Math 222: An Introduction to Galois Groups

Problem. Determine when a polynomial with integral coefficients is solvable by radicals.

Galois' Idea: To a polynomial $P(x)$ which is irreducible over the rational numbers $\mathbb{Q}$, associate a certain finite group $Gal(P(x))$. And translate the solvability problem to one in terms of groups.

STEP 1: Splitting Fields – Given an irreducible polynomial, we first consider the smallest field which contains all the zeros. The construction is analogous to that of $GF(p, P(x))$.

Example 1.0. Let $P(x) = x^5 - 1 = (x-1)(x^4 + x^3 + x^2 + x + 1) = (x-1)f(x)$. Then $f(x)$ is irreducible over $\mathbb{Q}$ with zeros ϵ, ϵ^2, ϵ^3, ϵ^4 as previously denoted. i.e. the non-trivial fifth roots of unity. Let

$$\mathbb{Q}(\epsilon) = \{a_0 + a_1\epsilon + a_2\epsilon^2 + a_3\epsilon^3 : a_i \in \mathbb{Q}\}$$

be a field under "polynomial" multiplication. Notice that ϵ^4 and all higher powers can be written in terms of smaller powers. The same arguments as for Galois Fields shows that this will always give a field. When working over $\mathbb{Z}_p$, we saw that all the zeros were necessarily in the Galois field. In this example, this is also clearly true, but this need not be true in general.

Example 2.0. Consider $q(x) = x^3 - 2$ which is irreducible over $\mathbb{Q}$. Let $\sqrt[3]{2}$ denote the real cube root of 2. Recall that the zeros are $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, and $\sqrt[3]{2}\omega^2$ where ω and ω^2 were the non-trivial cube roots of 1 and satifsy $x^2 + x + 1 = 0$. Then set

$$\mathbb{Q}(\sqrt[3]{2}) = \{a_0 + a_1\sqrt[3]{2} + a_2(\sqrt[3]{2})^2 : a_i \in \mathbb{Q}\}.$$

Since $(\sqrt[3]{2})^3 = 2$, we don't need any further powers. Although this is a field, it clearly does not contain the other zeros. So, one has to throw in powers of $\sqrt[3]{2}\omega$ as well as products with $\sqrt[3]{2}$ and get a bigger field. This turns out to be the field

$$\mathbb{Q}(\sqrt[3]{2}, \omega) = \{a_0 + a_1\sqrt[3]{2} + a_2\omega + a_3(\sqrt[3]{2})^2 + a_4\sqrt[3]{2}\omega + a_5\omega^2 + a_6(\sqrt[3]{2})^2\omega + a_7\sqrt[3]{2}\omega^2 + a_8(\sqrt[3]{2})^2\omega^2 : a_i \in \mathbb{Q}\}.$$

STEP 2: Groups of Automorphims – The Galois group of the polynomial is a group of automorphisms of the splitting field. Recall the notion of an automorphism of a field from the ring handout – it's a one-to-one, onto map, which preserves both addition and multiplication. The group structure will be function composition. But, we only take certain automorphisms.

Example 1.1. We define $Gal(f(x))$ to be the set of all automorphisms of the field $\mathbb{Q}(\epsilon)$ which "fix" $\mathbb{Q}$. Recall, that the field $\mathbb{Q}$ is a subfield of $\mathbb{Q}(\epsilon)$ and the assumption is that we want automorphisms $\phi : \mathbb{Q}(\epsilon) \to \mathbb{Q}(\epsilon)$ for which $\phi(a) = a$ for all $a \in \mathbb{Q}$.

Question: Where can ϵ go under such a ϕ? Remember that $\epsilon^5 = 1$ and hence $\phi(\epsilon^5) = \phi(1) = 1$ by the assumption. But, since ϕ preserves multiplication, we must have $\phi(\epsilon^5) = \phi(\epsilon)^5$. Hence $\phi(\epsilon)^5 = 1$. In other words ϵ must go to one of the other zeros! Since the map must be one-to-one ϵ cannot go to 1 and so can go to ϵ, ϵ^2, ϵ^3, or ϵ^4. Similarly, if you take any of the other zeros, one sees that they too must go to a zero. It turns out that the automorphisms we're looking for simply correspond to certain *permutations* of the zeros!

