Scratchwork: Symmetric Polynomials

Where do symmetric polynomials come from? The starting points are almost too obvious to even mention.

Ex. Find a cubic polynomial $f(x) = x^3 \times ax^2 + bx + c$ such that $f(0) = 1$ and $f(1) = 2$, $f(2) = 3$.

These constraints leads to simultaneous equations for the number a, b, c:

$$\begin{array}{ccccccccc} & & & & & & c & = & 1 \\ 1 & + & a & + & b & + & c & = & 2 \\ 8 & + & 4a & + & 2b & + & c & = & 3 \end{array}$$

A polynomial is just a made-up device that mathematicians use to solve equations anwyay. Why might such a thing be natural? if you're a believer in the Newton Leibniz calculus, there was the Taylor series expansion from 1715 or so:

$$f(x+a) = f(x) + f'(x)a + f''(x)\frac{a^2}{2} + f'''(x)\frac{a^3}{6} \dots$$

As long as you have enough derivatives. We are going to extrapolate nearby values basic on what we know at a single point, with itzero knowledge of f.

So we have matrix equation:

$$\begin{bmatrix} 0 & 0 & 1 \\ 1 & 1 & 1 \\ 4 & 2 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ -5 \end{bmatrix}$$

We seem to be on the right track. Cramér's rule first appears in 1750 but we've likely had simultaneous equations before that. First of all there is a single equation:

$$c = 1 \quad \text{and} \quad \begin{bmatrix} 1 & 1 \\ 4 & 2 \end{bmatrix} \begin{bmatrix} b \\ c \end{bmatrix} = \begin{bmatrix} 0 \\ -6 \end{bmatrix}$$

We only have two variables. So let's just solve them:

$$a = \frac{\begin{vmatrix} 0 & 1 \\ -6 & 2 \end{vmatrix}}{\begin{vmatrix} 1 & 1 \\ 4 & 2 \end{vmatrix}} = \frac{6}{-2} = -3 \quad \text{and} \quad b = \frac{\begin{vmatrix} 1 & 0 \\ 4 & -6 \end{vmatrix}}{\begin{vmatrix} 1 & 1 \\ 4 & 2 \end{vmatrix}} = \frac{-6}{-2} = 3$$

and now like good students we should restate our answer. The polynomial should be:

$$f(x) = x^3 - 3x^2 + 3x + 1$$

Additionally, we observe that Taylor series motivates order of operations:

$$f(3) = 1 \times (3 \times 3 \times 3) - 3 \times (3 \times 3) + 3 \times (3) + 1$$

This is just a sketch of how the grade school operations could have emerged.

We can talk for a moment about the formulas of Viete.

$$(x-a)(x-b)(x-c) = x^3-(a+b+c)x^2+(ab+bc+ca)x-abc$$

Then if we have a cubic equation which is very difficult to solve, we can still get information about the average behavior of the numbers:

$$x^3-3x^2+3x+1$$

and perhaps we can find the sum of the squares of the roots:

$$a^2+b^2+c^2 = (a+b+c)^2-2\times(ab+bc+ca) = (-3)^2-2\times 3 = 3$$

These things hide in front of your face. They're almost too obvious to state.[1]

Ex. Are the roots of $f(x)$ all real numbers? (1 real) + (2 imaginary)? Find $a^4+b^4+c^4$.

Ex. Derive Taylor's formula to 4th order. $(x, y) = (0, 0)$ is a point on the lemniscate: $(x^2+y^2)^2-2(x^2-y^2) = 0$. What are some nearby points? Can we get an exact answer?[2]

[1] is there a technical term for this??

[2] Gabriel Cramér "introuction a L'Analyse des Lines Courbes Algebraiques" https://archive.org/details/bub_gb_gtKvSzJPOOAC

6/8 While that's not nearly enough motivation, let's say I have a cubic polynomial, $f(x) = x^3 + ax^2 + bx + c$. How do we distinguish between these two cases:

- $f(x) = 0$ for three numbers $x_1, x_2, x_3 \in \mathbb{R}$ (the "totally real" case)
- $f(x) = 0$ for one number $x_1 \in \mathbb{R}$ and two complex conjugate numbers $x_2, \overline{x_2} \in \mathbb{C}$.

