ASUPRA B-MONOIZILOR

Rezumat

Definind B-monoidul ca acea mulțime M înzestrată cu o operație (.) satisfăcînd proprietățile (A) și (B), autorul arată că dacă elementul neutru $e \in M$, atunci (B) implică proprietățile de asociativitate și de comutativitate, iar dacă $a, b \in M$, atunci are loc (1). De asemenea se extinde noțiunea de ideal la B-monoizi, așa cum se face în cazul semigrupurilor.

ASUPRA ÎMPĂRȚIRII CU REST ÎN INELUL CUATERNIONILOR ÎNTREGI

DE

GEORGE C. OPAIȚ

În această Notă ne propunem să studiem posibilitatea determinării cîtului și restului împărțirii la stînga sau la dreapta a doi cuaternioni întregi și ajungem la concluzia că acest lucru este totdeauna posibil în semigrupul multiplicativ al cuaternionilor întregi de norme impare. Acest rezultat permite definirea și construirea celui mai mare divizor comun stîng sau drept a doi cuaternioni întregi de norme impare și, în cele din urmă, o caracterizare completă a cuaternionilor ireductibili.

1. Împărțirea unui cuaternion întreg la un număr întreg

Definiția 1. *Un cuaternion*

$$\alpha = a + bi + cj + dk$$

se numește:
— *cuaternion întreg, dacă* a, b, c, d *sînt numere întregi,*
— *cuaternion primitiv, dacă* $(a, b, c, d) = 1$ *și*
— *cuaternion primitiv în raport cu numărul întreg* m, *dacă* $(a, b, c, d, m) = 1$.

Teorema 1. *Fiind dat un cuaternion întreg* $\alpha = a + bi + cj + dk$ *și un număr întreg* m *cu* $|m| > 2$ *se poate determina un cuaternion întreg* ξ *așa ca* $N(\alpha - m.\xi) < m^2$.

Pentru a fixa ideile putem presupune $m > 0$, căci dacă am determinat un cuaternion întreg ξ așa ca $N(\alpha - m.\xi) < m^2$ cu $m < 0$, atunci avem și $N(\alpha - (-m).(-\xi)) < (-m)^2$ cu $-m > 0$.

Va fi suficient să ne ocupăm numai de cuaternionii primitivi în raport cu m, deoarece dacă $(a, b, c, d, m) = h \neq 1$ și avem un cuaternion

ξ aşa ca $N(\alpha - m.\xi) < m^2$, atunci $a = h.a_1$, $b = h.b_1$, $c = h.c_1$, $d = h.d_1$ şi $m = h.m_1$ cu $(a_1, b_1, c_1, d_1, m_1)=1$ şi $h.(a_1 + b_1 i + c_1 j + d_1 k) = h.\alpha_1$, aşa ca

$$N(\alpha - m.\xi) = N(h.\alpha_1 - h.m_1.\xi) = N(h.(\alpha_1 - m_1.\xi)) =$$
$$= h^2.N(\alpha_1 - m_1.\xi) < h^2.m_1^2 \text{ şi deci } N(\alpha_1 - m_1.\xi) < m_1^2,$$

şi reciproc, din această inegalitate se obţine inegalitatea iniţială prin înmulţire cu h^2.

Fie deci $\alpha = a + bi + cj + dk$ un cuaternion primitiv în raport cu un număr întreg $m > 0$. Fie $\xi = x + yi + zj + uk$. Atunci:

$$N(\alpha - m.\xi) = (a - mx)^2 + (b - my)^2 + (c - mz)^2 + (d - mu)^2.$$

Acum nu avem decît să impunem condiţiile

$$(a - mx)^2 < \frac{m^2}{4},\ (b - my)^2 < \frac{m^2}{4},\ (c - mz)^2 < \frac{m^2}{4},\ \text{şi } (d - m)^2 < \frac{m^2}{4},$$

ceea ce ne conduce la

$$-\frac{m}{2} < a - mx < \frac{m}{2},$$

. . . . . .

de unde rezultă $\dfrac{a}{m} - \dfrac{1}{2} < x < \dfrac{a}{m} + \dfrac{1}{2}$,

. . . . . .

