$ nu sunt în relaţia ρ.

Exemple.

1) Dacă $f : A \to B$ este o funcţie, atunci mulţimea $G_f = \{(a, b) \mid a \in A, b \in B \text{ şi } b = f(a)\}$ este o relaţie binară între A şi B. Mulţimea G_f se numeşte *graficul* funcţiei f. Invers, dacă $G \subseteq A \times B$ este o relaţie între A şi B cu proprietatea că oricare ar fi $a \in A$ există un unic $b \in B$ astfel încât $(a, b) \in G$, atunci putem defini funcţia $f : A \to B$ aşa încât $f(a) = b$. Se observă imediat că $G_f = G$.

2) Fie A o mulţime nevidă şi $\rho = \{(a, X) \in A \times \mathcal{P}(A) \mid a \in X\}$. Aceasta este relaţia de apartenenţă între elementele lui A şi submulţimile lui A. Dacă $a \in A$ şi $X \in \mathcal{P}(A)$, atunci $a \rho X$ este echivalent cu $a \in X$.

Când B = A, o relaţie binară ρ între A şi A se numeşte simplu *relaţie binară pe mulţimea A*. O relaţie binară pe o mulţime se notează de regulă cu unul din simbolurile: ρ, $\sim$, $\Re$, $\equiv$, etc.

Exemple.

1) Fie A o mulţime oarecare. Mulţimea $\Delta_A = \{(a, a) \mid a \in A\}$ se numeşte *diagonala* mulţimii A şi este o relaţie binară pe A.

2) Dacă A este o mulţime de numere naturale, atunci mulţimea

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

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

Definiţia 4.1. O relaţie binară pe A, notată „ρ", se numeşte *relaţie de echivalenţă* dacă următoarele condiţii sunt verificate pentru orice $a, b, c \in A$:

i) $a \rho a$ (reflexivitate);

ii) $a \rho b \Rightarrow b \rho a$ (simetrie);

iii) $a \rho b$ şi $b \rho c \Rightarrow a \rho c$ (tranzitivitate).

Exemple.

1) Dacă se consideră mulţimea numerelor întregi **Z** şi $n \geq 1$ un număr natural, atunci relaţia binară notată „$\equiv \pmod n$" (*congruenţa modulo n*):

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

este o relaţie de echivalenţă pe **Z**.

2) Dacă se consideră pe mulţimea **R** a numerelor reale relaţia „~":

$$a \sim b \Leftrightarrow a - b \in \mathbf{Z},$$

aceasta este o relaţie de echivalenţă pe **R**.

Dată o relaţie de echivalenţă „ρ" pe A, pentru orice $a \in A$ definim mulţimea:

$$[a] = \{b \in A \mid b \rho a\}.$$

Aceasta se numeşte *clasa de echivalenţă* a elementului *a*.

Clasa de echivalenţă a elementului *a* se mai notează şi astfel: â, ã, ā, etc.

Teorema 4.2. Fie A o mulţime nevidă şi „ρ" o relaţie de echivalenţă pe A. Atunci clasele de echivalenţă determinate de „ρ" pe A au proprietăţile:

1) $a \in [a]$ oricare ar fi $a \in A$. În particular, $[a] \neq \emptyset$.

2) $[a] = [b] \Leftrightarrow a \rho b$.

3) Dacă [a] şi [b] sunt două clase de echivalenţă, atunci

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

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

Demonstraţie. 1) Deoarece $a \rho a$ rezultă că $[a] \neq \emptyset$.

2) Dacă $[a] = [b]$, cum $a \in A$, atunci $a \in [b]$ şi deci $a \rho b$. Invers, presupunem că $a \rho b$. Fie $x \in [a]$; deci $x \rho a$ şi „ρ" este tranzitivă; obţinem că $x \rho b$, adică $x \in [b]$. Deci $[a] \subseteq [b]$. Similar rezultă $[b] \subseteq [a]$ şi deci avem egalitatea $[a] = [b]$.

3) Presupunem că $[a] \cap [b] \neq \emptyset$. Deci există $x \in [a] \cap [b]$. Atunci $x \rho a$ şi $x \rho b$. Cum „ρ" este simetrică avem $a \rho x$ şi deci $a \rho b$. Din afirmaţia 2) rezultă că $[a] = [b]$.

4) Rezultă din 1).

Definiţia 4.3. Fie A o mulţime nevidă şi „ρ" o relaţie de echivalenţă pe A. O familie de elemente din A, $(a_i)_{i \in I}$, se numeşte *sistem complet şi independent de reprezentanţi* (pe scurt, SCIR) relativ la relaţia de echivalenţă ρ dacă are următoarele proprietăţi:

i) oricare ar fi $i \neq j$, $a_i \rceil \rho a_j$.

ii) oricare ar fi $a \in A$, există $i \in I$ astfel încât $a \rho a_i$.

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

Fiind dată o relaţie de echivalenţă „ρ" pe mulţimea nevidă A, există întotdeauna un sistem de reprezentanţi asociat relaţiei „ρ". Într-adevăr, fie $(C_i)_{i \in I}$ mulţimea tuturor claselor de echivalenţă asociate relaţiei „ρ". 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 reprezentanţi pentru relaţia „ρ". Trebuie să observăm că acest sistem de reprezentanţi nu este unic.

Dacă $(a_i)_{i\in I}$ este un sistem de reprezentanţi relativ la relaţia „ρ", din Teorema 4.2 rezultă că $A = \bigcup_{i\in I} [a_i]$ iar mulţimile $[a_i]$, $i \in I$, sunt disjuncte două câte două.

Exemplu. Pe mulţimea **Z** a numerelor întregi considerăm relaţia „~":

$$a \sim b \Leftrightarrow |a| = |b|.$$

Se observă imediat că „~" este o relaţie de echivalenţă pe **Z**. Dacă $a \in \mathbf{Z}$ avem: $[a] = \{a, -a\}$, dacă $a \neq 0$ şi $[a] = \{0\}$, dacă $a = 0$. Un sistem de reprezentanţi poate fi considerat sistemul de numere: 0, 1, 2, 3, ..., adică mulţimea numerelor naturale **N**. Un alt sistem de reprezentanţi poate fi considerat şi sistemul de numere 0, –1, –2, –3, ..., adică mulţimea numerelor întregi negative.

Definiţia 4.4. Dată relaţia de echivalenţă „ρ" pe A, mulţimea claselor de echivalenţă determinate de „ρ" pe A se notează cu A/ρ şi se numeşte *mulţimea factor* (sau *mulţimea cât*) a lui A prin relaţia „ρ". Funcţia $p : A \to A/\rho$, $p(a) = [a]$, este o funcţie surjectivă şi se numeşte *proiecţia* (*surjecţia*) *canonică* a lui A pe mulţimea factor A/ρ.

Definiţia 4.5. O *partiţie* a unei mulţimi nevide A este o familie de submulţimi nevide disjuncte două câte două ale lui A şi a cărei reuniune este A.

Exemplu. Mulţimile $A_n = \{2n, 2n + 1\}$, $n \in \mathbf{N}$, formează o partiţie a lui **N**.

Mulţimea factor A/ρ este o partiţie a lui A, deci o relaţie de echivalenţă pe A dă naştere unei partiţii. Reciproc, dacă $(A_i)_{i\in I}$ este o partiţie a lui A definim o relaţie de echivalenţă pe A astfel: $a \sim b$ dacă şi numai dacă există $i \in I$ astfel încât $a, b \in A_i$. Clasele de echivalenţă ale lui „~" sunt chiar submulţimile A_i. Aşadar putem enunţa următorul rezultat:

Propoziţia 4.6. Dacă A este o mulţime nevidă, atunci asocierea $\rho \to A/\rho$ defineşte o bijecţie de la mulţimea relaţiilor de echivalenţă pe A la mulţimea partiţiilor lui A.

Demonstraţie. Exerciţiu.

Definiţia 4.7. Fie $f : A \to B$ o funcţie. Definim pe A o relaţie ρ_f astfel:

$$a \,\rho_f\, a' \Leftrightarrow f(a) = f(a').$$

ρ_f se numeşte *relaţia asociată funcţiei f.*

Se observă că ρ_f este o relaţie de echivalenţă pe A, iar mulţimea factor A/ρ_f se descrie astfel:

$$A/\rho_f = \{f^{-1}(b) \mid b \in \operatorname{Im} f\}.$$

Exemplu. Relaţia de echivalenţă pe **R** asociată funcţiei $f : \mathbf{R} \to \mathbf{C}$, $f(x) = \cos(2\pi x) + i\sin(2\pi x)$ este următoarea: $x \,\rho_f\, y$ dacă şi numai dacă $x - y \in \mathbf{Z}$.

Teorema 4.8. (Proprietatea de universalitate a mulţimilor factor) Fie A o mulţime nevidă şi „ρ" o relaţie de echivalenţă pe A. Fie $f : A \to B$ o funcţie şi „ρ_f" relaţia de

echivalenţă pe A asociată funcţiei f. Dacă $\rho \subseteq \rho_f$, atunci există o unică funcţie $\overline{f} : A/\rho \to B$ cu proprietatea că $\overline{f} \circ p = f$. Mai mult:

1) $\overline{f}$ este injectivă $\Leftrightarrow \rho = \rho_f$.

2) $\overline{f}$ este surjectivă $\Leftrightarrow$ f este surjectivă.

Demonstraţie. Definim $\overline{f} : A/\rho \to B$ astfel: $\overline{f}([a]) = f(a)$. Mai întâi vom arăta că funcţia este bine definită, adică [a] = [b] implică f(a) = f(b). Deoarece [a] = [b] rezultă că a ρ b şi cum $\rho \subseteq \rho_f$ obţinem a ρ_f b, deci f(a) = f(b). Este clar acum că $\overline{f} \circ p = f$. Din această relaţie rezultă şi unicitatea funcţiei $\overline{f}$.

1) $\overline{f}$ este injectivă dacă şi numai dacă $\overline{f}([a]) = \overline{f}([b]) \Rightarrow [a] = [b]$. Dar $\overline{f}([a]) = \overline{f}([b]) \Leftrightarrow f(a) = f(b) \Leftrightarrow a\ \rho_f\ b$ şi ca să obţinem [a] = [b] trebuie ca $\rho_f \subseteq \rho$, deci egalitate.

2) Se observă că Im $\overline{f}$ = Im f.

CURS III
LEGI DE COMPOZIŢIE. MONOIZI

§1. OPERAŢIE ALGEBRICĂ INTERNĂ

Definiţia 1.1. Fiind dată o mulţime nevidă M, se numeşte *operaţie algebrică* internă sau *lege de compoziţie* definită pe M orice funcţie

$$\varphi : M \times M \to M,$$

$$(x, y) \to \varphi(x, y).$$

În acest capitol, fiind vorba numai de operaţii algebrice interne, vom spune pe scurt operaţie algebrică în loc de operaţie algebrică internă.

Exemple.

1) Adunarea şi înmulţirea în mulţimea **N** a numerelor naturale, în mulţimea **Z** a numerelor întregi, în mulţimea **Q** a numerelor raţionale, în mulţimea **R** a numerelor reale şi în mulţimea **C** a numerelor complexe sunt operaţii algebrice.

2) În mulţimea **Z** a numerelor întregi, scăderea este o operaţie algebrică. Ea este definită astfel:

$$s : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z},$$

$$s(x, y) = x + (-y) = x - y.$$

De asemenea, scăderea este operaţie algebrică şi pe mulţimile: **Q**, **R, C.** Însă pe mulţimea **N** a numerelor naturale scăderea nu este operaţie algebrică, deoarece rezultatul acesteia nu este întotdeauna un număr natural.

3) Dacă M este o mulţime, pe mulţimea

$$\mathcal{F}(M) = \{f \mid f : M \to M\}$$

a funcţiilor de la M la M putem defini operaţia algebrică de compunere. Reamintim că dacă $f, g \in \mathcal{F}(M)$, atunci se defineşte compunerea $g \circ f$ ca fiind funcţia

$$g \circ f : M \to M, (g \circ f)(x) = g(f(x)).$$

4) Dacă M este o mulţime nevidă, iar

$$\mathcal{P}(M) = \{X \mid X \subseteq M\}$$

este mulţimea părţilor lui M, atunci reuniunea

$$(X, Y) \to X \cup Y, X, Y \in \mathcal{P}(M)$$

şi intersecţia

$$(X, Y) \to X \cap Y, X, Y \in \mathcal{P}(M)$$

sunt operaţii algebrice pe $\mathcal{P}(M)$.

5) Fie $n \geq 1$ un număr natural. Pe mulţimea $\mathbf{Z}_n = \{[0], [1], \ldots, [n-1]\}$ a claselor de resturi modulo n, definim următoarele operaţii algebrice:

$$([a], [b]) \to [a + b] \text{ (numită adunare)},$$

$$([a], [b]) \to [ab] \text{ (numită înmulţire)}.$$

Să arătăm mai întâi că adunarea este o operaţie algebrică pe $\mathbf{Z}_n$, adică nu depinde de alegerea reprezentanţilor. Într-adevăr, fie $[a] = [a_1]$ şi $[b] = [b_1]$; atunci $a \equiv a_1 \pmod n$ şi $b \equiv b_1 \pmod n$, adică $n \mid a - a_1$ şi $n \mid b - b_1$, de unde $n \mid (a + b) - (a_1 + b_1)$, adică $a + b \equiv a_1 + b_1 \pmod n$ şi deci $[a + b] = [a_1 + b_1]$.

La fel se arată că dacă $a \equiv a_1 \pmod n$ şi $b \equiv b_1 \pmod n$, atunci $[ab] = [a_1b_1]$ şi deci operaţia de înmulţire este bine definită.

Deseori, dacă $\varphi : M \times M \to M$ este o operaţie algebrică pe mulţimea M, în loc de $\varphi(x, y)$ se foloseşte ca şi în exemplele de mai înainte, o altă notaţie, ca de exemplu: $x * y$, $x \circ y$, $x \perp y$, $x \, T \, y$, $x + y$, xy, etc.

O mulţime nevidă M înzestrată cu o operaţie algebrică " $*$ " o notăm, uneori, prin perechea $(M, *)$, punând în evidenţă mulţimea şi operaţia algebrică.

Dacă notăm elementul $\varphi(x, y)$ prin $x + y$, pentru orice $x, y \in M$, operaţia algebrică se numeşte *adunare* (fără a fi vorba de adunarea numerelor), iar $x + y$ se numeşte suma lui x cu y; în acest caz se spune că am folosit *scrierea aditivă* a operaţiei algebrice. Dacă notăm elementul $\varphi(x, y)$ prin xy pentru orice $x, y \in M$, operaţia algebrică se numeşte *înmulţire* (de asemenea, fără a avea vreo legătură cu înmulţirea numerelor), iar xy se numeşte produsul lui x cu y; în acest caz, se spune că am folosit *scrierea multiplicativă* a operaţiei algebrice.

Dăm câteva proprietăţi ale operaţiilor algebrice, cu ajutorul cărora se definesc structurile de bază ale algebrei.

Asociativitatea. Fie $M \neq \emptyset$ o mulţime şi $\varphi : M \times M \to M$ o operaţie algebrică pe mulţimea M. Se spune că φ este o operaţie algebrică *asociativă* dacă oricare ar fi $x, y, z \in M$ are loc egalitatea

$$\varphi(x, \varphi(y, z)) = \varphi(\varphi(x, y), z).$$

În scriere aditivă condiţia de asociativitate se scrie

$$x + (y + z) = (x + y) + z, \text{ oricare ar fi } x, y, z \in M,$$

iar în scriere multiplicativă aceasta se scrie

$$x(yz) = (xy)z, \text{ oricare ar fi } x, y, z \in M.$$

Dacă φ nu este asociativă, se spune că φ este o operaţie algebrică *neasociativă*.

Exemple.

1) Operaţiile algebrice de adunare şi înmulţire pe mulţimile de numere **N**, **Z**, **Q**, **R**, **C** sunt asociative.

2) Scăderea numerelor pe **Z** nu este asociativă; de exemplu

$$3 - (2 - 4) \neq (3 - 2) - 4.$$

3) Operaţia algebrică de compunere a funcţiilor pe $\mathcal{F}(M)$ este asociativă.

4) Reuniunea şi intersecţia pe $\mathcal{P}(M)$ sunt operaţii algebrice asociative.

5) Adunarea şi înmulţirea pe $\mathbf{Z}_n$ sunt operaţii algebrice asociative. Într-adevăr, dacă $[a], [b], [c] \in \mathbf{Z}_n$, atunci

$$[a] + ([b] + [c]) = [a] + [b + c] = [a + (b + c)] = [(a + b) + c] = [a + b] + [c] = ([a] + [b]) + [c]$$

şi

$$[a]([b][c]) = [a][bc] = [a(bc)] = [(ab)c] = [ab][c] = ([a][b])[c].$$

Comutativitatea. Fie $M \neq \emptyset$ o mulţime şi $\varphi : M \times M \to M$ o operaţie algebrică pe mulţimea M. Se spune ca φ este e operaţie algebrică *comutativă*, dacă oricare ar fi $x, y \in M$ are loc egalitatea

$$\varphi(x, y) = \varphi(y, x).$$

Dacă folosim scrierea aditivă, respectiv scrierea multiplicativă, condiţia de comutativitate se scrie:

$$x + y = y + x, \text{ oricare ar fi } x, y \in M,$$

respectiv

$$xy = yx, \text{ oricare ar fi } x, y \in M.$$

Dacă φ nu este comutativă, se spune ca φ este o operaţie algebrică *necomutativă*.

Exemple.

1) Operaţiile algebrice de adunare şi înmulţire pe mulţimile de numere **N**, **Z**, **Q**, **R**, **C** sunt comutative.

2) Scăderea numerelor pe **Z** este necomutativă; de exemplu

$$5 - 2 \neq 2 - 5.$$

3) Operaţia algebrică de compunere pe $\mathcal{F}(M)$ nu este comutativă decât dacă M are un singur element.

4) Reuniunea şi intersecţia pe $\mathcal{P}(M)$ sunt operaţii algebrice comutative.

5) Adunarea şi înmulţirea pe $\mathbf{Z}_n$ sunt operaţii algebrice comutative.

Element neutru. Fie $\varphi : M \times M \to M$ o operaţie algebrică definită pe mulţimea $M \neq \emptyset$. Se spune că elementul $e \in M$ este *element neutru* pentru operaţia φ, dacă oricare ar fi $x \in M$ avem

$$\varphi(x, e) = \varphi(e, x) = x.$$

Dacă considerăm o operaţie algebrică oarecare, notată prin $* : M \times M \to M$, $(x, y) \to x * y$, atunci condiţia de mai înainte a elementului neutru se scrie

$$x * e = e * x = x, \text{ oricare ar fi } x \in M.$$

Să presupunem că e şi e' sunt elemente neutre pentru această operaţie algebrică. Atunci avem

$$e = e * e' = e'.$$

Deci elementul neutru, dacă există, este unic determinat.

Dacă folosim scrierea aditivă, elementul neutru se numeşte *elementul nul* sau *elementul zero* sau chiar *zero* şi se notează de obicei cu 0. Cu această notaţie, condiţia elementului zero devine

$$x + 0 = 0 + x = x, \text{ oricare ar fi } x \in M.$$

În scrierea multiplicativă, elementul neutru se numeşte *element unitate* şi se notează de obicei cu e sau chiar cu 1 (a nu se confunda cu numărul 1).

Cu aceste notaţii, condiţia elementului unitate devine

$$x \bullet 1 = 1 \bullet x = x, \text{ oricare ar fi } x \in M.$$

Exemple.

1) Pentru operaţia de adunare în **N**, **Z**, **Q**, **R**, **C**, numărul 0 este element neutru, iar pentru operaţia de înmulţire a numerelor, numărul 1 este element neutru.

2) Pentru operaţia de compunere a funcţiilor definită pe $\mathcal{F}(M)$, funcţia identică 1_M este element neutru.

3) Pentru operaţia de reuniune (respectiv intersecţie) pe mulţimea $\mathcal{P}(M)$ a părţilor unei mulţimi M, mulţimea vidă $\emptyset$ (respectiv mulţimea M) este element neutru.

4) Pentru adunarea pe mulţimea $\mathbf{Z}_n$ elementul neutru este [0], iar pentru înmulţire elementul neutru este [1].

5) Dacă se consideră mulţimea $2\mathbf{Z} = \{2n \mid n \in \mathbf{Z}\}$ a numerelor întregi pare, înmulţirea (obişnuită) a numerelor întregi este o operaţie algebrică internă care, în mod evident, nu are element neutru.

Elemente simetrizabile. Fie $M \neq \emptyset$ o mulţime şi φ o operaţie algebrică pe M care are un element neutru e. Fie $x \in M$. Se spune că x este *simetrizabil* faţă de operaţia dată dacă există un element $x' \in M$ astfel încât

$$\varphi(x, x') = \varphi(x', x) = e.$$

Elementul x' se numeşte element *simetric* al lui x.

Dacă folosim scrierea aditivă, 0 fiind elementul neutru, atunci un element simetric al lui x (dacă există) se numeşte *opus* al lui x, iar condiţia de mai înainte devine

$$x + x' = x' + x = 0.$$

În acest caz se spune că x este *opozabil* faţă de operaţia dată.

Dacă folosim scrierea multiplicativă, 1 fiind elementul neutru, atunci un element simetric al lui x (dacă există) se mai numeşte *invers* al lui x, iar condiţia de mai înainte devine

$$x \bullet x' = x' \bullet x = 1.$$

În acest caz se spune că x este *inversabil* faţă de operaţia dată.

Notăm cu $U((M, *))$ mulţimea elementelor simetrizabile ale lui M în raport cu o lege " $*$ ".

Observaţie. Dacă $M \neq \emptyset$ este o mulţime iar $* : M \times M \to M$, $(x, y) \to x * y$ este o operaţie algebrică pe M care admite element neutru e, atunci e este simetrizabil, simetricul său fiind e. Într-adevăr, avem $e * e = e$.

Propoziţia 1.2. Se consideră $M \neq \emptyset$ o mulţime înzestrată cu o operaţie algebrică asociativă $* : M \times M \to M$, $(x, y) \to x * y$ şi cu element neutru e. Dacă elementul $x \in M$ este simetrizabil, atunci acesta are un unic element simetric.

Demonstraţie. Fie $x \in M$, iar $x', x'' \in M$ simetrice ale lui x, adică $x * x' = x' * x = e$ şi $x * x'' = x'' * x = e$. Atunci $x'' * (x * x') = x'' * e = x''$, iar $(x'' * x) * x' = e * x' = x'$. Operaţia fiind asociativă, avem $x'' * (x * x') = (x'' * x) * x'$ şi deci $x' = x''$.

Observaţie. Faptul că operaţia este asociativă este esenţial pentru unicitatea elementului simetric. Mai precis, dacă operaţia nu este asociativă, nu rezultă unicitatea elementului simetric. Să luăm mulţimea $M = \{e, a, b\}$ şi să definim pe M o operaţie algebrică " $*$ " în modul următor:

$$e * x = x * e = x, \text{ pentru orice } x \in M,$$

$$a * a = a * b = e,\ b * a = e,\ b * b = a.$$

Această operaţie nu este asociativă; de exemplu,

$$(b * b) * a = a * a = e, \text{ iar } b * (b * a) = b * e = b.$$

Elementul *a* are ca simetrice pe *a* şi pe *b*.

În condiţiile de mai înainte, dacă x este un element simetrizabil pentru o operaţie asociativă, simetricul său, unic determinat, se notează cu x^{-1} dacă folosim scrierea multiplicativă şi se numeşte *inversul lui x*, şi se notează –x dacă folosim scrierea aditivă şi se numeşte *opusul lui x*.

Exemple.

1) În mulţimea **N** a numerelor naturale, numai 0 (elementul neutru) are un opus faţă de operaţia de adunare şi numai 1 are invers faţă de operaţia de înmulţire. În mulţimea **Z** a numerelor întregi, faţă de adunare orice element are un opus, iar faţă de înmulţire doar 1 şi –1 au invers. În **Q**, **R** şi **C** faţă de adunare orice element are un opus, iar faţă de înmulţire orice element nenul are un invers.

2) În mulţimea $\mathcal{F}(M)$, cu operaţia algebrică de compunere a funcţiilor, elementele inversabile sunt funcţiile bijective.

3) În mulţimea $\mathcal{P}(M)$, faţă de reuniune numai mulţimea vidă $\emptyset$ are un simetric, iar faţă de intersecţie numai mulţimea M are un simetric.

4) În mulţimea $\mathbf{Z}_n = \{[0], [1], \ldots, [n-1]\}$ cu operaţia algebrică de adunare, oricare ar fi $[a] \in \mathbf{Z}_n$ are un opus şi anume $[-a] \in \mathbf{Z}_n$. Dacă considerăm $\mathbf{Z}_n$ cu operaţia algebrică de înmulţire avem:

Propoziţia 1.3. $[a] \in \mathbf{Z}_n$ este inversabil dacă şi numai dacă *a* este prim cu *n*.

Demonstraţie. Într-adevăr, dacă [a] este inversabil, atunci există $[b] \in \mathbf{Z}_n$ astfel încât [a][b] = [1], echivalent [ab] = [1] şi deci $n \mid ab - 1$. Atunci există $k \in \mathbf{Z}$ astfel încât $ab - 1 = kn$ sau $ab + n(-k) = 1$ şi deci $(a, n) = 1$.

Reciproc, dacă $(a, n) = 1$, atunci există $u, v \in \mathbf{Z}$ astfel încât $au + nv = 1$, de unde $[au + nv] = [1]$ sau $[a][u] + [n][v] = [1]$. Dar $[n] = [0]$ şi deci $[a][u] = [1]$, adică [a] este inversabil în $\mathbf{Z}_n$.

În concluzie, $U(\mathbf{Z}_n) = \{[a] \mid (a, n) = 1\}$.

§ 2. MONOIZI

Definiţia 2.1. O mulţime nevidă M înzestrată cu o operaţie algebrică asociativă şi cu element neutru se numeşte *monoid*. Dacă, în plus, operaţia algebrică este comutativă, monoidul se numeşte *comutativ*.

Exemple.

1) Mulţimea **N** a numerelor naturale faţă de adunarea obişnuită formează un monoid comutativ. De asemenea, mulţimea **N** cu înmulţirea obişnuită este monoid comutativ. Mulţimile **Z**, **Q**, **R**, **C** faţă de adunarea obişnuită, cât şi faţă de înmulţirea obişnuită, formează monoizi comutativi.

2) Mulţimea $\mathcal{F}(M)$ a funcţiilor definite pe mulţimea M cu valori în M, cu operaţia de compunere, formează un monoid, în general, necomutativ.

3) Mulţimea $\mathcal{P}(M)$ a părţilor unei mulţimi M cu operaţia de reuniune (intersecţie) formează monoid comutativ.

4) Mulţimea $\mathbf{Z}_n$ a claselor de resturi modulo n cu operaţia de adunare, ca şi separat, cu cea de înmulţire este monoid comutativ.

Reguli de calcul într-un monoid

Fiind dat un monoid M cu operaţia algebrică notată multiplicativ, se poate defini, prin recurenţă, produsul unui număr finit de elemente $x_1, x_2, \ldots, x_n$ ($n \geq 1$) ale lui M, astfel: dacă notăm cu $x_1 \ldots x_n$ produsul acestor elemente, atunci

$$x_1x_2 \ldots x_n = (x_1x_2 \ldots x_{n-1})x_n.$$

Observaţie. Se poate arăta cu uşurinţă, prin inducţie, că pentru k, $0 < k < n$, are loc relaţia

$$a_1a_2 \ldots a_n = (a_1a_2 \ldots a_k)(a_{k+1}a_{k+2} \ldots a_n). \quad (1)$$

Lăsăm demonstraţia ca exerciţiu.

În cazul particular în care $a_1 = a_2 = \ldots = a_n = a$, în loc de $a_1a_2 \ldots a_n$ se scrie a^n. Avem $a^1 = a$, iar dacă $n = 0$ convenim să punem $a^0 = e$, e fiind elementul unitate al monoidului.

Din relaţia (1) deducem

$$a^m \bullet a^n = a^{m+n}$$

pentru $m, n \in \mathbf{N}$.

Prin inducţie, se demonstrează uşor că

$$(a^m)^n = a^{mn}.$$

Dacă în locul scrierii multiplicative folosim scrierea aditivă, atunci în loc de $a_1a_2 \ldots a_n$, se va scrie $a_1 + a_2 + \ldots + a_n$ iar relaţia (1) devine $a_1 + a_2 + \ldots + a_n = (a_1 + \ldots + a_k) + (a_{k+1} + \ldots + a_n)$. De asemenea, în loc de a^n se scrie na şi deci $1 \bullet a = a$, iar dacă $n = 0$, convenţia devine $0 \bullet a = 0$. Celelalte relaţii devin respectiv

$$ma + na = (m + n)a \text{ şi } n(ma) = (nm)a.$$

Morfisme de monoizi

Definiţia 2.2. Dacă M şi N sunt doi monoizi (notaţi multiplicativ), se numeşte *morfism de monoizi* o funcţie $f : M \to N$ astfel încât

1) $f(xy) = f(x)f(y)$, oricare ar fi $x, y \in M$;

2) $f(e) = e'$, unde e şi e' sunt respectiv, elementele unitate ale lui M şi N.

Exemple.

1) Dacă $(\mathbf{N}, +)$ este monoidul aditiv al numerelor naturale, iar $n \in \mathbf{N}$ este un număr natural oarecare, funcţia

$$\varphi_n : \mathbf{N} \to \mathbf{N}, \ \varphi_n(x) = nx,$$

este un morfism de monoizi.

Lăsăm ca exerciţiu demonstraţia faptului că orice morfism de monoizi de la monoidul $(\mathbf{N}, +)$ în el însuşi este de acest tip. Mai precis, dacă $f : \mathbf{N} \to \mathbf{N}$ este un morfism de monoizi, atunci există $n \in \mathbf{N}$, astfel încât $f = \varphi_n$ (adică $f(x) = nx$, oricare ar fi $x \in \mathbf{N}$).

2) Dacă $(\mathscr{P}(M), \cap)$ şi $(\mathscr{P}(M), \cup)$ sunt monoidul părţilor mulţimii M cu intersecţia şi respectiv cu reuniunea, atunci funcţia

$$g : (\mathscr{P}(M), \cap) \to (\mathscr{P}(M), \cup), \ g(X) = C_M X$$

($C_M X$ este complementara lui X faţă de M) este un morfism de monoizi.

Într-adevăr,

$$g(X \cap Y) = C_M(X \cap Y) = C_M X \cup C_M Y = g(X) \cup g(Y)$$

şi

$$g(M) = C_M M = \varnothing.$$

3) Se consideră monoidul $\mathbf{Z}$ în raport cu înmulţirea şi monoidul $(\mathbf{Z} \times \mathbf{Z}, \bullet)$ cu înmulţirea pe componente, adică $(a, b) \bullet (c, d) = (ac, bd)$. Fie $f : \mathbf{Z} \to \mathbf{Z} \times \mathbf{Z}$, $f(n) = (n, 0)$. Avem că $f(mn) = f(m)f(n)$ pentru orice $m, n \in \mathbf{Z}$, dar $f(1) \neq (1, 1)$. Aşadar f nu este morfism de monoizi.

Observaţie. Se poate demonstra prin inducţie că dacă $x_1, x_2, \ldots, x_n \in M$, atunci pentru orice morfism de monoizi $f : M \to N$ avem

$$f(x_1 x_2 \ldots x_n) = f(x_1)f(x_2) \ldots f(x_n).$$

În particular,

$$f(x^n) = (f(x))^n.$$

Compunerea morfismelor de monoizi

1) Dacă M, N, P sunt monoizi, iar $f : M \to N$, $g : N \to P$ sunt morfisme de monoizi, atunci compunerea $g \circ f : M \to P$ este morfism de monoizi.

