Math 676. Homework 11

1. 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).

2. 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.

3. Let n be a positive integer. Let K be a field with $\mathrm{char}(K)$ not dividing n, and assume that K contains a primitive nth root of unity. Recall that Kummer theory sets up a bijection between (possibly infinite) subgroups $B \subseteq K^\times/(K^\times)^n$ and (possibly infinite-degree) abelian extensions K'/K for which $\mathrm{Gal}(K'/K)$ has exponent n (that is, killed by n), via $B \mapsto K(B^{1/n})$; see Lang's *Algebra* for details on this.

(i) Assume that K is a non-archimedean discretely-valued field, and assume that the residue characteristic does not divide n (that is, n is a unit in the valuation ring). Prove that if $a \in K^\times$ then the cyclic extension $K(a^{1/n})/K$ (with Galois group of order dividing n) is unramified if and only if $n|\mathrm{ord}_K(a)$, where $\mathrm{ord}_K : K^\times \twoheadrightarrow \mathbf{Z}$ denotes the normalized order function.

(ii) Assume that K is the fraction field of a Dedekind domain A. A separable extension K'/K is *unramified* over A if every finite subextension is unramified at all maximal ideals of A; that is, the integral closure of A in every finite subextension is finite *étale* over A. Prove that this property is inherited by passing to intermediate extensions and under formation of composites over K, and deduce the existence and uniqueness (up to non-canonical isomorphism) of a separable extension K_A/K unramified outside of A that is maximal in the sense that all others admit a K-embedding into it, and prove that K_A/K is Galois.

(The case of interest in number theory is the ring $A = \mathscr{O}_{K,S}$ of S-integers for a global field K, with S a finite non-empty set of places that contains the archimedean places. The condition of being unramified over A is called "unramified outside S" for obvious reasons, and the field K_A is often denoted K_S and the Galois group $\mathrm{Gal}(K_S/K)$ is often denoted $G_{K,S}$. These are very important in number theory.)

(iii) With notation as in (ii), prove that if $A^\times$ is finitely generated with rank ρ then the extension $K((A^\times)^{1/n})/K$ obtained by extracting nth roots of all elements of $A^\times$ is a finite Galois extension with Galois group $\mathrm{Hom}(A^\times/(A^\times)^n, \mu_n(K))$ that is abstractly isomorphic to $(\mathbf{Z}/n\mathbf{Z})^{\rho+1}$ (note that $A^\times_{\mathrm{tor}}$ is cyclic and contains $\mu_n(K)$ with order n). The most important case of interest is $A = \mathscr{O}_{K,S}$ for a global field K and a finite non-empty set of places S that contains all archimedean places and all places with residue characteristic dividing n, in which case $\rho + 1 = |S|$.

(iv) Under the hypotheses as in (iii), assume also that $n \in A^\times$ (a condition that is automatic if $\mathrm{char}(K) > 0$, and otherwise says that all maximal ideals of A have residue characteristic not dividing n; for $A = \mathscr{O}_{K,S}$ with K a number field, it says that S contains all places with residue characteristic dividing n). Use Kummer theory and (i) to prove that if A has trivial class group then the extension constructed in (iii) is the *maximal* abelian extension of K with exponent n that is unramified over A. That is, any abelian extension of K with exponent n and no ramification over A is a subfield of $K((A^\times)^{1/n})$. Hence, in the special case when $A^\times$ is finitely generated with rank ρ, the quotient group $\mathrm{Gal}(K_A/K)^{\mathrm{ab}}/n\mathrm{Gal}(K_A/K)^{\mathrm{ab}}$ is *finite* with size $n^{\rho+1}$.

4. Let $K = k(t)$ for a finite field k with characteristic $p > 0$. For any $f \in k[t]$, let K_f/K be a splitting field for $X^p - X - f$, so K_f/K is trivial or cyclic of order p. Prove that this extension is unramified at all places of K away from ∞, and use Artin–Schreier theory to prove that there are infinitely many isomorphism classes of cylic p-extensions of K unramified away from ∞. Deduce that $G_{K,\infty}^{\mathrm{ab}}/pG_{K,\infty}^{\mathrm{ab}}$ is *infinite*.

5. 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 $F_{v,s}$. 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 $D(v'|v)$ 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.