Twierdzenie Lagrange'a

Mikołaj Stańczyk

26 marca 2010

1. Początki

Rozważania dotyczące przedstawiania liczby jako **sumy czterech kwadratów** pojawiają się już w słynnym dziele *Arytmetyka*, autorstwa Diofantosa — aleksandryjskiego matematyka żyjącego w 3. wieku n. e. W 1621 roku, w przygotowanej przez francuskiego matematyka Claude'a Gasparda Bacheta łacińskiej edycji tego dzieła, zamieszczone zostało następujące twierdzenie:

> Każda liczba naturalna jest sumą czterech kwadratów.

Zostało ono udowodniona przez znanego włoskiego matematyka **Josepha Louisa Lagrange'a** w 1770 roku — dlatego zostało nazwane jego imieniem.

Dowód twierdzenia Lagrange'a, który przedstawimy, opiera się na zastosowaniu metod algebraicznych. Zanim będziemy w stanie go przeprowadzić, musimy wprowadzić deficje kilku ważnych pojęć algebraicznych i omówić ich własności.

2. Kwaterniony Hamiltona

Przypomnijmy, że **liczbą zespoloną** nazywamy każdą liczbę postaci $a + bi$, gdzie a oraz b są liczbami rzeczywistymi, a i jest tak zwaną **jednostką urojoną**, która spełnia zależność $i^2 = -1$. Nie będziemy tutaj opisywać konstrukcji liczb zespolonych; ograniczymy się jedynie do stwierdzenia, że typowa konstrukcja zbioru liczb zespolonych $\mathbb{C}$ opiera się na wprowadzeniu działań dodawania i mnożenia na parach uporządkowanych liczb rzeczywistych. Konstrukcja taka pozwala w prosty sposób uzasadnić najważniejsze własności algebraiczne liczb zespolonych.

Liczby zespolone dają wyraźne korzyści, gdy zostaną wykorzystane w **geometrii płaszczyzny**. Fakt ten skłonił matematyków do poszukiwań podobnego systemu, który pozwoliłby w analogiczny sposób opisać **przestrzeń trójwymiarową**.

Sir William Rowan Hamilton, irlandzki matematyk, był jedną z osób, które poszukiwały odpowiedniego sposobu konstrukcji. Hamilton chciał zdefiniować działania na trójkach uporządkowanych, tak, aby otrzymać konstrukcję o podobnych własnościach do systemu $\mathbb{C}$. Z pewnych przyczyn okazało się to jednak niemożliwe.

W poniedziałek, 16 października 1843, podczas spaceru z żoną po rodzinnym Dublinie, Hamiltonowi przyszła do głowy koncepcja wprowadzenia działań na zbiorze czwórek — a nie trójek — uporządkowanych. Idea była dla niego tak ekscytująca, że wyrył reguły działań na kwaternionach na moście nad Kanałem

Królewskim. Pomysł istotnie okazał się rewelacyjny — czwórki uporządkowane, nazwane później **kwaternionami** odegrały znaczącą rolę w rozwoju nauki — przede wszystkim w matematyce, fizyce i astronomii, a ostatnio mają również szerokie zastosowanie w grafice komputerowej.

Nakreślimy teraz najważniejsze idee związane z pojęciem kwaternionów. Nie będziemy tutaj podawać formalnej konstrukcji — ograniczymy się jedynie do wymienienia podstawowych własności, które wystarczą do naszych bezpośrednich celów. Podkreślamy tutaj, że takie podejście nie daje nam informacji na temat tego *czym* tak naprawdę jest kwaternion; niemniej jednak przy definiowaniu jakichkolwiek liczb ważne jest, aby definicja zapewniała nam pożądane własności — kwestia budowy nie odgrywa na ogół żadnej roli. W szczególności, kwaterniony można definiować zarówno jako uporządkowane pary liczb zespolonych, jak i pewne szczególne macierze kwadratowe — w obu przypadkach otrzymujemy **identyczny pod względem własności obiekt**.

Określenie kwaternionu, które przyjmiemy jest podobne do określenia liczby zespolonej; jak się wkrótce przekonamy, każda liczba zespolona jest kwaternionem.

Określenie 2.1. **Kwaternionem** nazywamy wyrażenie $\xi = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$, gdzie a, b, c, d są liczbami rzeczywistymi. Zbiór wszystkich kwaternionów oznaczamy symbolem $\mathbb{H}$.

Określenie 2.2. Niech $\xi = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ oraz $\xi' = a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k}$. Kwaterniony ξ, ξ' nazywamy **równymi** jeśli $a = a' \wedge b = b' \wedge c = c' \wedge d = d'$.

Wprowadzimy teraz **działanie dodawania i odejmowania kwaternionów**. Są one bardzo podobne do odpowiadających im działań na liczbach zespolonych.

Określenie 2.3. Niech $\xi = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ oraz $\xi' = a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k}$. **Sumą kwaternionów** ξ, ξ' nazywamy kwaternion $\xi + \xi' := (a + a') + (b + b')\mathbf{i} + (c + c')\mathbf{j} + (d + d')\mathbf{k}$. **Różnicą kwaternionów** ξ, ξ' nazywamy kwaternion $\xi - \xi' := (a - a') + (b - b')\mathbf{i} + (c - c')\mathbf{j} + (d - d')\mathbf{k}$.

Znacznie bardziej złożone jest wprowadzenie **działania mnożenia**. Zanim podamy ogólny sposób mnożenia kwaternionów, zatrzymamy się na chwilę nad określeniem **mnożenia jednostek** $\mathbf{i}, \mathbf{j}, \mathbf{k}$. Jednostki te są oznaczane **kolejnymi trzema literami alfabetu łacińskiego**. Nie jest to przypadek — przy mnożeniu tych jednostek decydującą rolę odgrywa ich kolejność, częściowo określona przez kolejność alfabetyczną.

Przyjmujemy, że bezpośrednio po $\mathbf{i}$ następuje $\mathbf{j}$, a bezpośrednio po $\mathbf{j}$ następuje $\mathbf{k}$. Ponadto, dla naszych celów przyjmijmy, że bezpośrednio po $\mathbf{k}$ następuje $\mathbf{i}$. Zefiniowaliśmy **quasi-alfabetyczną kolejność**; w przeciwieństwie do „zwykłej" kolejności alfabetycznej, każda jednostka ma jedną następującą bezpośrednio po niej.

$$\ldots \mathbf{ijkijkijkijkijkijkijkijk} \ldots$$

Jest oczywiste, że w podobny sposób możemy określić **odwrotną kolejność quasi-alfabetyczną**:

$$\ldots \mathbf{kjikjikjikjikjikjikjikji} \ldots$$

Pokażemy teraz, jak powyższe rozważania mają się do **reguł mnożenia jednostek** w kwaternionach. Zauważmy, że iloczyn dwóch jednostek jest jednej z następujących postaci:

1. **Dwie kolejne w sensie kolejności quasi-alfabetycznej jednostki.** Są to iloczyny $\mathbf{ij}$, $\mathbf{jk}$ oraz $\mathbf{ki}$. W każdym z tych przypadków wynikiem będzie jednostka następująca bezpośrednio po drugim czynniku. Mówiąc inaczej, wynikiem będzie jednostka, która nie występowała w tym iloczynie. Na tej zasadzie mamy więc: $\mathbf{ij} = \mathbf{k}$, $\mathbf{jk} = \mathbf{i}$ oraz $\mathbf{ki} = \mathbf{j}$.

