Teoria Galois dla bardzo niecierpliwych

Łukasz WIECHECKI

Jeśli chcesz dowiedzieć się, jak dowodzi się nieistnienia wzorów na pierwiastki wielomianów stopni od 5 w górę, a nie lubisz ślęczeć dniami i nocami nad podręcznikami do matematyki „wyższej", to ten artykuł jest dla Ciebie. Ci, którzy są „w temacie", nie będą zawiedzeni, przedstawiamy tu bowiem rozwiązanie historycznie dość wczesne (co nie znaczy głupsze), dość różniące się od tego, co przedstawiane jest w standardowych podręcznikach teorii Galois.

Rozważamy ogólne równanie n-tego stopnia

$$X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 = 0,$$

którego pierwiastkami są $X_1, \ldots, X_n$. Mamy więc

$$X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 = (X - X_1)\ldots(X - X_n),$$

z czego wynikają wzory Viète'a:

$$\begin{cases} s_1(X_1, \ldots, X_n) = \sum_{i=1}^{n} X_i = -a_{n-1} \\ s_2(X_1, \ldots, X_n) = \sum_{1\le i<j\le n} X_iX_j = a_{n-2} \\ s_3(X_1, \ldots, X_n) = \sum_{1\le i\le j\le k} X_iX_jX_k = -a_{n-3} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ s_n(X_1, \ldots, X_n) = X_1X_2\ldots X_n = (-1)^n a_0. \end{cases}$$

Rozpoczynając walkę o pierwiastki, mamy do dyspozycji liczby wymierne, współczynniki a_i, cztery działania arytmetyczne oraz operacje pierwiastkowania dowolnego stopnia. Tymi właśnie narzędziami chcemy zbudować wyrażenia na pierwiastki. Na przykład pierwiastkami wielomianu $X^2 + a_1X + a_0 = 0$ są

$$\frac{-a_1 \pm \sqrt{a_1^2 - 4a_0}}{2},$$

a wielomianu $X^3 + a_2X^2 + a_1X + a_0$

$$\sqrt[3]{-\left(\frac{q}{2}\right) + \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}} + \sqrt[3]{-\left(\frac{q}{2}\right) + \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}},$$

gdzie $p = a_1 - \frac{a^2}{3}$ i $q = a_0 - \frac{a_2a_1}{3} + 2(\frac{a_2}{3})^3$. Papieru nie starczyłoby do wypisania wzorów stopień wyżej, ale da się.

Konstruując wzory na pierwiastki wielomianu, którego współczynniki $a_0, a_1, \ldots, a_{n-1}$ są bliżej niesprecyzowanymi symbolami, operujemy faktycznie na wyrażeniach wymiernych zmiennych $a_0, a_1, \ldots, a_{n-1}$, a także tym, co powstaje z nich przez wielokrotne wykonywanie operacji pierwiastkowania (dowolnego stopnia). Chcielibyśmy, aby jedno z takich wyrażeń było pierwiastkiem wielomianu. W naszych rozważaniach współczynniki $a_0, a_1, \ldots, a_{n-1}$ zamienimy na wielomiany s_i ze wzorów Viète'a. Zauważmy, że wielomiany te są symetryczne, co oznacza, że dowolne przestawienie zmiennych X_i nie zmienia tych wielomianów, co wyraża wzór: dla dowolnej permutacji $\sigma \in S_n$ mamy

$$s_i(X_1, X_2, \ldots, X_n) = s_i(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(n)}),$$

czyli w symbolice skróconej

$$s_i = s_i^\sigma.$$

Na początku naszej drogi mamy więc do dyspozycji wyrażenia symetryczne. Przy pierwiastkowaniu symetryczność wyrażenia może jednak zmniejszyć się, tzn. zbiór permutacji, które nie zmieniają wyrażenia, może być po spierwiastkowaniu mniejszy niż przed nim. Na przykład wyrażenie $(X_1 - X_2)^2$

Permutacją na zbiorze $\{1, 2, \ldots, n\}$ nazywamy odwzorowanie wzajemnie jednoznaczne tego zbioru na siebie. Permutacje zapisuje się np. tak: $\begin{pmatrix}123456\\231546\end{pmatrix}$. W zapisie tym pod każdą liczbą na górze stoi jej obraz przy danej permutacji, czyli 1 na 2, 2 na 3 i 3 z powrotem na 1, 4 na 5, 5 z powrotem na 4. Napis $(k_1k_2\ldots k_m)$ oznacza permutację, która przeprowadza k_1 na k_2, k_2 na k_3, ..., k_{n-1} na k_n, k_n na k_1, pozostałe zaś elementy na siebie. Napis (123)(45) oznacza po prostu złożenie permutacji (123) i (45) (najpierw wykonujemy (45) a później (123)).

