Lecture 1-17: Solvability by radicals

January 17, 2025

As mentioned last time, one of Galois's motivations for developing his theory was determining conditions under which a formula exists for the roots of a polynomial in terms of its coefficients, using only algebraic operations and the extraction of roots. Of course the quadratic formula is the most familiar example of such a formula; centuries before Galois's time similar formulas were known for cubic and quartic polynomials. Without asking for a *universal* formula for the roots of any polynomial of degree $n \geq 5$, one can ask whether any particular polynomial admits such a formula for its roots. I will answer that question by using the Galois group of the polynomial.

More precisely, one has the following

Definition, p. 627

A nonconstant polynomial p over a field K is said to be *solvable by radicals* if there is an extension L of a splitting field S for p over K and a chain of fields $K_0 = K \subset K_1 \subset \cdots \subset K_m = L$ such that each $K_i = K_{i-1}(\alpha_i)$ for some α_i with $\beta_i = \alpha_i^{n_i} \in K_{i-1}$ for some positive integer m_i.

Clearly any expression built from the coefficients of p using only field operations and roots represents an element of such a field L. It is important for technical reasons not to insist in this definition that L be a spitting field for p over K, but only to contain such a field.

As already mentioned, I will give a criterion for a polynomial to be solvable by radicals in terms of its Galois group. To do this I need a group-theoretic definition (introduced by Galois himself).

Definition, p. 105

A group G is called *solvable* if there is a finite chain $G = G_0 \supset G_1 \supset \cdots \supset G_n = 1$ of normal subgroups of G such that the quotients G_{i-1}/G_i are abelian.

This definition makes sense for any group, but in this course I will deal only with the finite case. It is clear from the definition that any quotient H/N of a subgroup H of a solvable group G by a normal subgroup is again solvable. The main result is

Galois Criterion: Theorem 39, p. 628

A nonconstant polynomial p over a field K of characteristic 0 is solvable by radicals if and only if its Galois group G is solvable.

Proof.

Suppose first that p is solvable by radicals and let $K_0 = K \subset K_1 \subset \cdots \subset K_m = L$ be a chain of fields as in the definition. The first step is to insert a new field and reduce to the case where each K_i is the full splitting field of $x^{n_i} - \beta_i$ over K_{i-1}. Let N be the product of the integers n_i appearing in the definition of solvability by radicals and let K_0' be the splitting field of $x^N - 1$ over K. Inductively let K_i' be the spitting field of $x^{n_i} - \beta_i$ over K_{i-1}' for $i \geq 1$. Then K_i' is generated by the same element α_i that generates K_i over K_{i-1}. □

Proof.

By enlarging the fields in the chain, we may also assume that each K_i' is Galois over K: having extended K_{i-1}' by an n_ith root of β_i to get K_i', extend it further by n_ith roots of all conjugates of β_i in K (that is, other roots of the minimal polynomial of β_i over K), continuing to denote this field by K_i'. Then K_i' is the splitting field of a polynomial over K, so is Galois over K and K_{i-1}'. □

Proof.

To the ascending chain $K_0 \subset K_0' \subset \cdots \subset K_m'$ of fields the Galois correspondence attaches the descending chain $G' = G_0 \supset G_1 \supset \cdots \supset G_m = 1$ of subgroups of $G' = \mathrm{Gal}(K_m'/K)$, with each G_i normal in both G and G_{i-1} since the K_i' are Galois over K_0. The Galois group H_i of K_i' over K_{i-1}' is then the quotient group G_{i-1}/G_i. For $i = 1$ this is the Galois group of $x^N - 1$ over K for some N; this group is a subgroup of the group $\mathbb{Z}_N^*$ of multiplicative units in $\mathbb{Z}_N$, since any automorphism of a cyclotomic field sends a primitive root of 1 to some power of itself. In particular it is abelian. □

Proof.

For $i > 1$ H_i is the Galois group of a suitable product $(x^{n_i} - \gamma_1) \dots (x^{n_i} - \gamma_r)$ for various γ_j over a field with n_i distinct roots of 1. Letting α_j be an n_ith root of γ_j in K_i', we find that any automorphism of K_i' fixing K_{i-1}' fixes every n_ith root of 1 and sends each α_j to itself times such a root. It follows that H_i is abelian, being a subgroup of the product of r copies of the cyclic group $\mathbb{Z}_{n_i}$ of order n_i. Hence G' is solvable. The Galois group of S (or of p) is then a quotient of a subgroup of G, so is also solvable, as claimed. □

Proof.