2. **Dwie kolejne w sensie odwrotnej kolejności quasi-alfabetycznej jednostki.** Są to iloczyny $\mathbf{ji}$, $\mathbf{kj}$ oraz $\mathbf{ik}$. W każdym z tych przypadków wynikiem będzie jednostka bezpośrednio poprzedzająca pierwszy czynnik, ale ze znakiem minus. Mówiąc inaczej, wynikiem będzie -1 razy jednostka, która nie występowała w tym iloczynie. Na tej zasadzie mamy więc: $\mathbf{ji} = -\mathbf{k}$, $\mathbf{kj} = -\mathbf{i}$ oraz $\mathbf{ik} = -\mathbf{j}$.

3. **Dwie identyczne jednostki.** Są to iloczyny $\mathbf{ii} = \mathbf{i}^2$, $\mathbf{jj} = \mathbf{j}^2$ oraz $\mathbf{kk} = \mathbf{k}^2$. Każdy z tych iloczynów jest równy -1. Mamy więc: $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$.

Określone powyżej reguły nazywamy regułami mnożenia. Żeby pomnożyć dwa dowolne kwaterniony, mnożymy każdy składnik pierwszego przez każdy składnik drugiego i dodajemy wyniki — jak w przypadku mnożenia wielomianów. Następnie, korzystając z reguł mnożenia zamieniamy wyrażenia w rodzaju $2\mathbf{ji}$, $-\mathbf{k}^2$, czy $5\mathbf{ki}$ na prostsze wyrażenia — w tym przypadku byłyby to odpowiednio: $-2\mathbf{k}$, 1, $5\mathbf{j}$. Następnie porządkujemy sumę doprowadzając ją do postaci $\xi = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$, gdzie $a, b, c, d \in \mathbb{R}$.

Przykład 2.4. $(3 + \mathbf{i} - \mathbf{j} + 2\mathbf{k})(1 - \mathbf{i} + 3\mathbf{j} - 2\mathbf{k}) = 3(1 - \mathbf{i} + 3\mathbf{j} - 2\mathbf{k}) + \mathbf{i}(1 - \mathbf{i} + 3\mathbf{j} - 2\mathbf{k}) - \mathbf{j}(1 - \mathbf{i} + 3\mathbf{j} - 2\mathbf{k}) + 2\mathbf{k}(1 - \mathbf{i} + 3\mathbf{j} - 2\mathbf{k}) = 3 - 3\mathbf{i} + 9\mathbf{j} - 6\mathbf{k} + \mathbf{i} - \mathbf{i}^2 + 3\mathbf{ij} - 2\mathbf{ik} - \mathbf{j} + \mathbf{ji} - 3\mathbf{j}^2 + 2\mathbf{jk} + 2\mathbf{k} - 2\mathbf{ki} + 6\mathbf{kj} - 4\mathbf{k}^2 = 3 - 3\mathbf{i} + 9\mathbf{j} - 6\mathbf{k} + \mathbf{i} + 1 + 3\mathbf{k} + 2\mathbf{j} - \mathbf{j} - \mathbf{k} + 3 + 2\mathbf{i} + 2\mathbf{k} - 2\mathbf{j} - 6\mathbf{i} + 4 = 11 - 6\mathbf{i} + 8\mathbf{j} - 2\mathbf{k}$

Przykład 2.5. $(\mathbf{i}+\mathbf{j})(1+\mathbf{k}) = \mathbf{i}(1+\mathbf{k})+\mathbf{j}(1+\mathbf{k}) = \mathbf{i}+\mathbf{ik}+\mathbf{j}+\mathbf{jk} = \mathbf{i}-\mathbf{j}+\mathbf{j}+\mathbf{i} = 2\mathbf{i}$
$(1 + \mathbf{k})(\mathbf{i} + \mathbf{j}) = \mathbf{i} + \mathbf{j} + \mathbf{k}(\mathbf{i} + \mathbf{j}) = \mathbf{i} + \mathbf{j} + \mathbf{ki} + \mathbf{kj} = \mathbf{i} + \mathbf{j} + \mathbf{j} - \mathbf{i} = 2\mathbf{j}$
$2\mathbf{i} = 0 + 2\mathbf{i} + 0\mathbf{j} + 0\mathbf{k}$
$2\mathbf{j} = 0 + 0\mathbf{i} + 2\mathbf{j} + 0\mathbf{k}$
Kwaterniony $2\mathbf{i}$ oraz $2\mathbf{j}$ różnią się współczynnikami przy jednostce $\mathbf{i}$ (jak również przy $\mathbf{j}$), dlatego nie są równe.
$(\mathbf{i} + \mathbf{j})(1 + \mathbf{k}) \neq (1 + \mathbf{k})(\mathbf{i} + \mathbf{j})$

Wniosek 2.6. *Mnożenie kwaternionów nie jest przemienne.*

Uwaga 2.7. Każda liczba rzeczywista x jest kwaternionem: $x = x+0\mathbf{i}+0\mathbf{j}+0\mathbf{k}$.
Każda liczba zespolona z jest kwaternionem: $z = a + b\mathbf{i} = a + b\mathbf{i} + 0\mathbf{j} + 0\mathbf{k}$.
$\mathbb{R} \subseteq \mathbb{C} \subseteq \mathbb{H}$

Definicja 2.8. Kwaternion $\xi = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$, którego wszystkie współczynniki a, b, c, d są liczbami całkowitymi nazywamy **kwaternionem o współczynnikach całkowitych**. Zbiór wszystkich kwaternionów o współczynnikach całkowitych oznaczamy symbolem $\mathbb{H}(\mathbb{Z})$.

Oznaczenie 2.9. Niech $p \in \mathbb{P}$. Zbiór wszystkich kwaternionów całkowitych, których wszystkie współczynniki są podzielne przez p oznaczamy symbolem $p\mathbb{H}(\mathbb{Z})$.

