

Kwaterniony uogólnione

1 Wstęp

Definicja 1 Kwaternionami uogólnionymi nad ciałem F będziemy nazywać F -algebry typu $A = \left(\frac{a,b}{F}\right)$, gdzie a, b są niezerowymi elementami ciała F . Bazą tej algebry jest czwórka $(1, i, j, k)$ z działaniami: $ij = -ji$, $i^2 = a$, $j^2 = b$, $k = ij$.

Bezpośrednio z łączności otrzymujemy:
 $k^2 = -ab$, $ki = -ik = -aj$, $kj = -jk = bi$.

Jeżeli F jest ciałem charakterystyki $\neq 2$ to A jest algebrą półprostą i prostą więc jest algebrą z dzieleniem lub izomorficzną z algebrą macierzy $M_2(F)$.

Centrum algebry A to F . Ponadto $A = F \oplus A_0$, Gdzie $F = \text{lin}\{1\}$, $A_0 = \text{lin}\{i, j, k\}$. W tym zapisie mnożenie przyjmuje postać:
 $(a + \alpha)(b + \beta) = ab + \alpha \bullet \beta + b\alpha + a\beta + \alpha \times \beta$, dla $a, b \in F$, $\alpha, \beta \in A_0$, gdzie $\alpha \bullet \beta$ jest dwuliniową formą symetryczną określoną wzorem:
 $(x_1i + x_2j + x_3k) \bullet (y_1i + y_2j + y_3k) = ax_1y_1 + bx_2y_2 - abx_3y_3$. "Iloczyn wektorowy" jest dwuliniową formą antysymetryczną określoną wzorem:

$$(x_1i + x_2j + x_3k) \times (y_1i + y_2j + y_3k) = \det \begin{pmatrix} x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \\ -bi & -aj & k \end{pmatrix}.$$

Stwierdzenie 2 Niech $\alpha, \beta, \gamma \in A_0$. Wówczas $-ab \det \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} = (\alpha \times \beta) \bullet \gamma$.

Dowód:

$\gamma = (z_1, z_2, z_3)$ i oznaczmy przez M_i minor macierzy bez trzeciego wiersza oraz i -tej kolumny.

$$L = ab(M_1z_1 - M_2z_2 + M_3z_3). \\ P = (-M_1bi + M_2aj + M_3k) \bullet (z_1 + z_2 + z_3) = -ab(M_1z_1 - M_2z_2 + M_3z_3) = L.$$

□

Wektory $\alpha, \beta \in A_0$ nazwiemy prostopadłymi gdy $\alpha \bullet \beta = 0$. Ponadto $\alpha \bullet (\alpha \times \beta) = 0$.

Stwierdzenie 3 $\alpha \bullet \beta = 0$ wtedy i tylko wtedy, gdy $\alpha\beta = -\beta\alpha$.

Dowód:

$$\alpha\beta + \beta\alpha = \alpha \bullet \beta + \alpha \times \beta + \beta \bullet \alpha + \beta \times \alpha = 2\alpha \bullet \beta.$$

□

Stwierdzenie 4 $A_0 = \{x \in A : x \notin F \text{ i } x^2 \in F\}$.

Dowód:

Niech $x = a + \alpha \in A \setminus F$ i $x^2 \in F$. $x^2 = a^2 + 2\alpha \bullet \alpha + 2a\alpha + \alpha \times \alpha = a^2 + 2\alpha \bullet \alpha + 2a\alpha$. Stąd $2a\alpha = 0 \Rightarrow a = 0$. Zatem $x = \alpha \in A_0$.

□

Podprzestrzeń A_0 jest "charakterystyczna" co opisujemy w twierdzeniu:

Twierdzenie 5 Niech $\phi : A \rightarrow B$ będzie zanurzeniem pierścieni,

gdzie $A = \left(\frac{a,b}{F}\right)$ i $B = \left(\frac{a',b'}{K}\right)$ są kwaternionami uogólnionymi

i B jest z dzieleniem. Wówczas:

1) $\phi(F) \subset K$.

2) $\phi(A_0) \subset B_0$.

Dowód:

Ad 1. Przypuśćmy, że $q \in F$ i $\phi(q) \notin K$. Rozpatrzmy centralizator $Z_B(\phi(q)) = Z_B(K(\phi(q))) = K(\phi(q))$, gdyż każde maksymalne podciało jest samocentralizujące. Dalej $i, j \in Z_A(q)$, więc $\phi(i), \phi(j) \in Z_B(\phi(q)) = K(\phi(q))$ są przemienne. Otrzymaliśmy sprzeczność.

Ad 2. Niech $\alpha \in A_0$. Wtedy $(\phi(\alpha))^2 = \phi(\alpha^2) \in K$ z 1). Zatem $\phi(\alpha) \in K$ lub $\phi(\alpha) \in B_0$. Ale istnieje $\beta \in A_0$ taka, że $\alpha\beta \neq \beta\alpha$. Stąd $\phi(\alpha)\phi(\beta) \neq \phi(\beta)\phi(\alpha)$ więc $\phi(\alpha) \notin K$.

