Math 248A. Homework 10

1. (optional) The purpose of this (optional!) problem is to extend Galois theory to the case of infinite extensions. It is optional because it is long; definitely work it out for yourself if you do not know it already. (Its results are used in subsequent exercises.) Recall that if K/k is an algebraic extension of fields then it is *separable* if all elements of K are separable over k, or equivalently if all intermediate fields of finite degree over k are separable over k, and it is *Galois* if every irreducible $f \in k[T]$ with a root in K (so f is separable) splits over K; equivalently, every finite subextension of K is contained in a Galois subextension. If K/k is Galois, we define $\mathrm{Gal}(K/k)$ to be $\mathrm{Aut}(K/k)$.

(*i*) Let k_s/k be a separable closure. Using the uniqueness of separable closure up to (non-unique) automorphism, prove that K/k is Galois if and only if K/k is separable and every k-embedding $K \hookrightarrow k_s$ has the same image.

(*ii*) Assume that K/k is Galois, and let K' be an intermediate extension (so K'/k is separable). Prove that K/K' is Galois and that K' is the fixed field of $\mathrm{Gal}(K/K')$ acting on K (hint: use (*i*) and uniqueness of separable closures up to isomorphism), and prove that K'/k is Galois if and only if $\mathrm{Gal}(K/K')$ is a normal subgroup of $\mathrm{Gal}(K/k)$, in which case the natural map of abstract groups $\mathrm{Gal}(K/k)/\mathrm{Gal}(K/K') \to \mathrm{Gal}(K'/k)$ is an isomorphism.

(*iii*) Assume K/k is Galois, and let Σ denote the set of subgroups of $\mathrm{Gal}(K/k)$ that arise in the form $\mathrm{Gal}(K/K')$ for intermediate extensions K'. By (*ii*), $K' \mapsto \mathrm{Gal}(K/K')$ is a bijection from the set of intermediate extensions to the set Σ, with K-Galois subextensions corresponding to normal subgroups in Σ, and that $H \mapsto K^H$ is the inverse bijection. In general Σ is not generally the set of *all* subgroups of $\mathrm{Gal}(K/k)$, but this is most easily seen using considerations with the Krull topology introduced below.

We define the *Krull topology* on $G = \mathrm{Gal}(K/k)$ as follows: a base of opens around σ is given by the subsets $U_F(\sigma) = \{g \in G \,|\, \sigma|_F = g|_F\}$ for subextensions F of finite degree over k. (That is, an element is "close" to σ if it agrees with σ on a large finite set of elements of K.) Prove that the subsets $U_F(\sigma)$ satisfy the axioms to be a base of opens for a topology on G, called the *Krull topology*, and that this induces exactly the subspace topology on G via the inclusion $G \subseteq \prod_F \mathrm{Gal}(F/k)$ as F ranges over the k-finite subextensions that are *Galois* over k and each finite group $\mathrm{Gal}(F/k)$ is given the discrete topology. (For example, if $[K : k]$ is finite then this gives the discrete topology to $\mathrm{Gal}(K/k)$.) Also prove that if $k_1 \to k_2$ is a map of fields and $K_1 \to K_2$ is a map of Galois extensions over $k_1 \to k_2$ then the induced map $\mathrm{Gal}(K_2/k_2) \to \mathrm{Gal}(K_1/k_1)$ is continuous; in particular, the Krull topology is *functorial*.

(*iv*) Prove that $G = \mathrm{Gal}(K/k)$ with its Krull topology is a topological group, and prove that G is closed in $\prod_F \mathrm{Gal}(F/k)$. (hint: Prove G is the set of tuples $(g_F)_F$ satisfying the collection of conditions $g_{F_1}|_{F_2} = g_{F_2}$ for all pairs F_1 and F_2 with $F_2 \subseteq F_1$.) Conclude that the Krull topology makes G *compact* and Hausdorff, and use this to prove that if K' is an intermediate extension then the natural injection $\mathrm{Gal}(K/K') \to \mathrm{Gal}(K/k)$ is a homeomorphism onto a closed subgroup and for K'/k Galois the natural map $\mathrm{Gal}(K/k)/\mathrm{Gal}(K/K') \to \mathrm{Gal}(K'/k)$ is an isomorphism of topological groups (using the quotient topology on the source).

