CURS IV
ELEMENTE DE TEORIA GRUPURILOR

§ 1. GRUPURI ŞI MORFISME DE GRUPURI

Grupuri

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

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

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

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

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

Exemple.

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

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

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

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

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

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

Grupul (U(**Z**), •) al elementelor inversabile ale monoidului multiplicativ (**Z**, •) al numerelor întregi este ({–1, 1}, •). 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 Propoziţia 1.3, Cursul 3. Să notăm că U((**Q**, •)) = (**Q***, •), U((**R**, •)) = (**R***, •) şi U((**C**, •)) = (**C***, •).

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

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

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

Exerciţii.

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

Reguli de calcul într-un grup

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

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

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

Într-adevăr, ţinând seama de asociativitate

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

ceea ce demonstrează relaţia de mai înainte.
În particular,

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

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

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

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

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

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

De asemenea, pentru grupuri, avem

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

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

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

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

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

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

Analog se demonstrează a doua lege de simplificare.

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

Morfisme de grupuri

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

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

Ca şi la monoizi, au loc următoarele afirmaţii:

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

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

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

1) f(e) = e';

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

Demonstraţie. 1) Avem

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

sau

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

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

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

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

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

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

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

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

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

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

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

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

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

Exemple.

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

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

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

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

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

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

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

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

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

Mai mult, este imediat că

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

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

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

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

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

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

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

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

Demonstraţie. Definim $f : G \to S(G)$ astfel: $f(x) = t_x$, unde $t_x : G \to G$ este dată prin $t_x(g) = xg$. Se verifică uşor că t_x este bijecţie, deci $t_x \in S(G)$.

- f injectivă: $f(x) = f(y)$ implică $t_x = t_y$ şi de aici rezultă că $t_x(e) = t_y(e)$, adică $xe = ye$, deci $x = y$.
- f morfism de grupuri: avem că $t_{xy}(g) = (xy)g = x(yg) = t_x(t_y(g)) = (t_x \circ t_y)(g)$ pentru orice $g \in G$, deci $t_{xy} = t_x \circ t_y$ ceea ce ne arată că $f(xy) = f(x) \circ f(y)$.

Exerciţii.

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

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

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

Produs direct de grupuri

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

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

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

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

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

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

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

şi

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

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

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

şi

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

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

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

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

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

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

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

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

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

introducem următoarea operaţie algebrică:

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

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

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

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

Aplicaţii.

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

Definim $\theta : \mathbf{Z}_{mn} \to \mathbf{Z}_m \times \mathbf{Z}_n$ prin $\theta(\overline{x}) = ([x], \{x\})$. Funcţia θ este bine definită, căci dacă $\bar{x} = \bar{y}$, adică $x \equiv y \pmod{mn}$, atunci $mn \mid x - y$, deci $m \mid x - y$ şi $n \mid x - y$, adică $x \equiv y \pmod{m}$ şi $x \equiv y \pmod{n}$, adică $[x] = [y]$ şi $\{x\} = \{y\}$ şi deci $([x], \{x\}) = ([y], \{y\})$, adică $\theta(\bar{x}) = \theta(\bar{y})$.

Avem că θ este morfism de grupuri, deoarece

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

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

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

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

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

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

Avem funcţia

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

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

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

şi

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

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

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

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

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

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

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

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

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

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

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