Geometria w algebrze?

Jerzy KONARSKI, Warszawa

Znane są liczne zastosowania algebry w geometrii. Na przykład, algebry liniowej używa się do opisu powierzchni drugiego stopnia, teorię ciał można zastosować przy konstrukcjach geometrycznych. Tutaj podamy (na odwrót) przykład użycia metod geometrycznych do dowodu pewnych twierdzeń z algebry, a ściślej, z teorii liczb. Pojęciem geometrycznym, które odegra w dowodzie istotną rolę, będzie pojęcie kraty. Przez $\mathbf{R}^n$ będziemy oznaczali n-wymiarową rzeczywistą przestrzeń liniową.

Definicja. Kratą n-wymiarową (w skrócie kratą) w przestrzeni $\mathbf{R}^n$ nazywamy podgrupę w grupie $(\mathbf{R}^n, +)$ generowaną przez dowolny n-elementowy podzbiór liniowo niezależny w $\mathbf{R}^n$.

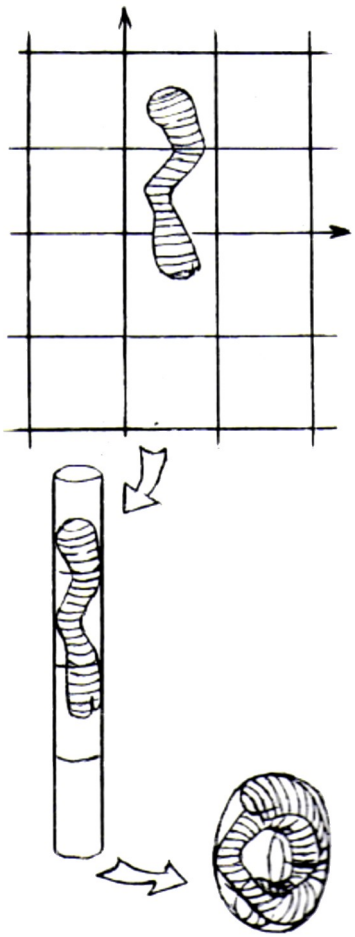
Niech $e_1, e_2, \ldots, e_n$ będzie liniowo niezależnym podzbiorem w $\mathbf{R}^n$. Wtedy krata L generowana przez ten podzbiór składa się ze wszystkich wektorów postaci $\sum_{i=1}^n a_i e_i$, gdzie a_i są liczbami całkowitymi.

Obszarem fundamentalnym kraty L będziemy nazywać zbiór $F = \{\sum_{i=1}^n a_i e_i : \ a_i \in \mathbf{R}, \ a_i \in [0,1)\}$. Oczywiście, obszar fundamentalny nie jest jednoznacznie wyznaczony przez kratę, a tylko przez jej układ generatorów.

Uwaga. Każdy wektor przestrzeni $\mathbf{R}^n$ leży w dokładnie jednym ze zbiorów postaci $F + l = \{f + l; \ f \in F\}$, dla pewnego $l \in L$.

(Dla dowodu wystarczy przedstawić wektor w postaci $\sum_{i=1}^n \alpha_i e_i$, gdzie $\alpha_i \in \mathbf{R}$, i wyłączyć z α_i część całkowitą.)

Oznaczmy przez T n-wymiarowy torus, czyli produkt $S^1 \times \ldots \times S^1$ i rozpatrzmy przekształcenie $\Phi : \mathbf{R}^n \to T$ zadane wzorem $\Phi\left(\sum_{i=1}^n a_i e_i\right) = (e^{2\pi i a_1}, \ldots, e^{2\pi i a_n})$. Odwzorowuje ono $\mathbf{R}^n$ na T i, jak łatwo sprawdzić, dwa wektory z $\mathbf{R}^n$ mają ten sam obraz w T wtedy i tylko wtedy, gdy różnią się o wektor z kraty L. Mówimy, że T jest przestrzenią ilorazową $\mathbf{R}^n/L$. Oznaczmy przez φ obcięcie Φ do zbioru fundamentalnego F, $\varphi = \Phi|_F$. Zauważmy, że φ jest bijekcją: jest różnowartościowe, ponieważ w F nie ma wektorów różniących się o niezerowy element kraty i odwzorowuje F na T na mocy Uwagi.



Za pomocą przekształcenia φ możemy zdefiniować pojęcie objętości dla podzbiorów torusa. Mianowicie, jeśli X jest podzbiorem T, to określamy $\mathrm{vol}_T(X) = \mathrm{vol}(\varphi^{-1}(X))$ (przy założeniu, że $\varphi^{-1}(X) \subset \mathbf{R}^n$ jest takim zbiorem, który ma zwykłą objętość $\mathrm{vol}(\varphi^{-1}(X))$ w $\mathbf{R}^n$).

