Lecture 3-10: Review, part I

March 10, 2025

I will spend the entire last week on review of the course material, beginning with Galois theory today. I will concentrate on *statements* of theorems throughout; don't worry about memorizing their proofs, but be able to apply the theorems.

If K and L are fields with $K \subset L$, then we say that L is an extension of K; its degree is $[L : K] = \dim_K L$, the dimension of L as a vector space over K. We are primarily interested here in the case where $[L : K]$ is finite. If M is a field between K and L then we have $[L : K] = [L : M][M : K]$; in particular, if L is finite over M and M is finite over K, then L is finite over K. Set $G = \mathrm{Aut}_K(L)$, the group of automorphisms of L fixing every element of K.

The nicest finite extension are the Galois ones, where the order $|G|$ of G equals the degree $[L : K]$; in general, we have $|G| \leq [L : K]$. In this case we call G the Galois group of L over K. A finite extension is Galois if and only if it is normal and separable. It is normal if and only if it is a splitting field of some nonconstant polynomial $p \in K[x]$, so that it is generated as a field (or as a ring) by K and the roots of p and p splits as the product of linear factors in $L[x]$. Equivalently, it is normal if and only if every irreducible polynomial in $K[x]$ with one root in L splits completely in $L[x]$. It is separable (algebraic) if and only if every $y \in L$ satisfies a polynomial in $K[x]$ with distinct roots in L. All extensions are separable in characteristic 0, but not in characteristic $p > 0$ in general; in characteristic p, the splitting field of an irreducible polynomial q is separable over K if and only if q is *not* a polynomial in x^p. Any finite separable extension is primitive in the sense that it is generated as a ring by a single element over the basefield.

If L is finite and Galois over K then we can completely characterize the fields between K and L in terms of the subgroups of its Galois group G; in particular, there are only finitely many such fields. More precisely, we have the Galois correspondence, which asserts that there is an inclusion-reversing bijection between subgroups of G and fields M with $K \subset M \subset L$. It sends a subgroup H to the subfield L^H of elements fixed by H in L, and a field M to the Galois group H of L over M, which is a subgroup of G. Two fields M, M' are conjugate under the action of G if and only if their corresponding subgroups H, H' are conjugate in G; in particular, a field M is normal over K if and only if its subgroup H is normal in G, in which case the Galois group of M over K is the quotient G/H.

The Galois group of the splitting field of a polynomial p is often called the Galois group of p for short (over the basefield K). Its elements permute the roots of p and so may be thought of as elements of the symmetric group S_n, where n is the degree of p. Thus one can use group-theoretic properties of permutations to compute Galois groups in certain cases. For example, if $p \in \mathbb{Q}[x]$ is irreducible of prime degree q and has exactly $q-2$ real roots, then its Galois group G is all of S_q. This follows since G must contain an element of order q, since it acts transitively on the q roots of p; but the only elements of S_q of order q are tht q-cycles. G also contains a transposition of two roots, corresponding to complex conjugation. Then it turns out that any q-cycle and any transposition generate all of S_q.

Fundamental examples to keep in mind include the cyclotomic fields $\mathbb{Q}[e^{2\pi i/n}]$ generated over the basefield $\mathbb{Q}$ by any primitive nth root ω_n of 1 in $\mathbb{C}$ and finite fields (necessarily of characteristic $p > 0$, regarded as extensions of the field $F_p = \mathbb{Z}_p\mathbb{Z}$ of p elements. In the first case the minimal polynomial of ω_n over $\shortparallel$ is the nth cyclotomic polynomial $\Phi_n(x) \in \mathbb{Z}[x]$, which is irreducible. The Galois group of this polynomial is $\mathbb{Z}_n^*$, the group of *multiplicative* units in $\mathbb{Z}_n$, the integers modulo n, a typical automorphism sending ω_n to ω_n^a for some a. Recall that $\mathbb{Z}_n^*$ is cyclic of order $p^m - p^{m-1}$ if $n = p^m$ is an odd prime power. In the second case there is a unique extension of F_p of degree n up to isomorphism, which is the unique field F_{p^n} of order p^n. It is the splitting field of $x^{p^n} - x$ over F_p and has cyclic Galois group of order n, generated by the Frobenius automorphism sending any x to x^p. (Also recall from last quarter that the multiplicative group $F_{[p^n}^*$ is cyclic of order $p^n - 1$, for any prime p).

The other high point of Galois theory is the Galois criterion, which asserts that a polynomial p over a field K of characteristic 0 is solvable by radicals (in the sense that there are expressions for all of its roots using only field operations, elements of K, and nth roots for some n) if and only if its Galois group G is solvable. This last condition means that there is a finite sequence $G_0 = G \supset G_1 \supset \cdots G_m = 1$ of normal subgroups G_i of G such that all quotients G_i/G_{i+1} are abelian. Since you saw last quarter that the alternating group A_n is simple for $n \geq 5$, it follows that no polynomial p of degree $n \geq 5$ whose Galois group is all of S_n or A_n is solvable by radicals. As previously observed, polynomials of any degree n exist over $\mathbb{Q}$ with Galois group S_n; no such polynomial is solvable by radicals if $n \geq 5$ (but universal radical formulas exist for the roots of any polynomial of degree $d \leq 4$ over a field of characteristic 0).

A key step in the proof ot the Galois criterion is Hilbert's Theorem 90, which asserts that a Galois extension with cyclic Galois group G of order n over a field K with n distinct nth roots of 1 is necessarily an extension by a single element α with $\alpha^n \in K$. This is used to show that if a polynomial has solvable Galois group, then it is solvable by radicals. Hilbert's Theorem 90 can be reformulated in terms of norms, as follows. Recall first that the norm $N(\alpha)$ of an element α lying in a finite Galois extension L of a field K with Galois group G is the product $\prod g\alpha \in K$ of the images of α under the elements of g, or the determinant of multiplication by α, regarded as a linear transformation from L to itself. Then Theorem 90 says that if G is cyclic and generated by g, then the elements of L of norm 1 are exactly the quotients $g\beta/\beta$ for some $\beta \in L^*$.

It is also worth remembering that the Galois correspondence can break down in various ways for non-Galois extensions, or for infinite extensions. If $L \supset K$ is not normal, then $G = \mathrm{Aut}_K L$ may have order strictly smaller than $[L : K]$, in which case there are typically too few subgroups of G to correspond to fields between K and L. Even if L is Galois over K but not finite, there may also be too many subgroups of G to correspond to intermediate fields. For example, if $K = \mathbb{Q}$ and L is generated by the square roots $\sqrt{p_i}$ of all primes $p_i \in \mathbb{Z}$, then G is an uncountable direct sum of copies of $\mathbb{Z}/2\mathbb{Z}$, but $[L : K]$ is countable, so there are more subgroups of G than even subsets of L.

Likewise even a simple transcendental extension $L = K(t)$ of an infinite field K behaves badly in the sense that many proper subgroups H of the Galois group $G = PGL_2(K)$ of L over K are such that $L^H = K$.