32 Solving Polynomial Equations

One application of Galois theory is the impossibility of a solution in radicals to polynomial equations of degree at least 5. The fundamental theorem of algebra states that a degree n polynomial has n (not necessarily distinct roots). For linear polynomials $ax+b$, the root is obviously $x=-b/a$; for quadratics, the quadratic formula is well-known. Even for degree 3 and 4 polynomials, the cubic and quartic equations (which are much longer) provide universal formulae to find the roots. For a long time, mathematicians searched for the elusive "quintic formula," but now we know that there is no way to "write down" the roots of polynomials of degree 5 or higher, and Galois theory is the key to proving this fact.

32.1 Solvable Groups

Last class, we established the following definition:

Definition 32.1
A finite group G is **solvable** if there exists a sequence of subgroups $G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_n = \{1\}$, such that for each i, G_i is a normal subgroup of G_{i-1}, and G_{i-1}/G_i is abelian.

Informally, a group is solvable if it can be built from putting together abelian groups.

Lemma 32.2
If $G/K \cong H$ (equivalently, if there is an onto map $G \twoheadrightarrow H$ with kernel K), then:

1. If K and H are solvable, then G is solvable.
2. If G is solvable, then H is solvable.

Proof sketch. The first direction is clear from the correspondence theorem — we can essentially put the filtrations for H and K together. If we have a filtration $H = H_0 \supset H_1 \supset \cdots \supset H_n = \{1\}$ with this property, we can take their pre-images $G = G_0 \supset G_1 \supset \cdots \supset G_n = K$. We then can place the filtration for K at the end.

For the second, we can take our filtration of G, and simply take its image. The intermediate subgroups we get for H will be quotients of the intermediate subgroups for G, and the quotient of an abelian group is also abelian; so this gives a valid filtration for H. □

We have the following group-theoretic lemma:

Lemma 32.3
S_5 is not solvable. In fact, A_5 is simple.

Recall that a group is *simple* if it has no normal subgroups except for itself and $\{1\}$.

This lemma is also true for $n \geq 5$ (meaning S_n is not solvable). But for $n < 5$ it's not true — we have $A_3 \cong \mathbb{Z}/3\mathbb{Z}$, which is abelian; while S_4 contains the Klein 4-group K_4 (consisting of (12)(34), (13)(24), (14)(23), and the identity), which is a normal subgroup.

Proof. The best proof is to think about the structure of conjugacy classes in symmetric groups; but we don't have time, so we'll do a more quick and dirty proof for just the case $n = 5$.

The class equation for A_5 is

$$60 = 1 + 15 + 20 + 12 + 12$$

(corresponding to the conjugacy classes of (12)(34), (123), (12345), and (13245)). Note also that if we have a 5-cycle in one of the conjugacy classes of size 12, its square is in the other.

If N is a normal subgroup, then it's a union of conjugacy classes, which means $|N|$ is a sum of 1, plus a subset of $\{15, 20, 24\}$. But it also has to divide 60. This is impossible — we have to take 1, but then we have to take 15 (or else the sum would be odd, and would need to divide 15). Then we have to take 20 (otherwise the sum would be 1 mod 3, and would have to divide 20). Then we must take 24 because otherwise the sum wouldn't be divisible by 5 (and would have to divide 12). □

Student Question. *How does this argument generalize to all $n \geq 5$?*

Answer. *This argument doesn't really generalize — but there is a slightly longer argument that does. We essentially just look at the possible cycle structures, take one conjugagy class, and show that the products of elements in that conjugacy class cover every other conjugacy class.*

32.2 Radical Extensions

Now we'll relate this to polynomial equations.

Definition 32.4
A finite extension E/F is a **radical extension** if $E = F(\alpha_1, \ldots, \alpha_n)$, where $\alpha_i^{n_i} \in F(\alpha_1, \ldots, \alpha^{i-1})$ for all i (for some positive integers n_i).

Informally, a radical extension is one that can be obtained by adjoining a bunch of radicals — in simple English, we're allowed to perform arithmetic operations and to extract radicals of any order.

Example 32.5
The extension
$$\mathbb{Q}\left(\sqrt[3]{3 + \sqrt[5]{7 + \sqrt{2}}}\right)$$
is a radical extension.

Proposition 32.6
Any radical extension is contained in a Galois extension with a solvable Galois group.

We'll assume that $\text{char}(F) = 0$ (although things do generalize to $\text{char}(F) = p$ with some more care).

The proof essentially hinges on the lemma discussed last class — that if F contains a primitive nth root of unity, and $E = F(\alpha)$ for some α with $\alpha^n \in F$, then E/F is a Galois extension whose Galois group is cyclic.

