Lecture 1-24: Galois groups over $\mathbb{Q}$

January 24, 2025

You have seen that every finite extension of a finite field is Galois with cyclic Galois group, generated by a power of the Frobenius automorphism send x to x^p (where p is the characteristic of the field). This very simple behavior can be exploited to produce explicit permutations in the Galois group of a polynomial over $\mathbb{Q}$.

Before stating the main result, I need an auxiliary one, of interest in its own right. This will be used later to prove something called the Normal Basis Theorem.

Corollary 8, p. 570

If $\sigma_1, \ldots, \sigma_n$ are distinct multiplicative homomorphisms of an integral domain D into a field K, then they are linearly independent over K as functions on D.

Proof.

Suppose we had a dependence relation $\sum_{i=1}^{m} k_i\sigma_i(x) = 0$ with the k_i in K. Of all such relations, choose one with the minimum number m of nonzero terms; then clearly $m > 1$. Since $\sigma_1 \neq \sigma_2$, there is $d \in D$ with $\sigma_1(d) \neq \sigma_2(d)$. Replacing x by dx, we get $\sum_{i=1}^{m} k_i\sigma_i(d)\sigma_i(x) = 0$. Subtracting a suitable multiple of the first equation from this one, we get another nontrivial dependence relation with fewer terms, a contradiction. $\square$

The main result on permutations in the Galois groups is then

Theorem, p. 640

Let $f \in \mathbb{Z}[x]$ be monic of degree n and let p be a prime such that the reduction f_p of f modulo p has no multiple roots. Suppose that f_p is the product of irreducible polynomials of degrees $n_1, \ldots, n_r$ in $\mathbb{Z}_p[x]$, so that $\sum n_i = n$. Then the Galois group G of f has a permutation of the roots that is the product of disjoint cycles of lengths $n_1, \ldots, n_r$.

Before proving this result, I give an example showing how it can be used. Since finite fields of all prime powers p^n exist and are simple extensions of $\mathbb{Z}_p$, it follows for any n that there are monic irreducible polynomials $p_n \in \mathbb{Z}_p[x]$ of degree n. Given n, choose $q_2 \in \mathbb{Z}_2[x]$ monic irreducible of degree n, $q_3 \in \mathbb{Z}_3[x]$ monic irreducible of degree $n-1$, and $q_p \in \mathbb{Z}_p[x]$ monic irreducible of degree 2, where p is a prime larger than $n-2$.. By the Chinese Remainder Theorem, there is a monic $f \in \mathbb{Z}[x]$ of degree n whose reductions mod $2, 3$, and p are q_2, xq_3, and $x(x+1)\ldots(x+n-3)q_p$, respectively. Then f is irreducible in $\mathbb{Z}[x]$ with separable reductions mod $2, 3$, and p, and the Galois group of f over $\mathbb{Q}$ contains an n-cycle, an $(n-1)$-cycle, and a 2-cycle. It is an easy exercise to show that the only transitive subgroup of S_n with these properties is S_n itself. Hence for every n there is a polynomial of degree n whose Galois group over $\mathbb{Q}$ is S_n (we saw this earlier if n is prime).

Proof.

Let D be the subring of the splitting field E of f over $\mathbb{Q}$ generated by the roots r_i of f. I first claim that there are homomorphisms ψ of D into the splitting field E_p of f_p over $\mathbb{Z}_p$. To prove this, note first that since the r_i are integral over $\mathbb{Z}$, the subring D is a finitely generated $\mathbb{Z}$-submodule, which is torsion-free and therefore free. A $\mathbb{Z}$-basis of D then spans a subring containing the r_i over $\mathbb{Q}$, which must be all of E, by an easy argument (the rank of D over $\mathbb{Z}$ coincides with the dimension N of E over $\mathbb{Q}$). Now consider pD: this is an ideal of D and $|D/pD| = p^N$. Enlarge pD to a maximal ideal M of D. $\square$

Proof.

Then the quotient $K = D/M$ is a field, necessarily of characteristic p since $M \supset pD$; we have $|K| = p^m$ for some $m \leq N$. The images of $\bar{r}_i$ of the r_i in K generate it over its prime subfield $\mathbb{Z}_p$ and the product of the factors $x - \bar{r}_i$ is the reduction f_p of f, so K is a splitting field of f_p over $\mathbb{Z}_p$, necessarily isomorphic to E_p. Combining the canonical map from D onto $K = D/M$ with the isomorphism from K to E_p, we get a homomorphism from D to E_p, as claimed. Any such homomorphism necessarily maps the set of roots r_i of f bijectively onto the corresponding set of roots $\bar{r}_i$ of f_p. Now for any $g \in G$ and homomorphism $\psi : D \to E_p$, the composite ψg is another homomorphism from D to E_p, distinct from ψ if $g \neq 1$ since g permutes the r_i nontrivially. In this way we get $N = |G|$ distinct homomorphisms from D to E_p. □

Proof.

