Math 505, 1/8

We continue with the setup from last time: L is a finite Galois extension of a field K with Galois group G. We head towards the *Galois correspondence*, which establishes a bijection between subfields of L containing K and subgroups of G. Let L' be such a subfield. Then L, as the splitting field of some polynomial p over K with no multiple roots, continues to be the splitting field of the same p over L', so that L is Galois over L'. We have seen that any $\alpha \in L'$ with $\alpha \notin K$ is a root of some nonlinear polynomial q over K', all of whose roots lie in L and are conjugate to α under a K-automorphism of L. It follows that we can recover K' as the set of all $x \in L$ fixed by $\mathrm{Aut}_(K', L)$, and this group is a subgroup H of $G = \mathrm{Aut}_K(L)$. Hence *the subfields L' of L containing K all take the form $L^H = \{x \in L : hx = x, h \in H\}$; in particular, there are only finitely many of them.* The same result holds even if L is only a finite separable extension of K, for then L lies in a finite Galois extension M of K (the splitting field of a suitable product of polynomials over K, one for each element of a K-basis of L). Now we want to see that there are *exactly* as many subfields L' as subgroups of G if L is Galois; we will prove this in steps, deriving other results interesting in their own right along the way. We first show that L is a *simple* extension of K, generated by a single element α. To see this, note first that it is immediate if K and L are finite, for then the multiplicative group L^* is cyclic (as you will prove in homework this week) and a generator also generates L as an extension of K. If K is infinite and $\alpha_1, \alpha_2 \in L$, then the subfield $L' = K(\alpha_1, \alpha_2)$ of L generated by K and α_1, α_2 has only finitely many fields between it and K, so there are distinct $c, d \in K$ with $K(\alpha_1 + c\alpha_2) = K(\alpha_1 + d(\alpha_2)$; this forces $(d-c)\alpha_2, \alpha_2$, and α_1 to lie in $K(\alpha_1 + c\alpha_2)$, so that the single element $\alpha_1 + c\alpha_2$ generates $L' = K(\alpha_1, \alpha_2)$. Iterating this result with a finite basis $\ell_1, \ldots, \ell_n$ of L as a K-vector space, we see that a suitable linear combination of the ℓ_i generates L as an extension of K, as claimed. Now let E be any field and H any finite group of automorphisms (not assumed to be F'-automorphisms for any particular subfield F of E for the moment). If $\alpha \in E$ and if $\alpha = \alpha_1, \ldots, \alpha_m$ are the distinct conjugates of α by the elements of H, then α is a root of the polynomial $(x - \alpha_1) \cdots (x - \alpha_m)$, whose roots are distinct and whose coefficients are fixed by H. It follows that E is a separable algebraic extension of the fixed field E^H and any subfield of E containing E^H and generated by finitely many elements and E^H is in fact generated by only one element and E^H, and that element satisfies a polynomial of degree at most $|H|$. But then the degree of E over E^H must be finite and at most $|H|$ (lest some subfield of E have too large a degree over E^H), whence the degree of E over E^H must be exactly $|H|$, since any finite extension of a field F admits at most as many F-automorphisms as its degree over F. We have shown that *given any field E and a finite group H of automorphisms of it, E is always Galois over the fixed field E^H, it has degree $|H|$ over this fixed field, and H is in fact the Galois group of E over E^H.* Returning to our original setting of a finite Galois extension L of a field K with Galois group G, we now know that *the map sending a subgroup H of G to the subfield L^H sets up a 1-1 inclusion-reversing correspondence between subfields* *of L containing K and subgroups of G.* This is the Galois correspondence. Note that L is always Galois over any intermediate field L^H, with Galois group H, a subgroup of G.

In the Galois correspondence conjugate subgroups H, xHx^{-1} of G correspond to conjugate subfields L', xL'. Hence a subfield L' is preserved by the group G (i.e. its elements are permuted but not necessarily fixed by G) if and only if its corresponding subgroup H is normal in G; in this case the Galois group of L' over K is the quotient group G/H.. Historically the notion of a normal extension of a field preceded that of a normal subgroup of a group; the first person to define the notion of normal subgroup (before the axioms of a group had even been written down) was Galois himself.

As a simple example of the Galois correspondence, look at the subfield $K = \mathbf{Q}(\sqrt{2}, \sqrt{3})$ of $\mathbf{C}$ generated by $\mathbf{Q}$ and $\sqrt{2}, \sqrt{3}$. This extension is Galois; the elements of the Galois group $\mathbf{Z}_2 \times \mathbf{Z}_2$ each preserve or interchange $\sqrt{2}, -\sqrt{2}$ and the same for $\sqrt{3}, -\sqrt{3}$. This group is well known to have three (not two) subgroups of order 2; correspondingly, there are exactly three fields strictly between $\mathbf{Q}$ and K, namely the "obvious" ones $\mathbf{Q}(\sqrt{2}), \mathbf{Q}(\sqrt{(}3)$, and $\mathbf{Q}(\sqrt{6})$, It would be tricky (and quite awkward) to show this directly without using Galois theory.