It'll be convenient to slightly generalize this lemma, to let us *simultaneously* extract a bunch of radicals.

Lemma 32.7
Under the same assumptions, if $E = F(\beta_1, \ldots, \beta_k)$ where $\beta_i^n \in F$ for all i (and F contains a primitive nth root of unity), then $\text{Gal}(E/F) \subset (\mathbb{Z}/n\mathbb{Z})^k$. In particular, $\text{Gal}(E/F)$ is still abelian.

The proof is the same as before — any element of the Galois group sends $\beta_i \mapsto \beta_i \zeta_n^{c_i}$ for some exponent c_i, and composing elements of the Galois group corresponds to adding each pair of c_i.

Proof of Proposition 32.6. Use induction on n. If $n = 1$, then $E \subset F(\zeta, \alpha)$ where $\alpha^n \in F$ and ζ is a primitive nth root of unity (we can't assume in this proof that F contains roots of unity, but we can essentially just add them). This is the splitting field of $x^n - \alpha^n$.

So we have a tower of field extensions $F(\zeta, \alpha)/F(\zeta)/F$. We know that $F(\zeta, \alpha)/F(\zeta)$ has a Galois group which is a subgroup of $\mathbb{Z}/n\mathbb{Z}$; meanwhile, $F(\zeta)/F$ has a Galois group which is a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$. Both are abelian, so the Galois group of $F(\zeta, \alpha)/F$ is solvable.

For the inductive step, assume that $F(\alpha_1, \ldots, \alpha_{i-1}) \subset E'$, where $\text{Gal}(E'/F)$ is solvable, and suppose $\alpha_i^{n_i} \in F(\alpha_1, \ldots, \alpha_{i-1})$.

We then want to start with E', and first add a primitive n_ith root of unity ζ. To make sure we get a splitting field over F (and not just E'), we need to also add all Galois conjugates of α_i — let $\beta_1, \ldots, \beta_d$ be all conjugates of $\alpha_i^{n_i}$ under $\text{Gal}(E'/F)$. Then we take
$$E = E'(\zeta, \sqrt[n_i]{\beta_1}, \ldots, \sqrt[n_i]{\beta_j}).$$

First, we want to show that E is a splitting field over F. Let Q be a polynomial such that E' is the splitting field of Q. Now if $\alpha_i^{n_i} = a$ (which lies in E'), we claim that E is the splitting field of

$$Q(x) \cdot (x^{n_i} - 1) \cdot \prod_{g \in \operatorname{Gal}(E'/F)} (x^{n_i} - g(a)).$$

(The reason we have this product over the Galois group, rather than simply the term $x^{n_i} - a$, is that a is not necessarily in F — but this product is, by the trick seen earlier.)

Now consider the tower of extensions $E/E'(\zeta)/E'/F$. Then $\operatorname{Gal}(E'/F)$ is solvable by the induction assumption; $\operatorname{Gal}(E'(\zeta)/E')$ is a subgroup of $(\mathbb{Z}/n_i\mathbb{Z})^\times$ and is therefore abelian; and $\operatorname{Gal}(E/E'(\zeta))$ is a subgroup of $(\mathbb{Z}/n\mathbb{Z})^d$, where $d = || \operatorname{Gal}(E'/F)|$. So $\operatorname{Gal}(E/F)$ is solvable as well, and we're done. □

Note 32.8
The proof contains a technicality in order to ensure that our extensions are all Galois extensions of F; this is why we needed to deal with the β_i. Other than that, it's essentially just a direct application of the lemma from earlier (about the Galois group when we just add a nth root).

The conclusion is now clear:

Corollary 32.9
There are many nonradical extensions of $\mathbb{Q}$.

For instance, the splitting field of any polynomial with Galois group S_5 (such as our example $2x^5 - 5x - 10$ from earlier) is a nonradical extension; this means the roots of such a polynomial can't have an expression in radicals.

32.3 Symmetric Polynomials

We'll now move on to a more concrete question:

Guiding Question
Given a polynomial, how do we compute $\operatorname{Gal}(E/F)$ and solve the equation when possible?

To answer this, we'll use the computational tool of symmetric polynomials (which can be understood independently of fields and Galois theory, and is an important branch of elementary algebra).

Consider the polynomial ring $\mathbb{Z}[x_1, \ldots, x_n]$ (we could do the same with rational-coefficient polynomials). We use $R_n = \mathbb{Z}[x_1, \ldots, x_n]^{S_n}$ to denote the subgroup of $\mathbb{Z}[x_1, \ldots, x_n]$ consisting of polynomials which are invariant under permutation of the variables.