întrucît $(a/m + 1/2) - (a/m - 1/2) = 1$, există valori întregi pentru x, y, z, u cuprinse în intervalele

$$\left(\frac{a}{m} - \frac{1}{2},\ \frac{a}{m} + \frac{1}{2}\right),\ \left(\frac{b}{m} - \frac{1}{2},\ \frac{b}{m} + \frac{1}{2}\right), \ldots$$

cu excepţia cazului în care unele dintre extremităţile acestor intervale se exprimă prin numere întregi consecutive. Dacă extremităţile a cel puţin unuia dintre cele patru intervale nu se exprimă prin numere întregi consecutive, de exemplu intervalul în care este cuprins x, atunci există o valoare întreagă a lui x care satisface dubla inegalitate

$$\frac{a}{m} - \frac{1}{2} < x < \frac{a}{m} + \frac{1}{2}.$$

iar pentru y, z, şi u putem lua cîte una dintre valorile extremităţilor corespunzătoare, întrucît dintre inegalităţile de mai sus care condiţionează valorile x, y, z şi u este suficient ca una singură să fie inegalitate strictă, în celelalte putîndu-se lua şi semnul egal.

Să presupunem acum că toate extremităţile acestor intervale se exprimă prin numere întregi consecutive. Deci

$$\frac{a}{m} - \frac{1}{2} = k_1 \text{ şi } \frac{a}{m} + \frac{1}{2} = k_1 + 1$$

. . . . . .

de unde rezultă

$$\frac{2.a}{m} = 2.k_1 + 1$$

. . . .

Acum vom deosebi două cazuri:

1.) $(m, 2) = 1 \Rightarrow m/a,\ m/b,\ m/c,\ m/d$, absurd.

2.) $(m, 2) > 1$.

Dacă $m > 2$, atunci avem în mod necesar $m = 2.m_1$ cu $m_1 > 1$ şi m_1/a, m_1/b, m_1/c, şi m_1/d, ceea ce nu se poate deoarece cuaternionul α a fost presupus primitiv în raport cu m.

Dacă $m = 2$, atunci

$$a = 2k_1 + 1,\ b = 2k_2 + 1,\ c = 2k_3 + 1 \text{ şi } d = 2k_4 + 1$$

şi în acest caz numerele întregi x, y, z şi u nu se pot determina.

Observaţie. Teorema este valabilă şi pentru $m = 2$, cu condiţia ca coordonatele cuaternionului întreg α să nu fie toate impare.

2. Împărţirea cu rest a doi cuaternioni întregi. Teorema 2. *Fiind daţi doi cuaternioni întregi α şi $\beta \neq 0$, se pot determina doi cuaternioni întregi χ şi ρ aşa încît*

$$\alpha = \beta\chi + \rho \text{ cu } N(\rho) < N(\beta) \tag{1}$$

şi doi cuaternioni întregi χ_1 şi ρ_1 aşa încît

$$\alpha = \chi_1.\beta + \rho_1 \text{ cu } N(\rho_1) < N(\beta), \tag{2}$$

cu excepţia cazului în care împărţitorul este un cuaternion de normă 2.

Demonstraţie. Luînd $\gamma = \bar{\beta}.\alpha$ şi $m = \bar{\beta}\beta$, putem determina un cuaternion întreg χ aşa ca $N(\gamma - m.\chi) < m^2$. Dar $N(\gamma - m.\chi) = N(\bar{\beta}\alpha - \bar{\beta}\beta.\chi) = N(\bar{\beta}.(\alpha - \beta.\chi)) = N(\beta).N(\alpha - \beta.\chi) < (N(\beta))^2$, de unde rezultă că $N(\alpha - \beta.\chi) < N(\beta)$ şi deci $\alpha = \beta\chi + \rho$, unde $\rho = \alpha - \beta\chi$ cu $N(\rho) < N(\beta)$.

