Uniwersytet Warszawski
Wydział Matematyki, Informatyki i Mechaniki

Łukasz Marecik
Nr albumu: 277561

Algebry kwaternionów

Praca licencjacka
na kierunku MATEMATYKA
w zakresie MATEMATYKI STOSOWANEJ

Praca wykonana pod kierunkiem
dr Barbary Terlikowskiej-Osłowskiej
Instytut Matematyki
Zakład Algebry i Teorii Liczb

Lipiec 2011

Oświadczenie kierującego pracą

Potwierdzam, że niniejsza praca została przygotowana pod moim kierunkiem i kwalifikuje się do przedstawienia jej w postępowaniu o nadanie tytułu zawodowego.

Data Podpis kierującego pracą

Oświadczenie autora (autorów) pracy

Świadom odpowiedzialności prawnej oświadczam, że niniejsza praca dyplomowa została napisana przeze mnie samodzielnie i nie zawiera treści uzyskanych w sposób niezgodny z obowiązującymi przepisami.

Oświadczam również, że przedstawiona praca nie była wcześniej przedmiotem procedur związanych z uzyskaniem tytułu zawodowego w wyższej uczelni.

Oświadczam ponadto, że niniejsza wersja pracy jest identyczna z załączoną wersją elektroniczną.

Data Podpis autora (autorów) pracy

Streszczenie

W pracy przedstawiono ogólną konstrukcję algebry kwaternionów nad dowolnym ciałem charakterystyki różnej od 2, podstawowe własności oraz zastosowania zarówno praktyczne (obroty $\mathbb{R}^3$) jak i teoretyczne (teoria liczb).

Słowa kluczowe

kwaterniony, algebry nieprzemienne, obroty $\mathbb{R}^3$, grupa wolna, twierdzenie Lagrange'a o czterech kwadratach

Dziedzina pracy (kody wg programu Socrates-Erasmus)

11.1 Matematyka

Klasyfikacja tematyczna

11R52. Quaternion and other division algebras: arithmetic, zeta functions
20E05. Free nonabelian groups

Tytuł pracy w języku angielskim

Quaternion algebras

Spis treści

Wprowadzenie 5

1. Podstawowe własności algebr kwaternionów 7
1.1. Pojęcia wstępne 7
1.2. Konstrukcja kwaternionów uogólnionych 8
1.3. Izomorfizm algebr kwaternionów 15

2. Mechanika przestrzeni trójwymiarowej 19

3. O wolnych podgrupach grupy elementów odwracalnych algebr kwaternionów 23
3.1. Motywacja oraz wprowadzenie notacji 23
3.2. Poszukiwania grupy wolnej 24

4. Twierdzenie Lagrange'a o czterech kwadratach 31
4.1. Kwaterniony Hurwitz'a 31
4.2. Dowód twierdzenia Lagrange'a 34

Bibliografia 37

Wprowadzenie

Historia kwaternionów rozpoczyna się w roku 1843 wraz z odkryciem irlandzkiego matematyka Williama Hamiltona algebry kwaternionów (zwanych dalej hamiltonowskimi) nad ciałem liczb rzeczywistych. Początkowo, ze względu na nieprzemienność, kwaterniony były uważane za twór patologiczny (należy mieć na uwadze, że pojawiły sie przed macierzami), jednakże idealnie się sprawdzały do opisu obrotów $\mathbb{R}^3$. W niniejszej pracy uogólnimy pojęcie kwaternionów. W rozdziale 1 podamy ogólną konstrukcję kwaternionów nad dowolnym ciałem charakterystyki różnej od 2. Zbadamy też kiedy dwie algebry kwaternionów nad tym samym ciałem są izomorficzne. W rozdziale 2 skupimy się na pierwotnym, praktycznym zastosowaniu kwaternionów hamiltonowskich: powiążemy je z obrotami przestrzeni trójwymiarowej. W rozdziale 3 zbadamy podpierścienie kwaternionów hamiltonowskich pod kątem występowania podgrupy wolnej generowanej przez dwa elementy w grupie elementów odwracalnych. Natomiast w rozdziale 4 pokażemy praktyczne zastosowanie kwaternionów w teorii liczb, udowadniając klasyczne twierdzenie Lagrange'a o sumie czterech kwadratów.

Od czytelnika wymagamy znajomości materiału kursowego Geometrii z Algebrą Liniową I/II oraz Algebry I, nie definiując pojęć jak np. grupa, pierścień, ciało, przestrzeń liniowa oraz nie przedstawiając ich własności. Ponadto zakładamy znajomość definicji i podstawowych własności pewnych pojęć wprowadzonych na proseminarium algebraicznym, takich jak grupa wolna (zob. np. [Kar76]) oraz moduł (zob. np. [Brow77]).

W całej pracy przez $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$ będziemy oznaczali odpowiednio: ciało liczb rzeczywistych, ciało liczb wymiernych, pierścień liczb całkowitych, przez $\mathbb{N}$ będziemy rozumieli zbiór liczb naturalnych (z zerem !), a przez $\mathbb{N}_+$ zbiór liczb naturalnych dodatnich.

Na początku każdego rozdziału będziemy podawali odnośniki do literatury, na podstawie której ów rozdział powstał.

Rozdział 1

Podstawowe własności algebr kwaternionów

W rozdziale pierwszym zaczynamy przygodę ze światem kwaternionów od zdefiniowania pojęcia 'algebra' oraz definicji samych kwaternionów. Ogólny szkic został zaczerpnięty z [Brow68] oraz [Pier82].

1.1. Pojęcia wstępne

W tym podrozdziale będziemy zakładali, że R oznacza pierścień przemienny z 1.

Definicja 1.1.1. *Niech A będzie lewostronnym $R-$modułem, w którym jest zdefiniowane dwuliniowe odwzorowanie $A \times A \to A$ (oznaczone niżej przez zestawienie argumentów i nazywane* mnożeniem*), które jest łączne ($x(yz) = (xy)z$ dla każdego $x, y, z \in A$) oraz istnieje element neutralny $1_A \in A$ taki, że $1_A x = x 1_A = x$ dla każdego $x \in A$. Moduł A z tak wprowadzoną strukturą będziemy nazywali* algebrą nad pierścieniem R *bądź* R–algebrą.

Założenie, że mnożenie jest dwuliniowe jest równoważne lewostronnej i prawostronnej rozdzielności względem dodawania oraz zgodności z działaniem mnożenia przez skalary:

$$r(xy) = (rx)y = x(ry) \text{ dla każdego } r \in R,\ x, y \in A \tag{1.1}$$

Każda $R-$algebra jest pierścieniem z jedynką. Odwrotnie, jeżeli A jest pierścieniem z jedynką oraz lewostronnym $R-$modułem, który spełnia (1.1), to A jest $R-$algebrą.

Powiemy, że algebra A jest z dzieleniem, jeżeli pierścień A jest z dzieleniem. Analogicznie algebra A jest nieprzemienna, jeżeli pierścień A jest nieprzemienny.

Przykłady 1.1.2.

- *Dowolny pierścień przemienny z jedynką (czyli w szczególności ciało) jest algebrą nad samym sobą.*
- *Każde rozszerzenie ciała $L \supseteq K$ może być traktowane jako $K-$algebra przemienna z mnożeniem zewnętrznym elementów z L przez elementy z K zdefiniowanym jako zawężenie mnożenia $\cdot : L \times L \to L$ do $\cdot|_K : K \times L \to L$.*
- *Algebra macierzy, tzn. zbiór macierzy kwadratowych stopnia n nad R z dodawaniem i mnożeniem (Cauchy'ego) oraz mnożeniem macierzy przez skalar, jest nieprzemienną algebrą nad R.*

- *Pierścień wielomianów $R[x_1, x_2, \ldots]$ z dodawaniem i mnożeniem wielomianów oraz mnożeniem wielomianów przez skalar jest $R-$algebrą.*

Definicja 1.1.3. *Niech A, B będą algebrami nad tym samym pierścieniem R . Powiemy, że algebry A, B są izomorficzne, gdy istnieje izomorfizm modułów $\varphi : A \to B$, który zachowuje mnożenie, tzn.*

$$\forall x, y \in A \quad \varphi(x)\varphi(y) = \varphi(xy)$$

Zatem w szczególności izomorfizm algebr jest też izomorfizmem pierścieni.

Ponieważ w kolejnych rozdziałach będziemy zajmować się algebrami nad ciałem, warto uczynić prostą uwagę:

Uwaga 1.1.4. *Niech F będzie ciałem. Wtedy $F-$algebra A to przestrzeń liniowa ze strukturą pierścienia spełniająca warunek (1.1), natomiast izomorfizm $F-$algebr to izomorfizm przestrzeni liniowych zachowujący mnożenie.*

Lemat 1.1.5. *Niech A, B będą algebrami nad ciałem F i niech $\alpha_1, \ldots, \alpha_n$ będzie bazą A. Wówczas każdy izomorfizm liniowy $\varphi : A \to B$, taki że $\varphi(\alpha_i)\varphi(\alpha_j) = \varphi(\alpha_i\alpha_j)$ dla każdego $i, j \in \{1, \ldots, n\}$ (φ zachowuje mnożenie na bazie) jest izomorfizmem $F-$algebr.*

Dowód. Wystarczy sprawdzić, że φ zachowuje mnożenie. Niech zatem $x = \sum_{i=1}^n a_i\alpha_i \in A$, $y = \sum_{j=1}^n b_j\alpha_j \in A$. Wtedy

$$\varphi(x)\varphi(y) = \varphi\left(\sum_{i=1}^n a_i\alpha_i\right)\varphi\left(\sum_{j=1}^n b_j\alpha_j\right) = \sum_{i=1}^n a_i\varphi(\alpha_i)\sum_{j=1}^n b_j\varphi(\alpha_j) = \sum_{i=1}^n\sum_{j=1}^n a_ib_j\varphi(\alpha_i)\varphi(\alpha_j) =$$
$$= \sum_{i=1}^n\sum_{j=1}^n a_ib_j\varphi(\alpha_i\alpha_j) = \varphi\left(\sum_{i=1}^n\sum_{j=1}^n a_ib_j\alpha_i\alpha_j\right) = \varphi\left(\sum_{i=1}^n a_i\alpha_i\sum_{j=1}^n b_j\alpha_j\right) = \varphi(xy)$$

□

W dalszej części rozdziału będziemy zakładali, że F oznacza ciało charakterystyki *różnej* od 2.

1.2. Konstrukcja kwaternionów uogólnionych

Niech a, b będą niezerowymi elementami ciała F. Niech A będzie czterowymiarową przestrzenią liniową nad F z bazą e_0, e_1, e_2, e_3. Określamy mnożenie na zbiorze $\{e_0, e_1, e_2, e_3\}$:

$$e_0e_i = e_ie_0 = e_i \text{ dla } i = 0, 1, 2, 3$$
$$e_1^2 = ae_0, \qquad e_2^2 = be_0, \qquad e_3^2 = -abe_0 \tag{1.2}$$
$$e_1e_2 = -e_2e_1 = e_3, \qquad e_1e_3 = -e_3e_1 = ae_2, \qquad e_2e_3 = -e_3e_2 = (-b)e_1$$

Następnie iloczyn dwóch dowolnych elementów A definiujemy następująco:

$$\left(\sum_{i=0}^3 \alpha_ie_i\right)\left(\sum_{j=0}^3 \beta_je_j\right) = \sum_{0\leqslant i,j\leqslant 3} \alpha_i\beta_j(e_ie_j) \tag{1.3}$$

gdzie $\alpha_i \in F, \beta_j \in F$ dla $i, j = 0, 1, 2, 3$.

Twierdzenie 1.2.1. *Przestrzeń liniowa A z mnożeniem określonym wyżej jest algebrą nieprzemienną nad ciałem F.*

Dowód. W myśl definicji 1.1.1 trzeba pokazać, że mnożenie ma oczekiwane własności. Zatem musumy sprawdzić, że

1. Mnożenie jest łączne.
2. Mnożenie jest rozdzielne względem dodawania.
3. W zbiorze $A \setminus \{0\}$ istnieje element neutralny mnożenia.
4. Mnożenie jest zgodne z mnożeniem przez skalary.

Najłatwiejszy jest warunek (3). Na mocy 1.2 i 1.3 elementem neutralnym mnożenia jest e_0, bo

$$e_0\left(\sum_{i=0}^{3}\alpha_i e_i\right) = \sum_{i=0}^{3}\alpha_i(e_0e_i) = \sum_{i=0}^{3}\alpha_i e_i$$
$$\left(\sum_{i=0}^{3}\alpha_i e_i\right)e_0 = \sum_{i=0}^{3}\alpha_i(e_ie_0) = \sum_{i=0}^{3}\alpha_i e_i$$

Niech teraz

$$\alpha = \sum_{i=0}^{3}\alpha_i e_i, \quad \beta = \sum_{j=0}^{3}\beta_j e_j, \quad \gamma = \sum_{k=0}^{3}\gamma_k e_k, \quad a \in F \tag{1.4}$$

Ponieważ

$$a\left(\sum_{i=0}^{3}\sum_{j=0}^{3}\alpha_i\beta_j(e_ie_j)\right) = \sum_{i=0}^{3}\sum_{j=0}^{3}(a\alpha_i)\beta_j(e_ie_j) = \sum_{i=0}^{3}\sum_{j=0}^{3}\alpha_i(a\beta_j)(e_ie_j)$$

otrzymujemy, że

$$a(\alpha\beta) = (a\alpha)\beta = \alpha(a\beta)$$

Zatem warunek (4) jest spełniony. Sprawdzimy teraz warunek (2) :

$$\alpha(\beta+\gamma) = \sum_{i=0}^{3}\alpha_i e_i \sum_{j=0}^{3}(\beta_j+\gamma_j)e_j = \sum_{i,j=0}^{3}\alpha_i(\beta_j+\gamma_j)(e_ie_j) = \sum_{i,j=0}^{3}(\alpha_i\beta_j+\alpha_i\gamma_j)(e_ie_j) =$$
$$= \sum_{i,j=0}^{3}(\alpha_i\beta_j)(e_ie_j) + \sum_{i,j=0}^{3}(\alpha_i\gamma_j)(e_ie_j) = \alpha\beta+\alpha\gamma$$

Sprawdzenie wzoru $(\beta+\gamma)\alpha = \beta\alpha+\gamma\alpha$ przebiega analogicznie.

Dowód łączności mnożenia zaczniemy od sprawdzenia łączności na elementach bazy. Dowód przebiega przez sprawdzenie wszystkich przypadków. Sprawdzimy tu tylko dla jednego, pozostałe sprawdza się identycznie korzystając z (1.2) oraz (1.3). Mamy $e_1(e_3e_2) = e_1(-e_2e_3) = e_1(be_1) = b(e_1e_1) = bae_0 = abe_0$ oraz $(e_1e_3)e_2 = (ae_2)(e_2) = a(e_2e_2) = abe_0$. Zatem $e_1(e_3e_2) = (e_1e_3)e_2$. Mając sprawdzaną łączność mnożenia na bazie, sprawdzamy łączność na dowolnych elementach z A, stosując oznaczenia (1.4) :

$$\alpha(\beta\gamma) = \sum_{i=0}^{3}\alpha_i e_i \sum_{j,k=0}^{3}(\beta_j\gamma_k)(e_je_k) = \sum_{i,j,k=0}^{3}(\alpha_i(\beta_j\gamma_k))(e_i(e_je_k)) =$$
$$= \sum_{i,j,k=0}^{3}((\alpha_i\beta_j)\gamma_k))((e_ie_j)e_k) = \sum_{i,j=0}^{3}(\alpha_i\beta_j)(e_ie_j)\sum_{k=0}^{3}\gamma_k e_k = (\alpha\beta)\gamma$$

Ponieważ z definicji $e_1e_2 = -e_2e_1$, a ciało F jest charakterystyki różnej od 2, rzeczywiście otrzymaliśmy algebrę nieprzemienną.

