34 Solving Polynomial Equations (continued)

34.1 Cubic Polynomials

Last class, we looked at cubic polynomials of the form $P(x) = x^3 + px + q$ (called *depressed cubics*), which have discriminant $D = -4p^3 - 27p^2$. For simplicity we assume the field has characteristic 0, as the cases of characteristic 2 and 3 are somewhat different. We saw that if E is the splitting field of P, then $E \supset F(\delta)$ where $\delta = \sqrt{D}$; and $\mathrm{Gal}(E/F(\delta)) = \mathbb{Z}/3\mathbb{Z}$. (It's possible that $\delta \in F$, though it usually isn't.) We saw that then $E = F(\delta)(\alpha)$, where α is a cube root of some element $a \in E$; our explicit construction was $\alpha = \beta + \omega\sigma(\beta) + \omega^2\sigma^2(\beta)$ for some $\beta \in E$ (which isn't in F).

It's actually possible to turn these ideas into a formula for the roots of P. Let β_1, β_2, β_3 be the roots of P (which are elements in E). Then some $\sigma \in \mathrm{Gal}(E/F[\delta])$ must permute the roots in a 3-cycle $\beta_1 \to \beta_2 \to \beta_3 \to \beta_1$; this means we can take

$$\alpha = \beta_1 + \omega\beta_2 + \omega^2\beta_3.$$

We know $\alpha^3 \in F(\delta)$. In fact, using symmetric polynomials, we can express α^3 in terms of p, q, and δ. It's possible to show this by a general argument — this is because

$$\alpha^3 = Q(\beta_1, \beta_2, \beta_3)$$

for a polynomial Q which isn't quite symmetric, but is invariant under *even* permutations. This is enough, as a result of a slight generalization of the theorem on the elementary symmetric polynomials seen earlier:

Fact 34.1
We have

$$\mathbb{Q}[x_1, \dots, x_n]^{A_n} = \mathbb{Q}[x_1, \dots, x_n]^{S_n} \oplus \delta\mathbb{Q}[x_1, \dots, x_n]^{S_n}.$$

Intuitively, δ is invariant under A_n but changes sign under S_n; but this essentially accounts for all the new polynomials allowed when we only consider even permutations.

Instead of using this theoretical argument, it's also possible to just write down the expression for α^3 directly — we have

$$\alpha^3 = \beta_1^3 + \beta_2^3 + \beta_3^3 + 6\beta_1\beta_2\beta_3 + \omega(\beta_1^2\beta_2 + \beta_2^2\beta_3 + \beta_3^2\beta_1) + \omega^2(\beta_1\beta_2^2 + \beta_2\beta_3^2 + \beta_3\beta_1^2).$$

The first few terms are symmetric — we have the formulas

$$\beta_1\beta_2\beta_3 = -q$$
$$\beta_1^3 + \beta_2^3 + \beta_3^3 = -3q.$$

Meanwhile, we can let $A = \beta_1^2\beta_2 + \beta_2^2\beta_3 + \beta_3^2\beta_1$ and $B = \beta_1\beta_2^2 + \beta_2\beta_3^2 + \beta_3\beta_1^2$. We can then calculate that

$$A + B = \sigma_1\sigma_2 - 3\sigma_3 = 3q.$$

Meanwhile, $A - B$ is not symmetric, but by expanding we can see that

$$A - B = (\beta_1 - \beta_2)(\beta_1 - \beta_3)(\beta_2 - \beta_3) = \delta.$$

Now we're basically done — we can solve for A and B, and get a formula for α — we have

$$\alpha = \sqrt[3]{-4q + 3\omega A + 3\omega^2 B}.$$

Then we can similarly define and compute $\alpha' = \beta_1 + \omega^2\beta_2 + \omega\beta_3$. We then have $\beta_1 = (\alpha + \alpha')/3$, and we can calculate the other roots similarly. We won't describe the full formula here, but it's in the textbook. In fact, a version of this formula was discovered by Cardano in 1545.

Student Question. *If this formula was discovered before Galois theory, how did people come up with it?*

Answer. *The approach described here, of writing down formulas for these expressions, was invented by Legendre. It doesn't really need Galois theory in its full strength — it's possible to just notice that if we write* $\alpha = \beta_1 + \omega\beta_2 + \omega^2\beta_3$*, then* α^3 *is an expression in the roots which can be calculated using symmetric polynomials (and the discriminant).*

But not only was the formula discovered before Galois theory, it was also discovered before complex numbers. Having to work with roots of negative numbers gave people a lot of trouble — this was controversial even in the early 19th century. It mattered to people whether they could operate with real numbers, or had to work with strange expressions involving roots of negative numbers.

In fact, suppose that P has 3 real roots. Then Δ is nonnegative, so δ is real. But the expression $\alpha = \beta_1 + \omega\beta_2 + \omega^2\beta_3$ is not *real! So when you write down the answer in radicals, the final answer will be real; but you'll still need to work with a complex cubic root. This was referred to as* casus irreducibilis.

