

CURS I

NOȚIUNI PRELIMINARE

§ 1. MULȚIMI

Prin *mulțime* înțelegem o colecție de obiecte care se numesc elementele mulțimii. Vom nota cu litere mari mulțimile, iar cu litere mici elementele lor. Dacă A este o mulțime și x un element al său, vom scrie $x \in A$ și vom citi „ x aparține lui A ”. Dacă x nu se găsește în A , atunci vom scrie $x \notin A$ și vom citi „ x nu aparține lui A ”.

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

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

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

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

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

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

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

Mulțimea vidă este submulțime a oricărei mulțimi. Între mulțimile 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 mulțimi A și B sunt *egale* dacă au aceleași elemente, adică $A = B \Leftrightarrow A \subseteq B$ și $B \subseteq A$ („ \Leftrightarrow ” înseamnă „dacă și numai dacă”).

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

- a) este reflexivă, adică $A \subseteq A$ (resp. $A = A$);
- b) este antisimetrică, adică din $A \subseteq B$ și $B \subseteq A$ rezultă $A = B$ (resp. este simetrică adică $A = B \Rightarrow B = A$);
- c) este tranzitivă, adică $A \subseteq B$ și $B \subseteq C \Rightarrow A \subseteq C$ (resp. $A = B$ și $B = C \Rightarrow A = C$).

Cu mulțimi se fac următoarele operații:

- *intersecția* a două mulțimi A și B înseamnă mulțimea

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

- *reuniunea* mulțimilor A și B înseamnă mulțimea

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

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

Operațiile de intersecție și reuniune au următoarele proprietăți:

$$A \cup \emptyset = A; A \cap \emptyset = \emptyset$$

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

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

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

$$A \subseteq B \text{ dacă și numai dacă } A \cup B = B; A \subseteq B \text{ dacă și numai dacă } A \cap B = A$$

Operațiile de intersecție și reuniune satisfac egalitățile:

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

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

numite *distributivitatea intersecției (resp. reuniunii) față de reuniune (resp. intersecție)*.

Prin *diferența* mulțimilor B și A înțelegem mulțimea

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

Să observăm că $A \subseteq B$ dacă și numai dacă $A \setminus B = \emptyset$.

Dacă A este o submulțime a lui B, atunci diferența $B \setminus A$ se numește *complementara* mulțimii A în B și se notează cu $C_B A$. De exemplu $C_B \emptyset = B$, iar $C_B B = \emptyset$. De asemenea, $A \cup C_B A = B$, iar $A \cap C_B A = \emptyset$, adică A și $C_B A$ sunt disjuncte.

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

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

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

numite *formulele lui De Morgan*.

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

Fie A și B două mulțimi arbitrare. Dacă $a \in A$ și $b \in B$, atunci putem forma *perechea ordonată* (a, b), adică perechea formată din elementele a și b unde este stabilită o anumită ordine în sensul că a este primul element iar b este al doilea element în această pereche. Rezultă că două perechi (a₁, b₁) și (a₂, b₂) sunt egale dacă și numai dacă a₁ = a₂ și b₁ = b₂. Prin *produsul cartezian* al mulțimilor A și B înțelegem mulțimea

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

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 mulțimea $A \times B$ are mn elemente.

§ 2. FUNCȚII

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

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

O funcție f este determinată atunci când se dă domeniul de definiție, codomeniul său și modul cum acționează f . O funcție f definită pe mulțimea A cu valori în B se notează $f : A \rightarrow B$.

Fie $f : A \rightarrow B$ o funcție. Prin *graficul* lui f se înțelege mulțimea $G_f = \{(a, b) \mid a \in A, b \in B \text{ și } b = f(a)\}$. Evident $G_f \subseteq A \times B$. Dacă știm graficul unei funcții, atunci putem identifica domeniul, codomeniul și „legea” funcției. De aceea este mult mai riguros să definim o funcție ca un triplet (A, B, G) format din trei mulțimi A, B și $G \subseteq A \times B$ cu proprietatea că $\forall a \in A \exists! b \in B$ astfel încât $(a, b) \in G$.

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

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

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

O funcție $f : A \rightarrow B$ se numește *restricție* a funcției $g : A' \rightarrow B$ dacă $A \subseteq A'$ și $f(a) = g(a)$, oricare ar fi $a \in A$. (Să observăm că $f = g \circ i$, unde $i : A \rightarrow A'$ este funcția incluziune.) f se notează cu $g|_A$. În această situație g se numește *extindere* a lui f .

O funcție $f : A \rightarrow B$ se numește *corestricție* a funcției $g : A \rightarrow B'$ dacă $\text{Im } g \subseteq B \subseteq B'$ și $f(a) = g(a)$, oricare ar fi $a \in A$.

Dacă A_1 și A_2 sunt două mulțimi oarecare, definim o funcție $p_1 : A_1 \times A_2 \rightarrow A_1$ prin $p_1((a_1, a_2)) = a_1$ oricare ar fi $(a_1, a_2) \in A_1 \times A_2$. Această funcție se numește *proiecția pe prima componentă*. Analog definim o funcție $p_2 : A_1 \times A_2 \rightarrow A_2$ prin $p_2((a_1, a_2)) = a_2$ oricare ar fi $(a_1, a_2) \in A_1 \times A_2$ și o numim *proiecția pe a doua componentă*.

Dacă A_1, A_2, B_1, B_2 sunt mulțimi oarecare și $f_1 : A_1 \rightarrow B_1, f_2 : A_2 \rightarrow B_2$ sunt două funcții, atunci putem defini o funcție $f_1 \times f_2 : A_1 \times A_2 \rightarrow B_1 \times B_2$ 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 funcție se numește *produsul cartezian* al lui f_1 cu f_2 .

Dacă A și T sunt două mulțimi și $A \subseteq T$, definim o funcție $\chi_A : T \rightarrow \{0, 1\}$ astfel: $\chi_A(t) = 1$ dacă $t \in A$, respectiv $\chi_A(t) = 0$ dacă $t \in T \setminus A$. Această funcție se numește *funcția caracteristică* a lui A .

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

Exercițiu. Fie A și A' submulțimi ale lui T . Arătați 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 și A' sunt disjuncte avem $\chi_{A \cup A'} = \chi_A + \chi_{A'}$.
- 3) $\chi_{A \setminus A'} = \chi_A(1 - \chi_{A'})$.

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

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

numită *imaginea directă* a lui A' prin funcția f și este o submulțime a lui B . În cazul particular când $A' = A$, notăm $f(A) = \text{Im } f$ și se numește *imaginea* funcției f .

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

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

Această submulțime se numește *imaginea inversă* a lui B' prin funcția f și este o submulțime a lui A .

Propoziția 2.1. Considerăm o funcție $f : A \rightarrow B$.

- a) Dacă $M \subseteq N \subseteq A$, atunci $f(M) \subseteq f(N)$.
- b) Dacă $M \subseteq A$ și $N \subseteq A$, atunci $f(M \cup N) = f(M) \cup f(N)$.
- c) Dacă $M \subseteq A$ și $N \subseteq A$, 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 $P \subseteq B$ și $Q \subseteq B$, atunci $f^{-1}(P \cup Q) = f^{-1}(P) \cup f^{-1}(Q)$.
- g) Dacă $P \subseteq B$ și $Q \subseteq B$, atunci $f^{-1}(P \cap Q) = f^{-1}(P) \cap f^{-1}(Q)$.
- h) Dacă $P \subseteq B$, atunci $f(f^{-1}(P)) \subseteq P$.

Exerciții.

1) Dați exemple de funcții $f : A \rightarrow B$ cu proprietatea că există $M \subseteq A$ și $N \subseteq A$ astfel încât $f(M \cap N) \subset f(M) \cap f(N)$.

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

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

O funcție $f : A \rightarrow B$ se numește *injectivă* dacă oricare ar fi $a, a' \in A$ cu $a \neq a'$ rezultă $f(a) \neq f(a')$ sau echivalent, din egalitatea $f(a) = f(a')$ rezultă $a = a'$.

Propoziția 2.2. (i) O funcție $f : A \rightarrow B$ este injectivă dacă și numai dacă $\forall M \subseteq A$ și $\forall N \subseteq A$, $f(M \cap N) = f(M) \cap f(N)$.

(ii) O funcție $f : A \rightarrow B$ este injectivă dacă și numai dacă $M = f^{-1}(f(M)) \quad \forall M \subseteq A$

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

Propoziția 2.3. O funcție $f : A \rightarrow B$ este surjectivă dacă și numai dacă $f(f^{-1}(P)) = P$, $\forall P \subseteq B$.

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

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

Dacă $f : A \rightarrow B$ este o funcție, atunci sunt evidente egalitățile:

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

O proprietate importantă a compunerii funcțiilor este următoarea:

Teorema 2.4. Compunerea funcțiilor este asociativă, adică fiind date funcțiile $f : A \rightarrow B$, $g : B \rightarrow C$ și $h : C \rightarrow D$ are loc egalitatea

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

Demonstrație. Într-adevăr, se vede mai întâi că funcțiile $h \circ (g \circ f)$ și $(h \circ g) \circ f$ au domeniul de definiție 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 $h \circ (g \circ f) = (h \circ g) \circ f$.

Propoziția 2.5. Fie funcțiile $f : A \rightarrow B$ și $g : B \rightarrow C$.

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

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

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

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

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

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

Demonstrație. a) Fie $a, a' \in A$ astfel încât $(g \circ f)(a) = (g \circ f)(a')$. Atunci avem că $g(f(a)) = g(f(a'))$ și cum g este injectivă rezultă $f(a) = f(a')$, de unde obținem 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 obținem că $a = a'$. Deci f este o funcție 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 $c \in C$ și $a \in A$ 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.

Exercițiu. Dați exemplul de funcții $f, g : \mathbb{N} \rightarrow \mathbb{N}$ cu proprietatea că $g \circ f = 1_{\mathbb{N}}$, dar g nu este injectivă, iar f nu este surjectivă.

O funcție $f : A \rightarrow B$ se numește *inversabilă* dacă există o funcție $g : B \rightarrow A$ astfel încât $g \circ f = 1_A$ și $f \circ g = 1_B$.

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

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

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

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

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

2) Avem

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

și

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

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

Următoarea teoremă caracterizează funcțiile inversabile:

Teorema 2.7. Dacă $f : A \rightarrow B$ este o funcție, atunci f este inversabilă dacă și numai dacă f este bijectivă.

Demonstrație. Presupunem că f este inversabilă. Atunci există o funcție $g : B \rightarrow A$

astfel încât $g \circ f = 1_A$ și $f \circ g = 1_B$. Din Propoziția 2.5 b) rezultă că f este injectivă iar din Propoziția 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 funcția $g : B \rightarrow A$ astfel: $g(b) = a_b$. Se verifică imediat că $g \circ f = 1_A$ și $f \circ g = 1_B$.

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

Teorema 2.8. Fie A o mulțime finită și $f : A \rightarrow A$ o funcție. Următoarele afirmații sunt echivalente:

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

Demonstrație. 1) \Rightarrow 2) și 1) \Rightarrow 3) sunt evidente.

2) \Rightarrow 1) Deoarece A este o mulțime finită, 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 $f(A) = A$ și deci f este și surjectivă, adică bijectivă.

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

Deoarece $A = \bigcup_{b \in A} f^{-1}(b)$ și mulțimile $f^{-1}(b)$ sunt disjuncte două 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 mulțimea A . Aceasta ne arată că f este neapărat o funcție injectivă.

§ 3. PRODUSUL CARTEZIAN AL UNEI FAMILII DE MULȚIMI

Fie $I \neq \emptyset$ și A o mulțime oarecare. O funcție $\varphi : I \rightarrow A$ se mai numește *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 notația $(a_i)_{i \in I} = (a_1, a_2, \dots, a_n)$ și (a_1, a_2, \dots, a_n) se mai numește *n-uplu*.

Dacă elementele lui A sunt mulțimi (sau submulțimi ale unei mulțimi T) obținem noțiunea de *familie de mulțimi* (respectiv *familie de submulțimi* a lui T).

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

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

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

Avem egalitățile:

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

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

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

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

se numește *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 mulțimea $A^I = \{\varphi : I \rightarrow A\}$, adică mulțimea funcțiilor 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 $n = 2$ obținem produsul cartezian a două mulțimi introdus în §1. Dacă $A_1 = A_2 = \dots = A_n = A$ vom nota $A^n = A_1 \times A_2 \times \dots \times A_n$.

Fie $j \in I$. Funcția $p_j : \prod_{i \in I} A_i \rightarrow A_j$, 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 numește *j-proiecția canonică* a produsului cartezian pe mulțimea A_j . Aceasta este în mod evident o funcție surjectivă.

Fie $(A_i)_{i \in I}$, $(B_i)_{i \in I}$ două familii de mulțimi și $f_i : A_i \rightarrow B_i$ o familie de funcții. Definim o funcție $\prod_{i \in I} f_i : \prod_{i \in I} A_i \rightarrow \prod_{i \in I} B_i$ prin $(\prod_{i \in I} f_i)((a_i)_{i \in I}) = (f_i(a_i))_{i \in I}$. Această funcție se numește *produsul cartezian* al familiei de funcții $(f_i)_{i \in I}$.

În teoria mulțimilor se admite următoarea axiomă:

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

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

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

CURS II

§ 4. RELAȚII DE ECHIVALENȚĂ

Fie A și B două mulțimi. O submulțime $\rho \subseteq A \times B$ se numește *relație binară* între A și B . Dacă $(a, b) \in \rho$, unde $a \in A$ și $b \in B$, spunem că *a este în relația ρ cu b* și notăm $a \rho b$. Când scriem $a \not\rho b$ înseamnă că elementele $a \in A$ și $b \in B$ nu sunt în relația ρ .

Exemple.

1) Dacă $f : A \rightarrow B$ este o funcție, atunci mulțimea $G_f = \{(a, b) \mid a \in A, b \in B \text{ și } b = f(a)\}$ este o relație binară între A și B . Mulțimea G_f se numește *graficul* funcției f . Invers, dacă $G \subseteq A \times B$ este o relație între A și 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 funcția $f : A \rightarrow B$ așa încât $f(a) = b$. Se observă imediat că $G_f = G$.

2) Fie A o mulțime nevidă și $\rho = \{(a, X) \in A \times \mathcal{P}(A) \mid a \in X\}$. Aceasta este relația de apartenență între elementele lui A și submulțimile lui A . Dacă $a \in A$ și $X \in \mathcal{P}(A)$, atunci $a \rho X$ este echivalent cu $a \in X$.

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

Exemple.

1) Fie A o mulțime oarecare. Mulțimea $\Delta_A = \{(a, a) \mid a \in A\}$ se numește *diagonală* mulțimii A și este o relație binară pe A .

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

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

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

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

- i) $a \rho a$ (reflexivitate);
- ii) $a \rho b \Rightarrow b \rho a$ (simetrie);
- iii) $a \rho b$ și $b \rho c \Rightarrow a \rho c$ (tranzitivitate).

Exemple.

1) Dacă se consideră mulțimea numerelor întregi \mathbb{Z} și $n \geq 1$ un număr natural, atunci relația binară notată „ $\equiv \pmod{n}$ ” (*congruența modulo n*):

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

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

2) Dacă se consideră pe mulțimea \mathbf{R} a numerelor reale relația „ \sim ”:

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

aceasta este o relație de echivalență pe \mathbf{R} .

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

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

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

Clasa de echivalență a elementului a se mai notează și astfel: \hat{a} , \tilde{a} , \bar{a} , etc.

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

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

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

3) Dacă $[a]$ și $[b]$ sunt două clase de echivalență, atunci

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

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

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

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

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

4) Rezultă din 1).

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

i) oricare ar fi $i \neq j$, $a_i \not\rho a_j$.

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

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

Fiind dată o relație de echivalență „ ρ ” pe mulțimea nevidă A , există întotdeauna un sistem de reprezentanți asociat relației „ ρ ”. Într-adevăr, fie $(C_i)_{i \in I}$ mulțimea tuturor claselor de echivalență asociate relației „ 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 reprezentanți pentru relația „ ρ ”. Trebuie să observăm că acest sistem de reprezentanți nu este unic.

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

Exemplu. Pe mulțimea \mathbf{Z} a numerelor întregi considerăm relația „ \sim ”:

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

Se observă imediat că „ \sim ” este o relație de echivalență pe \mathbf{Z} . Dacă $a \in \mathbf{Z}$ avem: $[a] = \{a, -a\}$, dacă $a \neq 0$ și $[a] = \{0\}$, dacă $a = 0$. Un sistem de reprezentanți poate fi considerat sistemul de numere: 0, 1, 2, 3, ..., adică mulțimea numerelor naturale \mathbf{N} . Un alt sistem de reprezentanți poate fi considerat și sistemul de numere 0, -1, -2, -3, ..., adică mulțimea numerelor întregi negative.

Definiția 4.4. Dată relația de echivalență „ ρ ” pe A , mulțimea claselor de echivalență determinate de „ ρ ” pe A se notează cu A/ρ și se numește *mulțimea factor* (sau *mulțimea cât*) a lui A prin relația „ ρ ”. Funcția $p : A \rightarrow A/\rho$, $p(a) = [a]$, este o funcție surjectivă și se numește *proiecția (surjecția) canonică* a lui A pe mulțimea factor A/ρ .

Definiția 4.5. O *partiție* a unei mulțimi nevide A este o familie de submulțimi nevide disjuncte două câte două ale lui A și a cărei reuniune este A .

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

Mulțimea factor A/ρ este o partiție a lui A , deci o relație de echivalență pe A dă naștere unei partiții. Reciproc, dacă $(A_i)_{i \in I}$ este o partiție a lui A definim o relație de echivalență pe A astfel: $a \sim b$ dacă și numai dacă există $i \in I$ astfel încât $a, b \in A_i$. Clasele de echivalență ale lui „ \sim ” sunt chiar submulțimile A_i . Așadar putem enunța următorul rezultat:

Propoziția 4.6. Dacă A este o mulțime nevidă, atunci asocierea $\rho \rightarrow A/\rho$ definește o bijecție de la mulțimea relațiilor de echivalență pe A la mulțimea partițiilor lui A .

Demonstrație. Exercițiu.

Definiția 4.7. Fie $f : A \rightarrow B$ o funcție. Definim pe A o relație ρ_f astfel:

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

ρ_f se numește *relația asociată funcției f* .

Se observă că ρ_f este o relație de echivalență pe A , iar mulțimea factor A/ρ_f se descrie astfel:

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

Exemplu. Relația de echivalență pe \mathbf{R} asociată funcției $f : \mathbf{R} \rightarrow \mathbf{C}$, $f(x) = \cos(2\pi x) + i \sin(2\pi x)$ este următoarea: $x \rho_f y$ dacă și numai dacă $x - y \in \mathbf{Z}$.

Teorema 4.8. (Proprietatea de universalitate a mulțimilor factor) Fie A o mulțime nevidă și „ ρ ” o relație de echivalență pe A . Fie $f : A \rightarrow B$ o funcție și „ ρ_f ” relația de

echivalență pe A asociată funcției f . Dacă $\rho \subseteq \rho_f$, atunci există o unică funcție $\bar{f}: A/\rho \rightarrow B$ cu proprietatea că $\bar{f} \circ p = f$. Mai mult:

- 1) \bar{f} este injectivă $\Leftrightarrow \rho = \rho_f$.
- 2) \bar{f} este surjectivă $\Leftrightarrow f$ este surjectivă.

Demonstrație. Definim $\bar{f}: A/\rho \rightarrow B$ astfel: $\bar{f}([a]) = f(a)$. Mai întâi vom arăta că funcția este bine definită, adică $[a] = [b]$ implică $\bar{f}([a]) = \bar{f}([b])$. Deoarece $[a] = [b]$ rezultă că $a \rho b$ și cum $\rho \subseteq \rho_f$ obținem $a \rho_f b$, deci $f(a) = f(b)$. Este clar acum că $\bar{f} \circ p = f$. Din această relație rezultă și unicitatea funcției \bar{f} .

- 1) \bar{f} este injectivă dacă și numai dacă $\bar{f}([a]) = \bar{f}([b]) \Rightarrow [a] = [b]$. Dar $\bar{f}([a]) = \bar{f}([b]) \Leftrightarrow f(a) = f(b) \Leftrightarrow a \rho_f b$ și ca să obținem $[a] = [b]$ trebuie ca $\rho_f \subseteq \rho$, deci egalitate.
- 2) Se observă că $\text{Im } \bar{f} = \text{Im } f$.

CURS III

LEGI DE COMPOZIȚIE. MONOIZI

§1. OPERAȚIE ALGEBRICĂ INTERNĂ

Definiția 1.1. Fiind dată o mulțime nevidă M , se numește *operație algebrică internă* sau *lege de compoziție* definită pe M orice funcție

$$\varphi : M \times M \rightarrow M,$$

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

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

Exemple.

1) Adunarea și înmulțirea în mulțimea \mathbf{N} a numerelor naturale, în mulțimea \mathbf{Z} a numerelor întregi, în mulțimea \mathbf{Q} a numerelor raționale, în mulțimea \mathbf{R} a numerelor reale și în mulțimea \mathbf{C} a numerelor complexe sunt operații algebrice.

2) În mulțimea \mathbf{Z} a numerelor întregi, scăderea este o operație algebrică. Ea este definită astfel:

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

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

De asemenea, scăderea este operație algebrică și pe mulțimile: \mathbf{Q} , \mathbf{R} , \mathbf{C} . Însă pe mulțimea \mathbf{N} a numerelor naturale scăderea nu este operație algebrică, deoarece rezultatul acesteia nu este întotdeauna un număr natural.

3) Dacă M este o mulțime, pe mulțimea

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

a funcțiilor de la M la M putem defini operația algebrică de compunere. Reamintim că dacă $f, g \in \mathcal{F}(M)$, atunci se definește compunerea $g \circ f$ ca fiind funcția

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

4) Dacă M este o mulțime nevidă, iar

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

este mulțimea părților lui M , atunci reuniunea

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

și intersecția

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

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

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

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

$$([a], [b]) \rightarrow [ab] \text{ (numită înmulțire).}$$

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

La fel se arată că dacă $a \equiv a_1 \pmod{n}$ și $b \equiv b_1 \pmod{n}$, atunci $[ab] = [a_1 b_1]$ și deci operația de înmulțire este bine definită.

