O matematykach, co równania rozwiązywali

Łukasz WIECHECKI, Warszawa

Wszyscy dobrze wiemy, że wzorów na pierwiastki wielomianów stopnia od 5 w górę nie ma i nie będzie. Jest to fakt prawie tak dobrze znany wśród opinii publicznej jak to, że „be kwadrat minus cztery a ce". Gorzej z jego uzasadnieniem, czy chociażby jakimiś szczątkowymi intuicjami na ten temat. Na pytanie dociekliwego ucznia szkoły średniej: „Dlaczego?", można by wprawdzie palnąć: „A dlatego, że grupa permutacji na zbiorze co najmniej 5-elementowym nie jest rozwiązalna", ale odpowiedź ta nie różniłaby się w tej sytuacji zasadniczo od np. „Nie garb się", czy też „A lekcje odrobione?". Oczywiście sprawa nie jest prosta. Rozwiązanie tego problemu zajęło ludzkości kilka wieków, więc naiwnością byłoby przypuszczać, że pełny dowód można by upakować w popularnym artykule. Nie mniej jednak możliwe jest przedstawienie pewnych intuicji dających dość dobry pogląd na sprawę. Musimy jednak cofnąć się do początku, czyli do pierwszej połowy XVI w., kiedy to niejaki Tartaglia wynalazł wzory na pierwiastki równania 3 stopnia. Fizyk R.P. Feynmann, laureat Nagrody Nobla, uważał, że zdarzenie to dało pośredniowiecznej nauce potężnego kopa, neutralizując kompleks ówczesnych geometrów jakoby starożytni Grecy to były mądre ludzie, a my to ciemne cymbały. Wreszcie bowiem dokonaliśmy czegoś, co było dla nich za trudne.

Ale do rzeczy. Stwierdzenie, że nie istnieją wzory na pierwiastki równań stopni wyższych, niż 4, jest tak naprawdę nieprecyzyjne. Wzory bowiem istnieją, ale nie takie o jakich byśmy marzyli, bo w postaci szeregów. Ludzie uparli się, że do wyrażenia pierwiastków wielomianów wolno wykorzystywać tylko następujące narzędzia (algebraiczne cyrkiel i linijka): liczby wymierne, współczynniki wielomianów (nie zakładamy, że muszą być liczbami wymiernymi), cztery działania arytmetyczne $+, -, \cdot, :$ oraz operacje pierwiastkowania dowolnego stopnia $\sqrt[n]{\ }$. Nic więcej. Liczby, które można otrzymać, wykorzystując powyższe narzędzia będziemy tutaj nazywać osiągalnymi. Zwróćmy uwagę na to, że wybór ten jest w pewnym sensie dość arbitralny, w każdym razie jeśli chodzi o ostatnie narzędzie. Mówimy bowiem: jeśli mamy daną liczbę osiągalną a, to pierwiastek wielomianu $X^n - a$ jest również liczbą osiągalną. Tak więc dokonujemy arbitralnego wyróżnienia wielomianów postaci $X^n - a$. Matematyk O. Perron zaproponował, aby wielomiany $X^n - a$ zastąpić wielomianami postaci $X^n + X - a$, czyli operację zwykłego pierwiastkowania liczby osiągalnej a zastąpić operacją wyciągania pierwiastka wielomianu $X^n + X - a$. Pomysł ten nie znalazł uznania. Z punktu widzenia praktycznych obliczeń znajdywanie pierwiastka wielomianu $X^n - a$ nie różni się złożonością od znajdywania pierwiastka wielomianu $X^n + X - a$. Zresztą wzory na pierwiastki wielomianów stopni 3 i 4 mają znikomą wartość z punktu widzenia obliczeń numerycznych. Faktem jest jednak, że matematycy w XVI w. układali te wzory z myślą o zastosowaniach do problemów praktycznych. Później jednak okazało się, że nadają się do tego jak drukarka laserowa do obierania marchewki. Newton przykładowo w ogóle nie zajmował się problemem wzorów na pierwiastki, koncentrując się na tworzeniu metod numerycznych. Tak czy inaczej w drugiej połowie XVII w. problem wzorów na pierwiastki był już uważany za domenę tzw. czystej matematyki nie mającą żadnych praktycznych zastosowań.

Wróćmy jednak do wzorów na pierwiastki równań stopnia 3 i 4. Spójrzmy jak wygląda oryginalna metoda Tartaglii, który wygadał się o niej niejakiemu Cardano, ten zaś spisał, poprawił, uzupełnił i dzięki temu mamy nazwę: wzory Cardano, a nie Tartaglii. Musimy pamiętać przy tym, że w owych czasach nie było zapisu symbolicznego, równania zapisywano całymi zdaniami, po łacinie, liczby ujemne były wyklęte, nie mówiąc już o liczbach zespolonych. Rozwiązywanie równań algebraicznych przypominało więc wtedy karkołomne akrobacje cyrkowe.

