31 Applications of the Galois Correspondence

31.1 Review

Last class, we saw that if E/F is a Galois extension and $G = \mathrm{Gal}(E/F)$, then there is a correspondence between subgroups $H \subset G$ and their fixed fields $E^H \subset E$. We saw that in the tower of extensions $E/E^H/F$, the top extension E/E^H is always Galois, with Galois group H. Meanwhile, E^H/F is not always Galois; but it's Galois if and only if H is normal, and in that case $G/H = \mathrm{Gal}(E^H/F)$ (so in some sense, the left-hand side makes sense if and only if the right-hand side does):

Proposition 31.1
If $K = E^H$, then K/F is Galois if and only if K is invariant under all $g \in G$, which occurs if and only if H is normal.

Student Question. *What does it mean that K is invariant under all $g \in G$?*

Answer. *This means that for any $g \in G$, we have $x \in K$ if and only if $g(x) \in K$. In other words, $g(K) = K$. (So each g permutes the elements of K; this doesn't mean that g fixes each element of K.)*

Student Question. *Did we prove the second equivalence (that K is invariant if and only if H is normal)?*

Answer. *At the end of last class — it follows from the correspondence being natural, and therefore compatible with the action of G. More precisely, if H corresponds to K, then gHg^{-1} corresponds to $g(K)$ (the action by g on subfields corresponds to the action by g on subgroups via conjugation — this is unsurprising, since conjugation is the natural action by group elements on subgroups). From this, we see that $g(K) = K$ if and only if $gHg^{-1} = H$.*

Then ghg^{-1} fixes $g(x)$ if and only if h fixes x — checking this is easy, as $ghg^{-1}(g(x)) = gh(x)$.

31.2 Cyclotomic Extensions

The main theorem can be used to answer our question about ruler and compass constructions:

Proposition 31.2
If $p = 2^k + 1$ is a Fermat prime, then a regular p-gon can be constructed by a compass and straightedge.

Proof. Let ζ be a pth root of unity. Then it suffices to show that $\mathbb{Q}(\zeta)$ can be obtained by iterating quadratic extensions — if we let $E = \mathbb{Q}(\zeta)$, then it suffices to show there exists a tower of subfields

$$\mathbb{Q} = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_n = E,$$

such that $[F_i : F_{i-1}] = 2$ for all i. Quadratic extensions can always be obtained by extracting the square root of some element; so this would mean we can obtain $\mathbb{Q}(\zeta)$ by starting with $\mathbb{Q}$ and successively applying arithmetic operations and square roots.

This is fairly clear from the Galois correspondence. We saw earlier that

$$\mathrm{Gal}(E/\mathbb{Q}) = (\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} = \mathbb{Z}/2^k\mathbb{Z}.$$

We can now write

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset \{0\},$$

where $G_1 = 2\mathbb{Z}/2^k\mathbb{Z}$, $G_2 = 4\mathbb{Z}/2^k\mathbb{Z}$, and so on. Then $G_i/G_{i+1} \cong \mathbb{Z}/2\mathbb{Z}$ for all i.

We can then take F_i to be the fixed field of G_i. We saw that the correspondence reverses inclusion, and we know how degrees correspond — we have $[E : F_i] = 2^i$ for each i, which implies that $[F_i : F_{i-1}] = 2$, as desired. $\square$

Example 31.3
Describe the first step in this construction (to find F_1).

Solution. We want to write down a quadratic extension of $\mathbb{Q}$. We know F_1 is the fixed field of G_1, and G_1 consists of the even residues in the language of $\mathbb{Z}/2^k\mathbb{Z}$; converting back to the language of $(\mathbb{Z}/p\mathbb{Z})^\times$, then G_1 consists of the squares (or *quadratic residues*) in $\mathbb{Z}/p\mathbb{Z}$ — elements of the form $a = b^2$ for some $b \neq 0$.

Suppose $\zeta = \exp(2\pi i/p)$, and let

$$\alpha = \sum_{a \in \mathrm{QR}} \zeta^a$$

(summing over all $(p-1)/2$ quadratic residues mod p — for example, if $p = 5$, then $\alpha = \zeta + \zeta^4$). It's clear that α is fixed by G_1, since multiplying all a by a quadratic residue only permutes them.