□

Definicja 1.2.2. *Algebrę A otrzymaną za pomocą powyższej konstrukcji oznaczać będziemy przez*

$$A = \left(\frac{a, b}{F}\right)$$

i nazywać algebrą kwaternionów (uogólnionych) nad ciałem F*, natomiast elementy A będziemy nazywali* kwaternionami.

Niech $\alpha \in F$. Korzystając ze zgodności mnożenia stwierdzamy, że elementy postaci αe_0 są przemienne z dowolnymi elementami z A, bo dla $\beta \in A$:

$$(\alpha e_0)\beta = \alpha(e_0\beta) = \alpha(\beta e_0) = \beta(\alpha e_0)$$

Określmy przekształcenie $\varphi : F \to A$ wzorem $\varphi(\alpha) = \alpha e_o$. Jest oczywiste, że φ jest homomorfizmem pierścieni, a ponieważ jądro jest zerowe, φ jest włożeniem ciała F w pierścień A. Zauważmy też, że mnożenie (w sensie przestrzeni liniowej) dowolnego kwaternionu przez $\alpha \in F$ daje ten sam wynik co mnożenie (w sensie działania pierścieniowego) tego kwaternionu przez αe_0. Zatem w dalszym ciągu zbiór elementów A postaci αe_0, gdzie $\alpha \in F$ będziemy utożsamiać z ciałem F, pisząc po prostu α zamiast αe_0.

Uwaga 1.2.3. *Elementy e_0, e_1, e_2, e_3 są często oznaczane przez $1, i, j, k$.*

W dalszej części tej pracy będziemy używać zamiennie tych oznaczeń, skłaniając się jednak w stronę przedstawiania bazy jako $1, i, j, k$ (notacja ta wydaje się bardziej czytelniejsza, natomiast notacja z „ponumerowanymi" współrzędnymi bywa elegantsza w dowodach).

Zatem tabelka mnożenia dla elementów bazowych wygląda następująco:

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	a	k	aj
j	j	$-k$	b	$-bi$
k	k	$-aj$	bi	$-ab$

Uwaga 1.2.4. *Niech R będzie pierścieniem przemiennym z jedynką bez (niewłaściwych) dzielników zera, dla którego $1 + 1 \neq 0$. W analogiczny sposób można zdefiniować nieprzemienną algebrę kwaternionów nad pierścieniem R, konstruując lewostronny $R-$moduł wolny z bazą e_0, e_1, e_2, e_3 i wprowadzając w nim mnożenie w myśl (1.2) oraz (1.3).*

Definicja 1.2.5. *Jeśli do konstrukcji kwaternionów weźmiemy $a = b = -1$, $F = \mathbb{R}$ to otrzymaną algebrę nazywamy* algebrą kwaternionów hamiltonowskich*. W dalszym ciągu będziemy ją oznaczali przez $\mathbb{H}$, tzn.*

$$\mathbb{H} = \left(\frac{-1, -1}{\mathbb{R}}\right)$$

Lemat 1.2.6. *Dla $a, b \in F \setminus \{0\}$, algebra $A = \left(\frac{a,b}{F}\right)$ jest prosta (tzn. A jako pierścień nie posiada nietrywialnych ideałów) i jej centrum jest równe F.*

Dowód. Niech $Z(A)$ oznacza centrum A. Dla wygody wprowadźmy operator nawiasu Liego: $[x,y] := xy - yx$. Niech $x = c_0 + c_1 i + c_2 j + c_3 k \in A$. Wtedy

$$[i,x] = [i, c_0 + c_1 i + c_2 j + c_3 k] = i(c_0 + c_1 i + c_2 j + c_3 k) - (c_0 + c_1 i + c_2 j + c_3 k)i = \\ = c_0 i + ac_1 + c_2 k + ac_3 j - c_0 i - ac_1 + c_2 k + ac_3 j = (2ac_2)j + (2c_2)k$$

Analogicznie sprawdzamy, że

$$[j,x] = (-2bc_3)i + (-2c_1)k, \quad [k,x] = (2bc_2)i + (-2ac_1)j$$

W szczególności, jeśli $x \in Z(A)$ to $[i,x] = [j,x] = [k,x] = 0$ i tym samym $c_1 = c_2 = c_3 = 0$ (bo $a, b \neq 0$ oraz charakterystyka F jest różna od 2). Zatem $Z(A) \subseteq F$. Ale też $F \subseteq Z(A)$, bo każdy element z ciała F jest przemienny z elementami z A. Zatem $Z(A) = F$. Pierwsza część lematu jest udowodniona.

Załóżmy teraz że I jest ideałem A oraz $0 \neq x \in I$. Z definicji ideału $[y,x] \in I$ dla każdego $y \in A$, a tym samym $[z,[y,x]] \in I$ dla każdego $y, z \in A$. W szczególności do I należy element postaci

$$[j,[i,x]] = [j, (2ac_2)j + (2c_2)k] = j((2ac_2)j + (2c_2)k) - ((2ac_2)j + (2c_2)k)j = \\ = 2abc_2 - 2bc_2 i - 2abc_2 - 2bc_2 i = (-4bc_2)i$$

oraz elementy: $[k,[j,x]] = (4abc_3)j$, $[i,[k,x]] = (-4ac_1)k$. Jeśli $c_1 = c_2 = c_3 = 0$, to I zawiera element odwracalny $0 \neq x = c_0 \in F$. W przeciwnym przypadku do I należy jakiś *niezerowy* element postaci $(-4bc_2)i$, $(4abc_3)j$, $(-4ac_1)k$. Mnożąc odpowiednio przez i, j lub k otrzymamy, że do I należy jakiś element z ciała F. We wszystkich przypadkach $I = A$ (bo zawiera element odwracalny). □

Definicja 1.2.7. *Niech* $A = \left(\frac{a,b}{F}\right)$. *Elementy podprzestrzeni* $A_+ = Fi \oplus Fj \oplus Fk$ *nazywamy* czystymi kwaternionami. *Oczywiście* $A = F \oplus A_+$, *gdzie* $\oplus$ *oznacza sumę prostą podprzestrzeni.*

Definicja 1.2.8. *Niech* $x \in A = \left(\frac{a,b}{F}\right)$ *będzie postaci* $x = c_0 + z$, *gdzie* $c_0 \in F, z \in A_+$. Sprzężeniem x *nazywamy element* $\overline{x} = c_0 - z$.

Uwaga 1.2.9. *Niech* $x, y \in A = \left(\frac{a,b}{F}\right), d \in F$. *Wówczas:*

1. $\overline{x+y} = \overline{x} + \overline{y}$
2. $\overline{xy} = \overline{y}\,\overline{x}$
3. $\overline{\overline{x}} = x$
4. $\overline{d} = d$
5. $\overline{dx} = d\overline{x}$

Z wyjątkiem punktu 2. równości są oczywiste. Niech $x = \sum_{i=0}^{3} \alpha_i e_i, y = \sum_{j=0}^{3} \beta_j e_j$, gdzie $\alpha_i, \beta_j \in F$. Chcemy pokazać że $\overline{xy} = \overline{y}\,\overline{x}$. Korzystając z punktów (1), (4) i (5) możemy zapisać lewą i prawą stronę jako:

$$L = \overline{xy} = \overline{\sum_{i,j=0}^{3} (\alpha_i \beta_j)(e_i e_j)} = \sum_{i,j=0}^{3} \alpha_i \beta_j (\overline{e_i e_j})$$

$$P = \overline{y}\,\overline{x} = \sum_{j=0}^{3} \beta_j \overline{e_j} \sum_{i=0}^{3} \alpha_i \overline{e_i} = \sum_{i,j=0}^{3} \alpha_i \beta_j (\overline{e_j}\,\overline{e_i})$$

Zatem sprowadziliśmy zadanie do udowodnienia, że $\overline{xy} = \overline{y}\,\overline{x}$ dla $x, y \in \{e_0, e_1, e_2, e_3\}$. By to pokazać sprawdzamy po prostu wszystkie możliwości:

- dla $i = 0$ lub $j = 0$ równość oczywista (bo $x = 1$ lub $y = 1$)
- dla $i = j \neq 0 : e_i \in A_+, e_i^2 \in F$, zatem $L = \overline{e_i^2} = e_i^2, \quad P = (\overline{e_i})^2 = (-e_i)^2 = e_i^2$
- dla $i \neq j, i, j \neq 0 : e_i, e_j \in A_+, e_i e_j \in A_+$, zatem $L = \overline{e_i e_j} = -e_i e_j, \quad P = \overline{e_j}\,\overline{e_i} = (-e_j)(-e_i) = e_j e_i = -e_i e_j$ przy czym ostatnia równość wynika bezpośrednio z definicji mnożenia (1.3)

Definicja 1.2.10. *Niech $x \in A = \left(\frac{a,b}{F}\right)$.* Normą *$x$ nazwiemy $N(x) = x\overline{x}$.*

Niech $x = c_0 + c_1 i + c_2 j + c_3 k$. Wtedy otrzymujemy, że $N(x) = c_0^2 - ac_1^2 - bc_2^2 + abc_3^2$. Zatem w szczególności $N(x) \in F$ oraz $N(x) = N(\overline{x}) = \overline{x}x$.

Uwaga 1.2.11. *Jeśli $x, y \in A = \left(\frac{a,b}{F}\right)$, $d \in F$, to $N(xy) = N(x)N(y)$ oraz $N(d) = d^2$.*

Rzeczywiście, korzystając z wymienionych wyżej podstawowych własności normy otrzymujemy, że $N(xy) = xy\overline{xy} = xy\overline{y}\,\overline{x} = xN(y)\overline{x} = x\overline{x}N(y) = N(x)N(y)$. Zatem norma iloczynu to iloczyn norm. Równość $N(d) = d^2$ jest oczywista.

Twierdzenie 1.2.12. *Niech $A = \left(\frac{a,b}{F}\right)$. Następujące warunki są równoważne :*

1. *A jest algebrą z dzieleniem.*
2. *$x \in A \setminus \{0\}$ implikuje $N(x) \neq 0$*
3. *jeżeli $(c_0, c_1, c_2) \in F^3$ spełnia $c_0^2 = ac_1^2 + bc_2^2$ to $c_0 = c_1 = c_2 = 0$*

Dowód. Z (1) wynika (2), bo niech $x \neq 0$, $x \in A$. Korzystając z uwagi 1.2.11 mamy, że $N(x)N(x^{-1}) = N(xx^{-1}) = N(1) = 1$, zatem $N(x) \neq 0$. (2) również implikuje (1), bo niech $x \neq 0$, wtedy $1 = N(x)N(x)^{-1} = x\overline{x}N(x)^{-1} = x(\overline{x}N(x)^{-1}) = (\overline{x}N(x)^{-1})x$, oraz analogicznie $1 = x(\overline{x}N(x)^{-1})$, zatem $\overline{x}N(x)^{-1}$ to element odwrotny do x.

Przypuśćmy, że z (2) nie wynika (3). Niech $(c_0, c_1, c_2) \neq (0, 0, 0)$ oraz $c_0^2 = ac_1^2 + bc_2^2$. Niech $x = c_0 + c_1 i + c_2 j$. Wtedy $N(x) = 0$, ale ponieważ x jest niezerowy, to otrzymujemy sprzeczność z przypuszczeniem. Aby dostać komplet równoważności wystarczy jeszcze wykazać, że z (3) wynika (2). Niech $N(x) = 0$ dla pewnego $x = d_0 + d_1 i + d_2 j + d_3 k$. Na mocy wcześniejszego spostrzeżenia $N(x) = d_0^2 - ad_1^2 - bd_2^2 + abd_3^2 = 0$, zatem $d_0^2 - bd_2^2 = a(d_1^2 - bd_3^2)$. Mnożąc obustronnie przez $(d_1^2 - bd_3^2)$ otrzymujemy:

$$a(d_1^2 - bd_3^2)^2 = (d_0^2 - bd_2^2)(d_1^2 - bd_3^2) = (d_0 d_1 + bd_2 d_3)^2 - b(d_0 d_1 + d_1 d_2)^2$$

Korzystając z (3) dostajemy, że $d_1^2 - bd_3^2 = 0$. Zatem $d_1^2 = bd_3 + a0^2$ i jeszcze raz korzystając z (3) otrzymujemy, że $d_1 = d_3 = 0$. Podstawiając do wyjściowego równania dostajemy $d_0^2 - bd_2^2 = 0$, więc znowu $d_0 = d_2 = 0$, co ostatecznie implikuje, że $x = 0$. □

Wniosek 1.2.13. *Kwaterniony hamiltonowskie $\left(\frac{-1,-1}{\mathbb{R}}\right)$ są algebrą z dzieleniem.*

Dowód. Istotnie, $c_0^2 = -c_1^2 - c_2^2$ implikuje, że $c_0 = c_1 = c_2 = 0$ dla $c_0, c_1, c_2 \in \mathbb{R}$. □

Do kolejnego wniosku potrzebujemy prostego faktu z teorii ciał skończonych:

Lemat 1.2.14. *Niech F_{p^n} oznacza ciało skończone o p^n elementach, niech $a, b \in F_{p^n} \setminus \{0\}$. Wtedy istnieją takie $x, y \in F_{p^n}$, że $ax^2 + by^2 = 1$.*

Dowód. Załóżmy, że $p = 2$. Niech $x, y \in F_{2^n}$. Wówczas $x^2 = y^2$ wtedy i tylko wtedy, gdy $x = y$ (bo w wielomian $x^2 - y^2 = (x-y)(x+y) = (x-y)^2$ ma jeden podwójny pierwiastek). Zatem przekształcenie $\sigma : F_{2^n} \to F_{2^n}$ zdefiniowane wzorem $\sigma(x) = x^2$ jest 'na' (bo jest różnowartościowe i jest pomiędzy zbiorami o tej samej, skończonej liczbie elementów). W szczególności istnieje takie $\lambda \in F_{2^n}$, że $\lambda^2 = a^{-1} \in F_{2^n}$. Biorąc $x = \lambda$, $y = 0$ otrzymujemy tezę.

Załóżmy teraz, że $p > 2$. Niech $x, y \in F_{p^n}$. Zauważmy, że $x^2 = y^2$ wtedy i tylko wtedy, gdy $x = \pm y$ (bo w ciele F_{p^n} wielomian $x^2 - y^2 = (x-y)(x+y)$ ma dwa pierwiastki). Oczywiście $x = -x$ wtedy i tylko wtedy, gdy $x = 0$. Zatem możemy podzielić $F_{p^n} \setminus \{0\}$ na $\frac{p^n-1}{2}$ par, które odpowiadają różnym kwadratom, różnym od zera. Zatem zbiór $\{x^2 \mid x \in F_{p^n}\}$ ma dokładnie $\frac{p^n-1}{2} + 1 = \frac{p^n+1}{2}$ elementów. Tyle samo elementów ma zbiór $\{tx^2 \mid x \in F_{p^n}\}$ dla dowolnego $t \in F_{p^n} \setminus \{0\}$, a tym samym tyle samo elementów ma zbiór „przesunięty" $\{sx^2 + 1 \mid x \in F_{p^n}\}$ dla dowolnego $s \in F_{p^n} \setminus \{0\}$. Biorąc $t = a$, $s = -b$ otrzymujemy, że zbiory $A = \{ax^2 \mid x \in F_{p^n}\}$, $B = \{-by^2 + 1 \mid y \in F_{p^n}\}$ mają łącznie $|A| + |B| = p^n + 1$ elementów, ale ponieważ w F_{p^n} jest tylko p^n elementów, to $A \cap B \neq \emptyset$. Zatem istnieją takie $x, y \in F_{p^n}$, że $ax^2 = -by^2 + 1$, a tym samym $ax^2 + by^2 = 1$. □

Wniosek 1.2.15. *Dowolna algebra kwaternionów nad ciałem skończonym nie jest algebrą z dzieleniem.*

Dowód. Istotnie, niech $A = \left(\frac{a,b}{F_{p^n}}\right)$ $(p > 2)$. Wtedy na mocy lematu 1.2.14 istnieją takie $x, y \in F_{p^n}$, że $ax^2 + by^2 + 1$, a ponieważ $(1, x, y) \neq (0, 0, 0)$ wystarczy zastosować kryterium (3) z twierdzenia 1.2.12. □

Uzyskany wniosek nie jest niczym porywającym. Jako ciekawostkę można podać fakt, że jest to przypadek szczególny klasycznego twierdzenia z teorii pierścieni: twierdzenie Wedderburna stanowi, że każdy skończony pierścień z dzieleniem jest ciałem. Kwaterniony nie są ciałem, bo (w szczególności) są nieprzemienne.

