Galois Theory in 1500 Words

Written by Tiny Epiphany

For a long time, people wondered whether it is possible to write down something like the "quadratic formula" for cubic, quartic and quintic polynomials with integer coefficients. We now know that for cubic and quartic polynomials, this is possible. But for degree 5 polynomials and beyond, it isn't. A proof of this was scribbled down hastily by Galois the night before his duel. Galois linked together field theory and group theory in a beautiful way to answer this very question.

Galois's Approach: The Big Idea

What does writing down a "formula" for roots of a polynomial really mean? For one, we'd be writing down the roots in terms of rational numbers and a combination of +, -, x, ÷, and radicals (taking n-th roots). This is a very limited set of operations, and certainly not all real numbers can be written this way -- π, for example, can't be written this way. We say that π is not solvable in radicals.

Are the roots of polynomials with *integer* coefficients solvable in radicals? Those roots aren't just *any* real number, and certainly π is not a root of any polynomial with integer coefficients. Yet Galois showed that there are some degree-5 polynomials with roots that are *not* solvable in radicals. To see how he did this, we first need some terminology about fields, field extensions, and groups.

Fields

The set of rational numbers Q is an example of a field: a set of things you can add, subtract, multiply and divide. We can "extend" Q into bigger fields by adjoining things to it. For example, L=Q(√2) -- pronounced "Q adjoined root two" -- is defined to be the smallest field that contains both Q and √2, and is closed under +, -, x, and ÷. Here elements of Q(√2) are exactly numbers that can be written in the form (a+b√2)/(c+d√2) where a, b, c, d are integers. We call such a field L a (field) extension over Q (written L/Q).

When we're adjoining √2 to Q to construct Q(√2), what we're really doing is adjoining to Q a root of the polynomial $f(x)=x^2-2$. We could do this with other higher-degree polynomials. Let p(x) be a polynomial with integer coefficients (and no repeating roots). We define the splitting field K of p(x) to be the smallest field containing both Q and all the roots of p(x). For example, the splitting field of $p(x)=x^2+1$ has roots i and $-i$ so a splitting field K of p(x) is $K=Q(i,-i)=Q(i)$. (The last equality is true because 0 and i are in Q(i), so $-i=0-i$ is also in Q(i)).
Conversely, we call an extension K/Q a Galois extension if it is the splitting field of some polynomial p(x). From before, Q(i)/Q is a Galois extension.

Q-Fixing Automorphisms

An automorphism F of a field K is an isomorphism from K to itself, where the algebraic structure is preserved -- specifically, F(a+b)=F(a)+F(b), F(ab)=F(a)F(b). In the case that K is an extension of Q, we're more interested in automorphisms of K that has F(x)=x for all x in Q (or that F fixes elements of Q). An automorphism F of K is a Q-fixing automorphism if it has this property.

There are two Q-fixing automorphisms of L=Q(√2): the identity automorphism (call it e) that takes each element of Q(√2) to itself, and an automorphism (call it t) that takes anything from Q to itself, and √2 to -√2. It is possible to show that there is exactly one such automorphism t.

Groups

A group is a set with a "composition" operation • with an identity element. From above, the set of Q-fixing automorphisms of K, denoted G(K/Q) is a group with • being function composition, and e being the identity element. Observe that we do not require • to be commutative (so a•b may not be the same as b•a in this case).

Two groups are isomorphic if they have the same algebraic structure -- i.e. they're essentially the same group except the elements have different names. It is useful to see whether G(K/Q) is isomorphic to a group that we know and understand. Two important classes of groups that are well understood are cyclic groups and permutation groups.

Examples of Groups

The cyclic group C(n) of order n is the set {0,1,2,3,..,n-1}, with • being addition mod n. From the example of L=Q(√2), L has G(L/Q)={e,t} with • being function composition. This is actually isomorphic to C(2)={0, 1}.

Permutation groups consist of functions that permute some "letters". We'll use S(n) to denote the group of permutations of n letters. For example, S(3) is all the permutations of letters {a, b, c}. A function F that takes a→b, b→a, c→c is one such permutation (and hence an element of S(3)).