Jumping ahead of ourselves, let's enumerate the possibilities for the Galois group:

- S_3 the group of permutations on three letters
- A_3 the group of (even) permutations in S_3
- C_3 the cyclic group on three symbols (like a wheel)
- $I = \{e\}$ the group with one element.

And just like a calculator, there are procedures for finding the information we want about any given field and any given prime number. There's even a few thousand pages of paper if you want to read them giving a few patterns in the behavior of these numbers.

- $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. Every number can be written as $x = a + b\sqrt[3]{2} + c\sqrt[3]{4}$. This is related to the equation $x^3 - 2 = 0$. This field is **not** Galois. $\frac{6}{3} = 2$ so we need a *quadratic* extension K over $\mathbb{Q}(\sqrt{2})$ so that $[K : \mathbb{Q}] = 6$.
$$x^2 + ax + b = 0$$
How do you feel about the quadratic formula if we know additionally that $a, b \in \mathbb{Q}(\sqrt[3]{2})$?
- The polynomial $x^3 - x - 1$ is called the "plastic number". It is also a *Pisot* number in that $x_1 \in \mathbb{R}$ and $|x_1| > 1$ while $|x_2|, |x_3| < 1$. How do we verify such information for ourselves? What is the Galois group of $\mathbb{Q}(x)/\mathbb{Q}$? (It's in fact, S_3.)

We should be leary, that even for such basic examples, we have to use a computer. And the entire existing literature is full of such a doubt.

Q Could we feel out the Galois group of a cubic using the averages of the coefficints, e.g. $f_n = x_1^n + x_2^n + x_3^n \in \mathbb{Z}$. Even thought we can't solve for $x_1, x_2, x_3 \in \mathbb{C}$ we could use the Viéte polynomials to get the various averages of the roots.

- $a = x_1 + x_2 + x_3$
- $b = x_1x_2 + x_2x_3 + x_3x_1$
- $c = x_1x_2x_3$

In the case of a quadratic, the sequence $f_n = x_1^n + x_2^n$ yields a kin of the Fibonacci numbers. And there's an exhaustic literature there, which nonetheless has open questions (somewhat on the deep end). So we even have a guess what the numbers are like.

Q: We have that $\overline{\mathbb{Q}(\sqrt[3]{2})} = \mathbb{R}$ (the "closure" of the set of rational numbers with respect to the absolute value $|\cdot|$ how can we best approximate numbers like $\sqrt{2}$, $\sqrt{3}$, $\sqrt[3]{5}$, π, etc.?

$$\frac{a_1 + \sqrt[3]{2}b_1 + \sqrt[3]{4}c_1}{a_2 + \sqrt[3]{2}b_2 + \sqrt[3]{4}c_2} = a + \sqrt[3]{2}b + \sqrt[3]{4}c$$

with $(a_1, b_1, c_1), (a_2, b_2, c_2) \in \mathbb{Z}^3$ and $a, b, c \in \mathbb{Q}$. Tautologically, the fractions can be written in the left way or the right way, but how do we feel about such a map?

References

[1] Artur Avila, Vincent Delecroix. **Some monoids of Pisot matrices** `arXiv:1506.03692`

6/10 Other than Galois Theory and Numerical Analysis do we have other candidates for usages of symmetric polynomials…? These arise in combinatorics and probability. Let's have probability distribution $1 = p_1 + p_2 + \cdots + p_n$. Then perhaps we could try to compute the moments:

$$\mathbb{E}[x_k] = p_1^k + \cdots + p_n^k$$

This is a symmetric polynomial. Therefore, all expectation values are symmetric in the probabilities. If we have information about the distribution, the numbers $\{1, \ldots, n\}$ start to look different. If we had a random permutation:

$$1 \mapsto (1,2,3), 2 \mapsto (1,3,2), 3 \mapsto (2,1,3), 4 \mapsto (2,3,1), \ldots$$

Then perhaps there is other symmetry. These symmetries are decidedly bland and look trivial – literally like a $\mathbf{0}$ – and yet have profound consequences.