Mamy dane równanie 3 stopnia

$$X^3 + aX^2 + bX + c = 0.$$

Podstawiając $x = X + \frac{a}{3}$ otrzymujemy równanie postaci $x^3 + px + q = 0$. Pożyteczny trick, o jedną literkę mniej. Teraz Tartaglia, niczym Pomysłowy Dobromir dokonuje podstawienia $x = u + v$: $\left(u^3 + v^3 + q\right) + (u + v)\,(3uv + p) = 0$. I co teraz? Cóż, zamiast jednej zmiennej x mamy teraz dwie u i v, możemy więc nałożyć na nie dodatkowy warunek. Zamiast tego jednego równania napiszemy dwa: $u^3 + v^3 = -q$ i $uv = -\frac{p}{3}$. Z obu tych równań wynika oczywiście równanie na $x = u + v$. Jeśli obliczymy z drugiego równania $v = -\frac{p}{3v}$ i wstawimy do pierwszego, to otrzymamy równanie kwadratowe na u^3:

$$\left(u^3\right)^2 + qu^3 - \left(\frac{p}{3}\right)^3 = 0.$$

Stąd np.

$$u^3 = -\left(\frac{q}{2}\right) + \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}$$

i z $v^3 = -q - u^3$ mamy

$$v^3 = -\left(\frac{q}{2}\right) - \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}.$$

Oczywiście drugie rozwiązanie powstanie, gdy zamienimy u^3 z v^3, ale to nie ma znaczenia, x będzie takie same. Możemy więc napisać schematycznie:

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

I oto nasze upragnione wzory Cardano. Dlaczego napisałem „schematycznie"? Wiadomo bowiem, że w dziedzinie zespolonej możemy wyciągać pierwiastek n-tego stopnia na n różnych sposobów, czyli każdy z napisów

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

kryje w sobie 3 różne wartości zespolone. Czyli co, w sumie x może przyjmować $3 \cdot 3 = 9$ różnych wartości? Nie, nie zapominajmy o warunku $uv = -\frac{p}{3}$: Jeśli ustalimy wartość jednego pierwiastka (czyli np. u), to v jest już automatycznie wyznaczone. Wszystkie 3 pierwiastki równania $x^3 + px + q = 0$ możemy również zapisać wzorami:

$$x_1 = \sqrt[3]{-\left(\frac{q}{2}\right) + \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}} + \sqrt[3]{-\left(\frac{q}{2}\right) + \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}},$$

$$x_2 = \zeta_3 \sqrt[3]{-\left(\frac{q}{2}\right) + \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}} + \zeta_3^2 \sqrt[3]{-\left(\frac{q}{2}\right) + \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}},$$

$$x_3 = \zeta_3^2 \sqrt[3]{-\left(\frac{q}{2}\right) + \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}} + \zeta_3 \sqrt[3]{-\left(\frac{q}{2}\right) + \sqrt{\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2}},$$

gdzie ζ_3 jest pierwiastkiem 3 stopnia z 1, czyli np. $\zeta_3 = \cos 120° + \mathrm{i} \sin 120°$. Oczywiście pod warunkiem, że pierwiastki sześcienne we wszystkich wzorach są wyciągnięte tak, by zachodził wzór $uv = -\frac{p}{3}$. Pamiętajmy, że operowanie liczbami zespolonymi w czasach Cardano sprawiało „torturę dla umysłu", więc nie było mowy o pisaniu jakichś tam ζ_3. Wszystko musiało być grzeczne i dodatnie. Wzory są wprawdzie imponujące, ale szybko okazało się, że sprawiają kłopoty. Proszę bowiem wziąć dowolny wielomian, mający trzy ładne pierwiastki rzeczywiste i obliczyć ze wzorów co wyjdzie. Oczom przerażonego Cardano, rozpatrującego równanie $x^3 = 15x + 4$ ukazał się wzór

$$4 = \sqrt[3]{2 + \sqrt{-121}} + \sqrt[3]{2 - \sqrt{-121}}.$$

No pięknie. Co gorsza, okazuje się, że liczba $\left(\frac{p}{3}\right)^3 + \left(\frac{q}{2}\right)^2$ pod pierwiastkiem kwadratowym jest ujemna dokładnie wtedy, gdy równanie ma trzy różne pierwiastki rzeczywiste. Wszystko to drastycznie zmieniło pogląd na liczby zespolone i już Bombelli (1526–1573) w swym wpływowym dziele „Algebra"