Pentru determinarea cuaternionilor întregi χ_1 şi ρ_1 luăm $\gamma = \alpha\bar{\beta}$ şi $m = \beta\bar{\beta}$.

Definiția 2. *Cuaternionii χ și ρ, determinați mai sus, se numesc cîtul respectiv restul împărțirii la stînga a cuaternionului întreg α la cuaternionul întreg $\beta \neq 0$, iar cuaternionii întregi χ_1 și ρ_1 se numesc cîtul respectiv restul împărțirii la dreapta a aceloraşi cuaternioni.*

Observație. Cuaternionii întregi χ și ρ respectiv χ_1 și ρ_1 nu se pot determina dacă $m = 2$, adică dacă $N(\beta) = 2$ și cuaternionul întreg α are toate coordonatele impare.

Singurii cuaternioni de normă 2 sînt:

$$1+i,\ 1-i,\ 1+j,\ 1-j,\ 1+k,\ 1-k,$$
$$i+j=(1+k).i,\ \text{deci asociat cu } 1+k,$$
$$i-j=(1-k).i,\ \text{deci asociat cu } 1-k,$$
$$i+k=i.(1+j),\ \text{deci asociat cu } 1+j,$$
$$i-k=i.(1-j),\ \text{deci asociat cu } 1-j,$$
$$j+k=(1+i).j,\ \text{deci asociat cu } 1+i,$$
$$j-k=(1-i).j,\ \text{deci asociat cu } 1-i$$

și opușii acestora care sînt asociați cu ei înșiși.

Să cercetăm acum ce formă trebuie să aibă un cuaternion întreg $\alpha = a + bi + cj + dk$ așa încît să nu se poată determina cîtul și restul împărțirii lui la stînga sau la dreapta printr-un cuaternion de normă 2. Vom cerceta numai cazurile în care împărțitorul este unul dintre cuaternionii:

$$1+i,\quad 1-i,\quad 1+j,\quad 1-j,\quad 1+k \quad \text{și} \quad 1-k.$$

Pentru $\beta = 1 + i$ avem:

$$\bar{\beta}\alpha = (a+b) + (b-a).i + (c+d).j + (d-c).k \text{ și } \alpha\bar{\beta} = (a+b) + (b-a).i + (c-d).j + c+d).k.$$

Deci nu se poate determina cîtul și restul împărțirii la stînga respectiv la dreapta al cuaternionului întreg α la cuaternionul întreg de normă 2, $1 + i$, dacă a și b pe de o parte și c și d pe de altă parte sînt de parități diferite.

Făcînd calculele și în celelalte cazuri, ajungem la concluzia că nu se poate determina cîtul și restul împărțirii la stînga sau la dreapta a unui cuaternion întreg α la un cuaternion întreg β cu $N(\beta) = 2$ dacă $N(\alpha) \equiv 0 \pmod 2$, dar $N(\alpha) \not\equiv 0 \pmod 4$.

Teorema 3. *Pentru orice cuaternion întreg α și orice număr prim $p > 2$ se poate construi un algoritm al lui Euclid.*

Demonstrație. În baza teoremei 1 putem scrie $\alpha = p.\chi + \rho$ cu $N(\rho) < p^2$. Deoarece $N(p) \not\equiv 0 \pmod 2$, putem scrie în baza teoremei 2

$$p = \rho\chi_1 + \rho_1 \text{ cu } N(\rho_1) < N(\rho).$$

indiferent dacă $N(\rho) = 2$ sau $N(\rho) \neq 2$. Dacă $N(\rho) = 2$, atunci $N(\rho_1) = 1$ sau 0. Dacă $N(\rho_1) = 0$, s-a terminat algoritmul, iar dacă $N(\rho_1) = 1$, mai

putem face o singură împărțire $\rho = \rho_1.\chi_2 + \rho_2$ cu $N(\rho_2) < N(\rho_1)$ și deci $N(\rho_2) = 0$ și de asemenea $\rho_2 = 0$. Să presupunem acum că $N(\rho) > 2$. Atunci avem

$$\alpha = p.\chi + \rho \qquad \text{cu } N(\rho) < p^2$$
$$p = \rho.\chi_1 + \rho_1 \qquad \text{cu } N(\rho_1) < N(\rho).$$