Przykład 1.2.16. *Niech $a \in F \setminus \{0\}$. Algebra kwaternionów $\left(\frac{a,1}{F}\right)$ jest izomorficzna z $M_{2\times 2}(F)$. (w szczególności nie jest to algebra z dzieleniem).*

Skonstruowanie odpowiedniego izomorfizmu jest bardzo trikowe. Idea jest bardzo prosta: ponieważ zarówno $\left(\frac{a,1}{F}\right)$ jak i $M_{2\times 2}(F)$ są algebrami nad ciałem F, naszym celem jest wskazanie izomorfizmu liniowego φ: $\left(\frac{a,1}{F}\right) \to M_{2\times 2}(F)$ przeprowadzającego pewną bazą $\left(\frac{a,1}{F}\right)$ na bazę $M_{2\times 2}(F)$ w ten sposób, by φ zachowywało mnożenie na wybranej bazie. Wtedy stosując lemat 1.1.5 otrzymamy, że φ jest izomorfizmem algebr. Zatem cała trudność polega na wskazaniu odpowiedniej bazy.

Weźmy więc :

$$e_{11} = \frac{1}{2}(1 - j) \qquad e_{22} = \frac{1}{2}(1 + j) \qquad e_{21} = \frac{1}{2a}(i - k) \qquad e_{12} = \frac{1}{2}(i + k)$$

Pokażemy, że tak zdefiniowany układ jest liniowo niezależny (a tym samym jest bazą $\left(\frac{a,1}{F}\right)$). Niech $c_1e_{11} + c_2e_{22} + c_3e_{21} + c_4e_{12} = 0$ dla $c_1, c_2, c_3, c_4 \in F$. Wtedy

$$0 = c_1\frac{1}{2}(1-j) + c_2\frac{1}{2}(1+j) + c_3\frac{1}{2a}(i-k) + c_4\frac{1}{2}(i+k) =$$
$$= \left(\frac{c_1}{2} + \frac{c_2}{2}\right) + \left(\frac{c_3}{2a} + \frac{c_4}{2}\right)i + \left(-\frac{c_1}{2} + \frac{c_2}{2}\right)j + \left(-\frac{c_3}{2a} + \frac{c_4}{2}\right)k$$

Patrząc na współrzędne przy 1 oraz j otrzymujemy, że $c_1 + c_2 = 0$ oraz $-c_1 + c_2 = 0$, a tym samym $c_1 = c_2 = 0$. Patrząc z kolei na współrzędne przy i oraz k mamy, że $c_3 + ac_4 = 0$ oraz $-c_3 + ac_4 = 0$, zatem $c_3 = c_4 = 0$. Układ jest liniowo niezależny.

Następnie policzmy iloczyny wszystkich elementów bazowych. Ograniczymy się tylko do wypisania kilku przykładowych obliczeń (reszta wykonywana jest zupełnie analogicznie) i wypisania tabliczki mnożenia:

$$e_{11} \cdot e_{22} = \frac{1}{2}(1-j)\frac{1}{2}(1+j) = \frac{1}{4}(1-j^2) = \frac{1}{4}(1-1) = 0$$

$$e_{11} \cdot e_{12} = \frac{1}{2}(1-j)\frac{1}{2}(i+k) = \frac{1}{4}(i+k+k+i) = \frac{1}{2}(i+k) = e_{12}$$

$$e_{21} \cdot e_{12} = \frac{1}{2a}(i-k)\frac{1}{2}(i+k) = \frac{1}{4a}(i^2+ik-ki-k^2) = \frac{1}{4a}(a+aj+aj+a) = \frac{1}{2}(1+j) = e_{22}$$

$$e_{21} \cdot e_{21} = \frac{1}{2a}(i-k)\frac{1}{2a}(i-k) = \frac{1}{4a^2}(i^2-ik-ki+k^2) = \frac{1}{4a^2}(a-aj+aj-a) = 0$$

Tabliczka mnożenia prezentuje się następująco:

$\cdot$	e_{11}	e_{12}	e_{21}	e_{22}
e_{11}	e_{11}	e_{12}	0	0
e_{12}	0	0	e_{11}	e_{12}
e_{21}	e_{21}	e_{22}	0	0
e_{22}	0	0	0	e_{22}

W tej chwili wyjaśnia się dlaczego wektory oznaczaliśmy dwoma indeksami: można bardzo łatwo dostrzec, że mnożenie na elementach bazowych jest określone wzorem: $e_{ij} \cdot e_{kl} = \delta_{jk}e_{il}$, gdzie δ_{jk} to delta Kroneckera.

Niech teraz

$$E_{11} = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \qquad E_{12} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \qquad E_{21} = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix} \qquad E_{22} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$$

E_{ij} to oczywiście baza $M_{2\times 2}(F)$, ponadto $E_{ij} \cdot E_{kl} = \delta_{jk}E_{il}$. Zdefiniujmy teraz przekształcenie φ na bazie: $\varphi(e_{ij}) = E_{ij}$ dla $i, j \in \{1, 2\}$. Mamy:

$$\varphi(e_{ij})\varphi(e_{kl}) = E_{ij}E_{kl} = \delta_{jk}E_{il} = \delta_{jk}\varphi(e_{il}) = \varphi(\delta_{jk}e_{il}) = \varphi(e_{ij}e_{kl}) \text{ dla } i, j, k, l \in \{1, 2\}$$

Lemat 1.1.5 dopełnia całość.

1.3. Izomorfizm algebr kwaternionów

Na podstawie poprzedniego podrozdziału możemy wskazać przykład dwóch algebr kwaternionów nad ciałem $\mathbb{R}$, które nie są izomorficzne: są to np. $\left(\frac{-1,-1}{\mathbb{R}}\right)$ (algebra z dzieleniem) oraz $\left(\frac{1,1}{\mathbb{R}}\right)$ (algebra izomorficzna z $M_2(\mathbb{R})$). Fundamentalnym problemem teorii algebr kwaternionów jest pytanie, kiedy $\left(\frac{a,b}{F}\right) \cong \left(\frac{a',b'}{F}\right)$? W tym podrozdziale wyrazimy ten problem w języku form kwadratowych.

Niech $x, y \in A = \left(\frac{a,b}{F}\right)$, zdefiniujmy pomocniczy operator:

$$\beta(x,y) = \frac{1}{2}\left(N(x+y) - N(x) - N(y)\right)$$

Niech $x = c_0 + z$, $y = d_0 + w$, $c_0, d_0 \in F$, $z = c_1 i + c_2 j + c_3 k \in A_+$, $w = d_1 i + d_2 j + d_3 k \in A_+$. Wtedy

$$\begin{aligned}\beta(x,y) = \frac{1}{2}\left((x+y)(\overline{x+y}) - x\overline{x} - y\overline{y}\right) = \frac{1}{2}(x\overline{y} + y\overline{x}) = \\ = \frac{1}{2}((c_0+z)(d_0-w) + (d_0+w)(c_0-z)) = c_0 d_0 - \frac{1}{2}(zw + wz) = \\ = c_0 d_0 - a c_1 d_1 - b c_2 d_2 + abc_3 d_3\end{aligned}$$

Mając powyższe wzory możemy stwierdzić, że $\beta : A \times A \to F$ jest funkcjonałem dwuliniowym symetrycznym (tzn. $\beta(x,y) = \beta(y,x)$), ponadto $N(x) = \beta(x,x)$ oraz

$$\text{jeżeli } z, w \in A_+ \text{ to } \beta(z,w) = -\frac{1}{2}(zw + wz), \text{ a to implikuje, że } N(z) = -z^2 \tag{1.5}$$

Twierdzenie 1.3.1. *Niech $A = \left(\frac{a,b}{F}\right)$, $A' = \left(\frac{a',b'}{F}\right)$ będą algebrami kwaternionów z normami odpowiednio N oraz N'. A jest izomorficzne z A' (jako $F-$algebra) wtedy i tylko wtedy, gdy istnieje izomorfizm przestrzeni wektorowych $\phi : A_+ \to A'_+$ taki, że $N'(\phi(z)) = N(z)$ (czyli ϕ zachowuje normę czystych kwaternionów).*

Dowód. $\Rightarrow$ Zaczniemy dowód od charakteryzacji A_+. Niech $x = c + z$, gdzie $c \in Z(A), z \in A_+$. Wtedy $x^2 = c^2 + z^2 + z(2c) = c^2 - N(z) + z(2c)$. Zatem $x^2 \in Z(A)$ wtedy i tylko wtedy, gdy $z = 0$ (czyli $x \in Z(A)$) lub $c = 0$ (czyli $x \in A_+$). To spostrzeżenie pokazuje że dla $x \in A \setminus \{0\}$

$$x \in A_+ \Leftrightarrow x \notin Z(A) \wedge x^2 \in Z(A) \tag{1.6}$$

Oczywiście zupełnie analogicznie można scharakteryzować A'_+. Zatem, skoro każdy izomorfizm $\phi : A \to A'$ spełnia warunki $\phi(Z(A)) = Z(A')$, $\phi(x^2) = \phi(x)^2$ to korzystając z charakteryzacji czystych kwaternionów z (1.6) mamy, że $\phi(A_+) = A'_+$, a tym samym

$$\forall_{z \in A_+} N'(\phi(z)) = -\phi(z)^2 = \phi(-z^2) = \phi(N(z)) = N(z)$$

przy czym pierwsza i trzecia równość zachodzi z (1.5) (bo z oraz $\phi(z)$ to czyste kwaterniony), a ostatnia jest prawdziwa, bo ϕ obcięte do F to identyczność. Zatem ϕ jest poszukiwanym izomorfizmem z A_+ w A'_+.

$\Leftarrow$ Załóżmy teraz że $\phi : A_+ \to A'_+$ jest izomorfizmem przestrzeni wektorowych takim że $N'(\phi(z)) = N(z)$ dla $z \in A_+$. By pokazać, że $A \cong A'$ skonstruujemy bazę A', dla której „tabliczka mnożenia" jest taka sama jak ta powiązana ze standardową bazą A. Korzystając z (1.5) mamy, że

$$\phi(i)^2 = -N'(\phi(i)) = -N(i) = a$$

Analogicznie otrzymujemy że $\phi(j)^2 = b$. Co więcej

$$\phi(i)\phi(j) + \phi(j)\phi(i) = -2\beta'(\phi(i), \phi(j)) = -2\beta(i,j) = ij + ji = 0$$

(pierwsza i ostatnia równość wynika z (1.5), ponadto skorzystaliśmy z oczywistego faktu, że skoro ϕ zachowuje normę to zachowuje także sprzężony z nią funkcjonał β, tzn. $\beta'(\phi(z), \phi(w)) = \beta(z,w)$ dla każdego $z, w \in A_+$). Zatem

$$\phi(j)\Big(\phi(i)\phi(j)\Big) = \phi(j)\left(-\phi(j)\phi(i)\right) = -\phi(j)\phi(j)\phi(i) = -\phi(j)^2\phi(i) = (-b)\phi(i)$$

$$\text{oraz} \qquad \Big(\phi(i)\phi(j)\Big)\phi(j) = \phi(i)\phi(j)^2 = b\phi(i)$$

z czego wynika że $\phi(i)\phi(j)$ jest elementem nie należącym do centrum. Ponadto

$$\left(\phi(i)\phi(j)\right)^2 = \phi(i)(\phi(j)\phi(i)\phi(j)) = \phi(i)\phi(i)(-b) = -ab$$

więc korzystając znowu z (1.6) dostajemy, że $\phi(i)\phi(j) \in A'_+$. Przez zupełnie analogiczne obliczenia otrzymujemy również, że

$$\phi(i)\Big(\phi(i)\phi(j)\Big) = a\phi(j) \qquad \text{oraz} \qquad \Big(\phi(i)\phi(j)\Big)\phi(i) = (-a)\phi(j)$$

Pokażemy teraz, że $\phi(i), \phi(j), \phi(i)\phi(j)$ stanowi bazę A'_+. Niech $c_1\phi(i)+c_2\phi(j)+c_3\phi(i)\phi(j) = 0$ dla pewnych $c_1, c_2, c_3 \in F$. Mnożąc z lewej strony przez $\phi(i)$ mamy, że $0 = \phi(i)(c_1\phi(i) + c_2\phi(j) + c_3\phi(i)\phi(j)) = ac_1 + c_2\phi(i)\phi(j) + ac_3\phi(j)$, co implikuje, że $c_1 = 0$. Podobnie mnożąc z prawej strony przez $\phi(j)$ mamy, że $0 = (c_2\phi(j)+c_3\phi(i)\phi(j))\phi(j) = bc_2+bc_3\phi(i)$, co implikuje, że $c_2 = 0$, a z tego mamy $c_3\phi(i)\phi(j) = 0$, więc $c_3 = 0$.

Zdefiniujmy przekształcenie liniowe $\psi : A \to A'$ na bazie A

$$\psi(1) = 1, \qquad \psi(i) = \phi(i), \qquad \psi(j) = \phi(j), \qquad \psi(k) = \phi(i)\phi(j)$$

Z prezentowanych wcześniej obliczeń wynika, że baza $1, \phi(i), \phi(j), \phi(i)\phi(j)$ ma identyczną „tabliczkę mnożenia" jak baza $1, i, j, k$, a tym samym mnożenie na standardowej bazie się zachowuje. Zatem stosując lemat 1.1.5 dostajemy, że ψ to szukany izomorfizm.

□

W ogólnym przypadku przekształcenie ψ zdefiniowane w powyższym dowodzie nie pokrywa się z ϕ. Klasa izometrii z A_+ do A'_+ jest „większa" niż klasa izomorfizmów algebr A oraz A'.

Główny rezultat tego rozdziału uzyskamy tłumacząc twierdzenie 1.3.1 na język form kwadratowych. Niech $z = c_1 i + c_2 j + c_3 k \in A_+$, $w = d_1 i + d_2 j + d_3 k \in A_+$, $z' = c'_1 i' + c'_2 j' + c'_3 k' \in A'_+$, $w' = d'_1 i' + d'_2 j' + d'_3 k' \in A'_+$ ($1, i', j', k'$ oznacza standardową bazę A'). Wtedy $N(z) = \Phi(c_1, c_2, c_3)$, gdzie Φ jest formą kwadratową $-ax_1^2 - bx_2^2 + abx_3^2$. Podobnie $N'(z') = \Phi'(c'_1, c'_2, c'_3)$, gdzie $\Phi' = -a'x_1^2 - b'x_2^2 + a'b'x_3^2$.