(1572) prowadzi obliczenia na liczbach zespolonych, pokazując m.in., że

$$\sqrt[3]{2+\sqrt{-121}} = 2+\sqrt{-1} \text{ i } \sqrt[3]{2-\sqrt{-121}} = 2-\sqrt{-1}.$$

Wzory na pierwiastki równań stopnia 4 zostały znalezione przez Ferrari'ego, ucznia Cardano. Nie wzbudziły one zbyt wielkiego zainteresowania, na równania patrzono wtedy raczej w sposób geometryczny, wielkości w nich występujące miały jednostki, a przecież metr^4 nie wyraża nic, więc po co się tym w ogóle zajmować. My jednak przyjrzymy się metodzie Ferrari dość dokładnie. Rozpatrujemy równanie

$$X^4 + aX^3 + bX^2 + cX + d = 0.$$

Podobnie, jak poprzednio poprzez zamianę zmiennych $x = X + \frac{a}{4}$ możemy się pozbyć członu z X^3. Rozwiązujemy więc równanie $x^4 + px^2 + qx + r = 0$. Narzuca się, by dwa pierwsze składniki uzupełnić czymś, co da pełny kwadrat: $\left(x^2 + \frac{p}{2}\right)^2 = -qx - r + \left(\frac{p}{2}\right)^2$. Marzy nam się następnie, żeby po prawej stronie stał też jakiś kwadrat. Ale nie stoi. Musimy więc drania poprawić, nie psując tego po lewej. Po lewej stronie napiszemy $\left(x^2 + \frac{p}{2} + y\right)^2$, a więc i prawą stronę musimy zmodyfikować: $-qx - r + \left(\frac{p}{2}\right)^2 + 2yx^2 + py + y^2$. Wprowadziliśmy tu zmienną y, którą możemy dowolnie kształtować, może więc przy pewnej jej wartości również po prawej stronie otrzymamy pełny kwadrat. Patrząc na to co jest przy x^2 i x dochodzimy do wniosku, że jeśli to ma być kwadrat, to musi być postaci $\left(\sqrt{2y}x - \frac{q}{2\sqrt{2y}}\right)^2$. Otrzymujemy więc równanie na y:

$$-qx - r + \left(\frac{p}{2}\right)^2 + 2yx^2 + py + y^2 = \left(\sqrt{2y}x - \frac{q}{2\sqrt{2y}}\right)^2,$$

czyli

$$-r + \left(\frac{p}{2}\right)^2 + py + y^2 = \frac{q^2}{8y}.$$

Po wyczyszczeniu mianownika otrzymujemy równanie stopnia 3 na y:

$$8y^3 + 8py^2 + \left(2p^2 - 8r\right)y - q^2 = 0,$$

które rozwiązujemy tak jak poprzednio. Otrzymaną wartość y (jest ona równa 0 tylko wtedy, gdy $q = 0$, a wtedy nasze pierwotne równanie strasznie się trywializuje) wstawiamy do równania $\left(x^2 + \frac{p}{2}\right)^2 = \left(\sqrt{2y}x - \frac{q}{2\sqrt{2y}}\right)^2$, pierwiastkujemy je i rozwiązujemy otrzymane równanie kwadratowe. Wypisanie wzoru na x zostawiamy jako znakomite ćwiczenie z kaligrafii.

Powyżej przedstawione metody rozwiązywania równań stopnia 3 i 4 są pomysłowe, ale tak naprawdę nie bardzo widać dlaczego one pracują, czy nie ma innych metod i wreszcie dlaczego nie można podobnymi triczkami rozwiązać równań wyższych stopni. Tak, tak, my już to wiemy, ale właściwie dopiero analiza tych metod, jak również metod wypracowanych w XVII w., przez Lagrange'a zaczęła zmieniać przekonanie, że wzory na pierwiastki równań stopni od 5 w górę istnieją, tylko my jesteśmy tak głupi, że nie potrafimy ich znaleźć. Wróćmy jednak jeszcze na chwilę do metod Cardano i Ferrari. Otóż w metodach tych jak gdyby lekceważymy fakt, że zazwyczaj wielomian n-tego stopnia ma n różnych pierwiastków. Mówimy więc: lepszy jeden pierwiastek w garści, niż cztery na dachu. Zauważmy jednak: to, że nic złego się nie stanie, jeśli dla dowolnego wielomianu o współczynnikach, powiedzmy, zespolonych napiszemy

$$X^n + a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \ldots + a_1X + a_0 = \\ = (X - X_1)(X - X_2)\ldots(X - X_n),$$

nie jest w gruncie rzeczy takie oczywiste. Właściwie dotykamy tutaj zasadniczego tw. algebry, które wprawdzie było uważane za oczywiste w XVIII w., ale udowodnił je w pełni dopiero Gauss w 1799 r. Nic więc dziwnego, że przez dłuższy czas na problem patrzono jak na jedno równanie

