

# 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  $\varphi$  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  $\varphi$  nu este asociativă, se spune că  $\varphi$  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  $\varphi$  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  $\varphi$  nu este comutativă, se spune ca  $\varphi$  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  $\varphi$ , 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  $\varphi$  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  $\alpha$  și  $\beta$  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  $L(A')$ .