Deseori, dacă $\varphi : M \times M \rightarrow M$ este o operație algebrică pe mulțimea M , în loc de $\varphi(x, y)$ se folosește ca și în exemplele de mai înainte, o altă notație, ca de exemplu: $x * y$, $x \circ y$, $x \perp y$, $x \top y$, $x + y$, xy , etc.

O mulțime nevidă M înzestrată cu o operație algebrică " $*$ " o notăm, uneori, prin perechea $(M, *)$, punând în evidență mulțimea și operația algebrică.

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

Dăm câteva proprietăți ale operațiilor algebrice, cu ajutorul cărora se definesc structurile de bază ale algebrei.

Asociativitatea. Fie $M \neq \emptyset$ o mulțime și $\varphi : M \times M \rightarrow M$ o operație algebrică pe mulțimea M . Se spune că φ este o operație 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 condiția 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 operație algebrică *neasociativă*.

Exemple.

1) Operațiile algebrice de adunare și înmulțire pe mulțimile de numere \mathbf{N} , \mathbf{Z} , \mathbf{Q} , \mathbf{R} , \mathbf{C} sunt asociative.

2) Scăderea numerelor pe \mathbf{Z} nu este asociativă; de exemplu

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

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

4) Reuniunea și intersecția pe $\mathcal{P}(M)$ sunt operații algebrice asociative.

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

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

și

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

Comutativitatea. Fie $M \neq \emptyset$ o mulțime și $\varphi : M \times M \rightarrow M$ o operație algebrică pe mulțimea M . Se spune ca φ este o operație 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, condiția 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 operație algebrică *necomutativă*.

Exemple.

1) Operațiile algebrice de adunare și înmulțire pe mulțimile de numere $\mathbf{N}, \mathbf{Z}, \mathbf{Q}, \mathbf{R}, \mathbf{C}$ sunt comutative.

2) Scăderea numerelor pe \mathbf{Z} este necomutativă; de exemplu

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

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

4) Reuniunea și intersecția pe $\mathcal{P}(M)$ sunt operații algebrice comutative.

5) Adunarea și înmulțirea pe \mathbf{Z}_n sunt operații algebrice comutative.

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

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

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

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

Să presupunem că e și e' sunt elemente neutre pentru această operație algebrică. Atunci avem

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

Deci elementul neutru, dacă există, este unic determinat.

Dacă folosim scrierea aditivă, elementul neutru se numește *elementul nul* sau *elementul zero* sau chiar *zero* și se notează de obicei cu 0. Cu această notație, condiția elementului zero devine

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

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

Cu aceste notații, condiția elementului unitate devine

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

Exemple.

1) Pentru operația de adunare în \mathbf{N} , \mathbf{Z} , \mathbf{Q} , \mathbf{R} , \mathbf{C} , numărul 0 este element neutru, iar pentru operația de înmulțire a numerelor, numărul 1 este element neutru.

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

3) Pentru operația de reuniune (respectiv intersecție) pe mulțimea $\mathcal{P}(M)$ a părților unei mulțimi M , mulțimea vidă \emptyset (respectiv mulțimea M) este element neutru.

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

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

Elemente simetrizabile. Fie $M \neq \emptyset$ o mulțime și φ o operație algebrică pe M care are un element neutru e . Fie $x \in M$. Se spune că x este *simetrizabil* față de operația dată dacă există un element $x' \in M$ astfel încât

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

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

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

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

În acest caz se spune că x este *opozabil* față de operația dată.

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

$$x \cdot x' = x' \cdot x = 1.$$

În acest caz se spune că x este *inversabil* față de operația dată.

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

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

Propoziția 1.2. Se consideră $M \neq \emptyset$ o mulțime înzestrată cu o operație algebrică asociativă $*$: $M \times M \rightarrow M$, $(x, y) \rightarrow x * y$ și cu element neutru e . Dacă elementul $x \in M$ este simetrizabil, atunci acesta are un unic element simetric.

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

Observație. Faptul că operația este asociativă este esențial pentru unicitatea elementului simetric. Mai precis, dacă operația nu este asociativă, nu rezultă unicitatea elementului simetric. Să luăm mulțimea $M = \{e, a, b\}$ și să definim pe M o operație 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 operație 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 și pe b .

În condițiile de mai înainte, dacă x este un element simetrizabil pentru o operație asociativă, simetricul său, unic determinat, se notează cu x^{-1} dacă folosim scrierea multiplicativă și se numește *inversul lui x* , și se notează $-x$ dacă folosim scrierea aditivă și se numește *opusul lui x* .

Exemple.

1) În mulțimea \mathbf{N} a numerelor naturale, numai 0 (elementul neutru) are un opus față de operația de adunare și numai 1 are invers față de operația de înmulțire. În mulțimea \mathbf{Z} a numerelor întregi, față de adunare orice element are un opus, iar față de înmulțire doar 1 și -1 au invers. În \mathbf{Q} , \mathbf{R} și \mathbf{C} față de adunare orice element are un opus, iar față de înmulțire orice element nenul are un invers.

2) În mulțimea $\mathcal{F}(M)$, cu operația algebrică de compunere a funcțiilor, elementele inversabile sunt funcțiile bijective.

3) În mulțimea $\mathcal{P}(M)$, față de reuniune numai mulțimea vidă \emptyset are un simetric, iar față de intersecție numai mulțimea M are un simetric.

4) În mulțimea $\mathbf{Z}_n = \{[0], [1], \dots, [n-1]\}$ cu operația algebrică de adunare, oricare ar fi $[a] \in \mathbf{Z}_n$ are un opus și anume $[-a] \in \mathbf{Z}_n$. Dacă considerăm \mathbf{Z}_n cu operația algebrică de înmulțire avem:

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

Demonstrație. Într-adevăr, dacă $[a]$ este inversabil, atunci există $[b] \in \mathbf{Z}_n$ astfel încât $[a][b] = [1]$, echivalent $[ab] = [1]$ și deci $n \mid ab - 1$. Atunci există $k \in \mathbf{Z}$ astfel încât $ab - 1 = kn$ sau $ab + n(-k) = 1$ și 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 $[n] = [0]$ și 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

Definiția 2.1. O mulțime nevidă M înzestrată cu o operație algebrică asociativă și cu element neutru se numește *monoid*. Dacă, în plus, operația algebrică este comutativă, monoidul se numește *comutativ*.

Exemple.

1) Mulțimea \mathbf{N} a numerelor naturale față de adunarea obișnuită formează un monoid comutativ. De asemenea, mulțimea \mathbf{N} cu înmulțirea obișnuită este monoid comutativ. Mulțimile \mathbf{Z} , \mathbf{Q} , \mathbf{R} , \mathbf{C} față de adunarea obișnuită, cât și față de înmulțirea obișnuită, formează monoizi comutativi.

2) Mulțimea $\mathcal{F}(M)$ a funcțiilor definite pe mulțimea M cu valori în M , cu operația de compunere, formează un monoid, în general, necomutativ.

3) Mulțimea $\mathcal{P}(M)$ a părților unei mulțimi M cu operația de reuniune (intersecție) formează monoid comutativ.

4) Mulțimea \mathbf{Z}_n a claselor de resturi modulo n cu operația de adunare, ca și separat, cu cea de înmulțire este monoid comutativ.

Reguli de calcul într-un monoid

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

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

Observație. Se poate arăta cu ușurință, prin inducție, că pentru $k, 0 < k < n$, are loc relația

$$a_1 a_2 \dots a_n = (a_1 a_2 \dots a_k)(a_{k+1} a_{k+2} \dots a_n). \quad (1)$$

Lăsăm demonstrația ca exercițiu.

În cazul particular în care $a_1 = a_2 = \dots = a_n = a$, în loc de $a_1 a_2 \dots a_n$ 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 relația (1) deducem

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

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

Prin inducție, se demonstrează ușor că

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

Dacă în locul scrierii multiplicative folosim scrierea aditivă, atunci în loc de $a_1 a_2 \dots a_n$, se va scrie $a_1 + a_2 + \dots + a_n$ iar relația (1) devine $a_1 + a_2 + \dots + a_n = (a_1 + \dots + a_k) + (a_{k+1} + \dots + a_n)$. De asemenea, în loc de a^n se scrie na și deci $1 \cdot a = a$, iar dacă $n = 0$, convenția devine $0 \cdot a = 0$. Celelalte relații devin respectiv

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

Morfisme de monoizi

Definiția 2.2. Dacă M și N sunt doi monoizi (notați multiplicativ), se numește *morfism de monoizi* o funcție $f : M \rightarrow N$ astfel încât

- 1) $f(xy) = f(x)f(y)$, oricare ar fi $x, y \in M$;
- 2) $f(e) = e'$, unde e și e' sunt respectiv, elementele unitate ale lui M și N .

Exemple.

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

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

este un morfism de monoizi.

Lăsăm ca exercițiu demonstrația faptului că orice morfism de monoizi de la monoidul $(\mathbf{N}, +)$ în el însuși este de acest tip. Mai precis, dacă $f : \mathbf{N} \rightarrow \mathbf{N}$ 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 $(\mathcal{P}(M), \cap)$ și $(\mathcal{P}(M), \cup)$ sunt monoidul părților mulțimii M cu intersecția și respectiv cu reuniunea, atunci funcția

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

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

Într-adevăr,

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

și

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

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

Observație. Se poate demonstra prin inducție că dacă $x_1, x_2, \dots, x_n \in M$, atunci pentru orice morfism de monoizi $f : M \rightarrow N$ avem

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

În particular,

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

Compunerea morfismelor de monoizi

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

2) Dacă M este un monoid, funcția identică 1_M a mulțimii 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 $f : M \rightarrow N$ este morfism de monoizi, atunci

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

Izomorfisme de monoizi

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

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

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

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

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

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

Observație. Relația de izomorfism între monoizi este o relație de echivalență:

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

2) Dacă monoidul M este izomorf cu monoidul N , atunci și 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).

Observație. Noțiunea de izomorfism este fundamentală în algebră. Din punct de vedere algebric două structuri algebrice izomorfe sunt la fel, deosebiriile dintre ele ținând doar de natura elementelor și a operației. Două structuri algebrice izomorfe se pot identifica.

Propoziția 2.3. Fie $f : M \rightarrow N$ un morfism de monoizi. Atunci f este izomorfism de monoizi dacă și numai dacă funcția f este bijectivă.

Demonstrație. Este cunoscut că o funcție este inversabilă dacă și numai dacă este bijectivă. De aici rezultă în mod evident că dacă f este izomorfism, atunci funcția f este bijectivă.

Reciproc, dacă f este bijectivă, atunci există o funcție $g : N \rightarrow M$ astfel încât $f \circ g = 1_N$ și $g \circ f = 1_M$. 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 $f(g(yy')) = f(g(y)g(y'))$ și 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 $f(e) = e'$ și deci $g(e') = e$.

Exemplu. Morfismul de monoizi

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

este izomorfism.

Produs direct de monoizi

Fie M_1 și M_2 doi monoizi. Pe produsul cartezian $M = M_1 \times M_2$ al mulțimilor M_1 și M_2 introducem următoarea operație algebrică:

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

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

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

$$\begin{aligned} (x_1, x_2)[(y_1, y_2)(z_1, z_2)] &= (x_1, x_2)(y_1 z_1, y_2 z_2) = (x_1(y_1 z_1), x_2(y_2 z_2)) = \\ &= ((x_1 y_1) z_1, (x_2 y_2) z_2) = (x_1 y_1, x_2 y_2)(z_1, z_2) = [(x_1, x_2)(y_1, y_2)](z_1, z_2). \end{aligned}$$

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

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

și

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

Monoidul M se numește *produs direct* al monoizilor M_1 și M_2 . Mai mult, dacă M_1 și M_2 sunt monoizi comutativi, atunci, de asemenea, M este monoid comutativ.

Construcția 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 operație algebrică:

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

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

Monoidul liber generat de o mulțime

Fie A o mulțime. Vom numi *cuvânt* de elemente din A un sistem finit ordonat de elemente din A , $a_1 a_2 \dots a_r$. Vom spune că două cuvinte cu elemente din A , $\alpha = a_1 a_2 \dots a_r$, $\beta = b_1 b_2 \dots b_s$, sunt egale dacă și numai dacă $r = s$ și $a_i = b_i$ pentru $i = 1, 2, \dots, r$. Pe mulțimea $L(A)$ a cuvintelor cu elemente din A introducem următoarea operație algebrică (notată multiplicativ): pentru α și β din $L(A)$ de forma de mai sus definim

$$\alpha\beta = a_1 a_2 \dots a_r b_1 b_2 \dots b_s.$$

Este clar că această operație este asociativă și are element unitate care este cuvântul „vid” (format din submulțimea vidă a lui A). Așadar $L(A)$ cu operația introdusă este monoid și se numește *monoidul liber* generat de mulțimea A .

Se vede că dacă mulțimea A are cel puțin două elemente distincte a și b , atunci operația 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 mulțimea 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 $a^n a^m = a^{n+m}$ și deci este clar că în acest caz $L(A)$ este monoid comutativ.

În continuare, în afară de cazul în care se menționează altfel, operația algebrică pe un monoid va fi notată multiplicativ. Însă, fără o mențiune expresă, \mathbf{N} va fi considerat ca monoid cu adunarea.

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

Demonstrație. Am văzut că, în ipoteza din propoziție, orice element al lui $L(A)$ este de forma a^n , cu $n \in \mathbf{N}$ și este clar că funcția $\varphi : L(A) \rightarrow \mathbf{N}$ 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, funcția $\varphi' : \mathbf{N} \rightarrow L(A)$, definită prin $\varphi'(n) = a^n$, este un morfism de monoizi și avem $\varphi' \circ \varphi = 1_{L(A)}$ și $\varphi \circ \varphi' = 1_{\mathbf{N}}$.

Din propoziția de mai sus rezultă ca toți monoizii liberi generați de un element sunt izomorfi, fapt care rezultă de altfel aproape imediat din definiția monoidului liber generat de o mulțime A , în care se vede că natura elementelor din A nu intervine. Deci la două mulțimi A și A' echipotente se asociază monoizi liberi izomorfi. Această afirmație rezultă și din următoarea teoremă.

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

Demonstrație. Va trebui să definim pe \bar{f} pentru orice cuvânt format cu elemente din A . Acest lucru se face astfel: dacă $\alpha \in L(A)$, $\alpha = a_1 a_2 \dots a_r$, $a_k \in A$, $k = 1, 2, \dots, r$ cu

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

$$\bar{f}(\alpha\beta) = f(a_1) \dots f(a_r)f(b_1) \dots f(b_s)$$

și

$$\bar{f}(\alpha) \bar{f}(\beta) = (f(a_1) \dots f(a_r)) (f(b_1) \dots f(b_s)).$$

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

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

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

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

CURS IV

ELEMENTE DE TEORIA GRUPURILOR

§ 1. GRUPURI ȘI MORFISME DE GRUPURI

Grupuri

Definiția 1.1. Se numește *grup* o mulțime nevidă G înzestrată cu o operație algebrică care satisface următoarele condiții:

- 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, operația este comutativă, se spune că grupul G este *comutativ* sau *abelian*.

De regulă, pentru operația algebrică dintr-un grup vom folosi scrierea multiplicativă; dacă grupul G este comutativ, vom folosi de obicei scrierea aditivă. Vom folosi, eventual, și alte notații pentru operația algebrică a unui grup, de exemplu, dacă sunt definite mai multe operații pe aceeași mulțime; oricum, nu vom folosi scrierea aditivă în cazul unui grup necomutativ (neabelian).

Exemple.

1) Mulțimile \mathbf{Z} , \mathbf{Q} , \mathbf{R} , \mathbf{C} sunt grupuri comutative în raport cu operația de adunare corespunzătoare fiecăreia dintre acestea.

2) Mulțimile \mathbf{Q}^* , \mathbf{R}^* , \mathbf{C}^* ale numerelor raționale nenule, reale nenule, respectiv complexe nenule, în raport cu operația de înmulțire, sunt grupuri comutative. Mulțimile \mathbf{Q}_+^* și \mathbf{R}_+^* ale numerelor raționale strict pozitive și numerelor reale strict pozitive, formează grupuri comutative față de înmulțire.

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

4) Fie M un monoid cu operația algebrică notată multiplicativ și notăm

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

Observăm că elementul neutru e aparține lui $U(M)$ și deci $U(M) \neq \emptyset$. Mai mult, dacă $x, y \in U(M)$, atunci există $x^{-1}, y^{-1} \in M$ astfel încât $x x^{-1} = x^{-1} x = e$ și $y y^{-1} = y^{-1} y = e$. Deci și $x^{-1}, y^{-1} \in U(M)$ și $(xy)(y^{-1}x^{-1}) = (y^{-1}x^{-1})(xy) = e$, adică $xy \in U(M)$. Am demonstrat astfel că operația algebrică de pe M induce o operație algebrică pe $U(M)$ și, mai mult, $U(M)$ împreună cu această operație este grup. Grupul $(U(M), \cdot)$ astfel obținut se numește *grupul elementelor inversabile* sau *grupul unităților* monoidului (M, \cdot) .

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

5) Fie M o mulțime și $S(M) = \{f : M \rightarrow M \mid f \text{ bijectivă}\}$, mulțimea funcțiilor bijective de la M la M . Deoarece compunerea a două funcții bijective este o funcție bijectivă, iar o funcție este bijectivă dacă și numai dacă este inversabilă, rezultă că pe $S(M)$ compunerea funcțiilor este o operație algebrică împreună cu care $S(M)$ este un grup, în general necomutativ. Acesta se numește *grupul permutărilor* (sau *grupul simetric* al) mulțimii M . Lăsăm ca exercițiu să se arate că $S(M)$ este comutativ dacă și numai dacă M are cel mult două elemente.

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

6) Un număr complex z se numește *rădăcină a unității* dacă există un număr natural $n \geq 1$ astfel încât $z^n = 1$. Față de înmulțirea obișnuită a numerelor complexe, mulțimea U_∞ a rădăcinilor unității formează un grup abelian. Dacă $n \geq 1$ este fixat, mulțimea $U_n = \{z \in \mathbb{C}^* \mid z^n = 1\}$ a *rădăcinilor de ordin n ale unității* formează, în raport cu operația de înmulțire a numerelor complexe, un grup abelian.

Exerciții.

- 1) Fie M_1 și M_2 doi monoizi. Arătați că $U(M_1 \times M_2) = U(M_1) \times U(M_2)$.
- 2) Fie M o mulțime nevidă. Mulțimea $\mathcal{P}(M)$ formează grup abelian în raport cu diferența simetrică: $X \Delta Y = (X \setminus Y) \cup (Y \setminus X)$.

Reguli de calcul într-un grup

După cum rezultă din definiție, orice grup este monoid, deci regulile de calcul date pentru monoizi sunt valabile și 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} și se citește *inversul* lui x sau cu $-x$ și se citește *opusul* lui x , după cum folosim scrierea multiplicativă sau aditivă.

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

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

Într-adevăr, ținând seama de asociativitate

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

ceea ce demonstrează relația de mai înainte.

În particular,

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

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

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

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

Relația (1) se extinde și 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 $m, n \in \mathbb{Z}$.

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

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

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

Într-adevăr, din $xy = xz$, prin înmulțire 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 exercițiu să se arate că dacă $a, b \in G$, atunci fiecare dintre ecuațiile $ax = b$ și $ya = b$ are soluție unică în G .

Morfisme de grupuri

Definiția 1.2. Fie G și G' două grupuri. Se numește *morfism* de grupuri de la G la G' o funcție $f : G \rightarrow G'$ astfel încât

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

Ca și la monoizi, au loc următoarele afirmații:

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

2) Dacă G este un grup, funcția identică 1_G a mulțimii G este morfism de grupuri. Mai mult, dacă $f : G \rightarrow G'$ este un morfism de grupuri, atunci $f \circ 1_G = f$ și $1_{G'} \circ f = f$.

Propoziția 1.3. Dacă G și G' sunt două grupuri, e și e' elementele neutre ale lui G , respectiv G' și $f : G \rightarrow G'$ un morfism de grupuri, atunci:

1) $f(e) = e'$;

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

Demonstrație. 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 înmulțind la stânga cu $f(e)^{-1}$), obținem

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

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

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

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

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

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

$$f \circ g = 1_{G'} \text{ și } g \circ f = 1_G.$$

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

Un morfism de grupuri definit pe grupul G și cu valori tot în G se numește *endomorfism* al lui G . Mulțimea endomorfismelor lui G se notează cu $\text{End}(G)$.

Un endomorfism al lui G care este și izomorfism se numește *automorfism* al lui G . Mulțimea automorfismelor lui G se notează cu $\text{Aut}(G)$.

Evident, $\text{Aut}(G) \subseteq \text{End}(G)$. Mai mult, $\text{End}(G)$ este monoid în raport cu operația de compunere a funcțiilor, iar $\text{Aut}(G)$ este grup în raport cu operația de compunere a funcțiilor, fiind de fapt grupul unităților monoidului $(\text{End}(G), \circ)$.

Exemple.

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

2) Funcția $f : \mathbf{Z} \rightarrow \{-1, 1\}$, definită prin

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

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

3) Fie $n \in \mathbf{Z}$ și funcția $\varphi_n : \mathbf{Z} \rightarrow \mathbf{Z}$ 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 $f : \mathbf{Z} \rightarrow \mathbf{Z}$ 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 și fie (\mathbf{R}^*_+, \cdot) grupul multiplicativ al numerelor reale strict pozitive. Funcția $f : \mathbf{R} \rightarrow \mathbf{R}^*_+$ 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 $g : \mathbf{R}^*_+ \rightarrow \mathbf{R}$, $g(y) = \ln y$, avem

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

5) Fie G un grup și $a \in G$ un element al său. Aplicația $\varphi_a : G \rightarrow G$ 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

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

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

6) Fie M o mulțime, $N \subset M$ o submulțime proprie, iar $S(M)$ și $S(N)$ grupurile permutărilor mulțimii M , respectiv N . Pentru $f \in S(N)$, definim $\mathbf{f} : M \rightarrow M$ prin

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

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

Propoziția 1.4. Fie $f : G \rightarrow G'$ un morfism de grupuri. Atunci f este izomorfism de grupuri dacă și numai dacă funcția f este bijectivă.

