O wkładaniu grupy kwaternionów w macierze

Andrzej Strojnowski
Institute of Mathematics
ul. Banacha 2
Uniwersytet Warszawski
01-950 Warsaw, Poland

Streszczenie

Abstract. Pokażemy dla czego grupa kwaternionów jest zawarta w $Gl(4,K)$ dla dowolnej przemiennej dziedziny z jedynką K, że jest zawarta w $Gl(2,K)$ dla dziedzin charakterystyki > 2. Nie jest zaś zawarta w macierzach rzeczywistych $Gl(3,\mathbb{R})$.

1 Dziedziny charakterystyki $\neq 2$.

Symbolem $Q_8 = \langle i, j \mid j^4 = e,\ i^2 = j^2,\ ij = ji^3 \rangle$ oznacza będziemy grupę kwaternionów.

Stwierdzenie 1.1 *Jeżeli* $charK \neq 2$ *oraz* i *jest rozwiązaniem równania* $x^2 + 1 = 0$ *w* K *to macierze* $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ *oraz* $\begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$ *generują grupę kwaternionów.*

Wniosek 1.2 *Jeżeli* $charK \neq 2$ *to macierze*
$$\left[\begin{array}{cc|cc} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ \hline 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{array}\right] \text{ oraz } \left[\begin{array}{cc|cc} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ \hline 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{array}\right]$$
generują grupę kwaternionów.

Twierdzenie 1.3 *Niech* K *będzie ciałem charakterystyki* $\neq 2$.
Wówczas równoważne są warunki:
1) Grupa Q_8 *jest zawarta w grupie* $Gl(3, K)$.
2) Grupa Q_8 *jest zawarta w grupie* $Gl(2, K)$.
3) Równanie $x^2 + y^2 + 1 = 0$ *ma rozwiązanie w ciele* K.

Wniosek 1.4 *Grupa macierzy rzeczywistych* $Gl(3, \mathbb{R})$ *nie zawiera podgrupy* Q_8.

Wniosek 1.5 *Jeżeli K jest skończonym nieparzystym rozszerzeniem ciała $\mathbb{Q}$ to grupa macierzy rzeczywistych $Gl(3,K)$ nie zawiera podgrupy Q_8.*

W dowodzie twierdzenia posłużymy się prostymi lematami:

Lemat 1.6 *Niech K będzie ciałem charakterystyki $\neq 2$, w którym równanie $x^2+1=0$ nie ma rozwiązań. Jeżeli $M \in Gl(n,K)$ ma rząd 4, to wielomian charakterystyczny macierzy M jest postaci $w_M(x) = (x^2+1)^\alpha(1-x)^\beta(-1-x)^\gamma$, gdzie $\alpha > 0$.*

Dowód:
Wielomian charakterystyczny ma w rozkładzie te same czynniki pierwsze co wielomian minimalny równy $m(x) = x^4 - 1 = (x^2+1)(1-x)(-1-x)$. Zaś $\alpha > 0$ bo $M^2 \neq I$.

$\square$

Lemat 1.7 *Niech K będzie ciałem charakterystyki $\neq 2$, w którym równanie $x^2+1=0$ nie ma rozwiązań. Niech $f, g \in Aut(K^3)$ spełniają warunki: $f^4 = g^4 = id$, $fg = gf^3$ to istnieje wektor własny $w \neq \theta$ i wartości własne $\varepsilon, \delta \in \{-1,1\}$, dla których $f(w) = \varepsilon w$ i $g(w) = \delta w$.*

Dowód:
Na mocy poprzedniego lematu wielomiany charakterystyczne automorfizmów f i g mają postać $w_f(x) = (x^2+1)(\varepsilon - x)$ i $w_g(x) = (x^2+1)(\delta - x)$, gdzie $\varepsilon, \delta \in \{-1,1\}$. Zatem każdy z tych automorfizmów ma jedną jednowymiarową podprzestrzeń złożoną z wektorów własnych. Niech $\mathrm{lin}\{w\}$ będzie jedyną podprzestrzenią własną automorfizmu f i $f(w) = \varepsilon w$. Wtedy $fg(w) = gf^3(w) = g(\varepsilon^3 w) = \varepsilon g(w)$. Zatem $g(w) \in \mathrm{lin}\{w\}$. Zatem $\mathrm{lin}\{w\}$ jest wspólną podprzestrzenią własną.

$\square$

Dowód:
Jeżeli równanie $x^2+1=0$ ma rozwiązanie w ciele K to warunki 1) 2) i 3) są spełnione. Możemy zatem przyjąć, że równanie to nie ma rozwiązań.