Lemat. Niech $Y \subset \mathbf{R}^n$ będzie zbiorem ograniczonym i takim, że $\mathrm{vol}(Y)$ istnieje. Jeśli $\mathrm{vol}_T(\Phi(Y)) \neq \mathrm{vol}(Y)$, to $\Phi|_Y$ nie jest przekształceniem różnowartościowym.

Dowód. Skoro Y jest zbiorem ograniczonym, to można go zapisać jako skończoną sumę $Y = \bigcup Y_l$, gdzie $Y_l = Y \cap (F + l)$. Niech $X_l = Y_l - l$ (tzn. X_l jest „przesuniętym do F" zbiorem Y_l) i niech $Z_l = \Phi(X_l) = \Phi(Y_l)$. Gdyby $\Phi|_Y$ było różnowartościowe, to dla $i \neq j$ mielibyśmy $X_i \cap X_j = \emptyset$, ale wtedy $\mathrm{vol}(Y) = \sum \mathrm{vol}(Y_l) = \sum \mathrm{vol}(X_l) = \sum \mathrm{vol}_T(Z_l) = \mathrm{vol}_T(\Phi(Y))$.

Twierdzenie Minkowskiego. Niech L będzie kratą n-wymiarową w $\mathbf{R}^n$ z obszarem fundamentalnym F i niech $X \subset \mathbf{R}^n$ będzie zbiorem wypukłym ograniczonym i symetrycznym względem $0 \in \mathbf{R}^n$. Jeśli $\mathrm{vol}(X) > 2^n \mathrm{vol}(F)$, to X zawiera różny od 0 punkt kraty L.

Dowód. Niech L' oznacza podwojoną kratę L, tzn. $L' = 2L = \{2l, \ l \in L\}$. Wtedy $F' = 2F$ jest jej obszarem fundamentalnym oraz $\mathrm{vol}(F') = 2^n \mathrm{vol}(F)$. Oznaczmy przez $\Phi' : \mathbf{R}^n \to \mathbf{R}^n/L' = T'$ przekształcenie ilorazowe. Mamy $\mathrm{vol}_{T'}(T') = \mathrm{vol}(F') = 2^n \mathrm{vol}(F)$, zatem z założenia $\mathrm{vol}(X) > \mathrm{vol}_{T'}(T')$, a więc na mocy Lematu przekształcenie $\Phi'|_X$ nie jest różnowartościowe. Oznacza to, że istnieją punkty $x_1, \ x_2 \in X$, $x_1 \neq x_2$ takie, że $x_1 - x_2 \in L'$, a więc $(x_1 - x_2)/2 \in L$. Skoro X jest symetryczny względem 0, to $-x_2 \in X$, a skoro X jest wypukły, to $(x_1 - x_2)/2 = (x_1 + (-x_2))/2 \in X$. Znaleźliśmy więc punkt $(x_1 - x_2)/2$ należący zarówno do X, jak i do kraty L, co kończy dowód.

Tyle geometrii, teraz przejdziemy do algebraicznych zastosowań twierdzenia Minkowskiego.

Twierdzenie. Każdą liczbę pierwszą postaci $4k+1$ można przedstawić jako sumę kwadratów dwóch liczb całkowitych.

Dowód. Niech $p = 4k+1$ będzie liczbą pierwszą. Wtedy grupa multyplikatywna Z_p^* ciała Z_p jest grupą cykliczną rzędu $4k$, zawiera więc pewien element u rzędu 4. W szczególności $u^2 = -1$ (w Z_p), tzn. $u^2 \equiv -1 \pmod p$, jeśli u traktować jako liczbę całkowitą. Określmy $L = \{(a,b) \in Z^2 : b \equiv ua \pmod p\}$. Jak łatwo sprawdzić, L jest dwuwymiarową kratą w $\mathbf{R}^2$ (generowaną na przykład przez wektory $w_1 = [0,p]$ i $w_2 = [1,u]$). Obszar fundamentalny F ma więc pole (objętość) $\mathrm{vol}(F) = |\det(w_1, w_2)| = p$. Jako zbiór X z twierdzenia Minkowskiego wybierzemy odpowiednie koło B o środku w 0. Jest ono zbiorem wypukłym, ograniczonym i symetrycznym względem 0, zatem pozostaje tylko warunek $\mathrm{vol}(B) > 2^2\,\mathrm{vol}(F)$, tzn. $\pi r^2 > 4p$ (gdzie r oznacza promień koła B). Wystarczy przyjąć $r = \sqrt{(3/2)p}$. Wtedy B zawiera punkt kratowy $(a,b) \neq 0$. Ponieważ $(a,b) \in B$, więc $a^2 + b^2 < r^2 = (3/2)p < 2p$. Ponieważ $(a,b) \in L$, więc $a^2 + b^2 \equiv a^2 + u^2a^2 \equiv 0 \pmod p$. Wynika stąd, że $a^2 + b^2$ musi być równe p, co kończy dowód twierdzenia.