Example 32.10
If $n = 3$, then $x_1^3 + x_2^3 + x_3^3 \in R_3$, while $x_1^3 \notin R_3$.

It's easy to write down polynomials in R_n — we can start with any polynomial, and average over all permutations. The easiest example to think about is probably power sums; but a particularly useful one will be something different, the *elementary symmetric functions*.

Definition 32.11

If we have n variables $x_1, \dots, x_n$, then the **elementary symmetric functions** $\sigma_1, \dots, \sigma_n$ are defined as

$$\begin{aligned}\sigma_1 &= x_1 + x_2 + \cdots + x_n,\\ \sigma_2 &= x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n,\\ \sigma_3 &= x_1x_2x_3 + \cdots + x_{n-2}x_{n-1}x_n,\end{aligned}$$

and so on: in general, σ_k is the sum of the $\binom{n}{k}$ monomials which are products of k distinct terms x_j:

$$\sigma_k = \sum_{1 \le j_1 < j_2 < \cdots < j_k \le n} x_{j_1} \cdots x_{j_k}.$$

The first reason the elementary symmetric functions are relevant is that if we have a polynomial whose roots we know, we can expand it as

$$(z - x_1) \cdots (z - x_n) = z^n - \sigma_1 z^{n-1} + \sigma_2 z^{n-2} - \cdots + (-1)^n \sigma_n,$$

by considering which term in each factor we choose when expanding the product.

Example 32.12

If $n = 2$, we have

$$(z - x)(z - y) = z - (x + y)z + xy.$$

A useful fact about the elementary symmetric functions is the following:

Theorem 32.13

We have

$$R_n = \mathbb{Z}[\sigma_1, \sigma_2, \dots, \sigma_n].$$

Given two symmetric polynomials, it's obvious that their sum and product are also symmetric polynomials. But the interesting part of this theorem is that every symmetric polynomial can be expressed as a polynomial in the elementary symmetric functions (and this expression is unique).

Example 32.14

We have

$$\begin{aligned}x_1^2 + x_2^2 + x_3^2 &= \sigma_1^2 - 2\sigma_2;\\ x_1^3 + x_2^3 + x_3^3 &= \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3.\end{aligned}$$

We'll prove the theorem later, but the reason it's useful here is the following:

Corollary 32.15

A symmetric polynomial in the roots of P can be written as a polynomial in the coefficients of P.

The strategy for how to compute the Galois group of a polynomial is based on this fact. In particular, one important symmetric polynomial in the roots is the *discriminant*:

Definition 32.16

The **discriminant** of $P(x) = \prod(x - \alpha_i)$ is

$$D(P(x)) = \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

When we square, it doesn't matter which of α_i and α_j had smaller index; so the discriminant is a symmetric polynomial in the roots. By the theorem, the discriminant is then some polynomial in the coefficients.

Unfortunately, the formulas quickly get complicated. However, there are some cases where the discriminant is reasonable to compute:

Example 32.17
If $P(x) = x^3 + px + q$, then $D = -4p^3 - 27q^2$.

Proof. We could compute D using the definition, but that's fairly messy. Instead, we'll look at degrees — we know D is a degree 6 polynomial in the roots α_1, α_2, and α_3. Meanwhile, p is a degree 2 polynomial in the roots, and q is a degree 3 polynomial. The only monomials in p and q which can have degree 6 are then p^3 and q^2, so $D = ap^2 + bq^2$ for some a and b. We can then plug in a few polynomials for P to solve for a and b — for example, $P(x) = x(x-1)(x+1)$ has $p = -1$, $q = 0$, and $D = 4$, so $a = -4$; meanwhile $P(x) = (x-1)^2(x+2) = x^3 - 3x + 2$ has $p = -3$, $q = 2$, and $D = 0$, so $b = -27$. □

Although this only works for cubic polynomials whose x^2 coefficient is 0, there's an easy trick to turn any cubic polynomial into this form — if we start with $x^3 + ax^2 + bx + c$, we can substitute $y = x + a/3$.

Note that $D = 0$ if and only if P has multiple roots. The main application to Galois theory is that $\sqrt{D}$ is always in the splitting field of P; and in fact $\sqrt{D} \in F$ if and only if the Galois group is a subset of A_n. We'll discuss this in more detail next class.

Resource: Algebra II Student Notes
Spring 2022
Instructor: Roman Bezrukavnikov
Notes taken by Sanjana Das and Jakin Ng