But now Corollary 8 tells us that these N homomorphisms are linearly independent over E_p; by counting dimensions we see that they must form a maximal E_p-linearly independent set of such homomorphisms (since D is free of rank N over $\mathbb{Z}$). Thus if ψ is one homomorphism from D to E_p then the composites ψg exhaust all the homomorphisms from D to E_p. The Frobenius map ϕ sending $x \in E_p$ to x^p acts on the $\bar{r}_i$ as the product of disjoint cycles of lengths $n_1, \ldots, n_r$ and the composite $\phi\psi$ is a homomorphism from D into E_p. Writing the homomorphism $\phi\psi$ as ψg for some $g \in G$, we see that g likewise permutes the r_i as the product of disjoint cycles of these lengths, as claimed. □

Thus the symmetric group S_n is a Galois group over $\mathbb{Q}$ for every n. A famous problem called the Inverse Galois problem asks which other finite groups H are Galois groups over $\mathbb{Q}$. The answer to this is still unknown, though it is widely believed that any finite group H has this property. (Note that the Galois correspondence shows that any subgroup of some S_n is a Galois group over some finite extension of $\mathbb{Q}$, but not over $\mathbb{Q}$ itself.) A theorem of Hilbert proved in the nineteenth century shows that any alternating group A_n is also a Galois group over $\mathbb{Q}$; more recently, a deep result of Shafarevich shows that any finite solvable group is a Galois group over $\mathbb{Q}$. Roughly speaking, this last result says that even when it is possible to solve a polynomial in $\mathbb{Q}[x]$ by radicals, it can be arbitrarily hard to do so.

There is a simple solution to the inverse Galois problem for any finite abelian group A. This is because an easy consequence of a homework problem in the first week, together with the classification of finite abelian groups, shows that any such group A is a homomorphic image of the multiplicative group $\mathbb{Z}_n^*$ of units in $\mathbb{Z}_n$ for some n; recall that this is the Galois group of the cyclotomic extension $Q_n = \mathbb{Q}[e^{2\pi i/n}]$ of $\mathbb{Q}$. By the Galois correspondence, then, A is the Galois group of a suitable extension of $\mathbb{Q}$ lying in Q_n, and in fact the Galois group of any normal extension lying in Q_n is a quotient of $\mathbb{Z}_n^*$ and so is abelian. A remarkable theorem due to Kronecker and Weber asserts that, conversely, any abelian extension of $\mathbb{Q}$, that is, any normal extension with abelian Galois group, lies in $\mathbb{Q}_n$ for some n.

This last result is especially surprising since many abelian extensions of $\mathbb{Q}$ (e.g $\mathbb{Q}[\sqrt{78}]$ seem to have nothing to do with cyclotomic fields. An advanced branch of number theory called class field theory seeks among other things to characterize the abelian extensions of fixed finite extensions E of $\mathbb{Q}$. This is tricky even for cyclic extensions, since cyclic extensions of order m of a field without a full complement of mth roots of 1 need not look anything like mth root extensions.

There is a field related to $\mathbb{Q}$ for which the inverse Galois problem is known to have a positive answer for all finite groups G. This is the field $R = \mathbb{C}(z)$ of rational functions in one variable over $\mathbb{C}$; note that even though $\mathbb{C}$ itself does not admit any proper finite extensions, by the Fundamental Theorem of Algebra, the field R certainly does. What makes it more tractable than $\mathbb{Q}$ for the inverse Galois problem is its deep connection to topology, more specifically to the Riemann sphere.

This sphere, often denoted $\mathbb{CP}^1$, is obtained from $\mathbb{C}$ by adding a single point called ∞ and putting a topology on it by declaring that the open neighborhoods of ∞ are the unions of ∞ and the open subsets of $\mathbb{C}$ containing all numbers of norm greater than N for some $N > 0$. It is a compact space that is simply connected as it stands, but by removing n points from it we get another space with a very large fundamental group, namely the free group F_n on n generators. Thus there is a very large collection of covering spaces of this last space; by exploiting these covering spaces, we (indirectly) get a finite extension of $\mathbb{C}(z)$ with an arbitrary finite group as Galois group.