Într-adevăr, dacă $x, y \in M$, atunci

$$(g \circ f)(xy) = g(f(xy)) = g(f(x)f(y)) = g(f(x))g(f(y)) = (g \circ f)(x)\,(g \circ f)(y).$$

De asemenea,

$$(g \circ f)(e) = g(f(e)) = g(e') = e''.$$

Compunerea morfismelor de monoizi este asociativă, deoarece este un caz particular de compunere de funcţii.

2) Dacă M este un monoid, funcţia identică 1_M a mulţimii M este un morfism de monoizi.

Într-adevăr, dacă $x, y \in M$, atunci $1_M(xy) = xy = 1_M(x)1_M(y)$, iar $1_M(e) = e$.

Mai mult, dacă $f : M \to N$ este morfism de monoizi, atunci

$$f \circ 1_M = f \text{ şi } 1_N \circ f = f.$$

Izomorfisme de monoizi

Un morfism de monoizi $f : M \to N$ se numeşte *izomorfism* dacă există un morfism de monoizi $g: N \to M$ astfel încât $f \circ g = 1_N$ şi $g \circ f = 1_M$.

Dacă $f : M \to N$ este un izomorfism de monoizi, atunci $g : N \to M$ definit mai înainte, este unic determinat. Într-adevăr, dacă $g' : N \to M$ este un alt morfism astfel încât $f \circ g' = 1_N$ şi $g' \circ f = 1_M$, atunci

$$g' \circ (f \circ g) = g' \circ 1_N = g' \text{ şi } (g' \circ f) \circ g = 1_M \circ g = g.$$

Dar $g' \circ (f \circ g) = (g' \circ f) \circ g$ şi deci $g' = g$.

Din definiţie rezultă că g este şi el un izomorfism de monoizi, numit izomorfismul invers lui f şi se notează cu f^{-1}.

Dacă există un izomorfism de monoizi $f : M \to N$ se spune că monoidul M este *izomorf* cu monoidul N. Dacă monoidul M este izomorf cu monoidul N, se mai spune că M şi N sunt monoizi izomorfi şi se scrie $M \cong N$.

Observaţie. Relaţia de izomorfism între monoizi este o relaţie de echivalenţă:

1) Orice monoid M este izomorf cu el însuşi, deoarece $1_M : M \to M$ este un izomorfism de monoizi;

2) Dacă monoidul M este izomorf cu monoidul N, atunci şi monoidul N este izomorf cu monoidul M (prin izomorfismul invers);

3) Dacă monoidul M este izomorf cu monoidul N, iar monoidul N este izomorf cu monoidul P, atunci M este izomorf cu P (prin compunerea izomorfismelor).

Observaţie. Noţiunea de izomorfism este fundamentală în algebră. Din punct de vedere algebric două structuri algebrice izomorfe sunt la fel, deosebirile dintre ele ţinând doar de natura elementelor şi a operaţiei. Două structuri algebrice izomorfe se pot identifica.

Propoziţia 2.3. Fie $f : M \to N$ un morfism de monoizi. Atunci f este izomorfism de monoizi dacă şi numai dacă funcţia f este bijectivă.

Demonstraţie. Este cunoscut că o funcţie este inversabilă dacă şi numai dacă este bijectivă. De aici rezultă în mod evident că dacă f este izomorfism, atunci funcţia f este bijectivă.

Reciproc, dacă f este bijectivă, atunci există o funcţie $g : N \to M$ astfel încât $f \circ g = 1_N$ şi $g \circ f = 1_M$. Totul rezultă dacă arătăm că g este morfism de monoizi. Fie $y, y' \in N$; atunci

$$yy' = 1_N(yy') = (f \circ g)(yy') = f(g(yy')).$$

Pe de altă parte,

$$yy' = 1_N(y)1_N(y') = (f \circ g)(y)(f \circ g)(y') = f(g(y))f(g(y')) = f(g(y)g(y')).$$

Deci $f(g(yy')) = f(g(y)g(y'))$ şi cum f este injectivă, rezultă

$$g(yy') = g(y)g(y').$$

De asemenea, avem $(g \circ f)(e) = e$, adică $g(f(e)) = e$. Dar $f(e) = e'$ şi deci $g(e') = e$.

Exemplu. Morfismul de monoizi

$$g : (\mathcal{P}(M), \cap) \to (\mathcal{P}(M), \cup),\ g(X) = C_M X$$

este izomorfism.

Produs direct de monoizi

Fie M_1 şi M_2 doi monoizi. Pe produsul cartezian $M = M_1 \times M_2$ al mulţimilor M_1 şi M_2 introducem următoarea operaţie algebrică:

$$(x_1, x_2)(y_1, y_2) = (x_1y_1, x_2y_2).$$

M împreună cu această operaţie devine un monoid. Într-adevăr,

1) operaţia este asociativă, deoarece oricare ar fi $(x_1, x_2), (y_1, y_2), (z_1, z_2) \in M$, avem

$$(x_1, x_2)[(y_1, y_2)(z_1, z_2)] = (x_1, x_2)(y_1z_1,\ y_2z_2) = (x_1(y_1z_1), x_2(y_2z_2)) =$$
$$= ((x_1y_1)z_1, (x_2y_2)z_2) = (x_1y_1, x_2y_2)(z_1, z_2) = [(x_1, x_2)(y_1, y_2)](z_1, z_2).$$

2) elementul neutru este (e_1, e_2), unde e_i este elementul neutru al lui M_i, $i = 1, 2$. Într-adevăr, oricare ar fi $(x, y) \in M$, avem

$$(x, y)(e_1, e_2) = (xe_1, ye_2) = (x, y),$$

şi

$$(e_1, e_2)(x, y) = (e_1x, e_2y) = (x, y).$$

Monoidul M se numeşte *produsul direct* al monoizilor M_1 şi M_2. Mai mult, dacă M_1 şi M_2 sunt monoizi comutativi, atunci, de asemenea, M este monoid comutativ.

Construcţia de mai sus se generalizează imediat la o familie arbitrară de monoizi. Fie $(M_i)_{i \in I}$ o familie nevidă de monoizi. Pe produsul cartezian

$$M = \prod_{i \in I} M_i$$

introducem următoarea operaţie algebrică:

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

În mod similar se verifică că M împreună cu această operaţie este monoid.

Monoidul liber generat de o mulţime

Fie A o mulţime. Vom numi *cuvânt* de elemente din A un sistem finit ordonat de elemente din A, $a_1a_2 \dots a_r$. Vom spune că două cuvinte cu elemente din A, $\alpha = a_1a_2 \dots a_r$, $\beta = b_1b_2 \dots b_s$, sunt egale dacă şi numai dacă $r = s$ şi $a_i = b_i$ pentru $i = 1, 2, \dots, r$. Pe mulţimea L(A) a cuvintelor cu elemente din A introducem următoarea operaţie algebrică (notată multiplicativ): pentru α şi β din L(A) de forma de mai sus definim

$$\alpha\beta = a_1a_2 \dots a_rb_1b_2 \dots b_s.$$

Este clar că această operaţie este asociativă şi are element unitate care este cuvântul „vid" (format din submulţimea vidă a lui A). Aşadar L(A) cu operaţia introdusă este monoid şi se numeşte *monoidul liber* generat de mulţimea A.

Se vede că dacă mulţimea A are cel puţin două elemente distincte a şi b, atunci operaţia algebrică introdusă pe L(A) nu este comutativă, căci $ab \neq ba$, unde ab este compunerea cuvântului a cu cuvântul b, iar ba compunerea cuvântului b cu cuvântul a. Dacă însă mulţimea A este constituită dintr-un singur element, $A = \{a\}$, atunci există un singur cuvânt de lungime $n > 0$, care poate fi notat cu a^n, iar pentru $n \geq 0$, $m \geq 0$, avem că $a^n a^m = a^{n+m}$ şi deci este clar că în acest caz L(A) este monoid comutativ.

În continuare, în afară de cazul în care se menţionează altfel, operaţia algebrică pe un monoid va fi notată multiplicativ. Însă, fără o menţiune expresă, **N** va fi considerat ca monoid cu adunarea.

Propoziţia 2.4. Dacă A este o mulţime formată dintr-un singur element, $A = \{a\}$, atunci monoidul liber L(A) generat de A este izomorf cu monoidul aditiv **N**.

Demonstraţie. Am văzut că, în ipoteza din propoziţie, orice element al lui L(A) este de forma a^n, cu $n \in \mathbf{N}$ şi este clar că funcţia $\varphi : L(A) \to \mathbf{N}$ definită prin $\varphi(a^n) = n$ este un morfism de monoizi fiindcă

$$\varphi(a^n a^m) = \varphi(a^{n+m}) = n + m = \varphi(a^n) + \varphi(a^m).$$

Analog, funcţia $\varphi' : \mathbf{N} \to L(A)$, definită prin $\varphi'(n) = a^n$, este un morfism de monoizi şi avem $\varphi' \circ \varphi = 1_{L(A)}$ şi $\varphi \circ \varphi' = 1_{\mathbf{N}}$.

Din propoziţia de mai sus rezultă ca toţi monoizii liberi generaţi de un element sunt izomorfi, fapt care rezultă de altfel aproape imediat din definiţia monoidului liber generat de o mulţime A, în care se vede că natura elementelor din A nu intervine. Deci la două mulţimi A şi A' echipotente se asociază monoizi liberi izomorfi. Această afirmaţie rezultă şi din următoarea teoremă.

Teorema 2.5. Fie A o mulţime, L(A) monoidul liber generat de A, M un monoid oarecare şi $f : A \to M$ o funcţie. Atunci există un unic morfism de monoizi $\overline{f} : L(A) \to M$ astfel ca $\overline{f} \circ i_A = f$, unde $i_A : A \to L(A)$ este incluziunea canonică a lui A în L(A).

Demonstraţie. Va trebui să definim pe $\overline{f}$ pentru orice cuvânt format cu elemente din A. Acest lucru se face astfel: dacă $\alpha \in L(A)$, $\alpha = a_1a_2 \dots a_r$, $a_k \in A$, $k = 1, 2, \dots, r$ cu

$r \geq 1$, atunci $\overline{f}(\alpha) = f(a_1) \ldots f(a_r)$ (compunerea elementelor $f(a_1)$, ... , $f(a_r)$ în M), iar pentru $r = 0$, adică cuvântului vid, îi asociem elementul unitate din M. Fie $\beta = b_1 \ldots b_s$ un alt element din L(A). Atunci avem prin definiţie:

$$\overline{f}(\alpha\beta) = f(a_1) \ldots f(a_r)f(b_1) \ldots f(b_s)$$

şi

$$\overline{f}(\alpha)\ \overline{f}(\beta) = (f(a_1) \ldots f(a_r))\ (f(b_1) \ldots f(b_s)).$$

Deoarece în M operaţia este asociativă avem că $\overline{f}(\alpha\beta) = \overline{f}(\alpha)\ \overline{f}(\beta)$, deci $\overline{f}$ este morfism de monoizi. Am construit astfel un morfism $\overline{f}$ cu proprietatea cerută.

Să arătăm acum că $\overline{f}$ este unicul morfism de monoizi cu această proprietate. Fie atunci $\overline{f}' : L(A) \to M$ un alt morfism astfel ca $\overline{f}' \circ i_A = f$. Fie $\alpha \in L(A)$ scris sub forma de mai sus. Atunci $\overline{f}'(\alpha) = \overline{f}'(a_1 \ldots a_r) = \overline{f}'(a_1) \ldots \overline{f}'(a_r) = f(a_1) \ldots f(a_r)$, adică $\overline{f}'(\alpha) = \overline{f}(\alpha)$, pentru orice $\alpha \in L(A)$ şi deci $\overline{f}' = \overline{f}$.

Proprietatea monoidului liber generat de o mulţime A demonstrată în teorema precedentă poartă numele de *proprietatea de universalitate a monoidului liber* generat de A.

Corolarul 2.6. Fie A şi A' două mulţimi astfel încât există $f : A \to A'$ o funcţie bijectivă. Atunci există un unic izomorfism de monoizi $\overline{f} : L(A) \to L(A')$ astfel ca $\overline{f} \circ i_A = i_{A'} \circ f$, unde $i_A : A \to L(A)$ este incluziunea canonică a lui A în L(A) iar $i_{A'} : A' \to L(A')$ este incluziunea canonică a lui A' în L(A').

CURS IV
ELEMENTE DE TEORIA GRUPURILOR

§ 1. GRUPURI ŞI MORFISME DE GRUPURI

Grupuri

Definiţia 1.1. Se numeşte *grup* o mulţime nevidă G înzestrată cu o operaţie algebrică care satisface următoarele condiţii:

1) este asociativă;
2) are element neutru;
3) orice element din G este simetrizabil.

Se mai spune că, în acest caz, pe G s-a dat o structură de grup.

Dacă, în plus, operaţia este comutativă, se spune că grupul G este *comutativ* sau *abelian*.

De regulă, pentru operaţia algebrică dintr-un grup vom folosi scrierea multiplicativă; dacă grupul G este comutativ, vom folosi de obicei scrierea aditivă. Vom folosi, eventual, şi alte notaţii pentru operaţia algebrică a unui grup, de exemplu, dacă sunt definite mai multe operaţii pe aceeaşi mulţime; oricum, nu vom folosi scrierea aditivă în cazul unui grup necomutativ (neabelian).

Exemple.

1) Mulţimile **Z**, **Q**, **R**, **C** sunt grupuri comutative în raport cu operaţia de adunare corespunzătoare fiecăreia dintre acestea.

2) Mulţimile $\mathbf{Q}^*$, $\mathbf{R}^*$, $\mathbf{C}^*$ ale numerelor raţionale nenule, reale nenule, respectiv complexe nenule, în raport cu operaţia de înmulţire, sunt grupuri comutative. Mulţimile $\mathbf{Q}^*_+$ şi $\mathbf{R}^*_+$ ale numerelor raţionale strict pozitive şi numerelor reale strict pozitive, formează grupuri comutative faţă de înmulţire.

3) Mulţimea $\mathbf{Z}_n$ a claselor de resturi modulo n, cu operaţia de adunare, este grup comutativ.

4) Fie M un monoid cu operaţia algebrică notată multiplicativ şi notăm

$$U(M) = \{x \in M \mid x \text{ inversabil}\}.$$

Observăm că elementul neutru *e* aparţine lui U(M) şi deci $U(M) \neq \emptyset$. Mai mult, dacă $x, y \in U(M)$, atunci există $x^{-1}, y^{-1} \in M$ astfel încât $x x^{-1} = x^{-1}x = e$ şi $y y^{-1} = y^{-1} y = e$. Deci şi $x^{-1}, y^{-1} \in U(M)$ şi $(xy)(y^{-1}x^{-1}) = (y^{-1}x^{-1})(xy) = e$, adică $xy \in U(M)$. Am demonstrat astfel că operaţia algebrică de pe M induce o operaţie algebrică pe U(M) şi, mai mult, U(M) împreună cu această operaţie este grup. Grupul $(U(M), \bullet)$ astfel obţinut se numeşte *grupul elementelor inversabile* sau *grupul unităţilor* monoidului $(M, \bullet)$.

Grupul $(U(\mathbf{Z}), \bullet)$ al elementelor inversabile ale monoidului multiplicativ $(\mathbf{Z}, \bullet)$ al numerelor întregi este $(\{-1, 1\}, \bullet)$. Grupul $(U(\mathbf{Z}_n), \bullet)$ al claselor de resturi inversabile ale monoidului $(\mathbf{Z}_n, \bullet)$ este $U(\mathbf{Z}_n) = \{[a] \in \mathbf{Z}_n \mid (a, n) = 1\}$, după cum rezultă din Propoziţia 1.3, Cursul 3. Să notăm că $U((\mathbf{Q}, \bullet)) = (\mathbf{Q}^*, \bullet)$, $U((\mathbf{R}, \bullet)) = (\mathbf{R}^*, \bullet)$ şi $U((\mathbf{C}, \bullet)) = (\mathbf{C}^*, \bullet)$.

5) Fie M o mulţime şi $S(M) = \{f : M \to M \mid f \text{ bijectivă}\}$, mulţimea funcţiilor bijective de la M la M. Deoarece compunerea a două funcţii bijective este o funcţie bijectivă, iar o funcţie este bijectivă dacă şi numai dacă este inversabilă, rezultă că pe S(M) compunerea funcţiilor este o operaţie algebrică împreună cu care S(M) este un grup, în general necomutativ. Acesta se numeşte *grupul permutărilor* (sau *grupul simetric* al) mulţimii M. Lăsăm ca exerciţiu să se arate că S(M) este comutativ dacă şi numai dacă M are cel mult două elemente.

Să notăm că grupul $(U(\mathcal{F}(M)), o)$ al elementelor inversabile ale monoidului $(\mathcal{F}(M), o)$ al funcţiilor de la M la M este grupul permutărilor S(M).

6) Un număr complex z se numeşte *rădăcină a unităţii* dacă există un număr natural $n \geq 1$ astfel încât $z^n = 1$. Faţă de înmulţirea obişnuită a numerelor complexe, mulţimea U_∞ a rădăcinilor unităţii formează un grup abelian. Dacă $n \geq 1$ este fixat, mulţimea $U_n = \{z \in \mathbf{C}^* \mid z^n = 1\}$ a *rădăcinilor de ordin n ale unităţii* formează, în raport cu operaţia de înmulţire a numerelor complexe, un grup abelian.

Exerciţii.

1) Fie M_1 şi M_2 doi monoizi. Arătaţi că $U(M_1 \times M_2) = U(M_1) \times U(M_2)$.
2) Fie M o mulţime nevidă. Mulţimea $\mathcal{P}(M)$ formează grup abelian în raport cu diferenţa simetrică: $X \Delta Y = (X \setminus Y) \cup (Y \setminus X)$.

Reguli de calcul într-un grup

După cum rezultă din definiţie, orice grup este monoid, deci regulile de calcul date pentru monoizi sunt valabile şi pentru grupuri. Astfel, dacă *a* este element al unui grup G, putem vorbi de a^n sau *na* ($n \geq 0$), după cum folosim scrierea multiplicativă sau aditivă. Mai mult, într-un grup, oricare ar fi x din G există simetricul său în G, care este unic determinat. Simetricul lui x se notează cu x^{-1} şi se citeşte *inversul* lui x sau cu –x şi se citeşte *opusul* lui x, după cum folosim scrierea multiplicativă sau aditivă.

Avem următorul rezultat: dacă $x_1, x_2, \ldots, x_n$ ($n \geq 1$) sunt elemente ale unui grup G, atunci

$$(x_1x_2 \ldots x_n)^{-1} = x_n^{-1} \ldots x_2^{-1}x_1^{-1}.$$

Într-adevăr, ţinând seama de asociativitate

$$(x_1x_2 \ldots x_n)(x_n^{-1} \ldots x_2^{-1}x_1^{-1}) = (x_n^{-1} \ldots x_2^{-1}x_1^{-1})(x_1x_2 \ldots x_n) = e,$$

ceea ce demonstrează relaţia de mai înainte.
În particular,

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

iar dacă $x_1 = \ldots = x_n = x$, atunci pentru $n \geq 0$,

(1) $$(x^n)^{-1} = (x^{-1})^n.$$

Puterea unui element într-un grup. În cazul unui grup putem defini puterea x^n pentru orice $n \in \mathbf{Z}$. Dacă $n < 0$, atunci $-n > 0$ şi definim $x^n = (x^{-1})^{-n} = (x^{-n})^{-1}$.

Relaţia (1) se extinde şi pentru $n < 0$. Într-adevăr,

$$(x^n)^{-1} = ((x^{-n})^{-1})^{-1} = ((x^{-1})^{-1})^{-n} = x^{-n} = (x^{-1})^n.$$

De asemenea, pentru grupuri, avem

$$x^m x^n = x^{m+n},$$

oricare ar fi m, n $\in$ **Z**.

Într-un grup G au loc următoarele reguli de simplificare:

1) Dacă x, y, z $\in$ G şi xy = xz, atunci y = z.

2) Dacă x, y, z $\in$ G şi xz = yz, atunci x = y.

Într-adevăr, din xy = xz, prin înmulţire la stânga cu x^{-1}, rezultă $x^{-1}(xy) = x^{-1}(xz)$ sau $(x^{-1}x)y = (x^{-1}x)z$, de unde ey = ez, adică y = z.

Analog se demonstrează a doua lege de simplificare.

Lăsăm ca exerciţiu să se arate că dacă a, b $\in$ G, atunci fiecare dintre ecuaţiile ax = b şi ya = b are soluţie unică în G.

Morfisme de grupuri

Definiţia 1.2. Fie G şi G' două grupuri. Se numeşte *morfism* de grupuri de la G la G' o funcţie f : G $\to$ G' astfel încât

$$f(xy) = f(x)f(y), \text{ oricare ar fi } x, y \in G.$$

Ca şi la monoizi, au loc următoarele afirmaţii:

1) Dacă G, G', G" sunt grupuri, iar f : G $\to$ G', g : G' $\to$ G" sunt morfisme de grupuri, atunci compunerea g o f : G $\to$ G" este un morfism de grupuri.

2) Dacă G este un grup, funcţia identică 1_G a mulţimii G este morfism de grupuri. Mai mult, dacă f : G $\to$ G' este un morfism de grupuri, atunci f o 1_G = f şi $l_{G'}$ o f = f.

Propoziţia 1.3. Dacă G şi G' sunt două grupuri, e şi e' elementele neutre ale lui G, respectiv G' şi f : G $\to$ G' un morfism de grupuri, atunci:

1) f(e) = e';

2) $f(x^{-1}) = (f(x))^{-1}$ pentru orice x $\in$G.

Demonstraţie. 1) Avem

$$f(e) = f(ee) = f(e)f(e),$$

sau

$$f(e)e' = f(e)f(e).$$

Simplificând ambii membri prin f(e) (adică înmulţind la stânga cu $f(e)^{-1}$), obţinem

$$e' = f(e).$$

2) Având în vedere unicitatea elementului invers, este suficient să demonstrăm că

$$f(x^{-1})f(x) = e' \text{ şi } f(x)f(x^{-1}) = e'.$$

Avem $f(x^{-1})f(x) = f(x^{-1}x) = f(e) = e'$ şi analog a doua relaţie.

Un morfism de grupuri f : G $\to$ G' astfel încât funcţia f să fie injectivă (respectiv, surjectivă) se numeşte *morfism injectiv* (respectiv, *surjectiv*) de grupuri.

Un morfism de grupuri f : G $\to$ G' se numeşte *izomorfism* de grupuri dacă există un morfism de grupuri g : G' $\to$ G astfel încât

$$f \text{ o } g = 1_{G'} \text{ şi } g \text{ o } f = 1_G.$$

Două grupuri G şi G' între care există un izomorfism se numesc *izomorfe*; scriem atunci $G \cong G'$.

Un morfism de grupuri definit pe grupul G şi cu valori tot în G se numeşte *endomorfism* al lui G. Mulţimea endomorfismelor lui G se notează cu End(G).

Un endomorfism al lui G care este şi izomorfism se numeşte *automorfism* al lui G. Mulţimea automorfismelor lui G se notează cu Aut(G).

Evident, $Aut(G) \subseteq End(G)$. Mai mult, End(G) este monoid în raport cu operaţia de compunere a funcţiilor, iar Aut(G) este grup în raport cu operaţia de compunere a funcţiilor, fiind de fapt grupul unităţilor monoidului (End(G), o).

Exemple.

1) Dacă G şi G' sunt două grupuri arbitrare, atunci funcţia $\theta : G \to G'$, $\theta(x) = e'$ (e' este elementul neutru al lui G') este evident un morfism de grupuri, numit *morfismul nul*.

2) Funcţia $f : \mathbf{Z} \to \{-1, 1\}$, definită prin

$$f(x) = \begin{cases} 1, \text{ dacă x este par} \\ -1, \text{ dacă x este impar,} \end{cases}$$

este un morfism de la grupul aditiv al numerelor întregi la grupul multiplicativ $\{-1, 1\}$. Verificarea acestui fapt este imediată.

3) Fie $n \in \mathbf{Z}$ şi funcţia $\varphi_n : \mathbf{Z} \to \mathbf{Z}$ definită prin $\varphi_n(x) = nx$. Este clar că φ_n este un endomorfism al grupului aditiv al numerelor întregi. Mai mult, orice endomorfism al grupului $(\mathbf{Z}, +)$ este de acest tip, adică dacă $f : \mathbf{Z} \to \mathbf{Z}$ este un endomorfism, atunci există $n \in \mathbf{Z}$ astfel încât $f = \varphi_n$ (adică $f(x) = nx$, oricare ar fi $x \in \mathbf{Z}$).

4) Să considerăm grupul aditiv $(\mathbf{R}, +)$ al numerelor reale şi fie $(\mathbf{R}^*_+, \bullet)$ grupul multiplicativ al numerelor reale strict pozitive. Funcţia $f : \mathbf{R} \to \mathbf{R}^*_+$ dată prin $f(x) = e^x$, unde *e* este baza logaritmilor naturali, este un morfism de grupuri. Mai mult, este chiar un izomorfism, deoarece dacă considerăm $g : \mathbf{R}^*_+ \to \mathbf{R}$, $g(y) = \ln y$, avem

$$f \circ g = 1_{\mathbf{R}^*_+} \text{ şi } g \circ f = 1_{\mathbf{R}}.$$

5) Fie G un grup şi $a \in G$ un element al său. Aplicaţia $\varphi_a : G \to G$ dată prin $\varphi_a(x) = axa^{-1}$ este un automorfism al lui G. Într-adevăr,

$$\varphi_a(xy) = a(xy)a^{-1} = (axa^{-1})(aya^{-1}) = \varphi_a(x)\varphi_a(y).$$

Mai mult, este imediat că

$$\varphi_{a^{-1}} \circ \varphi_a = \varphi_a \circ \varphi_{a^{-1}} = 1_G.$$

φ_a se numeşte *automorfism interior* al lui G, iar mulţimea $Int(G) = \{\varphi_a \mid a \in G\}$ se numeşte mulţimea automorfismelor interioare ale lui G.

6) Fie M o mulţime, $N \subset M$ o submulţime proprie, iar S(M) şi S(N) grupurile permutărilor mulţimii M, respectiv N. Pentru $f \in S(N)$, definim $\mathbf{f} : M \to M$ prin

$$\mathbf{f}(x) = \begin{cases} f(x), x \in N \\ x, x \in M \setminus N \end{cases}$$

Se verifică uşor că $\mathbf{f} \in S(M)$, iar funcţia $\psi : S(N) \to S(M)$, dată prin $\psi(f) = \mathbf{f}$, este un morfism injectiv de grupuri.

Propoziţia 1.4. Fie $f : G \to G'$ un morfism de grupuri. Atunci f este izomorfism de grupuri dacă şi numai dacă funcţia f este bijectivă.

Demonstraţie. A se vedea propoziţia analoagă de la morfisme de monoizi.

Teorema 1.5. (Teorema lui Cayley) Fie G un grup. Atunci există un morfism injectiv de grupuri de la G în S(G).

Demonstraţie. Definim $f : G \to S(G)$ astfel: $f(x) = t_x$, unde $t_x : G \to G$ este dată prin $t_x(g) = xg$. Se verifică uşor că t_x este bijecţie, deci $t_x \in S(G)$.
- f injectivă: $f(x) = f(y)$ implică $t_x = t_y$ şi de aici rezultă că $t_x(e) = t_y(e)$, adică $xe = ye$, deci $x = y$.
- f morfism de grupuri: avem că $t_{xy}(g) = (xy)g = x(yg) = t_x(t_y(g)) = (t_x \circ t_y)(g)$ pentru orice $g \in G$, deci $t_{xy} = t_x \circ t_y$ ceea ce ne arată că $f(xy) = f(x) \circ f(y)$.

Exerciţii.

1) Dacă M, N sunt monoizi şi $M \cong N$ (izomorfism de monoizi), atunci $U(M) \cong U(N)$ (izomorfism de grupuri).

2) Să se arate că orice endomorfism al grupului aditiv $(\mathbf{Z}, +)$ este de forma φ_n (adică oricare ar fi morfismul $f : (\mathbf{Z}, +) \to (\mathbf{Z}, +)$ există $n \in \mathbf{Z}$ astfel încât $f = \varphi_n$). În particular, obţinem că $(End(\mathbf{Z}), \circ) \cong (\mathbf{Z}, \bullet)$, izomorfism de monoizi. (De aici rezultă că $(Aut(\mathbf{Z}), \circ) \cong (\{-1, 1\}, \bullet)$, izomorfism de grupuri.)

3) Să se arate că $(End(\mathbf{Z}_n), \circ) \cong (\mathbf{Z}_n, \bullet)$, izomorfism de monoizi. (De aici rezultă că $(Aut(\mathbf{Z}_n), \circ) \cong (U(\mathbf{Z}_n), \bullet)$, izomorfism de grupuri.)

Produs direct de grupuri

Fie G_1 şi G_2 două grupuri. Pe produsul cartezian $G = G_1 \times G_2$ al mulţimilor G_1 şi G_2 introducem următoarea operaţie algebrică:

$$(x_1, x_2)(y_1, y_2) = (x_1y_1, x_2y_2).$$

G împreună cu această operaţie devine un grup. Într-adevăr,

1) operaţia este asociativă, deoarece oricare ar fi $(x_1, x_2), (y_1, y_2), (z_1, z_2) \in G$, avem

$$(x_1, x_2)[(y_1, y_2)(z_1, z_2)] = (x_1, x_2)(y_1z_1, y_2z_2) = (x_1(y_1z_1), x_2(y_2z_2)) =$$
$$= ((x_1y_1)z_1, (x_2y_2)z_2) = (x_1y_1, x_2y_2)(z_1, z_2) = [(x_1, x_2)(y_1, y_2)](z_1, z_2).$$

2) elementul neutru este (e_1, e_2), unde e_i este elementul neutru al lui G_i, $i = 1, 2$. Într-adevăr, oricare ar fi $(x_1, x_2) \in G$, avem

$$(x_1, x_2)(e_1, e_2) = (x_1e_1, x_2e_2) = (x_1, x_2),$$

şi

$$(e_1, e_2)(x_1, x_2) = (e_1x_1, e_2x_2) = (x_1, x_2).$$

3) inversul unui element oarecare $(x_1, x_2) \in G$ este $(x_1^{-1}, x_2^{-1}) \in G$, deoarece

$$(x_1, x_2)(x_1^{-1}, x_2^{-1}) = (x_1x_1^{-1}, x_2x_2^{-1}) = (e_1, e_2)$$

şi

$$(x_1^{-1}, x_2^{-1})(x_1, x_2) = (x_1^{-1}x_1, x_2^{-1}x_2) = (e_1, e_2).$$

Grupul G se numeşte *produsul direct* al grupurilor G_1 şi G_2 şi se notează $G = G_1 \times G_2$. Mai mult, dacă G_1 şi G_2 sunt grupuri comutative, atunci, de asemenea, G este grup comutativ.

Exemplu. Produsul direct de grupuri $(\mathbf{Z}_2, +) \times (\mathbf{Z}_2, +)$ este izomorf cu grupul lui Klein.

Putem defini de la G_1, respectiv G_2 la $G_1 \times G_2$ funcţiile $s_1 : G_1 \to G_1 \times G_2$, respectiv $s_2 : G_2 \to G_1 \times G_2$ astfel: $s_1(x_1) = (x_1, e_2)$, respectiv $s_2(x_2) = (e_1, x_2)$. Acestea sunt morfisme injective de grupuri şi se numesc *injecţiile canonice*.

De asemenea, reamintim că putem defini de la $G_1 \times G_2$ la G_1, respectiv G_2 funcţiile $p_1 : G_1 \times G_2 \to G_1$, respectiv $p_2 : G_1 \times G_2 \to G_2$ astfel: $p_1(x_1, x_2) = x_1$, respectiv $p_2(x_1, x_2) = x_2$. Acestea sunt morfisme surjective de grupuri şi se numesc *surjecţiile canonice*.

