Structuri algebrice. Monoid. Grup

October 9, 2020

Fie A o mulțime nevidă. O funcție $\cdot : A \times A \to A$ se numește *lege de compoziție* binară pe A.
Fie o lege de compoziție "$\cdot$" pe mulțimea A. Unei perechi $(x, y) \in A \times A$ îi corespunde un element notat $x \cdot y \in A$.

Definition

O mulțime A dotată cu o lege de compoziție se numește **magmă**.

Definition

Legea de compoziție $\cdot$ pe mulțimea A se numește:
a) **asociativă** dacă $(\forall)x, y, z \in A$ are loc $(x \cdot y) \cdot z = x \cdot (y \cdot z)$.
b) **comutativă** dacă $(\forall)x, y \in A$ are loc $x \cdot y = y \cdot x$.
c) **cu element neutru** dacă

$$(\exists)e \in A, \quad (\forall)x \in A, \quad x \cdot e = e \cdot x = x.$$

Definition

O mulțime A dotată cu o lege de compoziție asociativă se numește **semigrup**.

O submulțime $A' \subset A$ spunem că este parte stabilă în raport cu "$\cdot$" dacă

$$(\forall) x, y \in A', \quad x \cdot y \in A'.$$

Propozitia

Dacă legea de compoziție "$\cdot$" pe A admite element neutru, atunci acesta este unic.

Demonstrație: Fie e și e' două elemente din A cu proprietatea că $(\forall)x \in A$ are loc $x \cdot e = e \cdot x = x$ și $x \cdot e' = e' \cdot x = x$. Pentru $x = e'$ în primul șir de egalități și $x = e$ în al doilea, rezultă $e' = e' \cdot e = e$, deci elementul neutru este unic. □

In cazul notației aditive, elementul neutru (dacă există) îl notăm 0 și îl mai numim *elementul nul /zero*. În notație multiplicativă, elementul neutru se notează 1 și se mai numește *elementul unu/unitate*. În general, elementul neutru se notează cu e.

Definition

O mulțime A pe care s-a dat o lege de compoziție asociativă și cu element neutru se numește **monoid**.

Example

a) Mulțimile de numere: naturale, întregi, raționale, reale, sunt monoizi în raport cu adunarea, respectiv cu înmulțirea uzuale definite pe acestea.
b) Dată fiind o mulțime nevidă, mulțimea A^A a tuturor funcțiilor definite pe A cu valori în A este monoid în raport cu compunerea funcțiilor. Elementul neutru este aici funcția identică $\mathbf{1_A}$.

Fie $(A, \cdot)$ un monoid și e elementul său neutru.

Definition

Un element $x \in A$ se numește **simetrizabil** dacă există un element $x' \in A$ astfel încât

$$x \cdot x' = x' \cdot x = e.$$

Propozitia

Fie $(A, \cdot)$ un monoid. Dacă $x \in A$ este simetrizabil, atunci simetricul său este unic.

Demonstrație: Fie x' și x'' două elemente din monoidul $(A, \cdot)$ cu proprietatea că

$$x \cdot x' = x' \cdot x = e, \quad x \cdot x'' = x'' \cdot x = e.$$

Înmulțind primul șir de egalități la stânga cu x'' și al doilea la dreapta cu x', obținem

$$x'' = x'' \cdot x \cdot x' = x',$$

deci simetricul unui element, dacă există, este unic. □

Elementul x' din definiția anterioară se numește în general *simetricul lui* x. În cazul notației aditive, simetricul lui x (dacă există) se mai numește *opusul* lui x și se notează $-x$. În notație multiplicativă, simetricul lui x (dacă există) se mai numește *inversul* lui x și se notează x^{-1}.

Mulțimea elementelor simetrizabile ale monoidului A se notează $U(A)$.

Example

a) În monoidul $(\mathbb{N}, +)$ singurul element simetrizabil este 0, pe când în monoizii $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, toate elementele sunt simetrizabile, opusul unui element x fiind numărul $-x$.
b) În monoidul $(\mathbb{N}, \cdot)$ singurul element simetrizabil este 1, în monoidul $(\mathbb{Z}, \cdot)$ singurele elemente simetrizabile sunt $-1, 1$, pe când în monoizii $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, toate elementele diferite de zero sunt simetrizabile, inversul unui element nenul x fiind numărul $\frac{1}{x}$.
c) În monoidul $(A^A, \circ)$ elementele simetrizabile sunt funcțiile bijective, știut fiind faptul că orice funcție bijectivă este inversabilă și reciproc. Mulțimea $U(A^A)$ se notează $S(A)$ și se numește mulțimea permutărilor mulțimii A.