Demonstrație. A se vedea propoziția 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 $S(G)$.

Demonstrație. Definim $f : G \rightarrow S(G)$ astfel: $f(x) = t_x$, unde $t_x : G \rightarrow G$ este dată prin $t_x(g) = xg$. Se verifică ușor că t_x este bijecție, deci $t_x \in S(G)$.

- f injectivă: $f(x) = f(y)$ implică $t_x = t_y$ și 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 $f(xy) = f(x) \circ f(y)$.

Exerciții.

1) Dacă M, N sunt monoizi și $M \cong N$ (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 $f : (\mathbf{Z}, +) \rightarrow (\mathbf{Z}, +)$ există $n \in \mathbf{Z}$ astfel încât $f = \varphi_n$). În particular, obținem că $(\text{End}(\mathbf{Z}), \circ) \cong (\mathbf{Z}, \bullet)$, izomorfism de monoizi. (De aici rezultă că $(\text{Aut}(\mathbf{Z}), \circ) \cong (\{-1, 1\}, \bullet)$, izomorfism de grupuri.)

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

Produs direct de grupuri

Fie G_1 și G_2 două grupuri. Pe produsul cartezian $G = G_1 \times G_2$ al mulțimilor G_1 și G_2 introducem următoarea operație algebrică:

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

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

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

$$\begin{aligned} (x_1, x_2)[(y_1, y_2)(z_1, z_2)] &= (x_1, x_2)(y_1z_1, y_2z_2) = (x_1(y_1z_1), x_2(y_2z_2)) = \\ &= ((x_1y_1)z_1, (x_2y_2)z_2) = (x_1y_1, x_2y_2)(z_1, z_2) = [(x_1, x_2)(y_1, y_2)](z_1, z_2). \end{aligned}$$

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

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

și

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

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

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

și

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

Grupul G se numește *produsul direct* al grupurilor G_1 și G_2 și se notează $G = G_1 \times G_2$. Mai mult, dacă G_1 și 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 $G_1 \times G_2$ funcțiile $s_1 : G_1 \rightarrow G_1 \times G_2$, respectiv $s_2 : G_2 \rightarrow G_1 \times G_2$ astfel: $s_1(x_1) = (x_1, e_2)$, respectiv $s_2(x_2) = (e_1, x_2)$. Acestea sunt morfisme injective de grupuri și se numesc *injecțiile canonice*.

De asemenea, reamintim că putem defini de la $G_1 \times G_2$ la G_1 , respectiv G_2 funcțiile $p_1 : G_1 \times G_2 \rightarrow G_1$, respectiv $p_2 : G_1 \times G_2 \rightarrow G_2$ astfel: $p_1(x_1, x_2) = x_1$, respectiv $p_2(x_1, x_2) = x_2$. Acestea sunt morfisme surjective de grupuri și se numesc *surjecțiile 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 și $f_i : G_i \rightarrow H_i$, $i = 1, 2$ morfisme de grupuri. Atunci produsul cartezian al morfismelor de grupuri $f_1 \times f_2 : G_1 \times G_2 \rightarrow H_1 \times H_2$ este morfism de grupuri.

Construcția 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 operație algebrică:

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

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

Fie $(G_i)_{i \in I}$ o familie nevidă de grupuri și $j \in I$. Atunci j -proiecția canonică

$p_j : \prod_{i \in I} G_i \rightarrow G_j$ este morfism surjectiv de grupuri. Putem defini și un morfism injectiv de grupuri, numit *j-injecția canonică*, $s_j : G_j \rightarrow \prod_{i \in I} G_i$ 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 și $f_i : G_i \rightarrow H_i$ o familie de morfisme de grupuri. Atunci produsul cartezian al familiei de morfisme de grupuri $(f_i)_{i \in I}$, $\prod_{i \in I} f_i : \prod_{i \in I} G_i \rightarrow \prod_{i \in I} H_i$ este morfism de grupuri.

Aplicații.

1) Considerăm grupurile aditive $(\mathbf{Z}_m, +)$ și $(\mathbf{Z}_n, +)$ ale claselor de resturi modulo m , respectiv modulo n . Arătăm că dacă m și 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 $\theta : \mathbf{Z}_{mn} \rightarrow \mathbf{Z}_m \times \mathbf{Z}_n$ prin $\theta(\bar{x}) = ([x], \{x\})$. Funcția θ este bine definită,

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

Avem că θ este morfism de grupuri, deoarece

$$\begin{aligned}\theta(\bar{x} + \bar{y}) &= \theta(\overline{x + y}) = ([x + y], \{x + y\}) = \\ &= ([x] + [y], \{x\} + \{y\}) = ([x], \{x\}) + ([y], \{y\}) = \theta(\bar{x}) + \theta(\bar{y}).\end{aligned}$$

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

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

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

2) Considerăm acum monoizii multiplicativi (\mathbf{Z}_m, \bullet) și (\mathbf{Z}_n, \bullet) . Să arătăm că dacă m și 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 funcția

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

de la aplicația 1) și știm că aceasta este bine definită. Mai mult, θ este un morfism de monoizi. Într-adevăr,

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

și

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

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

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

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

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

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

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

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

Definiția 1.5. Pentru $n \in \mathbf{N}$, $n \geq 2$, definim $\varphi(n) = |U(\mathbf{Z}_n)|$. Funcția φ se numește *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 și $k \geq 1$ avem $\varphi(p^k) = p^k - p^{k-1}$. Așadar, cunoscând descompunerea lui n în factori primi putem afla imediat $\varphi(n)$. De exemplu, $\varphi(12) = \varphi(2^2 \cdot 3) = \varphi(2^2)\varphi(3) = (2^2 - 2)(3 - 1) = 4$.

Exercițiu. Arătați 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 notație multiplicativă ($G \times G \rightarrow G, (x, y) \rightarrow xy$) și H o submulțime nevidă a sa. Dacă oricare ar fi $x, y \in H$, avem $xy \in H$ (produsul efectuat conform operației algebrice din G), atunci se obține o funcție $H \times H \rightarrow H, (x, y) \rightarrow xy$, adică o operație algebrică pe H numită *operația indusă* pe H de operația din G . În acest caz se mai spune că operația din G induce o operație pe H .

Definiția 2.1. Se spune că o submulțime nevidă H a grupului G este *subgrup* al lui G , dacă operația algebrică din G induce pe H o operație algebrică față de care H este grup.

Notatie. $H \leq G$

Propoziția 2.2. Fie G un grup și H o submulțime nevidă a sa. Atunci următoarele afirmații 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) aparține lui H ;
- 3) Oricare ar fi $x, y \in H$, produsul xy^{-1} (efectuat în G) aparține lui H .

Demonstrație. 1) \Rightarrow 2) Afirmația i) rezultă din faptul că operația din G induce pe H o operație algebrică. H fiind subgrup are un element neutru notat e' . Cum e este elementul neutru al lui G , avem în G relația

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

Simplificând la dreapta relația $ee' = e'e'$ (adică o înmulțim la dreapta cu $(e')^{-1}$) obținem $e = e'$.

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 relație, obținem $x' = x^{-1}$, deci $x^{-1} \in H$.

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

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

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

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

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

Exemple.

1) Dacă G este un grup, atunci G însuși este un subgrup al lui G , numit *subgrupul total* al lui G . De asemenea submulțimea $\{e\}$ a lui G este subgrup numit *subgrupul trivial* al lui G . Subgrupul total și subgrupul trivial al unui grup G se numesc *subgrupuri improprii* ale lui G . Orice subgrup diferit de acestea se numește *subgrup propriu*.

2) Grupul aditiv \mathbf{Z} al numerelor întregi este subgrup al grupului aditiv \mathbf{Q} al numerelor raționale; grupul aditiv \mathbf{Q} este subgrup al grupului aditiv \mathbf{R} al numerelor reale; grupul aditiv \mathbf{R} este subgrup al grupului aditiv \mathbf{C} al numerelor complexe.

De asemenea, grupul multiplicativ \mathbf{Q}^* este subgrup al grupului multiplicativ \mathbf{R}^* iar ambele sunt subgrupuri ale grupului multiplicativ \mathbf{C}^* .

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

4) Fie M o mulțime, $N \subset M$ o submulțime proprie a lui M , iar $S(M)$ grupul permutărilor mulțimii M . Mulțimea $H = \{f \in S(M) \mid f(x) = x \text{ oricare ar fi } x \in M \setminus N\}$ este un subgrup al lui $S(M)$.

5) Mulțimea automorfismelor interioare $\text{Int}(G)$ ale unui grup G este subgrup al grupului automorfismelor $\text{Aut}(G)$.

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

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

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

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

Demonstrație. Fie $H \subseteq \mathbf{Z}$ un subgrup oarecare al grupului aditiv \mathbf{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 propoziției precedente, $-x \in H$. Rezultă că H conține numere întregi pozitive. Fie n cel mai mic număr întreg pozitiv din H . Avem că $0 \in H$, $n \in H$, $2n = n + n \in H$ și, în general, $kn \in H$ oricare ar fi k număr natural, după cum rezultă din punctul 1) al propoziției precedente. De asemenea, din punctul 2) al aceleiași propoziții, $kn \in H$ oricare ar fi k întreg negativ, deci $n\mathbf{Z} \subseteq H$.

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

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

Exercițiu. Determinați subgrupurile grupului lui Klein $\mathbf{Z}_2 \times \mathbf{Z}_2$.

Nucleul și imaginea unui morfism de grupuri

Fie G și G' două grupuri, iar $f: G \rightarrow G'$ un morfism de grupuri. Fie $H \leq G$ și $H' \leq G'$ 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 și

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

imaginea reciprocă a lui H' prin f .

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

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

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

Propoziția 2.4. Fie $f: G \rightarrow G'$ un morfism de grupuri. Avem:

1) Dacă H este subgrup al lui G , atunci $f(H)$ este subgrup al lui G' . (În particular, $\text{Im } f$ 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, $\text{Ker } f$ este un subgrup al lui G).

Demonstrație. 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

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

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

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 $xy^{-1} \in f^{-1}(H')$.

Propoziția 2.5. Un morfism de grupuri $f: G \rightarrow G'$ este injectiv dacă și numai dacă nucleul său este trivial, adică $\text{Ker } f = \{e\}$.

Demonstrație. Să presupunem că f este morfism injectiv. Avem $f(e) = e'$ și dacă $x \in \text{Ker } f$, atunci $f(x) = e'$, adică $f(x) = f(e)$. Cum funcția 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 $f(xy^{-1}) = e'$ și deci $xy^{-1} = e$, de unde $x = y$. Rezultă că f este injectivă.

Observație. În mod evident avem că un morfism de grupuri $f: G \rightarrow G'$ este surjectiv dacă și numai dacă $\text{Im } f = G'$.

Teorema 2.6. (Teorema de corespondență pentru subgrupuri) Fie $f: G \rightarrow G'$ un morfism *surjectiv* de grupuri. Există o corespondență bijectivă între mulțimea subgrupurilor lui G care conțin $\text{Ker } f$ și mulțimea tuturor subgrupurilor lui G' , dată prin $H \rightarrow f(H)$.

Demonstrație. Mai întâi observăm că dacă H este un subgrup al lui G care conține $\text{Ker } f$, 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 $\text{Ker } f \subseteq H$ obținem $xh^{-1} \in H$, deci $x \in H$.

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

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

Subgrupul generat de o submulțime 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 $i \in I$, și cum fiecare H_i este un subgrup rezultă că $xy^{-1} \in H_i$, oricare ar fi $i \in I$. Deci $xy^{-1} \in \bigcap_{i \in I} H_i$.

Definiția 2.7. Fie G un grup și X o submulțime a lui G . Intersecția tuturor subgrupurilor care conțin mulțimea X (această intersecție fiind un subgrup, conform celor precedente) se numește *subgrupul generat de X în G* . Vom nota acest subgrup cu $\langle X \rangle$. Deci

$$\begin{aligned} \langle X \rangle &= \bigcap_{\substack{X \subseteq K \\ K \subseteq G \text{ subgrup}}} K \end{aligned}$$

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 .

Observații.

- 1) $\langle X \rangle$ este cel mai mic subgrup al lui G care conține 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 conțin pe X se găsește X însuși și deci subgrupul generat de X este chiar X . Cum subgrupul generat de un subgrup este subgrupul însuși, rezultă că orice subgrup al unui grup G are cel puțin 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 submulțime nevidă X în G .

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

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

Demonstrație. Fie

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

Arătăm că H' este subgrup al lui G care conține 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 $x = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_k^{\varepsilon_k}$, $y = y_1^{\mu_1} y_2^{\mu_2} \dots y_s^{\mu_s}$, $\varepsilon_i = \pm 1$, $\mu_j = \pm 1$, $x_i, y_j \in X$, $1 \leq i \leq k$, $1 \leq j \leq s$, și deci $xy^{-1} = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_k^{\varepsilon_k} y_s^{-\mu_s} \dots y_2^{-\mu_2} y_1^{-\mu_1} \in H'$.

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

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

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

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

Dacă folosim scrierea aditivă, atunci

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

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 numește *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 aceștia 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 $[m, n] = \text{c.m.m.m.c.}(m, n)$ și $(m, n) = \text{c.m.m.d.c.}(m, n)$.

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

$n \mid x$. Deci $[m, n] \mid x$, adică $x \in [m, n]\mathbf{Z}$. Reciproc, dacă $x \in [m, n]\mathbf{Z}$, atunci $[m, n] \mid x$ și deci $m \mid x$ și $n \mid x$, adică $x \in m\mathbf{Z}$ și $x \in n\mathbf{Z}$, de unde $x \in m\mathbf{Z} \cap n\mathbf{Z}$.

Să demonstrăm (ii). Din teorema precedentă, în scriere aditivă, rezultă $\langle m, n \rangle = \{x \in \mathbf{Z} \mid x = mk + nl, \text{ unde } k, l \in \mathbf{Z}\}$. Dacă $x \in \langle m, n \rangle$, atunci $x = mk + nl$ cu $k, l \in \mathbf{Z}$ și cum $(m, n) \mid m$ și $(m, n) \mid n$ rezultă că $(m, n) \mid mk + nl$, adică $(m, n) \mid x$, de unde $x \in (m, n)\mathbf{Z}$. Cum $\langle m, n \rangle$ este subgrup al lui \mathbf{Z} , rezultă că există $d \in \mathbf{Z}$ astfel încât $\langle m, n \rangle = d\mathbf{Z}$. Dar $m, n \in \langle m, n \rangle$, adică $m, n \in d\mathbf{Z}$ și deci $d \mid m$ și $d \mid n$. Fie acum $x \in (m, n)\mathbf{Z}$, adică $(m, n) \mid x$. Cum d este un divizor comun al numerelor m și n , rezultă $d \mid (m, n)$ și deci $d \mid x$, adică $x \in d\mathbf{Z} = \langle m, n \rangle$.

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 și n au un c.m.m.d.c. și, mai mult, există $k, l \in \mathbf{Z}$ 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

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

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

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

Reciproc, dacă $(a, n) = 1$, atunci rezultă că $[a] \in U(\mathbf{Z}_n)$ și deci există $[b] \in \mathbf{Z}_n$ cu $[a][b] = 1$. Atunci, dacă $[x] \in \mathbf{Z}_n$, $[x] = [x \cdot 1] = [x][1] = [x][a][b] = [xb][a] = (xb)[a]$. Cum $xb \in \mathbf{Z}$ avem $[x] \in \langle [a] \rangle$. Așadar $\mathbf{Z}_n = \langle [a] \rangle$.

Exercițiu. Să se arate că grupul $(\mathbf{Z} \times \mathbf{Z}, +)$ este finit generat, dar nu este ciclic.

Exercițiu. (i) Să se arate că subgrupul lui $(\mathbf{Q}, +)$ generat de $1/2$ și $1/3$ este ciclic și să se determine un generator al acestuia.

(ii) Mai general, să se arate că orice subgrup finit generat al lui $(\mathbf{Q}, +)$ este ciclic.

(iii) Să se arate că grupul $(\mathbf{Q}, +)$ nu este finit generat.

Curs VI

ELEMENTE DE TEORIA GRUPURILOR

§ 3. RELAȚII DE ECHIVALENȚĂ PE UN GRUP ÎN RAPORT CU UN SUBGRUP AL SĂU

Fie G un grup și H un subgrup al său. Considerăm pe G relațiile binare R_H^s și R_H^d definite în modul următor: dacă $x, y \in G$, atunci

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

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

Aceste relații binare sunt relații de echivalență. Să demonstrăm, de exemplu, că prima relație binară este relație de echivalență, adică este reflexivă, simetrică și tranzitivă.

- 1) Dacă $x \in G$, atunci $x^{-1}x = e \in H$ și deci $x R_H^s x$ (reflexivitatea).
- 2) Dacă $x R_H^s y$, atunci $x^{-1}y \in H$ și deci $y^{-1}x = (x^{-1}y)^{-1} \in H$, de unde $y R_H^s x$ (simetria).
- 3) Dacă $x R_H^s y$ și $y R_H^s z$, atunci $x^{-1}y \in H$ și $y^{-1}z \in H$. 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 relație de echivalență.

Relațiile de echivalență R_H^s și R_H^d se numesc *relații de congruență la stânga*, respectiv *la dreapta*, în raport cu H (sau *modulo H*). Faptul că „ x este în relația R_H^s cu y ” (respectiv „ x este în relația R_H^d cu y ”) se mai citește *x este congruent cu y modulo H la stânga* (respectiv *x este congruent cu y modulo H la dreapta*) și 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 echivalență a elementului $x \in G$ în raport cu R_H^s , respectiv R_H^d , și o vom numi *clasa de echivalență la stânga*, respectiv *clasa de echivalență la dreapta a lui x modulo H* .

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

Exemple.

- 1) Dacă G este un grup, relațiile de congruență la stânga și la dreapta modulo $\{e\}$ coincid (adică $x R_{\{e\}}^s y$ dacă și numai dacă $x R_{\{e\}}^d y$). De asemenea, relațiile R_G^s și R_G^d modulo G coincid.
- 2) Dacă G este un grup comutativ, iar H un subgrup oarecare al lui G , atunci relațiile de congruență la stânga și la dreapta modulo H coincid.
- 3) Fie S_3 grupul permutărilor de 3 elemente, adică

$$S_3 = \left\{ \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix} \right\}$$

și

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

Este evident că H este un subgrup al lui S_3 .

Să construim mulțimile claselor de echivalență la stânga și la dreapta modulo H . Dacă $\sigma, \tau \in S_3$, atunci $\sigma^{-1}\tau \in H$ dacă și numai dacă $\sigma^{-1}\tau(3) = 3$, dacă și numai dacă $\sigma(3) = \tau(3)$. Deci obținem trei clase de echivalență la stânga și anume:

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

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

Dacă $\sigma, \tau \in S_3$, atunci $\sigma\tau^{-1} \in H$ dacă și numai dacă $\tau^{-1}(3) = \sigma^{-1}(3)$. Deci clasele de echivalență la dreapta sunt:

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

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

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

Notatii. Fie G un grup și fie A, B două submulțimi 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 $Ab = \{ab \mid a \in A\}$.

Exercițiu. Fie G un grup și $H, K \leq G$ două subgrupuri.

(i) Arătați că HK este subgrup dacă și numai dacă $HK = KH$.

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

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

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

Demonstrație. 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 $y \in [x]_s$.

Observație. Observăm că $[e]_s = eH = H$ și de asemenea $[e]_d = He = H$.

Propoziția 3.2. Dacă G este un grup și H un subgrup al său, atunci funcția

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

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

Demonstrație. Să arătăm mai întâi că φ este bine definită, adică nu depinde de alegerea reprezentanților. 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.

Funcția 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 mulțimile G/R_H^s sau G/R_H^d este finită, atunci și cealaltă este finită și au același 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 mulțimii G/R_H^s sau al mulțimii G/R_H^d , care este același, se numește *indicele lui H în G* și se notează $[G : H]$.

Exercițiu. Fie G un grup și $H, K \leq G$ subgrupuri de indice finit.

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

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

(iii) Dați un exemplu în care $\text{c.m.m.d.c.}([G : H], [G : K]) > 1$ și $[G : H \cap K] < [G : H][G : K]$.

(iv) Dați un exemplu din care să rezulte că reciproca proprietății (ii) este falsă.

Se spune că un grup G este finit dacă mulțimea pe care este definită structura de grup (adică mulțimea subiacentă) este finită, iar numărul de elemente ale lui G se numește *ordinul* său și se notează $\text{ord } G$ sau $|G|$.

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

Lema 3.3. Fie G un grup și H un subgrup al său. Atunci funcția

$$\psi : H \rightarrow xH,$$

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

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

Funcția ψ este evident surjectivă și deci este bijectivă.

În particular, dacă H este un subgrup finit, atunci toate clasele de echivalență la stânga ale lui G modulo H sunt mulțimi finite și au același număr de elemente ca și H .

Observație. Afirmatia din lema precedentă referitoare la clasele de echivalență la stânga este valabilă și pentru clasele de echivalență la dreapta.

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

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

Demonstrație. Conform propoziției de mai sus putem să facem demonstrația considerând, de exemplu, numai relația de echivalență R_H^s pe G .

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

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

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 și H un subgrup al său, atunci $\text{ord } H \mid \text{ord } G$. În particular, dacă $\text{ord } G$ este un număr prim, atunci G nu are subgrupuri proprii, deci este ciclic.

Observații.

1) Dacă G este un grup finit și $d \mid \text{ord } G$, nu rezultă numai decît că există H un subgrup al lui G cu $\text{ord } H = d$.

2) Dacă G este grup *abelian* finit și $d \mid \text{ord } G$, atunci există $H \leq G$ cu $\text{ord } H = d$.