$$X^n + a_{n-1}X^{n-1} + a_{n-2}X^{n-2} + \ldots + a_1X + a_0 = 0,$$

a nie jak na układ równań od n zmiennych:

$$s_1(X_1,\ldots,X_n) = \sum_{i=1}^{n} X_i = -a_{n-1},$$

$$s_2(X_1,\ldots,X_n) = \sum_{1\le i<j\le n} X_iX_j = a_{n-2},$$

$$s_3(X_1,\ldots,X_n) = \sum_{1\le i\le j\le k} X_iX_jX_k = -a_{n-3},$$

$$\ldots$$

$$s_n(X_1,\ldots,X_n) = X_1X_2\ldots X_n = (-1)^n a_0$$

(wzory Viéte'a).

No, dobrze, ale co właściwe daje ta zamiana? Czy to nie jest czasem niepotrzebne komplikowanie?

Zanim jednak damy odpór nowej metodzie i damy się unieść fali zniechęcenia, podeliberujmy kapkę.

Zwróćmy uwagę, wzory Viéte'a pozwalają wyeliminować symbole współczynników a_i na rzecz pewnych wyrażeń, będących wielomianami wielu zmiennych (symboli szukanych pierwiastków wielomianu). Wielomiany te, jako współczynniki, są nam dane, traktujemy je jako „osiągalne". Zauważmy, że wielomiany te są symetryczne, co oznacza, że dowolne przestawienie zmiennych X_i nie zmienia tych wielomianów, czyli wzorem: dla dowolnej permutacji $\sigma \in S_n$ mamy

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

czyli w symbolice skróconej: $s_i = s_i^\sigma$. W procesie rozwiązywania równań stopnia 3 i 4 wprowadzamy nowe zmienne, znajdujemy równania (prostsze od pierwotnego) na nie, rozwiązujemy je itd. Niejako konstruujemy budynek, u którego podstaw leżą współczynniki a_i, a na szczycie znajdują się pierwiastki. A gdybyśmy tak wszystkie kroki konstrukcyjne przetłumaczyli na język pierwiastków, czyli każdą wprowadzoną zmienną i każde otrzymane równanie pomocnicze wyrazili poprzez pierwiastki $X_1,\ldots,X_n$, a zamiast współczynnikami a_i operowali wielomianami s_i? Współczynniki są funkcjami symetrycznymi od pierwiastków, więc zapewne proces rozwiązywania ukaże nam się jako coś w rodzaju stopniowej desymetryzacji dostępnego arsenału wyrażeń osiągalnych. No, dobrze dość gadaniny, zabieramy się do roboty. Pierwszym matematykiem, który wykonał analizę, którą tu przedstawimy był Lagrange (1770).

Na wstępie twierdzenie

Tw. 1: *Niech $f(X_1,\ldots,X_n)$ i $g(X_1,\ldots,X_n)$ będą wielomianami takimi, że f/g jest funkcją symetryczną, tzn. $f^\sigma/g^\sigma = f/g$ dla dowolnej permutacji $\sigma \in S_n$. Wtedy istnieją wielomiany W i V od n zmiennych takie, że $f/g = W(s_1,\ldots,s_n)/U(s_1,\ldots,s_n)$.*

Innymi słowy dowolną symetryczną funkcję wymierną możemy otrzymać wykonując cztery działania arytmetyczne na podstawowyh wielomianach symetrycznych s_i. Twierdzenie to, jakkolwiek dość intuicyjne, wymaga dowodu. Mimo to Lagrange uważał je za „évident par soi-même", czyli właściwie nie wymagające dowodu.

Z twierdzenia tego wynika, że każde symetryczne wyrażenie wymierne od $X_1,\ldots,X_n$ można wyrazić jako funkcję wymierną od współczynników a_i wielomianu. Zaczynając nasz „quest for roots" mamy więc do dyspozycji wszystkie wyrażenia symetryczne. Przy pierwiastkowaniu wyrażeń wymiernych ich symetryczność będzie się stopniowo zmniejszać aż, wraz z osiągnięciem jednego z pierwiastków np. X_1, spadnie do satysfakcjonującego nas poziomu. Do mierzenia symetryczności będą nam jednak potrzebne pewne narzędzia. Dla funkcji wymiernej $w(X_1,\ldots,X_n)$ przez w^{S_n} będziemy oznaczać zbiór wszystkich funkcji wymiernych postaci w^σ, gdzie $\sigma \in S_n$. Ponadto $St(w)$ będzie zbiorem wszystkich permutacji, które nie ruszają w. Widać mniej więcej, że $|w^{S_n}|$

jest tym większe, im mniejsze jest $|St(w)|$. Wielkości te są nawet odwrotnie proporcjonalne: $|St(w)| \cdot |w^{S_n}| = n!$. Fakt ten wraz z dowodem znalazł się w pracy Lagrange'a i był pierwszą jaskółką teorii grup, działem współczesnej algebry traktującym m.in. o strukturze algebraicznej zbioru permutacji.

