MATH 676. HOMEWORK 12

1. Let F be a field endowed with a discretely-valued non-archimedean place v, and let F_v be the completion. Let F_s and $F_{v,s}$ denote separable closures of F and F_v respectively. Let $\overline{v}$ be a place on F_s lifting v. In Exercise 5 of Homework 11 you showed that there exists an embedding $F_s \to F_{v,s}$ over $F \to F_v$ that induces $\overline{v}$, and that this embedding is unique up to the action of the closed subgroup $D(\overline{v}|v) \subseteq \mathrm{Gal}(F_s/F)$. Use this embedding to construct a continuous map of topological groups $\mathrm{Gal}(F_{v,s}/F_v) \to D(\overline{v}|v)$ that is unique up to inner automorphism of $D(\overline{v}|v)$, and use Krasner's lemma to prove that this continuous map is an isomorphism of topological groups.

In particular, the map $\mathrm{Gal}(F_{v,s}/F_v) \to \mathrm{Gal}(F_s/F)$ that is canonical up to inner automorphism of $\mathrm{Gal}(F_s/F)$ is injective, and in fact is a topological isomorphism onto a closed subgroup of $\mathrm{Gal}(F_s/F)$.

2. Let $G = \mathrm{Gal}(\mathbf{Q}_p(\zeta_{p^n})/\mathbf{Q}_p)$ for a prime p and $n \geq 1$. Let G_i denote the ith ramification group (so G_0 is the inertia subgroup, and $G_i = 1$ for large i). For $i \geq 0$, use the definition of the higher ramification groups to prove that $G_i = \mathrm{Gal}(\mathbf{Q}_p(\zeta_{p^n})/\mathbf{Q}_p(\zeta_{p^j}))$ for $p^{j-1} \leq i \leq p^j - 1$ when $i < p^{n-1}$, and $G_i = 1$ for $i \geq p^{n-1}$.

3. Let K be a field. A $\mathbf{Z}_p$-*extension* of K is an abelian extension K'/K such that $\mathrm{Gal}(K'/K) \simeq \mathbf{Z}_p$ as topological groups.

(*i*) Let K'/K be any $\mathbf{Z}_p$-extension. Prove that for each $n \geq 1$ there exists a unique intermediate extension with degree p^n over K, and that this exhausts the set of *all* intermediate subfields not equal to K and K'. (Hint: $\mathbf{Z}$ is topologically dense in $\mathbf{Z}_p$.)

(*ii*) Let K be a number field and let $K' = K(\mu_{p^\infty})$ be the extension generated by all p-power roots of unity. Prove that the natural map $\mathrm{Gal}(K'/K) \to \mathrm{Gal}(\mathbf{Q}(\mu_{p^\infty})/\mathbf{Q}) \simeq \mathbf{Z}_p^\times$ is an isomorphism onto a closed subgroup with finite index, and so conclude that it is an isomorphism onto an open subgroup. Deduce via the p-adic logarithm and the absence of non-trivial torsion in $\mathbf{Z}_p$ that $\mathrm{Gal}(K'/K)$ has a *unique* quotient topologically isomorphic to $\mathbf{Z}_p$, and it corresponds to a subextension K_∞ that is a $\mathbf{Z}_p$-extension of K and over which K' has finite degree. We call K_∞ the *cyclotomic* $\mathbf{Z}_p$-*extension* of K.

(*iii*) Let K be a local field with residue characteristic not equal to p. Explain why its cyclotomic $\mathbf{Z}_p$-extension is unramified, and use Galois theory for finite fields to prove that this is the unique unramified $\mathbf{Z}_p$-extension of K. Use (*i*) above and Exercise 4(*ii*) below to prove that any $\mathbf{Z}_p$-extension *must* be unramified. (Hint: Show that the image of inertia must be tame, and contrast how Frobenius lifts act on tame inertia through conjugation as in Exercise 4(*ii*) and how conjugation behaves in the abelian group $\mathbf{Z}_p$.)

