Math 505, 1/18

We now prove the other half of the Galois Criterion: if a polynomial p over a field K of characteristic 0 has solvable Galois group, then p is solvable by radicals. The proof has a number of parallels with the proof of its converse, but also involves an important result from last quarter that was proved in two different ways; it is this result that requires the assumption of characteristic 0. So suppose that the Galois group G of the polynomial p over the field K is solvable. Applying the Galois correspondence we see that there is a chain of fields $K = K_0 \subset K_1 \subset \cdots \subset K_n$ with each K_i cyclic (Galois with cyclic Galois group) over K_{i-1} and K_n containing the splitting field of p over K. Let d_i be the degree of K_i over K_{i-1} for $1 \le i \le n$ and let N be the product of the d_i. We now tweak our chain of fields, as we did in proving the converse result, by adding roots of 1: let K_0' be the splitting field of $x^N - 1$ over K_0 and inductively K_i' the splitting field of p_i over K_{i-1}' for $i > 0$, where K_i is the splitting field of p_i over K_{i-1}. Then any K_{i-1}'-automorphism of K_i' restricts to a K_{i-1}-automorphism of K_i and is determined by this restriction, since the roots of p_i generate K_i' over K_{i-1}'. Hence the Galois group of K_i' over K_{i-1}' is a subgroup of the Galois group $\mathbf{Z}_{n_i}$ of K_i over K_{i-1} and so in particular is cyclic of order m_i dividing n_i. Now we invoke the result from last quarter: given any field F containing a primitive mth root of 1 and a cyclic extension E of it of degree m, we must have $E = F(\alpha)$ for some α with $\alpha^m \in F$. (We proved this in two different ways, first by using the rational canonical form of a matrix and later vis the cohomology of cyclic Galois groups. Note that it fails for extensions of degree p in characteristic p, which can be generated by a root of the polynomial $x^p - x - \beta$ for some β, rather than of $x^p - \beta$.) The hypothesis is satisfied by each of our fields K_i', since K_i contains a primitive Nth root and thus also a primitive m_ith root of 1, so each K_i' is a radical extension of K_{i-1}' for $i \ge 1$; likewise K_0' is clearly a radical extension of K_0, being generated by a primitive Nth root of 1. Since K_n' contains K_n, which in turn contains the splitting field of p, we are done: p is solvable by radicals.

We don't have to confine ourselves to the basefield $\mathbf{Q}$. Let K be any field of characteristic 0 and let L be the field of rational functions in n variables $x_1, \ldots, x_n$ over K. The symmetric group S_n acts on the variables x_i by permutations and thereby on L by automorphisms, whence L is Galois over its fixed field L^{S_n}, with Galois group S_n. For $n = 3$ or 4, then, the polynomial $(x - x_1) \cdots (x - x_n)$ must be solvable by radicals over L^{S_n}. Radical formulas for its roots (in the two cases $n = 3$ or 4) amount to two *universal* formulas (analogous to the quadratic formula), one for the roots of any cubic polynomial over K, the other for any quartic polynomial. We will derive these formulas later, using only high-school algebra (as when they were first proved).

How does one go about computing Galois groups of polynomials in general and thereby deciding whether they are solvable by radicals? (This question was a major concern to the referees of Galois's original paper, which Galois could not fully address; his paper was rejected.) We look at some simple examples, which turn out to be richer and less predictable than one might expect. Take first the polynomial $x^3 - 2$ over $\mathbf{Q}$. This polynomial is irreducible and its splitting field is generated by two elements over $\mathbf{Q}$, namely the real cube root $2^{1/3}$ of 2 and a complex cube root ω of 1, so its degree over $\mathbf{Q}$ is the maximum possible one of 6, and the Galois group is the largest possible one for any cubic, namely S_3. Now look at $x^4 - 2$ over $\mathbf{Q}$. The splitting field is generated by $2^{1/4}$, the positive real fourth root of 2, and i (a primitive fourth root of 1), so has degree 8 over $\mathbf{Q}$. Any automorphism of this field permutes the four root of this polynomial; it can do so cyclically (by fixing i), or by a reflection of the square formed by these roots in the complex plane (via complex conjugation). Hence the Galois group is the dihedral one D_4 of order 8. It looks like we have a pattern here; in both cases the Galois group of the polynomial happens to coincide with the symmetry group of the regular polygon formed by the roots in the complex plane. Alas, this pattern is broken already for $x^5 - 2$; it is not difficult to check that the splitting field has degree 20 over $\mathbf{Q}$ in this case, so the Galois group is too big to be the dihedral group of order 10. Matters are even worse for the polynomials $x^8 - 2$ and $x^8 - 3$: the first of these has Galois group of order 16 but is *not* isomorphic to the dihedral group of this order, while the second has Galois group of order 32. (The discrepancy arises because 2 is "closely related" in some sense to a primitive 8th root of 1 while 3 is not.)