CURS III
LEGI DE COMPOZIŢIE. MONOIZI

§1. OPERAŢIE ALGEBRICĂ INTERNĂ

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

$$\varphi : M \times M \to M,$$
$$(x, y) \to \varphi(x, y).$$

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

Exemple.

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

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

$$s : \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z},$$
$$s(x, y) = x + (-y) = x - y.$$

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

3) Dacă M este o mulţime, pe mulţimea

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

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

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

4) Dacă M este o mulţime nevidă, iar

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

este mulţimea părţilor lui M, atunci reuniunea

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

şi intersecţia

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

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

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

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

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

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

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

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

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

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

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

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

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

În scriere aditivă condiţia de asociativitate se scrie

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

iar în scriere multiplicativă aceasta se scrie

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

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

Exemple.

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

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

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

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

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

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

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

şi

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

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

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

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

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

respectiv

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

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

Exemple.

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

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

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

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

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

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

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

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

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

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

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

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

Deci elementul neutru, dacă există, este unic determinat.

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

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

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

Cu aceste notaţii, condiţia elementului unitate devine

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

Exemple.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Această operaţie nu este asociativă; de exemplu,

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

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

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

Exemple.

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

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

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

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

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

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

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

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

§ 2. MONOIZI

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

Exemple.

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

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

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

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

Reguli de calcul într-un monoid

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

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

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

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

Lăsăm demonstraţia ca exerciţiu.

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

Din relaţia (1) deducem

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

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

Prin inducţie, se demonstrează uşor că

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

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

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

Morfisme de monoizi

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

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

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

Exemple.

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

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

este un morfism de monoizi.

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

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

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

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

Într-adevăr,

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

şi

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

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

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

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

În particular,

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

Compunerea morfismelor de monoizi

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

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

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

De asemenea,

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

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

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

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

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

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

Izomorfisme de monoizi

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Pe de altă parte,

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

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

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

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

Exemplu. Morfismul de monoizi

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

este izomorfism.

Produs direct de monoizi

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

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

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

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

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

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

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

şi

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

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

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

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

introducem următoarea operaţie algebrică:

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

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

Monoidul liber generat de o mulţime

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

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

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

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

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

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

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

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

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

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

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

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

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

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

şi

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

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

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

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

Corolarul 2.6. Fie A şi A' două mulţimi astfel încât există $f : A \rightarrow A'$ o funcţie bijectivă. Atunci există un unic izomorfism de monoizi $\overline{f} : L(A) \rightarrow L(A')$ astfel ca $\overline{f} \circ i_A = i_{A'} \circ f$, 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').