Wygodnie jest zaprezentować te równania w postaci macierzowej. Oznaczmy zatem:

$$\alpha = \begin{bmatrix} -a & 0 & 0 \\ 0 & -b & 0 \\ 0 & 0 & ab \end{bmatrix}, \qquad \alpha' = \begin{bmatrix} -a' & 0 & 0 \\ 0 & -b' & 0 \\ 0 & 0 & a'b' \end{bmatrix},$$

$$\xi = \begin{bmatrix} c_1 \\ c_2 \\ c_3 \end{bmatrix}, \qquad \xi' = \begin{bmatrix} c'_1 \\ c'_2 \\ c'_3 \end{bmatrix}, \qquad \eta = \begin{bmatrix} d_1 \\ d_2 \\ d_3 \end{bmatrix}, \qquad \eta' = \begin{bmatrix} d'_1 \\ d'_2 \\ d'_3 \end{bmatrix}$$

Wtedy $z = [i, j, k]\xi$, $w = [i, j, k]\eta$, $z' = [i', j', k']\xi'$, $w' = [i', j', k']\eta$ [1] oraz

$$N(z) = \xi^T \alpha \xi, \qquad N'(z') = (\xi')^T \alpha' \xi'$$

(indeks górny T oznacza transpozycję macierzy). Co więcej

$$\beta(z, w) = \xi^T \alpha \eta, \qquad \beta'(z', w') = (\xi')^T \alpha' \eta'$$

Załóżmy teraz, że $\phi : A_+ \to A'_+$ jest *dowolnym* przekształceniem liniowym i niech

$$[\phi(i), \phi(j), \phi(k)] = [i', j', k']\delta$$

gdzie $\delta \in M_{3x3}(F)$. (Oczywiście przekształcenie ϕ jest izomorfizmem wtedy i tylko wtedy, gdy δ jest macierzą nieosobliwą). Otrzymujemy, że

$$\phi(z) = [\phi(i), \phi(j), \phi(k)]\xi = [i', j', k']\delta\xi$$

Podobnie $\phi(w) = [i', j', k']\delta\eta$. W rezultacie

$$\beta'(\phi(z), \phi(w)) = (\delta\xi)^T \alpha' (\delta\eta) = \xi^T (\delta^T \alpha' \delta)\eta$$

Zatem przekształcenie ϕ spełnia $N'(\phi(z)) = N(z)$ dla każdego $z \in A_+$ lub równoważnie $\beta'(\phi(z), \phi(w)) = \beta(z, w)$ dla każdego $z, w \in A_+$ wtedy i tylko wtedy, gdy $\xi^T \alpha \eta = \xi^T (\delta^T \alpha' \delta)\eta$ dla każdego $\xi, \eta \in F^3$. Ponieważ ξ, η są dowolne oraz macierze α, α' są nieosobliwe, to równanie sprowadza się do $\alpha = \delta^T \alpha' \delta$ (zauważmy, że jeżeli jest ono spełnione to δ jest również nieosobliwa, zatem ϕ jest izomorfizmem). Czyli naszą dyskusję możemy podsumować, mówiąc, że istnieje izometria pomiędzy A_+ i A'_+ wtedy i tylko wtedy, gdy macierze α i α' są *kongruentne*, z czego wynika następujące twierdzenie:

Twierdzenie 1.3.2. *Dwie algebry kwaternionów* $\left(\frac{a,b}{F}\right)$ *i* $\left(\frac{a',b'}{F}\right)$ *są izomorficzne wtedy i tylko wtedy, gdy formy kwadratowe* $ax_1^2 + bx_2^2 - abx_3^2$ *i* $a'x_1^2 + b'x_2^2 - a'b'x_3^2$ *są równoważne.*

Dowód. Przypomnijmy: dwie kwadratowe formy są równoważne, jeżeli można uzyskać jedną z drugiej przez odwracalną liniową zamianę zmiennych. Jeśli formy Ψ i Ψ' zaprezentujemy jako produkt macierzy $\Psi(x_1, x_2, x_3) = [x_1, x_2, x_3]\, \alpha \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$, $\Psi'(x_1, x_2, x_3) = [x_1, x_2, x_3]\, \alpha' \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix}$, to warunek, że Ψ oraz Ψ' są równoważne odpowiada istnieniu nieosobliwej macierzy δ takiej że $\alpha = \delta^T \alpha' \delta$. Zatem korzystając z wcześniejszych obserwacji otrzymujemy, że twierdzenie 1.3.2 to twierdzenie 1.3.1 wyrażone w języku form kwadratowych.

□

Wniosek 1.3.3. *Jeżeli* $a, b, c \in F \setminus \{0\}$, *to*

$$\left(\frac{ac^2, b}{F}\right) \cong \left(\frac{a, bc^2}{F}\right) \cong \left(\frac{a, b}{F}\right) \cong \left(\frac{b, a}{F}\right)$$

[1] Od tego miejsca aż do końca rozdziału, dla wygody oraz czytelności dalszych wyprowadzeń, pozwalamy sobie zmienić dotychczasową konwencję, zapisując skalar po *prawej* stronie wektora

Dowód. Oczywisty, korzystając z wcześniejszego twierdzenia wystarczy sprawdzić, że odpowiednie macierze są kongruentne:

$$\begin{pmatrix} -ac^2 & 0 & 0 \\ 0 & -b & 0 \\ 0 & 0 & (ac^2)b \end{pmatrix} = \begin{pmatrix} c & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & c \end{pmatrix} \cdot \begin{pmatrix} -a & 0 & 0 \\ 0 & -b & 0 \\ 0 & 0 & ab \end{pmatrix} \cdot \begin{pmatrix} c & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & c \end{pmatrix}$$

$$\begin{pmatrix} -a & 0 & 0 \\ 0 & -bc^2 & 0 \\ 0 & 0 & a(bc^2) \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & c & 0 \\ 0 & 0 & c \end{pmatrix} \cdot \begin{pmatrix} -a & 0 & 0 \\ 0 & -b & 0 \\ 0 & 0 & ab \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 \\ 0 & c & 0 \\ 0 & 0 & c \end{pmatrix}$$

$$\begin{pmatrix} -b & 0 & 0 \\ 0 & -a & 0 \\ 0 & 0 & ba \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} -a & 0 & 0 \\ 0 & -b & 0 \\ 0 & 0 & ab \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

□

Wniosek 1.3.4. *Podstawiając $F = \mathbb{R}$ we wniosku 1.3.3 otrzymujemy, że każda algebra kwaternionów nad $\mathbb{R}$ jest izomorficzna z $\left(\frac{1,1}{\mathbb{R}}\right)$, $\left(\frac{-1,1}{\mathbb{R}}\right)$ lub $\mathbb{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$. Jednakże z Przykładu 1.2.16 wiemy, że $\left(\frac{1,1}{\mathbb{R}}\right) \cong M_2(\mathbb{R}) \cong \left(\frac{-1,1}{\mathbb{R}}\right)$, zatem jedynymi istotnie różnymi (z dokładnością do izomorfizmu) algebrami kwaternionów rzeczywistych są $\left(\frac{1,1}{\mathbb{R}}\right)$ oraz $\mathbb{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$.*

Rozdział 2

Mechanika przestrzeni trójwymiarowej

W niniejszym rozdziale zbadamy powiązanie kwaternionów hamiltonowskich z obrotami w przestrzeni trójwymiarowej. Szkic rozdziału, a w szczególności główne twierdzenie, pochodzi z [Kop05].

Niech $\mathbb{H} = \mathbb{R} \bigoplus \mathbb{P}$, gdzie $\mathbb{P}$ oznacza 3-wymiarową przestrzeń czystych kwaternionów. Przestrzeń $\mathbb{R}^3$, w której będziemy rozważać obrót, będziemy utożsamiali z przestrzenią $\mathbb{P}$ ze 'standardowym' iloczynem skalarnym, dla którego i, j, k jest bazą ortonormalną. Na potrzeby tego rozdziału wprowadzimy inną reprezentację kwaternionów, dzięki której będziemy mogli zapisać mnożenie za pomocą iloczynu skalarnego oraz wektorowego.

Niech $q = a_0 + a_1 i + a_2 j + a_3 k \in \mathbb{H}$. Wtedy q możemy zapisać alternatywnie w postaci pary uporządkowanej (a_0, v), gdzie a_0 jest skalarem, zaś v to wektor trójwymiarowy, $v = a_1 i + a_2 j + a_3 k$.

Uwaga 2.0.5. *Niech $q = (a, u), \tau = (b, v) \in \mathbb{R} \bigoplus \mathbb{P} = \mathbb{H}$ będą dowolnymi kwaternionami. Wtedy*

$$q + \tau = (a, u) + (b, v) = (a + b, u + v)$$

$$q\tau = (a, u)(b, v) = (ab - u \bullet v, av + bu + u \times v)$$

gdzie $\bullet$ oznacza standardowy iloczyn skalarny, zaś $\times$ to standardowy iloczyn wektorowy.

Jak już zauważyliśmy w poprzednim rozdziale, $\mathbb{H}$ jest algebrą z dzieleniem. Dla każdego niezerowego $q = a_0 + a_1 i + a_2 j + a_3 k \in \mathbb{H}$ istnieje element odwrotny $q^{-1} = \frac{1}{N(q)}\overline{q}$, gdzie $N(q) = a_0^2 + a_1^2 + a_2^2 + a_3^2$ oznacza normę q, a $\overline{q}$ to element sprzężony do q. Ponadto to *standardową normą euklidesową* kwaternionu q będziemy oznaczali jako $||q||$. Oczywiście $||q|| = \sqrt{a_0^2 + a_1^2 + a_2^2 + a_3^2} = \sqrt{N(q)}$.

Dla dowolnego $q \in \mathbb{H} \setminus \{0\}$ zdefiniujmy przekształcenie $\varphi_q : \mathbb{P} \to \mathbb{P}$ wzorem

$$\varphi_q(v) := qvq^{-1}$$

Na początku pokażmy, że przeciwdziedziną jest rzeczywiście $\mathbb{P}$. W tym celu posłużmy się następującym kryterium:

$$\pi \in \mathbb{P} \Leftrightarrow \overline{\pi} = -\pi$$

Niech $v \in \mathbb{P}$, tzn. $\overline{v} = -v$. Wtedy $\overline{qvq^{-1}} = \overline{q^{-1}}\overline{v}\overline{q} = \overline{\frac{1}{N(q)}\overline{q}}(-v)\overline{q} = \left(\frac{1}{N(q)}q\right)(-v)\overline{q} = q(-v)\left(\frac{1}{N(q)}\overline{q}\right) = -\left(qvq^{-1}\right)$, czyli $\varphi_q(v) \in \mathbb{P}$.

Z rozdzielności dodawania względem mnożenia w pierścieniu kwaternionów wynika, że φ_q jest przekształceniem $\mathbb{R}$-liniowym. Ponadto φ_q zachowuje normę kwaternionów, bo dla $v \in \mathbb{P}$ mamy:

$$N\left(qvq^{-1}\right) = N(q)\,N(v)\,N\left(q^{-1}\right) = N(v)\,N(q)\,N\left(q^{-1}\right) = N(v)\,N\left(qq^{-1}\right) = N(v)$$

Skoro φ_q zachowuję normę kwaternionów, to tym samym zachowuje normę euklidesową, a z tego wynika że zachowuje długości wektorów w $\mathbb{P}$. Zatem φ_q to izometria $\mathbb{P}$. W dalszej części pokażemy, że φ_q to obrót przestrzeni trójwymiarowej oraz, że dla każdego obrotu ω przestrzeni trójwymiarowej istnieje takie $q \in \mathbb{H} \setminus \{0\}$, że $\omega = \varphi_q$.

Lemat 2.0.6. *Dla każdego niezerowego $q \in \mathbb{H}$ oraz $a \in \mathbb{R} \setminus \{0\}$ zachodzi $\varphi_{aq} = \varphi_q$.*

Dowód. Oczywisty: $\forall_{x\in\mathbb{P}}\ \varphi_{aq}(v) = (aq)v(aq)^{-1} = aqvq^{-1}a^{-1} = aa^{-1}qvq^{-1} = qvq^{-1} = \varphi_q$. □

Niech $q = (a, v) \in \mathbb{H} \setminus \{0\}$ będzie dowolnym kwaternionem. Jeżeli $v \neq 0$, to q możemy zapisać w postaci

$$q = ||q||\left(\frac{a}{||q||}, \frac{||v||}{||q||}\frac{v}{||v||}\right)$$

Ponieważ $\left(\frac{a}{||q||}\right)^2 + \left(\frac{||v||}{||q||}\right)^2 = \frac{1}{N(q)}(a^2 + v \bullet v) = \frac{1}{N(q)}N(q) = 1$, to istnieje $\alpha \in \mathbb{R}$ takie, że

$$\frac{a}{||q||} = \cos\alpha, \qquad \frac{||v||}{||q||} = \sin\alpha$$

i wówczas $q = ||q||\left(\cos\alpha, \sin\alpha\frac{v}{||v||}\right)$.

Jeżeli $v = 0$, to $q = (a, 0) = |a|\,(\cos 0, (\sin 0)v')$ lub $q = (a, 0) = |a|\,(\cos\pi, (\sin\pi)v')$ dla dowolnego v' wektora jednostkowego. Zatem każdy niezerowy kwaternion możemy zapisać w postaci

$$t(\cos\alpha, (\sin\alpha)v) \tag{2.1}$$

gdzie $||v|| = 1$, $\alpha \in \mathbb{R}$, $t \in \mathbb{R}$, $t > 0$.

Definicja 2.0.7. *Postać (2.1) będziemy nazywać* postacią trygonometryczną *kwaternionu.*

Definicja 2.0.8. *Niech $v \in \mathbb{P}$ będzie wektorem jednostkowym, $\beta \in \mathbb{R}$.* Obrotem o kąt β wokół *$lin(v)$ nazywamy przekształcenie liniowe $\omega : \mathbb{P} \to \mathbb{P}$ takie, że istnieje baza ortonormalna v, v_2, v_3 zgodnie zorientowana z bazą i, j, k, w której ω ma macierz*

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\beta & -\sin\beta \\ 0 & \sin\beta & \cos\beta \end{bmatrix}$$

W ten sposób zbliżamy się do centralnego twierdzenia tego rozdziału:

Twierdzenie 2.0.9. *Niech $q = ||q||\,(\cos\alpha, (\sin\alpha)v)$ będzie niezerowym kwaternionem. Wówczas φ_q jest* obrotem *przestrzeni trójwymiarowej wokół osi $lin(v)$ o kąt 2α. (Zatem w szczególności każdy obrót można opisać za pomocą pewnego φ_q).*

Dowód. Korzystając z Lematu 2.0.6 wystarczy przeprowadzić dowód twierdzenia w sytuacji, gdy q jest kwaternionem o jednostkowej normie euklidesowej. Zatem niech $q = (\cos\alpha, (\sin\alpha)v)$ dla pewnego $v \in \mathbb{P}$ wektora jednostkowego. Ponieważ na mocy wcześniejszej uwagi φ_q jest liniową izometrią przestrzeni liniowej, wystarczy pokazać jak φ_q zachowuje się na $lin(v)$ oraz $lin(v)^\perp$. Mamy

$$\varphi_q(v) = (\cos\alpha, (\sin\alpha)v)\,(0, v)\,(\cos\alpha, (-\sin\alpha)v) = (-\sin\alpha, (\cos\alpha)v)\,(\cos\alpha, (-\sin\alpha)v) = \\ = (0, (\sin\alpha^2 + \cos\alpha^2)v) = (0, v) = v$$

Ponieważ φ_q nie zmienia wektora v, to też zachowuje całą prostą $lin(v)$.

