33 Symmetric Polynomials and the Discriminant

33.1 Symmetric Polynomials

Last class, we began discussing symmetric polynomials and the discriminant. The goal is to develop some tools to understand the structure of the solutions to a polynomial — if not to compute them in radicals, then at least to see how this works when possible. Galois theory can be used for this as well, not just proving impossibility.

Last time, we considered the symmetric polynomials

$$\mathbb{Z}[x_1, \ldots, x_n] \supset \mathbb{Z}[x_1, \ldots, x_n]^{S_n} = R_n,$$

and stated the following fundamental theorem:

Theorem 33.1
We have $R_n = \mathbb{Z}[\sigma_1^{(n)}, \sigma_2^{(n)}, \ldots, \sigma_n^{(n)}]$, where

$$\begin{aligned}\sigma_1^{(n)} &= x_1 + \cdots + x_n,\\ \sigma_2^{(n)} &= x_1x_2 + \cdots + x_{n-1}x_n,\\ &\vdots\\ \sigma_n^{(n)} &= x_1 \cdots x_n.\end{aligned}$$

In other words, every symmetric polynomial $P \in R_n$ can be written in terms of the elementary symmetric functions.

Example 33.2
We have

$$\begin{aligned}x_1^2 + \cdots + x_n^2 &= \sigma_1^2 - 2\sigma_2,\\ x_1^3 + \cdots + x_n^3 &= \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3.\end{aligned}$$

We previously saw this example when $n = 3$. But a feature is that the right-hand side doesn't really depend on n — when we write the expression in terms of the symmetric polynomials, n sort of disappears.

The reason is that we have an obvious homomorphism $\mathbb{Z}[x_1, \ldots, x_n] \to \mathbb{Z}[x_1, \ldots, x_{n-1}]$ sending $x_n \to 0$ (so we essentially just kill one of the variables). Under this homomorphism, we have $R_n \to R_{n-1}$ (since if the polynomial was invariant under permutations of n variables, it's also invariant under permutations of the first $n-1$, where we killed the last variable). But this homomorphism is compatible with the elementary symmetric functions — it's clear that $\sigma_i^{(n)} \mapsto \sigma_i^{(n-1)}$, since the homomorphism essentially just kills the monomials containing x_n (and $\sigma_n^{(n)} \mapsto 0$).

Meanwhile, the power sums have the same property — we have $x_1^d + \cdots + x_n^d \mapsto x_1^d + \cdots + x_{n-1}^d$. This means if we can prove an identity for large n, we can automatically deduce it for smaller n as well.

On the other hand, we can also use degree considerations. For example, $x_1^3 + \cdots + x_n^3$ is a homogeneous polynomial of degree 3 in the x_i; while $\sigma_i^{(n)}$ is a homogeneous polynomial of degree i. This means we can only use $\sigma_1^{(n)}$, $\sigma_2^{(n)}$, and $\sigma_3^{(n)}$ in the expression; so if we can find the identity for $n = 3$, we can automatically deduce it for all larger n as well.

Putting these observations together, we see that a formula as in Example 33.2 for $n+1$ implies one for n, and conversely, using degree considerations it's enough to check it for small n. (In our example, $n = 3$ was enough; note that $n = 2$ is too small, because σ_3 is mapped to 0.)

We'll now prove the theorem.

Proof of Theorem 33.1. We use induction in the number of variables.

We need to check that every symmetric polynomial can be expressed as a polynomial in $\sigma_1^{(n)}$, ..., $\sigma_n^{(n)}$, and that this expression is unique. In other words, we can consider the map $\varphi_n : \mathbb{Z}[t_1, \ldots, t_n] \to R_n$, where $t_i \mapsto \sigma_i^{(n)}$.

Then we want to check that φ_n is an isomorphism, meaning that it's one-to-one and onto. We'll check these two parts separately.

First we'll check that φ_n is injective. Suppose there is some polynomial $Q(t_1, \dots, t_n)$ which φ_n maps to 0 (to prove injectivity, it suffices to show there is no such polynomial). We can first pull out the last variable, by writing $Q = t_n^d Q'$, where $t_n \nmid Q'$. Then $\varphi_n(t_n^d Q') = 0$, so we have

$$\left(\prod x_i\right)^d \cdot Q'(\sigma_1, \dots, \sigma_n) = 0.$$

Since the first factor is nonzero, this means $Q'(\sigma_1, \dots, \sigma_n) = 0$. So this essentially means that we can assume that Q is not divisible by t_n.