Zadanie: Znaleźć $(\prod_{i<j}(X_i - X_j))^{S_n}$.

Wróćmy do wzorów Cardano. Aby je otrzymać wprowadziliśmy zmienne u i v takie, że pierwiastkami wielomianu $X^3 + aX^2 + bX + c$ są

$$X_1 = -\left(\frac{a}{3}\right) + u + v,$$
$$X_2 = -\left(\frac{a}{3}\right) + \zeta_3 u + \zeta_3^2 v,$$
$$X_3 = -\left(\frac{a}{3}\right) + \zeta_3^2 u + \zeta_3 v.$$

Układy równań liniowych to my małym palcem... Kiwając nim i pamietając, że $a = -X_1 - X_2 - X_3$ oraz $\zeta_3^2 + \zeta_3 + 1 = 0$ otrzymujemy:

$$u = \frac{1}{3}\left(X_1 + \zeta_3^2 X_2 + \zeta_3 X_3\right)$$
$$v = \frac{1}{3}\left(X_1 + \zeta_3 X_2 + \zeta_3^2 X_3\right).$$

Pamiętamy, że u^3 było pierwiastkiem równania 2 stopnia $\left(u^3\right)^2 + qu^3 - \left(\frac{p}{3}\right)^3 = 0$. Jakie permutacje z S_n zachowują u^3? Jeśli $\sigma = (123)$, to

$$\left(u^3\right)^\sigma = [\frac{1}{3}\left(X_2 + \zeta_3^2 X_3 + \zeta_3 X_1\right)]^3 = \zeta_3^3[\frac{1}{3}\left(X_1 + \zeta_3^2 X_2 + \zeta_3 X_3\right)]^3 = u^3.$$

Podobnie $\sigma^2 = \sigma \circ \sigma = (132)$ oraz permutacja identycznościowa również zachowują u^3. Łatwo jednak sprawdzić, że pozostałe permutacje zmieniają u^3. Tak więc $|St\left(u^3\right)| = 3$, a więc działając na u^3 permutacjami z S_n możemy otrzymać dokładnie $\frac{3!}{3} = 2$ funkcje wymierne. Tyle samo ile stopień równania na u^3, którego współczynnikami są wyrażenia symetryczne na pierwiastkach. A co z u? Jest ono pierwiastkiem równania 6 stopnia $u^6 + qu^3 - \left(\frac{p}{3}\right)^3 = 0$, którego współczynniki są funkcjami symetrycznymi od $X_1, \ldots, X_n$. Widać jednocześnie, że przy działaniu permutacjami na u otrzymamy 6 różnych funkcji. Wynikałoby z tego, że jeśli chcemy ułożyć równanie minimalnego stopnia o współczynnikach będących funkcjami symetrycznymi na funkcję wymierną $w(X_1, \ldots, X_n)$, to należy się spodziewać, że równanie to będzie dokładnie stopnia w^{S_n}. Tak rzeczywiście jest. Udowodnimy ten fakt, bo jest bardzo ważny. Musimy się oswoić z nową sytuacją. Zamiast liczb, symboli współczynników a_i, rozważamy funkcje od $X_1, \ldots, X_n$. Tak więc zbiór funkcji wymiernych jest teraz domeną, po której będziemy się poruszać. Będziemy więc stwierdzać np., że $2X_1 - X_2$ jest pierwiastkiem równania

$$Y^2 - (X_1 + X_2)Y + \left(2X_1^2 + 2X_2^2 - 4X_1X_2\right) = 0,$$

którego zmienną jest Y. Współczynnikami tego równania są kolejno $1, -(X_1 + X_2), \left(2X_1^2 + 2X_2^2 - 4X_1X_2\right)$.