Acum putem continua, adică putem scrie

$$\rho = \rho_1.\chi_2 + \rho_2 \text{ cu } N(\rho_2) < N(\rho_1).$$

numai dacă $N(\rho_1) \neq 2$ sau dacă $N(\rho_1) = 2$ și $N(\rho) \not\equiv 0 \pmod 2$. Dar nu putem avea $N(\rho_1) = 2$ și $N(\rho) \equiv 0 \pmod 2$, căci atunci am avea și $N(\rho\chi_1) \equiv 0 \pmod 2$, ceea ce ne-ar conduce la $N(\rho) \equiv 0 \pmod 2$, ceea ce este absurd. Analog rezultă că în șirul împărțirilor succesive nu pot apărea două resturi consecutive pare.

Teorema 4. *Pentru orice cuaternioni de norme impare α și β se poate construi un algoritm al lui Euclid.*

Demonstrație. Fie α și β doi cuaternioni de norme impare. Atunci putem scrie

$$\alpha = \beta\chi + \rho \quad \text{cu} \quad N(\rho) < N(\beta).$$

Acum sau $N(\rho)$ este impară sau $N(\rho)$ este pară. În ambele cazuri se poate continua algoritmul.

$$\beta = \rho\chi_1 + \rho_1 \text{ cu } N(\rho_1) < N(\rho).$$

Algoritmul nu s-ar putea continua numai dacă $N(\rho_1) = 2$ și $2/N(\rho)$, dar atunci ar rezulta că $N(\beta)$ este pară, ceea ce este absurd. Deci cuaternionii ρ și ρ_1 nu pot fi ambii de norme pare așa că putem scrie $\rho = \rho_1.\chi_2 + \rho_2$ cu $N(\rho_2) < N(\rho_1)$ și de acum se repetă raționamentul.

3. Divizibilitatea în inelul cuaternionilor întregi. Definiția 3. *Dacă pentru doi cuaternioni întregi α și β are loc relația*

$$\alpha = \beta\chi, \text{ respectiv } \alpha = \chi_1.\beta,$$

unde χ și χ_1 sînt cuaternioni întregi, se zice că α se divide la stînga respectiv la dreapta prin β, sau că β este un divizor stîng sau la stînga respectiv drept sau la dreapta al lui α. Vom scrie β^s/α respectiv β^d/α.

Se deduce imediat că dacă β este un divizor stîng sau drept al lui α atunci $N(\beta)/N(\alpha)$.

Definiția 4. *Doi cuaternioni $\alpha \neq 0$ și $\beta \neq 0$ care se divid la stînga sau la dreapta unul prin celălalt se numesc cuaternioni asociați la stînga respectiv la dreapta.*

Consecință. Doi cuaternioni α și β asociați la stînga sau la dreapta diferă între ei printr-un factor drept respectiv stîng care este o unitate.

4. Cel mai mare divizor comun. Acum se poate defini cel mai mare divizor comun stîng sau drept a doi cuaternioni oarecare α și β, existența

justificîndu-se cu ajutorul algoritmului lui Euclid care este asigurat în semigrupul multiplicativ al cuaternionilor de norme impare. Se stabileşte că cel mai mare divizor comun stîng respectiv drept a doi cuaternioni întregi de norme impare α şi β aparţine idealului stîng respectiv drept generat de cuaternionii α şi β şi se demonstrează că acesta este cuaternionul de normă minimă din ideal. Apoi se mai demonstrează că cel mai mare divizor comun stîng sau drept a doi cuaternioni întregi de norme impare este determinat pînă la un factor drept respectiv stîng care este o unitate.