3) Pentru cazul neabelian există totuși o reciprocă parțială a teoremei lui Lagrange: Fie G un grup finit și p un număr prim cu proprietatea că $p \mid \text{ord } G$. Atunci există $H \leq G$ cu $\text{ord } H = p$. (Teorema lui Cauchy)

§ 4. ORDINUL UNUI ELEMENT

G fiind un grup și $a \in G$ 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 numește *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 \mathbf{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].

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

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

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

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

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

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

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

Demonstrație. Fie $n = \text{ord}(a)$. Din definiția ordinului lui a rezultă 1). Fie acum $k \in \mathbf{Z}$ astfel încât $a^k = e$. Conform teoremei împărțirii cu rest în mulțimea 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 $r = 0$ și deci n divide k .

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

Propoziția 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 și anume:

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

Demonstrație. 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 $a^{j-i} = e$ și $0 < j-i < n$, contradicție cu faptul că n este cel mai mic număr natural nenul astfel încât $a^n = e$.

Fie acum $n = \text{ord}(a)$ iar k un număr întreg. Din teorema împărțirii cu rest există $q, r \in \mathbf{Z}$ astfel încât $k = nq + r$ cu $0 \leq r < n$. Atunci $a^k = a^{nq+r} = (a^n)^q a^r = a^r$ și 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 .

Demonstrație. Rezultă din teorema lui Lagrange și propoziția precedentă.

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

Demonstrație. Rezultă din corolarul precedent.

Exemple.

1) Fie (\mathbf{C}^*, \cdot) 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}^*, \cdot) . 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 $a^2 + b^2 \neq 1$ este element de ordin infinit al grupului (\mathbf{C}^*, \cdot) .

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

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

Teorema 4.6. (Cauchy) Fie G un grup finit și p un număr prim cu proprietatea că $p \mid \text{ord } G$. Atunci există $a \in G$ cu $\text{ord}(a) = p$.

Demonstrație. Fie $n = \text{ord } G$ și definim $S = \{(a_1, \dots, a_p) \mid a_i \in G \text{ și } a_1 \cdots a_p = e\}$. Avem $|S| = n^{p-1}$ și cum $p \mid n$ 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, excepție făcând cazul în care $a_1 = \dots = a_p$. Clasa de echivalență a unui p -uplu de forma (a, \dots, a) are un singur element. Evident, S conține un astfel de p -uplu, și anume pe (e, \dots, e) . Dacă acesta este singurul p -uplu de forma (a, \dots, a) din S , atunci $|S| \equiv 1 \pmod{p}$, contradicție. Așadar există un element $a \neq e$ cu proprietatea că $(a, \dots, a) \in S$, deci $a^p = e$. Se consideră acum $H = \langle a \rangle$ și demonstrația este încheiată.

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

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

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

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

Exercițiu. Determinați elementele de ordin 30 din \mathbf{Z}_{240} .

Exercițiu. (i) Fie G_1, G_2 două grupuri și $x_1 \in G_1, x_2 \in G_2$ elemente de ordin finit. Arătați că $\text{ord}(x_1, x_2) = [\text{ord}(x_1), \text{ord}(x_2)]$.

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

Curs VII

ELEMENTE DE TEORIA GRUPURILOR

§ 5. SUBGRUPURI NORMALE

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

Notatie. $N \triangleleft G$

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

Propoziția 5.2. Dacă N este un subgrup al grupului G , afirmațiile următoare sunt echivalente:

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

Demonstrație. 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 și $(yx^{-1})^{-1} = xy^{-1} \in N$, adică $x R_N^d y$.

Analog se demonstrează că dacă $x R_N^d y$, atunci $x R_N^s y$, deci relațiile R_N^s și 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 $xN \in G/R_N^s$ și 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 $xN = yN$ și cum $xN = Nx$ și $yN = Ny$ rezultă că $Nx = Ny$, de unde $x R_N^d y$. Reciproc se arată la fel.

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

Exemple.

- 1) G și $\{e\}$ 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

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

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

4) Fie grupul S_3 al permutărilor de 3 elemente și permutarea $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$.

Submulțimea $H = \{e, \tau\}$ este un subgrup al lui 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 afirmație rezultă și din paragraful precedent, unde am arătat că mulțimile factor la stânga și la dreapta ale lui S_3 în raport cu H sunt diferite.)

Propoziția 5.3. Fie $f : G \rightarrow G'$ 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, $\text{Ker } f$ este subgrup normal al lui G .

Demonstrație. 1) Fie $g' \in G'$ și $h \in N$. Vrem să arătăm că $g'f(h)(g')^{-1} \in f(N)$. Deoarece f este surjectivă există $g \in G$ 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 $g \in G$ și $h \in f^{-1}(N')$. Vrem să arătăm că $ghg^{-1} \in f^{-1}(N')$, adică $f(ghg^{-1}) \in N'$. Dar $f(h) \in N'$ și cum N' este normal în G' rezultă că $f(g)f(h)f(g)^{-1} \in N'$, adică $f(ghg^{-1}) \in N'$.

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

Teorema 5.4. (Teorema de corespondență pentru subgrupuri normale) Fie $f : G \rightarrow G'$ un morfism *surjectiv* de grupuri. Există o corespondență bijectivă între mulțimea subgrupurilor normale ale lui G care conțin $\text{Ker } f$ și mulțimea tuturor subgrupurilor normale ale lui G' , dată prin $N \rightarrow f(N)$.

Demonstrație. Corespondența $N \rightarrow f(N)$ este corect definită după cum rezultă din propoziția 5.3. Restul este la fel ca în demonstrația teoremei 2.6 din cursul 5.

§ 6. GRUP FACTOR

Fie G un grup și N un subgrup normal al său. După cum rezultă din cele de mai înainte, relațiile de congruență R_N^s și R_N^d (la stânga și la dreapta modulo N) coincid. În acest caz vom spune, pe scurt, congruența modulo N , iar dacă $x, y \in G$, faptul că x este

congruent cu y modulo N îl vom scrie $x \equiv y \pmod{N}$. Cele două mulțimi factor G/R_N^s și G/R_N^d coincid, mulțimea factor fiind notată cu G/N .

Propoziția 6.1. Dacă G este un grup și N un subgrup normal al său, atunci pe mulțimea factor G/N se poate defini o operație algebrică împreună cu care G/N devine grup, iar funcția surjectivă $p: G \rightarrow G/N$, $p(x) = [x]$ este morfism de grupuri cu $\text{Ker } p = N$.

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

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

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

Să demonstrăm mai întâi că operația este bine definită, adică nu depinde de alegerea reprezentanților. Într-adevăr, dacă $[x] = [x']$ și $[y] = [y']$, atunci avem $x^{-1}x' \in N$ și $y^{-1}y' \in N$, adică există $h_1, h_2 \in N$ astfel încât $x^{-1}x' = h_1$ și $y^{-1}y' = h_2$, adică $x' = xh_1$ și $y' = yh_2$. 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 obține $x'y' = x(yh_3)h_2 = (xy)(h_3h_2)$, 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 operația algebrică este bine definită.

Operația este asociativă, deoarece dacă $[x], [y], [z] \in G/N$, atunci

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

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

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

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

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

Astfel am demonstrat că G/N este un grup.

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

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

Arătăm acum că $\text{Ker } p = N$. 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 $p(x) = [x] = [e]$ și deci $x \in \text{Ker } p$.

Definiția 6.2. Grupul G/N construit în propoziția precedentă se numește *grupul factor (cât) al lui G în raport cu subgrupul normal N* . Morfismul $p: G \rightarrow G/N$, $p(x) = [x]$ se numește *proiecția (surjecția) canonică a lui G pe grupul factor G/N* .

Observații.

1) Dacă G este un grup comutativ, atunci orice subgrup al său este normal și 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) Proiecția canonică $p: G \rightarrow G/\{e\}$ 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 și numai dacă $x - y \in n\mathbf{Z}$, dacă și numai dacă $n \mid x - y$, dacă și numai dacă $x \equiv y \pmod{n}$. Așadar, relația de echivalență pe \mathbf{Z} modulo subgrupul $n\mathbf{Z}$ coincide cu relația de congruență modulo n . Mai mult, operația 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 corespondență pentru subgrupuri (normale) obținem:

Propoziția 6.3. Fie G un grup și N un subgrup normal al lui G . Există o corespondență bijectivă între mulțimea subgrupurilor (normale) ale lui G care conțin pe N și mulțimea tuturor subgrupurilor (normale) ale lui G/N , dată prin $H \rightarrow H/N$.

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 conține pe $n\mathbf{Z}$. Ținând 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 și numai dacă $n\mathbf{Z} \subseteq d\mathbf{Z}$ dacă și numai dacă $d \mid n$. În concluzie, $K = d\mathbf{Z}/n\mathbf{Z}$ cu $d \mid n$. (Dacă ținem cont de izomorfismul dintre $\mathbf{Z}/n\mathbf{Z}$ și \mathbf{Z}_n putem scrie $K = [d]\mathbf{Z}_n$ cu $d \mid n$.)

În particular, grupul $(\mathbf{Z}_6, +)$ are 4 subgrupuri și 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 $f: G \rightarrow G'$ un morfism de grupuri și N un subgrup normal al lui G . Dacă $N \subseteq \text{Ker } f$, atunci există un morfism de grupuri $\bar{f}: G/N \rightarrow G'$ unic cu proprietatea că $\bar{f} \circ p = f$, unde $p: G \rightarrow G/N$ este proiecția canonică. Mai mult:

- 1) \bar{f} este injectiv $\Leftrightarrow N = \text{Ker } f$;
- 2) \bar{f} este surjectiv $\Leftrightarrow f$ este surjectiv.

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

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

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

Demonstrație. Definim $\bar{f}: G/\text{Ker } f \rightarrow \text{Im } f$, prin $\bar{f}([x]) = f(x)$.

Funcția \bar{f} este bine definită, adică nu depinde de alegerea reprezentanților. 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 $f(x) = f(y)$ și deci $\bar{f}([x]) = \bar{f}([y])$.

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

Să demonstrăm injectivitatea funcției \bar{f} . Într-adevăr, dacă $\bar{f}([x]) = \bar{f}([y])$, atunci $f(x) = f(y)$ și 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 $[x] = [y]$.

Ținând seama că f este morfism de grupuri, rezultă

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

adică \bar{f} este morfism de grupuri.

Deci \bar{f} este un izomorfism de grupuri.

Observație. Existența unui (izo)morfism de grupuri $\bar{f} : G/\text{Ker } f \rightarrow \text{Im } f$ se poate arăta folosind proprietatea de universalitate a grupurilor factor astfel: fie $f' : G \rightarrow \text{Im } f$ corestricția lui f la $\text{Im } f$. Deoarece $\text{Ker } f' = \text{Ker } f$, din proprietatea de universalitate a grupurilor factor există un morfism de grupuri $\bar{f} : G/\text{Ker } f \rightarrow \text{Im } f$ unic cu proprietatea că $\bar{f} \circ p = f'$, unde $p : G \rightarrow G/\text{Ker } f$ este proiecția canonică. Cum f' este surjectiv, rezultă că \bar{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 $\varphi : \mathbf{C}^* \rightarrow \mathbf{R}^*_+$ definită prin $\varphi(z) = |z|$. Avem că φ este morfism surjectiv de grupuri, adică $\text{Im } \varphi = \mathbf{R}^*_+$ și $\text{Ker } \varphi = S$. 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 $\psi : \mathbf{C}^* \rightarrow \mathbf{C}^*$ definită prin $\psi(z) = z/|z|$. Avem că ψ este morfism de grupuri, $\text{Ker } \psi = \mathbf{R}^*_+$ și $\text{Im } \psi = S$. 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 $f : \mathbf{Z}/n\mathbf{Z} \rightarrow \mathbf{Z}/d\mathbf{Z}$. Ținând seama de modul în care se definește f rezultă că $\text{Ker } f = d\mathbf{Z}/n\mathbf{Z}$. Atunci, din teorema fundamentală de izomorfism pentru grupuri, obținem că grupul factor $(\mathbf{Z}/n\mathbf{Z})/K$ este izomorf cu $\mathbf{Z}/d\mathbf{Z}$. (Dacă ținem cont de izomorfismul dintre $\mathbf{Z}/n\mathbf{Z}$ și \mathbf{Z}_n putem scrie astfel: $\mathbf{Z}_n/[d]\mathbf{Z}_n \cong \mathbf{Z}_d$.)

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

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

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

(Generalizați la un produs arbitrar de grupuri.)

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

Teorema 6.6. (A doua teoremă de izomorfism pentru grupuri) Fie G un grup și 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 și $HK/K \cong H/H \cap K$.

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

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

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

Curs VIII

ELEMENTE DE TEORIA GRUPURILOR

§ 7. GRUPURI DE PERMUTĂRI

Fie A o mulțime. Am observat că mulțimea $S(A)$ a funcțiilor bijective de la A în A formează față de compunere un grup numit *grupul permutărilor* mulțimii A .

Propoziția 7.1. Dacă A și A' sunt două mulțimi echipotente (sau între care există o funcție bijectivă), atunci grupurile de permutări $S(A)$ și $S(A')$ sunt izomorfe.

Demonstrație. Fie $f : A \rightarrow A'$ o funcție bijectivă. Definim o funcție $\varphi : S(A) \rightarrow S(A')$ care asociază oricărei funcții bijective $u \in S(A)$ funcția 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,
 $\varphi(u \circ v) = f \circ (u \circ v) \circ f^{-1} = f \circ u \circ (f^{-1} \circ f) \circ v \circ f^{-1} = (f \circ u \circ f^{-1}) \circ (f \circ v \circ f^{-1}) =$
 $\varphi(u) \circ \varphi(v),$

adică φ este morfism de grupuri.

Să arătăm că φ este bijecție. 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} și la dreapta cu f , rezultă $u = v$ și deci φ este injectivă. Dacă $u' \in S(A')$, atunci $f^{-1} \circ u' \circ f \in S(A)$ și

$$\varphi(f^{-1} \circ u' \circ f) = f \circ (f^{-1} \circ u' \circ f) \circ f^{-1} = (f \circ f^{-1}) \circ u' \circ (f \circ f^{-1}) = u',$$

deci φ este surjectivă.

Observație. În particular, dacă A este o mulțime finită cu n elemente, există o bijecție între A și mulțimea $\{1, 2, \dots, n\}$, deci grupurile de permutări $S(A)$ și $S(\{1, 2, \dots, n\})$ sunt izomorfe. Atunci, pentru a studia grupul de permutări al unei mulțimi cu n elemente este suficient să studiem grupul S_n al permutărilor mulțimii $\{1, 2, \dots, n\}$.

Definiția 7.2. Grupul S_n se numește *grupul simetric de grad n* sau *grupul permutărilor de grad n* . Elementele lui S_n se numesc *permutări* de n elemente sau *permutări de grad n* . Elementul neutru e din S_n se numește *permutarea identică* de grad n .

Să considerăm $\sigma \in S_n$ o permutare de n elemente, adică o funcție bijectivă de la mulțimea $\{1, 2, \dots, n\}$ în ea însăși. Punând în evidență valoarea $\sigma(i)$ a funcției σ pentru $i \in \{1, 2, \dots, n\}$, vom nota permutarea astfel

$$\sigma = \begin{bmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{bmatrix},$$

unde $\sigma(1), \sigma(2), \dots, \sigma(n)$ sunt numerele $1, 2, \dots, n$, eventual în altă ordine.

Vom arăta că S_n are $n!$ elemente. Vom demonstra acest fapt folosind teorema lui Lagrange. Notăm $\bar{S}_{n-1} = \{\sigma \in S_n \mid \sigma(n) = n\}$, mulțimea permutărilor de n elemente care invariază pe n . Este clar că \bar{S}_{n-1} este un subgrup al lui S_n , izomorf cu grupul S_{n-1} al permutărilor de $n-1$ elemente. Izomorfismul este dat de funcția

$$\theta : S_{n-1} \rightarrow \bar{S}_{n-1},$$

definită prin

$$\theta(\sigma) = \bar{\sigma}, \text{ unde } \bar{\sigma}(i) = \sigma(i), \text{ pentru } 1 \leq i \leq n-1 \text{ și } \bar{\sigma}(n) = n.$$

Deci $|S_{n-1}| = |\bar{S}_{n-1}|$.

Vom demonstra prin inducție după n că avem $|S_n| = n!$. Pentru $n = 1$ este evident că $|S_1| = 1 = 1!$. Să presupunem că $|S_{n-1}| = (n-1)!$. Conform teoremei lui Lagrange avem că $|S_n| = [S_n : \bar{S}_{n-1}] |\bar{S}_{n-1}|$ adică, $|S_n| = [S_n : \bar{S}_{n-1}] (n-1)!$.

Să calculăm indicele $[S_n : \bar{S}_{n-1}]$ al subgrupului \bar{S}_{n-1} în S_n , adică numărul claselor de echivalență (la stânga) modulo \bar{S}_{n-1} . Dacă $\sigma, \tau \in S_n$, atunci $\sigma \equiv_s \tau \pmod{\bar{S}_{n-1}}$ dacă și numai dacă $\sigma^{-1}\tau \in \bar{S}_{n-1}$, adică $\sigma^{-1}\tau(n) = n$ sau echivalent $\tau(n) = \sigma(n)$. Deci există n clase de echivalență (la stânga):

$$[\sigma_1], [\sigma_2], \dots, [\sigma_n],$$

unde $[\sigma_i] = \{\sigma \in S_n \mid \sigma(n) = i\}$, oricare ar fi $i = 1, 2, \dots, n$. Așadar, $[S_n : \bar{S}_{n-1}] = n$ și deci $|S_n| = n(n-1)! = n!$.

Definiția 7.3. Fie $\sigma = \begin{bmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{bmatrix}$ o permutare de n elemente. O

pereche (i, j) se numește *inversiune* a permutării σ dacă $i < j$ și $\sigma(i) > \sigma(j)$. Notăm cu $\text{inv}(\sigma)$ numărul inversiunilor permutării σ .

Dacă $\sigma \in S_n$ este o permutare, definim numărul

$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}$$

care se numește *semnul* (*signatura*) permutării σ .

Observăm că orice diferență $\sigma(j) - \sigma(i)$, cu $i < j$, de la numărătorul produsului din formula care definește $\varepsilon(\sigma)$, se simplifică cu una dintre diferențele de la numitor, care apare eventual cu semn schimbat dacă (i, j) este o inversiune. Deci $\varepsilon(\sigma)$ este un produs de $+1$ și -1 , factorul -1 apărând de atâtea ori câte inversiuni are permutarea σ . Deci $\varepsilon(\sigma) = (-1)^{\text{inv}(\sigma)}$.

O permutare σ se numește *pară* dacă $\varepsilon(\sigma) = 1$, adică are un număr par de inversiuni și se numește *impară* dacă $\varepsilon(\sigma) = -1$, adică are un număr impar de inversiuni.

Există permutări pare ca, de exemplu, permutarea identică. Vom arăta că pentru orice $n \geq 2$ există și permutări impare.

Fie $n \geq 2$ și $k, l \in \{1, 2, \dots, n\}$ cu $k \neq l$. Permutarea τ_{kl} definită prin

$$\tau_{kl}(k) = l, \tau_{kl}(l) = k, \tau_{kl}(i) = i, \text{ dacă } i \neq k \text{ și } i \neq l,$$

se numește *transpoziție*. Transpoziția τ_{kl} se mai notează $(k\ l)$.

Propoziția 7.4. Dacă $n \geq 2$ este un număr natural, atunci orice transpoziție din S_n este permutare impară.

Demonstrație. Fie transpoziția $(k\ l)$ și să presupunem că $k < l$. Atunci

$$(k\ l) = \begin{bmatrix} 1 & 2 & \dots & k-1 & k & \dots & l-1 & l & \dots & n \\ 1 & 2 & \dots & k-1 & l & \dots & l-1 & k & \dots & n \end{bmatrix}$$

și numărul de inversiuni este $(l-k) + (l-k-1) = 2(l-k) - 1$. Deci $\varepsilon((k, l)) = -1$.

Propoziția 7.5. Dacă $n \geq 2$ este un număr natural, funcția

$$\varepsilon : S_n \rightarrow \{-1, 1\},$$

de la grupul permutărilor S_n la grupul multiplicativ $\{-1, 1\}$, este un morfism surjectiv de grupuri.

Demonstrație. Fie $\sigma, \tau \in S_n$. Deoarece $\tau(1), \tau(2), \dots, \tau(n)$ sunt numerele $1, 2, \dots, n$, eventual într-o altă ordine și cum în produsul care-l dă pe $\varepsilon(\sigma)$ diferențele de la numitor se pot face și în altă ordine decât cea din definiție, rezultă că avem

$$\varepsilon(\sigma) = \prod_{1 \leq i < j \leq n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)}.$$

Atunci:

$$\begin{aligned} \varepsilon(\sigma \circ \tau) &= \prod_{1 \leq i < j \leq n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{j - i} = \prod_{1 \leq i < j \leq n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} \frac{\tau(j) - \tau(i)}{j - i} = \\ &= \prod_{1 \leq i < j \leq n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} \prod_{1 \leq i < j \leq n} \frac{\tau(j) - \tau(i)}{j - i} = \varepsilon(\sigma) \varepsilon(\tau), \end{aligned}$$

deci ε este un morfism de grupuri. Deoarece orice transpoziție este impară, iar permutarea identică este pară, rezultă că ε este surjectiv.

Definiția 7.6. Să notăm cu $A_n = \{\sigma \in S_n \mid \varepsilon(\sigma) = 1\}$, mulțimea permutărilor pare din S_n . Este clar că A_n este un subgrup (normal) al lui S_n , deci la rândul său este grup, numit *grupul altern de grad n* .

Evident $A_n = \text{Ker } \varepsilon$ și din teorema fundamentală de izomorfism pentru grupuri rezultă că grupul factor S_n/A_n este izomorf cu grupul multiplicativ $\{-1, 1\}$, deci indicele $[S_n : A_n]$ este 2.

Corolarul 7.7. A_n are $n!/2$ elemente.