Definicja 2.10. Kwaternion $\xi = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$, którego wszystkie współczynniki a, b, c, d są liczbami wymiernymi nazywamy **kwaternionem o współczynnikach wymiernych**. Zbiór wszystkich kwaternionów o współczynnikach wymiernych oznaczamy symbolem $\mathbb{H}(\mathbb{Q})$.

Uwaga 2.11. Natychmiast z definicji wynikają dosyć oczywiste inkluzje: $\mathbb{Z} \subseteq \mathbb{H}(\mathbb{Z})$, $\mathbb{Q} \subseteq \mathbb{H}(\mathbb{Q})$ oraz $\mathbb{H}(\mathbb{Z}) \subseteq \mathbb{H}(\mathbb{Q}) \subseteq \mathbb{H}$.

3. Sprzężenie i wartość bezwzględna kwaternionu

Definicja 3.1. **Sprzężeniem kwaternionu** $\xi = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ nazywamy kwaternion $\xi^* := a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}$. Kwaternion ξ^* nazywamy kwaternionem sprzężonym z ξ.

Uwaga 3.2. Jeżeli $z = a + b\mathbf{i}$, to $z^* = a - b\mathbf{i} - 0\mathbf{j} - 0\mathbf{k} = a - b\mathbf{i} = \overline{z}$. Definicja sprzężenia dla kwaternionów jest zatem uogólnieniem definicji sprzężenia liczby zespolonej. W związku z tym, sprzężenie kwaternionu ξ będziemy również oznaczać symbolem $\overline{\xi}$.

Definicja 3.3. **Wartością bezwzględną kwaternionu** $\xi = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ nazywamy liczbę rzeczywistą $||\xi|| := \sqrt{a^2 + b^2 + c^2 + d^2}$.

Uwaga 3.4. Jeżeli $x \in \mathbb{R}$, to $x = x + 0\mathbf{i} + 0\mathbf{j} + 0\mathbf{k}$, a więc $||x|| = \sqrt{x^2 + 3 \cdot 0^2} = \sqrt{x^2} = |x|$.
Jeżeli $z \in \mathbb{C}$, czyli $z = a + b\mathbf{i}$, to $z = a + b\mathbf{i} + 0\mathbf{j} + 0\mathbf{k}$, a zatem $||z|| = \sqrt{a^2 + b^2 + 0^2 + 0^2} = |z|$.
Wynika stąd, że definicja wartości bezwzględnej kwaternionu jest uogólnieniem definicji wartości bezwzględnej liczby rzeczywistej i zespolonej. W związku wartość bezwzględną kwaternionu ξ będziemy oznaczać symbolem $|\xi|$.

Uwaga 3.5. Zbiór wszystkich kwaternionów postaci $x + y\mathbf{i} + z\mathbf{j} + 0\mathbf{k}$ możemy utożsamiać ze zbiorem wszystkich uporządkowanych trójek (x, y, z) o współrzędnych rzeczywistych, a więc również z **przestrzenią trójwymiarową**. $|x + y\mathbf{i} + z\mathbf{j}| = \sqrt{x^2 + y^2 + z^2}$ jest odległością punktu (x, y, z) od początku układu współrzędnych.

Twierdzenie 3.6. *Dla każdego kwaternionu ξ prawdziwa jest równość:*

$$\xi\overline{\xi} = \overline{\xi}\xi = |\xi|^2$$

Dowód. Niech $\xi = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$; $a, b, c, d \in \mathbb{R}$.
$\overline{\xi} = a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}$
$\xi\overline{\xi} = (a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k})(a-b\mathbf{i}-c\mathbf{j}-d\mathbf{k}) = a^2 - ab\mathbf{i} - ac\mathbf{j} - ad\mathbf{k} + ab\mathbf{i} - b^2\mathbf{i}^2 - bc\mathbf{ij} - bd\mathbf{ik} + ac\mathbf{j} - bc\mathbf{ji} - c^2\mathbf{j}^2 - cd\mathbf{jk} + ad\mathbf{k} - bd\mathbf{ki} - cd\mathbf{kj} - d^2\mathbf{k}^2 = a^2 - ab\mathbf{i} - ac\mathbf{j} - ad\mathbf{k} + ab\mathbf{i} + b^2 - bc\mathbf{k} + bd\mathbf{j} + ac\mathbf{j} + bc\mathbf{k} + c^2 - cd\mathbf{i} + ad\mathbf{k} - bd\mathbf{j} + cd\mathbf{i} + d^2 = a^2 + b^2 + c^2 + d^2$
$\overline{\xi}\xi = (a-b\mathbf{i}-c\mathbf{j}-d\mathbf{k})(a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}) = a^2 + ab\mathbf{i} + ac\mathbf{j} + ad\mathbf{k} - ab\mathbf{i} - b^2\mathbf{i}^2 - bc\mathbf{ij} - bd\mathbf{ik} - ac\mathbf{j} - bc\mathbf{ji} - c^2\mathbf{j}^2 - cd\mathbf{jk} - ad\mathbf{k} - bd\mathbf{ki} - cd\mathbf{kj} - d^2\mathbf{k}^2 = a^2 + ab\mathbf{i} + ac\mathbf{j} + ad\mathbf{k} - ab\mathbf{i} + b^2 - bc\mathbf{k} + bd\mathbf{j} - ac\mathbf{j} + bc\mathbf{k} + c^2 - cd\mathbf{i} - ad\mathbf{k} - bd\mathbf{j} + cd\mathbf{i} + d^2 = a^2 + b^2 + c^2 + d^2$
$|\xi|^2 = (\sqrt{a^2 + b^2 + c^2 + d^2})^2 = a^2 + b^2 + c^2 + d^2$ □

