Math 250a: Higher Algebra
Problem Set #3 (13 October 2004): Infinite Galois theory
(and a bit of Kummer theory)

A field extension L/F, not necessarily finite, is said to be normal or Galois if every $a \in L$ is a root of a separable polynomial in $F[X]$ that splits completely in L. Examples are any finite Galois extension, the extension of $\mathbf{Q}$ generated by all roots of unity, an algebraic closure of a perfect field, or a separable closure of an arbitrary field. The Galois group $G = \mathrm{Gal}(L/F)$ of such an extension is defined as in the finite case: the group of all automorphisms of L/F, i.e., all automorphisms η of L such that $\eta(c) = c$ for all $c \in F$. This group carries a topology $\mathcal{T}$, that is, a distinguished collection of subsets called "open sets". A subset $S \subseteq G$ is said to be "open" if for each $\eta \in S$ the field L contains a field E, of finite dimension over F, such that $\eta' \in S$ for all η' that agree with η on E, i.e., such that $\eta'(x) = \eta(x)$ for all $x \in E$. (Equivalently:

$$N_E(\eta) := \{\eta' \in G \mid \forall x \in E,\ \eta'(x) = \eta(x)\}$$

is a neighborhood of η, and the family of such neighborhoods as E, η vary is a family of basic open sets for $\mathcal{T}$.) Note that we may assume that E/F is normal, because the normal closure of any finite E/F is again finite, and contained in L if E is.

1. Verify that $\mathcal{T}$ is indeed a topology, that is, that $\mathcal{T}$ contains $\emptyset$ and G and is closed under finite intersections and arbitrary unions. Prove that G is a topological group for $\mathcal{T}$, that is, that the group operations (inverse and product) on G are continuous. Check that if $[L : F] < \infty$ then $\mathcal{T}$ is the discrete topology (all subsets are open).

2. Let K be any subfield of L containing F. Prove that $\mathrm{Gal}(L/K)$ is a *closed* subgroup of $\mathrm{Gal}(L/F)$, and is a normal subgroup if K/F is normal. If H is any normal subgroup of $\mathrm{Gal}(L/F)$, prove that $g(L^H) = L^H$ for all $g \in \mathrm{Gal}(L/F)$.

For each normal finite extension E/F with $E \subseteq L$, we have a homomorphism ψ_E from G to the finite group $\mathrm{Gal}(E/F)$ (restrict each $\eta \in G$ to E — note that $\eta(E) = E$ because E is normal). This ψ_E is continuous by the definition of $\mathcal{T}$ (use the same E). Take the product over all E to obtain a homomorphism $\psi = \prod_E \psi_E$ from G to $\Gamma := \prod_E \mathrm{Gal}(E/F)$. Recall that each $\mathrm{Gal}(E/F)$ carries the discrete topology; we use these to give Γ its product topology.

If $E \subseteq E'$ then ψ_E is the composition of $\psi_{E'}$ with the restriction map from $\mathrm{Gal}(E'/F)$ to $\mathrm{Gal}(E/F)$. Thus $\psi(G)$ is contained in the subgroup of Γ consisting of all $\{\eta_E\}$ such that whenever $E \subseteq E'$ the image of $\eta_{E'}$ under that restriction map is η_E. Call this group Γ_0; this is the "projective limit" of the groups $\mathrm{Gal}(E/F)$ with respect to the restriction maps $\mathrm{Gal}(E'/F) \to \mathrm{Gal}(E/F)$. It is a closed subgroup of Γ, because it is the intersection of the closed subgroups obtained by imposing each (E, E') condition individually.

To go further, we use the Axiom of Choice, in its familiar guise as Zorn's Lemma. This is no great concession because Choice is needed to even construct many of the infinite Galois extensions L/F that interest us.

3. Show (under AC/Zorn) that $\psi(G) = \Gamma_0$. Verify that ψ is a hom**e**omorphism from G to Γ_0.

4. Suppose $F \subseteq K \subseteq K' \subseteq L$. Prove that if K' strictly contains K then $\mathrm{Gal}(L/K')$ is strictly smaller than $\mathrm{Gal}(L/K)$. Deduce that if $K' = L^H$ with $H = \mathrm{Gal}(L/K)$ then $K' = K$. Use this to complete the proof of a Galois correspondence between subfields of L and closed subgroups of G.

By Tychonoff's theorem, Γ is *compact*. Hence so is G, which is homeomorphic with the closed subset Γ_0 of Γ.

5. Prove that an open subgroup $H \subseteq G$ has finite index in G, and is thus also closed. Conversely, show that a closed subgroup of finite index in G is $\mathrm{Gal}(L/E)$ for some $E \subseteq L$ with $[E : F] < \infty$, and is thus open in G.

This shows where finite field extensions fit into the Galois correspondence for infinite normal extensions.

We next give two explicit examples of an infinite Galois group G. In both cases, we identify G with the "profinite completion" of $\mathbf{Z}$, usually denoted $\widehat{\mathbf{Z}}$. It is the completion of $\mathbf{Z}$ with respect to a non-archimedean metric such as

$$d(x, y) := 1/\min\{m > 0 \mid x \not\equiv y \bmod m\},$$

in which a sequence is Cauchy if and only if it is eventually constant mod m for each m. For instance, $\sum_{n=0}^{\infty} n!$ converges in $\widehat{\mathbf{Z}}$. The occurrence of this group in both settings is no coincidence.

6. Let F be a finite field of q elements, and L an algebraic closure of F. Show that the Frobenius map $\phi : x \mapsto x^q$ generates an infinite cyclic subgroup of $G = \mathrm{Gal}(L/F)$ that is dense in G.

7. Now take $F = \mathbf{C}(t)$, and let L be the union of all the fields $\mathbf{C}(t^{1/m})$ with $m = 1, 2, 3, \ldots$. Prove that L/F is normal, and that its Galois group G contains an element ϕ taking each $t^{1/m}$ to $e^{2\pi i/m} t^{1/m}$. Show that ϕ generates a dense infinite cyclic subgroup of G.
   [Can you interpret ϕ geometrically?]

And finally a bit on Kummer theory of (finite) cyclic extensions:

8. Let p be a prime, F the p-th cyclotomic field (splitting field of $x^p - 1$ over $\mathbf{Q}$), and $G = \mathrm{Gal}(F/\mathbf{Q}) = (\mathbf{Z}/p\mathbf{Z})^*$. We know that every normal extension K/F with Galois group $\mathbf{Z}/p\mathbf{Z}$ is the splitting field of $y^p - a$ for some $a \in F^*/(F^*)^p$.
   i) Give a necessary and sufficient condition on a that makes K a normal extension of $\mathbf{Q}$.
   ii) Give a necessary and sufficient condition on a that makes K an abelian extension of $\mathbf{Q}$.
   iii) Suppose $c \in F^*$ is such that the images in $F^*/(F^*)^p$ of the p^{p-1} elements $a = \prod_{\sigma \in G} (\sigma(c))^{\alpha_g}$ $(0 \leq \alpha_g < p)$ are distinct. Find necessary and sufficient conditions on the α_g that make $K = F(a^{1/p})$ a normal extension of $\mathbf{Q}$, and the further necessary and sufficient conditions for $K/\mathbf{Q}$ to be abelian.

Problem set is due in class Friday, October the 22th.