Definiția 7.8. O permutare $\sigma \in S_n$ se numește *ciclu de lungime m*, $2 \leq m \leq n$, 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° $\sigma(i_1) = i_2, \sigma(i_2) = i_3, \dots, \sigma(i_{m-1}) = i_m, \sigma(i_m) = i_1$.

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 și n putem să asociem cel puțin un ciclu de lungime m și, mai mult,

$$(i_1 i_2 \dots i_m) = (i_2 i_3 \dots i_m i_1) = \dots = (i_m i_1 \dots i_{m-1}).$$

Așadar, numărul ciclilor de lungime m, $2 \leq m \leq n$, este $C_n^m (m-1)!$. De exemplu, orice transpoziție este un ciclu de lungime 2. Prin urmare, rezultă că numărul transpozițiilor din grupul S_n este C_n^2 .

Propoziția 7.9. Dacă $\sigma = (i_1 i_2 \dots i_m) \in S_n$ este un ciclu de lungime m, atunci

1) $\sigma^{-1} = (i_m i_{m-1} \dots i_1)$,

2) $\text{ord}(\sigma) = m$.

Demonstrație. 1) Se verifică imediat.

2) Din definiția ciclului obținem că $\sigma^k(i_1) = i_{k+1}$ pentru orice $1 \leq k \leq m-1$ și $\sigma^m(i_1) = i_1$. Deoarece $i_1 \neq i_k$, pentru orice $2 \leq k \leq m$, avem că $\sigma^k \neq e$, pentru orice $1 \leq k \leq m-1$. Să arătăm că $\sigma^m = e$. Dacă $i \notin \{i_1, i_2, \dots, i_m\}$, atunci $\sigma(i) = i$ și deci $\sigma^m(i) = i$. Dacă $i = i_1$ am observat că $\sigma^m(i_1) = i_1$, iar dacă $i = i_{k+1}$, $1 \leq k \leq m-1$, 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 , $1 \leq i \leq n$, avem că $\sigma^m(i) = i$, adică $\sigma^m = e$. Am demonstrat astfel că $\text{ord}(\sigma) = m$.

Propoziția 7.10. Fie $\sigma, \tau \in S_n$, iar A, B două submulțimi nevide și disjuncte ale mulțimii $\{1, 2, \dots, n\}$ 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 $\sigma \tau = \tau \sigma$ și $\text{ord}(\sigma \tau) = \text{c.m.m.m.c.}(\text{ord}(\sigma), \text{ord}(\tau))$.

Demonstrație. Fie $r \in \{1, 2, \dots, n\}$ un element oarecare. Dacă $r \notin A \cup B$ atunci $\sigma(r) = r$ și $\tau(r) = r$ și deci $(\sigma \tau)(r) = (\tau \sigma)(r) = r$. Presupunem că $r \in A \cup B$. Dacă $r \notin A$, atunci $r \in B$ și 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 $\sigma(r) \notin B$ și deci $\tau(\sigma(r)) = \sigma(r)$. Rezultă că și 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 $\text{ord}(\sigma) = k$, $\text{ord}(\tau) = l$, $\text{ord}(\sigma \tau) = m$ și să notăm $u = \text{c.m.m.m.c.}(k, l)$. Avem $(\sigma \tau)^m = e$ și 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 $\sigma^m(r) \neq r$ și deci neapărat $r \in A$. Din $\sigma^m(r) = \tau^{-m}(r)$, avem $\tau^{-m}(r) \neq r$, deci $\tau^m(r) \neq r$ și deci neapărat $r \in B$. Așadar $r \in A \cap B$, contradicție cu faptul că $A \cap B = \emptyset$. Am obținut astfel că $\sigma^m = e = \tau^m$.

Prin urmare, $k \mid m$ și $l \mid m$ și deci $u \mid m$. Fie $k', l' \in \mathbf{N}$ astfel încât $u = kk'$ și $u = ll'$. Deci $(\sigma \tau)^u = \sigma^u \tau^u = (\sigma^l)^{l'} (\tau^k)^{k'} = e$, de unde obținem că $m \mid u$. Din $u \mid m$ și $m \mid u$ rezultă că $m = u$ și propoziția este demonstrată.

Corolarul 7.11. Fie $\sigma \in S_n$, $n \geq 2$, o permutare astfel încât $\sigma = \tau_1 \tau_2 \dots \tau_t$, unde $\tau_1, \tau_2, \dots, \tau_t$ sunt cicli disjuncți. Atunci $\text{ord}(\sigma) = \text{c.m.m.m.c.}(\text{ord}(\tau_1), \text{ord}(\tau_2), \dots, \text{ord}(\tau_t))$.

Demonstrație. Rezultă imediat prin generalizarea punctului 2 al propoziției de mai sus.

Definiția 7.12. Ciclurile $\sigma = (i_1 i_2 \dots i_m)$ și $\tau = (j_1 j_2 \dots j_k)$ se numesc *disjuncte* dacă

$$\{i_1, i_2, \dots, i_m\} \cap \{j_1, j_2, \dots, j_k\} = \emptyset.$$

Propoziția precedentă aplicată în cazul ciclurilor disjuncte σ și τ ne spune că $\sigma \tau = \tau \sigma$ și $\text{ord}(\sigma \tau) = \text{c.m.m.m.c.}(m, k)$.

Teorema 7.13. Orice permutare $\sigma \in S_n$, $\sigma \neq e$, se descompune ca un produs finit de cicli disjuncți. Mai mult, această descompunere este unică, abstracție făcând de ordinea factorilor.

Demonstrație. Fie n_σ numărul de elemente ale mulțimii $\{1, 2, \dots, n\}$ permutate efectiv de către σ , adică

$$n_\sigma = |\{i \mid \sigma(i) \neq i\}|.$$

Deoarece $\sigma \neq e$, există i astfel încât $\sigma(i) \neq i$ și cum σ este injectivă avem $\sigma(\sigma(i)) \neq \sigma(i)$ și deci $n_\sigma \geq 2$. Vom face demonstrația prin inducție după acest număr.

Dacă $\sigma \in S_n$, astfel încât $n_\sigma = 2$, atunci există $i \neq j$, astfel încât $\sigma(i) = j$, $\sigma(j) = i$ și $\sigma(k) = k$ oricare ar fi $k \neq i$ și $k \neq j$. În acest caz σ este transpoziția $(i j)$.

Presupunem teorema adevărată pentru toate permutările τ care permută efectiv mai puțin de n_σ elemente, adică $n_\tau < n_\sigma$, și să arătăm că ea este adevărată și 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 $t = \text{ord}(\sigma)$, atunci $\sigma^t = e$ și deci $\sigma^t(i_1) = i_1$, adică $i_{t+1} = i_1$. Din proprietatea de bună ordonare a mulțimii \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 $r \neq s$, și $1 \leq r, s \leq m$, atunci $\sigma^{r-1}(i_1) = \sigma^{s-1}(i_1)$. Să presupunem că $r > s$ și 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 contradicție cu alegerea numărului m .

Fie acum ciclul $\tau = (i_1 i_2 \dots i_m)$ și să considerăm permutarea $\sigma' = \tau^{-1}\sigma$. Dacă $\sigma(i) = i$, atunci $i \notin \{i_1, i_2, \dots, i_m\}$ și deci $\tau^{-1}(i) = i$, de unde $\sigma'(i) = i$. Mai mult, dacă $i_k \in \{i_1, \dots, i_m\}$ este clar că $\sigma'(i_k) = (\tau^{-1}\sigma)(i_k) = \tau^{-1}(\sigma(i_k)) = i_k$ și deci, în plus, elementele i_1, i_2, \dots ,

i_m rămân neschimbate dacă le aplicăm permutarea σ' . Așadar $n_{\sigma'} < n_{\sigma}$ și conform ipotezei de inducție există ciclurile disjuncte $\tau_2, \tau_3, \dots, \tau_t$ astfel încât $\sigma' = \tau_2 \tau_3 \dots \tau_t$ sau $\tau^{-1} \sigma = \tau_2 \tau_3 \dots \tau_t$, de unde $\sigma = \tau \tau_2 \tau_3 \dots \tau_t$. Mai mult, din demonstrație rezultă că ciclul τ este disjunct de fiecare din ciclurile disjuncte $\tau_2, \tau_3, \dots, \tau_t$. Notând $\tau_1 = \tau$ obținem descompunerea $\sigma = \tau_1 \tau_2 \tau_3 \dots \tau_t$ în produs de cicluri disjuncte. Tot din demonstrație se observă că această descompunere este unică, abstractie făcând de ordinea factorilor.

Propoziția 7.14. Orice ciclu din S_n este un produs de transpoziții.

Demonstrație. Dacă $\sigma = (i_1 i_2 \dots i_m)$ este un ciclu de lungime m , atunci prin calcul direct rezultă

$$\sigma = (i_1 i_m)(i_1 i_{m-1}) \dots (i_1 i_2) = (i_1 i_2)(i_2 i_3) \dots (i_{m-1} i_m).$$

Corolarul 7.15. Orice permutare $\sigma \in S_n$, $n \geq 2$, este produs de transpoziții.

Demonstrație. Dacă $\sigma = e$, atunci $\sigma = e = (1, 2)(1, 2)$. Dacă $\sigma \neq e$, afirmația rezultă din teorema și propoziția de mai sus.

Observație. Din cele de mai sus se observă că descompunerea unei permutări în produs de transpoziții nu este unică, în schimb paritatea numărului de transpoziții care apar în orice descompunere a unei permutări este aceeași. Într-adevăr, fie $\sigma = \tau_1 \tau_2 \dots \tau_t = \sigma_1 \sigma_2 \dots \sigma_s$, unde $\tau_1, \tau_2, \dots, \tau_t$ și $\sigma_1, \sigma_2, \dots, \sigma_s$ sunt transpoziții. Ținând cont că semnul unei transpoziții este -1 , obținem $\varepsilon(\sigma) = (-1)^t = (-1)^s$, de unde rezultă că t și s sunt în același timp pare sau impare.

Aplicație. Fie permutarea $\sigma \in S_{10}$, 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 cicluri disjuncte și ca produs de transpoziții. De asemenea, să determinăm ordinul permutării σ .

Considerăm numărul 1 care este permutat efectiv de σ , deoarece $\sigma(1) = 3$. Cum $\sigma(3) = 1$ obținem $\tau_1 = (1 \ 3)$. Considerăm acum următorul număr care este permutat efectiv de σ și care nu aparține mulțimii $\{1, 3\}$. Acesta este 2. Cum $\sigma(2) = 5$, $\sigma(5) = 7$, $\sigma(7) = 8$, $\sigma(8) = 2$ obținem ciclul $\tau_2 = (2 \ 5 \ 7 \ 8)$. Fie acum numărul 6 care este permutat efectiv de σ . Avem $\sigma(6) = 10$, $\sigma(10) = 9$, $\sigma(9) = 6$ și astfel obținem ciclul $(6 \ 10 \ 9)$. Deci σ se scrie ca produs de cicluri disjuncte astfel: $\sigma = (1 \ 3) (2 \ 5 \ 7 \ 8) (6 \ 10 \ 9)$.

Din ultima propoziție a acestui paragraf rezultă că σ se poate scrie ca produs de transpoziții astfel: $\sigma = (1 \ 3) (2 \ 8) (2 \ 7) (2 \ 5) (6 \ 9) (6 \ 10)$.

În final avem $\text{ord}(\sigma) = \text{c.m.m.m.c.}(2, 4, 3) = 12$.

INELE

1. GENERALITĂȚI

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

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

Dacă, în plus,

- 4) $ab = ba$ pentru orice $a, b \in R$,
atunci R se numește inel comutativ.

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

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

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

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

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

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

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

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

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

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

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

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

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

pentru orice $x \in X$. Acesta se numește *inelul funcțiilor definite pe X cu valori în R* . Elementul nul al acestui inel este funcția $\mathbf{0} : X \rightarrow R$ definită prin $\mathbf{0}(x) = 0$ pentru orice $x \in X$ (elementul unitate este funcția $\mathbf{1} : X \rightarrow R$ definită prin $\mathbf{1}(x) = 1$ pentru

orice $x \in X$).

(vi) Fie R un inel (unitar). Atunci $(M_n(R), +, \cdot)$ este inel (unitar) și se numește *inelul matricelor pătratice de ordin n peste R* . În cazul în care R este unitar, elementul unitate al lui $M_n(R)$ se notează cu I_n și este matricea care are 1 pe diagonala principală și 0 în rest. În general, $M_n(R)$ nu este inel comutativ.

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

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

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

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

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

Exercițiul 1.6. Să se arate că $(\mathbb{R}^{\mathbb{R}}, +, \circ)$ nu este inel.

Exercițiul 1.7. Fie R un inel și $n \geq 2$. Să se arate că inelul de matrice $M_n(R)$ este comutativ dacă și numai dacă $ab = 0$ pentru orice $a, b \in R$.

Avem următoarele reguli de calcul într-un inel:

Propoziția 1.8. Fie R un inel. Atunci

(i) $0a = a0 = 0$ pentru orice $a \in R$.

(ii) $a(-b) = (-a)b = -(ab)$ și $(-a)(-b) = ab$ pentru orice $a, b \in R$.

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

(iv) $(\sum_{i=1}^m a_i)(\sum_{j=1}^n b_j) = \sum_{i=1}^m \sum_{j=1}^n a_i b_j$ pentru orice $a_i, b_j \in R$.

(v) (Formula binomului lui Newton) Fie $a, b \in R$ cu proprietatea că $ab = ba$. Atunci

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

Definiția 1.9. Fie R un inel și $a \in R$. Atunci a se numește *divizor al lui zero la stânga* (la dreapta) *dacă există $b \in R, b \neq 0$ astfel încât $ab = 0$ (respectiv, $ba = 0$)*. Dacă a este divizor al lui zero la stânga și la dreapta, atunci se va numi *divizor al lui zero*.

Să observăm că dacă R nu este inelul nul, atunci 0 este divizor al lui zero.

Exercițiul 1.10. Arătați că dacă un inel are un divizor al lui zero la stânga (dreapta) nenul, atunci are un divizor al lui zero nenul.

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

Definiția 1.12. Fie R un inel nenul. Dacă R nu are divizori ai lui zero nenuli, atunci R se numește *inel integru*. Un inel integru și comutativ se numește *domeniu de integritate*.

Propoziția 1.13. Fie R un inel nenul. Atunci R este inel integru dacă și numai dacă oricare ar fi $a, b \in R$ cu $ab = 0$ rezultă $a = 0$ sau $b = 0$.

- Exemplul 1.14.** (i) $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ sunt domenii de integritate.
(ii) Un element $\hat{a} \in \mathbb{Z}_n$ este divizor al lui zero dacă și numai dacă $(a, n) \neq 1$. Așadar \mathbb{Z}_n este domeniu de integritate dacă și numai dacă n este număr prim.
(iii) Dacă R este un inel unitar nenul și $n \geq 2$, atunci $(M_n(R), +, \cdot)$ nu este inel integru. De exemplu, matricea $\begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix}$ este divizor al lui zero în $M_2(R)$.
(iv) Dacă R_1, R_2 sunt inele nenule, atunci $R_1 \times R_2$ nu este inel integru. De exemplu, perechea $(a_1, 0)$, unde $a_1 \in R_1$, $a_1 \neq 0$, este divizor al lui zero.
(v) Fie M o mulțime cu $|M| \geq 2$. Atunci inelul $(\mathcal{P}(M), \Delta, \cap)$ nu este integru.

- Exercițiul 1.15.** (i) Arătați că $f \in \mathbb{R}^{\mathbb{R}}$ este divizor al lui zero dacă și numai dacă există $x_0 \in \mathbb{R}$ astfel încât $f(x_0) = 0$.
(ii) Fie $\mathcal{C}(\mathbb{R}) = \{f : \mathbb{R} \rightarrow \mathbb{R} \mid f \text{ este continuă}\}$ cu operațiile de adunare și înmulțire a funcțiilor. Arătați că $f \in \mathcal{C}(\mathbb{R})$ este divizor al lui zero dacă și numai dacă există $(a, b) \subset \mathbb{R}$ astfel încât $f(x) = 0$ pentru orice $x \in (a, b)$.

Definiția 1.16. Fie R un inel unitar. Un element $a \in R$ se numește inversabil la stânga (la dreapta) dacă există $a' \in R$ astfel încât $a'a = 1$ (respectiv, $aa' = 1$). Dacă a este inversabil la stânga și la dreapta, atunci se va numi inversabil.

- Exercițiul 1.17.** Arătați că în inelul $M_n(\mathbb{R})$ orice element inversabil la stânga (dreapta) este inversabil la dreapta (stânga).

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

- Remarca 1.18.** (i) $a \in U(R)$ dacă și numai dacă există $a' \in R$ astfel încât $aa' = a'a = 1$.
(ii) $U(R)$ este grup în raport cu înmulțirea și se numește *grupul unităților lui R*.
(iii) Elementele inversabile nu sunt divizori ai lui zero. (În schimb există elemente inversabile la dreapta și care sunt divizori ai lui zero la stânga.)

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

$$U(M_n(R)) = \{A \in M_n(R) : \det A \in U(R)\}.$$

- (v) Fie R_1, R_2 inele unitare. Atunci $U(R_1 \times R_2) = U(R_1) \times U(R_2)$.

În afara elementelor inversabile și a divizorilor lui zero, mai există și alte elemente remarcabile într-un inel.

Definiția 1.20. Fie R un inel și $x \in R$. Elementul x se numește nilpotent dacă există $n \in \mathbb{N}^*$ astfel încât $x^n = 0$.

- Remarca 1.21.** (i) 0 este element nilpotent.
(ii) Un inel integru nu are elemente nilpotente nenule.

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

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

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

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

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

- (ii) Dacă R este inel unitar și $x \in R$ este idempotent, atunci și $1 - x$ este idempotent.
- (iii) Un inel integru nu are idempotenți netriviali.

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

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

Exercițiul 1.28. (i) Se consideră numărul natural $n \geq 2$ care are r factori primi distincți în descompunerea sa. Să se arate că numărul idempotenților lui \mathbb{Z}_n este 2^r .
(ii) Să se determine idempotenții inelului \mathbb{Z}_{36} .

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

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

2. SUBINELE. IDEALE

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

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

- (i) $x, y \in S \implies x - y \in S$,
 - (ii) $x, y \in S \implies xy \in S$,
- pentru orice $x, y \in S$.

Exemplul 2.3. (i) Dacă R este un inel, atunci $\{0\}$ și R sunt subinele.

- (ii) $\mathbb{Z} \subset \mathbb{Q}$ este subinel unitar.
- (iii) $2\mathbb{Z} \subset \mathbb{Z}$ este subinel, dar nu este unitar.
- (iv) $\widehat{5}\mathbb{Z}_{10} \subset \mathbb{Z}_{10}$ este subinel, dar nu este subinel unitar. Să remarcăm că $\widehat{5}\mathbb{Z}_{10}$ are totuși element unitate, pe $\widehat{5}$. (Mai general, dacă R este inel comutativ unitar și $e \in R$ un idempotent netrivial, atunci $Re \subset R$ este subinel, $1 \notin Re$, dar Re are element unitate pe e .)
- (v) $\mathcal{C}(\mathbb{R}) \subset \mathbb{R}^{\mathbb{R}}$ este subinel unitar.

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

- (i) $x, y \in I \implies x - y \in I$,
- (ii) $a \in R, x \in I \implies ax \in I$ (respectiv, $xa \in I$),
pentru orice $a \in R$ și $x, y \in I$.

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

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

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

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

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

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

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

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

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

(v) Fie $R = M_2(\mathbb{Q})$ și

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

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

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

Exercițiul 2.7. Fie R_1, R_2 inele unitare și $R = R_1 \times R_2$. Să se arate că idealele la stânga (la dreapta, bilaterale) ale lui R sunt de forma $I = I_1 \times I_2$, unde I_1, I_2 sunt ideale la stânga (la dreapta, bilaterale) în R_1, R_2 , respectiv.

Exercițiul 2.8. Fie R un inel unitar.

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

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

Lema 2.9. Fie R un inel și $I_\alpha \leq_s R$, $\alpha \in A$ o familie de ideale la stânga ale lui R . Atunci $\bigcap_{\alpha \in A} I_\alpha \leq_s R$. (Analog pentru ideale la dreapta, respectiv bilaterale.)

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

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

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

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

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

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

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

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

$$(X)_s = \{y \in R : y = \sum_{i=1}^n a_i x_i, a_i \in R, x_i \in X, n \in \mathbb{N}\},$$

$$(X)_d = \{y \in R : y = \sum_{i=1}^n x_i a_i, a_i \in R, x_i \in X, n \in \mathbb{N}\},$$

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

În particular,

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

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

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

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

3. MORFISME DE INELE

Definiția 3.1. Fie R, R' inele și $f : R \rightarrow R'$ o funcție. Aceasta se numește morfism de inele dacă

$$f(x + y) = f(x) + f(y),$$

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

pentru orice $x, y \in R$.

Dacă R, R' sunt inele unitare și $f(1) = 1'$, atunci f se numește morfism unitar.

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

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

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

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

morfism unitar și surjectiv de inele.

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

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

atunci f este morfism injectiv de inele. Dacă, în plus, R este unitar, atunci f este de asemenea morfism unitar.

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

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

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

Notăție: $R \simeq R'$.

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

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

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

Exercițiul 3.9. Arătați că avem următoarele izomorfisme de inele:

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

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

Exercițiul 3.11. Fie $m, n \geq 2$.

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

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

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

Propoziția 3.12. Fie $f : R \rightarrow R'$ un morfism de inele.

(i) Dacă $S \subseteq R$ este subinel, atunci $f(S) \subseteq R'$ este subinel.

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

(ii) Dacă $I \leq_s R$ și f este surjectiv, atunci $f(I) \leq_s R'$.

Dacă $I' \leq_s R'$, atunci $f^{-1}(I') \leq_s R$.

(Analog pentru ideale la dreapta, respectiv bilaterale.)