1) $\Rightarrow$ 2) Niech $\phi : Q_8 \to Gl(3,K)$. Ponieważ automorfizmy przestrzeni K^3 wyznaczone przez macierze $\phi(i)$ oraz $\phi(j)$ spełniają założenia lematu **??** więc, przechodząc w razie potrzeby do macierzy podobnych, możemy przyjąć:
$$\phi(i) = \left[\begin{array}{c|cc} \varepsilon & * & * \\ \hline 0 & \multicolumn{2}{c}{\multirow{2}{*}{A}} \\ 0 & & \end{array}\right] \text{ oraz } \phi(j) = \left[\begin{array}{c|cc} \delta & * & * \\ \hline 0 & \multicolumn{2}{c}{\multirow{2}{*}{B}} \\ 0 & & \end{array}\right].$$
Warunki $j^4 = e$, $i^2 = j^2$, $ij = ji^3$ implikują $B^4 = I$, $A^2 = B^2$ oraz $AB = BA^3$. Istnieje zatem homomorfizm $\Psi : Q_8 \to Gl(2,K)$ spełniający warunki $\Psi(i) = A$ oraz $\Psi(j) = B$.

Jeżeli Ψ nie jest zanurzeniem to $i^2 \in \ker \Psi$.

A wtedy $\phi(i^2) = \left[\begin{array}{c|cc} \varepsilon^2 & * & * \\ \hline 0 & \multicolumn{2}{c}{\multirow{2}{*}{A^2}} \\ 0 & & \end{array}\right] = \begin{bmatrix} 1 & * & * \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ nie jest macierzą rzędu 2

bo $\begin{bmatrix} 1 & x & y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 2x & 2y \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$.

2) $\Rightarrow$ 3) Niech $A, B \in GL(2, K)$ generują grupę kwaternionów zaś $f, g \in Aut(K^2)$ indukowanymi przekształceniami. Ponieważ, na mocy lematu **??**, wielomian charakterystyczny f jest nierozkładalny i równy x^2+1. Stąd w dowolnej bazie typu $w, f(w)$ macierz f ma postać $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$. Przyjmijmy $A = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ i $B = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$.

Równanie $AB = BA^3$ daje $\begin{bmatrix} -c & -d \\ a & b \end{bmatrix} = \begin{bmatrix} -b & a \\ -d & c \end{bmatrix}$, czyli $d = -a$, $c = b$.

Równanie $B^2 = A^2$ ma postać $\begin{bmatrix} a & b \\ b & -a \end{bmatrix}^2 = \begin{bmatrix} a^2+b^2 & 0 \\ 0 & a^2+b^2 \end{bmatrix} = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}$.

Stąd $a^2 + b^2 = -1$.

3) $\Rightarrow$ 1) Niech $a^2 + b^2 = -1$ w K. Wtedy macierze $A = \begin{bmatrix} 0 & -1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ i $B = \begin{bmatrix} a & b & 0 \\ b & -a & 0 \\ 0 & 0 & 1 \end{bmatrix}$ generują podgrupę kwaternionów.

□

Lemat 1.8 (Lagrange) *W ciałach skończonych równanie* $x^2 + y^2 + 1 = 0$ *ma rozwiązanie.*

Jako wniosek otrzymujemy:

Twierdzenie 1.9 *Niech K będzie dziedziną charakterystyki > 2 to $Gl(2, K)$ zawiera podgrupę Q_8.*

2 Dziedziny charakterystyki 2.

Stwierdzenie 2.1 *Jeżeli K jest dziedziną charakterystyki 2 to grupa $Gl(2, K)$ nie zawiera elementów rzędu 4.*

Stwierdzenie 2.2 *Jeżeli K jest dziedziną charakterystyki 2 to grupa $Gl(3, K)$ zawiera podgrupę Q_8 wtedy i tylko wtedy gdy K zawiera podciało 4 - elementowe.*

Dowód:

Niech $A, B \in Gl(3, K)$ będą generatorami grupy kwaternionów. Na mocy poprzedniego stwierdzenia i lematu podobnego do lematu **??** automorfizmy K^3 wyznaczone przez te macierze mają wspólny wektor własny. Ponieważ przestrzeń jest cykliczna względem f to wektor własny można uzupełnić do bazy Jordana. Zatem możemy przyjąć:

$$A = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix} \text{ i } B = \begin{bmatrix} 1 & a & b \\ 0 & c & d \\ 0 & x & y \end{bmatrix}$$

Równanie $AB = BA^3$ daje $\begin{bmatrix} 1 & a+c & b+d \\ 0 & c+x & d+y \\ 0 & x & y \end{bmatrix} = \begin{bmatrix} 1 & 1+a & 1+a+b \\ 0 & c & c+d \\ 0 & x & x+y \end{bmatrix}$.

Stąd

$c = 1 = y$, $x = 0$, $d = a + 1$.

