Kwaterniony i twierdzenie Lagrange'a o sumach kwadratów liczb całkowitych

Edmund R. PUCZYŁOWSKI *

Pierścień to struktura algebraiczna zbudowana podobnie do liczb całkowitych: w zbiorze określone jest dodawanie i mnożenie, przy czym dodawanie jest łączne i przemienne, istnieje zero (czyli element neutralny dodawania) i każdy element ma element przeciwny, zachodzą także prawa rozdzielności
$a \cdot (b + c) = a \cdot b + a \cdot c$
i $(b + c) \cdot a = b \cdot a + c \cdot a$.

Pierścień jest łączny (jest przemienny), gdy mnożenie jest łączne (jest przemienne); jest pierścieniem z jedynką, gdy jest w nim element neutralny mnożenia; jest pierścieniem z dzieleniem, gdy każdy element niezerowy ma element odwrotny. Itd.

Wydawałoby się, że pierścienie nieprzemienne (patrz margines) to abstrakcyjne obiekty, które żyją swoim własnym życiem i mają niewiele wspólnego z zagadnieniami matematyki szkolnej. Okazuje się, co pewnie dla niejednego będzie sporym zaskoczeniem, że mogą czasami ułatwiać (jeśli się dysponuje na ich temat nawet tylko bardzo podstawową wiedzą) rozwiązanie pewnych zagadnień matematyki elementarnej. Pokażemy tutaj, jak posługując się elementarną wiedzą z teorii pierścieni nieprzemiennych, można dowieść twierdzenia Lagrange'a, które mówi, że **dowolna liczba naturalna jest sumą czterech kwadratów liczb całkowitych**.

Będziemy korzystali jedynie z podstawowych pojęć i najprostszych faktów z tej teorii. Istotną rolę odegrają pierścienie kwaternionów, które okażą się „jak skrojone" do naszych celów. Oto, co trzeba o nich wiedzieć.

Kwaterniony Hamiltona to wyrażenia postaci $q = a_0 + a_1 i + a_2 j + a_3 k$, gdzie a_i są liczbami rzeczywistymi, nazywanymi współczynnikami q, natomiast i, j, k są pewnymi symbolami. Dwa kwaterniony są równe wtedy i tylko wtedy, gdy ich odpowiednie współczynniki są równe. Kwaterniony dodaje się „po współrzędnych", czyli dodając odpowiednie współczynniki. Określa się też ich mnożenie, które wywodzi się z reguł

$$i^2 = j^2 = k^2 = -1$$
$$ij = -ji = k, \quad jk = -kj = i, \quad ki = -ik = j$$

oraz zwyczajnego mnożenia liczb rzeczywistych i ich przemienności z i, j, k.

Przykład:

$$\begin{aligned}
&(1 + 2i - 3j + 4k)(2 - i + j - 3k) = \\
&= 2 + 4i - 6j + 8k - \\
&\quad - i - 2i^2 + 3ji - 4ki + \\
&\quad + j + 2ij - 3j^2 + 4kj - \\
&\quad - 3k - 6ik + 9jk - 12k^2 = \\
&= 2 + 4i - 6j + 8k - \\
&\quad - i + 2 - 3k - 4j + \\
&\quad + j + 2k + 3 - 4i - \\
&\quad - 3k + 6j + 9i + 12 = \\
&= 19 + 8i - 3j + 4k
\end{aligned}$$

Zbiór kwaternionów z tak określonymi działaniami jest nieprzemiennym pierścieniem łącznym.

Z każdym kwaternionem $q = a_0 + a_1 i + a_2 j + a_3 k$ wiąże się jego sprzężenie $\overline{q} = a_0 - a_1 i - a_2 j - a_3 k$ oraz normę $N(q) = a_0^2 + a_1^2 + a_2^2 + a_3^2$. Łatwo sprawdza się, że zachodzi $q\overline{q} = \overline{q}q = N(q)$ oraz $\overline{q_1 \cdot q_2} = \overline{q_2} \cdot \overline{q_1}$.

Z tych zależności wynika natychmiast, że $N(q_1 q_2) = N(q_1)N(q_2)$. Rozpisując tę równość w zależności od współczynników, otrzymujemy *tożsamość Eulera*, którą w skrócie można wypowiedzieć tak: *iloczyn sumy czterech kwadratów przez sumę czterech kwadratów jest sumą czterech kwadratów.* Tożsamość ta pozwala natychmiast zredukować dowód twierdzenia Lagrange'a do wykazania, że dowolna liczba pierwsza jest sumą czterech kwadratów liczb całkowitych – zatem tym się dalej zajmiemy.

