Lecture 1-31: Infinite Galois extensions

January 31, 2025

I now move beyond finite Galois extensions in a different way, this time looking at infinite algebraic extensions. You will see that the Galois correspondence between intermediate fields and subgroups of the Galois group again breaks down, but there is still interesting information to be gleaned form the interplay between field theory and group theory.

I begin by looking at the subfield K of $\mathbb{C}$ generated by $\sqrt{p}$ for all primes p. Clearly the degree $[K : \mathbb{Q}]$ is countably infinite; a spanning set for for K over $\mathbb{Q}$ is given by the set of $\sqrt{n}$ as n ranges over the products of distinct primes in $\mathbb{Z}$ (including the empty product, which by convention equals 1).

You will show in homework this week that the above spanning set is actually a basis: if $p_1, \ldots, p_n$ are the first n primes, then square roots of products of distinct p_i form a basis of the subfield F_n of $\mathbb{C}$ generated by the $\sqrt{p_i}$; this subfield is Galois over $\mathbb{Q}$ of degree 2^n and has Galois group the product of n copies of $\mathbb{Z}_2$..

It follows that an automorphism of K sends each $\sqrt{p_i}$ to $\pm\sqrt{p_i}$, the choice of sign being arbitrary for each i (that is, independent of the choice of sign for $j \neq i$). Hence the Galois group $G$of K over $\mathbb{Q}$, is uncountable, being the direct *product* (not sum) of countably many copies of $\mathbb{Z}_2$, or equivalently the direct sum of uncountably many copies of $\mathbb{Z}_2$.

Thus we find ourselves in exactly the opposite situation to the one observed earlier for the simple transcendental extension $F(t)$ of a finite field F: here the order of the Galois group is larger than the degree of the field extension. It is not difficult to show that there are more subgroups of G than *subsets* of K, so there cannot be a bijection between fields between $\mathbb{Q}$ and K and subgroups of G.

I will shortly indicate what one does to rectify this situation; for now I consider a different infinite Galois extension where it is easier to see what is going on. For a fixed prime p, we have a simple chain $F_1 = F_p \subset F_2 = F_{p^2} \subset \cdots \subset F_n = F_{p^{n!}} \subset \cdots$ of inclusions among the fields of orders $p, p^2, \ldots, p^{n!}, \ldots$ (recall that the fields $F_p, F_{p^2}, F_{p^3}, \ldots,$ by contrast, do *not* form such a chain). Then I can form the union P of all the fields in this chain. I define the field operations on pairs x, y of elements in it by choosing n large enough with $x, y \in F_n$ and defining $x + y, x - y, xy, x/y$ to have the values they have in F_n. This makes sense since there is a unique copy of F_n in F_m for any $n \leq m$.

Any finite extension of F_n, say of degree d, is contained in F_m if m is chosen large enough that $d|m$! Consequently P contains the splitting field of every polynomial q over any F_m, and thus the splitting field of any polynomial over itself, since any such polynomial necessarily has all coefficients in F_m for some m. Hence P is algebraically closed; it provides probably the simplest example of an algebraically closed field (though less familiar than the complex field $\mathbb{C}$). Note also that P contains a unique copy of F_{p^n}, the field of order p^n, for every n.

The Galois group H of P over its prime subfield F_p is infinite cyclic, generated as usual by the Frobenius automorphism π sending any x to x^p. The subgroups of H are of course generated by powers of π, the one generated by the nth power π^n corresponding to the subfield F_{p^n} of P. Thus we get a Galois correspondence of sorts between subfields of P and subgroups of H which is rich enough to accommodate all the finite subfields of P.

Unfortunately (or fortunately, depending on your point of view), there are many infinite proper subfields of P. For example, the fields $F_p, F_{p^2}, F_{p^4}, \ldots$ also form a single chain under inclusion, whose union P_2 could be called the quadratic closure of F_p; this union does not have any proper quadratic extension, but has many cubic ones, so that it is not all of P. Similarly, there are what could be called "*m*-fold" closures of F_p in P for all m.

The closure operations of the last slide can be massively generalized; there is a much wider variety of them starting with the rational field $\mathbb{Q}$. For example, we have the abelian closure of $\mathbb{Q}$, generated by all finite Galois extensions K with abelian Galois group; by the Kronecker-Weber Theorem mentioned earlier, this is the same as the subfield of $\mathbb{C}$ generated by $e^{2\pi i/n}$ for all integers n. We also have the solvable closure of $\mathbb{Q}$, generated by all finite Galois extensions with solvable Galois group. This is trickier to define, since such solvable extensions do not form a single chain under inclusion. Here however the composite K_1K_2 (in $\mathbb{C}$) of any two finite solvable extensions K_1, K_2 of $\mathbb{Q}$ is again solvable, so that one can in effect take the union of all such K_i, which will be a proper subfield of $\mathbb{C}$.

Finally, if L is infinite Galois over K, then a theorem due to Krull enables us to recover part of the Galois correspondence. Letting G be the Galois group of L over K, define a topology on G by declaring first that a subgroup H, or one of its cosets Hg or gH, is closed if the fixed field L^H is a finite extension of K. Then we decree that a set is open if and only if its complement is an intersection of closed sets of this type. Then one has

Theorem (Krull), p. 652

With notation as above, there is an inclusion-reversing bijection between closed subgroups of G and finite extensions of K lying in L, with an extension being normal over K if and only if the corresponding subgroup is normal in G.

Note that more subgroups of G are being excluded here than might at first be apparent. For example, the Galois group G of the extension K in the second slide is the direct product of infinitely many copies of $\mathbb{Z}_2$; as such it is a vector space over $\mathbb{Z}_2$ of uncountable dimension and thus has uncountably many subgroups of finite index. Only countably many of these correspond to fields between $\mathbb{Q}$ and K, as there are only countably many such fields.