In this case, everything is determined simply by $\phi(\epsilon)$. For example, $\phi(\epsilon^2) = \phi(e)^2$ and so on. As there are four choices for $\phi(\epsilon)$ we get precisely four automorphisms and a group of order four. With a little work one can check that $Gal(f(x)) \simeq (\mathbb{Z}_4, +)$.

General Facts: For an irreducible polynomial $P(x)$ of degree n over $\mathbb{Q}$, the Galois Group $Gal(P(x))$ is a subgroup of S_n, thought of as the set of permutations of the n zeros of $P(x)$.

Example 2.1. Return to $q(x) = x^3 - 2$. Here there are three zeros, so the Galois Group is a subgroup of S_3. In this case, everything is determined by $\phi(\sqrt[3]{2})$ and $\phi(\omega)$. Now, $\sqrt[3]{2}$ can go to any of the three zeros $\sqrt[3]{2}$, $\sqrt[3]{2}\omega$, or $\sqrt[3]{2}\omega^2$, while ω must go to either ω or ω^2. Hence there are $3 \cdot 2 = 6$ possible automorphisms and so $Gal(q(x))$ must be all of S_3.

Question: What's the point?

Once we've constructed these groups, there's an amazingly beautiful theorem of Galois which relates the structure of the groups to the structure of these "splitting fields". Indeed, the following is only a glimpse of the relationship.

STEP 3: Galois' Theorem. Let $P(x)$ be an irreducible polynomial over $\mathbb{Q}$ and $G = Gal(P(x))$ be the associated Galois group. Then $P(x)$ is solvable by radicals if and only if there exists a chain of subgroups

$$G = H_0 \supset H_1 \supset H_2 \supset \cdots \supset H_n = \{1_G\}$$

such that

(1) H_{i+1} is *normal* in H_i for each $0 \leq i \leq n-1$.
(2) For each $0 \leq i \leq n-1$, $|H_i|/|H_{i+1}| = p_i$ for some prime p_i. Equivalently, the quotient group H_i/H_{i+1} is isomorphic to $(\mathbb{Z}_{p_i}, +)$.

Moreover, let p_i be the largest index appearing in the chain. At least one of the zeros of $P(x)$ has degree p_i over the integers.

Example 1.2. Consider $f(x) = x^4 + x^3 + x^2 + x + 1$. We saw that $Gal(f(x)) \simeq (\mathbb{Z}_4, +)$. Indeed, we have the normal chain

$$\mathbb{Z}_4 = \{0, 1, 2, 3\} \supset \{0, 2\} \supset \{0\}.$$

Here the index is 2 at both steps. Hence all the solutions are degree 2 algebraic and hence constructible as we previously claimed.

Example 2.2. Consider $q(x) = x^3 - 2$. We saw that $Gal(q(x)) \simeq S_3$. One can check that there is only one normal subgroup:

$$S_3 \supset \langle (123) \rangle \simeq \mathbb{Z}_3 \supset \{Id\}.$$

At the first step the index is 2 and at the second it's 3. So, the solutions are algebraic, but at least one is degree 3. Notice that if one of the solutions was constructible, we could easily construct the others and so all three must have degree 3.

Example 3. Consider $g(x) = 3x^5 - 15x + 5$. Using Eisenstein's Criterion one can check that this is irreducible over $\mathbb{Q}$. Moreover, using a little Calculus, one can see that there are three distinct real roots and two complex roots. Under these conditions, with a little group theory, one can show that the Galois Group must be all of S_5. We pointed out in class that A_5 was normal in S_5 since it has index 2. In fact, this is the only normal subgroup of S_5.

But, A_5 is a so-called *simple* group – it has NO non-trivial normal subgroups. See Proposition 10.11. This is proved by playing with 3-cycles. Indeed it uses one of our homework problems (8.4 #13) in which we showed that every even permutation could be written as a product of 3-cycles.

Hence, the only normal chain we can form in this case is

$$S_5 \supset A_5 \supset \{Id\}.$$

The first step has index 2 which is ok, but the second step has index 60, which is not prime!! Hence, by Galois' Theorem at least one of the zeros is not solvable by radicals of any degree!!