□

Bezpośrednio otrzymujemy:

Wniosek 6

Jeżeli F nie jest ciałem formalnie rzeczywistym to nie istnieje zanurzenie algebry $A = \left(\frac{a,b}{F}\right)$ w kwaterniony.

Twierdzenie 7 Algebra A jest z dzieleniem wtedy i tylko wtedy, gdy

$\alpha \bullet \alpha = 0 \Leftrightarrow \alpha = 0$, dla $\alpha \in A_0$.

Dowód:

Algebra A jest z dzieleniem wtedy i tylko wtedy, gdy nie jest pierścieniem macierzy wtedy i tylko wtedy, gdy nie ma nietrywialnych nilpotentów. Niech $(a + \alpha)^2 = 0$ i $\alpha \neq 0$.

$0 = (a + \alpha)^2 = a^2 + 2\alpha \bullet \alpha + 2a\alpha + \alpha \times \alpha = a^2 + 2\alpha \bullet \alpha + 2a\alpha$. Stąd $2a\alpha = 0 \Rightarrow a = 0$. Zatem $\alpha \bullet \alpha = 0$.

□

Przykład 8 $A = \left(\frac{-1,1}{F}\right) \approx M_2(F)$, gdyż $(i + j)^2 = 0$.

Twierdzenie 9 Niech $F \subset \mathbb{R}$ zaś $a, b < 0$ i $\phi : A = \left(\frac{-a-b}{F}\right) \rightarrow H$ będzie zadany wzorami: $\phi(x) = x$ dla $x \in F$, $\phi(i) = i\sqrt{a}$ i $\phi(j) = j\sqrt{b}$. Wówczas ϕ jest zanurzeniem.

Dowód:

Sprawdzamy warunki. $\phi(i)^2 = -a = \phi(i^2)$, $\phi(j)^2 = -b = \phi(j^2)$ oraz $\phi(i)\phi(j) = -\phi(j)\phi(i)$.

□

2 Sumy kwadratów.

Opiszemy następujący podzbiór ciała liczb wymiernych:

$$G = \{q_1^2 + q_2^2 : q_1, q_2 \in \mathbb{Q}^+\}.$$

Twierdzenie 10 G jest podgrupą grupy mnożeniowej $\{\mathbb{Q}^+, \cdot\}$.

Ponadto liczba dodatnia wymierna nie należy do G wtedy i tylko wtedy, gdy można ją zapisać w postaci nq^2 , gdzie n jest bezkwadratową liczbą naturalną i pewna liczba pierwsza postaci $4k+3$ dzieli n .

Dowód:

- Zbiór G jest zamknięty na mnożenie zgodnie ze wzorem:
 $(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$.
- Zbiór G zawiera kwadraty, gdyż $q^2 = \left(q\frac{3}{5}\right)^2 + \left(q\frac{4}{5}\right)^2$.
- Zbiór G zawiera 2 i liczby pierwsze postaci $4k+1$.
- Niech $x = nq^2 = q_1^2 + q_2^2 \in G$, gdzie n jest bezkwadratową liczbą naturalną i pewna liczba pierwsza p dzieli n . Mnożąc obie strony otrzymujemy równanie $na^2 = b^2 + c^2$ w liczbach całkowitych. Bez zmniejszenia ogólności możemy przyjąć, że liczby a, b, c są parami względnie pierwsze i p nie dzieli b ani c . Przechodząc do ciała $\mathbb{Z}_p$ otrzymujemy: $0 = \bar{b}^2 + \bar{c}^2$ i $\bar{d}^2 + 1 = 0$. Stąd $\bar{d}$ jest elementem rzędu 4 w $\mathbb{Z}_p^*$ a więc p jest postaci $4k+1$.
- Niech $x = nq^2 \in G$, gdzie n jest bezkwadratową liczbą naturalną. Wówczas żadna pewna liczba pierwsza postaci $4k+3$ nie dzieli n . Ale $\frac{1}{x} = n\left(\frac{1}{nq}\right)^2$ jest tej samej postaci więc należy do G .

□

Twierdzenie 11 Grupa ilorazowa $\{\mathbb{Q}^+, \cdot\}/G$ ma naturalną strukturę przestrzeni liniowej nad ciałem $\mathbb{Z}_2$ o bazie złożonej z liczb pierwszych postaci $4k+3$. Ponadto jest izomorficzna z przestrzenią liniową nad ciałem $\mathbb{Z}_2$ na skończonych podzbiorach liczb pierwszych postaci $4k+3$ z różnicą symetryczną jako dodawaniem.

Dowód:

□

Uwaga 12 Niech $G_i = \{q_1^2 + q_2^2 + \dots + q_i : q_j \in \mathbb{Q}\}$. Wtedy G_1 i $G_4 = \mathbb{Q}^+$ są podgrupami oraz grupa ilorazowa G/G_1 ma naturalną strukturę przestrzeni liniowej nad ciałem $\mathbb{Z}_2$ o bazie złożonej z 2 i liczb pierwszych postaci $4k+1$.