(*v*) Prove that the closure of a subgroup H of a topological group G is also a subgroup (hint: for $h \in H$, prove $h \cdot \overline{H} = \overline{H} = \overline{H} \cdot h$, so $H \cdot \overline{h} \subseteq \overline{H}$ and $\overline{h} \cdot H \subseteq \overline{H}$ for all $\overline{h} \in \overline{H}$), and that if $H \subseteq \mathrm{Gal}(K/k)$ is a subgroup then $\mathrm{Gal}(K/K^H)$ is the closure of H with respect to the Krull topology. (hint: Use *finite* Galois theory to show that H surjects onto $\mathrm{Gal}(K'/K^H)$ for all subextensions K' that are finite Galois over K^H!) Deduce that the set Σ in (*iii*) is exactly the set of *closed* subgroups with respect to the Krull topology, so the Galois correspondence is rescued if we restrict attention to closed subgroups of G.

2. Let k be a field and let k_s be a separable closure. Let $G = \mathrm{Gal}(k_s/k)$. A Galois extension K/k is *abelian* if $\mathrm{Gal}(K/k)$ is abelian.

(*i*) Prove that a compositum of abelian extensions of k is abelian, and use k_s to prove the existence of an abelian extension k^{ab}/k that is maximal in the sense that every abelian extension of k admits a k-embedding into k^{ab}. Prove that an extension with such a property is unique up to (generally non-unique) k-isomorphism.

(*ii*) Prove that the closure of the commutator subgroup of G is a normal subgroup, and use the Galois correspondence to prove that the corresponding extension of k inside of k_s is a maximal abelian extension of k. The corresponding quotient of G is denoted G^{ab} (so it is usually *not* the algebraic abelianization).

(*iii*) If $k \to k'$ is a map of fields and k'_s/k' is a separable closure, prove that there exists a map of fields $i : k_s \to k'_s$ over $k \to k'$ and that it is unique up to a k-automorphism of k_s. Conclude that the induced map $\mathrm{Gal}(k'_s/k') \to \mathrm{Gal}(k_s/k)$ depends on i only up to conjugation on $\mathrm{Gal}(k_s/k)$.

(*iv*) Prove that the induced map $\mathrm{Gal}(k_s/k)^{\mathrm{ab}} \to \mathrm{Gal}(k'_s/k')^{\mathrm{ab}}$ is *canonical* (independent of i), and explain why $\mathrm{Gal}(k^{\mathrm{ab}}/k)$ is therefore *functorial* in k (whereas k^{ab} and $\mathrm{Gal}(k_s/k)$ generally are not).

(*v*) If k is finite then prove that the compact group $\mathrm{Gal}(k_s/k)$ is abelian, and more specifically it is *topologically* isomorphic to the compact group $\prod_\ell \mathbf{Z}_\ell$ where the product is taken over all primes ℓ. (Hint: If $k_n \subseteq k_s$ is the unique extension of k with degree n, use $x \mapsto x^{|k|}$ to construct isomorphisms $\mathrm{Gal}(k_n/k) \simeq \mathbf{Z}/n\mathbf{Z}$ that are *compatible* with replacing n with a positive multiple.)

3. Prove that $X^4 - 50 \in \mathbf{Q}_5[X]$ is irreducible, and let $L = \mathbf{Q}_5(\alpha)$ with $\alpha^4 = 50$. Prove that the quartic extension $L/\mathbf{Q}_5$ is cyclic and has maximal unramified subextension E that is quadratic over $\mathbf{Q}_5$, so L/E is a totally tamely ramified extension with degree 2. Thus, there must exist a uniformizer π_E of E such that $L = E(\sqrt{\pi_E})$. Find such a π_E explicitly (in terms of α). Can such a π_E be found inside of $\mathbf{Q}_5$? Justify your answer.