Exemplul 3.13. Imaginea unui ideal printr-un morfism nu este neapărat un ideal. De exemplu, imaginea lui $2\mathbb{Z}$ prin morfismul incluziune $i : \mathbb{Z} \rightarrow \mathbb{Q}$ nu este ideal.

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

Din cele demonstrate în capitolul despre grupuri știm că f este morfism injectiv dacă și numai dacă $\text{Ker } f = \{0\}$.

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

4. INELE FACTOR

Fie R un inel și $I \subseteq R$ un ideal bilateral. În particular, I este subgrup al lui $(R, +)$, iar $(R/I, +)$ este grup comutativ. Definim pe R/I o operație algebrică numită înmulțire astfel:

$$\widehat{a} \cdot \widehat{b} = \widehat{ab}.$$

Să arătăm că aceasta este bine definită: dacă $\widehat{a} = \widehat{a'}$ și $\widehat{b} = \widehat{b'}$, atunci $a - a' \in I$ și $b - b' \in I$. Scriem $ab - a'b' = a(b - b') + (a - a')b'$ și deoarece I este ideal bilateral $a(b - b') \in I$ și $(a - a')b' \in I$, deci $ab - a'b' \in I$ ceea ce este echivalent cu $\widehat{ab} = \widehat{a'b'}$. Acum rezultă cu ușurință că $(R/I, +, \cdot)$ este un inel.

Definiția 4.1. Inelul R/I se numește inelul factor al lui R în raport cu idealul bilateral I . Funcția $p : R \rightarrow R/I$ definită prin $p(x) = \widehat{x}$ este un morfism surjectiv de inele și se numește proiecția (surjecția) canonică a lui R pe R/I .

Remarca 4.2. (i) Dacă R este inel comutativ, atunci orice ideal al său este bilateral și deci putem vorbi de inelul factor al lui R în raport cu orice ideal al său.
(ii) Dacă R este inel unitar (comutativ), atunci R/I este inel unitar (comutativ).
(iii) Proiecția canonică $p : R \rightarrow R/\{0\}$ este izomorfism de inele.

Propoziția 4.3. Fie R un inel și $I \subseteq R$ un ideal bilateral. Există o corespondență bijectivă între mulțimea idealelor la stânga (la dreapta, bilaterale) ale lui R care conțin pe I și mulțimea tuturor idealelor la stânga (la dreapta, bilaterale) ale lui R/I , dată prin $J \mapsto J/I$.

Exemplul 4.4. Idealele lui $\mathbb{Z}/n\mathbb{Z}$ sunt de forma $d\mathbb{Z}/n\mathbb{Z}$ cu $d \mid n$.

Teorema 4.5. (Proprietatea de universalitate a inelelor factor) Fie $f : R \rightarrow R'$ un morfism de inele și I un ideal bilateral al lui R . Dacă $I \subseteq \text{Ker } f$, atunci există un morfism de inele $\bar{f} : R/I \rightarrow R'$ unic cu proprietatea că $\bar{f} \circ p = f$, unde $p : R \rightarrow R/I$ este proiecția canonică. Mai mult:

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

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

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

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

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

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

Exercițiul 4.8. Fie R_1, R_2 inele unitare, $R = R_1 \times R_2$ și $I = I_1 \times I_2$, unde I_1, I_2 sunt ideale bilaterale în R_1 , respectiv R_2 . Să se arate că inelele R/I și $R_1/I_1 \times R_2/I_2$ sunt izomorfe.

Exercițiul 4.9. Fie R un inel unitar și I ideal bilateral al lui R . Să se arate că inelele $M_2(R)/M_2(I)$ și $M_2(R/I)$ sunt izomorfe.

5. TEOREMA CHINEZĂ A RESTURILOR PENTRU IDEALE

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

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

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

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

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

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

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

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

CORPURI

1. GENERALITĂȚI

Definiția 1.1. Un inel unitar K cu $1 \neq 0$ se numește corp dacă orice element nenul al său este inversabil.

Dacă înmulțirea pe K este comutativă, atunci K se numește corp comutativ.

Notatie: $K^\times = K \setminus \{0\}$.

Exemplul 1.2. (i) $(\mathbb{Q}, +, \cdot)$ și $(\mathbb{R}, +, \cdot)$ sunt corpuri comutative.

(ii) \mathbb{Z}_n este corp dacă și 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.

Exercițiul 1.4. Arătați că orice inel unitar ($1 \neq 0$) integru și finit este corp.

Propoziția 1.5. Fie R un inel unitar cu $1 \neq 0$. Atunci R este corp dacă și numai dacă $\{0\}$ și R sunt singurele ideale la stânga (la dreapta) ale lui R .

Proof. "⇒" 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 și cum $a^{-1}a \in I$ rezultă $1 \in I$. De aici se obține că $r = r1 \in I$ pentru orice $r \in R$, deci $I = R$.

"⇐" 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 $a' \neq 0$ și un raționament analog ne arată că există $a'' \in R$ cu proprietatea că $a''a' = 1$. Înmulțind la dreapta cu a obținem $a''a'a = a$, adică $a'' = a$. În concluzie, $aa' = 1$, deci a este inversabil. \square

Remarca 1.6. Deși în orice corp $\{0\}$ și corpul însuși sunt singurele ideale bilaterale, reciproc este fals: în inelul $R = M_2(\mathbb{Q})$ singurele ideale bilaterale sunt $\{0\}$ și R și acesta nu este corp. (Un inel cu proprietatea că nu are ideale bilaterale netriviale se numește *inel simplu*).

Definiția 1.7. Fie K un corp și $K' \subseteq K$ o submulțime nevidă. Atunci K' se numește subcorp al lui K dacă $(K', +, \cdot)$ este corp. În acest caz se mai spune că K este o extindere a lui K' .

Propoziția 1.8. Fie K un corp și $K' \subseteq K$ o submulțime nevidă. Atunci K' este subcorp al lui K dacă și numai dacă sunt satisfăcute următoarele condiții:

(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 $\mathbb{Z}/p\mathbb{Z}$ și \mathbb{Q} nu au subcorpuri proprii.

Definiția 1.11. Fie K, K' corpuri și $f : K \rightarrow K'$ o funcție. Aceasta se numește morfism de corpuri dacă

$$\begin{aligned} f(x + y) &= f(x) + f(y), \\ f(xy) &= f(x)f(y), \\ f(1) &= 1', \end{aligned}$$

pentru orice $x, y \in K$.

Remarca 1.12. (i) În definiția 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 $x \in K^\times$.

Propoziția 1.13. Orice morfism de corpuri este injectiv.

Proof. Fie $f : K \rightarrow K'$ un morfism de corpuri. Deoarece $\text{Ker } f$ este ideal bilateral al lui K rezultă că $\text{Ker } f = \{0\}$, deci f este morfism injectiv. \square

Lema 1.14. Fie K un corp și $K_\alpha \subseteq K$, $\alpha \in A$ o familie de subcorpuri ale lui K . Atunci $\bigcap_{\alpha \in A} K_\alpha$ este un subcorp al lui K .

Dacă considerăm intersecția tuturor subcorpurilor unui corp dat obținem un subcorp care nu are subcorpuri proprii.

Definiția 1.15. Un corp care nu are subcorpuri proprii se numește corp prim.

Deci orice corp conține ca subcorp un corp prim. După cum am observat deja, $\mathbb{Z}/p\mathbb{Z}$ și \mathbb{Q} sunt corpuri prime. Este adevărat însă și reciproc.

Propoziția 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 și $\varphi : \mathbb{Z} \rightarrow K$ dată prin $\varphi(n) = n \cdot 1$. Este clar că φ este morfism de inele și avem două posibilități:

(i) $\text{Ker } \varphi = \{0\}$, caz în care $\mathbb{Z} \simeq \text{Im } \varphi$, deci K conține un subinel izomorf cu \mathbb{Z} . Rezultă că K conține un subcorp izomorf cu \mathbb{Q} și cum K este corp prim obținem $K \simeq \mathbb{Q}$.

(ii) $\text{Ker } \varphi = p\mathbb{Z}$, $p \in \mathbb{N} \setminus \{0, 1\}$. Avem $\mathbb{Z}/p\mathbb{Z} \simeq \text{Im } \varphi \subseteq K$, 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 și cum K este corp prim obținem $K \simeq \mathbb{Z}/p\mathbb{Z}$. \square

Definiția 1.17. Fie K un corp. Dacă K conține un subcorp prim izomorf cu \mathbb{Q} , atunci spunem că K este corp de caracteristică zero și scriem $\text{char } K = 0$. Dacă K conține un subcorp prim izomorf cu $\mathbb{Z}/p\mathbb{Z}$, atunci spunem că K este corp de caracteristică p și scriem $\text{char } K = p$.

Remarca 1.18. (i) $\text{char } K = 0$ dacă și numai dacă $\text{ord}(1) = \infty$ în grupul $(K, +)$, iar $\text{char } K = p$ dacă și numai dacă $\text{ord}(1) = p$ în grupul $(K, +)$.

(ii) Dacă $K' \subseteq K$ este o extindere de corpuri, atunci $\text{char } K' = \text{char } K$.

Exemplul 1.19. (i) $\text{char } \mathbb{Q} = 0$ și $\text{char } \mathbb{Z}/p\mathbb{Z} = p$.
(ii) $\text{char } \mathbb{R} = 0$ și $\text{char } \mathbb{Q}(\sqrt{2}) = 0$.

Propoziția 1.20. Fie K un corp, $\text{char } K = p > 0$ și $a, b \in K$ 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 $k \in \{1, \dots, p-1\}$, deci $\binom{p}{k} = 0$ în K . În concluzie, $(a + b)^p = a^p + b^p$. \square

Corolarul 1.21. Fie K un corp comutativ cu $\text{char } K = p > 0$. Atunci aplicația $\varphi : K \rightarrow K$ definită prin $\varphi(x) = x^p$ este morfism de corpuri.

Morfismul definit în corolarul precedent se numește *endomorfismul lui Frobenius*.

2. CONSTRUCȚII 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 ușor că \mathbb{C} este corp în raport cu adunarea și înmulțirea matricelor. Există un morfism de corpuri $f : \mathbb{R} \rightarrow \mathbb{C}$ 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 și înmulțirea 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 $\mathbb{H} = \left\{ \begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} : a, b \in \mathbb{C} \right\}$. Se verifică ușor că \mathbb{H} este corp *necomutativ* în raport cu adunarea și înmulțirea matricelor. Elementele lui \mathbb{H} se numesc *cuaternioni*. Există un morfism de corpuri $f : \mathbb{C} \rightarrow \mathbb{H}$ dat prin $f(a) = \begin{pmatrix} a & 0 \\ 0 & \bar{a} \end{pmatrix}$. 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 $\mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ și $\mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$. Scriem $a = x + iy$, $b = z + it$, cu $x, y, z, t \in \mathbb{R}$. Atunci

$$\begin{pmatrix} a & b \\ -\bar{b} & \bar{a} \end{pmatrix} = x + \mathbf{i}y + \mathbf{j}z + \mathbf{k}t.$$

Deci $\mathbb{H} = \{x + \mathbf{i}y + \mathbf{j}z + \mathbf{k}t : x, y, z, t \in \mathbb{R}\}$ și avem relațiile:

$$\begin{aligned}\mathbf{i}\mathbf{j} &= \mathbf{k}, \quad \mathbf{j}\mathbf{i} = -\mathbf{k}, \\ \mathbf{j}\mathbf{k} &= \mathbf{i}, \quad \mathbf{k}\mathbf{j} = -\mathbf{i}, \\ \mathbf{k}\mathbf{i} &= \mathbf{j}, \quad \mathbf{i}\mathbf{k} = -\mathbf{j}, \\ \mathbf{i}^2 &= \mathbf{j}^2 = \mathbf{k}^2 = -1.\end{aligned}$$

Remarca 2.1. Cuaternionii $\{\pm 1, \pm \mathbf{i}, \pm \mathbf{j}, \pm \mathbf{k}\}$ formează un grup necomutativ în raport cu înmulțirea numit *grupul cuternionilor*.

3. Corpul de fracții al unui domeniu de integritate

Fie R un domeniu de integritate (cu $1 \neq 0$). Vom construi un corp comutativ care îl conține pe R ca subinel și 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 mulțime definim o relație binară astfel: $(a, b) \sim (c, d)$ dacă și numai dacă $ad = bc$. Este imediat că " \sim " este o relație de echivalență. Fie $Q(R) = R \times R^\times / \sim$. Clasa de echivalență a unei perechi (a, b) în raport cu relația " \sim " se va nota $\frac{a}{b}$ și se va numi *fracție*. Definim pe $Q(R)$ două operații algebrice astfel:

$$\begin{aligned}\frac{a}{b} + \frac{c}{d} &= \frac{ad + bc}{bd}, \\ \frac{a}{b} \cdot \frac{c}{d} &= \frac{ac}{bd},\end{aligned}$$

pentru orice $a, b, c, d \in R$, $b \neq 0$, $d \neq 0$. Aceste operații sunt bine definite și $(Q(R), +, \cdot)$ este un corp comutativ, numit *corpul de fracții* 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 $\varphi : R \rightarrow Q(R)$ 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 conține pe R ca subinel.

INELE DE POLINOAME

Pe parcursul acestui capitol inelele vor fi comutative și unitare iar morfismele de inele vor fi unitare.

1. INELE DE POLINOAME ÎNTR-O NEDETERMINATĂ

Fie R un inel comutativ și unitar. Notăm cu $R^{(\mathbb{N})}$ mulțimea șirurilor $(a_n)_{n \in \mathbb{N}}$ cu elemente din R și care au doar un număr finit de termeni nenuli. Pe $R^{(\mathbb{N})}$ definim două operații algebrice:

$$\begin{aligned}(a_n)_{n \in \mathbb{N}} + (b_n)_{n \in \mathbb{N}} &= (a_n + b_n)_{n \in \mathbb{N}}, \\ (a_n)_{n \in \mathbb{N}} \cdot (b_n)_{n \in \mathbb{N}} &= (c_n)_{n \in \mathbb{N}},\end{aligned}$$

unde $c_n = \sum_{i+j=n} a_i b_j$.

Propoziția 1.1. $(R^{(\mathbb{N})}, +, \cdot)$ este inel comutativ și unitar.

Definim un morfism injectiv de inele unitare $\varepsilon : R \rightarrow R^{(\mathbb{N})}$, $\varepsilon(a) = (a, 0, 0, \dots)$ care ne permite să-l identificăm pe R cu un subinel al lui $R^{(\mathbb{N})}$. Vom nota cu X șirul $(0, 1, 0, 0, \dots)$ și-l vom numi *nedeterminată*. Observăm că

$$X^n = (\underbrace{0, \dots, 0}_n, 1, 0, 0, \dots)$$

pentru orice $n \in \mathbb{N}^*$. Ca de obicei, considerăm X^0 ca fiind egal cu elementul unitate. Se observă că $(a_0, a_1, \dots, a_n, 0, 0, \dots) = \varepsilon(a_0) + \varepsilon(a_1)X + \dots + \varepsilon(a_n)X^n$ iar prin identificarea lui R cu un subinel al lui $R^{(\mathbb{N})}$ dată de ε putem scrie

$$(a_0, a_1, \dots, a_n, 0, 0, \dots) = a_0 + a_1X + \dots + a_nX^n.$$

Definiția 1.2. Inelul $R^{(\mathbb{N})}$ se notează cu $R[X]$ și se numește inelul polinoamelor în nedeterminata X cu coeficienți în R .

Dacă $f \in R[X]$, atunci $f = a_0 + a_1X + \dots + a_nX^n$, $a_i \in R$ și f se numește *polinom în nedeterminata X* . Polinoamele X^n , $n \in \mathbb{N}$ se numesc *monoame în nedeterminata X* . Așadar orice polinom este în mod unic o combinație liniară de monoame cu coeficienți în R . Polinoamele a_iX^i cu $a_i \neq 0$ se numesc *termeni* ai lui f , iar $a_i \neq 0$ *coeficienți*. Definim $\deg f = \max\{i : a_i \neq 0\}$ și-l numim *gradul* lui f . Dacă $n = \deg f$, atunci a_n se numește *coeficientul dominant* al lui f . Polinoamele al căror coeficient dominant este 1 se numesc polinoame *monice*.

În cele ce urmează vom face următoarea convenție: $\deg 0 = -\infty$.

Propoziția 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 și numai dacă produsul coeficienților dominanți ai lui f și g este nenul.

Corolarul 1.4. Fie R un inel integră. Atunci $\deg(fg) = \deg f + \deg g$ pentru orice $f, g \in R[X]$. Mai mult, $R[X]$ este, de asemenea, inel integră.

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 $R = \mathbb{Z}/4\mathbb{Z}$ și $f = \hat{1} + \hat{2}X \in R[X]$. Avem $f^2 = \hat{1}$, deci $f \in U(R[X])$, dar $f \notin U(R)$.

Exercițiul 1.7. Fie R un inel comutativ unitar și $f = a_0 + a_1X + \cdots + a_nX^n \in R[X]$. Să se arate că:

- (i) f este nilpotent dacă și numai dacă a_i este nilpotent pentru orice $0 \leq i \leq n$.
- (ii) f este inversabil dacă și numai dacă a_0 este inversabil și a_i este nilpotent pentru orice $1 \leq i \leq n$.

Reamintim că există un morfism (canonic) de inele unitare $\varepsilon : R \rightarrow R[X]$ dat prin $\varepsilon(a) = a$ pentru orice $a \in R$.

Teorema 1.8. (Proprietatea de universalitate a inelelor de polinoame într-o nedeterminată) Fie $\varphi : R \rightarrow S$ un morfism de inele comutative unitare și $s \in S$. Atunci există un morfism unitar $\bar{\varphi} : R[X] \rightarrow S$ unic cu proprietatea că $\bar{\varphi} \circ \varepsilon = \varphi$ și $\bar{\varphi}(X) = s$.

Proof. Să vizualizăm această proprietate cu ajutorul următoarei diagrame:

$$\begin{array}{ccc} R & \xrightarrow{\varepsilon} & R[X] \\ & \searrow \varphi & \downarrow \bar{\varphi} \\ & & S \end{array}$$

Definim $\bar{\varphi}(a_0 + a_1X + \cdots + a_nX^n) = \varphi(a_0) + \varphi(a_1)s + \cdots + \varphi(a_n)s^n$. Se arată ușor că $\bar{\varphi}$ este morfism unitar de inele care satisface cele două proprietăți. Mai mult, acesta este unic, deoarece $\bar{\varphi}(X) = s$ conduce la $\bar{\varphi}(X^i) = s^i$ pentru orice $i \geq 1$ iar $\bar{\varphi} \circ \varepsilon = \varphi$ este echivalent cu $\bar{\varphi}(a) = \varphi(a)$ pentru orice $a \in R$. \square

1.1. Funcții polinomiale. Rădăcini. Fie S un inel comutativ și unitar, $R \subseteq S$ un subinel și $i : R \rightarrow S$ morfismul incluziune. Fie $s \in S$. Din proprietatea de universalitate a inelelor de polinoame într-o nedeterminată există un morfism unitar $\bar{i}_s : R[X] \rightarrow S$ unic cu proprietatea că $\bar{i}_s \circ \varepsilon = i$ și $\bar{i}_s(X) = s$.

$$\begin{array}{ccc} R & \xrightarrow{\varepsilon} & R[X] \\ & \searrow i & \downarrow \bar{i}_s \\ & & S \end{array}$$

Dacă $f \in R[X]$, $f = a_0 + a_1X + \cdots + a_nX^n$, atunci $\bar{i}_s(f) = a_0 + a_1s + \cdots + a_ns^n$. Notăm $a_0 + a_1s + \cdots + a_ns^n$ cu $f(s)$ și avem $\bar{i}_s(f) = f(s)$.

Definiția 1.9. Un element $s \in S$ cu proprietatea că $f(s) = 0$ se numește rădăcină a lui f .

Pentru orice polinom $f \in R[X]$ putem defini o funcție $\tilde{f} : S \rightarrow S$ prin $\tilde{f}(s) = f(s)$ pentru orice $s \in S$.

Definiția 1.10. Funcția $\tilde{f} : S \rightarrow S$ definită mai sus se numește funcția polinomială pe S asociată lui f . Când $S = R$, funcția $\tilde{f} : R \rightarrow R$ se numește funcția polinomială asociată lui f .

Remarca 1.11. Polinoame diferite pot avea funcții polinomiale egale. De exemplu, $f, g \in \mathbb{Z}_2[X]$, $f = X$ și $g = X^2$. Avem că $\tilde{f}, \tilde{g} : \mathbb{Z}_2 \rightarrow \mathbb{Z}_2$, $\tilde{f}(\hat{0}) = \tilde{g}(\hat{0}) = \hat{0}$ și $\tilde{f}(\hat{1}) = \tilde{g}(\hat{1}) = \hat{1}$.

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 ÎMPĂRȚIRE CU REST PENTRU POLINOAME ÎNTR-O NEDETERMINATĂ

Teorema 2.1. (Teorema de împărțire 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 $f = gq + r$ și $\deg r < \deg g$.

Proof. Dacă $\deg f < \deg g$, atunci scriem $f = g \cdot 0 + f$. În cazul în care $\deg f \geq \deg g$ facem inducție după $\deg f$.

Unicitatea rezultă imediat folosind Propoziția 1.3(ii). \square

Corolarul 2.2. Fie R un inel, $f \in R[X]$ și $\alpha \in R$. Atunci există $q \in R[X]$ și $r \in R$ unice cu proprietatea că $f = (X - \alpha)q + r$.

Corolarul 2.3. (Bézout) Fie R un inel, $f \in R[X]$ și $\alpha \in R$. Atunci $X - \alpha \mid f$ dacă și numai dacă $f(\alpha) = 0$.

Exercițiul 2.4. Fie R inel comutativ unitar și $\alpha \in R$. Atunci $R[X]/(X - \alpha) \simeq R$.

Exercițiul 2.5. Arătați că:

- (i) $\mathbb{R}[X]/(X^2 + 1) \simeq \mathbb{C}$.
- (ii) $\mathbb{Z}[X]/(X^2 - 2) \simeq \mathbb{Z}[\sqrt{2}]$.