Pozostaje wykazać, że φ_q to obrót na $lin(v)^\perp$. Weźmy zatem dowolny wektor jednostkowy $w \in lin(v)^\perp$. Oczywiście $v \bullet w = 0$. Niech $u := v \times w$. Jest oczywistym, że $u \in lin(v)^\perp$, co więcej v, w, u stanowią bazę ortonormalną zgodną z bazą standardową. Mamy zatem:

$$\varphi_q(w) = (\cos\alpha, (\sin\alpha)v)(0, w)(\cos\alpha, (-\sin\alpha)v) = (0, (\sin\alpha)u + (\cos\alpha)w)(\cos\alpha, (-\sin\alpha)v) = \\ = ((\sin^2\alpha)(u \bullet v) + (\sin\alpha\cos\alpha)(w \bullet v), \\ (-\sin^2\alpha)(u \times v) - (\sin\alpha\cos\alpha)(w \times v) + (\sin\alpha\cos\alpha)u + (\cos^2\alpha)w) = \\ = (0, (-\sin^2\alpha)w + (2\sin\alpha\cos\alpha)u + (\cos^2\alpha)w) = (0, \cos(2\alpha)w + \sin(2\alpha)u) = \\ = \cos(2\alpha)w + \sin(2\alpha)u$$

Zatem wektor prostopadły w jest obracany o kąt 2α. Z dowolności wyboru wektora otrzymujemy tezę. □

Wniosek 2.0.10. *Niech $q \in \mathbb{H} \setminus \mathbb{R}$, $q = (a, v)$, gdzie $v \neq 0$. Oś obrotu φ_q jest równoległa do v.*

Dowód wynika z twierdzenia 2.0.9 oraz własności przedstawienia q w postaci trygonometrycznej.

Niech $SO_3(\mathbb{R})$ oznacza grupę obrotów przestrzeni $\mathbb{R}^3$.

Twierdzenie 2.0.11. *Odwzorowanie $F : \mathbb{H} \setminus \{0\} \to SO_3(\mathbb{R})$ zadane wzorem $F(q) = \varphi_q$ jest homomorfizmem grup.*

Dowód. Niech $p, q \in \mathbb{H} \setminus \{0\}$. Wtedy $(F(p)F(q))(v) = p(qvq^{-1})q^{-1} = (pq)v(pq)^{-1} = F(pq)(v)$ dla każdego $v \in \mathbb{P}$. Zatem $F(p)F(q) = F(pq)$. □

Zgodnie z twierdzeniem 2.0.9 homomorfizm F jest 'na', co więcej, z lematu 2.0.6 wynika, że każdemu obrotowi z SO_3 odpowiada nieprzeliczalnie wiele kwaternionów z $\mathbb{H} \setminus \{0\}$.

Niech $S^3 = \{v \in \mathbb{H} \mid N(v) = 1\}$. Ponieważ iloczyn dwóch kwaternionów unormowanych jest unormowany oraz elementem odwrotnym do kwaternionu unormowanego jest sprzężenie tego kwaternionu (też unormowane) to S^3 jest podgrupą $\mathbb{H}$ ze względu na mnożenie.

Wniosek 2.0.12. *Odwzorowanie $F : S^3 \to SO_3(\mathbb{R})$ zadane wzorem $F(q) = \varphi_q$ jest homomorfizmem grup, przy tym każdy obrót jest obrazem* dokładnie dwóch *kwaternionów z S^3.*

Dowód. Ponieważ S^3 to podgrupa $\mathbb{H} \setminus \{0\}$, homomorfizm wynika z twierdzenia 2.0.11. Zajmiemy się drugą częścią wniosku.

Niech $\omega \in SO^3$. Jeżeli $\omega = id$, to w oczywisty sposób odpowiadają mu tylko kwaterniony $\pm 1 \in S^3$. Załóżmy teraz, że ω jest nietrywialnym obrotem o kąt 2α wokół osi $lin(v)$, gdzie v jest wektorem jednostkowym. Wtedy obrotowi ω oczywiście odpowiadają kwaterniony $q = (\cos\alpha, (\sin\alpha)v)$ oraz $-q$. Pokażemy, że nie ma ich więcej, korzystając ze związku postaci kwaternionu oraz obrotu. Obrót ω może alternatywnie zapisać w dwóch postaciach:

- Jako obrót o kąt $2\alpha + 2k\pi$ wokół osi $lin(v)$ dla $k \in \mathbb{Z}$
- Jako obrót o kąt $-2\alpha + 2k\pi$ wokół osi $lin(-v)$ dla $k \in \mathbb{Z}$

W pierwszym przypadku odpowiada mu kwaternion $q_2 = (\cos(\alpha + k\pi), \sin(\alpha + k\pi)v)$. Jeżeli k jest parzyste to $q_2 = (\cos\alpha, (\sin\alpha)v) = q$. Jeżeli k jest nieparzyste, to $q_2 = (\cos(\alpha + \pi), \sin(\alpha + \pi))v = (-\cos\alpha, (-\sin\alpha)v) = -q$.

W drugim przypadku

$$q_2 = (\cos(-\alpha + k\pi), \sin(-\alpha + k\pi)(-v)) = (\cos(\alpha - k\pi), -\sin(\alpha - k\pi)(-v)) = \\ = (\cos(\alpha + k\pi), \sin(\alpha + k\pi)v)$$

i sprowadziliśmy sytuację do przypadku pierwszego. □

Rozdział 3

O wolnych podgrupach grupy elementów odwracalnych algebr kwaternionów

W tym rozdziale zawęzimy pole naszych badań: przez „algebry kwaternionów" będziemy rozumieć podpierścienie kwaternionów hamiltonowskich, będące algebrą nad pewnym podpierścieniem $\mathbb{Q}$. Zajmiemy się badaniem pewnej algebraicznej własności kwaternionów: pokażemy kiedy grupa elementów odwracalnych algebry kwaternionów zawiera podgrupę wolną. Zawartość tego rozdziału powstała na podstawie pracy [Kre01].

3.1. Motywacja oraz wprowadzenie notacji

Na potrzeby tego rozdziału przypomnijmy przydatną notację: przez $U(R)$ będziemy oznaczali grupę elementów odwracalnych pierścienia R (dla którego $1 \neq 0$) z mnożeniem jako działaniem grupowym, $\mathcal{F}$ będzie oznaczać nieabelową grupę wolną generowaną przez dwa elementy. Ponadto przez $\langle a_1, \ldots, a_n \rangle$ będziemy rozumieli grupę generowaną przez elementy $a_1, \ldots, a_n$. Dopuścimy się też pewnego nadużycia notacyjnego: jeżeli G jest grupą, to pisząc $\mathcal{F} \subseteq G$ będziemy mieli na myśli, że G zawiera podgrupę izomorficzną z $\mathcal{F}$.

Niech $A \subseteq \mathbb{Q}$ będzie podpierścieniem. Przez $H(A)$ będziemy oznaczali algebrę kwaternionów nad A. Bardziej precyzyjnie:

$$H(A) = \{a_0 + a_1 i + a_2 j + a_3 k \mid a_0, a_1, a_2, a_3 \in A\}$$

$H(A)$ jest oczywiście podpierścieniem $\mathbb{H}$, bo jest zamknięte ze względu na dodawanie i mnożenie. Dla $n \in \mathbb{N}_+$ definiujemy: $A_n = \mathbb{Z}[\frac{1}{n}]$, $H_n = H(A_n)$. Ponadto $H_1 = H(\mathbb{Z})$ będziemy nazywali *kwaternionami całkowitymi*, a $H(\mathbb{Q})$ *kwaternionami wymiernymi.*

Lemat 3.1.1. *Niech A będzie podpierścieniem $\mathbb{Q}$. Wtedy*

$$U(H(A)) = \{\alpha \in H(A) : N(\alpha) \in U(A)\}$$

Dowód. $\supseteq$. Niech $\alpha \in H(A)$, $N(\alpha) \in U(A)$. Wtedy z wyprowadzonych w rozdziale 1 własności mamy bezpośredni wzór na element odwrotny: $\alpha^{-1} = \frac{1}{N(\alpha)}\overline{\alpha}$, oczywiście tak zdefiniowane $\alpha^{-1} \in H(A)$. Zatem $\alpha \in U(H(A))$.

$\subseteq$. Niech $\alpha \in U(H(A))$. Oznaczmy przez α^{-1} jego element odwrotny. Wtedy $\overline{\alpha}$ też należy do $U(H(A))$, bo jego element odwrotny to $\overline{\alpha^{-1}}$. Istotnie, sprawdźmy: $\overline{\alpha^{-1}}\overline{\alpha} = \overline{\alpha^{-1}\alpha} = \overline{1} = 1$,

tak samo mnożąc z drugiej strony. Ponieważ $U(H(A))$ to grupa, otrzymujemy że $N(\alpha) = \alpha\overline{\alpha} \in U(H(A))$. Ale również $N(\alpha) \in A$, więc stąd wnioskujemy że $N(\alpha) \in U(A)$.

□

Przykład 3.1.2. $U(H_1) = \{1, -1, i, -i, j, -j, k, -k\}$.

Przykład 3.1.3. $U(H(\mathbb{Q})) = H(\mathbb{Q}) \setminus \{0\}$.

W ramach motywacji, podamy jeszcze jedno twierdzenie, którego dowód pominiemy:

Twierdzenie 3.1.4. *Niech D będzie algebrą z dzieleniem, która jest skończenie wymiarowa nad swoim centrum. Jeżeli D nie jest ciałem, to $\mathcal{F} \subset U(D)$.*

Podane twierdzenie jest bardzo silne i mocno nietrywialne, jednakże jego dowód jest niekonstruktywny (zob. [Gon84]) . Korzystając z niego otrzymujemy od razu, że istnieje pewna kopia podgrupy wolnej w grupie elementów odwracalnych kwaternionów wymiernych. W szczególności mamy kolejny niekonstruktywny rezultat:

Lemat 3.1.5. *Istnieje $n \in \mathbb{N}_+$ takie że $\mathcal{F} \subset U(H_n)$.*

Dowód. Niech $\mathcal{F} = \langle u, v\rangle \subseteq U(H(\mathbb{Q}))$ (istnienie grupy $\mathcal{F}$ w grupie $U(H(\mathbb{Q}))$ wynika z twierdzenia 3.1.4), gdzie $N(u) = \frac{s_1}{s_2}$, $N(v) = \frac{t_1}{t_2}$ dla pewnych $s_1, s_2, t_1, t_2 \in \mathbb{N}_+$. Niech $n_1 = s_1 s_2$, wtedy $N(u) \in U(A_{n_1})$. Analogicznie dla $n_2 = t_1 t_2$ mamy $N(v) \in U(A_{n_2})$. Ponieważ $U(A_{n_1}) \subseteq U(A_{n_1 n_2})$ oraz $U(A_{n_2}) \subseteq U(A_{n_1 n_2})$ dostajemy, że $N(u), N(v) \in U(A_{n_1 n_2})$, a tym samym z lematu 3.1.1 mamy, że $u, v \in U(H_{n_1 n_2})$. Zatem wystarczy wziąć $n = n_1 n_2$. □

W tym rozdziale określimy jakie liczby naturalne dodatnie n spełniają tezę lematu 3.1.5. Naszym celem jest również wskazanie wprost nieskończenie wiele różnych kopii $\mathcal{F}$ w $U(H(\mathbb{Q}))$.

Z drugiej strony, korzystając z przykładu 3.1.2 wiemy, że podgrupa elementów odwracalnych kwaternionów całkowitych jest skończona rzędu 8 - zatem nie zawiera w sobie podgrupy wolnej. Ostatecznie dla dowolnego pośredniego pierścienia $\mathbb{Z} \subset A \subset \mathbb{Q}$ podamy kryterium, które rozstrzyga, czy $U(H(A))$ zawiera kopię $\mathcal{F}$ i w przypadku odpowiedzi twierdzącej wyznaczymy wprost tą podgrupę.

3.2. Poszukiwania grupy wolnej

Naszym głównym rezultatem jest:

Twierdzenie 3.2.1. *Niech $n \in \mathbb{N}_+$. Wówczas $\mathcal{F} \subseteq U(H_n))$ wtedy i tylko wtedy, gdy n nie jest potęgą 2.*

Pierwszym krokiem w kierunku dowodu twierdzenia 3.2.1 jest lemat dotyczący podgrupy ortogonalnych macierzy:

Lemat 3.2.2. *Niech*

$$A = \begin{bmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \cos\theta & -\sin\theta \\ 0 & \sin\theta & \cos\theta \end{bmatrix}$$

będą macierzami obrotu 3-wymiarowej przestrzeni Euklidesowej nad $\mathbb{R}$. Jeżeli $\cos\theta \notin \{0, \pm\frac{1}{2}, \pm 1\}$, ale jest liczbą wymierną, to grupa $\langle A, B\rangle$ jest podgrupą wolną grupy $SO_3(\mathbb{R})$.

Dowód wersji uproszczonej. Pełny dowód tego twierdzenia można znaleźć w [Świe94]. Rozpatruje się w nim dwa przypadki: a) gdy mianownik $\cos\theta$ nie jest potęgą 2, b) gdy mianownik $\cos\theta$ jest potęgą 2. Ponieważ w dalszej części pracy będziemy korzystali tylko z pierwszej sytuacji, w podanym dowodzie przyjmiemy *dodatkowe* założenie, że $\cos\theta \notin \{\pm\frac{1}{2^k} \mid k \in \mathbb{N}_+\}$ (zasygnalizujemy w dowodzie od którego miejsca z tego założenia korzystamy). Zainteresowanych dowodem drugiego przypadku odsyłam do wyżej wymienionej pozycji z uwagą, iż dowód jest nieco bardziej skomplikowany.

Niech $\cos\theta = \frac{a}{b}$, gdzie a, b to różne liczby naturalne. Niech $c = b^2 - a^2$. Pokażemy, że macierze

$$A = \begin{bmatrix} \frac{a}{b} & \frac{-\sqrt{c}}{b} & 0 \\ \frac{\sqrt{c}}{b} & \frac{a}{b} & 0 \\ 0 & 0 & 1 \end{bmatrix} \qquad B = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \frac{a}{b} & \frac{-\sqrt{c}}{b} \\ 0 & \frac{\sqrt{c}}{b} & \frac{a}{b} \end{bmatrix}$$

generują grupę wolną. Zakładamy przy tym, że $b > 0$, $|a| < b$ oraz $\frac{a}{b} \neq 0, \pm\frac{1}{2}, \pm 1$. Zatem możemy dodatkowo założyć, że $a \neq 0$, a, b są względnie pierwsze oraz $b > 2$. Musimy pokazać, że dla każdego $n \geqslant 1$ oraz dowolnego ciągu macierzy $C_1, \dots C_n$, takiego że $C_j = A^\varepsilon$ lub B^ε, gdzie $\varepsilon = \pm 1$ oraz $C_j \cdot C_{j+1} \neq I$ dla $1 \leqslant j \leqslant n$ (I jest macierzą jednostkową) mamy

$$C_1 \cdot C_2 \cdots C_n \neq I \tag{3.1}$$

Mnożąc obie strony (3.1) odpowiednio przez A^p oraz A^{-p} otrzymujemy, że równanie (3.1) jest równoważne $A^p \cdot C_1 \cdot C_2 \cdots C_n \cdot A^{-p} \neq I$, gdzie p jest dowolną liczbą całkowitą, zatem możemy dodatkowo zakładać, że $C_1 = A^{\pm 1}$.