4. Let F be a field equipped with a choice of non-trivial non-archimedean place v, and let F_v denote its completion. Let F_s and $F_{v,s}$ denote choices of separable closures of F and F_v respectively. Give $F_{v,s}$ its unique place lifting the canonical one on F_v. (That is, we may uniquely lift the natural absolute value on F_v – which is unique up to powers – to an absolute value on $F_{v,s}$.)

(*i*) Prove that there exists a place $\overline{v}$ on F_s lifting the place v on F (in the sense that all absolute values in the class $\overline{v}$ restrict to ones in the class v). Prove that for any $g \in \mathrm{Gal}(F_s/F)$ and representative $|\cdot|'$ for $\overline{v}$, the topological equivalence class of $|g^{-1}(\cdot)|'$ is independent of the representative $|\cdot|'$, so the corresponding place on F_s may be denoted $g(\overline{v})$. Prove that $g(\overline{v}) = \overline{v}$ if and only if $|g^{-1}(\cdot)|' = |\cdot|'$ for one representative $|\cdot|'$ for $\overline{v}$ (and hence for all such representatives).

(*ii*) Define the *decomposition group* $D(\overline{v}|v) \subseteq \mathrm{Gal}(F_s/F)$ at $\overline{v}$ to be the subgroup of elements g such that $g(\overline{v}) = \overline{v}$. Prove that this is a closed subgroup of $\mathrm{Gal}(F_s/F)$ and that if $\overline{v}'$ is a second place on F_s lifting v then there exists $g \in \mathrm{Gal}(F_s/F)$ such that $g(\overline{v}) = \overline{v}'$. Show also that $gD(\overline{v}|v)g^{-1} = D(\overline{v}'|v)$ for all such g, and that every place on F_s lifting v is induced by an embedding $F_s \to F_{v,s}$ over $F \to F_v$ that this embedding is unique up to the action of $D(\overline{v}|v)$.

(*iii*) Assume that v is discretely-valued and let $k(v)$ be the residue field attached to v on F, and assume $k(v)$ is perfect. Let $k(\overline{v})$ denote the residue field attached to $\overline{v}$ on F_s. Prove that $k(\overline{v})/k(v)$ is an algebraic closure, and that the natural map $D(\overline{v}|v) \to \mathrm{Gal}(k(\overline{v})/k(v))$ is a continuous surjection. Its closed (!) kernel $I(\overline{v}|v)$ is called the *inertia group* at $\overline{v}$; explain its dependence on the choice of $\overline{v}$ in terms of conjugations, much like for $D(\overline{v}|v)$.

(*iv*) Let F'/F be an arbitrary Galois extension (perhaps not a separable closure), and impose the assumptions on v as in (*iii*). Define closed subgroups $D(v'|v)$ and $I(v'|v)$ in $\mathrm{Gal}(F'/F)$ for places v' on F' lifting v, prove that $k(v')/k(v)$ is Galois with $D(v'|v)/I(v'|v) \to \mathrm{Gal}(k(v')/k(v))$ a topological isomorphism, and discuss variation in v' over v. We say that v is *unramified* in F' if $I(v'|v) = 1$ for one (and hence all!) v' over v on F', so for unramified v the group $D(v'|v)$ is topologically identified with $\mathrm{Gal}(k(v')/k(v))$.

(*v*) Let K be a global field and let K'/K be a Galois extension. For each non-archimedean place v on K that is unramified in K' (for example, any $v \notin S$ if $K' = K_S$) and each v' lifting v to K', define the *Frobenius element* $\phi(v'|v) \in \mathrm{Gal}(K'/K)$ to correspond to the $\#k(v)$th-power map in $\mathrm{Gal}(k(v')/k(v)) \simeq D(v'|v)$. Explain why the conjugacy class of $\phi(v'|v)$ depends only on v and not on v'. Conclude that if $\mathrm{Gal}(K'/K)$ is *abelian* then the element $\phi(v'|v)$ is independent of v'; it is then denoted $\phi_v \in \mathrm{Gal}(K'/K)$, and is called the *Frobenius element at* v. These are extraordinarily important throughout algebraic aspects of modern number theory.

For a concrete application, see the handout on quadratic characters.