(*iv*) Let K'/K be a $\mathbf{Z}_p$-extension of a number field. Using the absence of non-trivial torsion in $\mathbf{Z}_p$, prove that if v is a real place on K then its extensions to K' are real. (In particular, if K is totally real then all embeddings of K' into $\mathbf{C}$ are land in $\mathbf{R}$.) Use (*iii*) to prove that if v is a non-archimedean place of K with residue characteristic not equal to p then v is *unramified* in K'. Hence, K'/K is unramified away from the finite set of non-archimedean places of K with residue characteristic p.

4. Let F be a field that is complete with respect to a discretely-valued non-archimedean place v, and let F_s/F denote a separable closure. Let F_{un}/F denote the maximal unramified subextension (that is, the directed union of unramified finite subextensions), and let F_{t}/F denote the maximal tamely ramified subextension (that is, the directed union of tamely ramified finite subextensions). Endow these fields with their unique place extending that on F. The *tame quotient* I_{t} of the inertia group $I = \mathrm{Gal}(F_s/F_{\mathrm{un}})$ is $\mathrm{Gal}(F_{\mathrm{t}}/F_{\mathrm{un}})$.

(*i*) Explain why F_{un} is discretely-valued with residue field $k(v)'$ that is a separable closure of the residue field $k(v)$ at v on F. Prove that it is not complete if $[k(v)_{\mathrm{sep}} : k(v)]$ is infinite.

(*ii*) Prove that every finite subextension of $F_{\mathrm{t}}/F_{\mathrm{un}}$ is totally tamely ramified, and use Kummer theory to construct a canonical isomorphism of topological groups $I_{\mathrm{t}} \simeq \varprojlim_e \mu_e(k(v)')$ where the inverse limit is taken over $e \geq 1$ not divisible by $\mathrm{char}(k(v))$ and the transition maps in the inverse limit are the surjective (e'/e)th-power maps $\mu_{e'} \to \mu_e$ for $e|e'$. By using the short exact sequence

$$1 \to I_{\mathrm{t}} \to \mathrm{Gal}(F_{\mathrm{t}}/F) \to \mathrm{Gal}(k(v)'/k(v)) \to 1$$

with $I_{\rm t}$ abelian, explain how there results a natural action of $\mathrm{Gal}(k(v)'/k(v))$ on $I_{\rm t}$ through conjugation in $\mathrm{Gal}(F_{\rm t}/F)$, and describe this action in terms of the action of $\mathrm{Gal}(k(v)'/k(v))$ on roots of unity in $k(v)'$ with order not divisible by $\mathrm{char}(k(v))$.

(*iii*) By choosing suitably compatible primitive roots of unity, construct a non-canonical isomorphism of topological groups $I_{\rm t} \simeq \prod' \mathbf{Z}_\ell$, where $\prod'$ means that ℓ ranges over primes not divisible by $\mathrm{char}(k(v))$.

5. Let K be a global field. A *modulus* is a formal finite product $\mathfrak{m} = \prod \mathfrak{p}_v^{e_v}$ where the v's range over all places of K, $e_v \geq 0$ for all v with equality for all but finitely many v, $e_v \in \{0, 1\}$ for real v, and $e_v = 0$ for all complex v. We write $\mathfrak{m}|\mathfrak{m}'$ if $e_v \leq e'_v$ for all v.

For $a_v \in K_v^\times$, we say $a_v \equiv 1 \bmod \mathfrak{m}_v$ for $v \nmid \infty$ if $a_v \in \mathscr{O}_v^\times$ when $e_v = 0$ and if $\|a_v - 1\|_v \leq q_v^{-e_v}$ when $e_v > 0$ (*e.g.*, for $e_v = 1$ it says that a_v is a 1-unit). For $v|\infty$, the condition $a_v \equiv 1 \bmod \mathfrak{m}_v$ means nothing if $e_v = 0$ and means $a_v > 0$ in K_v if $e_v > 0$ (in which case K_v is *uniquely* isomorphic to $\mathbf{R}$). For $a \in K^\times$, we say $a \equiv 1 \bmod \mathfrak{m}$ if $a \equiv 1 \bmod \mathfrak{m}_v$ for all places v. In particular, this forces a to be a v-adic unit for all non-archimedean v not in the support of $\mathfrak{m}$.