Observăm că $p_i \circ s_i = 1_{G_i}$, pentru i = 1, 2.

Fie G_1, G_2, H_1, H_2 grupuri şi $f_i : G_i \to H_i$, i = 1, 2 morfisme de grupuri. Atunci produsul cartezian al morfismelor de grupuri $f_1 \times f_2 : G_1 \times G_2 \to H_1 \times H_2$ este morfism de grupuri.

Construcţia de mai sus se generalizează imediat la o familie arbitrară de grupuri. Fie $(G_i)_{i \in I}$ o familie nevidă de grupuri. Pe produsul cartezian

$$G = \prod_{i \in I} G_i$$

introducem următoarea operaţie algebrică:

$$(x_i)_{i \in I} (y_i)_{i \in I} = (x_iy_i)_{i \in I}.$$

În mod similar se verifică că G împreună cu această operaţie este grup.

Fie $(G_i)_{i \in I}$ o familie nevidă de grupuri şi $j \in I$. Atunci j-proiecţia canonică $p_j : \prod_{i \in I} G_i \to G_j$ este morfism surjectiv de grupuri. Putem defini şi un morfism injectiv de grupuri, numit *j-injecţia canonică*, $s_j : G_j \to \prod_{i \in I} G_i$ astfel: $s_j(a_j) = (a_i)_{i \in I}$, unde $a_i = e_i$, elementul neutru al lui G_i, pentru orice $i \neq j$. Observăm că $p_j \circ s_j = 1_{G_j}$.

Fie $(G_i)_{i \in I}$, $(H_i)_{i \in I}$ două familii de grupuri şi $f_i : G_i \to H_i$ o familie de morfisme de grupuri. Atunci produsul cartezian al familiei de morfisme de grupuri $(f_i)_{i \in I}$, $\prod_{i \in I} f_i : \prod_{i \in I} G_i \to \prod_{i \in I} H_i$ este morfism de grupuri.

Aplicaţii.

1) Considerăm grupurile aditive $(\mathbf{Z}_m, +)$ şi $(\mathbf{Z}_n, +)$ ale claselor de resturi modulo m, respectiv modulo n. Arătăm că dacă m şi n sunt prime între ele, atunci grupul produs direct $(\mathbf{Z}_m \times \mathbf{Z}_n, +)$ este izomorf cu grupul aditiv $(\mathbf{Z}_{mn}, +)$ al claselor de resturi modulo mn.

Definim $\theta : \mathbf{Z}_{mn} \to \mathbf{Z}_m \times \mathbf{Z}_n$ prin $\theta(\bar{x}) = ([x], \{x\})$. Funcţia θ este bine definită,

căci dacă $\bar{x} = \bar{y}$, adică $x \equiv y \pmod{mn}$, atunci $mn \mid x - y$, deci $m \mid x - y$ şi $n \mid x - y$, adică $x \equiv y \pmod{m}$ şi $x \equiv y \pmod{n}$, adică $[x] = [y]$ şi $\{x\} = \{y\}$ şi deci $([x], \{x\}) = ([y], \{y\})$, adică $\theta(\bar{x}) = \theta(\bar{y})$.

Avem că θ este morfism de grupuri, deoarece

$$\theta(\bar{x} + \bar{y}) = \theta(\overline{x + y}) = ([x + y], \{x + y\}) =$$

$$= ([x] + [y], \{x\} + \{y\}) = ([x], \{x\}) + ([y], \{y\}) = \theta(\bar{x}) + \theta(\bar{y}).$$

Mai mult, θ este morfism injectiv: dacă $\theta(\bar{x}) = \theta(\bar{y})$, atunci $([x], \{x\}) = ([y], \{y\})$, adică $[x] = [y]$ şi $\{x\} = \{y\}$, deci $m \mid x - y$ şi $n \mid x - y$ şi cum $(m, n) = 1$ rezultă că $mn \mid x - y$, adică $\bar{x} = \bar{y}$.

Cum θ este injectivă iar $\mathbf{Z}_{mn}$ şi $\mathbf{Z}_m \times \mathbf{Z}_n$ au acelaşi număr de elemente, rezultă că θ este şi surjectivă, deci bijectivă. Aşadar, θ este un izomorfism de grupuri.

Se poate demonstra şi reciproc, şi anume că dacă grupurile $\mathbf{Z}_{mn}$ şi $\mathbf{Z}_m \times \mathbf{Z}_n$ sunt izomorfe, atunci m şi n sunt prime între ele.

2) Considerăm acum monoizii multiplicativi $(\mathbf{Z}_m, \bullet)$ şi $(\mathbf{Z}_n, \bullet)$. Să arătăm că dacă m şi n sunt prime între ele, atunci monoidul produs direct $(\mathbf{Z}_m \times \mathbf{Z}_n, \bullet)$ este izomorf cu monoidul multiplicativ $(\mathbf{Z}_{mn}, \bullet)$ al claselor de resturi modulo mn.

Avem funcţia

$$\theta : \mathbf{Z}_{mn} \to \mathbf{Z}_m \times \mathbf{Z}_n, \ \theta(\bar{x}) = ([x], \{x\})$$

de la aplicaţia 1) şi ştim că aceasta este bine definită. Mai mult, θ este un morfism de monoizi. Într-adevăr,

$$\theta(\bar{x}\,\bar{y}) = \theta(\overline{x\,y}) = ([x\,y], \{x\,y\}) = ([x], \{x\})([y], \{y\}) = \theta(\bar{x})\,\theta(\bar{y})$$

şi

$$\theta(\bar{1}) = ([1], \{1\}).$$

La aplicaţia 1) am demonstrat că dacă $(m, n) = 1$, atunci θ este bijectivă, deci în acest caz θ este izomorfism de monoizi.

Dacă $U(\mathbf{Z}_{mn})$, $U(\mathbf{Z}_m)$ şi $U(\mathbf{Z}_n)$ sunt, respectiv, grupurile multiplicative ale elementelor inversabile din $\mathbf{Z}_{mn}$, $\mathbf{Z}_m$ şi $\mathbf{Z}_n$, iar m şi n sunt prime între ele, atunci avem

$$\bar{x} \in U(\mathbf{Z}_{mn}) \text{ dacă şi numai dacă } [x] \in U(\mathbf{Z}_m) \text{ şi } \{x\} \in U(\mathbf{Z}_n).$$

Într-adevăr, aceasta rezultă din faptul că dacă $(m, n) = 1$, atunci are loc afirmaţia:

$$(x, mn) = 1 \text{ dacă şi numai dacă } (x, m) = 1 \text{ şi } (x, n) = 1.$$

Prin urmare, dacă $(m, n) = 1$, atunci θ ne dă un izomorfism de grupuri multiplicative:

$\bar{\theta} : U(\mathbf{Z}_{mn}) \to U(\mathbf{Z}_m) \times U(\mathbf{Z}_n)$, unde $\bar{\theta}(\bar{x}) = ([x], \{x\})$.

Definiţia 1.5. Pentru $n \in \mathbf{N}$, $n \geq 2$, definim $\varphi(n) = |U(\mathbf{Z}_n)|$. Funcţia φ se numeşte *indicatorul lui Euler*.

Din cele de mai sus rezultă că $\varphi(mn) = \varphi(m)\varphi(n)$ pentru $(m, n) = 1$. Pe de altă parte, dacă p este un număr prim şi $k \geq 1$ avem $\varphi(p^k) = p^k - p^{k-1}$. Aşadar, cunoscând descompunerea lui n în factori primi putem afla imediat $\varphi(n)$. De exemplu, $\varphi(12) = \varphi(2^2 \cdot 3) = \varphi(2^2)\varphi(3) = (2^2 - 2)(3 - 1) = 4$.

Exerciţiu. Arătaţi că grupul $U(\mathbf{Z}_{12})$ este izomorf cu grupul lui Klein.

CURS V
ELEMENTE DE TEORIA GRUPURILOR

§ 2. SUBGRUPURI

Subgrupuri

Fie G un grup în notaţie multiplicativă ($G \times G \to G$, $(x, y) \to xy$) şi H o submulţime nevidă a sa. Dacă oricare ar fi $x, y \in H$, avem $xy \in H$ (produsul efectuat conform operaţiei algebrice din G), atunci se obţine o funcţie $H \times H \to H$, $(x, y) \to xy$, adică o operaţie algebrică pe H numită *operaţia indusă* pe H de operaţia din G. În acest caz se mai spune că operaţia din G induce o operaţie pe H.

Definiţia 2.1. Se spune că o submulţime nevidă H a grupului G este *subgrup* al lui G, dacă operaţia algebrică din G induce pe H o operaţie algebrică faţă de care H este grup.

Notaţie. $H \leq G$

Propoziţia 2.2. Fie G un grup şi H o submulţime nevidă a sa. Atunci următoarele afirmaţii sunt echivalente:

1) H este subgrup al lui G;

2) i) Oricare ar fi $x, y \in H$, produsul xy (efectuat în G) este un element din H;

ii) $e \in H$ (e fiind elementul neutru al lui G);

iii) Oricare ar fi $x \in H$, x^{-1} (inversul lui x în G) aparţine lui H;

3) Oricare ar fi $x, y \in H$, produsul xy^{-1} (efectuat în G) aparţine lui H.

Demonstraţie. 1) $\Rightarrow$ 2) Afirmaţia i) rezultă din faptul că operaţia din G induce pe H o operaţie algebrică. H fiind subgrup are un element neutru notat e'. Cum e este elementul neutru al lui G, avem în G relaţia

$$ee' = e' = e'e'.$$

Simplificând la dreapta relaţia $ee' = e'e'$ (adică o înmulţim la dreapta cu $(e')^{-1}$) obţinem $e = e'$.

Fie $x \in H$, x^{-1} inversul în G al lui x, iar x' inversul în H al lui x. Atunci, conform celor de mai înainte, avem în G

$$xx^{-1} = xx' = e.$$

Simplificând la stânga această relaţie, obţinem $x' = x^{-1}$, deci $x^{-1} \in H$.

2) $\Rightarrow$ 3) Dacă $x, y \in H$, conform cu iii), rezultă $y^{-1} \in H$ şi din i), $xy^{-1} \in H$.

3) $\Rightarrow$ 2) Dacă $x \in H$, atunci $xx^{-1} = e \in H$ şi $x^{-1} = ex^{-1} \in H$. De asemenea, dacă $y \in H$, cum $y^{-1} \in H$, se obţine

$$xy = x(y^{-1})^{-1} \in H.$$

2) $\Rightarrow$ 1) Asociativitatea operaţiei de pe H rezultă din faptul că operaţia lui G este asociativă. Restul este imediat.

Observaţie. Dacă G este un grup abelian, orice subgrup al său este abelian.

Exemple.

1) Dacă G este un grup, atunci G însuşi este un subgrup al lui G, numit *subgrupul total* al lui G. De asemenea submulţimea {e} a lui G este subgrup numit *subgrupul trivial* al lui G. Subgrupul total şi subgrupul trivial al unui grup G se numesc *subgrupuri improprii* ale lui G. Orice subgrup diferit de acestea se numeşte *subgrup propriu*.

2) Grupul aditiv **Z** al numerelor întregi este subgrup al grupului aditiv **Q** al numerelor raţionale; grupul aditiv **Q** este subgrup al grupului aditiv **R** al numerelor reale; grupul aditiv **R** este subgrup al grupului aditiv **C** al numerelor complexe.

De asemenea, grupul multiplicativ **Q*** este subgrup al grupului multiplicativ **R*** iar ambele sunt subgrupuri ale grupului multiplicativ **C***.

3) Grupul multiplicativ {–1, 1} este subgrup al grupului multiplicativ **Q***, iar grupul multiplicativ {–1, 1, – i, i} este subgrup al grupului multiplicativ **C***. Mai general, U_n este subgrup al grupului multiplicativ **C***. (De fapt, orice subgrup finit al lui **C*** este egal cu un U_n.)

4) Fie M o mulţime, $N \subset M$ o submulţime proprie a lui M, iar S(M) grupul permutărilor mulţimii M. Mulţimea $H = \{f \in S(M) \mid f(x) = x$ oricare ar fi $x \in M \setminus N\}$ este un subgrup al lui S(M).

5) Mulţimea automorfismelor interioare Int(G) ale unui grup G este subgrup al grupului automorfismelor Aut(G).

6) Fie **Z** grupul aditiv al numerelor întregi, iar $n \in \mathbf{Z}$ un număr întreg oarecare. Submulţimea $n\mathbf{Z} = \{nk \mid k \in \mathbf{Z}\}$ a lui **Z** este un subgrup al lui **Z.** Într-adevăr, dacă $x, y \in \mathbf{Z}$, $x = nh$ şi $y = nk$ cu $h, k \in \mathbf{Z}$, atunci

$$x - y = n(h - k) \in n\mathbf{Z}$$

şi conform punctului 3) al propoziţiei precedente rezultă că $n\mathbf{Z}$ este subgrup al lui **Z**. Observăm că $n\mathbf{Z} = (-n)\mathbf{Z}$. Mai mult, propoziţia următoare ne arată că orice subgrup al lui **Z** este de acest tip.

Propoziţia 2.3. Dacă H este un subgrup oarecare al grupului aditiv **Z**, atunci există $n \in \mathbf{Z}$, $n \geq 0$, astfel încât $H = n\mathbf{Z}$.

Demonstraţie. Fie $H \subseteq \mathbf{Z}$ un subgrup oarecare al grupului aditiv **Z**.

Dacă $H = \{0\}$, adică H este subgrupul nul, atunci $H = 0\mathbf{Z}$.

Dacă $H \neq \{0\}$, atunci există $x \in H$, $x \neq 0$. Datorită punctului 2) al propoziţiei precedente, $-x \in H$. Rezultă că H conţine numere întregi pozitive. Fie n cel mai mic număr întreg pozitiv din H. Avem că $0 \in H$, $n \in H$, $2n = n + n \in H$ şi, în general, $kn \in H$ oricare ar fi k număr natural, după cum rezultă din punctul 1) al propoziţiei precedente. De asemenea, din punctul 2) al aceleiaşi propoziţii, $kn \in H$ oricare ar fi k întreg negativ, deci $n\mathbf{Z} \subseteq H$.

Fie acum $x \in H$ un element oarecare. Conform teoremei împărţirii cu rest pentru numere întregi putem scrie $x = nq + r$, unde $0 \leq r < n$. Deoarece x şi nq sunt din H, rezultă că $r = x - nq$ aparţine lui H. Cum $0 \leq r < n$, iar n este cel mai mic număr natural nenul din H, rezultă că $r = 0$, deci $x = nq \in n\mathbf{Z}$.

Aşadar $H \subseteq n\mathbf{Z}$, de unde $H = n\mathbf{Z}$.

Exerciţiu. Determinaţi subgrupurile grupului lui Klein $\mathbf{Z}_2 \times \mathbf{Z}_2$.

Nucleul şi imaginea unui morfism de grupuri

Fie G şi G' două grupuri, iar $f : G \to G'$ un morfism de grupuri. Fie $H \leq G$ şi $H' \leq G'$ subgrupuri. Să considerăm

$$f(H) = \{x' \in G' \mid \text{există } x \in H \text{ astfel încât } x' = f(x)\},$$

imaginea (directă a) lui H prin f şi

$$f^{-1}(H') = \{x \in G \mid f(x) \in H'\},$$

imaginea reciprocă a lui H' prin f.

Se notează $\operatorname{Ker} f = f^{-1}(\{e'\})$ şi se numeşte *nucleul* morfismului f. De asemenea, $\operatorname{Im} f = f(G)$ şi se numeşte *imaginea* morfismului f. Deci

$$\operatorname{Ker} f = \{x \in G \mid f(x) = e'\} \text{ şi}$$

$$\operatorname{Im} f = \{x' \in G' \mid \text{există } x \in G \text{ astfel încât } x' = f(x)\} = \{f(x) \mid x \in G\}.$$

Propoziţia 2.4. Fie $f : G \to G'$ un morfism de grupuri. Avem:

1) Dacă H este subgrup al lui G, atunci f(H) este subgrup al lui G'. (În particular, Im f este un subgrup al lui G');

2) Dacă H' este subgrup al lui G', atunci $f^{-1}(H')$ este subgrup al lui G. (În particular, Ker f este un subgrup al lui G).

Demonstraţie. 1) Cum $H \neq \emptyset$ este evident că $f(H) \neq \emptyset$. Dacă $x', y' \in f(H)$, atunci există $x, y \in H$ astfel încât $x' = f(x)$, $y' = f(y)$. Avem

$$x'y'^{-1} = f(x)(f(y))^{-1} = f(x)f(y^{-1}) = f(xy^{-1})$$

şi cum H este subgrup rezultă că $xy^{-1} \in H$ şi deci $x'^{-1}y'^{-1} = f(xy^{-1}) \in f(H)$.

2) Cum $e' \in H'$, iar $f(e) = e'$, rezultă că $e \in f^{-1}(H')$, adică $f^{-1}(H') \neq \emptyset$. Dacă $x, y \in f^{-1}(H')$, atunci $f(x), f(y) \in H'$; cum H' este subgrup

$$f(xy^{-1}) = f(x)f(y)^{-1} = f(x)f(y^{-1}) \in H',$$

adică $xy^{-1} \in f(H')$.

Propoziţia 2.5. Un morfism de grupuri $f : G \to G'$ este injectiv dacă şi numai dacă nucleul său este trivial, adică $\operatorname{Ker} f = \{e\}$.

Demonstraţie. Să presupunem că f este morfism injectiv. Avem $f(e) = e'$ şi dacă $x \in \operatorname{Ker} f$, atunci $f(x) = e'$, adică $f(x) = f(e)$. Cum funcţia f este injectivă, rezultă $x = e$.

Reciproc, fie $f(x) = f(y)$. Atunci $f(x)(f(y))^{-1} = e'$, adică $f(x)f(y^{-1}) = e'$ sau $f(xy^{-1}) = e'$ şi deci $xy^{-1} = e$, de unde $x = y$. Rezultă că f este injectivă.

Observaţie. În mod evident avem că un morfism de grupuri $f : G \to G'$ este surjectiv dacă şi numai dacă $\operatorname{Im} f = G'$.

Teorema 2.6. (Teorema de corespondenţă pentru subgrupuri) Fie $f : G \to G'$ un morfism *surjectiv* de grupuri. Există o corespondenţă bijectivă între mulţimea subgrupurilor lui G care conţin Ker f şi mulţimea tuturor subgrupurilor lui G', dată prin $H \to f(H)$.

Demonstraţie. Mai întâi observăm că dacă H este un subgrup al lui G care conţine Ker f, atunci $f^{-1}(f(H)) = H$. Într-adevăr, $H \subseteq f^{-1}(f(H))$ iar dacă $x \in f^{-1}(f(H))$, atunci $f(x) \in f(H)$, deci există $h \in H$ astfel încât $f(x) = f(h)$. De aici rezultă că $f(xh^{-1}) = e'$, ceea ce înseamnă că $xh^{-1} \in \text{Ker } f$. Cum însă $\text{Ker } f \subseteq H$ obţinem $xh^{-1} \in H$, deci $x \in H$.

Acum rezultă imediat că aplicaţia dată este injectivă: dacă H şi K sunt subgrupuri ale lui G care conţin Ker f şi $f(H) = f(K)$, atunci $f^{-1}(f(H)) = f^{-1}(f(K))$, deci $H = K$.

Pentru a demonstra că aplicaţia este surjectivă considerăm H' un subgrup al lui G' şi fie $H = f^{-1}(H')$. Evident $H \supseteq \text{Ker } f$ şi deoarece f este funcţie surjectivă avem că $f(H) = H'$.

Subgrupul generat de o submulţime a unui grup

Observăm mai întâi că dacă $(H_i)_{i \in I}$ este o familie de subgrupuri ale unui grup G, atunci $\bigcap_{i \in I} H_i$ este un subgrup al lui G. Într-adevăr, fie $x, y \in \bigcap_{i \in I} H_i$. Atunci $x, y \in H_i$, oricare ar fi $i \in I$, şi cum fiecare H_i este un subgrup rezultă că $xy^{-1} \in H_i$, oricare ar fi $i \in I$. Deci $xy^{-1} \in \bigcap_{i \in I} H_i$.

Definiţia 2.7. Fie G un grup şi X o submulţime a lui G. Intersecţia tuturor subgrupurilor care conţin mulţimea X (această intersecţie fiind un subgrup, conform celor precedente) se numeşte *subgrupul generat* de X în G. Vom nota acest subgrup cu $\langle X \rangle$. Deci

$$\langle X \rangle = \bigcap_{\substack{X \subseteq K \\ K \subseteq G \text{ subgrup}}} K$$

Dacă $H = \langle X \rangle$, adică H este subgrupul generat de X, se spune că X este un *sistem de generatori* pentru H sau că X *generează* pe H.

Observaţii.

1) $\langle X \rangle$ este cel mai mic subgrup al lui G care conţine pe X.

2) Dacă $X = \emptyset$, atunci subgrupul generat de X este subgrupul trivial $\{e\}$.

3) Dacă X este un subgrup al lui G, atunci printre subgrupurile lui G care conţin pe X se găseşte X însuşi şi deci subgrupul generat de X este chiar X. Cum subgrupul generat de un subgrup este subgrupul însuşi, rezultă că orice subgrup al unui grup G are cel puţin un sistem de generatori.

Un subgrup H al lui G care admite un sistem finit de generatori se spune că este un subgrup *finit generat*. Un subgrup H al lui G care admite un sistem de generatori format dintr-un singur element se spune că este un subgrup *ciclic*. În acest caz vom scrie $H = \langle a \rangle$, unde $a \in H$.

Următoarea teoremă ne dă forma elementelor subgrupului generat de o submulţime nevidă X în G.

Teorema 2.8. Fie $X \neq \emptyset$ o submulţime a lui G. Atunci $\langle X \rangle$, subgrupul generat de X în G, este format din mulţimea elementelor lui G care se pot scrie sub forma

$$x_1^{\varepsilon_1} x_2^{\varepsilon_2} \ldots x_k^{\varepsilon_k}, \text{ unde } k \geq 0, \varepsilon_i = \pm 1, x_i \in X, 1 \leq i \leq k.$$

Demonstraţie. Fie

$$H' = \{x \in G \mid x = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \ldots x_k^{\varepsilon_k}, \text{ unde } k \geq 0, \varepsilon_i = \pm 1, x_i \in X, 1 \leq i \leq k\}.$$

Arătăm că H' este subgrup al lui G care conţine pe X. Într-adevăr, oricare ar fi $x \in X$, $x = x^1 \in H'$. Deci $X \subseteq H'$, de unde $H' \neq \emptyset$. Dacă $x, y \in H'$, atunci $x = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \ldots x_k^{\varepsilon_k}$, $y = y_1^{\mu_1} y_2^{\mu_2} \ldots y_s^{\mu_s}$, $\varepsilon_i = \pm 1$, $\mu_j = \pm 1$, $x_i, y_j \in X$, $1 \leq i \leq k$, $1 \leq j \leq s$, şi deci $xy^{-1} = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \ldots x_k^{\varepsilon_k} y_s^{-\mu_s} \ldots y_2^{-\mu_2} y_1^{-\mu_1} \in H'$.

Cum H' este un subgrup care conţine pe X, rezultă că H' include intersecţia tuturor subgrupurilor lui G care conţin pe X, adică $\langle X \rangle \subseteq H'$.

Reciproc, fie H este un subgrup al lui G care conţine pe X. Dacă $x_1, x_2, \ldots, x_k \in X \subseteq H$, rezultă că $x_1^{\varepsilon_1}, x_2^{\varepsilon_2}, \ldots, x_k^{\varepsilon_k} \in H$ şi H fiind subgrup avem că $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \ldots x_k^{\varepsilon_k} \in H$. Deci H conţine pe H'. Cum H este un subgrup arbitrar care conţine pe X, rezultă că H' este conţinut în intersecţia tuturor acestor subgrupuri, adică în $\langle X \rangle$.

Observaţii. În cazul în care grupul G este comutativ avem că

$$\langle X \rangle = \{x \in G \mid x = x_1^{n_1} x_2^{n_2} \ldots x_k^{n_k}, \text{ unde } k \geq 0, n_i \in \mathbf{Z}, x_i \in X, 1 \leq i \leq k\}.$$

Dacă folosim scrierea aditivă, atunci

$$\langle X \rangle = \{x \in G \mid x = n_1x_1 + n_2x_2 + \cdots + n_kx_k, \text{ unde } k \geq 0, n_i \in \mathbf{Z}, x_i \in X, 1 \leq i \leq k\}.$$

Dacă H este subgrup ciclic generat de elementul *a*, atunci din teorema precedentă rezultă că

$$H = \langle a \rangle = \{a^n \mid n \in \mathbf{Z}\}.$$

În scriere aditivă avem

$$H = \langle a \rangle = \{na \mid n \in \mathbf{Z}\}.$$

Elementul *a* se numeşte *generator* al subgrupului ciclic H.

Exemple.

1) Grupul aditiv $(\mathbf{Z}, +)$ al numerelor întregi este ciclic generat de 1 sau de –1, adică $(\mathbf{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$, iar în acest caz aceştia sunt singurii generatori posibili.

2) Dacă $m, n \in \mathbf{Z}$, atunci

(i) $m\mathbf{Z} \cap n\mathbf{Z} = [m, n]\mathbf{Z}$,

(ii) $\langle m, n \rangle = (m, n)\mathbf{Z}$,

unde $[m, n]$ = c.m.m.m.c.(m, n) şi (m, n) = c.m.m.d.c.(m, n).

Să demonstrăm (i). Dacă $x \in m\mathbf{Z} \cap n\mathbf{Z}$, adică $x \in m\mathbf{Z}$ şi $x \in n\mathbf{Z}$, atunci $m \mid x$ şi

n | x. Deci [m, n] | x, adică x ∈ [m, n]**Z**. Reciproc, dacă x ∈ [m, n]**Z**, atunci [m, n] | x şi deci m | x şi n | x, adică x ∈ m**Z** şi x ∈ n**Z**, de unde x ∈ m**Z** ∩ n**Z**.

Să demonstrăm (ii). Din teorema precedentă, în scriere aditivă, rezultă <m, n> = {x ∈ **Z** | x = mk + nl, unde k, l ∈ **Z**}. Dacă x ∈ <m,n>, atunci x = mk + nl cu k, l ∈ **Z** şi cum (m, n) | m şi (m, n) | n rezultă că (m, n) | mk + nl, adică (m, n) | x, de unde x ∈ (m, n)**Z**. Cum <m, n> este subgrup al lui **Z**, rezultă că există d ∈ **Z** astfel încât <m, n> = d**Z**. Dar m, n ∈ <m, n>, adică m, n ∈ d**Z** şi deci d | m şi d | n. Fie acum x ∈ (m, n)**Z**, adică (m, n) | x. Cum d este un divizor comun al numerelor m şi n, rezultă d | (m, n) şi deci d | x, adică x ∈ d**Z** = <m, n>.

Observăm că din (i) rezultă că orice două numere întregi au un c.m.m.m.c. Din (ii) rezultă că orice două numere întregi m şi n au un c.m.m.d.c. şi, mai mult, există k, l ∈ **Z** astfel încât (m, n) = mk + nl.

3) Grupul aditiv ($\mathbf{Z}_n$, +) al claselor de resturi modulo n este ciclic, generat de exemplu de [1], adică

$$(\mathbf{Z}_n, +) = < [1] >.$$

Să arătăm că [a] ∈ $\mathbf{Z}_n$ este generator al grupului ($\mathbf{Z}_n$,+) dacă şi numai dacă a şi n sunt prime între ele, adică (a, n) = 1.

Într-adevăr, dacă a este generator al lui $\mathbf{Z}_n$, adică $\mathbf{Z}_n$ = <[a]>, atunci există b ∈ **Z**, astfel încât [1] = b[a] sau [1] = [ba] deci n | 1 – ba, adică există k ∈ **Z** astfel încât 1 – ba = kn sau ab + nk = 1, ceea ce arată că (a, n) = 1.

Reciproc, dacă (a, n) = 1, atunci rezultă că [a] ∈ U($\mathbf{Z}_n$) şi deci există [b] ∈ $\mathbf{Z}_n$ cu [a][b] = 1. Atunci, dacă [x] ∈ $\mathbf{Z}_n$, [x] = [x • 1] = [x][1] = [x][a][b] = [xb][a] = (xb)[a]. Cum xb ∈ **Z** avem [x] ∈ <[a]>. Aşadar $\mathbf{Z}_n$ = <[a]>.

Exerciţiu. Să se arate că grupul (**Z** x **Z**, +) este finit generat, dar nu este ciclic.

Exerciţiu. (i) Să se arate că subgrupul lui (**Q**, +) generat de 1/2 şi 1/3 este ciclic şi să se determine un generator al acestuia.

(ii) Mai general, să se arate că orice subgrup finit generat al lui (**Q**, +) este ciclic.

(iii) Să se arate că grupul (**Q**, +) nu este finit generat.

Curs VI
ELEMENTE DE TEORIA GRUPURILOR

§ 3. RELAŢII DE ECHIVALENŢĂ PE UN GRUP ÎN RAPORT CU UN SUBGRUP AL SĂU

Fie G un grup şi H un subgrup al său. Considerăm pe G relaţiile binare R_H^s şi R_H^d definite în modul următor: dacă x, y ∈ G, atunci

$$x\ R_H^s\ y \text{ dacă şi numai dacă } x^{-1}y \in H,$$

$$x\ R_H^d\ y \text{ dacă şi numai dacă } xy^{-1} \in H.$$

Aceste relaţii binare sunt relaţii de echivalenţă. Să demonstrăm, de exemplu, că prima relaţie binară este relaţie de echivalenţă, adică este reflexivă, simetrică şi tranzitivă.

1) Dacă x ∈ G, atunci $x^{-1}x = e \in H$ şi deci $x\ R_H^s\ x$ (reflexivitatea).

2) Dacă $x\ R_H^s\ y$, atunci $x^{-1}y \in H$ şi deci $y^{-1}x = (x^{-1}y)^{-1} \in H$, de unde $y\ R_H^s\ x$ (simetria).

3) Dacă $x\ R_H^s\ y$ şi $y\ R_H^s\ z$, atunci $x^{-1}y \in H$ şi $y^{-1}z \in H$. Deci $x^{-1}z = (x^{-1}y)(y^{-1}z) \in H$, adică $x\ R_H^s\ z$ (tranzitivitatea).

Analog se demonstrează că R_H^d este relaţie de echivalenţă.

Relaţiile de echivalenţă R_H^s şi R_H^d se numesc *relaţii de congruenţă la stânga*, respectiv *la dreapta*, *în raport cu H* (sau *modulo H*). Faptul că „x este în relaţia R_H^s cu y” (respectiv „x este în relaţia R_H^d cu y”) se mai citeşte *x este congruent cu y modulo H la stânga* (respectiv *x este congruent cu y modulo H la dreapta*) şi scriem

$$x \equiv_s y \pmod H, \text{ respectiv } x \equiv_d y \pmod H.$$

Să notăm cu $[x]_s$, respectiv $[x]_d$, clasa de echivalenţă a elementului x ∈ G în raport cu R_H^s, respectiv R_H^d, şi o vom numi *clasa de echivalenţă la stânga*, respectiv *clasa de echivalenţă la dreapta a lui x modulo H*.

Fie G/R_H^s şi G/R_H^d mulţimile factor (cât) corespunzătoare lui R_H^s şi R_H^d, adică mulţimile claselor de echivalenţă la stânga, respectiv la dreapta modulo H.

Exemple.

1) Dacă G este un grup, relaţiile de congruenţă la stânga şi la dreapta modulo {e} coincid (adică $x\ R_{\{e\}}^s\ y$ dacă şi numai dacă $x\ R_{\{e\}}^d\ y$). De asemenea, relaţiile R_G^s şi R_G^d modulo G coincid.