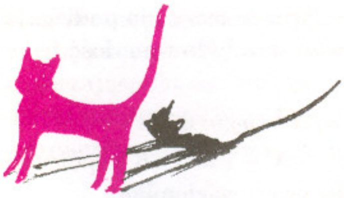
Zbiór wszystkich permutacji na zbiorze $\{1, 2, \ldots, n\}$ oznaczamy przez S_n.

Permutacje z S_n działają na wielomianach od n zmiennych. Działając permutacją σ na wielomianie $w(X_1, \ldots, X_n)$, otrzymamy nowy taki wielomian w^σ, że

$$w(X_1, \ldots, X_n) = w(X_{\sigma(1)}, \ldots, X_{\sigma(n)}),$$

czyli np.

$$(X_1^3 - 2X_2^2 + 5X_3)^{(123)} = X_2^3 - 2X_3^2 + 5X_1.$$



(tzw. delta dla wielomianu stopnia 2) jest w pełni symetryczne, ale $X_1 - X_2$ już nie. Tak więc wyobrażamy sobie, że w procesie znajdowania wzorów na pierwiastki przez kolejne pierwiastkowania (oczywiście w międzyczasie wykonujemy cztery działania arytmetyczne na arsenale wygenerowanych wyrażeń) dokonujemy niejako desymetryzacji dostępnych wyrażeń, dopóki nie wpadnie nam w łapy jeden z pierwiastków (prawda, że mało symetryczny?). Będziemy się przy tym starać, aby pozostawać cały czas w domenie funkcji wymiernych, czyli wyrażeń postaci $\frac{w(X_1,\ldots,X_n)}{v(X_1,\ldots,X_n)}$, gdzie w i v są wielomianami zmiennych $X_1, \ldots, X_n$.

Powstaje tu jednak drobny problem. Przecież pierwiastkując pewną funkcję wymierną (np. $s_1 = X_1 + X_2 + \ldots + X_n$), możemy nie otrzymać znowu funkcji wymiernej, lecz jakieś paskudztwo (nie istnieje funkcja wymierna, która byłaby równa $\sqrt{X_1 + X_2 + \ldots + X_n}$). Być może nie wychodząc poza obszar grzecznych funkcji wymiernych, nie da się otrzymać za pomocą naszych środków żadnego pierwiastka, ale da się to zrobić jakąś drogą okrężną, brodząc w błocie różnych niewymiernych paskudztw. Otóż pierwsza, dość długa i mało efektowna część dowodu polega na wykazaniu, że jeśli pierwiastek X_1 jest osiągalny, to można to zrobić, nie brudząc się w ten sposób. Pominiemy tę część dowodu i przejdziemy od razu do Grand Finale.

Rozwiązanie zadania M 934.
Niech O będzie środkiem okręgu. Załóżmy, że $P \neq O$ i $Q \neq O$ (przypadek, gdy $P = O$ lub $Q = O$ jest dość trywialny). Na czworokącie, którego wierzchołkami są M, P, Q, O można opisać okrąg, ponieważ $\angle MQO = \angle MPO = 90°$, przy czym odcinek MO jest jego średnicą o długości R. Mamy $\angle PMQ = \alpha$, więc $PQ = R \sin\alpha$ (okrąg opisany na $\triangle PQM$ ma średnicę R).

Lemat. Niech $u(X_1, \ldots, X_n)$ i $a(X_1, \ldots, X_n)$ $(n \geq 5)$ będą funkcjami wymiernymi (powiedzmy, o współczynnikach zespolonych, dla ustalenia uwagi), takimi, że $u^k = a$. Jeśli dla pewnej liczby naturalnej k funkcja a nie zmienia się przy działaniu permutacji $\sigma = (123)$ oraz $\tau = (345)$, to u również.

