Lecture 1-15: The Primitive Element Theorem and the Galois correspondence

January 15, 2025

Continuing from last time, I now head toward a bijection between subgroups of a Galois group and intermediate fields in the corresponding Galois extension. But before I do this, I need to prove a result of considerable interest in its own right.

The Primitive Element Theorem (p. 595)

Let K be a finite separable extension of F. Then K is simple, so that there is $\alpha \in K$ with $F(\alpha) = K$.

Proof.

If F and K are finite, this is clear, for we can take α to be a cyclic generator of the multiplicative group of K. So assume that F is infinite. We know that K is finitely generated over F; by induction on the number of generators it suffices to show that any subfield $K' = F(\beta, \gamma)$ of K generated over F by two elements is in fact generated by only one element. We know by the last result last time that there are only finitely many intermediate fields between F and the Galois closure $\overline{K'}$ of K', so only finitely many intermediate fields between F and K'. Letting c_1, c_2 run over F, it follows that two of the fields $F(\beta + c_1\gamma), F(\beta + c_2\gamma)$ coincide. But then $(c_2 - c_1)\gamma$ and γ both lie in both fields $K(\beta + c_i\gamma)$ and both of these fields coincide with K', as desired. $\square$

Next I prove a result also of independent interest which says that any finite group of automorphisms acting on a field is the Galois group of that field over the fixed field.

Theorem 9, p. 570

Let G be a finite group of automorphisms of a field K. Then K is Galois over the fixed field K^G with Galois group G; in particular, $[K : K^G] = |G|$.

Proof.

Let $\alpha \in K$ and let $\alpha = \alpha_1, \ldots, \alpha_m$ be the distinct conjugates of α under G. Since G permutes the α_i, it follows that the coefficients of the polynomial $p = \prod_{i=1}^{m}(x - \alpha_i)$ are fixed by G and clearly $p(\alpha) = 0$. Hence the elements of K are at least algebraic and separable over K^G. Choose $\beta \in K$ of maximal degree d over K^G; then $d \leq n = |G|$. Given any $\alpha \in K$, the Primitive Element Theorem shows that $K^G(\alpha, \beta)$ is generated by a single element γ, of degree at most d by choice of β; but $K^G(\beta)$ already has degree d, so $\alpha \in K^G(\beta)$ and β generates K over K^G. Thus K is finite over K^G, of degree at most n; but G is a group of n distinct automorphisms of K fixing K^G. Hence $[K : K^G] = n$ and β has n distinct conjugates $\beta_1, \ldots, \beta_n$ under G. Finally, K is the splitting field of the separable polynomial $\prod(x - \beta_i)$ over K^G, so K is Galois over K^G with Galois group G. □

The payoff is

The Galois correspondence: Theorem 14, p. 574

Let K be finite and Galois over K, with Galois group G. Then the map $H \leftrightarrow K^H$ establishes an order-reversing bijection between subgroups H of G and subfield of K containing F. K is also Galois over any intermediate field K^H, with Galois group H and degree $|H|$.

We have already seen that every field between F and K is K^H for some subgroup H; the previous result shows that H is the Galois group of K over K^H and so is uniquely determined by K^H. As noted above, it is clear that the correspondence is order-reversing.

As an immediate corollary we get

Galois correspondence II

With notation as above, two intermediate fields $K^H, K^{H'}$ are conjugate by $g \in G$ if and only if the subgroups H and H' are conjugate by g. A field K^H is preserved (as a set) by all $g \in G$ if and only if H is normal in G, in which case the Galois group of K^H over F is the quotient group G/H.

In general the field K^H is preserved by $g \in G$ exactly when g lies in the normalizer $N_G H$ of H in G; the quotient group $N_G H/H$ is the automorphism group of K^H over F. We also have $[K^H : F] = [G : H]$, the index of H in G, whether or not H is normal in G. It is easy to check that the composite $K^H K^{H'}$ of the subfields fixed by subgroups H, H' is just the subfield $K^{H \cap H'}$ fixed by $H \cap H'$.

