Lecture 1-22: General polynomials; cubics and quartics

January 22, 2025

I showed last time that there is no formula in terms of radicals for the roots of the very simple polynomial $x^5 - 6x + 3$ over $\mathbb{Q}$; in stark contrast, there are *universal* formulas for the roots of any cubic or quartic polynomial over any field of characteristic not 2 or 3. Today I will show first that this must be the case on general principles and then develop the formulas.

Definition, p. 607

The general polynomial of degree n over a field F is the polynomial $p_n = (x - x_1) \cdots (x - x_n)$; its coefficients lie in the rational function field $F_n = F(x_1, \ldots, x_n)$.

Multiplying out the terms, we see that $p_n = x^n + \sum_{i=0}^{n} (-1)^i s_i(x_1, \ldots, x_n) x^{n-i}$, where s_i is the ith elementary symmetric function of the x_j, that is, the sum of all products of i distinct x_j (p. 607). We take s_0 to be the constant function 1. We should therefore regard the basefield of p_n as the subfield $F'_n = F(s_1, \ldots, s_n)$ of F_n generated by the s_i over F. The field F_n is clearly the splitting field of p_n over F'_n.

Then we have

Theorem 32, p. 609

The extension F_n is Galois over F'_n with Galois group S_n, so that it is solvable by radicals if and only if $n \leq 4$.

Indeed, as mentioned above, F_n is the splitting field of the separable polynomial p_n over F'_n, so is Galois over the latter. The Galois grou permutes the roots of p_n, so is a subgroup of S_n; but conversely any permutation of the x_i fixes p_n and all of its coefficients. so the Galois group is all of S_n. The second assertion follows from the Galois criterion, the deifnitio of solvability, and the fact from last quarter that A_5 is not solvable. As a consequence, the field F' of functions in K fixed by the action of S_n coincides with F'_n, so that every rational function of the x_i invariant under S_n is a rational function of the s_i. In fact, every polynomial in the x_i invariant under S_n is a polynomial in the x_i. Such rational functions or polynomials are called symmetric.

To solve general cubic and quartic polynomials by radicals, then, it would suffice to solve p_3 and p_4 by radicals and then plug in the coefficients of an arbitrary cubic or quartic polynomial (up to sign) for the variables x_i in the formulas for the roots. This is in effect what is done in Chapter 14 of the text; but I prefer to solve these polynomials directly (as was done long before Galois). Given a cubic equation $x^3 + ax^2 + bx + c = 0$ over a field of characteristic not 2 or 3, first substitute $x = y - \frac{a}{3}$, rewriting the polynomial in terms of y. The coefficient of y^2 drops out, replacing the original equation by the reduced cubic $y^3 + py + q = 0$ for some p, q. Next, make the change of variable $y = z + \frac{k}{z}$, where k is a constant to be specified in a moment. The equation becomes $z^3 + (3k + p)z + (3k^2 + pk)z^{-1} + k^{-3}z^{-3} + q = 0$. Two terms drop out by the choice $k = -p/3$, making the equation $z^3 + q - \frac{p^3}{27}z^{-3} = 0$.

This last equation becomes quadratic in z^3 when multiplied by z^3. Applying the quadratic formula and simplifying, we get Cardano's formula: $y = (\frac{-q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}})^{1/3} + (\frac{-q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}})^{1/3}$ (p. 632). Here the cube roots must be chosen so that their product is $\frac{-p}{3}$, so that we get only three roots by this formula. A remarkable feature of the formula is that even if all the roots are real, it often happens that this expression (or any other) for them involves complex numbers. Here radical extensions do not produce the splitting field, but rather a proper extension of it.

The quartic equation $x^4 + bx^3 + cx^2 + dx + e = 0$ takes more work to solve and its solution relies on the solution to the cubic equation. The key idea (following Wikipedia) is to rewrite the left side of its as a product $(x^2 + px + q)(x^2 + rx + s)$ for suitable r and s, thus reducing the original quartic to two quadratics. Equating coefficients on both sides to solve for p, q, r, s, we get $b = p + r, c = q + s + pr, d = ps + qr, e = qs$. Now a trick similar to the one used above for cubic equations helps us again: changing the variable $x = y - \frac{b}{4}$, we may assume that $b = 0$, whence $r = -p$. Then $c + p^2 = s + q$ and $\frac{d}{p} = s - q$ (if $p = 0$ then $d = 0$ and the original quartic equation reduces to a quadratic equation in x^2). Since $(s + q)^2 - (s - q)^2 = 4sq = 4e$, we get $(c + p^2)^2 - (\frac{d}{p})^2 = 4e$, whence if we set $P = p^2$, we get $P^3 + 2cP^2 + (c^2 - 4e)P - d^2 = 0$. This last equation is called "the" resolvent cubic (in fact any of several cubic equations could be used to solve the quartic equation).