Exercițiul 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 $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Exercițiul 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 și că $\mathbb{Z}[X]/I$ nu este inel integru.

Exercițiul 2.8. Aflați inversul lui $\widehat{4X + 3}$ în inelul factor $\mathbb{Z}_{11}[X]/(X^2 + 1)$.

Propoziția 2.9. Fie R un inel integru și $f \in R[X]$, $\deg f = n$. Atunci f are cel mult n rădăcini distincte în R .

Proof. Fie $\alpha_1, \dots, \alpha_m \in R$ distincte cu proprietatea că $f(\alpha_i) = 0$ pentru orice $i = 1, \dots, m$. Vom demonstra prin inducție 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 inducție $(X - \alpha_1) \cdots (X - \alpha_{m-1}) \mid f$ și putem scrie $f = (X - \alpha_1) \cdots (X - \alpha_{m-1})g$ cu $g \in R[X]$. Din $f(\alpha_m) = 0$ obținem $(\alpha_m - \alpha_1) \cdots (\alpha_m - \alpha_{m-1})g(\alpha_m) = 0$. Dar cum R este integru și $\alpha_i \neq \alpha_m$ pentru orice $i \neq m$ rezultă $g(\alpha_m) = 0$ și din corolarul 2.3 deducem că $X - \alpha_m \mid g$.

În concluzie, $n = \deg f \geq m$. \square

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 șase rădăcini distincte în \mathbb{Z}_6 .

Corolarul 2.11. Fie R un inel integru infinit și $f, g \in R[X]$. Dacă $\tilde{f} = \tilde{g}$, atunci $f = g$.

Proof. Fie $h = f - g$. Deoarece $\tilde{f} = \tilde{g}$ avem $\tilde{h} = 0$, adică $h(\alpha) = 0$ pentru orice $\alpha \in R$. Din propoziția 2.9 rezultă $h = 0$. \square

Propoziția 2.12. (Relațiile lui Viète) Fie R un inel integru, $f \in R[X]$, $f = a_0 + a_1X + \dots + a_nX^n$, $a_n \neq 0$. Presupunem că f are n rădăcini $\alpha_1, \dots, \alpha_n \in R$. Atunci au loc relațiile:

$$\begin{aligned} \sum_{i=1}^n \alpha_i &= -\frac{a_{n-1}}{a_n} \\ \sum_{1 \leq i < j \leq n} \alpha_i \alpha_j &= \frac{a_{n-2}}{a_n} \\ &\dots\dots\dots \\ \prod_{i=1}^n \alpha_i &= (-1)^n \frac{a_0}{a_n} \end{aligned}$$

Proof. Arătăm prin inducție după n că $f = a_n(X - \alpha_1) \cdots (X - \alpha_n)$ și apoi identificăm coeficienții. \square

3. INELE DE POLINOAME ÎNTR-UN NUMĂR FINIT DE NEDETERMINATE

Definiția 3.1. Fie R un inel. Atunci inelul de polinoame în nedeterminatele X_1, \dots, X_n cu coeficienți în R se definește inductiv ca fiind $R[X_1, \dots, X_{n-1}][X_n]$ și se notează $R[X_1, \dots, X_n]$. Elementele inelului $R[X_1, \dots, X_n]$ se numesc polinoame în nedeterminatele X_1, \dots, X_n .

Remarca 3.2. Orice polinom $f \in R[X_1, \dots, X_n]$ se scrie (în mod unic) sub forma

$$f = f_0 + f_1X_n + \dots + f_rX_n^r$$

cu $f_i \in R[X_1, \dots, X_{n-1}]$ pentru orice $i = 0, 1, \dots, r$.

Propoziția 3.3. Pentru orice polinom $f \in R[X_1, \dots, X_n]$ există și sunt unice $k_1, \dots, k_n \in \mathbb{N}$ și $a_{i_1, \dots, i_n} \in R$, unde $0 \leq i_1 \leq k_1, \dots, 0 \leq i_n \leq k_n$ astfel încât

$$f = \sum_{i_1=0}^{k_1} \cdots \sum_{i_n=0}^{k_n} a_{i_1, \dots, i_n} X_1^{i_1} \cdots X_n^{i_n}.$$

Proof. Inducție după n . Scriem $f = f_0 + f_1X_n + \dots + f_{k_n}X_n^{k_n}$ cu $f_i \in R[X_1, \dots, X_{n-1}]$ și aplicăm ipoteza de inducție.

Pentru unicitate fie

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

și să presupunem că $f = 0$. Scriem

$$f = f_0 + f_1X_n + \dots + f_{k_n}X_n^{k_n},$$

unde $f_j = \sum_{i_1=0}^{k_1} \cdots \sum_{i_{n-1}=0}^{k_{n-1}} a_{i_1, \dots, i_{n-1}, j} X_1^{i_1} \cdots X_{n-1}^{i_{n-1}} \in R[X_1, \dots, X_{n-1}]$. Deoarece $f = 0$ rezultă $f_j = 0$ pentru orice $j = 0, 1, \dots, k_n$ și din ipoteza de inducție $a_{i_1, \dots, i_{n-1}, j} = 0$ pentru orice $j = 0, 1, \dots, k_n$. \square

Un polinom de forma $X_1^{i_1} \cdots X_n^{i_n}$ se va numi *monom în nedeterminatele* X_1, \dots, X_n iar *gradul* său se consideră a fi $i_1 + \cdots + i_n$. Așadar orice polinom $f \in R[X_1, \dots, X_n]$ este (în mod unic) o combinație liniară de monoame cu coeficienți în R . Polinoamele $a_{i_1, \dots, i_n} X_1^{i_1} \cdots X_n^{i_n}$ cu $a_{i_1, \dots, i_n} \neq 0$ se numesc *termeni* ai lui f , iar $a_{i_1, \dots, i_n} \neq 0$ *coeficienți*. Definim *gradul* lui f ca fiind maximul gradelor monoamelor care apar în scrierea sa. Dacă toate monoamele au același grad, atunci f se numește *polinom omogen*.

Remarca 3.4. Orice polinom se scrie în mod unic ca o sumă de polinoame omogene. Mai precis, dacă $f \in R[X_1, \dots, X_n]$, atunci $f = f_0 + f_1 + \cdots + f_t$ cu $f_i \in R[X_1, \dots, X_n]$ polinom omogen de grad i . În plus, $f = 0$ dacă și numai dacă $f_i = 0$ pentru orice $i = 0, 1, \dots, t$.

Propoziția 3.5. Fie $f, g \in R[X_1, \dots, X_n]$. 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 $R[X_1, \dots, X_n]$ este, de asemenea, integru și $\deg(fg) = \deg f + \deg g$ pentru orice $f, g \in R[X_1, \dots, X_n]$.

Proof. Prima afirmație rezultă imediat prin inducție 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 $f_p \neq 0$ și $g_q \neq 0$. De aici rezultă că $\deg f = p$ și $\deg g = q$. Cum însă $R[X_1, \dots, X_n]$ este inel integru vom avea $f_p g_q \neq 0$, deci $\deg(fg) = p + q$. \square

Corolarul 3.7. Fie R un inel integru. Atunci $U(R[X_1, \dots, X_n]) = U(R)$.

Reamintim că există un morfism canonic $\varepsilon : R \rightarrow R[X_1, \dots, X_n]$ 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 $\varphi : R \rightarrow S$ un morfism de inele comutative unitare și $s_1, \dots, s_n \in S$. Atunci există un morfism unitar de inele $\bar{\varphi} : R[X_1, \dots, X_n] \rightarrow S$ unic cu proprietatea că $\bar{\varphi} \circ \varepsilon = \varphi$ și $\bar{\varphi}(X_i) = s_i$ pentru orice $i = 1, \dots, n$.

Proof. Să vizualizăm această proprietate cu ajutorul următoarei diagrame:

$$\begin{array}{ccc} R & \xrightarrow{\varepsilon} & R[X_1, \dots, X_n] \\ & \searrow \varphi & \downarrow \bar{\varphi} \\ & & S \end{array}$$

Procedăm prin inducție după n aplicând în mod repetat teorema 1.8. \square

Exercițiul 3.9. Fie R inel comutativ unitar și $\alpha_1, \dots, \alpha_n \in R$. Atunci avem următorul izomorfism: $R[X_1, \dots, X_n]/(X - \alpha_1, \dots, X - \alpha_n) \simeq R$.

4. POLINOAME SIMETRICE

Fie R un inel comutativ și unitar, $n \geq 2$ și $\sigma \in S_n$. Din teorema 3.8 rezultă că există un morfism unitar de inele $\bar{\sigma} : R[X_1, \dots, X_n] \rightarrow R[X_1, \dots, X_n]$ cu proprietatea că $\bar{\sigma} \circ \varepsilon = \varepsilon$ și $\bar{\sigma}(X_i) = X_{\sigma(i)}$ pentru orice $i = 1, \dots, n$.

Exemplul 4.1. Fie $f \in R[X_1, X_2, X_3]$, $f = X_1^2 X_3 + X_1 X_2 X_3^2$ și $\sigma = (1 \ 2 \ 3)$. Atunci $\bar{\sigma}(f) = X_1 X_2^2 + X_1^2 X_2 X_3$.

În general vom avea că $\bar{\sigma}(f(X_1, \dots, X_n)) = f(X_{\sigma(1)}, \dots, X_{\sigma(n)})$ pentru orice $f \in R[X_1, \dots, X_n]$.

Remarca 4.2. (i) Dacă $\sigma, \tau \in S_n$, atunci $\overline{\sigma \circ \tau} = \bar{\sigma} \circ \bar{\tau}$.

(ii) $\bar{e}(f) = f$ pentru orice $f \in R[X_1, \dots, X_n]$, unde $e \in S_n$ este permutarea identică.

(iii) $\bar{\sigma}$ este un izomorfism, iar $\bar{\sigma}^{-1} = \overline{\sigma^{-1}}$.

Definiția 4.3. Fie $f \in R[X_1, \dots, X_n]$. Dacă $\bar{\sigma}(f) = f$ pentru orice $\sigma \in S_n$, atunci f se numește polinom simetric.

Remarca 4.4. $f \in R[X_1, \dots, X_n]$ este polinom simetric dacă și numai dacă $\bar{\tau}(f) = f$ pentru orice transpoziție $\tau \in S_n$.

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.

Propoziția 4.6. Mulțimea $\Sigma = \{f \in R[X_1, \dots, X_n] : f \text{ polinom simetric}\}$ este un subinel unitar al lui $R[X_1, \dots, X_n]$.

Proof. Rezultă din faptul că $\bar{\sigma}$ este morfism de inele pentru orice $\sigma \in S_n$. □

Propoziția 4.7. Polinoamele $s_k \in R[X_1, \dots, X_n]$ definite prin

$$s_k = \sum_{1 \leq i_1 < \dots < i_k \leq n} X_{i_1} \cdots X_{i_k},$$

pentru orice $k = 1, \dots, n$, sunt polinoame simetrice.

Proof. Se consideră polinomul

$$g(T) = (T - X_1) \cdots (T - X_n),$$

$g \in R[X_1, \dots, X_n][T]$. Avem că

$$g(T) = T^n - s_1 T^{n-1} + s_2 T^{n-2} - \cdots + (-1)^n s_n.$$

Fie $\sigma \in S_n$. Definim

$$\bar{\sigma} : R[X_1, \dots, X_n, T] \rightarrow R[X_1, \dots, X_n, T]$$

astfel: $\bar{\sigma}(X_i) = X_{\sigma(i)}$ pentru orice $i = 1, \dots, n$ și $\bar{\sigma}(T) = T$. Atunci

$$\bar{\sigma}(g) = (T - X_{\sigma(1)}) \cdots (T - X_{\sigma(n)}) = g.$$

Pe de altă parte,

$$\begin{aligned} \bar{\sigma}(g) &= \bar{\sigma}(T^n - s_1 T^{n-1} + s_2 T^{n-2} - \cdots + (-1)^n s_n) = \\ &= T^n - \bar{\sigma}(s_1) T^{n-1} + \bar{\sigma}(s_2) T^{n-2} - \cdots + (-1)^n \bar{\sigma}(s_n). \end{aligned}$$

De aici rezultă că $s_k = \bar{\sigma}(s_k)$ pentru orice $k = 1, \dots, n$, deci polinoamele s_k sunt simetrice. \square

Definiția 4.8. Polinoamele s_k , $k = 1, \dots, n$, definite mai sus se numesc polinoamele simetrice fundamentale în nedeterminatele X_1, \dots, X_n .

Definiția 4.9. Vom defini pe mulțimea monoamelor în n nedeterminate o relație de ordine astfel:

$$X_1^{i_1} \cdots X_n^{i_n} > X_1^{j_1} \cdots X_n^{j_n}$$

dacă există $s \in \{1, \dots, n\}$ cu proprietatea că $i_1 = j_1, \dots, i_{s-1} = j_{s-1}$ și $i_s > j_s$. Aceasta se va numi ordinea lexicografică.

Propoziția 4.10. Ordinea lexicografică este o relație de ordine totală pe mulțimea monoamelor.

Definiția 4.11. Fie $f \in R[X_1, \dots, X_n]$, $f \neq 0$ și 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 combinație liniară de monoame. Acesta se numește monomul principal al lui f și se notează $\text{LM}(f)$. Dacă $a \in R$, $a \neq 0$ este coeficientul monomului principal al lui f , atunci a se numește coeficientul principal al lui f și se notează $\text{LC}(f)$ iar $aX_1^{i_1} \cdots X_n^{i_n}$ se numește termenul principal al lui f și se notează $\text{LT}(f)$.

În mod evident avem $\text{LT}(f) = \text{LC}(f) \text{LM}(f)$.

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 $\text{LM}(f) = X_1^2X_2^2$, $\text{LC}(f) = 2$ și $\text{LT}(f) = 2X_1^2X_2^2$.

Lema 4.13. Fie $m_1, m_2 \in R[X_1, \dots, X_n]$ monoame cu $m_1 > m_2$. Atunci:

- (i) $m_1m > m_2m$, oricare ar fi $m \in R[X_1, \dots, X_n]$ monom.
- (ii) Dacă $m'_1, m'_2 \in R[X_1, \dots, X_n]$ sunt monoame și $m'_1 > m'_2$, atunci $m_1m'_1 > m_2m'_2$.

Proof. (i) Fie $m_1 = X_1^{i_1} \cdots X_n^{i_n}$, $m_2 = X_1^{j_1} \cdots X_n^{j_n}$ și $m = X_1^{k_1} \cdots X_n^{k_n}$. Deoarece $m_1 > m_2$ există $s \in \{1, \dots, n\}$ cu proprietatea că $i_1 = j_1, \dots, i_{s-1} = j_{s-1}$ și $i_s > j_s$. Atunci $i_1 + k_1 = j_1 + k_1, \dots, i_{s-1} + k_{s-1} = j_{s-1} + k_{s-1}$ și $i_s + k_s > j_s + k_s$, deci $m_1m > m_2m$.

(ii) Rezultă din (i): $m_1 > m_2 \implies m_1m'_1 > m_2m'_1$ iar $m'_1 > m'_2 \implies m_2m'_1 > m_2m'_2$. \square

Propoziția 4.14. Fie $f_1, f_2 \in R[X_1, \dots, X_n]$ polinoame nenule. Dacă $\text{LT}(f_1) = a_1m_1$, $\text{LT}(f_2) = a_2m_2$ și $a_1a_2 \neq 0$, atunci $\text{LT}(f_1f_2) = (a_1a_2)m_1m_2 = \text{LT}(f_1)\text{LT}(f_2)$.

Proof. Rezultă din lema 4.13. \square

Lema 4.15. Fie $f \in R[X_1, \dots, X_n]$, $f \neq 0$ polinom simetric și $\text{LM}(f) = X_1^{i_1} \cdots X_n^{i_n}$. Atunci $i_1 \geq \dots \geq i_n$.

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 și $\bar{\tau}(f) = f$, unde $\tau = (1\ 2)$. \square

Propoziția 4.16. *Orice șir 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 $s \in \{1, \dots, n\}$ cu proprietatea că $i_1 = j_1, \dots, i_{s-1} = j_{s-1}$ și $i_s > j_s$. 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 $k = 1, \dots, n$. Așadar 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. \square

Exercițiul 4.17. Arătați că orice șir 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 $f \in R[X_1, \dots, X_n]$ polinom simetric există și este unic un polinom $g \in R[X_1, \dots, X_n]$ astfel încât

$$f(X_1, \dots, X_n) = g(s_1(X_1, \dots, X_n), \dots, s_n(X_1, \dots, X_n)).$$

Existența: Fie $\text{LT}(f) = aX_1^{i_1} \cdots X_n^{i_n}$. Deoarece f este simetric avem $i_1 \geq \cdots \geq i_n$. Mai mult, $\text{LT}(s_k) = X_1 \cdots X_k$ pentru orice $k = 1, \dots, n$. De aici se obține că

$$\text{LT}(as_1^{i_1-i_2} \cdots s_{n-1}^{i_{n-1}-i_n} s_n^{i_n}) = \text{LT}(f).$$

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 și, în plus, $\text{LM}(f_1) < \text{LM}(f)$.

Unicitatea: Vom demonstra că dacă $h \in R[X_1, \dots, X_n]$ și $h(s_1, \dots, s_n) = 0$, atunci $h = 0$. Scriem

$$h = \sum_{i_1=0}^{k_1} \cdots \sum_{i_n=0}^{k_n} a_{i_1, \dots, i_n} X_1^{i_1} \cdots X_n^{i_n}$$

și din $h(s_1, \dots, s_n) = 0$ obținem

$$\sum_{i_1=0}^{k_1} \cdots \sum_{i_n=0}^{k_n} a_{i_1, \dots, i_n} s_1^{i_1} \cdots s_n^{i_n} = 0.$$

Se remarcăm acum că

$$\text{LM}(s_1^{i_1} \cdots s_n^{i_n}) = X_1^{k_1} \cdots X_n^{k_n},$$

unde $k_1 = i_1 + \cdots + i_n, k_2 = i_2 + \cdots + i_n, \dots, k_n = i_n$.

Se observă că dacă $(i_1, \dots, i_n) \neq (j_1, \dots, j_n)$, atunci $(k_1, \dots, k_n) \neq (l_1, \dots, l_n)$, unde $k_r = i_r + \cdots + i_n$, respectiv $l_r = j_r + \cdots + j_n$ pentru orice $r = 1, \dots, n$. Aceasta înseamnă că $\text{LM}(s_1^{i_1} \cdots s_n^{i_n}) \neq \text{LT}(s_1^{j_1} \cdots s_n^{j_n})$ dacă $(i_1, \dots, i_n) \neq (j_1, \dots, j_n)$, deci $a_{i_1, \dots, i_n} = 0$ pentru orice i_1, \dots, i_n . \square

Exercițiul 4.19. Să se arate că următoarele polinoame sunt simetrice și să se scrie fiecare dintre ele ca polinom de polinoamele simetrice fundamentale:

- (i) $X_1^3 X_2 + X_1^3 X_3 + X_1 X_2^3 + X_1 X_3^3 + X_2^3 X_3 + X_2 X_3^3$.
- (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 $f \in R[X_1, \dots, X_n]$ polinom simetric omogen de grad $k < n$. Dacă $f \neq 0$, atunci $f(X_1, \dots, X_k, 0, \dots, 0) \neq 0$.

Proof. Fie $\text{LM}(f) = X_1^{i_1} \cdots X_n^{i_n}$. Avem $i_1 \geq \dots \geq i_n$ și $i_1 + \dots + i_n = k$. Deoarece $k < n$ rezultă $i_{k+1} = \dots = i_n = 0$. Deci $\text{LM}(f) = X_1^{i_1} \cdots X_k^{i_k}$ și îl regăsim în $f(X_1, \dots, X_k, 0, \dots, 0)$. În concluzie, $f(X_1, \dots, X_k, 0, \dots, 0) \neq 0$. \square

Teorema 4.21. (Formulele lui Newton)

(i) $p_k - p_{k-1}s_1 + \dots + (-1)^n p_{k-n}s_n = 0$ pentru orice $k \geq n$.

(ii) $p_k - p_{k-1}s_1 + \dots + (-1)^{k-1} p_1 s_{k-1} + (-1)^k k s_k = 0$ pentru orice $k = 1, \dots, n-1$.

Proof. (i) Considerăm din nou polinomul $g \in R[X_1, \dots, X_n, T]$,

$$g(T) = (T - X_1) \cdots (T - X_n).$$

Avem că $g(T) = T^n - s_1 T^{n-1} + s_2 T^{n-2} - \dots + (-1)^n s_n$. Cum $g(X_i) = 0$ pentru orice $i = 1, \dots, n$ obținem

$$X_i^n - s_1 X_i^{n-1} + s_2 X_i^{n-2} - \dots + (-1)^n s_n = 0$$

pentru orice $i = 1, \dots, n$. Prin înmulțire cu X_i^{k-n} obținem

$$X_i^k - s_1 X_i^{k-1} + s_2 X_i^{k-2} - \dots + (-1)^n s_n X_i^{k-n} = 0$$

pentru orice $i = 1, \dots, n$. Adunăm aceste relații și obținem

$$p_k - s_1 p_{k-1} + \dots + (-1)^n s_n p_{k-n} = 0.$$

(ii) Fie $f = p_k - p_{k-1}s_1 + \dots + (-1)^{k-1} p_1 s_{k-1} + (-1)^k k s_k$, unde $k < n$. Acesta este polinom simetric omogen de grad k și

$$f(X_1, \dots, X_k, 0, \dots, 0) = p'_k - p'_{k-1}s'_1 + \dots + (-1)^{k-1} p'_1 s'_{k-1} + (-1)^k k s'_k,$$

unde p'_i, s'_j sunt polinoamele definite anterior, dar de data aceasta în nedeterminatele X_1, \dots, X_k . Din (i), cazul $k = n$, se obține $f(X_1, \dots, X_k, 0, \dots, 0) = 0$ și conform lemei 4.20, $f = 0$. \square

Exercițiul 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 $X^4 + X^3 + 2X^2 + X + 1$.