2) Dacă G este un grup comutativ, iar H un subgrup oarecare al lui G, atunci relaţiile de congruenţă la stânga şi la dreapta modulo H coincid.

3) Fie $\mathbf{S}_3$ grupul permutărilor de 3 elemente, adică

$$\mathbf{S}_3 = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

şi

$$H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}.$$

Este evident că H este un subgrup al lui $\mathbf{S}_3$.

Să construim mulţimile claselor de echivalenţă la stânga şi la dreapta modulo H. Dacă σ, $\tau \in \mathbf{S}_3$, atunci $\sigma^{-1}\tau \in H$ dacă şi numai dacă $\sigma^{-1}\tau(3) = 3$, dacă şi numai dacă $\sigma(3) = \tau(3)$. Deci obţinem trei clase de echivalenţă la stânga şi anume:

$$C_1^s = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\}, \quad C_2^s = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\},$$

$$C_3^s = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}.$$

Dacă σ, $\tau \in \mathbf{S}_3$, atunci $\sigma\tau^{-1} \in H$ dacă şi numai dacă $\tau^{-1}(3) = \sigma^{-1}(3)$. Deci clasele de echivalenţă la dreapta sunt:

$$C_1^d = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\}, \quad C_2^d = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\},$$

$$C_3^d = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}.$$

Se observă că mulţimile factor $S_3 / R_H^s = \{C_1^s, C_2^s, C_3^s\}$ şi $S_3 / R_H^d = \{C_1^d, C_2^d, C_3^d\}$ sunt diferite.

Notaţii. Fie G un grup şi fie A, B două submulţimi nevide ale sale. Notăm prin

$$AB = \{ab \mid a \in A,\ b \in B\}.$$

Dacă A = {a}, respectiv B = {b}, atunci în loc de AB scriem aB, respectiv Ab, adică $aB = \{ab \mid b \in B\}$, respectiv $Ab = \{ab \mid a \in A\}$.

Exerciţiu. Fie G un grup şi H, K ≤ G două subgrupuri.

(i) Arătaţi că HK este subgrup dacă şi numai dacă HK = KH.

(ii) Daţi un exemplu din care să rezulte că, în general, HK nu este subgrup.

Lema 3.1. Fie G un grup şi H un subgrup al său. Dacă x este un element oarecare al lui G, atunci

$$[x]_s = xH \text{ şi } [x]_d = Hx.$$

Demonstraţie. Să arătăm doar prima egalitate, a doua demonstrându-se analog. Fie $y \in [x]_s$. Atunci $x \, R_H^s \, y$, deci $x^{-1}y \in H$, adică $x^{-1}y = h \in H$, de unde $y = xh \in xH$.

Reciproc, dacă $y \in xH$, atunci $y = xh$ cu $h \in H$, deci $x^{-1}y = h \in H$ sau $x \, R_H^s \, y$, adică $y \in [x]_s$.

Observaţie. Observăm că $[e]_s = eH = H$ şi de asemenea $[e]_d = He = H$.

Propoziţia 3.2. Dacă G este un grup şi H un subgrup al său, atunci funcţia

$$\varphi: G / R_H^s \to G / R_H^d$$

dată prin $\varphi(xH) = Hx^{-1}$ este o funcţie bijectivă.

Demonstraţie. Să arătăm mai întâi că φ este bine definită, adică nu depinde de alegerea reprezentanţilor. Într-adevăr, dacă xH = yH, adică $x \, R_H^s \, y$, atunci $x^{-1}y \in H$ sau $x^{-1}(y^{-1})^{-1} \in H$. Deci $x^{-1} \, R_H^d \, y^{-1}$, adică $Hx^{-1} = Hy^{-1}$ sau $\varphi(xH) = \varphi(yH)$, ceea ce înseamnă că φ este bine definită.

Funcţia φ este injectivă căci dacă $\varphi(xH) = \varphi(yH)$, atunci $Hx^{-1} = Hy^{-1}$, adică $x^{-1} \, R_H^s \, y^{-1}$, deci $x^{-1}(y^{-1})^{-1} \in H$, de unde $x^{-1}y \in H$ sau $x \, R_H^s \, y$, deci xH = yH.

Faptul că φ este surjectivă este clar, deoarece $\varphi(x^{-1}H) = H(x^{-1})^{-1} = Hx$.

În particular, dacă una dintre mulţimile G / R_H^s sau G / R_H^d este finită, atunci şi cealaltă este finită şi au acelaşi număr de elemente. Se spune în acest caz că *H are indice finit în G* sau că *H este un subgrup de indice finit al lui G*, iar numărul de elemente al mulţimii G / R_H^s sau al mulţimii G / R_H^d, care este acelaşi, se numeşte *indicele lui H în G* şi se notează [G : H].

Exerciţiu. Fie G un grup şi H, K ≤ G subgrupuri de indice finit.

(i) Arătaţi că $[G : H \cap K] \leq [G : H][G : K]$.

(ii) Dacă c.m.m.d.c.([G : H], [G : K]) = 1, atunci $[G : H \cap K] = [G : H][G : K]$.

(iii) Daţi un exemplu în care c.m.m.d.c.([G : H], [G : K]) > 1 şi $[G : H \cap K] < [G : H][G : K]$.

(iv) Daţi un exemplu din care să rezulte că reciproca proprietăţii (ii) este falsă.

Se spune că un grup G este finit dacă mulţimea pe care este definită structura de grup (adică mulţimea subiacentă) este finită, iar numărul de elemente ale lui G se numeşte *ordinul* său şi se notează ord G sau |G|.

Este clar că dacă G este de ordin finit, atunci orice subgrup al său este de ordin finit şi, mai mult, indicele oricărui subgrup este finit.

Lema 3.3. Fie G un grup şi H un subgrup al său. Atunci funcţia

$$\psi : H \to xH,$$

dată de $\psi(h) = xh$, este bijectivă.

Demonstraţie. Dacă $\psi(h) = \psi(h')$, atunci $xh = xh'$, de unde prin simplificare, $h = h'$; deci ψ este injectivă.

Funcţia ψ este evident surjectivă şi deci este bijectivă.

În particular, dacă H este un subgrup finit, atunci toate clasele de echivalenţă la stânga ale lui G modulo H sunt mulţimi finite şi au acelaşi număr de elemente ca şi H.

Observaţie. Afirmaţia din lema precedentă referitoare la clasele de echivalenţă la stânga este valabilă şi pentru clasele de echivalenţă la dreapta.

Teorema 3.4. (Lagrange) Dacă G este un grup finit şi H un subgrup al său, atunci

$$\text{ord } G = [G : H] \text{ ord } H.$$

Demonstraţie. Conform propoziţiei de mai sus putem să facem demonstraţia considerând, de exemplu, numai relaţia de echivalenţă R_H^s pe G.

Fie x_1H, ... , x_kH clasele de echivalenţă la stânga modulo H; deci $k = [G : H]$. Atunci

$$G = \bigcup_{i=1}^{k} x_iH \text{ şi } x_iH \cap x_jH = \varnothing \text{ pentru orice } i \neq j,$$

de unde $|G| = \sum_{i=1}^{k} |x_iH|$. Având în vedere lema precedentă, rezultă că $|G| = k|H|$. Deci

$$\text{ord } G = [G : H] \text{ ord } H.$$

Corolarul 3.5. Dacă G este grup finit şi H un subgrup al său, atunci ord H | ord G. În particular, dacă ord G este un număr prim, atunci G nu are subgrupuri proprii, deci este ciclic.

Observaţii.

1) Dacă G este un grup finit şi d | ord G, nu rezultă numaidecât că există H un subgrup al lui G cu ord H = d.

2) Dacă G este grup *abelian* finit şi d | ord G, atunci există $H \leq G$ cu ord H = d.

3) Pentru cazul neabelian există totuşi o reciprocă parţială a teoremei lui Lagrange: Fie G un grup finit şi p un număr prim cu proprietatea că p | ord G. Atunci există $H \leq G$ cu ord H = p. (Teorema lui Cauchy)

§ 4. ORDINUL UNUI ELEMENT

G fiind un grup şi $a \in G$ un element oarecare, am numit $\langle a \rangle = \{a^k \mid k \in \mathbf{Z}\}$, *subgrupul ciclic generat de* a.

Reamintim că un grup G se numeşte *ciclic* dacă există $a \in G$ astfel încât $G = \langle a \rangle$. Elementul *a* este un *generator* al grupului ciclic G.

Am văzut că grupul aditiv **Z** este ciclic, generat de 1 sau –1. De asemenea, fiecare grup aditiv $\mathbf{Z}_n$ este ciclic, un generator al său fiind, de exemplu, [1].

Definiţia 4.1. Spunem că un element *a* al grupului G este de *ordin finit*, dacă există $i, j \in \mathbf{Z}$, $i \neq j$, astfel încât $a^i = a^j$. În caz contrar, adică dacă toate puterile lui *a* sunt distincte, spunem că *a* este element de *ordin infinit.*

Fie G un grup şi $a \in G$ un element al său. Să considerăm funcţia $\varphi: \mathbf{Z} \to G$ definită prin $\varphi(n) = a^n$. Avem, evident, $\text{Im}\,\varphi = \langle a \rangle$. Elementul *a* este de ordin finit dacă funcţia φ nu este injectivă şi este de ordin infinit dacă funcţia φ este injectivă.

Fie $a \in G$ un element de ordin finit şi $i < j$ astfel încât $a^i = a^j$. Atunci $a^{j-i} = e$ şi deci există o putere pozitivă a lui *a* egală cu elementul neutru. Aşadar mulţimea

$$M = \{k \in \mathbf{N}^* \mid a^k = e\}$$

este nevidă. Cum M este o submulţime nevidă de numere naturale, iar mulţimea numerelor naturale este bine ordonată, atunci M are un cel mai mic element. Numim *ordinul* elementului *a* şi-l notăm ord(a), cel mai mic număr întreg pozitiv n astfel încât $a^n = e$.

Deci $\text{ord}(a) = \min\{k \in \mathbf{N}^* \mid a^k = e\}$.

Propoziţia 4.2. Fie *a* un element de ordin finit al unui grup G şi n un număr natural nenul. Atunci $n = \text{ord}(a)$ dacă şi numai dacă sunt satisfăcute condiţiile:

1) $a^n = e$,

2) dacă $a^k = e$, $k \in \mathbf{Z}$, atunci $n \mid k$.

Demonstraţie. Fie $n = \text{ord}(a)$. Din definiţia ordinului lui *a* rezultă 1). Fie acum $k \in \mathbf{Z}$ astfel încât $a^k = e$. Conform teoremei împărţirii cu rest în mulţimea numerelor întregi, există $q, r \in \mathbf{Z}$ astfel încât $k = nq + r$, $0 \leq r < n$; atunci

$$a^r = a^{k-nq} = a^k a^{-nq} = a^k (a^n)^{-q} = ee^{-q} = e.$$

Cum n este cel mai mic număr natural nenul astfel încât $a^n = e$, iar $0 \leq r < n$, rezultă că $r = 0$ şi deci n divide k.

Reciproc, dacă n satisface 1) şi 2), iar $a^k = e$ cu $k \geq 1$, din 2) rezultă că n divide pe k, deci $n \leq k$. Aşadar, n este cel mai mic dintre numerele naturale nenule k astfel încât $a^k = e$, de unde $n = \text{ord}(a)$.

Propoziţia 4.3. Fie G un grup. Dacă $a \in G$ este un element de ordin n, atunci subgrupul ciclic generat de *a* are exact n elemente şi anume:

$$\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}.$$

Demonstraţie. Să demonstrăm mai întâi că $a^i \neq a^j$ oricare ar fi $i \neq j$, $0 \leq i, j \leq n-1$. Într-adevăr, dacă am avea $a^i = a^j$ cu $0 \leq i < j \leq n - 1$, atunci $a^{j-i} = e$ şi $0 < j - i < n$, contradicţie cu faptul că n este cel mai mic număr natural nenul astfel încât $a^n = e$.

Fie acum n = ord(a) iar k un număr întreg. Din teorema împărţirii cu rest există q, $r \in \mathbf{Z}$ astfel încât $k = nq + r$ cu $0 \le r \le n - 1$. Atunci $a^k = a^{nq+r} = (a^n)^q a^r = a^r$ şi deci $a^k \in \{e, a, \dots, a^{n-1}\}$.

Corolarul 4.4. Dacă G este un grup finit, atunci ordinul oricărui element al său divide ordinul lui G.

Demonstraţie. Rezultă din teorema lui Lagrange şi propoziţia precedentă.

Corolarul 4.5. Dacă G este un grup finit cu ord G = n, atunci $a^n = e$ pentru orice $a \in G$.

Demonstraţie. Rezultă din corolarul precedent.

Exemple.

1) Fie $(\mathbf{C}^*, \bullet)$ grupul multiplicativ al numerelor complexe nenule. Elementul $i \in \mathbf{C}^*$ are ordinul patru, iar $\langle i \rangle = \{1, -1, i, -i\}$.

2) Numărul complex $z_n = \cos(2\pi/n) + i \sin(2\pi/n)$ este un element de ordin n al grupului $(\mathbf{C}^*, \bullet)$. Mai mult, $\langle z_n \rangle = \{\cos(2k\pi/n) + i \sin(2k\pi/n) \mid k = 0, 1, \dots, n-1\}$.

3) Elementul [3] din grupul aditiv $(\mathbf{Z}_6, +)$ al claselor de resturi modulo 6 este de ordin 2.

4) Numărul complex nenul $z = a + bi$ cu $a^2 + b^2 \ne 1$ este element de ordin infinit al grupului $(\mathbf{C}^*, \bullet)$.

Aplicaţie. Am văzut că dacă se consideră monoidul multiplicativ $\mathbf{Z}_n$, al claselor de resturi modulo n, $n \ge 1$, atunci mulţimea $U(\mathbf{Z}_n)$ a elementelor inversabile din $\mathbf{Z}_n$ formează un grup multiplicativ. Mai mult, am demonstrat că $[a] \in U(\mathbf{Z}_n)$ dacă şi numai dacă $(a, n) = 1$ şi deci $|U(\mathbf{Z}_n)| = \varphi(n)$, unde φ este indicatorul lui Euler.

Dacă $a, n \in \mathbf{Z}$, $n \ge 1$ şi $(a, n) = 1$, atunci $[a] \in U(\mathbf{Z}_n)$ şi deci ord([a]) | φ(n). Prin urmare, există $m \in \mathbf{N}^*$ astfel încât $\varphi(n) = m \cdot \text{ord}([a])$, de unde rezultă că $[a^{\varphi(n)}] = [a]^{\varphi(n)} = ([a]^{\text{ord}([a])})^m = [1]^m = [1]$. Deci $[a]^{\varphi(n)} = [1]$, ceea ce este echivalent cu $a^{\varphi(n)} \equiv 1 \pmod n$, adică am obţinut o demonstraţie pentru *teorema lui Euler*.

Teorema 4.6. (Cauchy) Fie G un grup finit şi p un număr prim cu proprietatea că p | ord G. Atunci există $a \in G$ cu ord(a) = p.

Demonstraţie. Fie n = ord G şi definim $S = \{(a_1, \dots, a_p) \mid a_i \in G \text{ şi } a_1 \cdots a_p = e\}$. Avem $|S| = n^{p-1}$ şi cum p | n rezultă că $|S| \equiv 0 \pmod p$. Să mai observăm că o permutare ciclică a unui p-uplu $(a_1, \dots, a_p) \in S$ este tot un element al lui S.

Vom numi două p-upluri din S *echivalente* dacă unul este permutare ciclică a celuilalt. Astfel, $(a_1, \dots, a_p) \in S$ este echivalent cu exact p p-upluri distincte, excepţie facând cazul în care $a_1 = \dots = a_p$. Clasa de echivalenţă a unui p-uplu de forma (a, ... , a) are un singur element. Evident, S conţine un astfel de p-uplu, şi anume pe (e, ... , e). Dacă acesta este singurul p-uplu de forma (a, ... , a) din S, atunci $|S| \equiv 1 \pmod p$, contradicţie. Aşadar există un element $a \ne e$ cu proprietatea că $(a, \dots, a) \in S$, deci $a^p = e$. Se consideră acum $H = \langle a \rangle$ şi demonstraţia este încheiată.

Propoziţia 4.7. Dacă G este un grup şi $x \in G$ este un element de ordin n (finit), atunci $ord(x^k) = n/(n,k)$, pentru orice $k \in \mathbf{Z}$, $k \neq 0$.

Demonstraţie. Fie d = (n, k). Atunci putem scrie n = dm, k = dl, cu (m,l) = 1. Trebuie să arătăm că $ord(x^k) = m$.

Evident $(x^k)^m = x^{km} = x^{dlm} = x^{nl} = (x^n)^l = e^l = e$, deoarece ord(x) = n.

Fie $r \in \mathbf{Z}$ cu proprietatea că $(x^k)^r = e$. Atunci $x^{kr} = e$, de unde $n \mid kr$, deci $dm \mid dlr \Rightarrow m \mid lr \Rightarrow m \mid r$, deoarece (m, l) = 1.

O consecinţă imediată este faptul că $ord([k]) = n/(n,k)$ pentru orice $[k] \in \mathbf{Z}_n$.

Exerciţiu. Determinaţi elementele de ordin 30 din $\mathbf{Z}_{240}$.

Exerciţiu. (i) Fie G_1, G_2 două grupuri şi $x_1 \in G_1$, $x_2 \in G_2$ elemente de ordin finit. Arătaţi că ord $(x_1, x_2) = [ord(x_1), ord(x_2)]$.

(ii) Determinaţi ord ([3], [4]) în grupul $\mathbf{Z}_{24} \times \mathbf{Z}_{36}$.

Curs VII
ELEMENTE DE TEORIA GRUPURILOR

§ 5. SUBGRUPURI NORMALE

Definiţia 5.1. Un subgrup N al unui grup G se spune că este subgrup *normal* dacă oricare ar fi $x \in G$ şi $h \in N$, avem $xhx^{-1} \in N$.

Notaţie. $N \lhd G$

Observaţie. Pentru un grup G şi $x \in G$ am definit automorfismul interior $\varphi_x : G \to G$, $\varphi_x(g) = xgx^{-1}$. Din definiţie rezultă că un subgrup N al lui G este subgrup normal dacă şi numai dacă $\varphi_x(N) \subseteq N$, oricare ar fi $x \in G$.

Propoziţia 5.2. Dacă N este un subgrup al grupului G, afirmaţiile următoare sunt echivalente:

1) N este subgrup normal;
2) Relaţiile de congruenţă modulo N, adică R_N^s şi R_N^d coincid;
3) $xN = Nx$, oricare ar fi $x \in G$;
4) $G / R_N^s = G / R_N^d$.

Demonstraţie. 1) $\Rightarrow$ 2) Dacă $x \, R_N^s \, y$, atunci $x^{-1}y \in N$. Fie $h = x^{-1}y \in N$. Atunci $xh = y$. Dar cum N este subgrup normal, avem $xhx^{-1} \in N$, adică $yx^{-1} \in N$, deci şi $(yx^{-1})^{-1} = xy^{-1} \in N$, adică $x \, R_N^d \, y$.

Analog se demonstrează că dacă $x \, R_N^d \, y$, atunci $x \, R_N^s \, y$, deci relaţiile R_N^s şi R_N^d coincid.

2) $\Rightarrow$ 3) Dacă $y \in xN$, atunci $y = xh$ cu $h \in N$, deci $x^{-1}y = h \in N$, adică $x \, R_N^s \, y$. Deci $x \, R_N^d \, y$, adică $yx^{-1} \in N$ sau $yx^{-1} = h' \in N$, de unde $y = h'x \in Nx$; deci $xN \subseteq Nx$. Analog se demonstrează că $Nx \subseteq xN$.

3) $\Rightarrow$ 4) Evident.

4) $\Rightarrow$ 3) Fie $x \in G$. Avem $xN \in G / R_N^s$ şi cum $G / R_N^s = G / R_N^d$ rezultă că există $y \in G$ cu proprietatea că $xN = Ny$. Dar $x \in xN$, deci $x \in Ny \Rightarrow x \, R_N^d \, y \Rightarrow Ny = Nx$, deci $xN = Nx$.

3) $\Rightarrow$ 2) Fie $x, y \in G$ cu $x \, R_N^s \, y$. Atunci $xN = yN$ şi cum $xN = Nx$ şi $yN = Ny$ rezultă că $Nx = Ny$, de unde $x \, R_N^d \, y$. Reciproc se arată la fel.

3) $\Rightarrow$ 1) Dacă $x \in G$ şi $h \in N$, atunci $xh \in xN = Nx$ şi deci $xh = h'x$ cu $h' \in N$, de unde $xhx^{-1} = h' \in N$, adică N este subgrup normal.

Exemple.

1) G şi {e} sunt subgrupuri normale ale grupului G.
2) Dacă G este un grup abelian, este clar că orice subgrup al său este normal.

3) Orice subgrup de indice 2 al unui grup oarecare G este normal.

Într-adevăr, dacă H este subgrup al lui G astfel încât [G : H] = 2, atunci

$$G / R_H^s = \{H, G \setminus H\} \text{ şi } G / R_H^d = \{H, G \setminus H\}.$$

Deci $G / R_H^s = G / R_H^d$.

4) Fie grupul $\mathbf{S}_3$ al permutărilor de 3 elemente şi permutarea $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$.

Submulţimea H = {e, τ} este un subgrup al lui $\mathbf{S}_3$ care nu este normal. Într-adevăr, dacă

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \text{ atunci } \sigma\tau\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \notin H.$$

(Această afirmaţie rezultă şi din paragraful precedent, unde am arătat că mulţimile factor la stânga şi la dreapta ale lui $\mathbf{S}_3$ în raport cu H sunt diferite.)

Propoziţia 5.3. Fie f : G → G' un morfism de grupuri. Avem:

1) Dacă N este subgrup normal al lui G, iar f este surjectiv, atunci f(N) este subgrup normal al lui G'.

2) Dacă N' este subgrup normal al lui G', atunci $f^{-1}(N')$ este subgrup normal al lui G. În particular, Ker f este subgrup normal al lui G.

Demonstraţie. 1) Fie g' ∈ G' şi h ∈ N. Vrem să arătăm că $g'f(h)(g')^{-1} \in f(N)$. Deoarece f este surjectivă există g ∈ G astfel încât f(g) = g'. Atunci $g'f(h)(g')^{-1} = f(g)f(h)f(g)^{-1} = f(ghg^{-1}) \in f(N)$, deoarece N este subgrup normal.

2) Fie g ∈ G şi h ∈ $f^{-1}(N')$. Vrem să arătăm că $ghg^{-1} \in f^{-1}(N')$, adică $f(ghg^{-1}) \in N'$. Dar f(h) ∈ N' şi cum N' este normal în G' rezultă că $f(g)f(h)f(g)^{-1} \in N'$, adică $f(ghg^{-1}) \in N'$.

Exerciţiu. Daţi un exemplu de subgrup normal a cărui imagine printr-un morfism de grupuri să nu fie subgrup normal.

Teorema 5.4. (Teorema de corespondenţă pentru subgrupuri normale) Fie f : G → G' un morfism *surjectiv* de grupuri. Există o corespondenţă bijectivă între mulţimea subgrupurilor normale ale lui G care conţin Ker f şi mulţimea tuturor subgrupurilor normale ale lui G', dată prin N → f(N).

Demonstraţie. Corespondenţa N → f(N) este corect definită după cum rezultă din propoziţia 5.3. Restul este la fel ca în demonstraţia teoremei 2.6 din cursul 5.

§ 6. GRUP FACTOR

Fie G un grup şi N un subgrup normal al său. După cum rezultă din cele de mai înainte, relaţiile de congruenţă R_N^s şi R_N^d (la stânga şi la dreapta modulo N) coincid. În acest caz vom spune, pe scurt, congruenţa modulo N, iar dacă x, y ∈ G, faptul că x este

congruent cu y modulo N îl vom scrie $x \equiv y \pmod N$. Cele două mulţimi factor G / R_N^s şi G / R_N^d coincid, mulţimea factor fiind notată cu G/N.

Propoziţia 6.1. Dacă G este un grup şi N un subgrup normal al său, atunci pe mulţimea factor G/N se poate defini o operaţie algebrică împreună cu care G/N devine grup, iar funcţia surjectivă $p: G \to G/N$, $p(x) = [x]$ este morfism de grupuri cu Ker p = N.

Demonstraţie. Dacă $x, y \in G$, definim

$$[x][y] = [xy].$$

Să arătăm că în acest mod se defineşte o operaţie algebrică pe G/N, împreună cu care G/N devine grup.

Să demonstrăm mai întâi că operaţia este bine definită, adică nu depinde de alegerea reprezentanţilor. Într-adevăr, dacă [x] = [x'] şi [y] = [y'], atunci avem $x^{-1}x' \in N$ şi $y^{-1}y' \in N$, adică există $h_1, h_2 \in N$ astfel încât $x^{-1}x' = h_1$ şi $y^{-1}y' = h_2$, adică $x' = xh_1$ şi $y' = yh_2$. Deci $x'y' = (xh_1)(yh_2) = x(h_1y)h_2$. Dar cum N este subgrup normal, există $h_3 \in N$ astfel încât $h_1y = yh_3$ (deoarece Ny = yN), de unde se obţine $x'y' = x(yh_3)h_2 = (xy)(h_3h_2)$, iar $h_3h_2 \in N$. Deci $(xy)^{-1}(x'y') = h_3h_2 \in N$, adică xy este congruent modulo N cu x'y', de unde [xy] = [x'y']. Deci operaţia algebrică este bine definită.

Operaţia este asociativă, deoarece dacă [x], [y], [z] ∈ G/N, atunci

$$[x]([y][z]) = [x][yz] = [x(yz)] = [(xy)z] = [xy][z] = ([x][y])[z].$$

Operaţia admite ca element neutru [e] ∈ G/N (unde e este elementul neutru din G), deoarece oricare ar fi [x] ∈ G/N avem, în mod evident,

$$[x][e] = [e][x] = [x].$$

Orice element [x] ∈ G/N are un invers care este $[x^{-1}] \in G/N$, deoarece

$$[x][x^{-1}] = [xx^{-1}] = [e] \text{ şi } [x^{-1}][x] = [x^{-1}x] = [e].$$

Astfel am demonstrat că G/N este un grup.

Funcţia surjectivă $p: G \to G/N$, unde p(x) = [x], este un morfism de grupuri. Într-adevăr,

$$p(xy) = [xy] = [x][y] = p(x)p(y).$$

Arătăm acum că Ker p = N. Dacă $x \in \text{Ker } p$, atunci p(x) = [e], deci [x] = [e], de unde $x \equiv e \pmod N$ sau $xe^{-1} \in N$, adică $x \in N$. Reciproc, dacă $x \in N$, atunci $x \equiv e \pmod N$, adică [x] = [e], de unde p(x) = [x] = [e] şi deci $x \in \text{Ker } p$.

Definiţia 6.2. Grupul G/N construit în propoziţia precedentă se numeşte *grupul factor* (*cât*) al lui G în raport cu subgrupul normal N. Morfismul $p: G \to G/N$, p(x) = [x] se numeşte *proiecţia* (*surjecţia*) *canonică* a lui G pe grupul factor G/N.

Observaţii.

1) Dacă G este un grup comutativ, atunci orice subgrup al său este normal şi deci putem vorbi de grupul factor al lui G în raport cu orice subgrup al său. Mai mult, dacă G este comutativ, orice grup factor al său este comutativ.

2) Proiecţia canonică p: $G \to G/\{e\}$ este izomorfism de grupuri.

Exemplu. Să determinăm grupurile factor ale grupului aditiv ($\mathbf{Z}$, +).

Fie $H \subseteq \mathbf{Z}$ un subgrup al lui $\mathbf{Z}$. Atunci $H = n\mathbf{Z}$, unde $n \geq 0$.

Dacă $n = 0$, adică $H = \{0\}$, avem $\mathbf{Z}/\{0\} \cong \mathbf{Z}$.

Dacă $n \geq 1$, atunci pentru $x, y \in \mathbf{Z}$, avem $x \equiv y \pmod{n\mathbf{Z}}$ dacă şi numai dacă $x - y \in n\mathbf{Z}$, dacă şi numai dacă $n \mid x - y$, dacă şi numai dacă $x \equiv y \pmod{n}$. Aşadar, relaţia de echivalenţă pe $\mathbf{Z}$ modulo subgrupul $n\mathbf{Z}$ coincide cu relaţia de congruenţă modulo n. Mai mult, operaţia algebrică pe grupul factor $\mathbf{Z}/n\mathbf{Z}$ coincide cu adunarea claselor de resturi modulo n. Deci grupul factor ($\mathbf{Z}/n\mathbf{Z}$, +) al lui $\mathbf{Z}$ în raport cu subgrupul $n\mathbf{Z}$ este izomorf cu grupul aditiv al claselor de resturi modulo n, adică $\mathbf{Z}/n\mathbf{Z} \cong \mathbf{Z}_n$.

Din teorema de corespondenţă pentru subgrupuri (normale) obţinem:

Propoziţia 6.3. Fie G un grup şi N un subgrup normal al lui G. Există o corespondenţă bijectivă între mulţimea subgrupurilor (normale) ale lui G care conţin pe N şi mulţimea tuturor subgrupurilor (normale) ale lui G/N, dată prin $H \to H/N$.

Exemplu. Să determinăm subgrupurile grupului factor ($\mathbf{Z}/n\mathbf{Z}$, +), unde $n \geq 2$.

Fie $K \subseteq \mathbf{Z}/n\mathbf{Z}$ un subgrup al lui $\mathbf{Z}/n\mathbf{Z}$. Atunci $K = H/n\mathbf{Z}$, unde H este un subgrup al lui $\mathbf{Z}$ care-l conţine pe $n\mathbf{Z}$. Ţinând seama de forma subgrupurilor lui $\mathbf{Z}$ deducem că există un $d \in \mathbf{N}$ astfel ca $H = d\mathbf{Z}$. Dar $n\mathbf{Z} \subseteq H$ dacă şi numai dacă $n\mathbf{Z} \subseteq d\mathbf{Z}$ dacă şi numai dacă $d \mid n$. În concluzie, $K = d\mathbf{Z}/n\mathbf{Z}$ cu $d \mid n$. (Dacă ţinem cont de izomorfismul dintre $\mathbf{Z}/n\mathbf{Z}$ şi $\mathbf{Z}_n$ putem scrie $K = [d]\mathbf{Z}_n$ cu $d \mid n$.)

În particular, grupul ($\mathbf{Z}_6$, +) are 4 subgrupuri şi anume: $\langle[0]\rangle = \{[0]\}$; $\langle[1]\rangle = \mathbf{Z}_6$; $\langle[2]\rangle = \{[0], [2], [4]\}$; $\langle[3]\rangle = \{[0], [3]\}$.

Teorema 6.4. (Proprietatea de universalitate a grupurilor factor) Fie $f : G \to G'$ un morfism de grupuri şi N un subgrup normal al lui G. Dacă $N \subseteq \operatorname{Ker} f$, atunci există un morfism de grupuri $\overline{f} : G/N \to G'$ unic cu proprietatea că $\overline{f} \circ p = f$, unde $p : G \to G/N$ este proiecţia canonică. Mai mult:

1) $\overline{f}$ este injectiv $\Leftrightarrow N = \operatorname{Ker} f$;
2) $\overline{f}$ este surjectiv $\Leftrightarrow$ f este surjectiv.

Am observat mai înainte că dacă $f : G \to G'$ este un morfism de grupuri, atunci nucleul său, Ker f, este subgrup normal al lui G şi deci putem vorbi de grupul factor G/Ker f. De asemenea, am arătat că Im f este un subgrup al lui G'.