Równanie $B^2 = A^2$ ma postać

$$\begin{bmatrix} 1 & a & b \\ 0 & 1 & a+1 \\ 0 & 0 & 1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 2a & 2b + a^2 + a \\ 0 & 1 & 2a + 2 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Stąd $a^2 + a + 1 = 0$ i $F_2(a) \approx F_4$.

□

Twierdzenie 2.3 *Jeżeli K jest dziedziną charakterystyki 2 to grupa $Gl(4, K)$ zawiera podgrupę Q_8.*

Dowód:

Grupa taka jest generowana przez macierze

$$i = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \; j = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

□

3 Dziedziny charakterystyki 0.

Lemat 3.1 *Niezerowa liczba naturalna n jest sumą trzech kwadratów liczb wymiernych wtedy i tylko wtedy gdy równanie $x^2 + y^2 = -1$ ma rozwiązanie w ciele $Q(i\sqrt{n})$.*

Dowód:

$\Rightarrow$ Niech $n = a^2 + b^2 + c^2$. Wtedy

$\left(\frac{ac+bi\sqrt{n}}{a^2+b^2}\right)^2 + \left(\frac{bc-ai\sqrt{n}}{a^2+b^2}\right)^2 = \frac{a^2c^2-b^2n}{(a^2+b^2)^2} + i\frac{2acb\sqrt{n}}{(a^2+b^2)^2} + \frac{b^2c^2-a^2n}{(a^2+b^2)^2} - i\frac{2acb\sqrt{n}}{(a^2+b^2)^2} =$
$\frac{a^2c^2-b^2n}{(a^2+b^2)^2} + \frac{b^2c^2-a^2n}{(a^2+b^2)^2} = \frac{c^2-n}{a^2+b^2} = \frac{-a^2-b^2}{a^2+b^2} = -1$

$\Leftarrow$ Niech $(a+bi\sqrt{n})^2 + (c+di\sqrt{n})^2 = -1$. Co daje:
$a^2+2abi\sqrt{n}-nb^2+c^2+2cdi\sqrt{n}-nd^2 = -1$. Jest to równoważne układowi:
$a^2+c^2+1 = n(b^2+d^2)$ i $ab+cd = 0$.

Mnożąc pierwsze równanie przez (b^2+d^2) i uwzględniając drugie otrzymujemy:
$n(b^2+d^2)^2 = a^2b^2+c^2b^2+a^2d^2+c^2d^2+b^2+d^2 =$
$(ab+cd)^2+(ad-bc)^2+b^2+d^2 = (ad-bc)^2+b^2+d^2$

Zatem $n = \left(\frac{ad-bc}{b^2+d^2}\right)^2 + \left(\frac{b}{b^2+d^2}\right)^2 + \left(\frac{d}{b^2+d^2}\right)^2$.

$\square$

Twierdzenie 3.2 (Gauss) *Jeżeli n jest bezkwadratową liczbą naturalną to równoważne są warunki:*

1) n jest sumą trzech kwadratów liczb wymiernych,

2) n jest sumą trzech kwadratów liczb naturalnych,

3) n nie jest postaci $8k+7$.

Jako wniosek otrzymujemy:

Twierdzenie 3.3 *Jeżeli n jest bezkwadratową liczbą naturalną to równoważne są warunki:*

1) Grupa $Gl\Big(2, Q(i\sqrt{n})\Big)$ zawiera grupę Q_8.

2) Grupa $Gl\Big(3, Q(i\sqrt{n})\Big)$ zawiera grupę Q_8.

3) n nie jest postaci $8k+7$.

Twierdzenie 3.4 (Moser) *Niech $K = Q(\xi_n)$ będzie ciałem cyklotomicznym, gdzie ξ_m jest pierwiastkiem pierwotnym stopnia n z 1. Wówczas równanie $x^2+y^2 = -1$ ma rozwiązanie w ciele K wtedy i tylko wtedy gdy rząd 2 w grupie multyplikatywnej ciała Z_n jest liczbą parzystą.*

Jako wniosek otrzymujemy:

Twierdzenie 3.5 *Niech $K = Q(\xi_n)$ będzie ciałem cyklotomicznym, gdzie ξ_m jest pierwiastkiem pierwotnym stopnia n z 1. Wówczas równoważne są warunki:*

1) Grupa $Gl\Big(2, Q(\xi_n)\Big)$ zawiera grupę Q_8.

2) Grupa $Gl\Big(3, Q(\xi_n)\Big)$ zawiera grupę Q_8.

3) Rząd $1+1$ w grupie multyplikatywnej ciała Z_n jest liczbą parzystą.

4 Pytania

1) Które wynikania zostaną prawdziwe gdy w twierdzeniu 1.3 warunek K ciało zamienimy na "dziedzina z 1"?
2) Czy $Q_8 < Gl(2, \mathbb{Z}[i\sqrt{3}])$ lub $Q_8 < Gl(3, \mathbb{Z}[i\sqrt{3}])$?