$G_3 = \{nq^2 : q \in \mathbb{Q}, n \neq 8k+7 \text{ jest liczbą naturalną}\}$. Stąd G_3 jest zamknięte na odwracanie ale nie jest zamknięte na mnożenie, Np. $3 \cdot 5 = 8+7$.

3 Algebry wymiaru 4 nad $\mathbb{Q}$.

Twierdzenie 13 $A = \left(\frac{-1,a}{\mathbb{Q}}\right) \approx M_2(\mathbb{Q})$ wtedy i tylko wtedy, gdy $a \in G$.

Dowód:

$$\begin{aligned} \Rightarrow \text{Niech } 0 &= (xi + yj + zk)^2 = -x^2 + ay^2 + az^2. \text{ Stąd } a = \frac{x^2}{y^2+z^2} \in G \\ \Leftarrow \text{Niech } a \in G \text{ i } \frac{1}{a} &= y^2 + z^2. \text{ Wtedy } (i + yj + zk)^2 = -1 + ay^2 + az^2 = 0. \end{aligned}$$

□

Twierdzenie 14 Niech $a, b \in \mathbb{Q}^*$. Wówczas algebry $A = \left(\frac{-1,a}{\mathbb{Q}}\right)$ i $B = \left(\frac{-1,b}{\mathbb{Q}}\right)$ są izomorficzne wtedy i tylko wtedy, gdy a i b należą do tej samej warstwy $\{\mathbb{Q}^*, \cdot\}$ względem G .

Dowód:

$\Leftarrow$ Niech $b = a(x^2 + y^2)$. W algebrze A wybierzmy elementy i oraz $j' = xj + yk$. Wtedy $ij' = -j'i$ oraz $j' \bullet j' = ax^2 + by^2 = b$.
 $\Rightarrow$ Niech $f : A \rightarrow B$ będzie izomorfizmem. Wówczas $f(A_0) = B_0$. Przyjmijmy $f(i) = xi + yj + zk$, $t = yj - zk$. Wtedy $f(i)t = -tf(i)$ zatem $f(i)^\perp = \text{lin}\{t, tf(i)\}$. Ponieważ $f(j) \in f(i)^\perp$ więc $f(j) = ut + vtf(i)$. Teraz $f(j)^2 = u^2t + v^2(tf(i))^2$. Ale $(tf(i))^2 = t^2 = b(x^2 + y^2)$ więc $a = f(j)^2 = b(x^2 + y^2)(u^2 + v^2)$ jest w tej samej warstwie co b .

□

Twierdzenie 15 Algebra $A = \left(\frac{-1, a}{\mathbb{Q}} \right)$ jest zanurzalna w kwaterniony wtedy i tylko wtedy, gdy $a < 0$.

Dowód:

$\Leftarrow$ Wynika bezpośrednio z twierdzenia 9.

$\Rightarrow$ Niech $f : A \rightarrow H$ będzie zanurzeniem w kwaterniony.

Wówczas $a = f(a) = f(j^2) = f(j)^2 = -f(j)\overline{f(j)} < 0$.

□

Podsumowując, Każda algebra z dzieleniem typu, gdzie $a > 0$ jest izomorficzna z dokładnie jedną algebrą typu $\left(\frac{-1, n}{\mathbb{Q}} \right)$, gdzie n jest iloczynem różnych liczb pierwszych postaci $4k + 3$. Algebry te są niezanurzalne w kwaterniony.

Przykład 16 Niech $F = \mathbb{Q}(\sqrt{2})$ i $\phi : A = \left(\frac{-1, \sqrt{2}}{F} \right) \rightarrow H$ będzie zadany wzorami: $\phi(x + y\sqrt{2}) = x - y\sqrt{2}$ dla $x, y \in \mathbb{Q}$, $\phi(i) = i\sqrt[4]{2}$ i $\phi(j) = j\sqrt[4]{2}$. Wówczas ϕ jest zanurzeniem.

Sprawdzamy warunki. $\phi(i)^2 = -1 = \phi(i^2)$, $\phi(j)^2 = -\sqrt{2} = \phi(\sqrt{2}) = \phi(j^2)$ oraz $\phi(i)\phi(j) = -\phi(j)\phi(i)$.

Nie wiemy, czy każda algebra typu $\left(\frac{a, b}{\mathbb{Q}} \right)$ jest izomorficzna z algebrą typu $\left(\frac{-1, n}{\mathbb{Q}} \right)$.

Można pokazać, że $\left(\frac{-a^2, b}{\mathbb{Q}} \right)$ jest izomorficzna z algebrą typu $\left(\frac{-1, b}{\mathbb{Q}} \right)$ oraz, gdy a nie jest kwadratem to algebra $\left(\frac{a, b}{\mathbb{Q}} \right)$ jest izomorficzna z algebrą typu $\left(\frac{-1, n}{\mathbb{Q}} \right)$ gdy dla pewnych liczb wymiernych x, y, z zachodzi $b = y^2n + z^2n^2 - nx^2z^2$ lub $b = x^2 - (y^2 - z^2)^2$.