Twierdzenie 3.7. *Dla dowolnych kwaternionów ξ, ξ' prawdziwa jest równość:*

$$\overline{\xi \cdot \xi'} = \overline{\xi'} \cdot \overline{\xi}$$

Dowód. Niech $\xi = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k};\ a, b, c, d \in \mathbb{R}$.
$\xi' = a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k};\ a', b', c', d' \in \mathbb{R}$
$\xi\xi' = (a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})(a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k}) = aa' + ab'\mathbf{i} + ac'\mathbf{j} + ad'\mathbf{k} + ba'\mathbf{i} + bb'\mathbf{i}^2 + bc'\mathbf{ij} + bd'\mathbf{ik} + ca'\mathbf{j} + cb'\mathbf{ji} + cc'\mathbf{j}^2 + cd'\mathbf{jk} + da'\mathbf{k} + db'\mathbf{ki} + dc'\mathbf{kj} + dd'\mathbf{k}^2 = aa' + ab'\mathbf{i} + ac'\mathbf{j} + ad'\mathbf{k} + ba'\mathbf{i} - bb' + bc'\mathbf{k} - bd'\mathbf{j} + ca'\mathbf{j} - cb'\mathbf{k} - cc' + cd'\mathbf{i} + da'\mathbf{k} + db'\mathbf{j} - dc'\mathbf{i} - dd' = (aa' - bb' - cc' - dd') + (ab' + ba' + cd' - dc')\mathbf{i} + (ac' - bd' + ca' + db')\mathbf{j} + (ad' + bc' - cb' + da')\mathbf{k}$
$\overline{\xi \cdot \xi'} = (aa' - bb' - cc' - dd') + (-ab' - ba' - cd' + dc')\mathbf{i} + (-ac' + bd' - ca' - db')\mathbf{j} + (-ad' - bc' + cb' - da')\mathbf{k}$
$\overline{\xi'} = a' - b'\mathbf{i} - c'\mathbf{j} - d'\mathbf{k}$
$\overline{\xi} = a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}$
$\overline{\xi'} \cdot \overline{\xi} = (a' - b'\mathbf{i} - c'\mathbf{j} - d'\mathbf{k})(a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}) = aa' - a'b\mathbf{i} - a'c\mathbf{j} - a'd\mathbf{k} - b'a\mathbf{i} + b'b\mathbf{i}^2 + b'c\mathbf{ij} + b'd\mathbf{ik} - c'a\mathbf{j} + c'b\mathbf{ji} + c'c\mathbf{j}^2 + c'd\mathbf{jk} - d'a\mathbf{k} + d'b\mathbf{ki} + d'c\mathbf{kj} + d'd\mathbf{k}^2 = aa' - ba'\mathbf{i} - ca'\mathbf{j} - da'\mathbf{k} - ab'\mathbf{i} - bb' + cb'\mathbf{k} - db'\mathbf{j} - ac'\mathbf{j} - bc'\mathbf{k} - cc' + dc'\mathbf{i} - ad'\mathbf{k} + bd'\mathbf{j} - cd'\mathbf{i} - dd' = (aa' - bb' - cc' - dd') + (-ab' - ba' - cd' + dc')\mathbf{i} + (-ac' + bd' - ca' - db')\mathbf{j} + (-ad' - bc' + cb' - da')\mathbf{k}$
$\overline{\xi \cdot \xi'} = \overline{\xi'} \cdot \overline{\xi}$ □

Wniosek 3.8. *Dla dowolnych kwaterniotów ξ, ξ' prawdziwa jest równość:*

$$|\xi\xi'|^2 = |\xi|^2|\xi'|^2$$

Dowód. $|\xi\xi'|^2 = \xi\xi'\overline{\xi \cdot \xi'} = \xi\xi'\overline{\xi'} \cdot \overline{\xi} = \xi|\xi'|^2\overline{\xi} = |\xi'|^2\xi\overline{\xi} = |\xi'|^2|\xi|^2 = |\xi|^2|\xi'|^2$ □

4. Tożsamość Eulera

Sformułujemy teraz i udowodnimy jedną z ważniejszych tożsamości w teorii liczb; mianowicie, **tożsamość Eulera**.

Twierdzenie 4.1 (Tożsamość Eulera)**.** *Dla dowolnych $a, b, c, d, a', b', c', d' \in \mathbb{Z}$ następująca równość jest prawdziwa:* $(a^2+b^2+c^2+d^2)(a'^2+b'^2+c'^2+d'^2) = (aa'+bb'+cc'+dd')^2+(ab'-ba'-cd'+dc')^2+(ac'+bd'-ca'-db')^2+(ad'-bc'+cb'-da')^2$

Dowód. Niech:
$\xi = a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}$
$\xi' = a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k}$
$|\xi|^2|\xi'|^2 = (a^2 + b^2 + c^2 + d^2)(a'^2 + b'^2 + c'^2 + d'^2)$
$\xi\xi' = (a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k})(a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k}) = aa' + ab'\mathbf{i} + ac'\mathbf{j} + ad'\mathbf{k} - ba'\mathbf{i} - bb'\mathbf{i}^2 - bc'\mathbf{ij} - bd'\mathbf{ik} - ca'\mathbf{j} - cb'\mathbf{ji} - cc'\mathbf{j}^2 - cd'\mathbf{jk} - da'\mathbf{k} - db'\mathbf{ki} - dc'\mathbf{kj} - dd'\mathbf{k}^2 = aa' + ab'\mathbf{i} + ac'\mathbf{j} + ad'\mathbf{k} - ba'\mathbf{i} + bb' - bc'\mathbf{k} + bd'\mathbf{j} - ca'\mathbf{j} + cb'\mathbf{k} + cc' - cd'\mathbf{i} - da'\mathbf{k} - db'\mathbf{j} + dc'\mathbf{i} + dd' = (aa' + bb' + cc' + dd') + (ab' - ba' - cd' + dc')\mathbf{i} + (ac' + bd' - ca' - db')\mathbf{j} + (ad' - bc' + cb' - da')\mathbf{k}$
$|\xi\xi'|^2 = (aa' + bb' + cc' + dd')^2 + (ab' - ba' - cd' + dc')^2 + (ac' + bd' - ca' - db')^2 + (ad' - bc' + cb' - da')^2$
Ale $|\xi|^2|\xi'|^2 = |\xi\xi'|^2$, czyli
$(a^2 + b^2 + c^2 + d^2)(a'^2 + b'^2 + c'^2 + d'^2) = (aa' + bb' + cc' + dd')^2 + (ab' - ba' - cd' + dc')^2 + (ac' + bd' - ca' - db')^2 + (ad' - bc' + cb' - da')^2$ □

Z tożsamości Eulera wynika natychmiast niezwykle istotny wniosek.

Wniosek 4.2. *Iloczyn sum czterech kwadratów jest sumą czterech kwadratów.*

Kolejny wniosek odegra znaczącą rolę w dowodzie twierdzenia Lagrange'a.

Wniosek 4.3. *Twierdzenie Lagrange'a jest równoważne następującemu twierdzeniu:* ***Każda liczba pierwsza jest sumą czterech kwadratów liczb całkowitych.***

Dowód. Implikacja ($\Rightarrow$) jest oczywista. Udowodnimy implikację odwrotną. Niech $m \in \mathbb{N}$. Rozważmy trzy możliwości:

1. $m = 1$
   Wtedy $m = 1^2 + 0^2 + 0^2 + 0^2$.

2. $m \in \mathbb{P}$
   Wtedy m jest sumą czterech kwadratów z założenia.