Teorema 6.5. (Teorema fundamentală de izomorfism pentru grupuri) Fie $f : G \to G'$ un morfism de grupuri. Atunci există un izomorfism de grupuri

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

Demonstraţie. Definim $\overline{f} : G/\operatorname{Ker} f \to \operatorname{Im} f$, prin $\overline{f}([x]) = f(x)$.

Funcţia $\overline{f}$ este bine definită, adică nu depinde de alegerea reprezentanţilor. Într-adevăr, dacă [x] = [y], rezultă $x^{-1}y \in \text{Ker } f$, adică $f(x^{-1}y) = e'$. Dar $f(x^{-1}y) = f(x^{-1})f(y) = (f(x))^{-1}f(y)$, de unde $(f(x))^{-1}f(y) = e'$, adică $f(x) = f(y)$ şi deci $\overline{f}([x]) = \overline{f}([y])$.

Faptul că $\overline{f}$ este surjectivă este clar, deoarece orice element din Im f se scrie sub forma f(x), cu $x \in G$, iar $\overline{f}([x]) = f(x)$.

Să demonstrăm injectivitatea funcţiei $\overline{f}$. Într-adevăr, dacă $\overline{f}([x]) = \overline{f}([y])$, atunci $f(x) = f(y)$ şi deci $(f(x))^{-1}f(y) = e'$, adică $f(x^{-1}y) = e'$, de unde $x^{-1}y \in \text{Ker } f$, ceea ce înseamnă că [x] = [y].

Ţinând seama că f este morfism de grupuri, rezultă

$$\overline{f}([x][y]) = \overline{f}([xy]) = f(xy) = f(x)f(y) = \overline{f}([x])\ \overline{f}([y]),$$

adică $\overline{f}$ este morfism de grupuri.

Deci $\overline{f}$ este un izomorfism de grupuri.

Observaţie. Existenţa unui (izo)morfism de grupuri $\overline{f} : G/\text{Ker } f \to \text{Im } f$ se poate arăta folosind proprietatea de universalitate a grupurilor factor astfel: fie $f' : G \to \text{Im } f$ corestricţia lui f la Im f. Deoarece Ker f' = Ker f, din proprietatea de universalitate a grupurilor factor există un morfism de grupuri $\overline{f} : G/\text{Ker } f \to \text{Im } f$ unic cu proprietatea că $\overline{f} \circ p = f'$, unde $p : G \to G/\text{Ker } f$ este proiecţia canonică. Cum f' este surjectiv, rezultă că $\overline{f}$ este izomorfism.

Exemple.

Fie $\mathbf{R}^*_+$ grupul multiplicativ al numerelor reale strict pozitive, $\mathbf{C}^*$ grupul multiplicativ al numerelor complexe nenule, iar S subgrupul numerelor complexe de modul 1. Atunci:

1) Grupul factor $\mathbf{C}^*/S$ este izomorf cu $\mathbf{R}^*_+$.

Într-adevăr, fie $\varphi : \mathbf{C}^* \to \mathbf{R}^*_+$ definită prin $\varphi(z) = |z|$. Avem că φ este morfism surjectiv de grupuri, adică $\text{Im } \varphi = \mathbf{R}^*_+$ şi $\text{Ker } \varphi = S$. Din teorema fundamentală de izomorfism pentru grupuri rezultă că $\mathbf{C}^*/S \cong \mathbf{R}^*_+$.

2) Grupul factor $\mathbf{C}^*/\mathbf{R}^*_+$ este izomorf cu S.

Fie $\psi : \mathbf{C}^* \to \mathbf{C}^*$ definită prin $\psi(z) = z/|z|$. Avem că ψ este morfism de grupuri, $\text{Ker } \psi = \mathbf{R}^*_+$ şi $\text{Im } \psi = S$. Din teorema precedentă rezultă că $\mathbf{C}^*/\mathbf{R}^*_+ \cong S$.

3) Grupurile factor ale lui $\mathbf{Z}/n\mathbf{Z}$.

Fie $K = d\mathbf{Z}/n\mathbf{Z}$, $d \mid n$, un subgrup al lui $\mathbf{Z}/n\mathbf{Z}$. Din proprietatea de universalitate a grupurilor factor deducem că există un morfism surjectiv de grupuri $f : \mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/d\mathbf{Z}$. Ţinând seama de modul în care se defineşte f rezultă că $\text{Ker } f = d\mathbf{Z}/n\mathbf{Z}$. Atunci, din teorema fundamentală de izomorfism pentru grupuri, obţinem că grupul factor $(\mathbf{Z}/n\mathbf{Z})/K$ este izomorf cu $\mathbf{Z}/d\mathbf{Z}$. (Dacă ţinem cont de izomorfismul dintre $\mathbf{Z}/n\mathbf{Z}$ şi $\mathbf{Z}_n$ putem scrie astfel: $\mathbf{Z}_n/[d]\mathbf{Z}_n \cong \mathbf{Z}_d$.)

Mai rezultă că $|d\mathbf{Z}/n\mathbf{Z}| = n/d$.

Exerciţiu. Fie G_1, G_2 două grupuri şi H_1, respectiv H_2 subgrupuri normale. Arătaţi că $H_1 \times H_2$ este subgrup normal al lui $G_1 \times G_2$. Mai mult, avem că

$$(G_1 \times G_2)/(H_1 \times H_2) \cong G_1/H_1 \times G_2/H_2.$$

(Generalizaţi la un produs arbitrar de grupuri.)

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

Teorema 6.6. (A doua teoremă de izomorfism pentru grupuri) Fie G un grup şi H, K subgrupuri ale lui G. Dacă K este subgrup normal, atunci HK este un subgrup al lui G, $H \cap K$ este subgrup normal al lui H şi $HK/K \cong H/H \cap K$.

Demonstraţie. Se consideră morfismul $f : H \to HK/K$ definit prin $f(h) = hK$, se observă că f este surjectiv şi $\text{Ker } f = H \cap K$ iar apoi se aplică teorema fundamentală de izomorfism pentru grupuri.

Teorema 6.7. (A treia teoremă de izomorfism pentru grupuri) Fie G un grup şi H, K subgrupuri normale ale lui G cu $H \leq K$. Atunci K/H este subgrup normal al lui G/H şi $(G/H)/(K/H) \cong G/K$.

Demonstraţie. Se consideră morfismul $f : G/H \to G/K$ definit prin $f(xH) = xK$, se observă că f este surjectiv şi $\text{Ker } f = K/H$ iar apoi se aplică teorema fundamentală de izomorfism pentru grupuri.

Curs VIII
ELEMENTE DE TEORIA GRUPURILOR

§ 7. GRUPURI CICLICE

Am observat anterior că grupurile aditive **Z** şi $\mathbf{Z}_n$, $n \geq 1$, sunt ciclice. Următoarea teoremă arată că acestea sunt singurele tipuri de grupuri ciclice.

Teorema 7.1. (Teorema de structură a grupurilor ciclice) Orice grup ciclic G este izomorf fie cu grupul **Z** al numerelor întregi, fie cu un anumit grup $\mathbf{Z}_n$, $n \geq 1$, de clase de resturi modulo n.

Demonstraţie. Dacă G = <a>, considerăm funcţia φ: $\mathbf{Z} \to G$, $\varphi(n) = a^n$, definită mai înainte. Avem

$$\varphi(m + n) = a^{m+n} = a^m a^n = \varphi(m)\varphi(n)$$

şi deci φ este morfism de grupuri. Mai mult, φ este evident morfism surjectiv, deci Im φ = G. Considerând nucleul lui φ, Ker φ, distingem două cazuri:

1) Ker $\varphi = \{0\}$;

2) Ker $\varphi \neq \{0\}$.

În primul caz, conform teoremei fundamentale de izomorfism, avem

$$\mathbf{Z}/\{0\} \cong \text{Im } \varphi, \text{ adică } \mathbf{Z} \cong G;$$

În cazul al doilea, Ker φ este de forma $n\mathbf{Z}$ cu $n \geq 1$ un număr întreg şi deci

$$\mathbf{Z}/n\mathbf{Z} \cong \text{Im } \varphi, \text{ adică } \mathbf{Z}_n \cong G.$$

Observaţie. Din teorema de mai înainte rezultă că dacă G este un grup ciclic şi *a* un generator al său, atunci:

1) Dacă *a* este de ordin infinit, atunci G este izomorf cu grupul aditiv **Z** al numerelor întregi.

2) Dacă *a* este de ordin n (finit), atunci G este izomorf cu grupul aditiv $\mathbf{Z}_n$ al claselor de resturi modulo n.

Propoziţia 7.2. Orice subgrup şi orice grup factor al unui grup ciclic este ciclic.

Demonstraţie. Dacă G = <a> este un grup ciclic, iar H un subgrup al său, atunci grupul factor G/H este ciclic generat de [a], clasa lui a modulo H, adică G/H = <[a]>.

Să arătăm acum că orice subgrup al unui grup ciclic este ciclic. Într-adevăr, dacă G este izomorf cu **Z**, am arătat că subgrupurile lui **Z** sunt de forma $n\mathbf{Z}$, adică sunt ciclice; deci şi subgrupurile lui G sunt ciclice.

Fie G un grup ciclic finit al cărui generator *a* este de ordin n şi fie H un subgrup al său. Dacă H = {e}, atunci, evident, H este ciclic generat de elementul e. Dacă $H \neq \{e\}$, atunci există $x \in H$, $x \neq e$. Dar cum $x \in G$, avem că $x = a^k$ cu $k \neq 0$. De asemenea, $x^{-1} \in H$, adică $a^{-k} \in H$, deci există $r \geq 1$ astfel încât $a^r \in H$. Mulţimea de numere naturale $M = \{n \mid a^n \in H, n > 0\}$ este nevidă şi cum **N** este bine ordonată, M are un cel mai mic

element m. Vom arăta că $H = \langle a^m \rangle$, adică H este ciclic generat de a^m. Fie $x \in \langle a^m \rangle$; atunci $x = (a^m)^k$, $k \in \mathbf{Z}$ şi cum H este subgrup, iar $a^m \in H$ rezultă că $x \in H$. Reciproc, dacă $y \in H$, atunci $y \in G$, adică $y = a^t$ cu $t \in \mathbf{Z}$. Din teorema împărţirii cu rest pentru numere întregi, $t = mq + r$ cu $q, r \in \mathbf{Z}$ iar $0 \leq r < m$ şi deci $y = a^t = a^{mq+r} = a^{mq} a^r = (a^m)^q a^r$, de unde $a^r = (a^m)^{-q} y$. Deci $a^r \in H$ şi cum m este cel mai mic element al lui M, rezultă $r = 0$ şi deci $t = mq$. Aşadar $y = a^{mq} = (a^m)^q = \langle a^m \rangle$.

Observaţie. Dacă $G = \langle a \rangle$ este un grup ciclic de ordin n, din teorema precedentă rezultă că izomorfismul dintre G şi grupul aditiv $\mathbf{Z}_n$ este dat de funcţia $\varphi : \mathbf{Z}_n \to G$, definită prin $\varphi([k]) = a^k$. Aşadar, având în vedere caracterizarea generatorilor grupului aditiv $\mathbf{Z}_n$ dată în secţiunea 2, avem că elementul a^k este generator al lui G dacă şi numai dacă k este prim cu n.

Fie acum $n \geq 1$ un număr natural şi U_n grupul multiplicativ al rădăcinilor de ordinul n ale unităţii, adică

$$U_n = \{z \in \mathbf{C} \mid z^n = 1\}.$$

Avem că $U_n = \{\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{n-1}\}$, unde

$$\varepsilon_k = \cos(2k\pi/n) + i \sin(2k\pi/n), \quad 0 \leq k \leq n - 1.$$

Din formula lui Moivre avem că $\varepsilon_k = \varepsilon_1^k$ şi deci U_n este grup ciclic de ordinul n, un generator al său fiind ε_1.

Definiţia 7.3. Un generator al grupului U_n se numeşte *rădăcină primitivă de ordinul n a unităţii*.

Conform celor de mai înainte rezultă că ε_k este rădăcină primitivă de ordinul n a unităţii dacă şi numai dacă k este relativ prim cu n.

Exerciţiu. Arătaţi că grupurile $(\mathbf{Q}, +)$, $(\mathbf{R}, +)$ şi $(\mathbf{C}, +)$ nu sunt ciclice.

§ 8. GRUPUL DIEDRAL D_4. GRUPUL CUATERNIONILOR.

Exerciţiu. Daţi un exemplu de grup G care are două subgrupuri H, K cu proprietatea că $H \lhd K$ şi $K \lhd G$, dar H nu este normal în G.

Curs VIII
ELEMENTE DE TEORIA GRUPURILOR

§ 7. GRUPURI DE PERMUTĂRI

Fie A o mulţime. Am observat că mulţimea S(A) a funcţiilor bijective de la A în A formează faţă de compunere un grup numit *grupul permutărilor* mulţimii A.

Propoziţia 7.1. Dacă A şi A' sunt două mulţimi echipotente (sau între care există o funcţie bijectivă), atunci grupurile de permutări S(A) şi S(A') sunt izomorfe.

Demonstraţie. Fie $f : A \to A'$ o funcţie bijectivă. Definim o funcţie $\varphi : S(A) \to S(A')$ care asociază oricărei funcţii bijective $u \in S(A)$ funcţia bijectivă $f \circ u \circ f^{-1} \in S(A')$, deci

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

Să demonstrăm că φ este un izomorfism de grupuri. Într-adevăr,

$$\varphi(u \circ v) = f \circ (u \circ v) \circ f^{-1} = f \circ u \circ (f^{-1} \circ f) \circ u \circ f^{-1} = (f \circ u \circ f^{-1}) \circ (f \circ v \circ f^{-1}) = \varphi(u) \circ \varphi(y),$$

adică φ este morfism de grupuri.

Să arătăm că φ este bijecţie. Dacă $\varphi(u) = \varphi(v)$, atunci

$$f \circ u \circ f^{-1} = f \circ v \circ f^{-1},$$

de unde compunând la stânga cu f^{-1} şi la dreapta cu f, rezultă $u = v$ şi deci φ este injectivă. Dacă $u' \in S(A')$, atunci $f^{-1} \circ u' \circ f \in S(A)$ şi

$$\varphi(f^{-1} \circ u' \circ f) = f \circ (f^{-1} \circ u' \circ f) \circ f^{-1} = (f \circ f^{-1}) \circ u' \circ (f \circ f^{-1}) = u',$$

deci φ este surjectivă.

Observaţie. În particular, dacă A este o mulţime finită cu n elemente, există o bijecţie între A şi mulţimea {1, 2, ... , n}, deci grupurile de permutări S(A) şi S({l, 2, ... , n}) sunt izomorfe. Atunci, pentru a studia grupul de permutări al unei mulţimi cu n elemente este suficient să studiem grupul $\mathbf{S}_n$ al permutărilor mulţimii {1, 2, ... , n}.

Definiţia 7.2. Grupul $\mathbf{S}_n$ se numeşte *grupul simetric de grad n* sau *grupul permutărilor de grad n*. Elementele lui $\mathbf{S}_n$ se numesc *permutări* de n elemente sau permutări de grad n. Elementul neutru e din $\mathbf{S}_n$ se numeşte *permutarea identică* de grad n.

Să considerăm $\sigma \in \mathbf{S}_n$ o permutare de n elemente, adică o funcţie bijectivă de la mulţimea {1, 2, ... , n} în ea însăşi. Punând în evidenţă valoarea σ(i) a funcţiei σ pentru $i \in \{1, 2, \dots, n\}$, vom nota permutarea astfel

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix},$$

unde σ(l), σ(2), ... , σ(n) sunt numerele 1, 2, ... , n, eventual în altă ordine.

Vom arăta că $\mathbf{S}_n$ are n! elemente. Vom demonstra acest fapt folosind teorema lui Lagrange. Notăm $\overline{\mathbf{S}}_{n-1} = \{\sigma \in \mathbf{S}_n \mid \sigma(n) = n\}$, mulţimea permutărilor de n elemente care invariază pe n. Este clar că $\overline{\mathbf{S}}_{n-1}$ este un un subgrup al lui $\mathbf{S}_n$, izomorf cu grupul $\mathbf{S}_{n-1}$ al permutărilor de n – 1 elemente. Izomorfismul este dat de funcţia

$$\theta : \mathbf{S}_{n-1} \to \overline{\mathbf{S}}_{n-1},$$

definită prin

$$\theta(\sigma) = \overline{\sigma}, \text{ unde } \overline{\sigma}(i) = \sigma(i), \text{ pentru } 1 \le i \le n-1 \text{ şi } \overline{\sigma}(n) = n.$$

Deci $|\mathbf{S}_{n-1}| = |\overline{\mathbf{S}}_{n-1}|$.

Vom demonstra prin inducţie după n că avem $|\mathbf{S}_n| = n!$. Pentru n = 1 este evident că $|\mathbf{S}_1| = 1 = 1!$. Să presupunem că $|\mathbf{S}_{n-1}| = (n-1)!$. Conform teoremei lui Lagrange avem că $|\mathbf{S}_n| = [\mathbf{S}_n : \overline{\mathbf{S}}_{n-1}]\,|\overline{\mathbf{S}}_{n-1}|$ adică, $|\mathbf{S}_n| = [\mathbf{S}_n : \overline{\mathbf{S}}_{n-1}]\,(n-1)!$.

Să calculăm indicele $[\mathbf{S}_n : \overline{\mathbf{S}}_{n-1}]$ al subgrupului $\overline{\mathbf{S}}_{n-1}$ în $\mathbf{S}_n$, adică numărul claselor de echivalenţă (la stânga) modulo $\overline{\mathbf{S}}_{n-1}$. Dacă $\sigma, \tau \in \mathbf{S}_n$, atunci $\sigma \equiv_s \tau \pmod{\overline{\mathbf{S}}_{n-1}}$ dacă şi numai dacă $\sigma^{-1}\tau \in \overline{\mathbf{S}}_{n-1}$, adică $\sigma^{-1}\tau(n) = n$ sau echivalent $\tau(n) = \sigma(n)$. Deci există n clase de echivalenţa (la stânga):

$$[\sigma_1], [\sigma_2], \ldots, [\sigma_n],$$

unde $[\sigma_i] = \{\sigma \in \mathbf{S}_n \mid \sigma(n) = i\}$, oricare ar fi i = 1, 2, ... , n. Aşadar, $[\mathbf{S}_n : \overline{\mathbf{S}}_{n-1}] = n$ şi deci

$$|\mathbf{S}_n| = n\,(n-1)! = n!.$$

Definiţia 7.3. Fie $\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$ o permutare de n elemente. O pereche (i, j) se numeşte *inversiune* a permutării σ dacă i < j şi σ(i) > σ (j). Notăm cu inv(σ) numărul inversiunilor permutării σ.

Dacă $\sigma \in \mathbf{S}_n$ este o permutare, definim numărul

$$\varepsilon(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(j) - \sigma(i)}{j - i}$$

care se numeşte *semnul* (*signatura*) permutării σ.

Observăm că orice diferenţă σ(j) – σ(i), cu i < j, de la numărătorul produsului din formula care defineşte ε(σ), se simplifică cu una dintre diferenţele de la numitor, care apare eventual cu semn schimbat dacă (i, j) este o inversiune. Deci ε(σ) este un produs de +1 şi –1, factorul –1 apărând de atâtea ori câte inversiuni are permutarea σ. Deci $\varepsilon(\sigma) = (-1)^{\text{inv}(\sigma)}$.

O permutare σ se numeşte *pară* dacă ε(σ) = l, adică are un număr par de inversiuni şi se numeşte *impară* dacă ε(σ) = –1, adică are un număr impar de inversiuni.

Există permutări pare ca, de exemplu, permutarea identică. Vom arăta că pentru orice n ≥ 2 există şi permutări impare.

Fie n ≥ 2 şi k, l ∈ {1, 2, … , n} cu k ≠ l. Permutarea τ_{kl} definită prin

$$\tau_{kl}(k) = l,\ \tau_{kl}(l) = k,\ \tau_{kl}(i) = i, \text{ dacă } i \ne k \text{ şi } i \ne l,$$

se numeşte *transpoziţie*. Transpoziţia τ_{kl} se mai notează (k l).

Propoziţia 7.4. Dacă $n \geq 2$ este un număr natural, atunci orice transpoziţie din $\mathbf{S}_n$ este permutare impară.

Demonstraţie. Fie transpoziţia (k l) şi să presupunem că $k < l$. Atunci

$$(k\ l) = \begin{pmatrix} 1 & 2 \ldots k-1 & k \ldots l-1 & l & \ldots n \\ 1 & 2 \ldots k-1 & l \ldots l-1 & k & \ldots n \end{pmatrix}$$

şi numărul de inversiuni este $(l - k) + (l - k - 1) = 2(l - k) - l$. Deci $\varepsilon((k, l)) = -1$.

Propoziţia 7.5. Dacă $n \geq 2$ este un număr natural, funcţia

$$\varepsilon : \mathbf{S}_n \to \{-1, 1\},$$

de la grupul permutărilor $\mathbf{S}_n$ la grupul multiplicativ $\{-1, 1\}$, este un morfism surjectiv de grupuri.

Demonstraţie. Fie $\sigma, \tau \in \mathbf{S}_n$. Deoarece $\tau(1), \tau(2), \ldots, \tau(n)$ sunt numerele 1, 2, … , n, eventual într-o altă ordine şi cum în produsul care-l dă pe $\varepsilon(\sigma)$ diferenţele de la numitor se pot face şi în altă ordine decât cea din definiţie, rezultă că avem

$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)}.$$

Atunci:

$$\varepsilon(\sigma \circ \tau) = \prod_{1 \leq i < j \leq n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{j - i} = \prod_{1 \leq i < j \leq n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} \frac{\tau(j) - \tau(i)}{j - i} =$$

$$= \prod_{1 \leq i < j \leq n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} \prod_{1 \leq i < j \leq n} \frac{\tau(j) - \tau(i)}{j - i} = \varepsilon(\sigma)\, \varepsilon(\tau),$$

deci ε este un morfism de grupuri. Deoarece orice transpoziţie este impară, iar permutarea identică este pară, rezultă că ε este surjectiv.

Definiţia 7.6. Să notăm cu $A_n = \{\sigma \in \mathbf{S}_n \mid \varepsilon(\sigma) = 1\}$, mulţimea permutărilor pare din $\mathbf{S}_n$. Este clar că A_n este un subgrup (normal) al lui $\mathbf{S}_n$, deci la rândul său este grup, numit *grupul altern de grad n*.

Evident $A_n = \operatorname{Ker} \varepsilon$ şi din teorema fundamentală de izomorfism pentru grupuri rezultă că grupul factor $\mathbf{S}_n/A_n$ este izomorf cu grupul multiplicativ $\{-1, 1\}$, deci indicele $[\mathbf{S}_n : A_n]$ este 2.

Corolarul 7.7. A_n are n!/2 elemente.

Definiţia 7.8. O permutare $\sigma \in \mathbf{S}_n$ se numeşte *ciclu de lungime m*, $2 \le m \le n$, dacă există m numere $i_1, i_2, \dots, i_m \in \{1, 2, \dots, n\}$ astfel încât să avem:

1° oricare ar fi $i \notin \{i_1, i_2, \dots, i_m\}$, $\sigma(i) = i$,

2° $\sigma(i_1) = i_2$, $\sigma(i_2) = i_3$, ... , $\sigma(i_{m-1}) = i_m$, $\sigma(i_m) = i_1$.

Acest ciclu

$$\sigma = \begin{pmatrix} 1 & \dots & i_1 & \dots & i_2 & \dots & i_3 & \dots & i_{m-1} & \dots & i_m & \dots & n \\ 1 & \dots & i_2 & \dots & i_3 & \dots & i_4 & \dots & i_m & \dots & i_1 & \dots & n \end{pmatrix}$$

îl vom nota $\sigma = (i_1\ i_2\ \dots\ i_m)$.

Observăm că la orice sistem de m numere $i_1, i_2, \dots, i_m$ cuprinse între 1 şi n putem să asociem cel puţin un ciclu de lungime m şi, mai mult,

$$(i_1\ i_2 \dots i_m) = (i_2\ i_3\ \dots\ i_m\ i_1) = \dots = (i_m\ i_1\ \dots\ i_{m-1}).$$

Aşadar, numărul ciclilor de lungime m, $2 \le m \le n$, este $C_n^m\,(m-1)!$. De exemplu, orice transpoziţie este un ciclu de lungime 2. Prin urmare, rezultă că numărul transpoziţiilor din grupul $\mathbf{S}_n$ este C_n^2.

Propoziţia 7.9. Dacă $\sigma = (i_1\ i_2 \dots i_m) \in \mathbf{S}_n$ este un ciclu de lungime m, atunci

1) $\sigma^{-1} = (i_m\ i_{m-1}\ \dots\ i_1)$,

2) $\text{ord}(\sigma) = m$.

Demonstraţie. 1) Se verifică imediat.

2) Din definiţia ciclului obţinem că $\sigma^k(i_1) = i_{k+1}$ pentru orice $1 \le k \le m-1$ şi $\sigma^m(i_1) = i_1$. Deoarece $i_1 \ne i_k$, pentru orice $2 \le k \le m$, avem că $\sigma^k \ne e$, pentru orice $1 \le k \le m-1$. Să arătăm că $\sigma^m = e$. Dacă $i \notin \{i_1, i_2, \dots, i_m\}$, atunci $\sigma(i) = i$ şi deci $\sigma^m(i) = i$. Dacă $i = i_1$ am observat că $\sigma^m(i_1) = i_1$, iar dacă $i = i_{k+1}$, $1 \le k \le m-1$, atunci $\sigma^m(i) = \sigma^m(\sigma^k(i_1)) = \sigma^k(\sigma^m(i_1)) = \sigma^k(i_1) = i$. Deci oricare ar fi i, $1 \le i \le n$, avem că $\sigma^m(i) = i$, adică $\sigma^m = e$. Am demonstrat astfel că $\text{ord}(\sigma) = m$.

Propoziţia 7.10. Fie $\sigma, \tau \in \mathbf{S}_n$, iar A, B două submulţimi nevide şi disjuncte ale mulţimii $\{1, 2, \dots, n\}$ astfel încât:

1. Dacă $s \notin A$, atunci $\sigma(s) = s$, iar dacă $s \in A$, atunci $\sigma(s) \in A$;

2. Dacă $t \notin B$, atunci $\tau(t) = t$, iar dacă $t \in B$, atunci $\tau(t) \in B$.

Atunci $\sigma\tau = \tau\sigma$ şi $\text{ord}(\sigma\tau) = \text{c.m.m.m.c.}(\text{ord}(\sigma), \text{ord}(\tau))$.

Demonstraţie. Fie $r \in \{1, 2, \dots, n\}$ un element oarecare. Dacă $r \notin A \cup B$ atunci $\sigma(r) = r$ şi $\tau(r) = r$ şi deci $(\sigma\tau)(r) = (\tau\sigma)(r) = r$. Presupunem că $r \in A \cup B$. Dacă $r \notin A$, atunci $r \in B$ şi deci $\tau(r) = r$. Avem $(\sigma\tau)(r) = \sigma(\tau(r)) = \sigma(r)$, iar $(\tau\sigma)(r) = \tau(\sigma(r))$. Dar cum $\sigma(r) \in A$, atunci $\sigma(r) \notin B$ şi deci $\sigma(\tau(r)) = \sigma(r)$. Rezultă că şi în acest caz $(\sigma\tau)(r) = (\tau\sigma)(r)$. Analog, dacă $r \in B$, rezultă $(\sigma\tau)(r) = (\tau\sigma)(r)$. Deci $(\sigma\tau)(r) = (\tau\sigma)(r)$, oricare ar fi $r \in \{1, 2, \dots, n\}$, adică $\sigma\tau = \tau\sigma$.

Fie acum $\text{ord}(\sigma) = k$, $\text{ord}(\tau) = l$, $\text{ord}(\sigma\tau) = m$ şi să notăm $u = \text{c.m.m.m.c.}(k, l)$. Avem $(\sigma\tau)^m = e$ şi cum $\sigma\tau = \tau\sigma$, rezultă $\sigma^m\tau^m = e$ sau $\sigma^m = \tau^{-m}$. Vom arăta că $\sigma^m = e =$

τ^m. Într-adevăr, dacă $\sigma^m \neq e$, atunci există $r \in \{1, 2, \dots, n\}$ astfel încât $\sigma^m(r) \neq r$ şi deci neapărat $r \in A$. Din $\sigma^m(r) = \tau^{-m}(r)$, avem $\tau^{-m}(r) \neq r$, deci $\tau^m(r) \neq r$ şi deci neapărat $r \in B$. Aşadar $r \in A \cap B$, contradicţie cu faptul că $A \cap B = \emptyset$. Am obţinut astfel că $\sigma^m = e = \tau^m$.

Prin urmare, $k \mid m$ şi $l \mid m$ şi deci $u \mid m$. Fie $k', l' \in \mathbf{N}$ astfel încât $u = kk'$ şi $u = ll'$. Deci $(\sigma\tau)^u = \sigma^u \tau^u = (\sigma^l)^{l'} (\tau^k)^{k'} = e$, de unde obţinem că $m \mid u$. Din $u \mid m$ şi $m \mid u$ rezultă că $m = u$ şi propoziţia este demonstrată.

Corolarul 7.11. Fie $\sigma \in \mathbf{S}_n$, $n \geq 2$, o permutare astfel încât $\sigma = \tau_1 \tau_2 \dots \tau_t$, unde $\tau_1, \tau_2, \dots, \tau_t$ sunt cicli disjuncţi. Atunci $ord(\sigma) = c.m.m.m.c.(ord(\tau_1), ord(\tau_2), \dots, ord(\tau_t))$.

Demonstraţie. Rezultă imediat prin generalizarea punctului 2 al propoziţiei de mai sus.

Definiţia 7.12. Ciclurile $\sigma = (i_1\ i_2\ \dots\ i_m)$ şi $\tau = (j_1\ j_2\ \dots\ j_k)$ se numesc *disjuncte* dacă

$$\{i_1, i_2, \dots, i_m\} \cap \{j_1, j_2, \dots, j_k\} = \emptyset.$$

Propoziţia precedentă aplicată în cazul ciclurilor disjuncte σ şi τ ne spune că

$$\sigma\tau = \tau\sigma \text{ şi } ord(\sigma\tau) = c.m.m.m.c.(m, k).$$

Teorema 7.13. Orice permutare $\sigma \in \mathbf{S}_n$, $\sigma \neq e$, se descompune ca un produs finit de cicli disjuncţi. Mai mult, această descompunere este unică, abstracţie făcând de ordinea factorilor.

Demonstraţie. Fie n_σ numărul de elemente ale mulţimii $\{1, 2, \dots, n\}$ permutate efectiv de către σ, adică

$$n_\sigma = |\{i \mid \sigma(i) \neq i\}|.$$

Deoarece $\sigma \neq e$, există i astfel încât $\sigma(i) \neq i$ şi cum σ este injectivă avem $\sigma(\sigma(i)) \neq \sigma(i)$ şi deci $n_\sigma \geq 2$. Vom face demonstraţia prin inducţie după acest număr.

Dacă $\sigma \in \mathbf{S}_n$, astfel încât $n_\sigma = 2$, atunci există $i \neq j$, astfel încât $\sigma(i) = j$, $\sigma(j) = i$ şi $\sigma(k) = k$ oricare ar fi $k \neq i$ şi $k \neq j$. În acest caz σ este transpoziţia $(i\ j)$.

Presupunem teorema adevărată pentru toate permutările τ care permută efectiv mai puţin de n_σ elemente, adică $n_\tau < n_\sigma$, şi să arătăm că ea este adevărată şi pentru σ.