Dowód. Zastosujmy σ do równości $u^k = a$. Dostaniemy $\sigma(u)^k = \sigma(a) = a$, a więc $\sigma(u)^k = u^k$. Założymy, że $u \neq 0$, bo tak będzie przyjemniej. Wtedy możemy napisać $(\frac{\sigma(u)}{u})^k = 1$, czyli $\sigma(u) = \omega_\sigma u$, gdzie ω_σ jest pewnym pierwiastkiem stopnia k z 1. Działając na ostatnią równość przekształceniem σ, otrzymamy $\sigma^2(u) = \omega_\sigma^2 u$ i jeszcze raz $\sigma^3(u) = \omega_\sigma^3 u$. No dobrze, ale σ^3 jest identycznością, więc $\sigma^3(u) = u$, a stąd $\omega_\sigma^3 = 1$. Analogiczna argumentacja prowadzi do wniosku, że $\tau(u) = \omega_\tau u$, gdzie ω_τ jest pierwiastkiem stopnia k z 1 oraz $\omega_\tau^3 = 1$. Stąd $\sigma\tau(u) = \omega_\sigma\omega_\tau u$ i $\sigma^2\tau(u) = \omega_\sigma^2\omega_\tau u$. Jak łatwo obliczyć, mamy $\sigma\tau = (12345)$ i $\sigma^2\tau = (13452)$, a więc $(\sigma\tau)^5 = (\sigma^2\tau)^5 = \mathrm{id}$. Stąd wnioskujemy $(\omega_\sigma\omega_\tau)^5 = (\omega_\sigma\omega_\tau)^5 = 1$. Ponieważ zaś $\omega_\sigma = \omega_\sigma^6(\omega_\sigma\omega_\tau)^5(\omega_\sigma^2\omega_\tau)^{-5}$, więc na mocy wyprowadzonych równości $\omega_\sigma = 1$. Stąd i z $(\omega_\sigma\omega_\tau)^5 = 1$ dostajemy $\omega_\tau^5 = 1$. Równość $\omega_\tau = \omega_\tau^6\omega_\tau^{-5}$ daje więc $\omega_\tau = 1$. To kończy dowód. ■

Jeden rzut beretem do mety:

Zasadnicze Twierdzenie Tego Artykułu

Nie istnieją wzory na pierwiastki równań stopnia większego niż 4.

Dowód. Z lematu wynika, że jakkolwiek byśmy pierwiastkowali w obrębie funkcji wymiernych, zawsze otrzymywane funkcje wymierne będą niezmiennicze przy działaniu permutacji (123) i (345) (startujemy od funkcji symetrycznych). A to znaczy, że nigdy nie dobijemy się do X_1, który taki nie jest. Jest jasne, że w takim razie pozostałych pierwiastków również nie osiągniemy. Z opuszczonej pierwszej części dowodu wynika teraz teza. ■

Rozwiązanie zadania M 935.
Na czworokątach $DMSN$ i $BKSL$ można opisać okręgi, ponieważ w obu z nich jest para przeciwległych kątów prostych. Wynika stąd, że $\angle DSN = \angle DMN$ i $\angle BSL = \angle BKL$. Ponieważ $\angle BKL = \angle DMN$ (odcinki MN i KL są równoległe), więc $\angle DSN = \angle BSL$. Oznacza to, że punkty D, S, B leżą na jednej prostej, czyli $S \in BD$.

Metoda dowodu tu przedstawiona ma swoje zady i walety. Z jednej strony dość szybko prowadzi do celu, z drugiej zaś nie wnikamy w niej za bardzo w strukturę algebraiczną zbioru permutacji, przez co mamy raczej zamkniętą drogę do rozmaitych uogólnień. Można się pytać, dlaczego w dowodzie lematu wzięliśmy właśnie permutacje (123) i (345) oraz dlaczego żaden tego typu trick nie przechodzi dla $n = 3$ i 4. Poza tym zwróćmy uwagę na jedną kwestię. Udowodniliśmy, że jednego ogólnego wzoru nie ma, ale może dla każdego konkretnego wielomianu, powiedzmy o współczynnikach wymiernych, istnieją inne wzory. Słowem nie udowodniliśmy, że istnieje wielomian, powiedzmy o współczynnikach wymiernych, którego pierwiastki nie dadzą się osiągnąć narzędziami: liczby wymierne, cztery działania arytmetyczne i operacje

pierwiastkowania dowolnych stopni. To jak gdyby dwie różne sprawy. W dowodzie operowaliśmy na symbolach, które z natury rzeczy nie podlegają żadnym nietrywialnym relacjom algebraicznym, wszystko było tam dość sztywne. Jeśli jednak w napisie symbolicznym

$$X^5 + a_4X^4 + a_3X^3 + a_2X^2 + a_1X + a_0 = 0$$

zastąpimy literki a_i konkretnymi liczbami, np. $X^5 - X - 1 = 0$, to współczynniki będą spełniać różne relacje, np. $a_1^2 + a_0 = 0$ (podstawowe wielomiany symetryczne s_i nie spełniają żadnych tego typu relacji – to można wykazać) i kto wie, czy przy odpowiednim manipulowaniu nie dobijemy się do pierwiastków tego jednego konkretnego wielomianu za pomocą naszych ulubionych narzędzi. Faktem jest, że akurat dla $X^n - X - 1 = 0$ $(n \geq 5)$ jest to niemożliwe (wynik z 1987 r.), ale teorię, która pozwala rozpracowywać takie przypadki, stworzył dopiero genialny Galois (1811–1832). Ale to już za długa bajka...