3. m jest liczbą złożoną.
   $m = p_1^{\alpha_1} \dots p_n^{\alpha_n};\ p_1, \dots, p_n \in \mathbb{P};\ \alpha_1, \dots, \alpha_n \in \mathbb{N}$
   Z założenia:
   $p_1 = a_1^2 + b_1^2 + c_1^2 + d_1^2;\ a_1, b_1, c_1, d_1 \in \mathbb{Z}$
   $\vdots$
   $p_n = a_n^2 + b_n^2 + c_n^2 + d_n^2;\ a_n, b_n, c_n, d_n \in \mathbb{Z}$
   Zatem:
   $m = (a_1^2 + b_1^2 + c_1^2 + d_1^2)^{\alpha_1} \dots (a_n^2 + b_n^2 + c_n^2 + d_n^2)^{\alpha_n}$
   Ale iloczyn sum czterech kwadratów jest sumą czterech kwadratów. Wynika stąd, że m jest sumą czterech kwadratów.

□

5. Pierścienie

Pierścienie są jednymi z podstawowych obiektów w algebrze. Oprócz definicji podamy także kilka ich podstawowych własności, które okażą się przydane na naszej drodze do udowodnienia twierdzenia Lagrange'a. Zanim jednak będziemy w stanie podać definicję pierścienia, musimy zdefiniować nieco prostszy obiekt noszący nazwę **grupy**.

Definicja 5.1. Zbiór G z działaniem $\star$ nazywamy **grupą**, jeśli spełnione są następujące warunki:

1. $\forall a, b, c \in G\Big((a \star b) \star c = a \star (b \star c)\Big)$ (łączność)
2. $\exists e \in G \forall a \in G(e \star a = a \star e = a)$ — taki element e nazywamy elementem neutralnym
3. $\forall a \in G \exists b \in G(a \star b = b \star a = e)$ — taki element b nazywamy elementem odwrotnym do elementu a.

Definicja 5.2. Grupę G z działaniem $\star$ nazywamy **grupą abelową**, jeśli $\forall a, b \in G(a \star b = b \star a)$.

Symbolem działania niekoniecznie musi być $\star$. Najczęściej działanie oznaczamy symbolem $+$ lub $\cdot$. W pierwszym przypadku mówimy, że działanie jest zapisane **addytywnie** — element neutralny nazywamy wtedy **zerem** i oznaczamy symbolem 0. Zamiast mówić o elemencie odwrotnym mówimy wówczas o **elemencie przeciwnym**. W drugim przypadku mówimy, że działanie jest zapisane **multiplikatywnie** — element neutralny nazywamy wtedy **jedynką** i oznaczamy symbolem 1.

Twierdzenie 5.3. *Niech G będzie grupą.*

1. *Element neutralny grupy G jest unikalny.*
2. *Dla każdego $a \in G$ element odwrotny b do elementu a jest jednoznacznie określony. Oznaczamy go symbolem a^{-1} lub symbolem $-a$ jeśli działanie jest zapisane addytywnie.*
3. $\forall a \in G\Big((a^{-1})^{-1} = a\Big)$
4. $\forall a, b \in G\Big((ab)^{-1} = b^{-1}a^{-1}\Big)$

Dowód. Dowodzimy kolejno odpowiednich punktów twierdzenia:

1. Jeżeli e, e' są elementami neutralnymi grupy G, to $e = ee' = e'$.
2. Jeśli $ab = ba = e$ oraz $ab' = b'a = e$, to $b' = b'e = b'(ab) = (b'a)b = eb = b$.
3. Z definicji mamy $aa^{-1} = a^{-1}a = e$, zatem elementem odwrotnym do a^{-1} jest a.
4. $(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aea^{-1} = aa^{-1} = e$
   $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e$

□

Definicja 5.4. Mówimy, że niepusty podzbiór H grupy G jest **podgrupą** w G, jeżeli $\forall c, d \in H(cd^{-1} \in H)$.

Twierdzenie 5.5. *Niech H będzie podgrupą grupy G z działaniem $\cdot$.*

1. *Element neutralny e grupy G należy do H.*
2. $\forall c, d \in H(cd \in H)$
3. *Zbiór H z działaniem $\cdot|_{H\times H}$ jest grupą.*

Dowód. Dowodzimy kolejno odpowiednich punktów twierdzenia:

1. $H \neq \varnothing$, zatem pewien element c zbioru G jest również elementem zbioru H. Wynika stąd, że $cc^{-1} \in H$, ale $cc^{-1} = e$, a więc $e \in H$.
2. Niech $c, d \in H$. Ponieważ $e \in H$, zatem $ed^{-1} \in H$. Ale $ed^{-1} = d^{-1}$, a więc $d^{-1} \in H$. Ponieważ dodatkowo $c \in H$, zatem $c(d^{-1})^{-1} = cd \in H$.

3. Udowodniliśmy już, że element neutralny jest elementem H oraz, że H jest domknięty ze względu na działanie $\cdot$. Ponadto wiemy już, że każdy element zbioru H ma element odwrotny w H. Ostatnim koniecznym do sprawdzenia warunkiem jest łączność — jednak oczywiste jest, że jeśli działanie jest łączne, to działanie zawężone również jest łączne.

□

Możemy teraz podać definicję **pierścienia**. Ta struktura algebraiczna odegra znaczącą rolę w dowodzie twierdzenia Lagrange'a.

Definicja 5.6. Zbiór R z działaniami $+$ i $\cdot$ nazywamy **pierścieniem**, jeśli spełnione są następujące warunki:

1. Zbiór R z działaniem $+$ jest grupą abelową; element neutralny tej grupy oznaczamy przez 0.
2. $\forall a,b,c \in R\Big(a(bc) = (ab)c\Big)$
3. $\forall a,b,c \in R\Big(a(b+c) = ab+ac \wedge (a+b)c = ac+bc\Big)$ (rozdzielność mnożenia względem dodawania).

Definicja 5.7. Pierścień R nazywamy **pierścieniem przemiennym** jeśli $\forall a,b \in R(ab = ba)$.

Definicja 5.8. Pierścień R nazywamy**pierścieniem z jedynką** jeśli $R \neq \{0\}$ oraz mnożenie ma element neutralny — który nazywamy jedynką pierścienia i oznaczamy symbolem 1.

Definicja 5.9. Pierścień z jedynką R nazywamy **pierścieniem z dzieleniem**, jeśli $\forall a \in R\backslash\{0\}\exists b \in R(ab = ba = 1)$.

Przykład 5.10. Zbiór $\mathbb{H}$ z dodawaniem i mnożeniem tworzy **pierścień z dzieleniem**. Elementem odwrotnym dla $\xi \neq 0$ jest kwaternion $\frac{\bar{\xi}}{|\xi|^2}$. Istotnie, jeśli $\xi \neq 0$, to $|\xi|^2 \neq 0$ — ze wzoru mamy $\xi \cdot \frac{\bar{\xi}}{|\xi|^2} = \frac{\xi\bar{\xi}}{|\xi|^2} = \frac{|\xi|^2}{|\xi|^2} = 1$ oraz $\frac{\bar{\xi}}{|\xi|^2} \cdot \xi = \frac{\bar{\xi}\xi}{|\xi|^2} = \frac{|\xi|^2}{|\xi|^2} = 1$. Natomiast $\mathbb{H}$ z dodawaniem i mnożeniem **nie jest pierścieniem przemiennym**, jak już się przekonaliśmy.