If you're interested in the history and philosophy of this story, a book by Barry Mazur called Imagining Numbers, Especially $\sqrt{-15}$ *talks about this history and reflects about how the understanding of such topics developed. Essentially, people were working with complex numbers three centuries before they were fully realized and accepted as existing.*

34.2 Quartic Polynomials

We'll also briefly discuss quartics. The key point is that the analysis of solutions can be guided by the structure of the Galois group.

The Galois group is a subgroup of S_4. We know S_4 contains the normal subgroup K_4 (the Klein 4-group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$), consisting of $\{(12)(34), (13)(24), (14)(23), 1\}$. We then have $S_4/K_4 \cong S_3$, corresponding to the *resolvent cubic.*

So if $P(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)(x - \alpha_4)$, we can write down the expressions

$$\beta_1 = \alpha_1\alpha_2 + \alpha_3\alpha_4,$$
$$\beta_2 = \alpha_1\alpha_3 + \alpha_2\alpha_4,$$
$$\beta_3 = \alpha_1\alpha_4 + \alpha_2\alpha_3.$$

These expressions are permuted by the Galois group, and we know that if we take

$$Q(x) = (x - \beta_1)(x - \beta_2)(x - \beta_3),$$

then when we expand, the coefficients will be symmetric polynomials in the α_i. So if $P(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$, then we have $Q(x) = x^3 + b_2x^2 + b_1x + b_0$ where the b_i are polynomials in the a_i — for concreteness, the exact formulas are $b_2 = -a_2$, $b_1 = a_1a_3 - 4a_0$, and $b_0 = 4a_0a_2 - a_1^2 - a_0a_3^2$.

Now to find a root, we first find the roots of the resolvent cubic $Q(x)$ (since we already know how to solve a cubic polynomial). Then, since $K_4 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, it just remains to solve a few quadratic equations. More explicitly, we can write the equations

$$(\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4) = \beta_1 + \beta_3$$
$$\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = -a_3.$$

This gives a quadratic for $\alpha_1 + \alpha_2$ and $\alpha_3 + \alpha_4$, which we know how to solve. We can similarly find the other pairwise sums, and then compute the roots themselves by solving the resulting linear system.

This shows how to find the roots explicitly, but similarly to the cubic case, we can also try to compute the Galois group:

Guiding Question

How do we compute $\text{Gal}(E/F)$ for a given polynomial $P(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$?

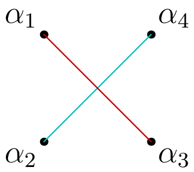
In degree 3, all we needed to know was whether the discriminant was a square or not — this determined whether the group was $\mathbb{Z}/3\mathbb{Z}$ or S_3. In this case, the process is longer, but somewhat similar.

First, there are five transitive subgroups of S_4 — these are S_4, A_4, K_4 (the Klein 4-group, described earlier), C_4 (the cyclic group, generated by (1234)), and D_4 (the dihedral group, generated by (1234) and (24), which we can think of as the group of symmetries of a square).

One test we can perform still uses the discriminant. It's a lengthy expression, so we won't explicitly write it down, but it's still theoretically possible to compute it. Then $\sqrt{D} \in F$ if and only if $G \subset A_4$. The groups which are subsets of A_4 are K_4 and A_4 itself.

Then we can obtain more information from looking at the resolvent cubic (since we've already seen how to analyze cubics). We know that $Q(x)$ splits completely in F if and only if $G = K_4$ (since then all elements of G fix $\alpha_1\alpha_2 + \alpha_3\alpha_4$ and the other two expressions, which means they must lie in K_4).

Meanwhile, if $Q(x)$ has exactly one root in F, then the elements of G preserve one root of Q, say $\alpha_1\alpha_3 + \alpha_2\alpha_4$. In this case, we claim that the Galois group is C_4 or D_4 — we can visualize this by considering a square.



The square naturally splits into two subsets, by drawing its diagonals. So any permutation which fixes the square will either fix or swap $\alpha_1\alpha_3$ and $\alpha_2\alpha_4$, which means it fixes $\alpha_1\alpha_3 + \alpha_2\alpha_4$ (while not every permutation in C_4 fixes the other two expressions).

So this information resolves nearly all cases — the only ambiguity left is whether the group is C_4 or D_4. We won't explain how to distinguish between them, but an explanation is in Keith Conrad's notes.

34.3 Main Theorem of Algebra

We'll finish with another application of Galois theory — we'll use it to give another proof of the Main Theorem of Algebra. We'll see that this proof brings in some nice considerations about finite groups, although it's somewhat less direct than the proof we've seen before.