Fie $(A, \cdot)$ un monoid și n un întreg pozitiv. Notăm

$$x^n = \underbrace{x \cdot x \cdot \ldots \cdot x}_{n} \in A.$$

În notație aditivă pentru un monoid $(A, +)$, egalitatea de mai sus se scrie

$$nx = \underbrace{x + x + \ldots + x}_{n}.$$

Propozitia

a) Dacă $x, y \in U(A)$, *atunci* $x \cdot y \in U(A)$ *și* $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$.
b) Dacă $x \in U(A)$, *atunci* $x^{-1} \in U(A)$ *și* $(x^{-1})^{-1} = x$.
c) Pentru orice întregi pozitivi n, m *și* $x \in A$, *au loc relațiile:*

$$e^n = e, \quad x^n \cdot x^m = x^{n+m}, \quad (x^n)^{-1} = (x^{-1})^n, \quad (x^m)^n = x^{nm}.$$

d) Pentru orice $x, y \in A$ *astfel încât* $x \cdot y = y \cdot x$, *are loc egalitatea*

$$(x \cdot y)^n = x^n \cdot y^n.$$

Fie $(A, \cdot)$, $(B, *)$ monoizi, cu elementele neutre e_A, respectiv e_B.

Definition

O funcție $f : A \to B$ se numește **morfism de monoizi** dacă verifică:

$$f(x \cdot y) = f(x) * f(y), \quad (\forall) x, y \in A.$$

Observatia

În multe monografii se consideră morfism de monoizi doar acele morfisme care satisfac și condiția $f(e_A) = e_B$, așa numitele morfisme unitare de monoizi.

Fie I o mulțime nevidă, cel mult numărabilă, numită *alfabet*. Elementele ei le numim simboluri. Numim *cuvânt de lungime n în alfabetul I* imaginea ordonată a unei funcții

$$f : \{1, 2, ..., n\} \to I, \quad \alpha = f(1)f(2)...f(n),$$

sau, altfel spus, o secvență finită, ordonată, de n elemente din I:

$$\alpha = a_1 a_2 ... a_n, \quad a_i \in I, \quad i = \overline{1, n},$$

unde $n \in \mathbb{N}^*$. Am notat $a_i = f(i)$ simbolul de pe poziția i în cuvântul α. Numim lungimea cuvântului α numărul simbolurilor sale. Dacă $\alpha = a_1 a_2 ... a_n$, atunci notăm lungimea sa $l(\alpha) = n$.

Din definiția cuvintelor ca funcții, este evident că două cuvinte $\alpha = a_1 a_2 ... a_n$ și $\beta = b_1 b_2 ... b_m$ sunt egale dacă $n = m$ (au aceeași lungime) și $a_i = b_i$, pentru orice $i = \overline{1, n}$.

Fie $L(I)$ mulțimea tuturor cuvintelor cu simboluri din I. Facem convenția că în $L(I)$ există și cuvântul e care nu are niciun simbol, adică $l(e) = 0$.
Pe $L(I)$ definim operația de concatenare (juxtapunere / alăturare), care acționează astfel:

$$(\forall)\alpha = a_1 a_2 ... a_n, \quad \beta = b_1 b_2 ... b_m, \quad \alpha\beta = a_1 a_2 ... a_n b_1 b_2 ... b_m.$$

Concatenarea este o lege de compoziție pe $L(I)$, asociativă și care admite elementul neutru e. Prin urmare $(L(I), \cdot)$ este un monoid, numit monoidul liber generat de I.
Funcția lungime $l : L(I) \to \mathbb{N}$, unde $l(\alpha)$ este lungimea cuvântului α, este morfism unitar surjectiv de monoizi.