Przykład 5.11. Zbiór $\mathbb{H}(\mathbb{Z})$ wraz z działaniami dodawania i mnożenia tworzy **pierścień z jedynką**.

Przykład 5.12. Zbiór $\mathbb{H}(\mathbb{Q})$ z działaniami dodawania i mnożenia jest **pierścieniem z dzieleniem**.

Twierdzenie 5.13. *Niech R będzie pierścieniem.*

1. $\forall a \in R(0a = a0 = 0)$
2. $\forall a,b \in R\Big((-a)b = a(-b) = -(ab)\Big)$
3. *Jeśli R jest pierścieniem z jedynką, to* $\forall a \in R\Big((-1)a = -a\Big)$.
4. *Jeśli R jest niezerowym pierścieniem z jedynką, to* $1 \neq 0$.

Dowód. Dowodzimy kolejno odpowiednich punktów twierdzenia:

1. $0a = 0a + 0a - (0a) = (0+0)a - (0a) = 0a - (0a) = 0$
   $a0 = a0 + a0 - (a0) = a(0+0) - (a0) = a0 - (a0) = 0$
2. $(-a)b + ab = (-a+a)b = 0b = 0$
   $a(-b) + ab = a(-b+b) = a0 = 0$
3. $(-1)a = -(1a) = -a$
4. Przypuśćmy, że $1 = 0$. Wtedy dla dowolnego $a \in R$: $a = a1 = a0 = 0$, czyli R jest pierścieniem zerowym — sprzeczność.

□

Jednym z ważnych pojęć związanych z pierścieniami jest pojęcie **ideału**.

Definicja 5.14. Niech R z działaniami $+$ i $\cdot$ będzie pierścieniem. Zbiór $I \subseteq R$ nazywamy **ideałem prawostronnym pierścienia** R jeśli:

1. I z działaniem $+$ tworzy podgrupę R;
2. $\forall a \in I \forall r \in R(ar \in I)$

Jeżeli natomiast zbiór $I \subseteq R$ spełnia warunki:

1. I z dodawaniem jest podgrupą R;
2. $\forall a \in I \forall r \in R(ra \in I)$

to I nazywamy **lewostronnym ideałem pierścienia** R.
Dodatkowo, jeśli $I \neq R$, to ideał I nazywamy **właściwym**.

Uwaga 5.15. Jest jasne, że w przypadku pierścieni przemiennych rozróżnienie ideałów prawostronnych i lewostronnych nie ma sensu. Jeżeli podzbiór I pierścienia przemiennego spełnia warunki definicji ideału prawostronnego (lewostronnego), to spełnia również warunki ideału lewostronnego (prawostronnego). Taki zbiór I nazywamy krótko **ideałem**.

6. Ciała $\mathbb{Z}_p$

Definicja 6.1. Zbiór F z działaniami $+$ i $\cdot$ nazywamy **ciałem**, jeśli spełnione są następujące warunki:

1. F z działaniem $+$ jest grupą abelową
2. $F \backslash \{0\}$ z działaniem $\cdot$ jest grupą abelową
3. $\forall a, b, c \in F\Big((a+b)c = ac + bc\Big)$

Twierdzenie 6.2. *Jeżeli F jest ciałem, to $\forall a, b \in F(ab = 0 \Rightarrow a = 0 \vee b = 0)$.*

Dowód. Przypuśćmy, że $ab = 0$ dla $a, b \in F \backslash \{0\}$. Jednakże $b = 1 \cdot b = (a^{-1}a)b = a^{-1}(ab) = a^{-1}0 = 0$ — sprzeczność. □

Definicja 6.3. Niech p będzie liczbą pierwszą. Zbiorem $\mathbb{Z}_p$ nazywamy zbiór $\{0, 1, \ldots, p-1\}$. Dla dowolnych elementów a, b zbioru $\mathbb{Z}_p$ ich **sumą modulo** p nazywamy resztę z dzielenia sumy $a + b$ przez p; ich **iloczynem modulo** p nazywamy resztę z dzielenia iloczynu ab przez p.

Sumę i iloczyn będziemy oznaczać w taki sam sposób jak „zwykłą" sumę i iloczyn. To, czy pisząc $a + b$ mamy na myśli sumę czy sumę modulo p, gdzie $p = 2, 3, 5, 7, 11, \ldots$ będzie zawsze wynikało z kontekstu. Analogiczna uwaga odnosi się do iloczynu.

Twierdzenie 6.4. *Dla dowolnej liczby pierwszej p zbiór $\mathbb{Z}_p$ z dodawaniem modulo p i mnożeniem modulo p jest ciałem.*

Dowód. Przemienność i łączność dodawania i mnożenia są oczywiste. Elementem neutralnym dodawania jest 0, a elementem neutralnym mnożenia jest 1. Liczbą przeciwną do $a \in \mathbb{Z}_p$ jest oczywiście $-a = p-a$. Równość $a(b+c) = ab+ac$ uzasadniamy za pomocą indukcji po a: $1(b + c) = b + c = 1b + 1c$. Załóżmy, że $(a - 1)(b + c) = (a - 1)b + (a - 1)c$. Korzystając z tego założenia otrzymujemy $a(b + c) = (a - 1)(b + c) + (b + c) = (a - 1)b + (a - 1)c + b + c = (a - 1)b + b + (a - 1)c + c = ab + ac$. Na koniec pozostało nam pokazać, że każdy element $a \neq 0$ ma element odwrotny. Tutaj po raz pierwszy skorzystamy z założenia, że $p \in \mathbb{P}$. Mianowicie, jeśli $a \neq 0$ i $b \neq 0$, to iloczyn ab nie jest podzielny przez p, to znaczy $ab \neq 0$. Ustalmy $a \in \mathbb{Z}_p$ i zauważmy, że $p - 1$ iloczynów: $a1,\ a2,\ \ldots,\ a(p-1)$ musi być parami różnych — gdyby dla pewnych $b, c \in \mathbb{Z}_p\backslash\{0\}$, $b \neq c$ zachodziło $ab = ac$, to stąd $a(b - c) = 0$, gdzie $b - c \neq 0$ — sprzeczność. Zatem $p - 1$ iloczynów $a1,\ a2,\ \ldots,\ a(p-1)$ jest parami różnych, a ponieważ żaden z nich nie jest równy zeru, więc wśród tych iloczynów istnieje taki, który jest równy 1. □

7. Preludium do dowodu twierdzenia Lagrange'a

Udowodnimy teraz dwa lematy, za pomocą których będziemy mogli udowodnić twierdzenie Lagrange'a.