Dacă $i_1 \in \{1, 2, \dots, n\}$ astfel încât $\sigma(i_1) \neq i_1$, notăm $i_2 = \sigma(i_1)$, $\dots$, $i_{k+1} = \sigma(i_k)$, $\dots$. Este clar că $i_{k+1} = \sigma^k(i_1)$, oricare ar fi $k \geq 1$. Dacă $t = ord(\sigma)$, atunci $\sigma^t = e$ şi deci $\sigma^t(i_1) = i_1$, adică $i_{t+1} = i_1$. Din proprietatea de bună ordonare a mulţimii $\mathbf{N}$ a numerelor naturale, există un cel mai mic număr natural nenul m cu proprietatea că $i_{m+1} = i_1$.

Numerele $i_1, i_2, \dots, i_m$ sunt distincte. Într-adevăr, dacă $i_r = i_s$, cu $r \neq s$, şi $1 \leq r, s \leq m$, atunci $\sigma^{r-1}(i_1) = \sigma^{s-1}(i_1)$. Să presupunem că $r > s$ şi fie $p = r - s$. Atunci $\sigma^{r-s}(i_1) = i_1$, adică $\sigma^p(i_1) = i_1$ sau $i_{p+1} = i_1$. Dar egalitatea $i_{p+1} = i_1$, unde $0 < p < m$, este în contradicţie cu alegerea numărului m.

Fie acum ciclul $\tau = (i_1\ i_2\ \dots\ i_m)$ şi să considerăm permutarea $\sigma' = \tau^{-1}\sigma$. Dacă $\sigma(i) = i$, atunci $i \notin \{i_1, i_2, \dots, i_m\}$ şi deci $\tau^{-1}(i) = i$, de unde $\sigma'(i) = i$. Mai mult, dacă $i_k \in \{i_1, \dots, i_m\}$ este clar că $\sigma'(i_k) = (\tau^{-1}\sigma)(i_k) = \tau^{-1}(\sigma(i_k)) = i_k$ şi deci, în plus, elementele $i_1, i_2, \dots,$

i_m rămân neschimbate dacă le aplicăm permutarea σ'. Aşadar $n_{\sigma'} < n_\sigma$ şi conform ipotezei de inducţie există ciclurile disjuncte $\tau_2, \tau_3, \ldots, \tau_t$ astfel încât $\sigma' = \tau_2 \tau_3 \ldots \tau_t$ sau $\tau^{-1}\sigma = \tau_2 \tau_3 \ldots \tau_t$, de unde $\sigma = \tau \tau_2 \tau_3 \ldots \tau_t$. Mai mult, din demonstraţie rezultă că ciclul τ este disjunct de fiecare din ciclurile disjuncte $\tau_2, \tau_3, \ldots, \tau_t$. Notând $\tau_1 = \tau$ obţinem descompunerea $\sigma = \tau_1 \tau_2 \tau_3 \ldots \tau_t$ în produs de cicli disjuncţi. Tot din demonstraţie se observă că această descompunere este unică, abstracţie făcând de ordinea factorilor.

Propoziţia 7.14. Orice ciclu din $\mathbf{S}_n$ este un produs de transpoziţii.

Demonstraţie. Dacă $\sigma = (i_1\ i_2 \ldots i_m)$ este un ciclu de lungime m, atunci prin calcul direct rezultă

$$\sigma = (i_1 i_m)(i_1\ i_{m-1}) \ldots (i_1\ i_2) = (i_1\ i_2)(i_2\ i_3) \ldots (i_{m-1}\ i_m).$$

Corolarul 7.15. Orice permutare $\sigma \in \mathbf{S}_n$, $n \geq 2$, este produs de transpoziţii.

Demonstraţie. Dacă σ = e, atunci σ = e = (l, 2)(1, 2). Dacă $\sigma \neq e$, afirmaţia rezultă din teorema şi propoziţia de mai sus.

Observaţie. Din cele de mai sus se observă că descompunerea unei permutări în produs de transpoziţii nu este unică, în schimb paritatea numărului de transpoziţii care apar în orice descompunere a unei permutări este aceeaşi. Într-adevăr, fie $\sigma = \tau_1 \tau_2 \ldots \tau_t = \sigma_1 \sigma_2 \ldots \sigma_s$, unde $\tau_1, \tau_2, \ldots, \tau_t$ şi $\sigma_1, \sigma_2, \ldots, \sigma_s$ sunt transpoziţii. Ţinând cont că semnul unei transpoziţii este –1, obţinem $\varepsilon(\sigma) = (-1)^t = (-1)^s$, de unde rezultă că r şi s sunt în acelaşi timp pare sau impare.

Aplicaţie. Fie permutarea $\sigma \in \mathbf{S}_{10}$, unde

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 5 & 1 & 4 & 7 & 10 & 8 & 2 & 6 & 9 \end{pmatrix}.$$

Să scriem permutarea σ ca produs de cicli disjuncţi şi ca produs de transpoziţii. De asemenea, să determinăm ordinul permutării σ.

Considerăm numărul 1 care este permutat efectiv de σ, deoarece σ(l) = 3. Cum σ(3) = l obţinem $\tau_1 = (1\ 3)$. Considerăm acum următorul număr care este permutat efectiv de σ şi care nu aparţine mulţimii {1, 3}. Acesta este 2. Cum σ(2) = 5, σ(5) = 7, σ(7) = 8, σ(8) = 2 obţinem ciclul $\tau_2 = (2\ 5\ 7\ 8)$. Fie acum numărul 6 care este permutat efectiv de σ. Avem σ(6) =10, σ(10) = 9, σ(9) = 6 şi astfel obţinem ciclul (6 10 9). Deci σ se scrie ca produs de cicluri disjuncte astfel: σ = (l 3) (2 5 7 8) (6 10 9).

Din ultima propoziţie a acestui paragraf rezultă că σ se poate scrie ca produs de transpoziţii astfel: σ = (1 3) (2 8) (2 7) (2 5) (6 9) (6 10).

În final avem ord(σ) = c.m.m.m.c.(2, 4, 3) = 12.

INELE

1. Generalităţi

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

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

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

Exerciţiul 1.3. (i) Să se determine numărul structurilor neizomorfe de inel care pot fi definite pe grupul $(\mathbb{Z}_p,+)$, unde p este un număr prim.
(ii) Să se determine numărul structurilor de inel unitar ce pot fi definite pe grupul $(\mathbb{Z}_n,+)$ şi să se arate că acestea sunt izomorfe.

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

Exemplul 1.5. (i) $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ sunt inele comutative şi unitare.
(ii) $(2\mathbb{Z},+,\cdot)$ este inel comutativ, dar nu este unitar.
(iii) $(\mathbb{Z}_n,+,\cdot)$ este inel comutativ şi unitar.
(iv) Fie G grup comutativ. Atunci $(\mathrm{End}(G),+,\circ)$ este inel unitar şi se numeşte *inelul endomorfismelor lui G*.
(v) Fie R un inel (unitar) şi X o mulţime nevidă. Definim pe mulţimea R^X a funcţiilor $f : X \to R$ o structură de inel (unitar) astfel: dacă $f,g \in R^X$, atunci

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

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

pentru orice $x \in X$. Acesta se numeşte *inelul funcţiilor definite pe X cu valori în R*. Elementul nul al acestui inel este funcţia $\mathbf{0} : X \to R$ definită prin $\mathbf{0}(x) = 0$ pentru orice $x \in X$ (elementul unitate este funcţia $\mathbf{1} : X \to R$ definită prin $\mathbf{1}(x) = 1$ pentru

orice $x \in X$).
(vi) Fie R un inel (unitar). Atunci $(M_n(R), +, \cdot)$ este inel (unitar) şi se numeşte *inelul matricelor pătratice de ordin n peste R*. În cazul în care R este unitar, elementul unitate al lui $M_n(R)$ se notează cu I_n şi este matricea care are 1 pe diagonala principală şi 0 în rest. În general, $M_n(R)$ nu este inel comutativ.
(vii) Fie R_1, R_2 inele şi $R = R_1 \times R_2$. Atunci $(R, +, \cdot)$ este inel, unde

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

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

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

Exerciţiul 1.6. Să se arate că $(\mathbb{R}^{\mathbb{R}}, +, \circ)$ nu este inel.

Exerciţiul 1.7. Fie R un inel şi $n \geq 2$. Să se arate că inelul de matrice $M_n(R)$ este comutativ dacă şi numai dacă $ab = 0$ pentru orice $a, b \in R$.

Avem următoarele reguli de calcul într-un inel:

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

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

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

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

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

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

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

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

Exemplul 1.14. (i) $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ sunt domenii de integritate.
(ii) Un element $\widehat{a}\in\mathbb{Z}_n$ este divizor al lui zero dacă şi numai dacă $(a,n)\neq 1$. Aşadar $\mathbb{Z}_n$ este domeniu de integritate dacă şi numai dacă n este număr prim.
(iii) Dacă R este un inel unitar nenul şi $n\geq 2$, atunci $(M_n(R),+,\cdot)$ nu este inel integru. De exemplu, matricea $\begin{pmatrix}1&0\\1&0\end{pmatrix}$ este divizor al lui zero în $M_2(R)$.
(iv) Dacă R_1,R_2 sunt inele nenule, atunci $R_1\times R_2$ nu este inel integru. De exemplu, perechea $(a_1,0)$, unde $a_1\in R_1$, $a_1\neq 0$, este divizor al lui zero.
(v) Fie M o mulţime cu $|M|\geq 2$. Atunci inelul $(\mathcal{P}(M),\Delta,\cap)$ nu este integru.

Exerciţiul 1.15. (i) Arătaţi că $f\in\mathbb{R}^{\mathbb{R}}$ este divizor al lui zero dacă şi numai dacă există $x_0\in\mathbb{R}$ astfel încât $f(x_0)=0$.
(ii) Fie $\mathcal{C}(\mathbb{R})=\{f:\mathbb{R}\to\mathbb{R}\mid f \text{ este continuă}\}$ cu operaţiile de adunare şi înmulţire a funcţiilor. Arătaţi că $f\in\mathcal{C}(\mathbb{R})$ este divizor al lui zero dacă şi numai dacă există $(a,b)\subset\mathbb{R}$ astfel încât $f(x)=0$ pentru orice $x\in(a,b)$.

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

Exerciţiul 1.17. Arătaţi că în inelul $M_n(\mathbb{R})$ orice element inversabil la stânga (dreapta) este inversabil la dreapta (stânga).

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

Remarca 1.18. (i) $a\in U(R)$ dacă şi numai dacă există $a'\in R$ astfel încât $aa'=a'a=1$.
(ii) $U(R)$ este grup în raport cu înmulţirea şi se numeşte *grupul unităţilor lui R.*
(iii) Elementele inversabile nu sunt divizori ai lui zero. (În schimb există elemente inversabile la dreapta şi care sunt divizori ai lui zero la stânga.)

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

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

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

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

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

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

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

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

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

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

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

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

Exerciţiul 1.28. (i) Se consideră numărul natural $n \geq 2$ care are r factori primi distincţi în descompunerea sa. Să se arate că numărul idempotenţilor lui $\mathbb{Z}_n$ este 2^r.
(ii) Să se determine idempotenţii inelului $\mathbb{Z}_{36}$.

Exerciţiul 1.29. Fie $R = M_2(\mathbb{Z}_2)$.
(i) Să se determine numărul elementelor lui R;
(ii) Să se afle numărul divizorilor lui zero ai lui R;
(iii) Aflaţi câte elemente nilpotente are R;
(iv) Aflaţi câte elemente idempotente are R.

2. Subinele. Ideale

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

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

Exemplul 2.3. (i) Dacă R este un inel, atunci $\{0\}$ şi R sunt subinele.
(ii) $\mathbb{Z} \subset \mathbb{Q}$ este subinel unitar.
(iii) $2\mathbb{Z} \subset \mathbb{Z}$ este subinel, dar nu este unitar.
(iv) $\widehat{5}\,\mathbb{Z}_{10} \subset \mathbb{Z}_{10}$ este subinel, dar nu este subinel unitar. Să remarcăm că $\widehat{5}\,\mathbb{Z}_{10}$ are totuşi element unitate, pe $\widehat{5}$. (Mai general, dacă R este inel comutativ unitar şi $e \in R$ un idempotent netrivial, atunci $Re \subset R$ este subinel, $1 \notin Re$, dar Re are element unitate pe e.)
(v) $\mathcal{C}(\mathbb{R}) \subset \mathbb{R}^{\mathbb{R}}$ este subinel unitar.

Definiţia 2.4. *Fie R un inel şi $I \subseteq R$ o submulţime nevidă. Atunci I se numeşte* ideal la stânga (dreapta) *al lui R dacă sunt satisfăcute următoarele condiţii:*
(i) $x, y \in I \implies x - y \in I$,
(ii) $a \in R$, $x \in I \implies ax \in I$ *(respectiv,* $xa \in I$*),*
pentru orice $a \in R$ şi $x, y \in I$.
Un ideal la stânga şi la dreapta al lui R se numeşte ideal bilateral *al lui R.*

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

Remarca 2.5. (i) Fie R un inel comutativ şi $I \subseteq R$ o submulţime nevidă. Atunci I este ideal la stânga al lui R dacă şi numai dacă I este ideal la dreapta al lui R dacă şi numai dacă I este ideal bilateral al lui R. În acest caz, I se numeşte *ideal* al lui R.
(ii) Evident, orice ideal este subinel, dar nu şi reciproc: $\mathbb{Z} \subset \mathbb{Q}$ este subinel, dar nu este ideal.
(iii) Fie R inel unitar şi $I \subseteq R$ un ideal la stânga (la dreapta, bilateral). Atunci $I = R$ dacă şi numai dacă I conţine un element inversabil.

Exemplul 2.6. (i) Dacă R este un inel, atunci $\{0\}$ şi R sunt ideale bilaterale.
(ii) Idealele lui $\mathbb{Z}$ sunt $n\mathbb{Z}$, $n \in \mathbb{N}$.
(iii) Idealele lui $\mathbb{Z}_n$ sunt $\widehat{d}\mathbb{Z}_n$, $d \mid n$.
(iv) Idealele lui $\mathbb{Q}$ sunt $\{0\}$ şi $\mathbb{Q}$. (Analog pentru $\mathbb{R}$.)
(v) Fie $R = M_2(\mathbb{Q})$ şi

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

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

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

Exerciţiul 2.7. Fie R_1, R_2 inele unitare şi $R = R_1 \times R_2$. Să se arate că idealele la stânga (la dreapta, bilaterale) ale lui R sunt de forma $I = I_1 \times I_2$, unde I_1, I_2 sunt ideale la stânga (la dreapta, bilaterale) în R_1, R_2, respectiv.

Exerciţiul 2.8. Fie R un inel unitar.
(i) Să se arate că idealele bilaterale ale lui $M_2(R)$ sunt de forma $M_2(I)$, unde I este ideal bilateral al lui R.
(ii) Daţi exemplu de ideal la stânga al lui $M_2(R)$ care nu este de forma $M_2(J)$, cu J ideal la stânga al lui R.

Lema 2.9. *Fie R un inel şi $I_\alpha \leq_s R$, $\alpha \in A$ o familie de ideale la stânga ale lui R. Atunci $\bigcap_{\alpha \in A} I_\alpha \leq_s R$. (Analog pentru ideale la dreapta, respectiv bilaterale.)*

Definiţia 2.10. *Fie R un inel unitar şi $X \subseteq R$ o submulţime. Notăm cu $(X)_s$ intersecţia tuturor idealelor la stânga care conţin pe X. Acesta este un ideal la stânga al lui R şi se numeşte* idealul la stânga generat de X.

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

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

Definiţia 2.12. *Fie R un inel unitar şi $X \subseteq R$ o submulţime. Elementele lui X se numesc* generatori *pentru $(X)_s$.*
Dacă $I \leq_s R$ şi există $X \subseteq I$ o submulţime finită astfel încât $I = (X)_s$, atunci idealul I se numeşte finit generat. *Dacă X are un singur element, atunci idealul I se numeşte* principal.

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

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

Propoziţia 2.14. *Fie R un inel unitar şi $X \subseteq R$ o submulţime. Atunci*

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

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

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

În particular,

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

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

3. Morfisme de inele

Definiţia 3.1. *Fie R, R' inele şi $f : R \to R'$ o funcţie. Aceasta se numeşte* morfism de inele *dacă*

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

pentru orice $x, y \in R$.
Dacă R, R' sunt inele unitare şi $f(1) = 1'$, atunci f se numeşte morfism unitar.

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

Exemplul 3.3. (i) Funcţia $f : R \to R'$ definită prin $f(x) = 0'$ pentru orice $x \in R$ este morfism de inele şi se numeşte *morfismul nul.*
(ii) Incluziunea $i : \mathbb{Z} \to \mathbb{Q}$ definită prin $i(x) = x$ pentru orice $x \in \mathbb{Z}$ este morfism unitar şi injectiv de inele.
(iii) Surjecţia canonică $p : \mathbb{Z} \to \mathbb{Z}_n$ definită prin $p(x) = \widehat{x}$ pentru orice $x \in \mathbb{Z}$ este

morfism unitar şi surjectiv de inele.
(iv) Dacă R este un inel şi $f : R \to M_n(R)$ se defineşte prin

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

atunci f este morfism injectiv de inele. Dacă, în plus, R este unitar, atunci f este de asemenea morfism unitar.
(v) Fie R un inel (unitar) şi X o mulţime nevidă. Pentru orice $x \in X$ definim un morfism de inele (unitare) $\varphi_x : R^X \to R$ prin $\varphi_x(f) = f(x)$. Acesta se numeşte *morfismul de evaluare în* x.

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

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

Notaţie: $R \simeq R'$.

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

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

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

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

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

Exerciţiul 3.11. Fie $m, n \geq 2$.
(i) Arătaţi că există un morfism de inele unitare $\mathbb{Z}_m \to \mathbb{Z}_n$ dacă şi numai dacă $n \mid m$.
(ii) Arătaţi că un morfism de inele $f : \mathbb{Z}_m \to \mathbb{Z}_n$ este unic determinat de condiţiile: $mf(1) = 0$ şi $f(1) = f(1)^2$.
(iii) Să se determine toate morfismele de inele de la $\mathbb{Z}_{12}$ la $\mathbb{Z}_{28}$.

Propoziţia 3.12. *Fie $f : R \to R'$ un morfism de inele.*
(i) Dacă $S \subseteq R$ este subinel, atunci $f(S) \subseteq R'$ este subinel.
Dacă $S' \subseteq R'$ este subinel, atunci $f^{-1}(S') \subseteq R$ este subinel.
(ii) Dacă $I \leq_s R$ şi f este surjectiv, *atunci $f(I) \leq_s R'$.*
Dacă $I' \leq_s R'$, atunci $f^{-1}(I') \leq_s R$.
(Analog pentru ideale la dreapta, respectiv bilaterale.)

Exemplul 3.13. Imaginea unui ideal printr-un morfism nu este neapărat un ideal. De exemplu, imaginea lui $2\mathbb{Z}$ prin morfismul incluziune $i : \mathbb{Z} \to \mathbb{Q}$ nu este ideal.

Definiţia 3.14. *Fie $f : R \to R'$ un morfism de inele. Atunci* $\operatorname{Im} f \subseteq R'$ *este un subinel numit* imaginea lui f, *iar* $\operatorname{Ker} f = f^{-1}(0)$ *este un ideal bilateral numit* nucleul lui f.

Din cele demonstrate în capitolul despre grupuri ştim că f este morfism injectiv dacă şi numai dacă $\operatorname{Ker} f = \{0\}$.

Teorema 3.15. (Teorema de corespondenţă pentru ideale) *Fie $f : R \to R'$ un morfism* surjectiv *de inele. Există o corespondenţă bijectivă între mulţimea idealelor la stânga (la dreapta, bilaterale) ale lui R care conţin pe* $\operatorname{Ker} f$ *şi mulţimea tuturor idealelor la stânga (la dreapta, bilaterale) ale lui R', dată prin $I \mapsto f(I)$.*

4. Inele factor

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

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

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

Definiţia 4.1. *Inelul R/I se numeşte* inelul factor *al lui R în raport cu idealul bilateral I. Funcţia $p : R \to R/I$ definită prin $p(x) = \widehat{x}$ este un morfism surjectiv de inele şi se numeşte* proiecţia (surjecţia) canonică *a lui R pe R/I.*

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

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

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

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

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

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

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

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

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

Exerciţiul 4.8. Fie R_1, R_2 inele unitare, $R = R_1 \times R_2$ şi $I = I_1 \times I_2$, unde I_1, I_2 sunt ideale bilaterale în R_1, respectiv R_2. Să se arate că inelele R/I şi $R_1/I_1 \times R_2/I_2$ sunt izomorfe.

Exerciţiul 4.9. Fie R un inel unitar şi I ideal bilateral al lui R. Să se arate că inelele $M_2(R)/M_2(I)$ şi $M_2(R/I)$ sunt izomorfe.

5. Teorema Chineză a Resturilor pentru ideale

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

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

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

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

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

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

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

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

CORPURI

1. Generalităţi

Definiţia 1.1. *Un inel unitar K cu $1 \neq 0$ se numeşte* corp *dacă orice element nenul al său este inversabil.*
Dacă înmulţirea pe K este comutativă, atunci K se numeşte corp comutativ.

Notaţie: $K^\times = K \setminus \{0\}$.

Exemplul 1.2. (i) $(\mathbb{Q}, +, \cdot)$ şi $(\mathbb{R}, +, \cdot)$ sunt corpuri comutative.
(ii) $\mathbb{Z}_n$ este corp dacă şi numai dacă n este număr prim.
(iii) $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ este corp comutativ.

Remarca 1.3. Orice corp este inel integru.

Exerciţiul 1.4. Arătaţi că orice inel unitar ($1 \neq 0$) integru şi finit este corp.

Propoziţia 1.5. *Fie R un inel unitar cu $1 \neq 0$. Atunci R este corp dacă şi numai dacă $\{0\}$ şi R sunt singurele ideale la stânga (la dreapta) ale lui R.*

Proof. "$\Rightarrow$" Fie I un ideal la stânga al lui R. Presupunem că $I \neq \{0\}$. Atunci există $a \in I$, $a \neq 0$. Deoarece R este corp, elementul a este inversabil şi cum $a^{-1}a \in I$ rezultă $1 \in I$. De aici se obţine că $r = r1 \in I$ pentru orice $r \in R$, deci $I = R$.
"$\Leftarrow$" Fie $a \in R$, $a \neq 0$. Idealul la stânga Ra este nenul, deoarece $a = 1a \in Ra$. Din ipoteză $Ra = R$, deci există $a' \in R$ astfel încât $a'a = 1$. Evident $a' \neq 0$ şi un raţionament analog ne arată că există $a'' \in R$ cu proprietatea că $a''a' = 1$. Înmulţind la dreapta cu a obţinem $a''a'a = a$, adică $a'' = a$. În concluzie, $aa' = 1$, deci a este inversabil. □

Remarca 1.6. Deşi în orice corp $\{0\}$ şi corpul însuşi sunt singurele ideale bilaterale, reciproc este fals: în inelul $R = M_2(\mathbb{Q})$ singurele ideale bilaterale sunt $\{0\}$ şi R şi acesta nu este corp. (Un inel cu proprietatea că nu are ideale bilaterale netriviale se numeşte *inel simplu*).

Definiţia 1.7. *Fie K un corp şi $K' \subseteq K$ o submulţime nevidă. Atunci K' se numeşte* subcorp *al lui K dacă $(K', +, \cdot)$ este corp. În acest caz se mai spune că K este o* extindere *a lui K'.*

Propoziţia 1.8. *Fie K un corp şi $K' \subseteq K$ o submulţime nevidă. Atunci K' este subcorp al lui K dacă şi numai dacă sunt satisfăcute următoarele condiţii:*
(i) $x, y \in K' \implies x - y \in K'$,
(ii) $x, y \in K', x \neq 0 \implies x^{-1}y \in K'$,
pentru orice $x, y \in K'$.

Să observăm că din (ii) rezultă imediat că $1 \in K'$.

Exemplul 1.9. (i) Orice corp este un subcorp al său.
(ii) $\mathbb{Q} \subseteq \mathbb{R}$ este subcorp.
(iii) $\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$ este subcorp.

Remarca 1.10. Corpurile $\mathbb{Z}/p\mathbb{Z}$ şi $\mathbb{Q}$ nu au subcorpuri proprii.

Definiţia 1.11. *Fie K, K' corpuri şi $f : K \to K'$ o funcţie. Aceasta se numeşte* morfism de corpuri *dacă*

$$f(x+y) = f(x) + f(y),$$
$$f(xy) = f(x)f(y),$$
$$f(1) = 1',$$

pentru orice $x, y \in K$.

Remarca 1.12. (i) În definiţia de mai sus f este morfism de corpuri dacă este morfism unitar de inele.
(ii) Dacă f este morfism de corpuri, atunci $f(x^{-1}) = f(x)^{-1}$ pentru orice $x \in K^\times$.

Propoziţia 1.13. *Orice morfism de corpuri este injectiv.*

Proof. Fie $f : K \to K'$ un morfism de corpuri. Deoarece $\operatorname{Ker} f$ este ideal bilateral al lui K rezultă că $\operatorname{Ker} f = \{0\}$, deci f este morfism injectiv. □

Lema 1.14. *Fie K un corp şi $K_\alpha \subseteq K$, $\alpha \in A$ o familie de subcorpuri ale lui K. Atunci $\bigcap_{\alpha \in A} K_\alpha$ este un subcorp al lui K.*

Dacă considerăm intersecţia tuturor subcorpurilor unui corp dat obţinem un subcorp care nu are subcorpuri proprii.

Definiţia 1.15. *Un corp care nu are subcorpuri proprii se numeşte* corp prim.

Deci orice corp conţine ca subcorp un corp prim. După cum am observat deja, $\mathbb{Z}/p\mathbb{Z}$ şi $\mathbb{Q}$ sunt corpuri prime. Este adevărat însă şi reciproc.

Propoziţia 1.16. *Orice corp prim este izomorf cu $\mathbb{Q}$ sau cu $\mathbb{Z}/p\mathbb{Z}$, p prim.*

Proof. Fie K un corp prim şi $\varphi : \mathbb{Z} \to K$ dată prin $\varphi(n) = n \cdot 1$. Este clar că φ este morfism de inele şi avem două posibilităţi:
(i) $\operatorname{Ker} \varphi = \{0\}$, caz în care $\mathbb{Z} \simeq \operatorname{Im} \varphi$, deci K conţine un subinel izomorf cu $\mathbb{Z}$. Rezultă că K conţine un subcorp izomorf cu $\mathbb{Q}$ şi cum K este corp prim obţinem $K \simeq \mathbb{Q}$.
(ii) $\operatorname{Ker} \varphi = p\mathbb{Z}$, $p \in \mathbb{N} \setminus \{0, 1\}$. Avem $\mathbb{Z}/p\mathbb{Z} \simeq \operatorname{Im} \varphi \subseteq K$, deci $\mathbb{Z}/p\mathbb{Z}$ este inel integru. De aici rezultă că p este număr prim, deci $\mathbb{Z}/p\mathbb{Z}$ este corp şi cum K este corp prim obţinem $K \simeq \mathbb{Z}/p\mathbb{Z}$. □

Definiţia 1.17. *Fie K un corp. Dacă K conţine un subcorp prim izomorf cu $\mathbb{Q}$, atunci spunem că K este* corp de caracteristică zero *şi scriem* $\operatorname{char} K = 0$. *Dacă K conţine un subcorp prim izomorf cu $\mathbb{Z}/p\mathbb{Z}$, atunci spunem că K este* corp de caracteristică p *şi scriem* $\operatorname{char} K = p$.

Remarca 1.18. (i) $\operatorname{char} K = 0$ dacă şi numai dacă $\operatorname{ord}(1) = \infty$ în grupul $(K, +)$, iar $\operatorname{char} K = p$ dacă şi numai dacă $\operatorname{ord}(1) = p$ în grupul $(K, +)$.
(ii) Dacă $K' \subseteq K$ este o extindere de corpuri, atunci $\operatorname{char} K' = \operatorname{char} K$.

Exemplul 1.19. (i) $\operatorname{char}\mathbb{Q} = 0$ şi $\operatorname{char}\mathbb{Z}/p\mathbb{Z} = p$.
(ii) $\operatorname{char}\mathbb{R} = 0$ şi $\operatorname{char}\mathbb{Q}(\sqrt{2}) = 0$.

Propoziţia 1.20. *Fie K un corp, $\operatorname{char} K = p > 0$ şi $a, b \in K$ cu $ab = ba$. Atunci $(a+b)^{p^n} = a^{p^n} + b^{p^n}$ pentru orice $n \geq 1$.*

Proof. Este suficient să demonstrăm cazul $n = 1$. Pentru aceasta folosim formula binomului lui Newton. Avem $(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k$. Însă $p \mid \binom{p}{k}$ pentru orice $k \in \{1, \ldots, p-1\}$, deci $\binom{p}{k} = 0$ în K. În concluzie, $(a+b)^p = a^p + b^p$. □

Corolarul 1.21. *Fie K un corp comutativ cu $\operatorname{char} K = p > 0$. Atunci aplicaţia $\varphi : K \to K$ definită prin $\varphi(x) = x^p$ este morfism de corpuri.*

Morfismul definit în corolarul precedent se numeşte *endomorfismul lui Frobenius*.

2. Construcţii de corpuri

Vom construi acum trei exemple importante de corpuri.

1. Corpul numerelor complexe

Fie $\mathbb{C} = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R} \right\}$. Se verifică uşor că $\mathbb{C}$ este corp în raport cu adunarea şi înmulţirea matricelor. Există un morfism de corpuri $f : \mathbb{R} \to \mathbb{C}$ dat prin $f(a) = aI_2$. Astfel putem identifica pe $\mathbb{R}$ cu un subcorp al lui $\mathbb{C}$. Fie $i = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Atunci $i^2 = -I_2$ iar $\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = aI_2 + bi$. Cum I_2 este elementul unitate al lui $\mathbb{C}$ vom scrie $a + bi$ în loc de $aI_2 + bi$. Deci $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$ este un corp cu adunarea şi înmulţirea date astfel:

$$(a + bi) + (c + di) = (a + c) + (b + d)i,$$

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i,$$

pentru orice $a, b, c, d \in \mathbb{R}$.

2. Corpul cuaternionilor

Fie $\mathbb{H} = \left\{ \begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} : a, b \in \mathbb{C} \right\}$. Se verifică uşor că $\mathbb{H}$ este corp *necomutativ* în raport cu adunarea şi înmulţirea matricelor. Elementele lui $\mathbb{H}$ se numesc *cuaternioni*. Există un morfism de corpuri $f : \mathbb{C} \to \mathbb{H}$ dat prin $f(a) = \begin{pmatrix} a & 0 \\ 0 & \overline{a} \end{pmatrix}$. Astfel putem identifica pe $\mathbb{C}$ cu un subcorp al lui $\mathbb{H}$. Orice $a \in \mathbb{R}$ se identifică cu aI_2, iar $i \in \mathbb{C}$ se identifică cu $\mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$. Considerăm acum cuaternionii $\mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ şi $\mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$. Scriem $a = x + iy$, $b = z + it$, cu $x, y, z, t \in \mathbb{R}$. Atunci

$$\begin{pmatrix} a & b \\ -\overline{b} & \overline{a} \end{pmatrix} = x + \mathbf{i}y + \mathbf{j}z + \mathbf{k}t.$$

Deci $\mathbb{H} = \{x + \mathbf{i}y + \mathbf{j}z + \mathbf{k}t : x, y, z, t \in \mathbb{R}\}$ şi avem relaţiile:

$$\mathbf{ij} = \mathbf{k},\ \mathbf{ji} = -\mathbf{k},$$
$$\mathbf{jk} = \mathbf{i},\ \mathbf{kj} = -\mathbf{i},$$
$$\mathbf{ki} = \mathbf{j},\ \mathbf{ik} = -\mathbf{j},$$
$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1.$$

Remarca 2.1. Cuaternionii $\{\pm 1, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$ formează un grup necomutativ în raport cu înmulţirea numit *grupul cuternionilor*.