Tw. 2: *Funkcja wymierna $w(X_1, \ldots, X_n)$ jest pierwiastkiem pewnego wielomianu Φ stopnia $|w^{S_n}|$ o współczynnikach będących symetrycznymi funkcjami wymiernymi. Jeśli wielomian o współczynnikach, będących funkcjami symetrycznymi, ma pierwiastek w, to jego stopień jest równy co najmniej $|w^{S_n}|$.*

Dowód: Niech $m = |w^{S_n}|$ i niech $\{w_1 = w, w_2 \ldots, w_m\} = w^{S_n}$. Przyjmijmy $\Phi(Y) = (Y - w_1)(Y - w_2)\ldots(Y - w_m)$. Jego pierwiastkiem jest oczywiście w, ale czy jego współczynniki są symetryczne? No to weźmy dowolną permutację $\sigma \in S_n$ i podziałajmy nią na Φ (będzie ona permutować zmienne X_i, zaś Y zostawi w spokoju) i zobaczmy, czy coś się zmieni. Jeśli nie, to znaczy, że współczynniki są symetryczne.

$$\Phi^\sigma(Y) = (Y - w_1^\sigma)(Y - w_2^\sigma)\ldots(Y - w_m^\sigma).$$

No tak, ale zbiór czynników $(Y - w_i^\sigma)$ to zbiór czynników $(Y - w_i)$ tylko trochę pomieszany. Tak więc wartość iloczynu tych czynników po podziałaniu σ nie zmieni się.

Załóżmy teraz, że $\Psi(Y)$ jest wielomianem o współczynnikach symetrycznych, którego pierwiastkiem jest w. Działając różnymi permutacjami na równanie $\Psi(w) = 0$ dostaniemy, że każdy w_i jest też pierwiastkiem Ψ (w zmieni się w w_i, a współczynniki pozostaną takie same). Tak więc jego stopień musi być co najmniej m.

Rozumowanie dość charakterystyczne dla teorii równań algebraicznych. Zauważmy, że jeśli chcemy przykładowo ułożyć ładne równanie na funkcję $X_1 + X_2$, to wystarczy wziąć

$$(Y - (X_1 + X_2))(Y - (X_1 + X_3))(Y - (X_2 + X_3))$$

i otworzyć nawiasy. Współczynniki tego wielomianu będziemy mogli (tylko na specjalne życzenie klienta) następnie wyrazić poprzez współczynniki wielomianu, którego pierwiastkami są $X_1, \ldots, X_n$.

Spójrzmy jak nasze wypracowywane w pocie czoła intuicje działają w przypadku równania 4 stopnia. Rozpatrujemy równanie

$$X^4 + aX^3 + bX^2 + cX + d = 0$$

i poprzez zamianę zmiennych $x = X + \frac{a}{4}$ dostajemy

$$x^4 + px^2 + qx + r = 0.$$

Znajdujemy następnie takie y, że

$$\left(x^2 + \frac{p}{2} + y\right)^2 = \left(\sqrt{2y}x - \frac{q}{2\sqrt{2y}}\right)^2.$$

Dążymy teraz do wyrażenia y za pomocą pierwiastków równania. Pierwiastkując to równanie otrzymujemy de facto dwa równania

$$x^2 + \frac{p}{2} + y = \sqrt{2y}x - \frac{q}{2\sqrt{2y}}$$

$$x^2 + \frac{p}{2} + y = -\left(\sqrt{2y}x - \frac{q}{2\sqrt{2y}}\right).$$

Pierwiastki pierwotnego równania pooznaczamy tak, aby x_1 i x_2 były pierwiastkami pierwszego z powyższych równań, zaś x_3 i x_4 – drugiego. Wzory Viéte'a na wyrazy wolne dają:

$$x_1x_2 = \frac{p}{2} + y + \frac{q}{2\sqrt{2y}},$$

$$x_3x_4 = \frac{p}{2} + y - \frac{q}{2\sqrt{2y}},$$

Dodając stronami oba równania dostajemy

$$x_1x_2 + x_3x_4 = p + 2y.$$

No, ale ze wzorów Viéte'a

$$p = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4,$$

czyli

$$y = -\frac{1}{2}(x_1 + x_2)(x_3 + x_4).$$

Pamiętajmy jednak, że musimy wrócić do naszego pierwotnego równania $X^4 + aX^3 + bX^2 + cX + d = 0$. Mamy jednak $x_i = X_i + \frac{a}{4}$. Wstawiając do wzoru na y i pamietając, że $a = -(X_1 + X_2 + X_3 + X_4)$ dostaniemy

$$y = \frac{1}{8}(X_1 + X_2 - X_3 - X_4)^2.$$

Pamiętamy: y było pierwiastkiem równania 3 stopnia. Liczba $|y^{S_n}|$ powinna być również równa 3. I rzeczywiście, wszystkie funkcje, które możemy otrzymać z y, to:

$$\frac{1}{8}(X_1 + X_2 - X_3 - X_4)^2,$$

$$\frac{1}{8}(X_1 + X_3 - X_2 - X_4)^2,$$

$$\frac{1}{8}(X_1 + X_4 - X_2 - X_3)^2.$$

Funkcje powyższe są właśnie pierwiastkami równania na y. Jakież to proste. Wyrażając wszystko za pomocą pierwiastków $X_1, \ldots, X_n$ możemy tak łatwo konstruować wszystkie pierwiastki równania z jednego.