But now we can use the homomorphism from earlier — let r_n be the restriction map $R_n \to R_{n-1}$ sending $x_n \mapsto 0$. Then we have

$$r_n(Q'(\sigma_1, \dots, \sigma_n)) = 0$$

(because we assumed $Q'(\sigma_1, \dots, \sigma_n) = 0$). But we have

$$r_n\left(Q'\left(\sigma_1^{(n)}, \dots, \sigma_n^{(n)}\right)\right) = \overline{Q}\left(\sigma_1^{(n-1)}, \dots, \sigma_{n-1}^{(n-1)}\right),$$

where $\overline{Q}$ is not identically 0 (since we assumed Q' is not divisible by t_n, and r_n just maps $t_n \mapsto 0$). But this contradicts the inductive assumption (because then φ_{n-1} would map a nonzero polynomial $\overline{Q}_{n-1}$ to 0). (The base case of the induction is $n = 1$, which is trivial.)

Now we'll check that φ_n is surjective. Start with a polynomial $P \in R_n$; we can assume P is homogeneous of degree d. We want to check that $P = \varphi_n(Q)$ for some Q; we'll use induction on d.

The idea is again to reduce the number of variables. Let

$$r_n(P) = T(\sigma_1^{(n-1)}, \dots, \sigma_{n-1}^{(n-1)})$$

(by the inductive assumption). Now consider the polynomial

$$P - T\left(\sigma_1^{(n)}, \dots, \sigma_{n-1}^{(n)}\right).$$

We know that r_n maps this polynomial to 0. But the kernel of r_n is generated by x_n, so then

$$x_n \mid P - T\left(\sigma_1^{(n)}, \dots, \sigma_{n-1}^{(n)}\right).$$

Since the RHS, it then follows that each x_i divides it; but by unique factorization, this means

$$x_1 \cdots x_n \mid P - T\left(\sigma_1^{(n)}, \dots, \sigma_{n-1}^{(n)}\right).$$

So then we can write

$$P - T\left(\sigma_1^{(n)}, \dots, \sigma_{n-1}^{(n)}\right) = \sigma_n \cdot Q,$$

where Q is a symmetric polynomial of smaller degree. But $Q = S(\sigma_1, \dots, \sigma_n)$ by the inductive assumption, so

$$P = S(\sigma_1, \dots, \sigma_n) + T(\sigma_1, \dots, \sigma_n),$$

as desired. □

This is one possible proof, emphasizing the inductive structure; but in applications, the proof won't matter that much.

33.2 The Discriminant

By Theorem 33.1, we can write

$$\prod_{i<j}(x_i - x_j)^2 = \Delta_n(\sigma_1, \dots, \sigma_)$$

for some polynomial Δ_n (since the LHS is a symmetric polynomial).

Definition 33.3

The **discriminant** of a polynomial $P(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_0$ is

$$D = \Delta_n(-a_{n-1}, a_{n-2}, \ldots, (-1)^n a_0).$$

In particular, we see that $D = 0$ if and only if P has a multiple root.

Example 33.4

We can calculate the discriminant explicitly when P has low degree — for $P(x) = x^2 + bx + c$ we have $D = b^2 - 4c$, while for $P(x) = x^3 + px + q$ we have $D = -4p^3 - 27q^2$.

Proof. We proved this last time, but we'll outline the proof of the second statement again. Degree considerations give that $D = ap^3 + bq^2$ for some a and b. Then we can take $P(x) = x^3 - x$ (which has discriminant 4) to get that $a = -4$, and $P(x) = (x-1)^2(x+2)$ (which has discriminant 0) to get that $b = -27$. □

Student Question. *How did we show that $D = ap^3 + bq^2$?*

Answer. *To simplify the formulas, we assumed that $\sigma_1 = 0$, so we're trying to compute $\Delta_3(0, p, -q)$. But Δ_3 is homogeneous of degree 6, as a polynomial in the x_i; meanwhile σ_i is homogeneous of degree i. We only have σ_2 (of degree 2) and σ_3 (of degree 3), and the only way to make 6 from 2's and 3's is $2+2+2$ and $3+3$, so the only possible terms we can have are σ_2^3 and σ_3^2.*

Student Question. *Does this argument only work when $\sigma_1 = 0$?*

Answer. *Yes — in the general case, there is still a formula for Δ_3, but it's longer. But the case $\sigma_1 = 0$ is actually enough for practical purposes, since it's possible to reduce any cubic to this form (by shifting the variable).*

We'll now get to the role of the discriminant in Galois theory. We can also consider

$$\delta_n(x_1, \ldots, x_n) = \prod_{i<j}(x_j - x_i),$$

so $\Delta_n = \delta_n^2$. Note that δ_n is not symmetric — if we swap x_i and x_{i+1}, then this swaps the sign of δ_n. This means

$$\delta\left(x_{\sigma(1)}, \ldots, x_{\sigma(n)}\right) = (-1)^{\text{sgn}(\sigma)}\delta(x_1, \ldots, x_n),$$

so they have the same sign if σ is even and opposite sign if σ is odd. (Here σ denotes an arbitrary permutation of $\{1, \ldots, n\}$.)

Now let E/F be a field extension, where E is the splitting field of $P \in F[x]$. Assume that P does not have multiple roots (but it is allowed to be reducible).