5. Caracterizarea cuaternionilor ireductibili. Definiţia 5. *Un cuaternion întreg $\pi \neq 0$, care nu este o unitate şi pentru care orice reprezentare de forma $\pi = \alpha.\beta$ nu este posibilă decît dacă α sau β este o unitate se numeşte cuaternion ireductibil.*

Observaţie. Dacă norma unui cuaternion întreg α este număr prim, atunci α este cuaternion ireductibil.

Consecinţă. Dacă cuaternionii întregi α şi β au un divizor comun la dreapta sau la stînga δ care nu este o unitate, atunci $N(\alpha)$ şi $N(\beta)$ au un divizor comun diferit de 1 şi anume pe $N(\delta)$.

Teorema 5. *Un cuaternion întreg α de normă impară şi un cuaternion întreg β de normă impară permutabil cu totalitatea cuaternionilor întreg sînt în acelaşi timp primi între ei la dreapta şi la stînga sau nu după cum $N(\alpha)$ şi $N(\beta)$ sînt prime între ele sau nu.*

Demonstraţie. În baza consecinţei precedente putem afirma că dacă cuaternionii întregi α şi β au un divizor comun δ care nu este o unitate, atunci $N(\alpha)$ şi $N(\beta)$ au un divizor comun diferit de 1 şi anume pe $N(\delta)$, aşa că $N(\alpha)$ şi $N(\beta)$ nu sînt prime între ele. Acum este suficient să demonstrăm că dacă cuaternionii α şi β sînt primi între ei la stînga şi la dreapta, atunci $N(\alpha)$ şi $N(\beta)$ sînt prime între ele. Pentru demonstraţie vom considera numai divizibilitatea la dreapta. Să luăm drept β pe r, unde r este un număr întreg. Se ştie că centrul algebrei cuaternionilor întregi este inelul întregilor [3].

Dacă cuaternionii întregi α şi r sînt primi între ei la dreapta atunci avem relaţia $\alpha_0\alpha + \beta_0 r = 1$, cu α_0 şi β_0 cuaternioni întregi, aşa că putem scrie

$$\alpha_0\alpha = 1 - \beta_0 r,$$

apoi

$$N(\alpha_0.\alpha) = N(1 - \beta_0.r) = (1 - \beta_0.r).(\overline{1 - \beta_0.r}) =$$
$$(1 - \beta_0.r).(1 - \overline{\beta}_0.r)$$
$$N(\alpha_0).N(\alpha) = 1 - \beta_0.r - \overline{\beta}_0.r + r^2.N(\beta_0).$$

Orice divizor prim al lui $N(\alpha)$ şi al lui $N(r) = r^2$ divide toţi termenii din membrul drept al ultimei egalităţi cu excepţia lui 1, aşa că un asemenea divizor $\neq 1$ nu există şi deci $N(\alpha)$ şi $N(\beta) = N(r) = r^2$ sînt prime între ele.

Teorema 6. *Un număr prim p considerat întreg nu este ireductibil.*

Pentru demonstraţie vom considera două cazuri:

1. Numărul prim considerat este 2.
2. Numărul prim considerat este impar.

Pentru numărul prim 2 afirmaţia decurge din faptul că

$$2 = (1 + i).(1 - i) = (1 + j).(1 - j) = (1 + k).(1 - k),$$

iar pentru un număr prim impar din faptul că orice număr natural se poate pune sub formă de sumă de patru pătrate perfecte (teorema lui Lagrange) [1], şi deci sub formă de produs de doi cuaternioni conjugaţi.

Teorema 7. *Condiţia necesară şi suficientă ca un cuaternion întreg π de formă impară să fie ireductibil este ca norma sa, $N(\pi)$, să fie un număr prim.*

Demonstraţie. Dacă $N(\pi)$ este un număr prim, atunci π este cuaternion ireductibil, căci dacă π n-ar fi cuaternion ireductibil, am avea $\pi = \alpha\beta$ cu $N(\alpha) \neq 1$ şi $N(\beta) \neq 1$ şi atunci am avea $N(\pi) = N(\alpha).N(\beta)$ şi deci $N(\pi)$ n-ar fi număr prim.