Exercițiul 4.23. Considerăm elementele $x_1, \dots, x_n \in \mathbb{C}$ cu proprietatea că $x_1^k + \dots + x_n^k = 0$ pentru orice $1 \leq k \leq n$. Să se arate că $x_1 = \dots = x_n = 0$.

Exercițiul 4.24. Să se rezolve în numere reale ecuația $\sqrt[4]{97-x} + \sqrt[4]{x} = 5$.

Exercițiul 4.25. Să se rezolve în numere reale sistemul de ecuații

$$\begin{cases} x^5 + y^5 = 33 \\ x + y = 3 \end{cases}$$

ARITMETICA ÎN \mathbb{Z} ȘI $K[X]$

1. DIVIZIBILITATE. ALGORITMUL LUI EUCLID.

Să începem prin a observa că inelele \mathbb{Z} și $K[X]$ (K corp comutativ) sunt domenii de integritate, $U(\mathbb{Z}) = \{-1, 1\}$ și $U(K[X]) = K^\times$.

Teorema 1.1. (Teorema de împărțire 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 $a = bq + r$ și $0 \leq r < |b|$.

Proof. Existența. Fie $r = \min\{a - bx : x \in \mathbb{Z} \text{ și } a - bx \geq 0\}$. Scriem $r = a - bq$, $q \in \mathbb{Z}$. Dacă $r \geq |b|$, atunci $0 \leq a - b(q + \text{sgn}(b)) < r$, contradicție. Așadar $r < |b|$.

Unicitatea. Fie $q', r' \in \mathbb{Z}$ cu proprietatea că $a = bq' + r'$ și $0 \leq r' < |b|$. Atunci $b(q - q') = r' - r$ și de aici obținem $|b||q - q'| = |r' - r| < |b|$, deci $q = q'$ și $r = r'$. \square

Definiția 1.2. Numărul întreg q din teorema de mai sus se numește câtul împărțirii lui a la b , iar r se numește restul împărțirii lui a la b .

Exemplul 1.3. Fie $a = -17$ și $b = 2$. Scriem $-17 = 2(-9) + 1$, deci $q = -9$ și $r = 1$.

În cele ce urmează R va desemna \mathbb{Z} sau $K[X]$.

Definiția 1.4. Fie $a, b \in R$. Spunem că b divide a dacă există $c \in R$ astfel încât $a = bc$ și 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) $1 \mid a$ și $a \mid 0$ pentru orice $a \in R$.

(ii) Dacă $b \neq 0$, atunci $b \mid a$ dacă și numai dacă restul împărțirii lui a la b este 0.

(iii) Dacă $b \mid a$ și $a \neq 0$, atunci $|b| \leq |a|$ pentru $R = \mathbb{Z}$, respectiv $\deg b \leq \deg a$ pentru $R = K[X]$.

Să enunțăm acum câteva proprietăți simple ale relației de divizibilitate.

Propoziția 1.6. (i) $a \mid b$ dacă și numai dacă $bR \subseteq aR$.

(ii) $a \mid a$ oricare ar fi $a \in R$.

(iii) $a \mid b$ și $b \mid c \Rightarrow a \mid c$.

(iv) $a \mid b_i, \forall i = 1, \dots, n \Rightarrow a \mid \sum_{i=1}^n \alpha_i b_i, \forall \alpha_i \in R$.

Definiția 1.7. Fie $a, b \in R$. Spunem că a și b sunt asociate în divizibilitate dacă $a \mid b$ și $b \mid a$.

Notăție: $a \sim b$.

Remarca 1.8. (i) " \sim " este o relație de echivalență pe R .

(ii) $a \sim 1$ dacă și numai dacă $a \in U(R)$.

Din propoziția 1.6(i) rezultă imediat că a este asociat în divizibilitate cu b dacă și numai dacă $aR = bR$.

Propoziția 1.9. Fie $a, b \in R$. Atunci a și b sunt asociate în divizibilitate dacă și numai dacă $b = \pm a$ pentru $R = \mathbb{Z}$, respectiv $b = au$, $u \in K^\times$ pentru $R = K[X]$.

Definiția 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) $d \mid a$ și $d \mid b$,
- (ii) $d' \mid a$ și $d' \mid b$ implică $d' \mid d$.

Notăție: c.m.m.d.c.(a, b) sau $\gcd(a, b)$ sau (a, b) .

Definiția 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) $a \mid m$ și $b \mid m$,
- (ii) $a \mid m'$ și $b \mid m'$ implică $m \mid m'$.

Notăție: c.m.m.m.c.(a, b) sau $\text{lcm}(a, b)$ 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 $d_1 \sim d_2$ și d_1 este un cel mai mare divizor comun al elementelor a, b , atunci și 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 și vom spune că c.m.m.d.c.(a, b) este unic până la o asociere în divizibilitate.

(ii) Considerații similare sunt valabile și pentru cel mai mic multiplu comun a două elemente $a, b \in R$.

Definiția 1.13. Două elemente $a, b \in R$ se numesc prime între ele sau relativ prime dacă $\text{c.m.m.d.c.}(a, b) = 1$.

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 $b = r_1q_2 + r_2$ cu $0 \leq r_2 < r_1$, respectiv $\deg r_2 < \deg r_1$. Dacă $r_2 \neq 0$, atunci scriem $r_1 = r_2q_3 + r_3$ cu $0 \leq r_3 < r_2$, respectiv $\deg r_3 < \deg r_2$ și așa mai departe. Obținem astfel un șir strict descrescător de numere naturale $r_1 > r_2 > \dots$, respectiv $\deg r_1 > \deg r_2 > \dots$ care nu poate fi infinit, deci va exista un $n \in \mathbb{N}^*$ astfel încât $r_n \neq 0$ și $r_{n+1} = 0$.

Să arătăm că r_n este un c.m.m.d.c. al elementelor $a, b \in R$. Deoarece $r_{n+1} = 0$ avem $r_{n-1} = r_nq_{n+1}$, deci $r_n \mid r_{n-1}$. Din relația $r_{n-2} = r_{n-1}q_n + r_n$ deducem că $r_n \mid r_{n-2}$. Astfel obținem $r_n \mid r_i$ pentru orice $i = 1, \dots, n$. Din relația $b = r_1q_2 + r_2$ 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 și b .

Fie acum d un divizor comun al lui a și b . Din relația $a = bq_1 + r_1$ deducem că $d \mid r_1$ și pas cu pas obținem $d \mid r_i$ pentru orice $i = 1, \dots, n$. 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 $a = 18$ și $b = 24$. Avem $18 = 24 \cdot 0 + 18$, $24 = 18 \cdot 1 + 6$, $18 = 6 \cdot 3$. Așadar $(18, 24) = 6$.

Exercițiul 1.15. Calculați $(24, 54)$ în \mathbb{Z} cu algoritmul lui Euclid.

Exercițiul 1.16. Calculați $(X^4 - 4X^3 + 1, X^3 - 3X^2 + 1)$ în $\mathbb{R}[X]$ cu algoritmul lui Euclid.

Propoziția 1.17. Fie $a, b, c \in R \setminus \{0\}$.

- (i) Dacă $d = (a, b)$, atunci există a', b' cu $a = da'$, $b = db'$ și $(a', b') = 1$.
- (ii) $(ac, bc) = (a, b)c$.
- (iii) $(a, b) = 1$ și $(a, c) = 1$ implică $(a, bc) = 1$.
- (iv) (Lema lui Euclid) $a \mid bc$ și $(a, b) = 1$ implică $a \mid c$.
- (v) $a \mid c$, $b \mid c$ și $(a, b) = 1$ implică $ab \mid c$.
- (vi) Există $[a, b]$ și $(a, b)[a, b]$ este asociat în divizibilitate cu ab .

Proof. (i) Fie $d' = (a', b')$. Deoarece $d' \mid a'$ și $d' \mid b'$ rezultă că $dd' \mid a$ și $dd' \mid b$, deci $dd' \mid d$ și cum $d \neq 0$ obținem $d' \mid 1$, adică $d' \sim 1$.

(ii) Egalitatea rezultă din algoritmul lui Euclid.

(iii) Fie $d = (a, bc)$. Din $d \mid a$ și $a \mid ac$ rezultă că $d \mid ac$, deci $d \mid (ac, bc)$. Din (ii) obținem $d \mid c$ și cum $d \mid a$ rezultă $d \mid 1$.

(iv) Din (ii) avem că $(ac, bc) = c$. Dar $a \mid ac$ și $a \mid bc$, deci $a \mid c$.

(v) Din (ii) avem că $(ac, bc) = c$. Dar $ab \mid ac$ și $ab \mid bc$, deci $ab \mid c$.

(vi) Fie $d = (a, b)$. Atunci există a', b' cu $a = da'$, $b = db'$ și $(a', b') = 1$. Fie $m = da'b'$. Deoarece $m = ab' = ba'$ rezultă $a \mid m$ și $b \mid m$. Fie $m' \in R$ astfel încât $a \mid m'$ și $b \mid m'$. Avem că $a' \mid \frac{m'}{d}$ și $b' \mid \frac{m'}{d}$. Din (v) rezultă $a'b' \mid \frac{m'}{d}$, deci $m \mid m'$. \square

Propoziția 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 $r = b - aq \in I$ și atunci neapărat $r = 0$, deci $b = aq \in aR$. \square

Propoziția 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 $aR \subseteq dR$ și $bR \subseteq dR$ rezultă $d \mid a$ și $d \mid b$. Fie acum $d' \in R$ cu proprietatea că $d' \mid a$ și $d' \mid b$, echivalent $aR \subseteq d'R$ și $bR \subseteq d'R$. 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 $mR \subseteq aR$ și $mR \subseteq bR$ rezultă $a \mid m$ și $b \mid m$. Fie acum $m' \in R$ cu proprietatea că $a \mid m'$ și $b \mid m'$, echivalent $m'R \subseteq aR$ și $m'R \subseteq bR$. Avem $m'R \subseteq aR \cap bR = mR$, deci $m \mid m'$. \square

Corolarul 1.20. Fie $a, b \in R$ și $d = (a, b)$. Atunci există $r, s \in R$ astfel încât $d = ar + bs$.

Remarca 1.21. Folosind corolarul precedent putem da o altă demonstrație propoziției 1.17.

Exercițiul 1.22. Determinați $(X^2 - 1)\mathbb{Q}[X] \cap (X^3 - 1)\mathbb{Q}[X]$ și $(X^2 - 1)\mathbb{Q}[X] + (X^3 - 1)\mathbb{Q}[X]$.

2. ELEMENTE PRIME. ELEMENTE IREDUCTIBILE

În continuare R va desemna \mathbb{Z} sau $K[X]$.

Definiția 2.1. (i) Un element $p \in R$ se numește prim dacă $p \neq 0$, $p \notin U(R)$ și $p \mid ab$ implică $p \mid a$ sau $p \mid b$.

(ii) Un element $q \in R$ se numește ireductibil dacă $q \neq 0$, $q \notin U(R)$ și $q = ab$ implică $a \in U(R)$ sau $b \in U(R)$.

Un element care nu este ireductibil se numește reductibil.

Remarca 2.2. Un element asociat cu un element prim (ireductibil) este de asemenea element prim (ireductibil).

Propoziția 2.3. Orice element prim este ireductibil.

Proof. Dacă $p \in R$ este element prim și $p = ab$, atunci $p \mid ab$ și de aici rezultă $p \mid a$ sau $p \mid b$. Să presupunem că $p \mid a$. Atunci există $a' \in R$ astfel încât $a = pa'$ și înlocuind în $p = ab$ obținem $p = pa'b$, de unde $1 = a'b$, deci $b \in U(R)$. \square

Este adevărat și reciproc.

Propoziția 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 $q = dq'$ și $a = da'$. Deoarece q este ireductibil rezultă $d \in U(R)$ sau $q' \in U(R)$. În primul caz $1 = (q, a)$ și din Lema lui Euclid obținem $q \mid b$. În cazul al doilea $q = (q, a)$ și astfel $q \mid a$. \square

Remarca 2.5. (i) Un număr $p \in \mathbb{Z}$ este prim dacă $p \notin \{-1, 0, 1\}$ și are ca divizori doar pe ± 1 și $\pm p$.

(ii) Un polinom $f \in K[X]$ este ireductibil dacă nu se poate scrie ca produs de două polinoame de grad ≥ 1 .

Definiția 2.6. Un număr întreg care nu este prim se numește compus, iar un polinom care nu este ireductibil se numește reductibil.

Exemplul 2.7. (i) Numerele $\pm 2, \pm 3, \pm 5, \dots$ sunt numere prime.

(ii) X este polinom ireductibil, iar X^2 este reductibil.

Propoziția 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 și 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 $\deg f = 2, 3$ și nu are rădăcini în K , atunci f este ireductibil, altminteri s-ar descompune într-un produs de două polinoame dintre care cel puțin unul are gradul 1. Dar orice polinom de grad 1 din $K[X]$ are o rădăcină în K , contradicție. \square

Exemplul 2.9. (i) Polinomul $X^2 - 2$ este ireductibil în $\mathbb{Q}[X]$, dar este reductibil în $\mathbb{R}[X]$.

(ii) Polinoamele $X^2 + X + 1$ și $X^3 + X + 1$ 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 $\mathbb{Z}_2[X]$: $X^4 + X^2 + 1 = (X^2 + X + 1)^2$.

Exercițiul 2.10. Determinați polinoamele ireductibile de grad ≤ 5 din $\mathbb{Z}_2[X]$.

Exercițiul 2.11. Descompuneți polinomul $X^{56} - X^{49} - X^7 + 1$ în produs de polinoame ireductibile în $\mathbb{Z}_7[X]$.

Propoziția 2.12. Fie $p \in R$ element prim. Atunci inelul factor R/pR este corp.

Proof. Fie $\hat{a} \in R/pR$, $\hat{a} \neq \hat{0}$. Aceasta înseamnă că $a \notin pR$, adică $p \nmid a$. Așadar $(p, a) = 1$. Atunci există $u, v \in R$ cu proprietatea că $pu + av = 1$. Trecând la clase de resturi modulo idealul pR obținem $\hat{a}\hat{v} = \hat{1}$, deci \hat{a} este inversabil. \square

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.

Propoziția 2.14. Dacă $a \in R$ este un element nenul și neinvertibil, atunci acesta admite o descompunere în produs finit de elemente prime și această scriere este unică (până la o asociere în divizibilitate și abstracție făcând de ordinea factorilor).

Proof. Existența. Presupunem că există $a \in R$ nenul și neinvertibil 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 și neinvertibile astfel încât $a = a_1 a_2$. 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 și a este produs de numere prime, respectiv produs de polinoame ireductibile, contradicție.

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 inducție după m) că $m = n$ și există $\sigma \in S_n$ astfel încât $p_i \sim p'_{\sigma(i)}$ pentru orice $i = 1, \dots, m$.

Dacă $m = 1$, atunci $p_1 = p'_1 \cdots p'_n$. Deoarece p_1 este prim acesta este ireductibil și rezultă că $n = 1$.

Presupunem acum că $m > 1$. Din $p_m \mid p'_1 \cdots p'_n$ obținem că există j astfel încât $p_m \mid p'_j$ și cum p'_j este ireductibil rezultă $p_m \sim p'_j$. Să considerăm $j = n$, scriem $p_m = up'_n$ cu $u \in U(R)$ și prin simplificare obținem $p_1 \cdots (up_{m-1}) = p'_1 \cdots p'_{n-1}$. Acum aplicăm ipoteza de inducție și deducem că $m - 1 = n - 1$ și există $\sigma' \in S_{n-1}$ astfel încât $p_i \sim p'_{\sigma'(i)}$ pentru orice $i = 1, \dots, m - 1$. \square

Corolarul 2.15. Fie $a, b \in R$ nenule și neinvertibile. 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 $(a, b) = \prod_{i=1}^r p_i^{\min(k_i, l_i)}$ și $[a, b] = \prod_{i=1}^r p_i^{\max(k_i, l_i)}$.

Teorema 2.16. Mulțimea numerelor prime pozitive, respectiv mulțimea polinoamelor ireductibile și monice din $K[X]$ este infinită.

Proof. Presupunem că mulțimea numerelor prime pozitive, respectiv mulțimea polinoamelor ireductibile și monice din $K[X]$ este finită. Să notăm cu p_1, \dots, p_r elementele sale. Atunci $N = p_1 \cdots p_r + 1$ admite o descompunere în factori primi,

respectiv polinoame ireductibile și de aici rezultă că există $i \in \{1, \dots, r\}$ cu proprietatea că $p_i \mid N$. Dar cum $p_i \mid p_1 \cdots p_r$ rezultă $p_i \mid 1$, contradicție. \square

Exercițiul 2.17. Determinați c.m.m.d.c. și c.m.m.m.c. pentru polinoamele $f = (X-1)(X^2-1)(X^3-1)(X^4-1)$ și $g = (X+1)(X^2+1)(X^3+1)(X^4+1)$ din $\mathbb{Q}[X]$.

3. TEOREMA FUNDAMENTALĂ A ALGEBREI

Teorema 3.1. (Teorema lui Kronecker) *Fie K un corp și $f \in K[X]$ cu $\deg f \geq 1$. Atunci există o extindere L a lui K în care f are cel puțin o rădăcină.*

Proof. Deoarece f se descompune în produs de polinoame ireductibile este suficient să demonstrăm teorema pentru cazul în care f este ireductibil și de grad ≥ 2 . Fie $L = K[X]/(f)$. Știm că L este corp iar morfismul canonic $K \rightarrow L$ 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 $\alpha \in L$ și $f(\alpha) = 0$. \square

Corolarul 3.2. *Fie K un corp și $f \in K[X]$ 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 puțin 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 și numai dacă $\deg f = 1$.*

(ii) *Fie $f \in \mathbb{R}[X]$ cu $\deg f \geq 1$. Atunci f este ireductibil dacă și numai dacă $\deg f = 1$ sau $\deg f = 2$ și 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 $a \in \mathbb{C}^\times$, $a_1, \dots, a_m \in \mathbb{C}$ distincte și $k_1, \dots, k_m \in \mathbb{N}^$.*

(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 $a \in \mathbb{R}^\times$, $a_1, \dots, a_r \in \mathbb{R}$ distincte, $b_1, c_1, \dots, b_s, c_s \in \mathbb{R}$ cu $b_i^2 < 4c_i$ pentru orice $i = 1, \dots, s$ și $k_1, \dots, k_r, l_1, \dots, l_s \in \mathbb{N}^$.*

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 $n \geq 1$.

Exercițiul 3.7. Arătați că polinomul $X^n - 2$ este ireductibil în $\mathbb{Q}[X]$ pentru orice $n \geq 1$.

Exercițiul 3.8. Descompuneți polinomul $X^n - 1$, $1 \leq n \leq 6$, în produs de polinoame ireductibile în $\mathbb{Q}[X]$, $\mathbb{R}[X]$, respectiv $\mathbb{C}[X]$.

4. TEOREMA CHINEZĂ A RESTURILOR

Fie $n_1, n_2 \geq 2$ două numere întregi prime între ele. Fie a_1, a_2 numere întregi fixate. Considerăm sistemul de congruențe

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \end{cases}$$

Vom arăta că sistemul dat are soluții și vom determina cea mai mică soluție pozitivă a acestuia.

Deoarece $(n_1, n_2) = 1$ avem că \hat{n}_1 este inversabil în $\mathbb{Z}/n_2\mathbb{Z}$, respectiv \hat{n}_2 este inversabil în $\mathbb{Z}/n_1\mathbb{Z}$. Așadar există $y_1, y_2 \in \mathbb{Z}$ cu proprietatea că $n_1 y_1 \equiv 1 \pmod{n_2}$, respectiv $n_2 y_2 \equiv 1 \pmod{n_1}$. Fie acum $x = a_1 n_2 y_2 + a_2 n_1 y_1$. Este evident că x este o soluție a sistemului de congruențe dat. Mai mult, sistemul are o infinitate de soluții, deoarece $x + kn_1 n_2$ este de asemenea soluție, oricare ar fi $k \in \mathbb{Z}$.

Ne propunem acum să determinăm cea mai mică soluție pozitivă a sistemului. Scriem $x = n_1 n_2 q + r$ cu $0 \leq r < n_1 n_2$. Dacă $r = 0$, atunci cea mai mică soluție pozitivă este $n_1 n_2$. În caz contrar, r este cea mai mică soluție pozitivă. Este evident că r este o soluție a sistemului. Să arătăm că este cea mai mică. Fie $0 < r' < r$ o altă soluție. Atunci $r \equiv r' \pmod{n_1}$ și $r \equiv r' \pmod{n_2}$, deci $n_1 \mid r - r'$ și $n_2 \mid r - r'$. Cum $(n_1, n_2) = 1$ deducem că $n_1 n_2 \mid r - r'$. Pe de altă parte, $0 < r - r' < n_1 n_2$, contradicție. \square

Să remarcăm că $(n_1, n_2) = 1$ este, în general, o condiție necesară: de exemplu, sistemul de congruențe

$$\begin{cases} x \equiv 1 \pmod{4} \\ x \equiv 2 \pmod{6} \end{cases}$$

nu are soluții.

Exercițiul 4.1. Să se afle cea mai mică soluție pozitivă a sistemului de congruențe

$$\begin{cases} x \equiv 5 \pmod{18} \\ x \equiv 27 \pmod{35} \end{cases}$$

Exercițiul 4.2. Rezolvați sistemul de congruențe

$$\begin{cases} 6x \equiv 2 \pmod{8} \\ 5x \equiv 5 \pmod{6} \end{cases}$$

Rezultatele de mai sus se pot generaliza la mai mult de două numere.

Teorema 4.3. (Teorema chineză a resturilor) Fie $s \geq 2$ și fie $n_1, \dots, n_s \geq 2$ numere întregi oricare două prime între ele. Fie a_1, \dots, a_s numere întregi fixate. Considerăm sistemul de congruențe

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ \dots\dots\dots \\ x \equiv a_s \pmod{n_s} \end{cases}$$

Acesta are o unică soluție $0 < x \leq n_1 \cdots n_s$.