By definition, this means $E = F(\alpha_1, \ldots, \alpha_n)$, where $P(x) = \prod(x - \alpha_i)$. We know that $G = \text{Gal}(E/F)$ is a subgroup of S_n, since elements of G must permute the roots of P.

Now let E/F be a field extension, where E is a splitting field of a polynomial $P \in F[x]$. Let $P(x) = \prod(x - \alpha_i)$, and assume that P doesn't have multiple roots (we don't need to assume it's irreducible).

By definition, this means $E = F(\alpha_1, \ldots, \alpha_n)$. We know that $G = \text{Gal}(E/F)$ must permute the roots α_i, and is therefore a subgroup of S_n (where we look at how it permutes those roots). Now if we let $\delta = \prod_{i<j}(\alpha_j - \alpha_i)$, we know that $\delta \in E$ and $\delta^2 \in F$. We can immediately see how G acts on δ — for any $\sigma \in G$, we know

$$\sigma(\delta) = \begin{cases} \delta & \text{if } \sigma \text{ is even} \\ -\delta & \text{if } \sigma \text{ is odd.} \end{cases}$$

In particular, this means $\delta \in F$ if and only if all permutations $\sigma \in G$ are even. (This is because F is exactly the fixed field of G, by the main theorem; so δ is fixed by all elements of G if and only if it's in F.) So the conclusion is the following:

Proposition 33.5
We have $\text{Gal}(P) \subset A_n$ if and only if the discriminant Δ of P is a square.

33.3 Cubic Polynomials

We can now apply this to a concrete situation: suppose that $n = 3$, and we know P is irreducible. There are only two transitive subgroups of S_3, which are A_3 and S_3. So these are the only options for $\text{Gal}(P)$, and we have a concrete way of distinguishing between these two cases — the Galois group is S_3 when Δ is not a square, and A_3 when Δ is a square.

Example 33.6
Find the Galois group of $P(x) = x^3 - 3x - 1$ over $\mathbb{Q}$.

Solution. The discriminant of P is

$$D = 4 \cdot 27 - 27 = 81,$$

which is square; so the Galois group is $A_3 \cong \mathbb{Z}/3\mathbb{Z}$. □

Example 33.7
Suppose F contains a cube root of unity ω; find the Galois group of $P(x) = x^3 - a$ (assuming P is irreducible).

Solution. The discriminant is $D = -27a^2$. But since $\omega \in F$, then -27 is a square (since $\omega = \frac{1 \pm \sqrt{-3}}{2}$, we have that $\sqrt{-3} \in F$). So then $\text{Gal}(P) \cong \mathbb{Z}/3\mathbb{Z}$. (This is a special case of the theorem we saw last time.) □

We've now seen an effective way to find the Galois group for cubic polynomials; we'll finish by discussing how to actually solve them.

Proposition 33.8
If F contains a primitive cube root of unity ω, and E/F is a Galois extension with $\text{Gal}(E/F) = \mathbb{Z}/3$, then $E = F(\alpha)$ for some $\alpha^3 = a \in F$.

The proof we'll give is constructive, and if we explicitly write out the construction, this leads to Cardano's Formula for the solutions to a cubic (which was actually published in 1545).

Proof. Let σ be a generator for $\text{Gal}(E/F)$. It suffices to find $\alpha \in E$ such that $\sigma(\alpha) = \omega\alpha$ or $\omega^2\alpha$ — then we have $\sigma(\alpha^3) = \alpha^3$, and since σ generates the Galois group, this means *all* elements of the Galois group fix α^3, so $\alpha^3 \in F$. Meanwhile, the Galois group does not fix α itself; so the degree of α is 3. Since the degree of the *extension* is 3 as well, this means $E = F(\alpha)$.

Pick some $\beta \in E$ which is not in F, and let

$$\alpha_1 = \beta + \omega\sigma(\beta) + \omega^2\sigma^2(\beta),$$
$$\alpha_2 = \beta + \omega^2\sigma(\beta) + \omega\sigma^2(\beta).$$

Then it's clear that $\sigma(\alpha_1) = \omega^2\alpha_1$ and $\sigma(\alpha_2) = \omega\alpha_2$, so it suffices to check that one of α_1 and α_2 is nonzero. But otherwise, $(\beta, \sigma(\beta), \sigma^2(\beta))$ would be a solution to the system of linear equations

$$a + \omega b + \omega^2 c = a + \omega^2 b + \omega c = 0.$$

Then orthogonality of characters for $\mathbb{Z}/3\mathbb{Z}$ (from the representation theory of cyclic groups) shows that the only solution is $a = b = c$. But then $\sigma(\beta) = \beta$, which contradicts the fact that $\beta \notin F$ (since if σ fixed β, then the entire Galois group would fix β). So one of α_1 and α_2 must be nonzero. □

Note 33.9

The same proof works with 3 replaced with any prime; and with a bit more work, it can be generalized to any n.

This can be used to prove the converse of the theorem from last class — last class, we saw that any radical extension is solvable. But this shows that any extension with a solvable Galois group is radical.

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