Rozwiązanie zadania M 936.
Niech O będzie środkiem okręgu przechodzącego przez A, B, D. Oznaczmy $\angle ACB = \gamma$, $\angle ABC = \beta$, $\angle BAC = \alpha$. Mamy $\angle ADB = 2\gamma$ (D jest środkiem odpowiedniego okręgu). Poza tym $\angle AMB = \angle ADB = \angle ANB = 2\gamma$ (wszystkie trzy kąty są oparte na tym samym łuku okręgu o środku O). Stąd $\angle MBA = 180^\circ - 2\gamma - \alpha$ oraz $\angle NAB = 180^\circ - 2\gamma - \beta$. Następnie $\angle MOA = 2\angle MBA = 360^\circ - 4\gamma - 2\alpha$ oraz $\angle NOB = 2\angle NAB = 360^\circ - 4\gamma - 2\beta$. Mamy również $\angle AOB = 360^\circ - 2\angle ADB = 360^\circ - 4\gamma$ ($\angle AOB$ oznacza tutaj kąt zawierający punkt D). Mamy więc

$$\angle MON = \angle AOB - \angle MOA - \angle NOB = (360^\circ - 4\gamma) - (360^\circ - 4\gamma - 2\alpha) - (360^\circ - 4\gamma - 2\beta) = \\ = -360^\circ + 4\gamma + 2\alpha + 2\beta = 2\gamma.$$

Ostatecznie $\angle MON = 2\gamma$. Jeśli zatem odbijemy trójkąt MNC względem prostej MN, to punkt C „wyląduje” na okręgu opisanym na $\triangle ABD$. wynika z tego, że promienie okręgów opisanych na $\triangle ADB$ i $\triangle MNC$ są równe.

Eksploracja przestrzeni kosmicznej najdonioślejszą zdobyczą XX wieku

Krzysztof ZIOŁKOWSKI

Na początku 1999 roku amerykańska telewizja CNN przeprowadziła sondaż mający wskazać, które z dziesięciu zaproponowanych wydarzeń kończącego się stulecia można uznać za najważniejsze. Prawie połowa (48%) spośród ponad 45 tys. respondentów uznała, że był to lot człowieka na Księżyc w 1969 r. Następnie wymieniono Holocaust (15%) i zrzucenie bomby atomowej na Hiroszimę (15%). Na czwartym miejscu (9%) znalazł się pierwszy lot samolotu braci Wright w 1903 r. Wyniki tej ankiety nie tylko potwierdzają powszechną na ogół opinię, że wiek XX był okresem ogromnych kontrastów, ale także wydają się ujawniać aktualność odwiecznych marzeń człowieka o wzbiciu się ponad Ziemię, symbolizowanych ciągle żywym w kulturze euroatlantyckiej mitem o Dedalu i Ikarze. Ich urzeczywistnienie jest wynikiem wysiłku wielu pokoleń, rozpoczętego u progu czasów nowożytnych niezwykłymi projektami maszyn latających Leonarda da Vinci.

W drugiej połowie XX stulecia wykrystalizowała się nowa dyscyplina współczesnego przyrodoznawstwa, łącząca dzięki wykorzystaniu technik kosmicznych różne elementy poznawcze i aplikacyjne fizyki, astronomii i nauk o Ziemi. Określa się ją zwykle mianem badań kosmicznych. Za jej początek można przyjąć wystrzelenie pierwszego sztucznego satelity Ziemi w dniu 4 października 1957 r. oraz pierwszy lot kosmiczny człowieka 12 kwietnia 1961 r. Po 40 latach od tamtych wydarzeń eksploracja przestrzeni kosmicznej jest już czymś tak naturalnym i oczywistym, że obecnie nawet nie bardzo zdajemy sobie sprawę z tego, jak wiele zawdzięczamy rozwojowi nauki i techniki w tym zakresie.

Aktywność człowieka w przestrzeni kosmicznej obejmuje obecnie cztery rodzaje działalności:
- skierowaną ku Ziemi, służącą różnym dziedzinom nauk o Ziemi oraz ich zastosowaniom w meteorologii, telekomunikacji, nawigacji, teledetekcji itp.;
- wykorzystującą unikatowe warunki przestrzeni kosmicznej (np. próżnię, stan nieważkości) do eksperymentowania w dziedzinie fizyki, chemii, biologii, medycyny itp., a także do wykonywania różnych zadań produkcyjnych;