Dla $j = 1, \dots, n$, $k = 1, 2, 3$ zdefiniujmy liczby $d_k^{(j)}$ za pomocą:

$$C_1 \cdot C_2 \cdot \cdots \cdot C_j = \begin{bmatrix} \frac{d_1^{(j)}}{b^j} & \frac{d_2^{(j)}\sqrt{c}}{b^j} & \frac{d_3^{(j)}}{b^j} \\ * & * & * \\ * & * & * \end{bmatrix} \tag{3.2}$$

Pokażemy, że $d_2^{(n)} \neq 0$, a z tego od razu wynika teza twierdzenia. Zacznijmy od wypisania rekurencyjnych zależności na $d_k^{(j)}$:

Jeżeli $C_{j+1} = A^\varepsilon$, $j \geqslant 1$, wtedy:

$$d_1^{(j+1)} = ad_1^{(j)} + \varepsilon c d_2^{(j)} \qquad d_2^{(j+1)} = -\varepsilon d_1^{(j)} + ad_2^{(j)} \qquad d_3^{(j+1)} = bd_3^{(j)} \tag{3.3}$$

(uzyskujemy to mnożąc równanie (3.2) z prawej strony przez A^ε).

Jeżeli $C_{j+1} = B^\varepsilon$, $j \geqslant 1$, wtedy:

$$d_1^{(j+1)} = bd_1^{(j)} \qquad d_2^{(j+1)} = ad_2^{(j)} + \varepsilon d_3^{(j)} \qquad d_3^{(j+1)} = -\varepsilon c d_2^{(j)} + ad_3^{(j)} \tag{3.4}$$

Ponieważ $C_1 = A^\varepsilon$, to dostajemy, że $d_1^{(1)} = a$, $d_2^{(1)} = -\varepsilon$ oraz $d_2^{(1)} = 0$. Stąd pierwszym wnioskiem z (3.3) oraz (3.4) jest stwierdzenie, że wszystkie $d_k^{(j)}$ to liczby całkowite. Dla wygody określimy d_k^0 tak, by równania (3.3) oraz (3.4) były również spełnione dla $j = 0$: niech $d_1^0 = 1$, $d_2^0 = d_3^0 = 0$.

Korzystając z rekurencyjnych zależności, pokażemy że jeżeli $C_j = C_{j+1}$ to liczbę $d_2^{(j+1)}$ możemy wyrazić tylko za pomocą $d_2^{(j)}$ oraz $d_2^{(j-1)}$.

Zatem niech $C_j = C_{j+1}$, $j \geqslant 1$. Wtedy

$$d_2^{(j+1)} = 2ad_2^{(j)} - b^2 d_2^{(j-1)} \tag{3.5}$$

By to sprawdzić, zastosujemy (3.3) lub (3.4) trzy razy. Dla $C_j = C_{j+1} = A^{\pm 1}$ mamy

$$\begin{aligned} d_2^{(j+1)} = -\varepsilon d_1^{(j)} + a d_2^{(j)} = -\varepsilon \left(a d_1^{(j-1)} + \varepsilon c d_2^{(j-1)} \right) + a d_2^{(j)} = \\ = a d_2^{(j)} - a\varepsilon d_1^{(j-1)} + a^2 d_2^{(j-1)} - (a^2 + c) d_2^{(j-1)} = \\ = a d_2^{(j)} + a \left(-\varepsilon d_1^{(j-1)} + a d_2^{(j-1)} \right) - (a^2 + (b^2 - a^2)) d_2^{(j-1)} = \\ = 2a d_2^{(j)} - b^2 d_2^{(j-1)} \end{aligned}$$

Dla $C_j = C_{j+1} = B^{\pm 1}$, $j > 1$ (bo pierwsza macierz to zawsze A w potędze ± 1 z założenia). Otrzymujemy:

$$\begin{aligned} d_2^{(j+1)} = a d_2^{(j)} + \varepsilon d_3^{(j)} = a d_2^{(j)} + \varepsilon \left(-\varepsilon c d_2^{(j)} + a d_3^{(j)} \right) = \\ = a d_2^{(j)} + a\varepsilon c d_3^{(j-1)} + a^2 d_2^{(j-1)} - (a^2 + c) d_2^{(j-1)} = \\ = a d_2^{(j)} + a \left(a d_2^{(j-1)} + \varepsilon c d_3^{(j-1)} \right) - (a^2 + (b^2 - a^2)) d_1^{(j-1)} = \\ = 2a d_2^{(j)} - b^2 d_2^{(j-1)} \end{aligned}$$

Pozostaje nam przypadek gdy sąsiednie macierze nie są równe. Dla $C_j \neq C_{j+1}$ korzystając z (3.3) i (3.4) otrzymujemy, że:

Jeżeli $C_j = A^{\pm 1}$, $C_{j+1} = B^{\varepsilon}$, $j \geqslant 1$, to:

$$d_2^{(j+1)} = a d_2^{(j)} + \varepsilon d_3^{(j)} = a d_2^{(j)} + \varepsilon b d_3^{(j-1)} \tag{3.6}$$

Jeżeli $C_j = B^{\pm 1}$, $C_{j+1} = A^{\varepsilon}$, $j \geqslant 1$, to:

$$d_2^{(j+1)} = a d_2^{(j)} - \varepsilon d_1^{(j)} = a d_2^{(j)} - \varepsilon b d_1^{(j-1)} \tag{3.7}$$

Mając wyprowadzone potrzebne wzorki, możemy przystąpić do właściwej części dowodu. Od tego miejsca zaczniemy korzystać z tego, że b nie jest potęgą liczby 2.

Niech zatem $b = 2^m s$, gdzie s jest liczbą nieparzystą > 1. Oczywiście s jest względnie pierwsze z $2a$. Pokażemy za pomocą indukcji, że $d_2^{(j)}$ nie jest podzielne przez s dla $j = 1, \ldots, n$, uzyskując tym samym, że $d_2^{(n)} \neq 0$.

1° Jak zauważyliśmy wcześniej, $d_2^{(1)} = -\varepsilon$, zatem $s \nmid d_2^{(1)}$ i baza indukcji jest spełniona.

2° Załóżmy że $s \nmid d_2^{(j)}$. Jeżeli $C_j = C_{j+1}$ to korzystając z (3.5) mamy $d_2^{(j+1)} = 2a d_2^{(j)} - (2^m s)^2 d_2^{(j-1)}$, w przeciwnym przypadku z (3.6) oraz (3.7) mamy, że $d_2^{(j+1)} = a d_2^{(j)} \pm 2^m s \varepsilon d_k^{(j-1)}$, (gdzie $k = 1$ lub 3). W obu przypadkach drugi składnik jest podzielny przez s, natomiast pierwszy to iloczyn liczby całkowitej względnie pierwszej z s oraz liczby niepodzielnej przez s (z założenia indukcyjnego). Otrzymujemy zatem, że $s \nmid d_2^{(j+1)}$

Z zasady indukcji matematycznej nasze twierdzenie jest udowodnione.

□

W tym miejscu przypomnijmy własności homomorfizmu zdefiniowanego w rozdziale 2. Z każdym kwaternionem $\xi \in \mathbb{H}$ skojarzyliśmy odwzorowanie φ_ξ, będące izometrią: jest to albo obrót $\mathbb{P}$ z osią równoległą do 'czystej' części ξ jeżeli $\xi \notin \mathbb{R}$, albo identyczność, jeżeli $\xi \in \mathbb{R}$. Bardziej precyzyjnie: jeśli $\xi = x_0 + x_1 i + x_2 j + x_3 k$, wtedy w standardowej bazie $\mathbb{P}$ macierz φ_ξ, oznaczona przez M_ξ, wygląda następująco:

$$M_\xi = \frac{1}{N(\xi)} \begin{pmatrix} x_0^2 + x_1^2 - x_2^2 - x_3^2 & 2(x_1 x_2 - x_0 x_3) & 2(x_0 x_2 + x_1 x_3) \\ 2(x_0 x_3 + x_1 x_2) & x_0^2 - x_1^2 + x_2^2 - x_3^2 & 2(x_2 x_3 - x_0 x_1) \\ 2(x_1 x_3 - x_0 x_2) & 2(x_0 x_1 + x_2 x_3) & x_0^2 - x_1^2 - x_2^2 + x_3^2 \end{pmatrix} \tag{3.8}$$

Licząc ślad M_ξ w bazie standardowej otrzymamy:

$$tr(M_\xi) = \frac{1}{N(\xi)}(3x_0^2 - x_1^2 - x_2^2 - x_3^2) = 1 + 2\frac{x_0^2 - x_1^2 - x_2^2 - x_3^2}{x_0^2 + x_1^2 + x_2^2 + x_3^2}$$

natomiast licząc ślad M_ξ w bazie ortonormalnej zawierającej oś obrotu otrzymujemy:

$$tr(M_\xi) = 1 + 2\cos\theta$$

gdzie θ jest kątem obrotu M_ξ. Stąd

$$\cos\theta = \frac{x_0^2 - x_1^2 - x_2^2 - x_3^2}{x_0^2 + x_1^2 + x_2^2 + x_3^2} \tag{3.9}$$

W dalszym ciąg przez f będziemy oznaczali homomorfizm z $\mathbb{H} \setminus \{0\}$ do $SO_3(\mathbb{R})$ przyporządkowujący kwaternionowi izometrię.

Lemat 3.2.3. *Niech u, v będą generatorami grupy wolnej $\mathcal{F}$. Niech G będzie grupą generowaną przez a oraz b. Ponadto załóżmy że istnieje homomorfizm $h : G \to \mathcal{F}$, dla którego $h(a) = u$, $h(b) = v$. Wtedy G jest również grupą wolną o generatorach a, b.*

Dowód. Korzystając z własności uniwersalnej grupy wolnej $\mathcal{F}$ konstruujemy homomorfizm odwrotny $p : \mathcal{F} \to G$ zadając go na generatorach: $p(u) = a$, $p(v) = b$. Otrzymujemy, że $h \circ p = id_{\mathcal{F}}$, bo przeprowadza generatory $\mathcal{F}$ na siebie, również $p \circ h = id_G$ z analogicznych powodów. Zatem h jest izomorfizmem, a p to izomorfizm do niego odwrotny. □

Lemat 3.2.4. *Niech $a, b, c \in \mathbb{N}_+$ tworzą trójkę pitagorejską ($a^2 + b^2 = c^2$), gdzie c jest nieparzyste. Wtedy elementy $u = a + bi$ oraz $v = a + bk$ generują kopię $\mathcal{F} \subset U(H_c)$.*

Dowód. Z wyboru elementów u i v mamy że $N(u) = N(v) = c^2$, zatem z lematu 3.1.1 otrzymujemy, że $u, v \in U(H_c)$. Z (3.8) obroty $\varphi_u = f(u)$ oraz $\varphi_v = f(v)$ mają następujące macierze w bazie standardowej:

$$M_u = \frac{1}{c^2}\begin{bmatrix} c^2 & 0 & 0 \\ 0 & a^2 - b^2 & -2ab \\ 0 & 2ab & a^2 - b^2 \end{bmatrix} \quad M_v = \frac{1}{c^2}\begin{bmatrix} a^2 - b^2 & -2ab & 0 \\ 2ab & a^2 - b^2 & 0 \\ 0 & 0 & c^2 \end{bmatrix}$$

W obu przypadkach $\cos\theta = \frac{a^2-b^2}{a^2+b^2} = \frac{a^2-b^2}{c^2}$. Ponieważ a, b, c tworzą trójkę pitagorejską, otrzymujemy że $\cos\theta \notin \{0, \pm 1\}$. Gdyby $\cos\theta = \frac{\varepsilon}{2^k}$, gdzie $\varepsilon = \pm 1$, $k \in \mathbb{N}_+$, to otrzymalibyśmy $\varepsilon c^2 = 2^k a^2 - 2^k b^2$, co nie jest możliwe, bo c jest nieparzyste. Zatem z lematu 3.2.2 otrzymujemy, że grupa $\langle f(u), f(v)\rangle \cong \langle M_u, M_v\rangle$ jest wolna, a tym samym, korzystając z lematu 3.2.3, wnioskujemy, że również grupa $\langle u, v\rangle$ jest wolna.

□

Lemat 3.2.5. *Niech $a, b, c \in \mathbb{N}_+$ będą takie, że $a^2 + b^2 + c^2 = d^2$ dla pewnego nieparzystego $d \in \mathbb{N}_+$. Wtedy elementy $u = a + bi + cj$ oraz $v = a + ci - bj$ generują kopię $\mathcal{F} \subset U(H_d)$.*

Dowód. $N(u) = N(v) = d^2$, zatem z lematu 3.1.1 otrzymujemy, że u, $v \in U(H_d)$. Oś obrotu φ_u jest równoległa do wektora $(b, c, 0)$, natomiast oś obrotu φ_v jest równoległa do $(c, -b, 0)$. Kwaterniony u i v zostały tak dobrane, by wektory $(b, c, 0)$, $(c, -b, 0)$ były ortogonalne. Podstawiając współrzędne do (3.9) otrzymujemy, że dla obu obrotów cosinus kąta jest dokładnie taki sam i wynosi

$$\frac{a^2-b^2-c^2}{a^2+b^2+c^2} = \frac{a^2-b^2-c^2}{d^2}$$

Ponadto cosinus kąta nie należy do $\{0, \pm 1\} \cup \left\{\pm\frac{1}{2^k} \mid k \in \mathbb{N}_+\right\}$ ponieważ d jest nieparzyste. Rozważmy bazę ortonormalną $\mathcal{B} = \{\frac{1}{b^2+c^2}(c,-b,0), \beta, \frac{1}{b^2+c^2}(b,c,0)\}$ gdzie $\beta \in \mathbb{P}$ jest wektorem ortogonalnym do pozostałych i $||\beta|| = 1$. Zastanówmy się jak wyglądają macierze $\varphi_u = f(u)$ oraz $\varphi_v = f(v)$ w tej bazie. Jedyne czego nam brakuje to kąt obrotu - znamy tylko jego cosinus. Oznaczmy przez θ dowolny kąt o wybranym przez nas cosinusie. W bazie $\mathcal{B}$ macierz M_u ma jedną z dwóch postaci:

$$M_u^{(1)} = \begin{bmatrix} \cos\theta & -\sin\theta & 0 \\ \sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{bmatrix} \text{ lub } M_u^{(2)} = \begin{bmatrix} \cos(-\theta) & -\sin(-\theta) & 0 \\ \sin(-\theta) & \cos(-\theta) & 0 \\ 0 & 0 & 1 \end{bmatrix} = \begin{bmatrix} \cos\theta & \sin\theta & 0 \\ -\sin\theta & \cos\theta & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

Analogicznie macierz M_v ma jedną z dwóch postaci $M_v^{(1)}$ lub $M_v^{(2)}$. Zauważmy przy tym, że $\left(M_u^{(1)}\right)^{-1} = M_u^{(2)}$ oraz $\left(M_v^{(1)}\right)^{-1} = M_v^{(2)}$. Zatem $\langle f(u), f(v)\rangle \cong \langle M_u, M_v\rangle = \left\langle M_u^{(1)}, M_v^{(1)}\right\rangle$ (bo niezależnie czy weźmiemy jakiś element czy element do niego odwrotny zostanie wygenerowana ta sama grupa), korzystając z lematu 3.2.2 otrzymujemy, że $\left\langle M_u^{(1)}, M_v^{(1)}\right\rangle$ jest grupą wolną, a tym samym z lematu 3.2.3 grupa $\langle u, v\rangle \subset U(H_d)$ jest wolna. □

Kolejnym celem jest wykazanie, że grupa $U(H_2)$ nie zawiera podgrupy izomorficznej z $\mathcal{F}$. W tym celu potrzebujemy wprowadzić pewne pomocnicze narzędzie z teorii grup.