Następną rzeczą, jaką robimy podczas naszej bitwy o pierwiastki równania 4 stopnia, jest obliczenie $\sqrt{2y}$ i wstawienie do jednego z dwóch równań. Mamy (i taty):

$$\sqrt{2y} = \frac{1}{2}(X_1 + X_2 - X_3 - X_4).$$

Dokonujemy dalszej desymetryzacji osiągalnych wyrażeń. $\sqrt{2y}$ ma już 6 obrazów permutacyjnych. Nie dziwota, w końcu $\sqrt{2y}$ jest pierwiastkiem równania stopnia 6. Stąd już tylko krok do pierwiastków, wystarczy rozwiązać równania kwadratowe.

Lagrange nie daje nam jednak wytchnienia i wytacza taką armatę, że głowa puchnie. Przyglądnijmy się jej jednak dokładnie, bo strzelając z niej rozwalimy mur dziubdzianiny i otworzy nam się okno na wszelakiej maści ogólne spekulacje.

Tw. 3: *Niech f i g będą funkcjami wymiernymi od zmiennych $X_1, \ldots, X_n$. Jeśli działając na f wszystkimi permutacjami nie ruszającymi g otrzymamy dokładnie m różnych funkcji, to f jest pierwiastkiem równania stopnia m, którego współczynniki są wyrażeniami wymiernymi od g i elementarnych wielomianów symetrycznych $s_1, \ldots, s_n$.*

O co tu chodzi? Wiemy z tw. 2, że równanie na f, którego współczynniki byłyby funkcjami wymiernymi od $s_1, \ldots, s_n$, ma stopień równy liczbie permutacyjnych obrazów funkcji f. No, dobrze, ale jeśli zgodzimy się na to, by we współczynnikach równania występowała również funkcja g, to może stopień tego równania dałoby się zmniejszyć. Jak się domyślamy z przebiegu dowodu tw. 2, równaniem tym jest $(Y - f_1)(Y - f_2)\ldots(Y - f_m)$, gdzie f_i są wszystkimi obrazami f przy działaniu poprzez permutacje, które nie ruszają g. Trzeba tylko dowieść, że rzeczywiście współczynniki tego wielomianu można wyrazić za pomocą $s_1, \ldots, s_n$ i g.

Wydaje się, że armata powyższa rzeczywiście jest w stanie utorować drogę do jakichś owocnych uogólnień. Możemy z jej pomocą usankcjonować następującą ogólną strategię rozwiązywania ogólnego równania stopnia n: należy znaleźć ciąg funkcji wymiernych $V_0, V_1, \ldots, V_r$ od n zmiennych $X_1, \ldots, X_n$ taki, że V_0 jest funkcją symetryczną, V_r jest jakimś pierwiastkiem np. $V_r = X_1$ oraz dla każdego $i = 1, \ldots, r$ zachodzi jeden z warunków:

1) $V_i^k = V_{i-1}$,
2) liczba obrazów funkcji V_i przy działaniu permutacjami, które nie ruszają V_{i-1}, jest mniejsza niż n.

W pierwszym przypadku V_i możemy po prostu obliczyć poprzez spierwiastkowanie V_{i-1}, w drugim zaś V_i można znaleźć, rozwiązując równanie stopnia mniejszego niż n.

Dla $n = 2$ dobry jest następujący ciąg: $V_0 = (X_1 - X_2)^2$ (toż to ta nieszczęsna delta), $V_1 = X_1 - X_2$, $V_2 = X_1$. V_0 jest symetryczna, V_1 jest pierwiastkiem V_0, zaś V_2 spełnia warunek 2 (zresztą $V_2 = \frac{1}{2}(V_1 + (X_1 + X_2))$).

Dla $n = 3$ można wziąć: V_0 =dowolna funkcja symetryczna,

$$V_1 = \left(X_1 + \zeta_3 X_2 + \zeta_3^2 X_3\right)^3, \quad V_2 = X_1 + \zeta_3 X_2 + \zeta_3^2 X_3, \quad V_3 = X_1.$$

Ponieważ V_1 przyjmuje tylko dwie wartości przy działaniu permutacjami, więc można ją obliczyć z równania kwadratowego, V_2 obliczamy z V_1 poprzez wyciągnięcie pierwiastka sześciennego, zaś V_3 jest niezmienncza ze względu na działanie permutacji, które nie ruszają V_2 (bo jedyną permutacją, która nie rusza V_2 jest identyczność).