Zauważmy, że jeśli $q \neq 0$, to $N(q) \neq 0$ oraz $q\frac{\overline{q}}{N(q)} = 1$, a więc dowolny niezerowy kwaternion jest odwracalny (czyli kwaterniony Hamiltona tworzą pierścień z dzieleniem).

Nietrudno sobie wyobrazić, że analogicznie jak kwaterniony Hamiltona można budować kwaterniony o współczynnikach innych niż rzeczywiste (nawet wziętych z dowolnego pierścienia), otrzymując także pierścienie. Dalej będziemy wykorzystywali kwaterniony $H(Z)$ o współczynnikach całkowitych, $H(Q)$ – o współczynnikach wymiernych i $H(Z_p)$ – o współczynnikach z ciała reszt modulo p, gdzie p jest ustaloną liczbą pierwszą.

Ciało reszt Z_p, gdzie p jest liczbą pierwszą, to pierścień złożony z liczb $0, 1, \ldots, p-1$, w którym wynik działania określa się jako resztę z dzielenia standardowego wyniku przez p. Jest to pierścień łączny, przemienny z jedynką i z dzieleniem.

Nietrudno sprawdzić, podobnie jak dla kwaternionów Hamiltona, że $H(Q)$ jest także pierścieniem z dzieleniem i zauważyć, że $H(Z)$ nie jest pierścieniem z dzieleniem. Z następującego lematu wynika, że również $H(Z_p)$ nie jest pierścieniem z dzieleniem.

Lemat 1. *Dla dowolnej liczby pierwszej p istnieją takie $x, y \in Z_p$, że $x^2 + y^2 + 1 = 0$.*

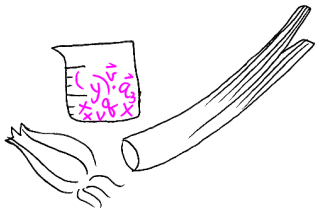
*Instytut Matematyki, Uniwersytet Warszawski

Dowód. Dla $p = 2$ lemat jest oczywisty. Załóżmy więc, że $p > 2$. Zauważmy, że dla dowolnych $a, b \in Z_p$, jest $a^2 = b^2$ wtedy i tylko wtedy, gdy zachodzi $a = \pm b$. Oczywiście, $a = -a$ wtedy i tylko wtedy, gdy $a = 0$. Zatem zbiór $Z_p \setminus \{0\}$ można rozbić na $\frac{p-1}{2}$ par, które odpowiadają różnym kwadratom elementów $Z_p \setminus \{0\}$. W efekcie zbiór $\{x^2 \mid x \in Z_p\}$ zawiera dokładnie $\frac{p+1}{2}$ elementów. Tyle samo ma też, „przesunięty" o 1, zbiór $A = \{x^2 + 1 \mid x \in Z_p\}$ i zbiór „przeciwny" $B = \{-y^2 \mid y \in Z_p\}$. Ale w Z_p jest tylko p elementów, więc $A \cap B \neq \emptyset$. Istnieją zatem takie $x, y \in Z_p$, że $x^2 + 1 = -y^2$, czyli $x^2 + y^2 + 1 = 0$.

Zauważmy, że z tego lematu wynika, iż istnieją takie $x, y \in Z_p$, że dla $q = 1 + xi + yj$, $q\overline{q} = 0$, co w szczególności pokazuje, że to q nie ma w $H(Z_p)$ odwrotności. Przechodząc do $H(Z)$, możemy na podstawie lematu powiedzieć, iż istnieją takie liczby całkowite x, y, że $p \mid 1 + x^2 + y^2$. Rozważmy związany z tymi liczbami kwaternion $t = 1 + xi + yj$ i zbiór $L = \{q \in H(Z) \mid qt \in pH(Z)\}$. Oczywiście, $pH(Z) \subseteq L$ oraz $\overline{t} \in L \setminus pH(Z)$. Zauważmy ponadto, że L jest właściwym ideałem lewostronnym $H(Z)$ (tzn. $L \neq H(Z)$ oraz dla dowolnych $a, b \in L$ również $a + b \in L$ i dla dowolnego $q \in H(Z)$, $qa \in L$).

aX to zbiór złożony z elementów X przemnożonych przez a

Wykażemy teraz, że, podobnie jak liczby całkowite, kwaterniony $H(Z)$ można dzielić z resztą.