Twierdzenie. Każdą liczbę naturalną można przedstawić jako sumę kwadratów czterech liczb całkowitych.

Dowód. Niech m będzie liczbą naturalną. Rozpatrzymy trzy przypadki.

1) $m = 1$, wtedy $m = 0^2 + 0^2 + 0^2 + 1^2$,
   $m = 2$, wtedy $m = 0^2 + 0^2 + 1^2 + 1^2$.

2) $m \neq 2$ jest liczbą pierwszą.

Lemat. Istnieją takie liczby całkowite u, v, że $u^2 + v^2 + 1 \equiv 0 \pmod m$.

Dowód lematu. Gdy u przebiega wszystkie możliwe elementy Z_m, to u^2 przyjmuje $(m+1)/2$ wartości (bo $u^2 = (-u)^2$). Analogicznie, gdy v przebiega wszystkie elementy Z_m, to $-v^2 - 1$ przyjmuje $(m+1)/2$ wartości. Ponieważ $(m+1)/2 + (m+1)/2 > m$, więc zbiory wartości funkcji u^2 i funkcji $-v^2 - 1$ nie mogą być rozłączne, a zatem istnieją takie $u, v \in Z_m$, że $u^2 = -v^2 - 1$ (w Z_m). To kończy dowód lematu.

Postąpimy teraz podobnie, jak w dowodzie twierdzenia poprzedniego. Niech $L = \{(a,b,c,d) \in Z^4;\ c \equiv ua + vb,\ d \equiv ub - va\}$. L jest kratą generowaną przez układ wektorów $w_1 = [1,0,u,-v]$, $w_2 = [1,0,m+u,-v]$, $w_3 = [0,1,v,u]$, $w_4 = [0,1,v,m+u]$, ma więc obszar fundamentalny F o objętości $\mathrm{vol}(F) = |\det(w_1, w_2, w_3, w_4)| = m^2$. Jako zbiór X weźmy teraz czterowymiarową kulę B o promieniu $r = \sqrt{1{,}9m}$ (wtedy, jak łatwo sprawdzić, $r^4 > 32m^2/\pi^2$). Mamy więc $\mathrm{vol}(B) = \pi^2 r^4/2 > 16m^2 = 2^4\,\mathrm{vol}(F)$. Z twierdzenia Minkowskiego wynika, że istnieje niezerowy punkt $(a,b,c,d) \in L \cap B$. Warunek $(a,b,c,d) \in B$ implikuje nierówność $0 < a^2 + b^2 + c^2 + d^2 \leq r^2 < 2m$; warunek $(a,b,c,d) \in L$ implikuje $a^2 + b^2 + c^2 + d^2 \equiv a^2 + b^2 + (ua + vb)^2 + (ub - va)^2 \equiv (a^2 + b^2)(u^2 + v^2 + 1) \equiv$ $\equiv 0 \pmod m$. Z tego wynika, że $a^2 + b^2 + c^2 + d^2 = m$, co kończy dowód punktu 2).

3) m jest dowolną liczbą naturalną. Wystarczy skorzystać z równości
$(a^2 + b^2 + c^2 + d^2)(A^2 + B^2 + C^2 + D^2) = (aA - bB - cC - dD)^2 +$
$+(aB + bA + cD - dC)^2 + (aC - bD + cA + dB)^2 + (aD + bC - cB + dA)^2$
i z punktów 1) i 2). Dodajmy, że równość ostatnia to multyplikatywność normy kwaternionów.

Oba podane twierdzenia o przedstawieniu liczb w postaci sumy kwadratów pochodzą od P. Fermata (połowa XVII w.). Pełny dowód pierwszego z twierdzeń podał w roku 1754 L. Euler, a drugiego – J.L. Lagrange w roku 1770. Dowody te były algebraiczne, twierdzenie H. Minkowskiego pochodzi z roku 1896. Na zakończenie warto dodać, że w teorii liczb istnieją twierdzenia, których jedyne znane dowody korzystają z twierdzenia Minkowskiego.

Przykłady takich twierdzeń można znaleźć np. w I.N. Stewart, D.O. Tall, *Algebraic Number Theory*, Chapman and Hall, London.