Dla $n = 4$ wybieramy V_0 =dowolna funkcja wymierna,

$$V_1 = (X_1 + X_2)(X_3 + X_4) \quad , V_2 = X_1 + X_2, \quad V_3 = X_1.$$

Ponieważ V_1 ma tylko trzy obrazy, więc jest pierwiastkiem równania stopnia 3, V_2 ma tylko dwa obrazy przy permutacjach nie ruszających V_1, podobna historia dla V_3.

Widać więc, że twierdzenie jest rzeczywiście mocne. Czy strategia powyższa da radę równaniom wyższych stopni? Lagrange jako pierwszy zaczął wątpić w istnienie wzorów dla równań wyższych stopni. Jego heurystyczne uzasadnienia związane są z analizą jeszcze innej metody rozwiązywania równań, zaproponowanej przez Bezouta kilka lat przed pojawieniem się pracy Lagrange'a. Metoda ta polega na szukaniu za jednym zamachem wszystkich pierwiastków równania n-tego stopnia w postaci $a_0 + a_1\omega + a_2\omega^2 + \ldots + a_{n-1}\omega^{n-1}$, gdzie za ω należy podstawić kolejno wszystkie pierwiastki stopnia n z 1. Okazuje się, że metoda ta pracuje znakomicie dla równań stopni 3 i 4. Analizując tę metodę Lagrange doszedł do wniosku, że już dla równań stopnia 5 pojawiają się trudności być może nie do przezwyciężenia.

Praca Lagrange'a zaowocowała próbami udowodnienia nieistnienia nieszczęsnych wzorów. Pierwszym śmiałkiem był Paolo Ruffini, który w 1799 r. opublikował potężną dwutomową cegłę, w której, jak twierdził, znajdował się kompletny dowód. Praca Ruffiniego nie została raczej przychylnie przyjęta. 516 stron skutecznie odstraszało potencjalnych fanów jego talentu. Jednak mimo, że okazało się później, iż dowód zawiera istotne luki, to całe zdarzenie spowodowało kompletną zmianę poglądów na całą sprawę. Ludzie już niejako wiedzieli, że wzorów nie ma. W 1826 Abel, niezależnie od Ruffiniego, opublikował inny dowód, który wprawdzie również miał dziury, ale był jak najbardziej reformowalny i ubytki szybko zaplombowano. Poniżej przedstawimy szkic dowodu, który jest jak gdyby połączeniem najbardziej udanych fragmentów prac Ruffiniego i Abela.

Spójrzmy generalskim okiem na pole bitwy. Mamy 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

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

z czego wynikają wzory Viéte'a. Rozpoczynając walkę o pierwiastki mamy do dyspozycji liczby wymierne, współczynniki a_i, cztery działania arytmetyczne oraz operacje pierwiastkowania dowolnego stopnia. Zgodnie z ideologią przedstawioną wyżej symbole współczyników zamienimy na elementarne wielomiany symetryczne s_i. Na mocy tw. 1, stosując cztery działania arytmetyczne możemy otrzymać dokładnie wszystkie funkcje symetryczne od zmiennych X_i. Za każdym razem jednak, gdy wykonamy pierwiastkowanie, a następnie wygenerujemy wszystko co możliwe za pomocą czterech operacji arytmetycznych, arsenał dostępnych funkcji powiększy się. Zbiór osiągalnych funkcji będziemy powiększać i powiększać, dopóki nie wpadnie nam w łapy jeden z pierwiastków X_i. 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 pokazaniu, 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.

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 $u^p = a$. Jeśli dla pewnej liczby pierwszej p funkcja a nie zmienia się przy działaniu permutacji $\sigma = (123)$ oraz $\tau = (345)$, to u również.*

Dowód: Zastosujmy σ do równości $u^p = a$. Dostaniemy $\sigma(u)^p = \sigma(a) = a$, a więc $\sigma(u)^p = u^p$. Załóżymy, że $u \neq 0$, bo tak będzie przyjemniej. Wtedy możemy

napisać $\left(\frac{\sigma(u)}{u}\right)^p = 1$, czyli $\sigma(u) = \omega_\sigma u$, gdzie ω_σ jest pewnym pierwiastkiem stopnia p z 1. Działając na ostatnią równość poprzez 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 p 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 nie pierwiastkowali (wyciąganie pierwiastka dowolnego stopnia n można złożyć z pierwiastkowań o stopniach będących liczbami pierwszymi) 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.

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 na rozmaite uogólnienia. 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 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 1987r.), ale teorię, która pozwala rozpracowywać takie przypadki stworzył dopiero genialny Galois (1811–1832). Ale to już za długa bajka...

Literatura

Jean-Pierre Tignol – *Galois' theory of algebraic equations*,
J. Browkin – *Teoria ciał*,
A. Białynicki-Birula – *Zarys algebry*.