Fie $\alpha \in L(I)$. Notăm

$$\alpha^0 = e, \quad \alpha^2 = \alpha\alpha, \quad \alpha^n = \alpha\alpha^{n-1}, \quad (\forall) n \in \mathbb{N}.$$

Dacă $I = \{a\}$, atunci $L(I) = \{e, a, a^2, ..., a^n, ...\}$ este un monoid comutativ. Mai mult, funcția

$$f : \mathbb{N} \to L(I), \quad f(n) = a^n, \quad (\forall) n \in \mathbb{N}$$

, este bijectivă, fiind inversa funcției lungime definită pe acest monoid.
Dacă $|I| \geq 2$, atunci $(L(I), \cdot)$ este monoid necomutativ. Într-adevăr, dacă există două simboluri diferite $a \neq b$ în I, atunci cuvintele ab și ba sunt diferite.

Deoarece egalitatea a două cuvinte revine la identificarea simbolurilor, putem afirma că monoidul liber generat de o mulțime este un monoid cu simplificare la stânga, adică

$$\alpha\beta = \alpha\gamma \Leftrightarrow \beta = \gamma.$$

Cuvântul α se numește *prefix* al cuvântului $\alpha\beta$. Regula de mai sus spune că dacă două cuvinte au același prefix, atunci sunt egale dacă stergând prefixul de la ambele, cuvintele rămase sunt egale.

Următoarele afirmații reprezintă așa-numitele *Proprietăți aritmetice ale monoidului liber generat de o mulțime*:

Propozitia

Fie I o mulțime nevidă și $(L(I), \cdot)$ monoidul liber generat de I. Dacă pentru cuvintele $p, q \in L(I)$ există un număr natural nenul n astfel încât $p^n = q^n$, atunci $p = q$.

Demonstrație: Pentru $n = 1$ este evident. Pentru $n \geq 2$, din egalitatea $l(p^n) = l(q^n)$ rezultă $l(p) = l(q)$. Fie $p = a_1 a_2 .. a_k$ și $q = b_1 b_2 ... b_k$. Egalitatea din ipoteză se scrie

$$a_1 a_2 .. a_k p^{n-1} = b_1 b_2 ... b_k q^{n-1}.$$

Identificând simbolurile, rezultă $a_i = b_i$, $(\forall) i = \overline{1, k}$, deci $p = q$. □

Propozitia

Fie p și q două cuvinte peste alfabetul I, cu proprietarea $pq = qp$. Atunci există $r \in L(I)$ și $n, m \in \mathbb{N}$ astfel încât $p = r^n$, $q = r^m$.

Demonstrație: Vom face demonstrația prin inducție matematică, după lungimea cuvântului pq.
Dacă $l(pq) = 0$, atunci $p = e$ și $q = e$, iar concluzia este adevărată.
Presupunem că pentru orice cuvinte p, q cu $l(pq) < n$ și $pq = qp$, există un cuvânt astfel încât p și q sunt puteri ale sale.
Fie acum cuvintele p, q cu $l(pq) = n$ și $pq = qp$. Fără a restrânge generalitatea, putem presupune $l(p) < l(q)$. Egalitatea $pq = qp$ spune că p este prefix al lui q, deci există $p_1 \in L(I)$ astfel încât $q = pp_1$. Simplificând la dreapta cu p relația $ppp_1 = pp_1p$, obținem $pp_1 = p_1p$. Mai mult, are loc și $l(pp_1) < n$. Aplicând ipoteza de inducție, rezultă că există $r \in L(I)$ și numerele naturale m, n astfel încât $p = r^n$, $p_1 = r^m$. Rezultă $q = r^{n+m}$. □

Propozitia

Dacă p, q, r sunt cuvinte peste alfabetul I pentru care există un număr natural nenul k astfel încât $pq^k = r^k p$, atunci pentru orice număr natural n are loc egalitatea $pq^n = r^n p$.

Exemplu:
Fie I un alfabet și $p, q, r \in L(I)$ astfel încât $pq^2 = r^2p$, $l(p) = 8$, $l(r) = 3$. Atunci $pq = rp$.
Într-adevăr, din egalitatea de cuvinte de mai sus rezultă mai întâi că $l(pq^2) = l(r^2p)$, deci $l(q) = l(r)$, apoi, prin inducție matematică, $pq^{2m} = r^{2m}p$, pentru orice număr natural m.
Evaluăm apoi egalitatea $pq^2 = r^2p$ din punct de vedere al lungimilor: $l(p) = 8$ este mai mic decât $l(r^2) = 6$. Considerăm egalitatea $pq^4 = r^4p$, de unde, din $l(p) < l(r^4)$, rezultă că p este un prefix de lungime 8 al cuvântului r^4. Adică p este format din primele 8 simboluri din cele 12 ale lui r^4. Deoarece $l(r) = 3$ putem scrie $r = a_1a_2a_3$ și obținem $p = r^2a_1a_2$.