Să demonstrăm acum că dacă π este cuaternion ireductibil, atunci $N(\pi)$ este număr prim.

Fie π un cuaternion ireductibil şi p un factor prim al lui $N(\pi)$. În acest caz cuaternionul π şi p considerat ca un cuaternion întreg de normă impară, au un divizor comun care nu este o unitate şi prin urmare, ca divizor al cuaternionului ireductibil π trebuie să fie asociat cu π, aşa că p este divizibil prin π. Deci $p = \pi.\pi_1$, şi prin urmare $p^2 = N(\pi).N(\pi_1)$. π_1 nu poate fi o unitate, căci altfel $p = \pi.\pi_1$ ar fi asociat cu π şi deci ar fi un cuaternion ireductibil, ceea ce ar contrazice teorema 6. Trebuie să avem în mod necesar $N(\pi) = p$ şi $N(\pi_1) = p$, de unde rezultă că $N(\pi)$ este un număr prim, precum şi că π_1 este cuaternionul conjugat lui π.

BIBLIOGRAFIE

1. Buhstab A. A. — *Teorija cisel*, Moskva, 1960.
2. Creangă I. şi Reischer C. — *Algebra liniară*, Ediţia a II-a, Editura didactică şi pedagogică, Bucureşti, 1970.
3. Hurwitz A. — *Zahlentheorie der Quaternionen*, Berlin 1919.
4. Moisil Gr. C. — *Introducere în algebră. Inele şi Ideale*, vol. I, Bucureşti, 1954.
5. Opaiţ G. — *La notion d'espace cuaternionique*, Analele Univ. din Timişoara, Seria ştiinţe matematice, vol. VII, Fasc. 2, pg. 1969.

SUR LA DIVISION DANS L'ANNEAU DES QUATERNIONS ENTIERS

Résumé

Dans cette Note nous étudions la possibilité de déterminer le quotient et le reste de la division à gauche ou à droite de deux quaternions entiers et on conclut que c'est possible dans le demigroupe des quaternions entiers dont les normes sont impaires, ce qui permet la définition et la construction du plus grand commun diviseur à gauche ou à droite de deux quaternions de normes impaires.

Enfin on donne une condition nécessaire et suffisante pour qu'un quaternion entier soit irréductible.

ON THE ISOMORPHISM OF DIGRAPHS

BY

C. SMADICI and L. SMADICI

Theorem 1. *Let D_1, D_2 be two digraphs with the same number of nodes and A_1, A_2 be their adjacency matrices obtained for some arrangement of the nodes. The digraphs D_1 and D_2 are isomorphic if and only if there exists a permutation matrix P so that*

$$A_1P = PA_2.$$

The proof results from the definition of the isomorphism for two digraphs.

If D is a digraph with p nodes and A its adjacency matrix, let us consider the digraphs $D^j (1 \leqslant j \leqslant p)$ obtained from D by removing all the incident to v_j lines and let A^j be their corresponding matrices for the same degree of nodes. We shall denote by $a \oplus b = \max(a, b)$, a and b being real numbers.

Main Lemma. *If $p > 3$, then*

$$A = A \oplus A^2 \oplus A^3 \oplus \dots \oplus A^p.$$

Proof. Let a_{ij} be the element of i-th row and j-th column of the matrix A and b_{ij} the element of i-th row and j-th column of the matrix $B = A^1 \oplus A^2 \oplus A^3 \oplus \dots \oplus A^p$.

Case 1: If $a_{ij} = 1$, because $p > 3$, it follows that there exists $k \neq i, j$ so that $a^k_{ij} = 1$, where a^k_{ij} denotes the element of i-th row and j-th column of the matrix A^k, hence $b_{ij} = 1$.

Case 2: If $a_{ij} = 0$, it follows that for all integer k, $1 \leqslant k \leqslant p$, $a^k_{ij} = 0$, hence $b_{ij} = 0$ and therefore the lemma is proved.

Now, let us consider that we know the digraphs D_1 and D_2 with the same number of nodes and that for some order of nodes from D_1, there