3. Corpul de fracţii al unui domeniu de integritate

Fie R un domeniu de integritate (cu $1 \neq 0$). Vom construi un corp comutativ care îl conţine pe R ca subinel şi care este cel mai mic corp cu această proprietate. Să considerăm produsul cartezian $R \times R^\times = \{(a, b) : a, b \in R, b \neq 0\}$. Pe această mulţime definim o relaţie binară astfel: $(a, b) \sim (c, d)$ dacă şi numai dacă $ad = bc$. Este imediat că "$\sim$" este o relaţie de echivalenţă. Fie $Q(R) = R \times R^\times / \sim$. Clasa de echivalenţă a unei perechi (a, b) în raport cu relaţia "$\sim$" se va nota $\frac{a}{b}$ şi se va numi *fracţie*. Definim pe $Q(R)$ două operaţii algebrice astfel:

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

pentru orice $a, b, c, d \in R$, $b \neq 0$, $d \neq 0$. Aceste operaţii sunt bine definite şi $(Q(R), +, \cdot)$ este un corp comutativ, numit *corpul de fracţii* al lui R.

Exemplul 2.2. (i) $Q(\mathbb{Z}) = \mathbb{Q}$.
(ii) Fie $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$. Atunci $Q(\mathbb{Z}[\sqrt{2}]) = \mathbb{Q}(\sqrt{2})$.

Există un morfism injectiv de inele unitare $\varphi : R \to Q(R)$ dat prin $\varphi(a) = \frac{a}{1}$.

Remarca 2.3. Fie R un domeniu de integritate. Atunci $Q(R)$ este cel mai mic corp comutativ cu proprietatea că îl conţine pe R ca subinel.

INELE DE POLINOAME

Pe parcursul acestui capitol inelele vor fi comutative şi unitare iar morfismele de inele vor fi unitare.

1. Inele de polinoame într-o nedeterminată

Fie R un inel comutativ şi unitar. Notăm cu $R^{(\mathbb{N})}$ mulţimea şirurilor $(a_n)_{n\in\mathbb{N}}$ cu elemente din R şi care au doar un număr finit de termeni nenuli. Pe $R^{(\mathbb{N})}$ definim două operaţii algebrice:

$$(a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}} = (a_n + b_n)_{n\in\mathbb{N}},$$
$$(a_n)_{n\in\mathbb{N}} \cdot (b_n)_{n\in\mathbb{N}} = (c_n)_{n\in\mathbb{N}},$$

unde $c_n = \sum_{i+j=n} a_i b_j$.

Propoziţia 1.1. *$(R^{(\mathbb{N})}, +, \cdot)$ este inel comutativ şi unitar.*

Definim un morfism injectiv de inele unitare $\varepsilon : R \to R^{(\mathbb{N})}$, $\varepsilon(a) = (a, 0, 0, \dots)$ care ne permite să-l identificăm pe R cu un subinel al lui $R^{(\mathbb{N})}$. Vom nota cu X şirul $(0, 1, 0, 0, \dots)$ şi-l vom numi *nedeterminată*. Observăm că

$$X^n = (\underbrace{0, \dots, 0}_{n \text{ termeni}}, 1, 0, 0, \dots)$$

pentru orice $n \in \mathbb{N}^*$. Ca de obicei, considerăm X^0 ca fiind egal cu elementul unitate. Se observă că $(a_0, a_1, \dots, a_n, 0, 0, \dots) = \varepsilon(a_0) + \varepsilon(a_1)X + \cdots + \varepsilon(a_n)X^n$ iar prin identificarea lui R cu un subinel al lui $R^{(\mathbb{N})}$ dată de ε putem scrie

$$(a_0, a_1, \dots, a_n, 0, 0, \dots) = a_0 + a_1 X + \cdots + a_n X^n.$$

Definiţia 1.2. *Inelul $R^{(\mathbb{N})}$ se notează cu $R[X]$ şi se numeşte* inelul polinoamelor în nedeterminata X cu coeficienţi în R.

Dacă $f \in R[X]$, atunci $f = a_0 + a_1 X + \cdots + a_n X^n$, $a_i \in R$ şi f se numeşte *polinom în nedeterminata X*. Polinoamele X^n, $n \in \mathbb{N}$ se numesc *monoame în nedeterminata X*. Aşadar orice polinom este în mod unic o combinaţie liniară de monoame cu coeficienţi în R. Polinoamele $a_i X^i$ cu $a_i \neq 0$ se numesc *termeni* ai lui f, iar $a_i \neq 0$ *coeficienţi*. Definim $\deg f = \max\{i : a_i \neq 0\}$ şi-l numim *gradul* lui f. Dacă $n = \deg f$, atunci a_n se numeşte *coeficientul dominant* al lui f. Polinoamele al căror coeficient dominant este 1 se numesc polinoame *monice*.

În cele ce urmează vom face următoarea convenţie: $\deg 0 = -\infty$.

Propoziţia 1.3. *Fie $f, g \in R[X]$. Atunci:*
(i) $\deg(f + g) \leq \max(\deg f, \deg g)$.
(ii) $\deg(fg) \leq \deg f + \deg g$, *cu egalitate dacă şi numai dacă produsul coeficienţilor dominanţi ai lui f şi g este nenul.*

Corolarul 1.4. *Fie R un inel integru. Atunci* $\deg(fg) = \deg f + \deg g$ *pentru orice $f, g \in R[X]$. Mai mult, $R[X]$ este, de asemenea, inel integru.*

Corolarul 1.5. *Fie R un inel integru. Atunci $U(R[X]) = U(R)$.*

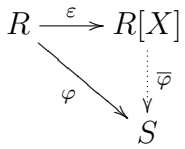
Remarca 1.6. Proprietatea de mai sus nu mai rămâne adevărată dacă R nu este inel integru. Fie $R = \mathbb{Z}/4\mathbb{Z}$ şi $f = \widehat{1} + \widehat{2}X \in R[X]$. Avem $f^2 = \widehat{1}$, deci $f \in U(R[X])$, dar $f \notin U(R)$.

Exerciţiul 1.7. Fie R un inel comutativ unitar şi $f = a_0 + a_1X + \cdots + a_nX^n \in R[X]$. Să se arate că:
(i) f este nilpotent dacă şi numai dacă a_i este nilpotent pentru orice $0 \leq i \leq n$.
(ii) f este inversabil dacă şi numai dacă a_0 este inversabil şi a_i este nilpotent pentru orice $1 \leq i \leq n$.

Reamintim că există un morfism (canonic) de inele unitare $\varepsilon : R \to R[X]$ dat prin $\varepsilon(a) = a$ pentru orice $a \in R$.

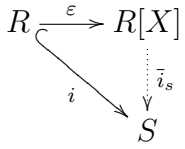
Teorema 1.8. (Proprietatea de universalitate a inelelor de polinoame într-o nedeterminată) *Fie $\varphi : R \to S$ un morfism de inele comutative unitare şi $s \in S$. Atunci există un morfism unitar $\overline{\varphi} : R[X] \to S$ unic cu proprietatea că $\overline{\varphi} \circ \varepsilon = \varphi$ şi $\overline{\varphi}(X) = s$.*

Proof. Să vizualizăm această proprietate cu ajutorul următoarei diagrame:



Definim $\overline{\varphi}(a_0 + a_1X + \cdots + a_nX^n) = \varphi(a_0) + \varphi(a_1)s + \cdots + \varphi(a_n)s^n$. Se arată uşor că $\overline{\varphi}$ este morfism unitar de inele care satisface cele două proprietăţi. Mai mult, acesta este unic, deoarece $\overline{\varphi}(X) = s$ conduce la $\overline{\varphi}(X^i) = s^i$ pentru orice $i \geq 1$ iar $\overline{\varphi} \circ \varepsilon = \varphi$ este echivalent cu $\overline{\varphi}(a) = \varphi(a)$ pentru orice $a \in R$. □

1.1. **Funcţii polinomiale. Rădăcini.** Fie S un inel comutativ şi unitar, $R \subseteq S$ un subinel şi $i : R \to S$ morfismul incluziune. Fie $s \in S$. Din proprietatea de universalitate a inelelor de polinoame într-o nedeterminată există un morfism unitar $\overline{i}_s : R[X] \to S$ unic cu proprietatea că $\overline{i}_s \circ \varepsilon = i$ şi $\overline{i}_s(X) = s$.



Dacă $f \in R[X]$, $f = a_0 + a_1X + \cdots + a_nX^n$, atunci $\overline{i}_s(f) = a_0 + a_1s + \cdots + a_ns^n$. Notăm $a_0 + a_1s + \cdots + a_ns^n$ cu $f(s)$ şi avem $\overline{i}_s(f) = f(s)$.

Definiţia 1.9. *Un element $s \in S$ cu proprietatea că $f(s) = 0$ se numeşte* rădăcină a lui f.

Pentru orice polinom $f \in R[X]$ putem defini o funcţie $\widetilde{f} : S \to S$ prin $\widetilde{f}(s) = f(s)$ pentru orice $s \in S$.

Definiţia 1.10. *Funcţia $\widetilde{f} : S \to S$ definită mai sus se numeşte* funcţia polinomială pe S asociată lui f. *Când $S = R$, funcţia $\widetilde{f} : R \to R$ se numeşte* funcţia polinomială asociată lui f.

Remarca 1.11. Polinoame diferite pot avea funcţii polinomiale egale. De exemplu, $f, g \in \mathbb{Z}_2[X]$, $f = X$ şi $g = X^2$. Avem că $\widetilde{f}, \widetilde{g} : \mathbb{Z}_2 \to \mathbb{Z}_2$, $\widetilde{f}(\widehat{0}) = \widetilde{g}(\widehat{0}) = \widehat{0}$ şi $\widetilde{f}(\widehat{1}) = \widetilde{g}(\widehat{1}) = \widehat{1}$.

Vom vedea însă că acest lucru nu mai este posibil dacă $f, g \in R[X]$, unde R este un domeniu de integritate *infinit*.

2. Teorema de împărţire cu rest pentru polinoame într-o nedeterminată

Teorema 2.1. (Teorema de împărţire cu rest) *Fie R un inel, $f, g \in R[X]$, $g \neq 0$ iar coeficientul dominant al lui g este inversabil. Atunci există $q, r \in R[X]$ unice cu proprietatea că $f = gq + r$ şi $\deg r < \deg g$.*

Proof. Dacă $\deg f < \deg g$, atunci scriem $f = g \cdot 0 + f$. În cazul în care $\deg f \geq \deg g$ facem inducţie după $\deg f$.
Unicitatea rezultă imediat folosind Propoziţia 1.3(ii). □

Corolarul 2.2. *Fie R un inel, $f \in R[X]$ şi $\alpha \in R$. Atunci există $q \in R[X]$ şi $r \in R$ unice cu proprietatea că $f = (X - \alpha)q + r$.*

Corolarul 2.3. (Bézout) *Fie R un inel, $f \in R[X]$ şi $\alpha \in R$. Atunci $X - \alpha \mid f$ dacă şi numai dacă $f(\alpha) = 0$.*

Exerciţiul 2.4. Fie R inel comutativ unitar şi $\alpha \in R$. Atunci $R[X]/(X - \alpha) \simeq R$.

Exerciţiul 2.5. Arătaţi că:
(i) $\mathbb{R}[X]/(X^2 + 1) \simeq \mathbb{C}$.
(ii) $\mathbb{Z}[X]/(X^2 - 2) \simeq \mathbb{Z}[\sqrt{2}]$.

Exerciţiul 2.6. Să se arate că $R = \mathbb{Z}[X]/(2, X^2 + 1)$ este un inel cu 4 elemente, dar R nu este izomorf cu $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Exerciţiul 2.7. Considerăm idealul $I = (3, X^3 - X^2 + 2X + 1)$ în $\mathbb{Z}[X]$. Să se arate că I nu este ideal principal şi că $\mathbb{Z}[X]/I$ nu este inel integru.

Exerciţiul 2.8. Aflaţi inversul lui $\widehat{4X + 3}$ în inelul factor $\mathbb{Z}_{11}[X]/(X^2 + 1)$.

Propoziţia 2.9. *Fie R un inel integru şi $f \in R[X]$, $\deg f = n$. Atunci f are cel mult n rădăcini distincte în R.*

Proof. Fie $\alpha_1, \ldots, \alpha_m \in R$ distincte cu proprietatea că $f(\alpha_i) = 0$ pentru orice $i = 1, \ldots, m$. Vom demonstra prin inducţie după m că $(X - \alpha_1) \cdots (X - \alpha_m) \mid f$. Cazul $m = 1$ rezultă din corolarul 2.3. Dacă $m > 1$, atunci, din ipoteza de inducţie $(X - \alpha_1) \cdots (X - \alpha_{m-1}) \mid f$ şi putem scrie $f = (X - \alpha_1) \cdots (X - \alpha_{m-1})g$ cu $g \in R[X]$. Din $f(\alpha_m) = 0$ obţinem $(\alpha_m - \alpha_1) \cdots (\alpha_m - \alpha_{m-1})g(\alpha_m) = 0$. Dar cum R este integru şi $\alpha_i \neq \alpha_m$ pentru orice $i \neq m$ rezultă $g(\alpha_m) = 0$ şi din corolarul 2.3 deducem că $X - \alpha_m \mid g$.
În concluzie, $n = \deg f \geq m$. □

Remarca 2.10. Dacă R nu este integru, atunci proprietatea de mai sus este falsă. De exemplu, polinomul $f \in \mathbb{Z}_6[X]$, $f = X^3 - X$ are şase rădăcini distincte în $\mathbb{Z}_6$.

Corolarul 2.11. *Fie R un inel integru infinit şi $f, g \in R[X]$. Dacă $\widetilde{f} = \widetilde{g}$, atunci $f = g$.*

Proof. Fie $h = f - g$. Deoarece $\widetilde{f} = \widetilde{g}$ avem $\widetilde{h} = 0$, adică $h(\alpha) = 0$ pentru orice $\alpha \in R$. Din propoziţia 2.9 rezultă $h = 0$. □

Propoziţia 2.12. (Relaţiile lui Viète) *Fie R un inel integru, $f \in R[X]$, $f = a_0 + a_1X + \cdots + a_nX^n$, $a_n \neq 0$. Presupunem că f are n rădăcini $\alpha_1, \ldots, \alpha_n \in R$. Atunci au loc relaţiile:*

$$\sum_{i=1}^{n} \alpha_i = -\frac{a_{n-1}}{a_n}$$

$$\sum_{1 \leq i < j \leq n}^{n} \alpha_i \alpha_j = \frac{a_{n-2}}{a_n}$$

$$\cdots\cdots\cdots$$

$$\prod_{i=1}^{n} \alpha_i = (-1)^n \frac{a_0}{a_n}$$

Proof. Arătăm prin inducţie după n că $f = a_n(X - \alpha_1) \cdots (X - \alpha_n)$ şi apoi identificăm coeficienţii. □

3. Inele de polinoame într-un număr finit de nedeterminate

Definiţia 3.1. *Fie R un inel. Atunci* inelul de polinoame în nedeterminatele $X_1, \ldots, X_n$ cu coeficienţi în R *se defineşte inductiv ca fiind $R[X_1, \ldots, X_{n-1}][X_n]$ şi se notează $R[X_1, \ldots, X_n]$. Elementele inelului $R[X_1, \ldots, X_n]$ se numesc* polinoame în nedeterminatele $X_1, \ldots, X_n$..

Remarca 3.2. Orice polinom $f \in R[X_1, \ldots, X_n]$ se scrie (în mod unic) sub forma

$$f = f_0 + f_1X_n + \cdots + f_rX_n^r$$

cu $f_i \in R[X_1, \ldots, X_{n-1}]$ pentru orice $i = 0, 1, \ldots, r$.

Propoziţia 3.3. *Pentru orice polinom $f \in R[X_1, \ldots, X_n]$ există şi sunt unice $k_1, \ldots, k_n \in \mathbb{N}$ şi $a_{i_1,\ldots,i_n} \in R$, unde $0 \leq i_1 \leq k_1, \ldots, 0 \leq i_n \leq k_n$ astfel încât*

$$f = \sum_{i_1=0}^{k_1} \cdots \sum_{i_n=0}^{k_n} a_{i_1,\ldots,i_n} X_1^{i_1} \cdots X_n^{i_n}.$$

Proof. Inducţie după n. Scriem $f = f_0 + f_1X_n + \cdots + f_{k_n}X_n^{k_n}$ cu $f_i \in R[X_1, \ldots, X_{n-1}]$ şi aplicăm ipoteza de inducţie.
Pentru unicitate fie

$$f = \sum_{i_1=0}^{k_1} \cdots \sum_{i_n=0}^{k_n} a_{i_1,\ldots,i_n} X_1^{i_1} \cdots X_n^{i_n}$$

şi să presupunem că $f = 0$. Scriem

$$f = f_0 + f_1X_n + \cdots + f_{k_n}X_n^{k_n},$$

unde $f_j = \sum_{i_1=0}^{k_1} \cdots \sum_{i_{n-1}=0}^{k_{n-1}} a_{i_1,\ldots,i_{n-1},j} X_1^{i_1} \cdots X_{n-1}^{i_{n-1}} \in R[X_1, \ldots, X_{n-1}]$. Deoarece $f = 0$ rezultă $f_j = 0$ pentru orice $j = 0, 1, \ldots, k_n$ şi din ipoteza de inducţie $a_{i_1,\ldots,i_{n-1},j} = 0$ pentru orice $j = 0, 1, \ldots, k_n$. □

Un polinom de forma $X_1^{i_1} \cdots X_n^{i_n}$ se va numi *monom în nedeterminatele* $X_1, \ldots, X_n$ iar *gradul* său se consideră a fi $i_1 + \cdots + i_n$. Aşadar orice polinom $f \in R[X_1, \ldots, X_n]$ este (în mod unic) o combinaţie liniară de monoame cu coeficienţi în R. Polinoamele $a_{i_1,\ldots,i_n} X_1^{i_1} \cdots X_n^{i_n}$ cu $a_{i_1,\ldots,i_n} \neq 0$ se numesc *termeni* ai lui f, iar $a_{i_1,\ldots,i_n} \neq 0$ *coeficienţi*. Definim *gradul lui* f ca fiind maximul gradelor monoamelor care apar în scrierea sa. Dacă toate monoamele au acelaşi grad, atunci f se numeşte *polinom omogen*.

Remarca 3.4. Orice polinom se scrie în mod unic ca o sumă de polinoame omogene. Mai precis, dacă $f \in R[X_1, \ldots, X_n]$, atunci $f = f_0 + f_1 + \cdots + f_t$ cu $f_i \in R[X_1, \ldots, X_n]$ polinom omogen de grad i. În plus, $f = 0$ dacă şi numai dacă $f_i = 0$ pentru orice $i = 0, 1, \ldots, t$.

Propoziţia 3.5. *Fie* $f, g \in R[X_1, \ldots, X_n]$. *Atunci:*
(i) $\deg(f + g) \leq \max(\deg f, \deg g)$.
(ii) $\deg(fg) \leq \deg f + \deg g$.

Corolarul 3.6. *Fie* R *un inel integru. Atunci* $R[X_1, \ldots, X_n]$ *este, de asemenea, integru şi* $\deg(fg) = \deg f + \deg g$ *pentru orice* $f, g \in R[X_1, \ldots, X_n]$.

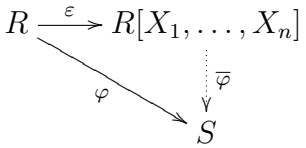
Proof. Prima afirmaţie rezultă imediat prin inducţie după $n \geq 1$. Pentru cea de-a doua vom scrie $f = f_0 + f_1 + \cdots + f_p$, respectiv $g = g_0 + g_1 + \cdots + g_q$ cu f_i, g_j polinoame omogene de grad i (respectiv, j). Presupunem că $f_p \neq 0$ şi $g_q \neq 0$. De aici rezultă că $\deg f = p$ şi $\deg g = q$. Cum însă $R[X_1, \ldots, X_n]$ este inel integru vom avea $f_p g_q \neq 0$, deci $\deg(fg) = p + q$. □

Corolarul 3.7. *Fie* R *un inel integru. Atunci* $U(R[X_1, \ldots, X_n]) = U(R)$.

Reamintim că există un morfism canonic $\varepsilon : R \to R[X_1, \ldots, X_n]$ dat prin $\varepsilon(a) = a$ pentru orice $a \in R$.

Teorema 3.8. (Proprietatea de universalitate a inelelor de polinoame într-un număr finit de nedeterminate) *Fie* $\varphi : R \to S$ *un morfism de inele comutative unitare şi* $s_1, \ldots, s_n \in S$. *Atunci există un morfism unitar de inele* $\overline{\varphi} : R[X_1, \ldots, X_n] \to S$ *unic cu proprietatea că* $\overline{\varphi} \circ \varepsilon = \varphi$ *şi* $\overline{\varphi}(X_i) = s_i$ *pentru orice* $i = 1, \ldots, n$.

Proof. Să vizualizăm această proprietate cu ajutorul următoarei diagrame:



Procedăm prin inducţie după n aplicând în mod repetat teorema 1.8. □

Exerciţiul 3.9. Fie R inel comutativ unitar şi $\alpha_1, \ldots \alpha_n \in R$. Atunci avem următorul izomorfism: $R[X_1, \ldots, X_n]/(X - \alpha_1, \ldots, X - \alpha_n) \simeq R$.

4. Polinoame simetrice

Fie R un inel comutativ şi unitar, $n \geq 2$ şi $\sigma \in S_n$. Din teorema 3.8 rezultă că există un morfism unitar de inele $\overline{\sigma} : R[X_1, \ldots, X_n] \to R[X_1, \ldots, X_n]$ cu proprietatea că $\overline{\sigma} \circ \varepsilon = \varepsilon$ şi $\overline{\sigma}(X_i) = X_{\sigma(i)}$ pentru orice $i = 1, \ldots, n$.

Exemplul 4.1. Fie $f \in R[X_1, X_2, X_3]$, $f = X_1^2X_3 + X_1X_2X_3^2$ şi $\sigma = (1\ 2\ 3)$. Atunci $\overline{\sigma}(f) = X_1X_2^2 + X_1^2X_2X_3$.

În general vom avea că $\overline{\sigma}(f(X_1, \ldots, X_n)) = f(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$ pentru orice $f \in R[X_1, \ldots, X_n]$.

Remarca 4.2. (i) Dacă $\sigma, \tau \in S_n$, atunci $\overline{\sigma \circ \tau} = \overline{\sigma} \circ \overline{\tau}$.
(ii) $\overline{e}(f) = f$ pentru orice $f \in R[X_1, \ldots, X_n]$, unde $e \in S_n$ este permutarea identică.
(iii) $\overline{\sigma}$ este un izomorfism, iar $\overline{\sigma}^{-1} = \overline{\sigma^{-1}}$.

Definiţia 4.3. *Fie $f \in R[X_1, \ldots, X_n]$. Dacă $\overline{\sigma}(f) = f$ pentru orice $\sigma \in S_n$, atunci f se numeşte* polinom simetric.

Remarca 4.4. $f \in R[X_1, \ldots, X_n]$ este polinom simetric dacă şi numai dacă $\overline{\tau}(f) = f$ pentru orice transpoziţie $\tau \in S_n$.

Exemplul 4.5. Polinomul $f \in R[X_1, X_2]$, $f = X_1^2 + X_2^2$ este simetric. Să observăm că dacă îl considerăm pe f ca polinom în $R[X_1, X_2, X_3]$, atunci acesta nu mai este simetric.

Propoziţia 4.6. *Mulţimea $\Sigma = \{f \in R[X_1, \ldots, X_n] : f$ polinom simetric$\}$ este un subinel unitar al lui $R[X_1, \ldots, X_n]$.*

Proof. Rezultă din faptul că $\overline{\sigma}$ este morfism de inele pentru orice $\sigma \in S_n$. □

Propoziţia 4.7. *Polinoamele $s_k \in R[X_1, \ldots, X_n]$ definite prin*

$$s_k = \sum_{1 \leq i_1 < \cdots < i_k \leq n} X_{i_1} \cdots X_{i_k},$$

pentru orice $k = 1, \ldots, n$, sunt polinoame simetrice.

Proof. Se consideră polinomul

$$g(T) = (T - X_1) \cdots (T - X_n),$$

$g \in R[X_1, \ldots, X_n][T]$. Avem că

$$g(T) = T^n - s_1T^{n-1} + s_2T^{n-2} - \cdots + (-1)^n s_n.$$

Fie $\sigma \in S_n$. Definim

$$\overline{\sigma} : R[X_1, \ldots, X_n, T] \to R[X_1, \ldots, X_n, T]$$

astfel: $\overline{\sigma}(X_i) = X_{\sigma(i)}$ pentru orice $i = 1, \ldots, n$ şi $\overline{\sigma}(T) = T$. Atunci

$$\overline{\sigma}(g) = (T - X_{\sigma(1)}) \cdots (T - X_{\sigma(n)}) = g.$$

Pe de altă parte,

$$\overline{\sigma}(g) = \overline{\sigma}(T^n - s_1T^{n-1} + s_2T^{n-2} - \cdots + (-1)^n s_n) =$$
$$= T^n - \overline{\sigma}(s_1)T^{n-1} + \overline{\sigma}(s_2)T^{n-2} - \cdots + (-1)^n \overline{\sigma}(s_n).$$

De aici rezultă că $s_k = \overline{\sigma}(s_k)$ pentru orice $k = 1, \ldots, n$, deci polinoamele s_k sunt simetrice. □

Definiţia 4.8. *Polinoamele s_k, $k = 1, \ldots, n$, definite mai sus se numesc* polinoamele simetrice fundamentale în nedeterminatele $X_1, \ldots, X_n$.

Definiţia 4.9. *Vom defini pe mulţimea monoamelor în n nedeterminate o relaţie de ordine astfel:*

$$X_1^{i_1} \cdots X_n^{i_n} > X_1^{j_1} \cdots X_n^{j_n}$$

dacă există $s \in \{1, \ldots, n\}$ cu proprietatea că $i_1 = j_1, \ldots, i_{s-1} = j_{s-1}$ şi $i_s > j_s$. Aceasta se va numi ordinea lexicografică.

Propoziţia 4.10. *Ordinea lexicografică este o relaţie de ordine totală pe mulţimea monoamelor.*

Definiţia 4.11. *Fie $f \in R[X_1, \ldots, X_n]$, $f \neq 0$ şi fie $X_1^{i_1} \cdots X_n^{i_n}$ cel mai mare monom în ordinea lexicografică dintre cele care apar în scrierea lui f ca o combinaţie liniară de monoame. Acesta se numeşte* monomul principal al lui f *şi se notează* $\mathrm{LM}(f)$. *Dacă $a \in R$, $a \neq 0$ este coeficientul monomului principal al lui f, atunci a se numeşte* coeficientul principal al lui f *şi se notează* $\mathrm{LC}(f)$ *iar $aX_1^{i_1} \cdots X_n^{i_n}$ se numeşte* termenul principal al lui f *şi se notează* $\mathrm{LT}(f)$.

În mod evident avem $\mathrm{LT}(f) = \mathrm{LC}(f)\,\mathrm{LM}(f)$.

Exemplul 4.12. Fie $f \in \mathbb{Q}[X_1, X_2, X_3]$, $f = 2X_1^2X_2^2 + 3X_1X_2^3X_3 - X_1^2X_2X_3^5$. Atunci $\mathrm{LM}(f) = X_1^2X_2^2$, $\mathrm{LC}(f) = 2$ şi $\mathrm{LT}(f) = 2X_1^2X_2^2$.

Lema 4.13. *Fie $m_1, m_2 \in R[X_1, \ldots, X_n]$ monoame cu $m_1 > m_2$. Atunci:*
(i) $m_1 m > m_2 m$, oricare ar fi $m \in R[X_1, \ldots, X_n]$ monom.
(ii) Dacă $m_1', m_2' \in R[X_1, \ldots, X_n]$ sunt monoame şi $m_1' > m_2'$, atunci $m_1 m_1' > m_2 m_2'$.

Proof. (i) Fie $m_1 = X_1^{i_1} \cdots X_n^{i_n}$, $m_2 = X_1^{j_1} \cdots X_n^{j_n}$ şi $m = X_1^{k_1} \cdots X_n^{k_n}$. Deoarece $m_1 > m_2$ există $s \in \{1, \ldots, n\}$ cu proprietatea că $i_1 = j_1, \ldots, i_{s-1} = j_{s-1}$ şi $i_s > j_s$. Atunci $i_1 + k_1 = j_1 + k_1, \ldots, i_{s-1} + k_{s-1} = j_{s-1} + k_{s-1}$ şi $i_s + k_s > j_s + k_s$, deci $m_1 m > m_2 m$.
(ii) Rezultă din (i): $m_1 > m_2 \implies m_1 m_1' > m_2 m_1'$ iar $m_1' > m_2' \implies m_2 m_1' > m_2 m_2'$. □

Propoziţia 4.14. *Fie $f_1, f_2 \in R[X_1, \ldots, X_n]$ polinoame nenule. Dacă $\mathrm{LT}(f_1) = a_1 m_1$, $\mathrm{LT}(f_2) = a_2 m_2$ şi $a_1 a_2 \neq 0$, atunci $\mathrm{LT}(f_1 f_2) = (a_1 a_2) m_1 m_2 = \mathrm{LT}(f_1)\,\mathrm{LT}(f_2)$.*

Proof. Rezultă din lema 4.13. □

Lema 4.15. *Fie $f \in R[X_1, \ldots, X_n]$, $f \neq 0$ polinom simetric şi $\mathrm{LM}(f) = X_1^{i_1} \cdots X_n^{i_n}$. Atunci $i_1 \geq \cdots \geq i_n$.*

Proof. Să presupunem, de exemplu, că $i_1 < i_2$. Atunci

$$X_1^{i_2} X_2^{i_1} \cdots X_n^{i_n} > X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}.$$

Dar monomul $X_1^{i_2} X_2^{i_1} \cdots X_n^{i_n}$ apare cu certitudine în f, deoarece f este simetric şi $\overline{\tau}(f) = f$, unde $\tau = (1\ 2)$. □

Propoziţia 4.16. *Orice şir strict descrescător de monoame $X_1^{i_1}\cdots X_n^{i_n}$ cu $i_1 \geq \cdots \geq i_n$ este finit.*

Proof. Reamintim că $X_1^{i_1}\cdots X_n^{i_n} > X_1^{j_1}\cdots X_n^{j_n}$ dacă există $s \in \{1,\ldots,n\}$ cu proprietatea că $i_1 = j_1, \ldots, i_{s-1} = j_{s-1}$ şi $i_s > j_s$. Deoarece avem $j_1 \geq \cdots \geq j_n$ rezultă că $i_s > j_s \geq j_{s+1} \geq \cdots \geq j_n$, deci $i_1 \geq j_k$ pentru orice $k = 1,\ldots,n$. Aşadar numărul monoamelor $X_1^{j_1}\cdots X_n^{j_n}$ cu $j_1 \geq \cdots \geq j_n$ care sunt mai mici decât $X_1^{i_1}\cdots X_n^{i_n}$ este finit. □

Exerciţiul 4.17. Arătaţi că orice şir strict descrescător de monoame este finit.