Solving for p, setting $r = -p, 2s = c + p^2 + \frac{d}{p}, 2q = c + p^2 - \frac{d}{p}$, we get a pair of quadratic equations $x^2 + px + q = 0$ and $x^2 + rs + s = 0$; the two roots of each of them combine to produce the four roots of the quartic. The three roots of the cubic equation arise from the three ways to pair up the four roots of the quartic equation, each of which leads to a different pair of quadratic polynomials with product $x^4 + cx^2 + dx + e$. Recall also that the symmetric group S_4 is solvable precisely because its Klein four-subgroup K, consisting of the permutations $(12)(34), (13)(24)$, and $(14)(23)$ in addition to the identity, is normal. The quotient S_4/K is isomorphic to S_3. Thus it is entirely predictable from group theory alone that the solution to the quartic equation crucially involves the solution to the cubic one.

It is also quite interesting to observe that if an irreducible polynomial q of prime degree p can be solved by radicals at all, then in fact it can be so solved (in principle) pretty easily. The key fact is that the Galois group G of any such q acts transitively on its roots. It is an easy exercise to show in general that if a group acts transitively on a set S, then the orbits in S of any normal subgroup of the group are permuted by the action of the group; in particular, any two orbits of the normal subgroup have the same size. In the present situation, the group G has a nontrivial abelian normal subgroup A, which also acts transitively on the roots of q. As its order is a multiple of p it must contain the cyclic subgroup C generated by p-cycle. No subgroup strictly containing C is abelian, so we must have $A = C$.

It follows that G is a subgroup of $N(C)$, the normalizer of C in S_p, which is isomorphic to $\mathbb{Z}_p \ltimes \mathbb{Z}_p^*$, the semidirect product of $\mathbb{Z}_p$ and its automorphism group Z_p^*. The group $N(C)$ has order $p(p-1)$; it has a cyclic normal subgroup and the quotient by this group is also cyclic. In field-theoretic terms, this implies that after adjoining primitive pth and $(p-1)$st roots of 1 to the basefield of the polynomial q, one can always solve it by radicals by adjoining just one more pth root and one more $(p-1)$st root (if it can be solved by radicals at all).

In particular, if $p = 5$, there are only three possible Galois groups of irreducible quintic polynomials over $\mathbb{Q}$ that are solvable by radicals, namely $\mathbb{Z}_5$, the dihedral group D_5 of order 10, and the group $\mathbb{Z}_5 \ltimes \mathbb{Z}_5^*$ mentioned on the last slide. In the text on p. 639, an explicit purely numerical criterion is given for a quintic polynomial over $\mathbb{Q}$ to be solvable by radicals (which takes half a page to state): this holds if and only if another polynomial constructed from the coefficients of the given one has a rational root.

The very rich theory of finite Galois extensions of $\mathbb{Q}$ has no counterpart for the real field $\mathbb{R}$. There is just one proper finite extension of $\mathbb{R}$ and none at all of $\mathbb{C}$, as follows from the next result.

Fundamental Theorem of Algebra: Theorem 35, p. 616

The only finite extensions of $\mathbb{R}$ are $\mathbb{R}$ and $\mathbb{C}$. The only finite extension of $\mathbb{C}$ is $\mathbb{C}$ itself.

Proof.

Since $\mathbb{R}$ has characteristic 0, any extension of it is separable, so any finite extension is contained in a Galois extension. Given such an extension E, with Galois group G, let S be a 2-Sylow subgroup of G. This corresponds to an extension E' of $\mathbb{R}$ of odd degree. But now any polynomial $p(x)$ of odd degree is such that $p(x)$ is large and positive for x large enough and positive (or large enough and negative), and then large and negative for x large enough and negative (or large enough and positive), whence by continuity p must have a real root. Thus there are no nonlinear irreducible polynomials in $\mathbb{R}[x]$ of odd degree, whence we must have $E' = \mathbb{R}, S = G$. Passing now to a normal subgroup of S of index 2, we get a quadratic extension of $\mathbb{R}$, which must be $\mathbb{C}$ by the quadratic formula. Finally, $\mathbb{C}$ is closed under square roots, so does not admit a quadratic extension, and so no finite extension at all. □