We also want to find its Galois conjugate β. To do that, we apply an element of the Galois group *not* in G_1, which gives

$$\beta = \sum_{b \in \mathrm{NQR}} \zeta^b$$

(summing over all quadratic nonresidues mod p — for example, if $p = 5$, then $\alpha = \zeta^2 + \zeta^3$.) We now want to compute the quadratic equation that α satisfies. We know

$$\alpha + \beta = \zeta^1 + \zeta^2 + \cdots + \zeta^{p-1} = -1.$$

On the other hand, we can compute

$$\alpha\beta = \sum n_c \zeta^c,$$

where n_c is the number of ways to write $a + b = c$ where a is a quadratic residue, and b is a quadratic nonresidue.

This is a combinatorial problem, which we can solve — first, $n_0 = 0$, since -1 is a square (this means if a is a square, so is $-a$, so we can't have $a + b = 0$ where a is square and b isn't). On the other hand, we claim that $n_1, \ldots, n_{p-1}$ are all equal — for any c and c', we can write $c' = tc$ for some t (since $\mathbb{Z}/p\mathbb{Z}$ is a field). If t is a square, then we can get a bijection between (a, b) with sum c and sum c', by multiplying by t. Meanwhile, if t is not a square, then we can get a bijection by multiplying and swapping — given (a, b) with sum c, we can take (tb, ta) with sum c'. This means $n_c = n_{c'}$. Finally, we have $n_0 + \cdots + n_{p-1} = ((p-1)/2)^2$, since this is the number of ways to choose a summand from each of α and β. This means

$$n_c = \begin{cases} \frac{p-1}{4} & \text{if } c \neq 0 \\ 0 & \text{if } c = 0, \end{cases}$$

so then our sum is

$$\alpha\beta = \sum_{c=1}^{p-1} \frac{p-1}{4} \zeta^c = -\frac{p-1}{4}.$$

This means our quadratic equation is

$$\alpha^2 + \alpha - \frac{p-1}{4} = 0 \implies \alpha = \frac{-1 \pm \sqrt{p}}{2}.$$

So we have $F_1 = \mathbb{Q}(\sqrt{p})$. ∎

Note 31.4
This argument works for any prime $p \equiv 1 \pmod 4$, meaning that the quadratic extension of $\mathbb{Q}$ contained in $\mathbb{Q}(\zeta_p)$ is still $\mathbb{Q}(\sqrt{p})$. Meanwhile, when $p \equiv 3 \pmod 4$, we instead get $\mathbb{Q}(\sqrt{-p})$.

The description of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ can be generalized to apply to all n (meaning ζ is an nth root of unity), not just primes.

Definition 31.5
The nth **cyclotomic polynomial** Φ_n is the monic polynomial in $\mathbb{Z}[x]$ whose roots are exactly the primitive nth roots of unity.

We then have
$$x^n - 1 = \prod_{d \mid n} \Phi_d(x).$$
This is because the roots of $x^n - 1$ are all elements whose order in $\mathbb{C}^\times$ divides n, and the right-hand side groups such terms by their order d).

This formula lets us compute Φ_n.

Example 31.6
We have $\Phi_1(x) = x - 1$, and
$$\Phi_p(x) = x^{p-1} + \cdots + 1.$$
We can also compute other polynomials $\Phi_n(x)$, such as
$$\Phi_{12}(x) = x^4 - x^2 + 1.$$

The cyclotomic polynomials don't always have all coefficients 0 or ± 1, but the smallest counterexample is 105 (the smallest product of three distinct odd primes). But from this formula, it's easy to show by induction that all Φ_n have integer coefficients.

Fact 31.7
Φ_n is irreducible in $\mathbb{Q}[x]$.

We proved this fact for primes; we won't prove it for general n, since the proof is longer.

Also note that $\deg(\Phi_n)$ is the number of elements of order n in the additive group $\mathbb{Z}/n\mathbb{Z}$, which is $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$. If $n = p_1^{d_1} \cdots p_k^{d_k}$, we have the explicit formula
$$\varphi(n) = \prod_i (p_i^{d_i} - p_i^{d_i - 1}).$$

Now we have
$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n),$$
and $\mathbb{Q}(\zeta)$ is a splitting field (for the same reason as in the prime case — all roots of Φ_n are powers of ζ). By the same reasoning as the prime case, we then have
$$\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^*.$$
Note that this is not necessarily cyclic — in fact, it's not cyclic unless n is a prime power or twice a prime power (and it's also not cyclic if $n \geq 8$ is a power of 2). It'll be the *product* of cyclic groups (since it's still abelian), but there will usually be multiple factors of even order in this product.