Definicja 3.2.6. *Grupę G nazwiemy* prawie abelową *wtedy i tylko wtedy, gdy zawiera abelowy dzielnik normalny A taki że G/A jest grupą skończoną.*

Wniosek 3.2.7. *Grupa prawie abelowa nie zawiera nieabelowej podgrupy wolnej generowanej przez dwa elementy.*

Dowód. Niech G będzie grupą prawie abelową, niech A będzie jej abelowym dzielnikiem normalnym takim, że grupa G/A jest skończona. Załóżmy, że G zawiera nieabelową podgrupę wolną, niech $g, h \in G$ będą jej generatorami. Ponieważ G/A jest skończona, istnieje $n \in \mathbb{N}_+$ takie, że $(gA)^n = A$, a tym samym $g^n \in A$. Analogicznie istnieje $m \in \mathbb{N}_+$ takie, że $h^m \in A$. Ponieważ A jest abelowe, otrzymujemy, że $g^n h^m = h^m g^n$, a tym samym $h^{-m} g^n h^m g^{-n} = 1$. Sprzeczność, g, h nie generują grupy wolnej. □

Lemat 3.2.8. *Jeżeli suma kwadratów czterech liczb całkowitych jest podzielna przez 8, to wszystkie te liczby są parzyste.*

Dowód. Kwadrat liczby nieparzystej modulo 8 to zawsze 1, kwadrat liczby parzystej modulo 8 należy do zbioru $\{0, 4\}$. Gdybyśmy wzięli 4 liczby nieparzyste to suma ich kwadratów modulo 8 wynosiłaby 4, gdybyśmy wzięli 1, 2 lub 3 liczby nieparzyste to suma kwadratów modulo 4 należałaby odpowiednio do zbioru $\{1, 5\}$, $\{2, 6\}$, $\{3, 7\}$. We wszystkich przypadkach uzyskujemy sumę niepodzielną przez 8. □

Po krótkim wprowadzeniu dysponujemy już potrzebnymi narzędziami, by udowodnić, następujący lemat:

Lemat 3.2.9. *Grupa $U(H_2)$ jest prawie abelowa, więc nie zawiera kopii $\mathcal{F}$.*

Dowód. Z lematu 3.1.1 otrzymujemy, że $\alpha \in U(H_2)$ wtedy i tylko wtedy $N(\alpha) \in U(A_2)$, a to zachodzi wtedy i tylko wtedy, gdy $N(\alpha) = 2^n$ dla pewnego $n \in \mathbb{Z}$. Zatem dowolne $\alpha \in U(H_2)$ możemy przedstawić w postaci $2^m\beta$, gdzie $m \in \mathbb{Z}$, $\beta = b_0 + b_1 i + b_2 j + b_3 k \in H$, a co najmniej jedno b_i jest nieparzyste. Oczywiście $N(\beta) = 2^k$ dla pewnego $k \in \mathbb{N}$.

Rozpatrzmy teraz podgrupę $\langle 2 \rangle \subset U(H_2)$. Ta podgrupa należy do centrum, zatem jest abelowa i jest dzielnikiem normalnym. Korzystając z obserwacji poczynionej wyżej jako reprezentantów warstw względem $\langle 2 \rangle$ możemy wybrać $\beta \in H$, gdzie co najmniej jedna współrzędna jest nieparzysta. Ale korzystając z tego, że norma β jest potęgą 2 oraz z lematu 3.2.8 otrzymujemy, że wystarczy ograniczyć się do takich $\beta \in H$, że $N(\beta) \in \{1, 2, 4\}$, a tych jest tylko skończenie wiele. Zatem $\langle 2 \rangle$ jest dzielnikiem normalnym skończonego indeksu. □

Lemat 3.2.10. *Niech p będzie nieparzystą liczbą pierwszą.*

- *Jeżeli $p \equiv 1 \pmod 4$ to p^2 jest nietrywialną sumą dwóch kwadratów.*
- *Jeżeli $p \equiv 3 \pmod 4$ to p^2 jest nietrywialną sumą trzech kwadratów.*

Dowód. W dowodzie pierwszej własności skorzystamy z pewnego elementarnego twierdzenia z teorii liczb, którego nie dowodzimy, jedynie podamy pozycje, w której zainteresowany czytelnik może ów dowód znaleźć. Zatem jeżeli $p = 4m + 1$, to ogólnie wiadomo, korzystając np. z [Sier59], że $p = a^2 + b^2$, dla pewnych $a, b \in \mathbb{N}_+$. Wtedy $p^2 = (a^2 - b^2)^2 + (2ab)^2$ i oba składniki są niezerowe.

Teraz niech $p = 4m+3$. Korzystając z twierdzenia Lagrange'a o sumie czterech kwadratów, (które de facto udowodnimy później w rozdziale 4) wiemy, że $p = a^2+b^2+c^2+d^2$ dla pewnych $a, b, c, d \in \mathbb{N}$. Ponieważ kwadrat liczby nieparzystej modulo 4 to 1, a kwadrat liczby parzystej modulo 4 to 0, otrzymujemy, że dokładnie trzy z pośród liczb a, b, c, d są nieparzyste, a tym samym przynajmniej trzy są niezerowe. W ten sposób otrzymujemy, że $p^2 = (a^2 + b^2 + c^2 + d^2)^2 = (a^2 + b^2 - c^2 - d^2)^2 + (2ac + 2bd)^2 + (2ad - 2bc)^2$. Pozostaje zweryfikować, że wszystkie 3 elementy są niezerowe:

- Jeżeli $a^2+b^2-c^2-d^2 = 0$ to dodając stronami równanie $a^2+b^2+c^2+d^2 = p$ otrzymamy, że $2(a^2 + b^2) = p$. Sprzeczność, bo p jest liczbą pierwszą większą od 2.
- 2ac + 2bd jest z pewnością niezerowe, bo maksymalnie jedna z liczb a, b, c, d jest zerowa.
- Załóżmy że $2ad - 2bc = 0$. Wtedy $ad = bc$. Jak zauważyliśmy wyżej dokładnie jedna z liczb a, b, c, d jest parzysta. Ale wtedy w równaniu $ad = bc$ mamy po jednej stronie liczbę parzystą, a po drugiej nieparzystą. Sprzeczność.

□

Możemy teraz przystąpić do dowodu głównego twierdzenia tego rozdziału, które orzeka, że dla $n \in \mathbb{N}_+ : \mathcal{F} \subseteq U(H_n))$ wtedy i tylko wtedy, gdy n nie jest potęgą 2.

Dowód twierdzenia 3.2.1. Niech $A_n \subseteq \mathbb{Q}$ dla pewnego $n \in \mathbb{N}_+$. Jeżeli n nie jest potęgą 2 to niech p będzie nieparzystym dzielnikiem pierwszym n. Oczywiście $A_p \subseteq A_n$. Z lematu 3.2.10 mamy, że p^2 jest sumą dwóch lub trzech nietrywialnych kwadratów, a wtedy korzystając z lematu 3.2.4 albo 3.2.5 otrzymujemy, że $\mathcal{F} \subseteq U(H_p) \subseteq U(H_n)$. Ponadto generatory $\mathcal{F}$ są wyznaczone *wprost* z podanych lematów.

Jeżeli n jest potęgą 2 to $A_n = \mathbb{Z}$ (i $U(H_1)$ nie zawiera $\mathcal{F}$) lub $A_n = A_2$ (i również z lematu 3.2.9 grupa $U(H_n)$ nie zawiera $\mathcal{F}$). □

Wniosek 3.2.11. *Niech $A \subseteq \mathbb{Q}$ będzie dowolnym podpierścieniem. Wtedy $\mathcal{F} \subseteq U(H(A))$ wtedy i tylko wtedy, gdy $A \nsubseteq A_2$.*

Dowód. Niech $A \subseteq \mathbb{Q}$ będzie podpierścieniem takim, że $A \nsubseteq A_2$. Istnieje nieskracalny ułamek $\frac{a}{b} \in A$ taki że $a, b \in \mathbb{N}_+$ oraz b nie jest potęgą 2. Wiemy też, że $1 = \frac{b}{b} \in A$. Liczby a, b są względnie pierwsze, zatem z rozszerzonego algorytmu Euklidesa $xa + yb = 1$ dla pewnych $x, y \in \mathbb{Z}$. Zatem mamy, że

$$\underbrace{\left(sgn(x)\frac{a}{b}\right) + \cdots \left(sgn(x)\frac{a}{b}\right)}_{|x|} + \underbrace{\left(sgn(y)\frac{b}{b}\right) + \cdots \left(sgn(y)\frac{b}{b}\right)}_{|y|} = \frac{xa + yb}{b} = \frac{1}{b}$$

gdzie $sgn(z)$ oznacza znak liczby całkowitej z. Zatem $\frac{1}{b} \in A$, a z tego wynika, że $H_b \subseteq A$, a z twierdzenia 3.2.1 wiemy, że $\mathcal{F} \subseteq U(H_b) \subseteq U(H(A))$.

Implikacja w drugą stronę jest oczywista z lematu 3.2.9 . □

Rozdział 4

Twierdzenie Lagrange'a o czterech kwadratach

W tym rozdziale pokażemy jak można zastosować kwaterniony w teorii liczb, udowadniając klasyczne twierdzenie Lagrange'a, mówiące że każdą liczbę naturalną można przedstawić jako sumę kwadratów czterech liczb naturalnych. Dowód ten można również przeprowadzić wykorzystując tylko mechanizmy teorioliczbowe (patrz np. [Sier59]), jednakże dla nas jest świetnym pretekstem do wprowadzenia nowego podpierścienia kwaternionów hamiltonowskich, który sam w sobie ma interesujące własności: jest 'prawie' pierścieniem Euklidesowym. 'Prawie' - ponieważ w oczywisty sposób brakuje jednej ważnej własności: mamy do czynienia z pierścieniem nieprzemiennym. Mimo to, analogicznie do pierścienia Euklidesowego, można w bardzo łatwy sposób scharakteryzować ideały *lewostronne*. Użyta charakteryzacja zostanie wykorzystana w dowodzie twierdzenia Lagrange'a.

Szkic dowodu został zapożyczony z [Her64].

4.1. Kwaterniony Hurwitz'a

W dalszej pracy przez ζ będziemy oznaczali kwaternion postaci: $\frac{1}{2}(1+i+j+k)$.

Definicja 4.1.1. *Niech*

$$H = \{m_0\zeta + m_1 i + m_2 j + m_3 k \mid m_0, m_1, m_2, m_3 \in \mathbb{Z}\} \subseteq \mathbb{H}$$

H będziemy nazywali pierścieniem Hurwitz'a kwaternionów całkowitych *lub w skrócie* kwaternionami Hurwitz'a.

Zanim pokażemy że H to rzeczywiście podpierścień $\mathbb{H}$, zauważmy, że podstawiając za m_0 liczby parzyste otrzymamy zwykłe kwaterniony całkowite, natomiast podstawiając liczby nieparzyste otrzymamy kwaternion o współrzędnych należących do zbioru $\left\{x + \frac{1}{2} \mid x \in \mathbb{Z}\right\} =: \mathbb{Z} + \frac{1}{2}$. Zatem możemy zapisać H w alternatywnej postaci:

$$H = \left\{m_0 + m_1 i + m_2 j + m_3 k \mid m_0, m_1, m_2, m_3 \in \mathbb{Z} \text{ lub } m_0, m_1, m_2, m_3 \in \mathbb{Z} + \frac{1}{2}\right\}$$

$$= \frac{1}{2}\left\{m_0 + m_1 i + m_2 j + m_3 k \mid m_0, m_1, m_2, m_3 \in \mathbb{Z} \text{ i są tej samej parzystości}\right\} \tag{4.1}$$

Czyli jeżeli $x \in H$ to albo $x = q$, albo $x = q + \zeta$, gdzie q to pewien kwaternion całkowity.

H jest podgrupą $\mathbb{H}$ w oczywisty sposób, zawiera też 1. Musimy pokazać że mnożenie jest działaniem wewnętrznym w H. Niech $x, y \in H$, $x = p + \delta_1\zeta$, $y = q + \delta_2\zeta$, gdzie p, q to kwaterniony całkowite, a δ_1, δ_2 przyjmują odpowiednio wartości 0 lub 1.

$$xy = (p + \delta_1\zeta)(q + \delta_2\zeta) = pq + \delta_1(\zeta q) + \delta_2(p\zeta) + \delta_1\delta_2(\zeta^2)$$

Oczywiście pierwszy składnik należy do H, ostatni również bo $\zeta^2 = \left(\frac{1}{2}(1+i+j+k)\right)^2 = \frac{1}{4}(-2+2i+2j+2k) = \frac{1}{2}(-1+i+j+k) \in H$. Pozostaje wykazać że $p\zeta, \zeta q \in H$ dla dowolnych p, q. Niech zatem $p = a_0 + a_1 i + a_2 j + a_3 k$. Wtedy

$$p\zeta = (a_0 + a_1 i + a_2 j + a_3 k)\left(\frac{1}{2}(1+i+j+k)\right) = \frac{1}{2}\left((a_0 + a_1 i + a_2 j + a_3 k)(1+i+j+k)\right) = \frac{1}{2}(b_0 + b_1 i + b_2 j + b_3 k)$$

gdzie wszystkie współrzędne b_i są postaci $a_0 \pm a_1 \pm a_2 \pm a_3$. Dodając do nich $a_0 + a_1 + a_2 + a_3$ otrzymamy liczbę parzystą, zatem wszystkie b_i są tej samej parzystości, zatem z (4.1) mamy, że $p\zeta \in H$. Dowód dla ζq jest analogiczny, dlatego go pominiemy.

Lemat 4.1.2. *Niech $x \in H$. Wtedy $\overline{x} \in H$ oraz $N(x)$ jest liczbą naturalną.*

Dowód. Pierwsza część jest oczywista z charakterystyki (4.1).

Niech teraz $x = \frac{a_0}{2} + \frac{a_1}{2}i + \frac{a_2}{2}j + \frac{a_3}{2}k$, gdzie a_0, a_1, a_2, a_3 są liczbami całkowitymi tej samej parzystości. Wtedy $N(x) = \frac{a_0^2+a_1^2+a_2^2+a_3^2}{2}$. Jeżeli wszystkie a_i są nieparzyste to $a_i^2 \equiv 1 \pmod 4$, w przeciwnym wypadku $a_i^2 \equiv 0 \pmod 4$. Zarówno w pierwszej jak i w drugiej sytuacji z (4.1) otrzymujemy, że licznik jest liczbą naturalną podzielną przez 4. □

Lemat 4.1.3. *Jeżeli $a \in H$ to $a^{-1} \in H$ wtedy i tylko wtedy, gdy $N(a) = 1$.*

Dowód. $\Rightarrow$ Jeżeli $a, a^{-1} \in H$, to z lematu 4.1.2 wiemy, że $N(a), N(a^{-1}) \in \mathbb{N}$, ponadto $N(a)N(a^{-1}) = N(aa^{-1}) = N(1) = 1$, zatem jedyna możliwość to $N(a) = 1$.

$\Leftarrow$ Jeżeli $a \in H$ oraz $N(a) = 1$, to korzystając z równości $a\overline{a} = N(a) = 1$ otrzymujemy że $a^{-1} = \overline{a}$ oraz $\overline{a} \in H$ z lematu 4.1.2. □

W tym miejscu warto poczynić pewną uwagę. Dlaczego właściwie wybraliśmy taki 'nienaturalny' i dziwny pierścień H ? Czy nie prościej było skorzystać ze zwykłych całkowitych kwaternionów ? Okazuje się, że pierścień całkowitych kwaternionów jest w pewnych sensie „za mały" i nie zachodzi w nim lemat, który poniżej udowodnimy, a który przybliża kwaterniony Hurwitz'a do czegoś na wzór pierścienia Euklidesowego: w kwaternionach Hurwitz'a można (w pewnym sensie) wykonywać dzielenie z resztą.