Proposition 34.2
Every p-group is solvable — if G is a finite group with $|G| = p^n$ for a prime p, then G is solvable. Moreover, there exists a chain of subgroups

$$G = G_0 \supset G_1 \supset \cdots \supset G_n = \{1\},$$

such that for all i, G_{i+1} is a normal subgroup of G_i and $G_i/G_{i+1} \cong \mathbb{Z}/p$.

Proof. We'll essentially start from the right end (instead of the left). We'll need the following lemma:

Lemma 34.3
G has a nontrivial center.

Proof. Consider the class equation mod p. Every conjugacy class has size p^m for some m. But the class equation states that

$$p^n = 1 + \sum |C_i|$$

(where the 1 comes from the conjugacy class of the identity, which has 1 element). If all other conjugacy classes contained more than one element, then $|C_i|$ would be divisible by p for all i, and the right-hand side would be 1 mod p, contradiction. So there must exist conjugacy classes of size 1 (other than the one of the identity), and their elements are in the center of G. □

Now to prove the proposition, we induct on n. By the lemma, we have $G \supset Z$ (where Z is the center, and $Z \neq \{1\}$). Then we can find an element $g \in Z$ of order p (the center is a nontrivial p-group, so if we pick any element, it will have some power which has order p). Then let $\overline{G} = G/\langle g \rangle$ (which is valid because g is in the center of G, so $\langle g \rangle$ is clearly normal).

We have $|\overline{G}| = p^{n-1}$, so by the inductive assumption, $\overline{G}$ is solvable. Suppose we have a chain of subgroups

$$\overline{G} = \overline{G}_0 \supset \cdots \supset \overline{G}_d = \{1\}.$$

Now let G_i be the pre-image of $\overline{G}_i$, and let $G_{d+1} = \{1\}$; this works by the homomorphism theorem. □

Now we can prove the Main Theorem of Algebra:

Theorem 34.4
$\mathbb{C}$ is the only finite extension of $\mathbb{R}$.

This implies the standard formulation, that every polynomial (over $\mathbb{C}$) has a root in $\mathbb{C}$.

Proof. Let $F = \mathbb{R}$, and suppose E is a finite extension. Without loss of generality assume E is a splitting field (since it's a finite extension, it's obtained by adding some of the roots of some polynomial, and we can add in all the remaining roots), so E/F is a Galois extension. Let $G = \text{Gal}(E/F)$.

Lemma 34.5
$|G|$ is a power of 2.

Proof. Let $H \subset G$ be a Sylow 2-subgroup (a subgroup of order 2^n, where n is the exponent of 2 in $|G|$). Then consider the extension E^H/F — we have that

$$[E^H : F] = \frac{[E : F]}{[E^H : E]} = \frac{|G|}{|H|},$$

which is odd. But any odd-degree polynomial in $\mathbb{R}[x]$ has a real root (by the intermediate value theorem — the polynomial goes to $+\infty$ on one end and $-\infty$ on the other). So this means there are no odd-degree extensions of $\mathbb{R}$; so $H = G$, which means $|G| = 2^n$. (This argument works even if G is odd, as then H is trivial.) □

But now we can use the proposition — we have

$$G = G_0 \supset G_1 \supset \cdots \supset G_k = \{1\}$$

where $G_i/G_{i+1} \cong \mathbb{Z}/2\mathbb{Z}$ for all i, and we can consider their fixed fields

$$\mathbb{R} = F_0 \supset F_1 \supset \cdots \supset F_k = E,$$

where F_i is the fixed field of G_i. Then we have $[F_{i+1} : F_i] = 2$ for all i.

But it's clear that $\mathbb{C}$ is the only *quadratic* extension of $\mathbb{R}$, and $\mathbb{C}$ itself has no quadratic extensions (we can check that every quadratic over $\mathbb{C}$ has a root, since we can extract square roots using the trigonometric form of a complex number). So then G is $\{1\}$ or $\mathbb{Z}/2\mathbb{Z}$, and E is $\mathbb{R}$ or $\mathbb{C}$. □

Next class, we'll discuss the Galois group of extensions of finite fields. We'll see that

$$\text{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q) = \mathbb{Z}/n\mathbb{Z},$$

which essentially follows from the fact that $\mathbb{F}_q = \{x \mid x^q = x\}$ (we previously thought of these x as roots of a polynomial, but we can now think of them as fixed points under the map $t \mapsto t^q$).

Student Question. *How did we get that $|G| = |H|$ (when showing $|G|$ was a power of 2)?*

Answer. *By the Primitive Element Theorem (assuming $E^H \neq F$), the extension E^H/F is generated by one element. We can consider the minimal polynomial of this element; the degree of the minimal polynomial is equal to the degree of the extension. So the minimal polynomial has odd degree, which is a contradiction (since if it has a root, it's reducible).*

It's actually possible to avoid using the Primitive Element Theorem — if we take any *element in E^H, the degree of its minimal polynomial has to divide the degree of the extension (by the fact that $[K : F] = [K : E][E : F]$ for a tower of extensions $K/E/F$), and therefore has to be odd.*

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