Lemat 2. *Dla dowolnych $x, q \in H(Z)$, jeśli $q \neq 0$, to istnieją takie $y, r \in H(Z)$, że $x = yq + r$, przy czym $N(r) \leqslant N(q)$. Jeśli $N(r) = N(q)$, to*

$$2r = (\pm 1 \pm i \pm j \pm k)q.$$

Dowód. Ponieważ $q \neq 0$ i $H(Q)$ jest pierścieniem z dzieleniem, więc istnieje takie $t = a_0 + a_1 i + a_2 j + a_3 k \in H(Q)$, że $xq^{-1} = t$, czyli $x = tq$. Niech b_i, dla $0 \leqslant i \leqslant 3$, będą takimi liczbami całkowitymi, że $\mid a_i - b_i \mid \leqslant \frac{1}{2}$ oraz

$$y = b_0 + b_1 i + b_2 j + b_3 k$$

i

$$r = (t - y)q = ((a_0 - b_0) + (a_1 - b_1)i + (a_2 - b_2)j + (a_3 - b_3)k)q.$$

Oczywiście, $x = yq + r$. Ponieważ $x, yq \in H(Z)$, więc również $r = x - yq \in H(Z)$. Teraz

$$\begin{aligned} N(r) =& N(t - y)N(q) = \\ =& ((a_0 - b_0)^2 + (a_1 - b_1)^2 + (a_2 - b_2)^2 + (a_3 - b_3)^2)N(q) \leqslant \\ \leqslant& (4 \cdot \tfrac{1}{4})N(q) = N(q) \end{aligned}$$

i $N(q)$ jest równe $N(r)$ wtedy i tylko wtedy, gdy wszystkie różnice $a_i - b_i$ są równe $\pm\frac{1}{2}$, a więc gdy $2r = (\pm 1 \pm i \pm j \pm k)q$.

Możemy stąd uzyskać prosty dowód twierdzenia Lagrange'a. W tym celu wystarczy wykazać, że $p = N(q)$ dla pewnego $q \in H(Z)$. Ponieważ dla $p = 2$ jest to oczywiste, zakładamy, że $p > 2$. Wybierzmy w L kwaternion $q \notin pH(Z)$ o możliwie najmniejszej normie. Możemy go przedstawić w postaci

$$q = w + c_0 + c_1 i + c_2 j + c_3 k,$$

gdzie $w \in pH(Z)$ oraz c_i są takimi liczbami całkowitymi, że

$$-\frac{p-1}{2} \leqslant c_i \leqslant \frac{p-1}{2}.$$

Teraz $N(q - w) \leqslant 4\frac{(p-1)^2}{4} < p^2$ i $q - w \in L$. Z minimalności $N(q)$ wynika więc, że $N(q) < p^2$. Oczywiście, $N(q) = \overline{q}q \in L$. Ponieważ $L \neq H(Z)$, więc $1 \notin L$ i, w szczególności, $N(q) \neq 1$. Z Lematu 2 otrzymujemy, że $p = yq + r$ dla pewnych $y, r \in H(Z)$, przy czym $N(r) \leqslant N(q)$. Ponieważ L jest ideałem lewostronnym $H(Z)$, więc $r = p - yq \in L$. Zatem jeśli $N(r) < N(q)$, to z minimalności $N(q)$ oraz z tego, że dla $0 \neq a \in pH(z)$ jest $N(a) \geqslant p^2$, wynika, że $r = 0$, czyli $p = yq$ i $p^2 = N(p) = N(y)N(q)$. Stąd, z faktu, że p jest liczbą pierwszą oraz z tego, że $1 < N(q) < p^2$ wynika, iż $p = N(q)$. Załóżmy więc, że $N(q) = N(r)$. Wówczas, na podstawie Lematu 2, mamy $2p = (2y \pm 1 \pm i \pm j \pm k)q$. Zauważmy, że $N(2y \pm 1 \pm i \pm j \pm k) = 4n$ dla pewnej liczby naturalnej n. W efekcie $4p^2 = N(2p) = 4nN(q)$. Ponieważ $1 < N(q) < p^2$, więc $p = N(q)$ i twierdzenie Lagrange'a jest udowodnione.