Now conversely suppose that the Galois group G of a polynomial $p \in K[x]$ with splitting field S is solvable and let $G = G_0 \supset G_1 \supset \cdots \supset G_m = 1$ be a chain of normal subgroups with G_{i-1}/G_i abelian for all i. By the classification of finite abelian groups, we may insert other subgroups into this chain to arrive at another chain $G = G_0 \supset \cdots \supset G'_n = 1$ such that $H_i = G'_{i-1}/G'_i$ is cyclic for all i, say of order n_i. Corresponding to this chain we get a chain of subfields $K_0 = K \subset \cdots K_n = S$ with each K_i Galois over K_{i-1} with cyclic Galois group of order n_i. □

Proof.

Once again, it is convenient at this point to adjoin some roots of 1. Let N be the product of the n_i and let K_0' the splitting field of $x^N - 1$ over K_0. For $i \geq 1$ if K_i is the splitting field of a polynomial p_i over K_{i-1} then inductively let K_i' be the splitting field of p_i over K_{i-1}'. Any automorphism of K_i' fixing K_{i-1}' restricts to an automorphism of K_i fixing K_{i-1}, so the Galois group H_i' of K_i' over K_{i-1}' is cyclic of order dividing n_i. Now it will follow that p can be solved by radicals if we can show that any Galois extension L of degree d with cyclic Galois group G over a field K with a full set of distinct dth roots of 1 is generated by a single element α with $\alpha^d \in K$ (Proposition 36, p. 626) □

Proof.

The proof of this last assertion is a beautiful application of canonical forms of matrices. Let g be a generator of G. Then g acts on L by a K-linear transformation all of whose eigenvalues lie in K since it contains a full set of dth roots of 1. Hence g acts on L by a diagonalizable matrix. But now if $x, y \in L$ are eigenvectors of g with the same eigenvalue β, then g and G fix xy^{-1}, whence $xy^{-1} \in K$. Thus all eigenspaces of g have dimension 1 and every dth root of 1 occurs as an eigenvalue of g exactly once. Letting $\alpha \in L$ be an eigenvector of g whose eigenvalue is a primitive dth root of 1, it follows that powers of α span L over K and α^d is fixed by G, so lies in K. Hence $L = K(\alpha)$ and $\alpha^d \in K$, as desired. The proof of the Galois Criterion is at last complete. □

Continuing with this line of reasoning, we can now prove a fundamental negative result of Abel and Galois.

Theorem, p. 629

There are polynomials of degree 5 over $\mathbb{Q}$ that are not solvable by radicals.

Proof.

Note first that the splitting field of any polynomial p over any field is generated by the roots of this polynomial, which are permuted by the Galois group, so any Galois group can be naturally regarded as a subgroup of some permutation group S_n. Now I claim that an irreducible polynomial q over $\mathbb{Q}$ of prime degree p with exactly $p-2$ real roots has Galois group $G = S_p$. □

Proof.

To see this, note first that G acts transitively on the p roots of q, so its order must be a multiple of p. By Sylow's Theorem and properties of p-groups (or Cauchy's Theorem), $G \subset S_p$ has an element of order p, which must be a p-cycle c. G also contains a transposition t, corresponding to complex conjugation in the splitting field. Replacing c by a suitable power of itself, we may assume that the roots flipped by the transposition appear next to each other in the cycle, so that (labelling the roots by integers from 1 to p) we have $c = (12 \dots p), t = (12)$. □

Proof.

Conjugating t by powers of c, we get the transposition $(i, i+1)$ in G for $1 \leq i \leq p-1$. But now transpositions of adjacent indices are well known to generate the entire symmetric group S_p, so $G = S_p$: every permutation of the roots of q extends to an automorphism of its splitting field. Note that this very strong field-theoretic property was proved using only group theory. Now the polynomial $q = x^5 - 6x + 3$ is irreducible over $\mathbb{Q}$ (by Eisenstein) and has exactly three real roots (by calculus). Finally q is not solvable by radicals, by the Galois Criterion, since S_5 is not solvable (its subgroup A_5 is simple and thus not solvable). In fact, *none* of the roots of q can be expressed in terms of radicals, for if one could, then since G acts transitively on the roots of q and sends mth roots to mth roots for any m, all the roots of q could be so expressed and q could be solved by radicals. □

By the way, given a field K of characteristic $p > 0$, a Galois extension of degree p is *never* an extension by a pth root, since the polynomial $x^p - \alpha$ is never separable over such a field. Instead, using the Jordan form, one can show that any such extension of K is generated by an element β with $\beta^p - \beta = \alpha \in K$. Both this fact and the corresponding fact in characteristic 0 will be reproved later, using the cohomology of finite groups.