Math 505, 1/4

I will begin this quarter with Galois theory. As most of you have seen this material in a fair amount of detail before, I will go quickly. For any result that I mention whose proof you have not seen, I suggest that you take it on faith for now (most results are fairly intuitive and none should come as any great surprise) and look in the literature (e.g. Dummit and Foote, or many other sources) at your leisure to find the proofs.

The setting will be a pair of fields K, L with L containing K and finite (that is, finite-dimensional as a vector space) over it; we denote its dimension by $[L : K]$ and call it the *degree* of L over K. The main example is the case where L is generated as a field by K and a single element α, which must then be algebraic over K. The degree of the (unique monic) minimal polynomial p of α over K then matches that of $L = K(\alpha)$. Conversely, if p is any irreducible polynomial in $K[x]$, then the quotient $K[x]/(p)$ is a field and finite over K. If K, L, M are three fields with L finite over K and M finite over L, then M is finite over K and $[M : K] = [M : L][L : K]$. Given any nonconstant polynomial $p \in K[x]$, we let q be an irreducible factor of p and we pass to the extension $K[x]/(q)$; iterating this construction, we arrive at a finite extension L of K that is generated over K by the roots of p and in which p factors completely into linear factors. We call L the *splitting field of* p over K; it is unique up to isomorphism. We now get groups into the picture. Given a finite extension L of K, let G be the (Galois) group $\mathrm{Aut}_K(L)$ of K-automorphisms of L; that is, automorphisms of L that are also K-linear maps (so that they fix every element of K). More generally, if M is another finite extension of K, denote by $\mathrm{End}_K(L, M)$ the set of homomorphisms from L into M that are the identity on K. It will be of crucial importance to know how big $\mathrm{Aut}_K(L)$ and $\mathrm{End}_K(L, M)$ can be and in particular to know that they are finite in all cases. To see this, let $\alpha \in L$. Then α is necessarily algebraic over K; let p be its minimal polynomial. If p has degree d, then there are at most d roots of p in L or M and $f(\alpha)$ must be such a root if f is a K-homomorphism, so there are at most d K-homomorphisms from $K(\alpha)$ into L or M. If $K(\alpha) \neq L$, then we iterate this, letting β be an element of L that is not in $K(\alpha)$. Then β has a minimal polynomial q over $K(\alpha)$. Given a K-homomorphism f from $K(\alpha)$ into M, it does not necessarily fix q, but it must send q to another polynomial of the same degree e. Hence there are at most e ways to extend any such f to $K(\alpha, \beta)$. Continuing this and bearing in mind the multiplicativity of field degrees, we conclude that *both* $Aut_K(L)$ *and* $End_K(L, M)$ *are finite and of order at most* $[L : K]$. If $G = \mathrm{Aut}_K(L)$ has the largest possible order then we call L *Galois* over K; in any case (even if L is not Galois over K) we call G the Galois group of L over K. If there is a finite extension M of K for which $\mathrm{End}_K(L, M)$ has the largest possible order $[L : K]$, then we call L *separable* over K (this definition is often not given in undergraduate courses covering Galois theory).

Now let K be a field and $q = \sum_{i=0}^{n} a_i x^i \in K[x]$. If q has a multiple root α in any extension field L of K, then it is well known (and easy to check) that α is also a root of the formal derivative $q' = \sum_{i=1}^{n} i a_i x^{i-1}$ of q. This is impossible if q

is irreducible, **unless** $q' = 0$; this in turn happens if and only if the characteristic p of K is prime and $q = g(x^p) = g(x)^p$ for some $g \in K[x]$. Taking M to be the splitting field of a suitable polynomial over K, it follows that *any finite extension of a field K of characteristic 0 is separable, while no proper extension of the from $K(\alpha)$ with $\alpha^p \in K$ is separable if K has characteristic p.* We call extensions $K(\alpha)$ of this last form (with $\alpha^p \in K$ and K of characteristic p) *purely inseparable*. If q is a nonconstant polynomial in $K[x]$ with no multiple roots in its splitting field L over K, then we see that L is Galois over K (since we can get from K to L by repeatedly adjoining roots α of q; the minimal polynomial of α will always divide q, so there will always be enough distinct choices for the image of α in an automorphism of L). In this case, if r is any irreducible polynomial over K with one root iα n L, then in fact all roots of r must lie in L and be distinct; to see this, note that if it fails and r has degree d, then there are fewer than d homomorphisms over K from $K(\alpha)$ into L, whence ultimately fewer than $[L : K]$ elements of G.

As a simple example, take $K = \mathbf{Q}$, the field of rational numbers, and let $p_1, \ldots, p_n$ be distinct prime numbers. Then $\sqrt{p_1}$ is irrational, so $K_1 = K(\sqrt{p_1}$ is a proper Galois extension of K, with Galois group $\mathbf{Z}_2$. But then $\sqrt{p_2} \notin K_1$, for if p_2 had a square root β in K_1, then the image of β under the nontrivial automorphism of K_1 would also be a square root of p_2, forcing either $\sqrt{p_2}$ or $\sqrt{p_2/p_1}$ to be rational. Iterating the construction, we see that $K_n = K(\sqrt{p_1}, \ldots, \sqrt{p_n})$ is Galois over K for all n, with Galois group $(\mathbf{Z}_2)^n$.