Teorema 4.18. (Teorema fundamentală a polinoamelor simetrice) *Orice polinom simetric se scrie în mod unic ca polinom de polinoamele simetrice fundamentale.*

Proof. Mai precis, avem de demonstrat că oricare ar fi $f \in R[X_1,\ldots,X_n]$ polinom simetric există şi este unic un polinom $g \in R[X_1,\ldots,X_n]$ astfel încât

$$f(X_1,\ldots,X_n) = g(s_1(X_1,\ldots,X_n),\ldots,s_n(X_1,\ldots,X_n)).$$

Existenţa: Fie $\mathrm{LT}(f) = aX_1^{i_1}\cdots X_n^{i_n}$. Deoarece f este simetric avem $i_1 \geq \cdots \geq i_n$. Mai mult, $\mathrm{LT}(s_k) = X_1\cdots X_k$ pentru orice $k = 1,\ldots,n$. De aici se obţine că

$$\mathrm{LT}(as_1^{i_1-i_2}\cdots s_{n-1}^{i_{n-1}-i_n}s_n^{i_n}) = \mathrm{LT}(f).$$

Fie $f_1 = f - as_1^{i_1-i_2}\cdots s_{n-1}^{i_{n-1}-i_n}s_n^{i_n}$. În mod evident f_1 este polinom simetric şi, în plus, $\mathrm{LM}(f_1) < \mathrm{LM}(f)$.
Unicitatea: Vom demonstra că dacă $h \in R[X_1,\ldots,X_n]$ şi $h(s_1,\ldots,s_n) = 0$, atunci $h = 0$. Scriem

$$h = \sum_{i_1=0}^{k_1}\cdots\sum_{i_n=0}^{k_n} a_{i_1,\ldots,i_n}X_1^{i_1}\cdots X_n^{i_n}$$

şi din $h(s_1,\ldots,s_n) = 0$ obţinem

$$\sum_{i_1=0}^{k_1}\cdots\sum_{i_n=0}^{k_n} a_{i_1,\ldots,i_n}s_1^{i_1}\cdots s_n^{i_n} = 0.$$

Se remarcăm acum că

$$\mathrm{LM}(s_1^{i_1}\cdots s_n^{i_n}) = X_1^{k_1}\cdots X_n^{k_n},$$

unde $k_1 = i_1 + \cdots + i_n, k_2 = i_2 + \cdots + i_n, \ldots, k_n = i_n$.
Se observă că dacă $(i_1,\ldots,i_n) \neq (j_1,\ldots,j_n)$, atunci $(k_1,\ldots,k_n) \neq (l_1,\ldots,l_n)$, unde $k_r = i_r + \cdots + i_n$, respectiv $l_r = j_r + \cdots + j_n$ pentru orice $r = 1,\ldots,n$. Aceasta înseamnă că $\mathrm{LM}(s_1^{i_1}\cdots s_n^{i_n}) \neq \mathrm{LT}(s_1^{j_1}\cdots s_n^{j_n})$ dacă $(i_1,\ldots,i_n) \neq (j_1,\ldots,j_n)$, deci $a_{i_1,\ldots,i_n} = 0$ pentru orice $i_1,\ldots,i_n$. □

Exerciţiul 4.19. Să se arate că următoarele polinoame sunt simetrice şi să se scrie fiecare dintre ele ca polinom de polinoamele simetrice fundamentale:
(i) $X_1^3X_2 + X_1^3X_3 + X_1X_2^3 + X_1X_3^3 + X_2^3X_3 + X_2X_3^3$.
(ii) $(X_1^2 + X_2^2)(X_1^2 + X_3^2)(X_2^2 + X_3^2)$.

În cele ce urmează vom nota $p_i = X_1^i + \cdots + X_n^i$, pentru orice $i \geq 1$. Evident, acestea sunt polinoame simetrice. În mod uzual definim $p_0 = n$.

Lema 4.20. *Fie $f \in R[X_1, \ldots, X_n]$ polinom simetric omogen de grad $k < n$. Dacă $f \neq 0$, atunci $f(X_1, \ldots, X_k, 0, \ldots, 0) \neq 0$.*

Proof. Fie $\mathrm{LM}(f) = X_1^{i_1} \cdots X_n^{i_n}$. Avem $i_1 \geq \cdots \geq i_n$ şi $i_1 + \cdots + i_n = k$. Deoarece $k < n$ rezultă $i_{k+1} = \cdots = i_n = 0$. Deci $\mathrm{LM}(f) = X_1^{i_1} \cdots X_k^{i_k}$ şi îl regăsim în $f(X_1, \ldots, X_k, 0, \ldots, 0)$. În concluzie, $f(X_1, \ldots, X_k, 0, \ldots, 0) \neq 0$. □

Teorema 4.21. (Formulele lui Newton)
(i) $p_k - p_{k-1}s_1 + \cdots + (-1)^n p_{k-n}s_n = 0$ pentru orice $k \geq n$.
(ii) $p_k - p_{k-1}s_1 + \cdots + (-1)^{k-1}p_1 s_{k-1} + (-1)^k k s_k = 0$ pentru orice $k = 1, \ldots, n-1$.

Proof. (i) Considerăm din nou polinomul $g \in R[X_1, \ldots, X_n, T]$,

$$g(T) = (T - X_1) \cdots (T - X_n).$$

Avem că $g(T) = T^n - s_1 T^{n-1} + s_2 T^{n-2} - \cdots + (-1)^n s_n$. Cum $g(X_i) = 0$ pentru orice $i = 1, \ldots, n$ obţinem

$$X_i^n - s_1 X_i^{n-1} + s_2 X_i^{n-2} - \cdots + (-1)^n s_n = 0$$

pentru orice $i = 1, \ldots, n$. Prin înmulţire cu X_i^{k-n} obţinem

$$X_i^k - s_1 X_i^{k-1} + s_2 X_i^{n-2} - \cdots + (-1)^n s_n X_i^{k-n} = 0$$

pentru orice $i = 1, \ldots, n$. Adunăm aceste relaţii şi obţinem

$$p_k - s_1 p_{k-1} + \cdots + (-1)^n s_n p_{k-n} = 0.$$

(ii) Fie $f = p_k - p_{k-1}s_1 + \cdots + (-1)^{k-1}p_1 s_{k-1} + (-1)^k k s_k$, unde $k < n$. Acesta este polinom simetric omogen de grad k şi

$$f(X_1, \ldots, X_k, 0, \ldots, 0) = p'_k - p'_{k-1}s'_1 + \cdots + (-1)^{k-1}p'_1 s'_{k-1} + (-1)^k k s'_k,$$

unde p'_i, s'_j sunt polinoamele definite anterior, dar de data aceasta în nedeterminatele $X_1, \ldots, X_k$. Din (i), cazul $k = n$, se obţine $f(X_1, \ldots, X_k, 0, \ldots, 0) = 0$ şi conform lemei 4.20, $f = 0$. □

Exerciţiul 4.22. (i) Să se calculeze $x_1^5 + x_2^5 + x_3^5$, unde x_1, x_2, x_3 sunt rădăcinile polinomului $X^3 - 3X + 1$.
(ii) Să se calculeze $x_1^3 + x_2^3 + x_3^3 + x_4^3$, unde x_1, x_2, x_3, x_4 sunt rădăcinile polinomului $X^4 + X^3 + 2X^2 + X + 1$.

Exerciţiul 4.23. Considerăm elementele $x_1, \ldots, x_n \in \mathbb{C}$ cu proprietatea că $x_1^k + \cdots + x_n^k = 0$ pentru orice $1 \leq k \leq n$. Să se arate că $x_1 = \cdots = x_n = 0$.

Exerciţiul 4.24. Să se rezolve în numere reale ecuaţia $\sqrt[4]{97 - x} + \sqrt[4]{x} = 5$.

Exerciţiul 4.25. Să se rezolve în numere reale sistemul de ecuaţii

$$\begin{cases} x^5 + y^5 = 33 \\ x + y = 3 \end{cases}$$

ARITMETICA ÎN $\mathbb{Z}$ ŞI $K[X]$

1. Divizibilitate. Algoritmul lui Euclid.

Să începem prin a observa că inelele $\mathbb{Z}$ şi $K[X]$ (K corp comutativ) sunt domenii de integritate, $U(\mathbb{Z}) = \{-1, 1\}$ şi $U(K[X]) = K^\times$.

Teorema 1.1. (Teorema de împărţire cu rest în $\mathbb{Z}$) *Fie $a, b \in \mathbb{Z}$, $b \neq 0$. Atunci există $q, r \in \mathbb{Z}$ unice cu proprietatea că $a = bq + r$ şi $0 \leq r < |b|$.*

Proof. Existenţa. Fie $r = \min\{a - bx : x \in \mathbb{Z} \text{ şi } a - bx \geq 0\}$. Scriem $r = a - bq$, $q \in \mathbb{Z}$. Dacă $r \geq |b|$, atunci $0 \leq a - b(q + \operatorname{sgn}(b)) < r$, contradicţie. Aşadar $r < |b|$. *Unicitatea.* Fie $q', r' \in \mathbb{Z}$ cu proprietatea că $a = bq' + r'$ şi $0 \leq r' < |b|$. Atunci $b(q - q') = r' - r$ şi de aici obţinem $|b||q - q'| = |r' - r| < |b|$, deci $q = q'$ şi $r = r'$. □

Definiţia 1.2. *Numărul întreg q din teorema de mai sus se numeşte* câtul împărţirii lui a la b, *iar r se numeşte* restul împărţirii lui a la b.

Exemplul 1.3. Fie $a = -17$ şi $b = 2$. Scriem $-17 = 2(-9) + 1$, deci $q = -9$ şi $r = 1$.

În cele ce urmează R va desemna $\mathbb{Z}$ sau $K[X]$.

Definiţia 1.4. *Fie $a, b \in R$. Spunem că b* divide *a dacă există $c \in R$ astfel încât $a = bc$ şi scriem $b \mid a$. Se mai spune că b* este divizor al lui *a sau că a* este multiplu al lui *b.*

Remarca 1.5. (i) $1 \mid a$ şi $a \mid 0$ pentru orice $a \in R$.
(ii) Dacă $b \neq 0$, atunci $b \mid a$ dacă şi numai dacă restul împărţirii lui a la b este 0.
(iii) Dacă $b \mid a$ şi $a \neq 0$, atunci $|b| \leq |a|$ pentru $R = \mathbb{Z}$, respectiv $\deg b \leq \deg a$ pentru $R = K[X]$.

Să enunţăm acum câteva proprietăţi simple ale relaţiei de divizibilitate.

Propoziţia 1.6. *(i) $a \mid b$ dacă şi numai dacă $bR \subseteq aR$.*
(ii) $a \mid a$ oricare ar fi $a \in R$.
(iii) $a \mid b$ şi $b \mid c \Rightarrow a \mid c$.
(iv) $a \mid b_i$, $\forall\, i = 1, \ldots, n \Rightarrow a \mid \sum_{i=1}^{n} \alpha_i b_i$, $\forall\, \alpha_i \in R$.

Definiţia 1.7. *Fie $a, b \in R$. Spunem că a* şi *b* sunt asociate în divizibilitate *dacă $a \mid b$ şi $b \mid a$.*

Notaţie: $a \sim b$.

Remarca 1.8. (i) "$\sim$" este o relaţie de echivalenţă pe R.
(ii) $a \sim 1$ dacă şi numai dacă $a \in U(R)$.

Din propoziţia 1.6(i) rezultă imediat că a este asociat în divizibilitate cu b dacă şi numai dacă $aR = bR$.

Propoziţia 1.9. *Fie $a, b \in R$. Atunci a şi b sunt asociate în divizibilitate dacă şi numai dacă $b = \pm a$ pentru $R = \mathbb{Z}$, respectiv $b = au$, $u \in K^\times$ pentru $R = K[X]$.*

Definiţia 1.10. *Fie $a, b \in R$. Spunem că un element $d \in R$ este un* cel mai mare divizor comun *al elementelor a, b dacă:*
(i) $d \mid a$ şi $d \mid b$,
(ii) $d' \mid a$ şi $d' \mid b$ implică $d' \mid d$.

Notaţie: c.m.m.d.c.(a, b) sau $\gcd(a, b)$ sau (a, b).

Definiţia 1.11. *Fie $a, b \in R$. Spunem că un element $m \in R$ este un* cel mai mic multiplu comun *al elementelor a, b dacă:*
(i) $a \mid m$ şi $b \mid m$,
(ii) $a \mid m'$ şi $b \mid m'$ implică $m \mid m'$.

Notaţie: c.m.m.m.c.(a, b) sau $\operatorname{lcm}(a, b)$ sau $[a, b]$.

Remarca 1.12. (i) Dacă $d_1, d_2 \in R$ sunt fiecare un cel mai mare divizor comun al elementelor a, b, atunci $d_1 \sim d_2$. Reciproc, dacă $d_1 \sim d_2$ şi d_1 este un cel mai mare divizor comun al elementelor a, b, atunci şi d_2 este un cel mai mare divizor comun al elementelor a, b. De aceea vom considera ca fiind c.m.m.d.c.(a, b) orice element al lui R care este un cel mai mare divizor comun al elementelor a, b şi vom spune că c.m.m.d.c.(a, b) *este unic până la o asociere în divizibilitate.*
(ii) Consideraţii similare sunt valabile şi pentru cel mai mic multiplu comun a două elemente $a, b \in R$.

Definiţia 1.13. *Două elemente $a, b \in R$ se numesc* prime între ele *sau* relativ prime *dacă* c.m.m.d.c.$(a, b) = 1$.

Vom demonstra că în inelul R orice două elemente au un c.m.m.d.c.

Algoritmul lui Euclid. Fie $a, b \in R$, $b \neq 0$. Scriem $a = bq_1 + r_1$ cu $0 \leq r_1 < |b|$, respectiv $\deg r_1 < \deg b$. Dacă $r_1 \neq 0$, atunci scriem $b = r_1 q_2 + r_2$ cu $0 \leq r_2 < r_1$, respectiv $\deg r_2 < \deg r_1$. Dacă $r_2 \neq 0$, atunci scriem $r_1 = r_2 q_3 + r_3$ cu $0 \leq r_3 < r_2$, respectiv $\deg r_3 < \deg r_2$ şi aşa mai departe. Obţinem astfel un şir strict descrescător de numere naturale $r_1 > r_2 > \cdots$, respectiv $\deg r_1 > \deg r_2 > \cdots$ care nu poate fi infinit, deci va exista un $n \in \mathbb{N}^*$ astfel încât $r_n \neq 0$ şi $r_{n+1} = 0$.

Să arătăm că r_n este un c.m.m.d.c. al elementelor $a, b \in R$. Deoarece $r_{n+1} = 0$ avem $r_{n-1} = r_n q_{n+1}$, deci $r_n \mid r_{n-1}$. Din relaţia $r_{n-2} = r_{n-1} q_n + r_n$ deducem că $r_n \mid r_{n-2}$. Astfel obţinem $r_n \mid r_i$ pentru orice $i = 1, \ldots, n$. Din relaţia $b = r_1 q_2 + r_2$ rezultă $r_n \mid b$ iar apoi din $a = bq_1 + r_1$ rezultă $r_n \mid a$. În concluzie, r_n este un divizor comun al lui a şi b.

Fie acum d un divizor comun al lui a şi b. Din relaţia $a = bq_1 + r_1$ deducem că $d \mid r_1$ şi pas cu pas obţinem $d \mid r_i$ pentru orice $i = 1, \ldots, n$. În particular, $d \mid r_n$.

În concluzie, c.m.m.d.c.(a, b) este ultimul rest nenul din algoritmul lui Euclid aplicat perechii (a, b).

Exemplul 1.14. Fie $a = 18$ şi $b = 24$. Avem $18 = 24 \cdot 0 + 18$, $24 = 18 \cdot 1 + 6$, $18 = 6 \cdot 3$. Aşadar $(18, 24) = 6$.

Exerciţiul 1.15. Calculaţi $(24, 54)$ în $\mathbb{Z}$ cu algoritmul lui Euclid.

Exerciţiul 1.16. Calculaţi (X^4-4X^3+1, X^3-3X^2+1) în $\mathbb{R}[X]$ cu algoritmul lui Euclid.

Propoziţia 1.17. *Fie $a,b,c \in R\setminus\{0\}$.*
(i) Dacă $d=(a,b)$, atunci există a',b' cu $a=da'$, $b=db'$ şi $(a',b')=1$.
(ii) $(ac,bc)=(a,b)c$.
(iii) $(a,b)=1$ şi $(a,c)=1$ implică $(a,bc)=1$.
(iv) (Lema lui Euclid) *$a \mid bc$ şi $(a,b)=1$ implică $a \mid c$.*
(v) $a \mid c$, $b \mid c$ şi $(a,b)=1$ implică $ab \mid c$.
(vi) Există $[a,b]$ şi $(a,b)[a,b]$ este asociat în divizibilitate cu ab.

Proof. (i) Fie $d'=(a',b')$. Deoarece $d' \mid a'$ şi $d' \mid b'$ rezultă că $dd' \mid a$ şi $dd' \mid b$, deci $dd' \mid d$ şi cum $d \neq 0$ obţinem $d' \mid 1$, adică $d' \sim 1$.
(ii) Egalitatea rezultă din algoritmul lui Euclid.
(iii) Fie $d=(a,bc)$. Din $d \mid a$ şi $a \mid ac$ rezultă că $d \mid ac$, deci $d \mid (ac,bc)$. Din (ii) obţinem $d \mid c$ şi cum $d \mid a$ rezultă $d \mid 1$.
(iv) Din (ii) avem că $(ac,bc)=c$. Dar $a \mid ac$ şi $a \mid bc$, deci $a \mid c$.
(v) Din (ii) avem că $(ac,bc)=c$. Dar $ab \mid ac$ şi $ab \mid bc$, deci $ab \mid c$.
(vi) Fie $d=(a,b)$. Atunci există a',b' cu $a=da'$, $b=db'$ şi $(a',b')=1$. Fie $m=da'b'$. Deoarece $m=ab'=ba'$ rezultă $a \mid m$ şi $b \mid m$. Fie $m' \in R$ astfel încât $a \mid m'$ şi $b \mid m'$. Avem că $a' \mid \frac{m'}{d}$ şi $b' \mid \frac{m'}{d}$. Din (v) rezultă $a'b' \mid \frac{m'}{d}$, deci $m \mid m'$. □

Propoziţia 1.18. *Orice ideal al lui R este principal.*

Proof. Fie I un ideal nenul al lui R. Fie $a \in I$, $a \neq 0$ cu $|a|$ minim dacă $R=\mathbb{Z}$, respectiv $\deg a$ minim dacă $R=K[X]$. Vom arăta că $I=aR$. Evident, $aR \subseteq I$. Reciproc, fie $b \in I$. Atunci $b=aq+r$ cu $0 \leq r < |a|$, respectiv $\deg r < \deg a$. Dar $r=b-aq \in I$ şi atunci neapărat $r=0$, deci $b=aq \in aR$. □

Propoziţia 1.19. *Fie $a,b \in R$. Avem:*
(i) $aR+bR=(a,b)R$;
(ii) $aR \cap bR=[a,b]R$.

Proof. (i) Deoarece R este inel principal, $aR+bR$ este ideal principal, deci există $d \in R$ cu proprietatea că $aR+bR=dR$. Cum $aR \subseteq dR$ şi $bR \subseteq dR$ rezultă $d \mid a$ şi $d \mid b$. Fie acum $d' \in R$ cu proprietatea că $d' \mid a$ şi $d' \mid b$, equivalent $aR \subseteq d'R$ şi $bR \subseteq d'R$. Avem $dR=aR+bR \subseteq d'R$, deci $d' \mid d$.
(ii) Deoarece R este inel principal, $aR \cap bR$ este ideal principal, deci există $m \in R$ cu proprietatea că $aR \cap bR=mR$. Cum $mR \subseteq aR$ şi $mR \subseteq bR$ rezultă $a \mid m$ şi $b \mid m$. Fie acum $m' \in R$ cu proprietatea că $a \mid m'$ şi $b \mid m'$, equivalent $m'R \subseteq aR$ şi $m'R \subseteq bR$. Avem $m'R \subseteq aR \cap bR=mR$, deci $m \mid m'$. □

Corolarul 1.20. *Fie $a,b \in R$ şi $d=(a,b)$. Atunci există $r,s \in R$ astfel încât $d=ar+bs$.*

Remarca 1.21. Folosind corolarul precedent putem da o altă demonstraţie propoziţiei 1.17.

Exerciţiul 1.22. Determinaţi $(X^2-1)\mathbb{Q}[X] \cap (X^3-1)\mathbb{Q}[X]$ şi $(X^2-1)\mathbb{Q}[X]+(X^3-1)\mathbb{Q}[X]$.

2. Elemente prime. Elemente ireductibile

În continuare R va desemna $\mathbb{Z}$ sau $K[X]$.

Definiţia 2.1. *(i) Un element $p \in R$ se numeşte* prim *dacă $p \neq 0$, $p \notin U(R)$ şi $p \mid ab$ implică $p \mid a$ sau $p \mid b$.*
(ii) Un element $q \in R$ se numeşte ireductibil *dacă $q \neq 0$, $q \notin U(R)$ şi $q = ab$ implică $a \in U(R)$ sau $b \in U(R)$.*
Un element care nu este ireductibil se numeşte reductibil.

Remarca 2.2. Un element asociat cu un element prim (ireductibil) este de asemenea element prim (ireductibil).

Propoziţia 2.3. *Orice element prim este ireductibil.*

Proof. Dacă $p \in R$ este element prim şi $p = ab$, atunci $p \mid ab$ şi de aici rezultă $p \mid a$ sau $p \mid b$. Să presupunem că $p \mid a$. Atunci există $a' \in R$ astfel încât $a = pa'$ şi înlocuind în $p = ab$ obţinem $p = pa'b$, de unde $1 = a'b$, deci $b \in U(R)$. □

Este adevărat şi reciproc.

Propoziţia 2.4. *Orice element ireductibil este prim.*

Proof. Fie $q \in R$ un element ireductibil. Să presupunem că $q \mid ab$. Fie $d = (q, a)$. Scriem $q = dq'$ şi $a = da'$. Deoarece q este ireductibil rezultă $d \in U(R)$ sau $q' \in U(R)$. În primul caz $1 = (q, a)$ şi din Lema lui Euclid obţinem $q \mid b$. În cazul al doilea $q = (q, a)$ şi astfel $q \mid a$. □

Remarca 2.5. (i) Un număr $p \in \mathbb{Z}$ este *prim* dacă $p \notin \{-1, 0, 1\}$ şi are ca divizori doar pe ± 1 şi $\pm p$.
(ii) Un polinom $f \in K[X]$ este *ireductibil* dacă nu se poate scrie ca produs de două polinoame de grad ≥ 1.

Definiţia 2.6. *Un număr întreg care nu este prim se numeşte* compus*, iar un polinom care nu este ireductibil se numeşte* reductibil.

Exemplul 2.7. (i) Numerele $\pm 2, \pm 3, \pm 5, \ldots$ sunt numere prime.
(ii) X este polinom ireductibil, iar X^2 este reductibil.

Propoziţia 2.8. *(i) Orice polinom de gradul întâi din $K[X]$ este ireductibil.*
(ii) Un polinom de grad 2 sau 3 din $K[X]$ este ireductibil dacă şi numai dacă nu are rădăcini în K.

Proof. (i) Evident.
(ii) În general, un polinom ireductibil $f \in K[X]$ nu are rădăcini în K. Aceasta rezultă imediat din lema lui Bézout. Reciproc, dacă $f \in K[X]$ cu $\deg f = 2, 3$ şi nu are rădăcini în K, atunci f este ireductibil, altminteri s-ar descompune într-un produs de două polinoame dintre care cel puţin unul are gradul 1. Dar orice polinom de grad 1 din $K[X]$ are o rădăcină în K, contradicţie. □

Exemplul 2.9. (i) Polinomul $X^2 - 2$ este ireductibil în $\mathbb{Q}[X]$, dar este reductibil în $\mathbb{R}[X]$.
(ii) Polinoamele $X^2 + X + 1$ şi $X^3 + X + 1$ sunt ireductibile în $\mathbb{Z}_2[X]$. Pe de altă

parte, polinomul X^4+X^2+1 nu are rădăcini în $\mathbb{Z}_2$, dar este reductibil în $\mathbb{Z}_2[X]$: $X^4+X^2+1=(X^2+X+1)^2$.

Exerciţiul 2.10. Determinaţi polinoamele ireductibile de grad ≤ 5 din $\mathbb{Z}_2[X]$.

Exerciţiul 2.11. Descompuneţi polinomul $X^{56}-X^{49}-X^7+1$ în produs de polinoame ireductibile în $\mathbb{Z}_7[X]$.

Propoziţia 2.12. *Fie $p\in R$ element prim. Atunci inelul factor R/pR este corp.*

Proof. Fie $\widehat{a}\in R/pR$, $\widehat{a}\neq\widehat{0}$. Aceasta înseamnă că $a\notin pR$, adică $p\nmid a$. Aşadar $(p,a)=1$. Atunci există $u,v\in R$ cu proprietatea că $pu+av=1$. Trecând la clase de resturi modulo idealul pR obţinem $\widehat{a}\,\widehat{v}=\widehat{1}$, deci $\widehat{a}$ este inversabil. □

Remarca 2.13. Rezultatul de mai sus ne ajută să construim corpuri finite. De exemplu, $\mathbb{Z}_2[X]/(X^2+X+1)$ este corp finit cu 4 elemente.

Propoziţia 2.14. *Dacă $a\in R$ este un element nenul şi neinversabil, atunci acesta admite o descompunere în produs finit de elemente prime şi această scriere este unică (până la o asociere în divizibilitate şi abstracţie făcând de ordinea factorilor).*

Proof. Existenţa. Presupunem că există $a\in R$ nenul şi neinversabil care nu se scrie ca produs de numere prime, respectiv ca produs de polinoame ireductibile. Îl alegem pe a de modul, respectiv grad minim cu această proprietate. Cum a nu poate fi număr prim, respectiv polinom ireductibil, există $a_1,a_2\in R$ nenule şi neinversabile astfel încât $a=a_1a_2$. Atunci $|a_i|<|a|$, respectiv $\deg a_i<\deg a$ pentru $i=1,2$. Datorită alegerii lui a, elementele a_1,a_2 se pot scrie ca produs de numere prime, respectiv ca produs de polinoame ireductibile. Dar atunci şi a este produs de numere prime, respectiv produs de polinoame ireductibile, contradicţie.
Unicitatea. Fie $a=p_1\cdots p_m=p_1'\cdots p_n'$ cu $p_i,p_j'\in R$ elemente prime. Vom demonstra (prin inducţie după m) că $m=n$ şi există $\sigma\in S_n$ astfel încât $p_i\sim p'_{\sigma(i)}$ pentru orice $i=1,\ldots,m$.
Dacă $m=1$, atunci $p_1=p_1'\cdots p_n'$. Deoarece p_1 este prim acesta este ireductibil şi rezultă că $n=1$.
Presupunem acum că $m>1$. Din $p_m\mid p_1'\cdots p_n'$ obţinem că există j astfel încât $p_m\mid p_j'$ şi cum p_j' este ireductibil rezultă $p_m\sim p_j'$. Să considerăm $j=n$, scriem $p_m=up_n'$ cu $u\in U(R)$ şi prin simplificare obţinem $p_1\cdots(up_{m-1})=p_1'\cdots p_{n-1}'$. Acum aplicăm ipoteza de inducţie şi deducem că $m-1=n-1$ şi există $\sigma'\in S_{n-1}$ astfel încât $p_i\sim p'_{\sigma'(i)}$ pentru orice $i=1,\ldots,m-1$. □

Corolarul 2.15. *Fie $a,b\in R$ nenule şi neinversabile. Dacă $a=\prod_{i=1}^r p_i^{k_i}$, $b=\prod_{i=1}^r p_i^{l_i}$, unde p_i sunt elemente prime, atunci $(a,b)=\prod_{i=1}^r p_i^{\min(k_i,l_i)}$ şi $[a,b]=\prod_{i=1}^r p_i^{\max(k_i,l_i)}$.*

Teorema 2.16. *Mulţimea numerelor prime pozitive, respectiv mulţimea polinoamelor ireductibile şi monice din $K[X]$ este infinită.*

Proof. Presupunem că mulţimea numerelor prime pozitive, respectiv mulţimea polinoamelor ireductibile şi monice din $K[X]$ este finită. Să notăm cu $p_1,\ldots,p_r$ elementele sale. Atunci $N=p_1\cdots p_r+1$ admite o descompunere în factori primi,

respectiv polinoame ireductibile şi de aici rezultă că există $i \in \{1, \ldots, r\}$ cu proprietatea că $p_i \mid N$. Dar cum $p_i \mid p_1 \cdots p_r$ rezultă $p_i \mid 1$, contradicţie. □

Exerciţiul 2.17. Determinaţi c.m.m.d.c. şi c.m.m.m.c. pentru polinoamele $f = (X-1)(X^2-1)(X^3-1)(X^4-1)$ şi $g = (X+1)(X^2+1)(X^3+1)(X^4+1)$ din $\mathbb{Q}[X]$.

3. Teorema fundamentală a algebrei

Teorema 3.1. (Teorema lui Kronecker) *Fie K un corp şi $f \in K[X]$ cu $\deg f \geq 1$. Atunci există o extindere L a lui K în care f are cel puţin o rădăcină.*

Proof. Deoarece f se descompune în produs de polinoame ireductibile este suficient să demonstrăm teorema pentru cazul în care f este ireductibil şi de grad ≥ 2. Fie $L = K[X]/(f)$. Ştim că L este corp iar morfismul canonic $K \to L$ este injectiv, deci putem considera că L este o extindere a lui K. Fie $\alpha = X \bmod (f)$ (clasa lui X modulo idealul (f)). Este imediat că $\alpha \in L$ şi $f(\alpha) = 0$. □

Corolarul 3.2. *Fie K un corp şi $f \in K[X]$ cu $\deg f \geq 1$. Atunci există o extindere L a lui K în care f are toate rădăcinile.*

Teorema 3.3. (Teorema fundamentală a algebrei) *Orice polinom $f \in \mathbb{C}[X]$ cu $\deg f \geq 1$ are cel puţin o rădăcină în $\mathbb{C}$.*

Corolarul 3.4. *(i) Fie $f \in \mathbb{C}[X]$ cu $\deg f \geq 1$. Atunci f este ireductibil dacă şi numai dacă $\deg f = 1$.*
(ii) Fie $f \in \mathbb{R}[X]$ cu $\deg f \geq 1$. Atunci f este ireductibil dacă şi numai dacă $\deg f = 1$ sau $\deg f = 2$ şi f nu are rădăcini reale.

Corolarul 3.5. *(i) Fie $f \in \mathbb{C}[X]$ cu $\deg f \geq 1$. Atunci f se scrie în mod unic sub forma*

$$f = a(X - a_1)^{k_1} \cdots (X - a_m)^{k_m}$$

cu $a \in \mathbb{C}^\times$, $a_1, \ldots, a_m \in \mathbb{C}$ distincte şi $k_1, \ldots, k_m \in \mathbb{N}^*$.
(ii) Fie $f \in \mathbb{R}[X]$ cu $\deg f \geq 1$. Atunci f se scrie în mod unic sub forma

$$f = a(X - a_1)^{k_1} \cdots (X - a_r)^{k_r}(X^2 + b_1X + c_1)^{l_1} \cdots (X^2 + b_sX + c_s)^{l_s}$$

cu $a \in \mathbb{R}^\times$, $a_1, \ldots, a_r \in \mathbb{R}$ distincte, $b_1, c_1, \ldots, b_s, c_s \in \mathbb{R}$ cu $b_i^2 < 4c_i$ pentru orice $i = 1, \ldots, s$ şi $k_1, \ldots, k_r, l_1, \ldots, l_s \in \mathbb{N}^*$.

Remarca 3.6. În $\mathbb{Q}[X]$ există polinoame ireductibile de orice grad. De exemplu, polinomul $X^n - 2$ este ireductibil în $\mathbb{Q}[X]$ pentru orice $n \geq 1$.

Exerciţiul 3.7. Arătaţi că polinomul $X^n - 2$ este ireductibil în $\mathbb{Q}[X]$ pentru orice $n \geq 1$.

Exerciţiul 3.8. Descompuneţi polinomul $X^n - 1$, $1 \leq n \leq 6$, în produs de polinoame ireductibile în $\mathbb{Q}[X]$, $\mathbb{R}[X]$, respectiv $\mathbb{C}[X]$.