Lemat 4.1.4 (Algorytm lewostronnego dzielenia)**.** *Niech $a, b \in H$, oraz $b \neq 0$. Wtedy istnieją elementy $c, d \in H$ takie, że $a = cb + d$ oraz $N(d) < N(b)$.*

Dowód. Na początku rozpatrzmy łatwiejszy przypadek: b jest liczbą naturalną dodatnią. Niech zatem $a = t_0\zeta + t_1 i + t_2 j + t_3 k$, gdzie t_0, t_1, t_2, t_3 są liczbami całkowitymi, $b = n$ dla pewnej liczby naturalnej dodatniej n. Niech $c = x_0\zeta + x_1 i + x_2 j + x_3 k$ będzie szukanym kwaternionem, którego całkowite współczynniki x_0, x_1, x_2, x_3 musimy ustalić. Naszym celem jest taki ich dobór by zachodziło: $N(a - cn) < N(n) = n^2$.

$$a - cn = \left(t_0\left(\frac{1+i+j+k}{2}\right) + t_1 i + t_2 j + t_3 k\right) - nx_0\left(\frac{1+i+j+k}{2}\right) - nx_1 i - nx_2 - nx_3 k =$$
$$= \frac{1}{2}(t_0 - nx_0) + \frac{1}{2}(t_0 + 2t_1 - n(t_0 + 2x_1))i + \frac{1}{2}(t_0 + 2t_1 - n(t_0 + 2x_2))j$$
$$+\frac{1}{2}(t_0 + 2t_3 - n(t_0 + 2x_3))k$$

Trzeba pokazać, że można tak dobrać x_0, x_1, x_2, x_3, by następujące oszacowania na współrzędne były prawdziwe: $|t_0 - nx_0| \leqslant \frac{1}{2}n$, $|t_0 + 2t_d - n(t_0 + 2x_d)| \leqslant n$ dla $d \in \{1, 2, 3\}$. Wtedy dostaniemy, że

$$N(a-cn) = \frac{(t_0 - nx_0)^2}{4} + \frac{(t_0 + 2t_1 - n(t_0 + 2x_1))^2}{4} + \cdots \leqslant \frac{1}{16}n^2 + \frac{1}{4}n^2 + \frac{1}{4}n^2 + \frac{1}{4}n^2 < n^2 = N(n)$$

Ale to już łatwo spełnić, bo

- Z własności dzielenia z resztą w liczbach całkowitych istnieje liczba całkowita x_0 taka że $t_0 = x_0 n + r$, gdzie $-\frac{n}{2} \leqslant r \leqslant \frac{n}{2}$, i dla niej $|t_0 - x_0 n| = |r| \leqslant \frac{n}{2}$.

- Ustalmy $d \in \{1, 2, 3\}$. Ponownie z tej samej własności istnieje taka liczba naturalna k, że $t_0 + 2t_d = kn + r$ oraz $0 \leqslant r < n$. Mamy teraz dwa przypadki:

  - $k - t_0$ jest parzyste. Wybierając x_d t. że $2x_d = k - t_0$ mamy $t_0 + 2t_d = (2x_d + t_0)n + r$ i w rezultacie $|t_0 + 2t_d - (2x_d + t_0)n| = r < n$
  - $k - t_0$ jest nieparzyste. Wybieramy x_d t. że $2x_d = k - t_0 + 1$. Wtedy $t_0 + 2t_d = (2x_d + t_0 - 1)n + r = (2x_d + t_0)n + r - n$ i w rezultacie $|t_0 + 2t_d - (2x_d + t_0)n| = |r - n| \leqslant n$

  Zatem zawsze możemy znaleźć takie x_d całkowite, że $|t_0 + 2t_d - (2x_d + t_0)n| \leqslant n$

Dowód łatwiejszego przypadku został zakończony.

Niech teraz b będzie dowolnym niezerowym elementem H. Z lematu (4.1.2) $n = b\bar{b}$ jest liczbą całkowitą, zatem z pierwszej części niniejszego dowodu otrzymujemy, że istnieje takie $c \in H$, że $a\bar{b} = cn + d_1$, gdzie $N(d_1) < N(n)$. Zatem $N(a\bar{b} - cn) < N(n)$. Rozpisując lewą stronę otrzymamy, że $N(a\bar{b} - cn) = N(a\bar{b} - cb\bar{b}) = N((a - cb)\bar{b}) = N(a - cb)N(\bar{b})$, natomiast rozpisując prawą: $N(n) = N(b\bar{b}) = N(b)N(\bar{b})$. Uzyskaliśmy, że $N(a - cb)N(\bar{b}) < N(b)N(\bar{b})$, a ponieważ $N(\bar{b}) > 0$ otrzymujemy, że $N(a - cb) < N(b)$. Czyli biorąc po prostu $d = a - cb$ otrzymujemy, że $a = cb + d$ oraz $N(d) < N(b)$. Dowód ogólnego przypadku został zakończony. □

Na Algebrze I dla pierścieni Euklidesowych R, w których zachodzi własność dzielenia z resztą, dowodzi się podstawowy fakt, mówiący że R jest dziedziną ideałów głównych. Mając lemat 4.1.4 jesteśmy w stanie udowodnić analogon tej własności odpowiedni dla przypadku nieprzemiennego.

Twierdzenie 4.1.5. *Niech L będzie lewostronnym ideałem H. Wtedy istnieje element $u \in L$ taki, że każdy każdy element z L jest* lewostronną wielokrotnością *u. Innymi słowy: istnieje element $u \in L$ taki, że każdy element $x \in L$ jest postaci $x = ru$ dla pewnego $r \in H$.*

Dowód. Jeżeli $L = \{0\}$ to nie ma czego dowodzić, po prostu bierzemy $u = 0$.

Załóżmy, że L zawiera jakiś niezerowy element. Z lematu 4.1.2 norma niezerowych elementów jest liczbą naturalną, zatem weźmy $u \in L$ o najmniejszej dodatniej normie. Pokażemy że to nasz szukany element. Niech zatem $x \in L$ będzie dowolne. Na mocy lematu 4.1.4 istnieją takie $c, d \in H$, że $x = cu + d$ oraz $N(d) < N(u)$. Ponieważ L jest lewostronnym ideałem oraz $d = x - cu$, gdzie $x, u \in L$ otrzymujemy także, że $d \in L$. Ale norma d jest mniejsza od normy u – zatem z wyboru u musi być równa 0, a tym samym $d = 0$. W rezultacie $x = cu$. □

4.2. Dowód twierdzenia Lagrange'a

Mając opisane własności kwaternionów H potrzebujemy jeszcze kilka szczegółów technicznych.

Lemat 4.2.1 (Tożsamość Eulera)**.** *Niech $\alpha_0, \alpha_1, \alpha_2, \alpha_3, \beta_0, \beta_1, \beta_2, \beta_3 \in \mathbb{R}$. Wtedy*

$$\begin{aligned}(\alpha_0^2+\alpha_1^2+\alpha_2^2+\alpha_3^2)(\beta_0^2+\beta_1^2+\beta_2^2+\beta_3^2) = \\ (\alpha_0\beta_0-\alpha_1\beta_1-\alpha_2\beta_2-\alpha_3\beta_3)^2+(\alpha_0\beta_1+\alpha_1\beta_0+\alpha_2\beta_3-\alpha_3\beta_2)^2 \\ +(\alpha_0\beta_2-\alpha_1\beta_3+\alpha_2\beta_0+\alpha_3\beta_1)^2+(\alpha_0\beta_3+\alpha_1\beta_2-\alpha_2\beta_1+\alpha_3\beta_0)^2\end{aligned}$$

Dowód. Oczywiście najprościej byłoby przeliczyć wszystko po współrzędnych, jednakże mając już wyprowadzą pewną maszynerię możemy to zrobić znacznie prościej. Rozważmy kwaterniony $p = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k \in \mathbb{H}$, $q = \beta_0 + \beta_1 i + \beta_2 j + \beta_3 k \in \mathbb{H}$. Lewa strona równania to $N(p)N(q)$, prawa strona równania to $N(pq)$. Wobec własności $N(p)N(q) = N(pq)$ lemat uznajemy za udowodniony. □

Wniosek 4.2.2. *Biorąc w lemacie 4.2.1 zamiast liczb rzeczywistych liczby całkowite wnioskujemy, że iloczyn sumy czterech kwadratów przez sumę czterech kwadratów jest sumą czterech kwadratów.*

Lemat 4.2.3. *Dla dowolnej liczby pierwszej p istnieją takie $x, y \in \mathbb{Z}_p$, że $x^2 + y^2 + 1 = 0$.*

Dowód. Biorąc $a = b = -1$ zauważmy, że jest to szczególny przypadek lematu 1.2.14 z rozdziału 1. □

Wreszcie możemy udowodnić główne twierdzenie tego rozdziału:

Twierdzenie 4.2.4 (Lagrange'a o czterech kwadratach)**.** *Każda liczba naturalna n da się przedstawić jako sumę kwadratów czterech liczb naturalnych.*

Dowód. Oczywiście $0 = 0^2 + 0^2 + 0^2 + 0^2$ oraz $1 = 1^2 + 0^2 + 0^2 + 0^2$, zatem w dalszym ciągu zakładamy, że n jest większe od 1. Korzystając z wniosku 4.2.2 możemy od razu zredukować sytuację do przypadku, gdy n jest liczbą pierwszą. Oznaczmy ją przez p. Naszym pierwszym celem jest skonstruować taki ideał lewostronny L, że mamy ciąg niewłaściwych inkluzji ideałów lewostronnych: $pH \subsetneq L \subsetneq H$. Niech x, y będą liczbami z lematu 4.2.3. Przechodząc do $\mathbb{Z}$ otrzymujemy, że $p|1 + x^2 + y^2$. Weźmy kwaternion $t = 1 + xi + yj \in H$. Niech

$$L = \{q \mid qt \in pH\}$$

Pokażemy że tak zdefiniowany zbiór ma oczekiwane własności, czyli:

- L jest ideałem lewostronnym H.

  L jest oczywiście podgrupą H. Ponadto niech $q \in L, a \in H$, wtedy $(aq)t = a(qt) \in pH$, bo $qt \in pH$ oraz pH jest ideałem lewostronnym. Zatem $aq \in L$

- $L \neq H$

  Istotnie, $1 \notin L$, ponieważ $1t = t \notin pZ$.

- $pH \subsetneq L$

  Niech $a \in pH$. Wtedy $a = pq$ dla pewnego $q \in H$. Mamy więc $at = (pq)t = p(qt) \in pH$. Zatem $pH \subseteq L$. Ponadto weźmy $\bar{t} = 1 - xi - yj$. Oczywiście $\bar{t} \notin pH$. Ale $\bar{t}t = N(t) = 1 + x^2 + y^2 \in pH$, zatem $\bar{t} \in L$.

Mając skonstruowane potrzebne ideały, z twierdzenia 4.1.5 wiemy, że istnieje taki $u \in L$, że każdy element z L jest lewostronną wielokrotnością u. Ponieważ $p \in pH \subset L$, to $p = cu$ dla pewnego $c \in H$. Oczywiście $u \notin pH$, zatem c nie może mieć odwrotności w H, bo wtedy $u = c^{-1}p$ należałoby do pH. Stosując lemat 4.1.3 otrzymujemy, że $N(c) > 1$. Ponadto ponieważ $L \neq H$, to u również nie może mieć odwrotności w H, a tym samym ponownie z lematu 4.1.3 mamy, że $N(u) > 1$. Ostatecznie otrzymujemy, że $p^2 = N(p) = N(cu) = N(c)N(u)$, a ponieważ zarówno $N(c)$, jak i $N(u)$ to liczby naturalne większe od 1, jedyna możliwość to $N(u) = N(c) = p$.

Już prawie skończyliśmy. Korzystając z charakteryzacji (4.1) otrzymujemy w szczególności, że $u = \frac{1}{2}u'$ dla pewnego $u' \in H$, $u = m_0 + m_1 i + m_2 j + m_3 k$, a tym samym $p = N(u) = N\left(\frac{1}{2}u'\right) = \frac{m_0^2+m_1^2+m_2^2+m_3^2}{4}$. Zatem $4p = m_0^2 + m_1^2 + m_2^2 + m_3^2$.

By zakończyć dowód zastosujemy stary trik Eulera: jeżeli $2a = x_0^2 + x_1^2 + x_2^2 + x_3^2$, gdzie a, x_0, x_1, x_2, x_3 są liczbami całkowitymi, to $a = y_0^2+y_1^2+y_2^2+y_3^2$ dla pewnych liczb całkowitych y_0, y_1, y_2, y_3. Na początku zauważmy, że ponieważ $2a$ jest parzyste, to albo wszystkie x_i dla $i = 0, 1, 2, 3$ są parzyste, albo wszystkie są nieparzyste, albo dwa są parzyste, a drugie dwa nieparzyste. Zatem możemy je tak przenumerować, by liczby:

$$y_0 = \frac{x_0 + x_1}{2}, \qquad y_1 = \frac{x_0 - x_1}{2}, \qquad y_2 = \frac{x_2 + x_3}{2}, \qquad y_3 = \frac{x_2 - x_3}{2}$$

też były całkowite. Wtedy

$$y_0^2 + y_1^2 + y_2^2 + y_3^2 = \left(\frac{x_0 + x_1}{2}\right)^2 + \left(\frac{x_0 - x_1}{2}\right)^2 + \left(\frac{x_2 + x_3}{2}\right)^2 + \left(\frac{x_2 - x_3}{2}\right)^2 = \\ = \frac{1}{2}(x_0^2 + x_1^2 + x_2^2 + x_3^2) = \frac{1}{2}(2a) = a$$

Ponieważ $4p$ jest sumą czterech kwadratów, stosując podany trick otrzymujemy, że $2p$ również jest sumą czterech kwadratów. Stosując go jeszcze raz uzyskujemy taki samy wniosek dla p. Zatem $p = a_0^2 + a_1^2 + a_2^2 + a_3^2$ dla liczb naturalnych a_0, a_1, a_2, a_3 i tym samym dowód twierdzenia Lagrange'a został zakończony. □

Bibliografia

[Brow68] Jerzy Browkin, *Wybrane zagadnienia algebry*, PWN, Warszawa 1968.

[Brow77] Jerzy Browkin, *Podstawy teorii ciał*, PWN, Warszawa 1977.

[Gon84] J. Z. Gonçalves, *Free subgroups of units in group rings*, Canad. Math. Bull. 27 (1984), 309-312.

[Her64] I. N. Hernstein, *Topics in algebra*, Blaisdell Publishing Company, 1964.

[Kar76] M. I. Kargapołow, J. I. Mierzlakow, *Podstawy teorii grup*, PWN, Warszawa 1976.

[Kop05] Przemysław Koprowski, *Okruchy geometrii komputerowej*, 2003-2005, praca dostępna elektronicznie: http://z2.math.us.edu.pl/perry/papers/okruchy.pdf .

[Kre01] Jan Krempa, *On free subgroups of units in quaternion algebras*, Colloq. Math. 88 (2001), 21-27.

[Pier82] Richard S. Pierce, *Associative Algebras*, Springer-Verlag, New York, 1982.

[Sier59] Wacław Sierpiński, *Arytmetyka teoretyczna*, wydanie drugie zmienione, PWN, Warszawa 1959.

[Świe94] S. Świerczkowski, *A class of free rotation groups*, Indag. Math. (NS) 5 (1994), 221-226.