31.3 Kummer Extensions

We'll now consider extensions E/F where $E = F(\alpha)$ for some α such that $\alpha^n \in F$ for a positive integer n (and $\alpha \neq 0$). Assume that F contains all nth roots of unity, meaning that
$$\mu_n(F) = \{x \in F \mid x^n = 1\}$$
has exactly n elements (and therefore $\mu_n(F) \cong \mathbb{Z}/n\mathbb{Z}$); this is equivalent to requiring that F contains a primitive nth root of 1.

Our main example is over characteristic 0, but this can be done over characteristic p as well, with the additional requirement that $p \nmid n$.

Proposition 31.8
In this case E/F is Galois, and
$$\mathrm{Gal}(E/F) \cong \mathbb{Z}/m\mathbb{Z}$$
for some $m \mid n$. In fact, if $x^n - a$ is irreducible in $F[x]$, then $m = n$.

Proof. We have
$$x^n - a = \prod(x - \zeta^i \alpha),$$
where $0 \le i \le n-1$ and ζ is a primitive nth root of 1 (since all $\zeta^i\alpha$ are roots of $x^n - a$, and they are all distinct). So if we're given one root of $x^n - a$, then all possible roots are obtained by multiplication by roots of unity (which are in F). So E is the splitting field of $x^n - a$.

Now an element $\sigma \in G = \mathrm{Gal}(E/F)$ is uniquely determined by $\sigma(\alpha)$, which must be $\zeta^i\alpha$ for some i. For each i, let σ_i be the element in G such that $\sigma_i(\alpha) = \zeta^i\alpha$, if it exists (the element σ_i doesn't necessarily exist for all i).

It's clear that
$$\sigma_i\sigma_j(\alpha) = \sigma_i(\zeta^j\alpha) = \zeta^{i+j}\alpha = \sigma_{i+j}(\alpha)$$
(because $\zeta \in F$, so σ must fix it). So then $\sigma_i\sigma_j = \sigma_{i+j}$. This means G is isomorphic to a subgroup in $\mathbb{Z}/n\mathbb{Z}$, and every such subgroup must be of the form $\mathbb{Z}/m\mathbb{Z}$ where $m \mid n$.

In fact $m = \deg(E/F)$, so $m = n$ if and only if $x^n - a$ is irreducible. (When $x^n - a$ to be reducible, this fails in a trivial way — then a *smaller* power of α is in F.) $\square$

31.4 Quintic Equations

Using these ideas, we can obtain the famous application of Galois theory to the impossibility of solving a general polynomial equation of degree at least 5.

Definition 31.9
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 all i, G_i is a normal subgroup of G_{i-1} and G_{i-1}/G_i is abelian.

The main idea of the proof is the following two propositions:

Proposition 31.10
Given an extension E/F and some $\alpha \in E$ such that α can be obtained from elements of F by arithmetic operations (addition, subtraction, multiplication, and division) and extracting arbitrary nth roots (where we're allowed to choose any of the possible nth roots), then α lies in a Galois extension of F with a solvable Galois group.

Proposition 31.11
S_n is not solvable for $n \ge 5$.

The first proposition essentially follows from what we've already discussed — we'll discuss it in more detail next class, but the idea is to first add the roots of unity; then when we extract a nth root, we get an extension with cyclic Galois group. Then when we extract nth roots repeatedly, we get a sequence of subgroups with abelian quotients. Meanwhile, the second is an elementary finite group argument.

Corollary 31.12
A root of a polynomial P of degree 5 with Galois group S_5 cannot be expressed through the rational numbers in radicals.

Saying the root can't be expressed in radicals is shorthand for the longer sentence from earlier — it simply means that it can't be obtained by arithmetic operations and extracting nth roots.

So this means not only is there no universal formula for the roots using radicals (as there is in lower degrees), there isn't even a way to write down the roots of a *specific* polynomial.

Proof of corollary. If it were possible to express all roots of P in radicals, then the splitting field K of P would be contained in a Galois extension of $\mathbb{Q}$ with solvable Galois group G. But then we have an onto homomorphism

$G \twoheadrightarrow \mathrm{Gal}(K/\mathbb{Q}) = S_5$. But the quotient of a solvable group is again solvable; so this would imply S_5 is solvable, contradiction. $\square$

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