Example

Let K be the splitting field $x^4 - 2$ over $\mathbb{Q}$. This field is generated over $\mathbb{Q}$ by $\alpha = 2^{1/4}$, the positive real fourth root of 2, and i; since $x^4 - 2$ is irreducible over $\mathbb{Q}$ while i is not real, we see that $[K : \mathbb{Q}] = 8$. It follows that $x^4 - 2$ is irreducible over $\mathbb{Q}[i]$ as well as $\mathbb{Q}$. Thus there is an automorphism r of K fixing $\mathbb{Q}$ and i and sending α to αi (one of the other roots of its minimal polynomial). One checks directly that $r^4 = 1$. Then complex conjugation preserves K; denote its restriction to K by s. One easily checks that $s^2 = 1, srs = r^3 = r^{-1}$. But these are exactly the defining relations for D_4, the dihedral group of order 8. Thus the Galois group of K over $\mathbb{Q}$ is D_4. Note that one might have expected this result, given that the four roots of $x^4 - 2$ in the complex plane happen to be the vertices of a square, whose geometric symmetries happen to match the algebraic symmetries of the roots exactly.

Example

Continuing this example, we note that there are three subgroups of D_4 of order 4, all of them normal, namely the cyclic one $\langle r \rangle$ consisting of all the reflections and the Klein four-groups generated by the central rotation r^2 and either s or sr. These groups correspond respectively to the Galois extensions $\mathbb{Q}[i], \mathbb{Q}[\sqrt{2}]$, and $\mathbb{Q}[\sqrt{2}i]$ of $\mathbb{Q}$. Next, there are five subgroups of order 2, four of them generated by a reflection sr^i and the other by r^2. Only the last of these is normal; it corresponds to the Galois extension $\mathbb{Q}[\sqrt{2}, i]$. The others correspond to $\mathbb{Q}[\alpha], \mathbb{Q}[\alpha i], \mathbb{Q}[\alpha\zeta]$, and $\mathbb{Q}[\alpha i\zeta]$, where $\zeta = e^{2\pi/8}$ is a primitive 8th root of 1 (which lies in K). Finally, of course, there is the trivial subgroup 1, corresponding to K and D_4, corresponding to $\mathbb{Q}$.

The coincidence of geometric and algebraic symmetries in this example is however misleading. For example, the Galois group of the very similar polynomial $x^5 - 2$ over $\mathbb{Q}$ is *not* the dihedral group D_5 of order 10. Here the splitting field contains the cyclotomic field $\mathbb{Q}[e^{2\pi i/5}]$, which has degree 4 over $\mathbb{Q}$, and the field $\mathbb{Q}[2^{1/5}]$, which has degree 5, so its degree is 20. The Galois group is the semidirect product of the cyclic group $\mathbb{Z}_5$ and its automorphism group $\mathbb{Z}_5^*$ of multiplicative units, which is cyclic of order 4. The roots of $x^5 - 2$ form a regular pentagon in $\mathbb{C}$, but half of the automorphisms in the Galois group fail to be symmetries of this pentagon.

On pp. 577–581 of the text, the example of the splitting field K of $x^8 - 2$ over $\mathbb{Q}$ is worked out in great detail. We saw earlier that this field has degree 16 over $\mathbb{Q}$, so one might expect the Galois group to be dihedral of order 16. This is almost but not quite the case. We still get an automorphism r of K sending the real positive root $\beta = 2^{1/8}$ to $\beta\zeta$ and fixing i, with ζ as above, and we still have the conjugation automorphism s, but now it turns out that $srs = r^3$ rather than $srs = r^{-1}$. The Galois group is defined by this relation together with $r^8 = s^2 = 1$; it is called *quasi-dihedral*.

Returning to the constructibility of regular n-gons one last time, we now see that if n is the product of a power of 2 and distinct Fermat primes, then the cyclotomic field $L = \mathbb{Q}[e^{2\pi i/n}]$ has degree a power of 2 over $\mathbb{Q}$, so that its Galois group is a 2-group. We know that any such group admits a chain of normal subgroups, of index 2 in the next bigger one, so we can get to L from $\mathbb{Q}$ by a sequence of quadratic extensions. Hence the real and imaginary parts of $e^{2\pi i/n}$ are both constructible with compass and straightedge, as is the regular n-gon. Gauss proved this by a direct calculation, without the benefit of Galois theory. Later a German professor spent ten years writing out an explicit construction of the regular 65537-gon, which is still lovingly preserved under glass.

Next time I will use Galois theory to address the problem that originally motivated Galois, namely to decide given a polynomial p over $\mathbb{Q}$ whether there is an expression for its roots using only arithmetic operations and mth roots of numbers.