Lemat 7.1. $\forall p \in \mathbb{P} \exists x, y \in \mathbb{Z}_p (x^2 + y^2 + 1 = 0)$

Dowód. Dla $p = 2$ lemat jest oczywisty. Istotnie, kładąc $x = 1$ i $y = 0$ otrzmujemy $x^2 + y^2 + 1 = 1 + 0 + 1 = 0$.

Załóżmy teraz, że $p > 2$. Niech $a, b \in \mathbb{Z}_p$. Zauważmy, że $a^2 = b^2 \Leftrightarrow (a - b)(a + b) = 0 \Leftrightarrow a = b \vee a = -b$, gdzyż $\mathbb{Z}_p$ jest ciałem. Jest jasne, że $a = -a \Leftrightarrow a = 0$. Z naszych rozważań wynika, że możemy podzielić zbiór $\mathbb{Z}_p\backslash\{0\}$ na $\frac{p-1}{2}$ par postaci $\{a, b\}$, gdzie $a \neq b$ i $a^2 = b^2$. W efekcie zbiór $\{x^2\}_{x\in\mathbb{Z}_p}$ ma $\frac{p-1}{2} + 1 = \frac{p+1}{2}$ elementów. Wynika stąd, że również zbiory $\mathcal{X} = \{x^2 + 1\}_{x\in\mathbb{Z}_p}$ oraz $\mathcal{Y} = \{-y^2\}_{y\in\mathbb{Z}}$ mają $\frac{p+1}{2}$ elementów. Zbiory $\mathcal{X}$ oraz $\mathcal{Y}$ są podzbiorami p-elementowego zbioru $\mathbb{Z}_p$, a zatem nie mogą być rozłączne. Oznacza to, że dla pewnych $x, y \in \mathbb{Z}_p$ zachodzi równość $x^2 + 1 = -y^2$, czyli $x^2 + y^2 + 1 = 0$. □

Wniosek 7.2. *Dla dowolnej liczby pierwszej p istnieją takie $x, y \in \mathbb{Z}_p$, że kwaternion $\xi = 1 + x\mathbf{i} + y\mathbf{j}$ spełnia zależność $\xi\bar{\xi} = 0$.*

Dowód. Niech p będzie liczbą pierwszą.

Z lematu wynika, że istnieją takie liczby $x, y \in \mathbb{Z}_p$, że $x^2 + y^2 + 1 = 0$. Niech $\xi = 1 + x\mathbf{i} + y\mathbf{j}$. $\xi\overline{\xi} = |\xi|^2 = \left(\sqrt{1 + x^2 + y^2}\right)^2 = 0$. □

Wniosek 7.3. *Dla dowolnej liczby pierwszej p pierścień $\mathbb{H}(\mathbb{Z}_p)$ nie jest pierścieniem z dzieleniem.*

Dowód. Niech p będzie liczbą pierwszą.

Z poprzedniego wniosku wynika, że istnieją takie $x, y \in \mathbb{Z}_p$, że dla kwaternionu $\xi = 1 + x\mathbf{i} + y\mathbf{j}$ prawdziwa jest równość $\xi\overline{\xi} = 0$. Oczywiście $\xi \neq 0$, zatem jeśli pokażemy, że ξ nie ma elementu odwrotnego, to zakończymy dowód.

Przypuśćmy, że ξ ma element odwrotny ξ^{-1}. Ponieważ $\xi\overline{\xi} = 0$, zatem $\xi^{-1}\xi\overline{\xi} = 0$. Ale $\xi^{-1}\xi\overline{\xi} = 1 \cdot \overline{\xi} = \overline{\xi}$, czyli $\overline{\xi} = 0$ — sprzeczność. □

Wniosek 7.4. *Dla dowolnej liczby pierwszej p istnieją takie liczby $x, y \in \mathbb{Z}$, że $p|x^2 + y^2 + 1$.*

Dowód. Niech p będzie liczbą pierwszą.

Wiemy już, że istnieją takie liczby $x, y \in \mathbb{Z}$, że $x^2 + y^2 + 1 = 0$ w ciele $\mathbb{Z}_p$. Ale z definicji działań w $\mathbb{Z}_p$ oznacza to, że $p|x^2 + y^2 + 1$. □

Pokazaliśmy, że dla każdej liczby pierwszej p istnieje kwaternion $\eta = 1 + x\mathbf{i} + y\mathbf{j} \in \mathbb{H}(\mathbb{Z})$ (zależny od p) taki, że $p|1 + x^2 + y^2$. Określmy:

$$\mathcal{L} := \{\xi \in \mathbb{H}(\mathbb{Z}) | \xi\eta \in p\mathbb{H}(\mathbb{Z})\}.$$

Jest oczywiste, że $p\mathbb{H}(\mathbb{Z}) \subseteq \mathcal{L}$ oraz, że $\overline{\eta} \in \mathcal{L} \backslash p\mathbb{H}(\mathbb{Z})$. Ponadto $\mathcal{L}$ jest **właściwym ideałem lewostronnym** pierścienia $\mathbb{H}(\mathbb{Z})$.

Definicja 7.5. Niech $\xi \in \mathbb{H}$. **Normą** kwaternionu ξ nazywamy liczbę rzeczywistą $\mathrm{N}(\xi) := |\xi|^2$.

Lemat 7.6 (O dzieleniu kwaternionów całkowitych)**.** *Niech $x, q \in \mathbb{H}(\mathbb{Z})$, $q \neq 0$. Istnieją $y, r \in \mathbb{H}(\mathbb{Z})$ takie, że*

$$x = yq + r, \ \mathrm{N}(r) \leqslant \mathrm{N}(q).$$

Ponadto, jeśli $\mathrm{N}(r) = \mathrm{N}(q)$, to $2r = (\pm 1 \pm \mathbf{i} \pm \mathbf{j} \pm \mathbf{k})q$.