Înlocuind expresia obținută pentru p în relația $pq^4 = rp$ putem calcula:

$$r^2 a_1 a_2 q^4 = r^4 r^2 a_1 a_2 \Rightarrow a_1 a_2 q^4 = (a_1 a_2 a_3)^4 a_1 a_2 \Rightarrow a_1 a_2 q^4 = a_1 a_2 a_3 (a_1 a_2 a$$

care implică $q^4 = (a_3 a_1 a_2)^4$, deci, conform Propoziției 3.1, $q = a_3 a_1 a_2$. Am obținut astfel

$$pq = r^2 a_1 a_2 a_3 a_1 a_2 = r^3 a_1 a_2 = rp.$$

Demonstrație: Pentru $n = 0$, este adevărat.
Dacă demonstrăm pentru $n = 1$, adică $pq = rp$, atunci prin inducție matematică se demonstrează pentru orice n. Într-adevăr, presupunând că $pq^i = r^i p$, concatenăm la dreapta cu q, deci $pq^{i+1} = r^i pq$, iar din $pq = rp$ rezultă $pq^{i+1} = r^i rp$, adică $pq^{i+1} = r^{i+1} p$. Conform principiului inducției matematice $pq^n = r^n p$ pentru orice număr natural n.

A rămas să demonstrăm $pq = rp$. Din ipoteză, există $k \in \mathbb{N}^*$ astfel încât $pq^k = r^k p$. Dacă $k = 1$, atunci am terminat. Dacă $k \geq 2$, atunci, prin inducție matematică rezultă $pq^{km} = r^{km} p$, pentru orice $m \in \mathbb{N}^*$.
Egalitatea cuvintelor $pq^k = r^k p$ conduce la faptul că au aceeași lungime și aceleași simboluri, în aceeași ordine. Primul fapt $l(pq^k) = l(r^k p)$ implică $l(p) + kl(q) = kl(r) + l(p)$, deci cuvintele q și r au aceeași lungime. Pentru a folosi identitatea simbolurilor, vom compara lungimea lui p cu lungimea lui r^k.

Dacă $l(p) \leq l(r^k)$, atunci p este prefix de lungime $l(p)$ al cuvântului r^k.
Dacă $l(p) < l(r^k)$, atunci există un număr natural m pentru care $l(p) < l(r^{mk})$. Îl alegem pe cel mai mic m cu această proprietate. Mai exact, acest număr este $\left[\frac{l(p)}{kl(r)}\right] + 1$. Considerăm egalitatea $pq^{km} = r^{km}p$, de unde rezultă că p este prefix al cuvântului r^{mk}, adică este de forma $p = r^s r_1$, unde am scris $r = r_1 r_2$ pentru a exprima acel prefix al cuvântului r care intră în componența lui p, după eventuale s expresii întregi ale lui r. Avem $s = \left[\frac{l(p)}{l(r)}\right]$, iar r_1 este prefixul de lungime $l(p) - sl(r)$ al lui r.

Revenind în egalitatea $pq^{km} = r^{km}p$ cu forma $p = r^s r_1$, obținem succesiv

$$r^s r_1 q^{km} = r^{mk+s} r_1 \Rightarrow r_1 q^{km} = r^{km} r_1 \Rightarrow r_1 q^{km} = r_1 r_2 r^{km-1} r_1 \Rightarrow$$

$$q^{km} = r_2 (r_1 r_2)^{km-1} r_1 \Rightarrow q^{km} = (r_2 r_1)^{km}.$$

Folosind Propoziția 3.1, rezultă $q = r_2 r_1$.
Calculăm $pq = r^s r_1 r_2 r_1 = r^{s+1} r_1$ și $rp = r r^s r_1 = r^{s+1} r_1$, de unde obținem $pq = rp$, ceea ce trebuia demonstrat. □