

## 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  $U_\infty$  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  $\varphi_n$  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

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

$\varphi_a$  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  $f \in S(M)$ , iar funcția  $\psi : S(N) \rightarrow S(M)$ , dată prin  $\psi(f) = f$ , 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  $\varphi_n$  (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  $(\text{End}(\mathbf{Z}), \circ) \cong (\mathbf{Z}, \cdot)$ , izomorfism de monoizi. (De aici rezultă că  $(\text{Aut}(\mathbf{Z}), \circ) \cong (\{-1, 1\}, \cdot)$ , izomorfism de grupuri.)

3) Să se arate că  $(\text{End}(\mathbf{Z}_n), \circ) \cong (\mathbf{Z}_n, \cdot)$ , izomorfism de monoizi. (De aici rezultă că  $(\text{Aut}(\mathbf{Z}_n), \circ) \cong (U(\mathbf{Z}_n), \cdot)$ , 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  $\theta$  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  $\theta$  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,  $\theta$  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  $\theta$  este injectivă iar  $\mathbf{Z}_{mn}$  și  $\mathbf{Z}_m \times \mathbf{Z}_n$  au același număr de elemente, rezultă că  $\theta$  este și surjectivă, deci bijectivă. Așadar,  $\theta$  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,  $\theta$  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  $\theta$  este bijectivă, deci în acest caz  $\theta$  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  $\theta$  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  $\varphi$  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.