Dowód. Ustalmy $x, q \in \mathbb{H}(\mathbb{Z})$, $q \neq 0$. Ponieważ $q \neq 0$, istnieje element q^{-1} odwrotny do q w ciele $\mathbb{H}(\mathbb{Q})$. Niech $t = a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}$ będzie takim kwaternionem wymiernym, że $xq^{-1} = t$, czyli $x = tq$. Jest jasne, że istnieją liczby całkowite b_0, b_1, b_2, b_3 takie, że

$$|a_0 - b_0| \leqslant \frac{1}{2}, \ |a_1 - b_1| \leqslant \frac{1}{2}, \ |a_2 - b_2| \leqslant \frac{1}{2}, \ |a_3 - b_3| \leqslant \frac{1}{2}.$$

Określmy teraz kwaternion $y := b + 0 + b_1\mathbf{i} + b_2\mathbf{j} + b_3\mathbf{k} \in \mathbb{H}(\mathbb{Z})$. Połóżmy $r := (t - y)q = \big((a_0 - b_0) + (a_1 - b_1)\mathbf{i} + (a_2 - b_2)\mathbf{j} + (a_3 - b_3)\mathbf{k}\big)q$. Mamy $x = tq = yq + r$, a więc $r = x - yq \in \mathbb{H}(\mathbb{Z})$. Ponadto $\mathrm{N}(r) = \mathrm{N}(t - y)\mathrm{N}(q) = \big((a_0 - b_0)^2 + (a_1 - b_1)^2 + (a_2 - b_2)^2 + (a_3 - b_3)^2\big)\mathrm{N}(q) \leqslant 4 \cdot \frac{1}{4}\mathrm{N}(q) = \mathrm{N}(q)$.

Załóżmy teraz, że $\mathrm{N}(r) = \mathrm{N}(q)$. Zatem $\mathrm{N}(r) = \big((a_0-b_0)^2 + (a_1-b_1)^2 + (a_2-b_2)^2 + (a_3-b_3)^2\big)\mathrm{N}(q)$. Wynika stąd, że

$$\underbrace{(a_0-b_0)^2}_{\leqslant\frac{1}{4}} + \underbrace{(a_1-b_1)^2}_{\leqslant\frac{1}{4}} + \underbrace{(a_2-b_2)^2}_{\leqslant\frac{1}{4}} + \underbrace{(a_3-b_3)^2}_{\leqslant\frac{1}{4}} = 1.$$

Zatem $|a_0-b_0| = |a_1-b_1| = |a_2-b_2| = |a_3-b_3| = \frac{1}{2}$, czyli $r = (\pm\frac{1}{2} \pm \frac{1}{2}\mathbf{i} \pm \frac{1}{2}\mathbf{j} \pm \frac{1}{2}\mathbf{k})q$, czyli $2r = (\pm 1 \pm \mathbf{i} \pm \mathbf{j} \pm \mathbf{k})q$. □

8. Dowód twierdzenia Lagrange'a

Podamy teraz dowód twierdzenia Lagrange'a.

Twierdzenie 8.1 (Lagrange'a)**.** *Każda liczba naturalna jest sumą czterech kwadratów.*

Dowód. Z naszych rozważań wiemy już, że twierdzenie Lagrange'a jest równoważne twierdzeniu **„Każda liczba pierwsza jest sumą czterech kwadratów"**. To zdanie z kolei, jest równoważne wypowiedzi **„Dla każdej liczby pierwszej p istnieje kwaternion $q \in \mathbb{H}(\mathbb{Z})$ taki, że $p = \mathrm{N}(q)$"**. Jeżeli $p = 2$ to w roli q wystarczy wziąć kwaternion $1 + \mathbf{i}$. Niech $p > 2$. Weźmy kwaternion $q \in \mathcal{L} \setminus p\mathbb{H}(\mathbb{Z})$ o możliwie najmniejszej normie. (Ma to sens, gdyż norma każdego z kwaternionów w tym zbiorze jest liczbą naturalną bądź zerem.)

Kwaternion q można przedstawić w postaci $q = w + c_0 + c_1\mathbf{i} + c_2\mathbf{j} + c_3\mathbf{k}$, gdzie $w \in p\mathbb{H}(\mathbb{Z})$ oraz $c_0,\ c_1,\ c_2,\ c_3$ są takimi liczbami całkowitymi, że

$$-\frac{p-1}{2} \leqslant c_s \leqslant \frac{p-1}{2}$$

dla $s = 0, 1, 2, 3$.

Zauważmy, że $\mathrm{N}(q-w) \leqslant 4\frac{(p-1)^2}{4} < p^2$. $\mathcal{L}$ jest ideałem, a więc ponieważ $q, w \in \mathcal{L}$, zatem również $q - w \in \mathcal{L}$. $\mathrm{N}(q)$ jest minimalna, ponadto $1, \mathbf{i}, \mathbf{j}, \mathbf{k} \notin \mathcal{L}$, więc $1 < \mathrm{N}(q) < p^2$.

Z lematu o dzieleniu kwaternionów całkowitych z resztą wynika, że $p = yq + r$ dla pewnych $y, r \in \mathbb{H}(\mathbb{Z})$ takich, że $\mathrm{N}(r) \leqslant \mathrm{N}(q)$. $\mathcal{L}$ jest ideałem lewostronnym $\mathbb{H}(\mathbb{Z})$, a więc $r = p - yq \in \mathcal{L}$.

Rozważmy teraz dwie sytuacje.

1. $\mathrm{N}(r) < \mathrm{N}(q)$

   Ponieważ $\mathrm{N}(q)$ jest minimalna oraz każdy niezerowy element $p\mathbb{H}(\mathbb{Z})$ ma normę nie mniejszą niż p^2, zatem $r = 0$.

   Stąd otrzymujemy, że $p = yq$, więc $p^2 = \mathrm{N}(p) = \mathrm{N}(y)\mathrm{N}(q)$, co biorąc pod uwagę, że p jest liczbą pierwszą i że $1 < \mathrm{N}(q) < p^2$ pozwala nam stwierdzić, że $\mathrm{N}(q) = p$.

2. $\mathrm{N}(r) = \mathrm{N}(q)$

   Z lematu o dzieleniu kwaternionów całkowitych z resztą wynika, że $2p = (2y \pm 1 \pm \mathbf{i} \pm \mathbf{j} \pm \mathbf{k})q$. Dla pewnej liczby naturalnej n musi zachodzić $\mathrm{N}(2y \pm 1 \pm \mathbf{i} \pm \mathbf{j} \pm \mathbf{k}) = 4n$. Stąd otrzymujemy, że $4p^2 = \mathrm{N}(2p) = 4n\mathrm{N}(q)$. Wynika stąd, że $1 < \mathrm{N}(q) < p^2$, czyli — ponieważ $p \in \mathbb{P}$ — że $p = \mathrm{N}(q)$.

□

Literatura

1. *Edmund R. Puczyłowski: Kwaterniony i twierdzenie Lagrange'a o sumach kwadratów liczb całkowitych. „Delta" 2007 nr 4, s. 4-5*

2. *Grzegorz Banaszak, Wojciech Gajda: „Elementy algebry liniowej. Część I". Wydanie 1. Warszawa. WNT 2002. 83-204-2566-2*

3. *Andrzej Białynicki-Birula: „Algebra". Wydanie 4. Warszawa. PWN 2009. 978-83-01-15817-0*