The Fundamental Theorem of Galois Theory

Galois noticed that for a Galois extension K/Q, there is a link between "subfields" of K containing Q, and "subgroups" of G=G(K/Q). The quoted words mean exactly what you might think -- a subfield of K is a field L that is contained in K (and is closed under +, -, x, ÷). For example, Q is a subfield of R, and Q is a subfield of Q(√2). A subgroup of G is a group H that is contained in G (that is closed under • and contains the identity element). For example, the subset {0,2,4} is a subgroup of C(6) = {0,1,2,3,4,5}.

More concretely, there is a 1-1 correspondence between subfields of L and subgroups of H:

- For a subfield L of K containing Q, there is a subgroup H of G corresponding exactly to the automorphisms that fix all of L -- i.e. f(x)=x for all x in L, not just Q.
- The reverse is true as well: if H is a subgroup of G, then there is some subfield L of K containing Q that is fixed by all of H.

In particular, whenever L/Q is itself a Galois extension, H is a normal subgroup of G (i.e., gH = Hg for all g in G), so that the quotient G/H = {gH: g in G} is another group. This group G/H turns out to be isomorphic to G(L/Q).

For a concrete example, let's take K=Q(i, $\sqrt[3]{2}$). It's possible to show that K/Q is a Galois extension, and that G=G(K/Q) is isomorphic to S(3). In particular, the subfields of K are Q(*i*) and Q($\sqrt[3]{2}$), and they correspond to subgroups of S(3) isomorphic to C(3) and S(2). We saw before that Q(i) is a Galois extension, and C(3) happens to be normal in S(3).

Linking Back to the Big Idea

Suppose p(x) is a degree 5 polynomial, and that it has a root x that is solvable in radicals. Then really, x is in some field K containing Q, where K can be "built up" from Q by successively adjoining ($\sqrt[n]{\alpha}$), the n-th root of α, for some n, and some α in the current field. For example, take x=$\sqrt{(2+\sqrt{5})}$. We set L=Q($\sqrt{5}$) and K=L($\sqrt{(2+\sqrt{5})}$) to "build up" K in this manner.

Solvable Fields

In general, we call an extension K/Q solvable if K=K0⊇K1⊇K2⊇...⊇Q, where each K(i-1)=Ki($\sqrt[n]{\alpha}$) for some n, and some α in Ki. This is exactly the construction we had a paragraph ago. As another example, K=Q(i, $\sqrt[3]{2}$) is a solvable extension since Q(i, $\sqrt[3]{2}$)=Q(i)($\sqrt[3]{2}$)⊇Q(i)⊇Q is in the desired form (recall i=$\sqrt{(-1)}$).

For a polynomial p(x) in Q, the splitting field K of p(x) is the smallest field containing all the roots of p(x), so the roots of p(x) are solvable in radicals if and only if K is solvable.

Solvable Groups

We can actually assume (ignoring some subtleties) that each K(i-1)/Ki from above is a Galois extension. In this case each G(K(i-1)/Ki) is actually isomorphic to C(n) for some n.

Thus in order for a field extension K/Q to be solvable, G=G(K/Q) must be in a particular form: there has to be a chain of subgroups, G=G0⊇G1⊇G2⊇...⊇{e}, where each Gi is a normal subgroup of G(i-1) and Gi/G(i-1)=C(n) for some n, and {e} is the trivial group with just the identity element. In the case of K=Q(i, $\sqrt[3]{2}$), the chain of subgroups looks like G(K/Q)=S(3)⊇C(3)⊇{e}.

A Quintic Formula Cannot Exist

To recap, roots of p(x) being solvable in radicals requires the splitting field K of p(x) to be a solvable field, which in turn requires G(K/Q) to be a solvable group.

But with a little group theory, we can show that S(5) is not solvable. Further, any quintic polynomial with two non-real roots has Galois group S(5). These last facts require some more concepts to develop, but in any case -- not all roots of quintic polynomials are solvable in radicals.