The *generalized ideal class group* $\mathrm{Cl}_{\mathfrak{m}}(K)$ *with modulus* $\mathfrak{m}$ is the quotient group $I_K(\mathfrak{m})/P_K(\mathfrak{m})$ where $I_K(\mathfrak{m})$ is the free abelian group on the non-archimedean places v with $e_v = 0$ and $P_K(\mathfrak{m})$ is the subgroup of elements $\sum_v \mathrm{ord}_v(a)v$ for $a \in K^\times$ satisfying $a \equiv 1 \bmod \mathfrak{m}_v$ for all v with $e_v \neq 0$. If K is a number field then in the special case $e_v = 0$ for all v we recover the usual ideal class group, and if $e_v > 0$ precisely for real v then we obtain the *narrow ideal class group*: the group of invertible fractional ideals of $\mathscr{O}_K$ modulo the principal ideals that admit a generator $a \in K^\times$ that is positive in all $K_v \simeq \mathbf{R}$. (Such elements $a \in K^\times$ are called *totally positive*.)

(*i*) For $K = \mathbf{Q}$ and $\mathfrak{m} = N\mathbf{Z}$ for a nonzero integer N, construct an isomorphism $(\mathbf{Z}/N\mathbf{Z})^\times/\langle -1\rangle \simeq \mathrm{Cl}_{\mathfrak{m}}(K)$ and an isomorphism $(\mathbf{Z}/N\mathbf{Z})^\times \simeq \mathrm{Cl}_{\mathfrak{m}\infty}(K)$.

(*ii*) Assume K is a number field. Use weak approximation to prove that the natural map $\mathrm{Cl}_{\mathfrak{m}}(K) \to \mathrm{Cl}(K)$ is surjective with finite kernel. Conclude that the cardinality $h_{\mathfrak{m}}$ of $\mathrm{Cl}_{\mathfrak{m}}(K)$ is *finite* for every modulus $\mathfrak{m}$ when K is a number field.

(*iii*) Let $U_{\mathfrak{m}} \subseteq \mathbf{A}_K^\times$ be the open subgroup of (x_v) such that $x_v \equiv 1 \bmod \mathfrak{m}_v$ for all v. Prove $U_{\mathfrak{m}} \subseteq U_{\mathfrak{m}'}$ if $\mathfrak{m}'|\mathfrak{m}$ (the converse can fail due to residue fields with order 2), and prove that if K is a global function field then the $U_{\mathfrak{m}}$'s are a base of open neighborhoods around the identity in $\mathbf{A}_K^\times$ whereas if K is a number field then the $U_{\mathfrak{m}}$'s are a cofinal system of open subgroups but *not* a base of open neighborhoods around the identity in $\mathbf{A}_K^\times$.

Prove that for all global fields K, $K^\times U_{\mathfrak{m}}/K^\times \subseteq \mathbf{A}_K^\times/K^\times$ is a cofinal system of open subgroups in the *idele class group* $\mathbf{A}_K^\times/K^\times$, with infinite index if K is a global function field. (By (*v*) below, the index is *finite* when K is a number field, so all open subgroups of $\mathbf{A}_K^\times/K^\times$ have finite index when K is a number field.)

(*iv*) Let $\mathbf{A}_{K,\mathfrak{m}}^\times \subseteq \mathbf{A}_K^\times$ be the open subgroup of ideles (x_v) such that $x_v \equiv 1 \bmod \mathfrak{m}_v$ for all v in the support of $\mathfrak{m}$, so $U_{\mathfrak{m}} \subseteq \mathbf{A}_{K,\mathfrak{m}}^\times$. Let $K_{\mathfrak{m}}^\times = K^\times \cap \mathbf{A}_{K,\mathfrak{m}}^\times$ inside of $\mathbf{A}_K^\times$. Prove that the map

$$\mathbf{A}_{K,\mathfrak{m}}^\times/K_{\mathfrak{m}}^\times U_{\mathfrak{m}} \to \mathrm{Cl}_{\mathfrak{m}}(K)$$

defined by sending (x_v) to the class of $\sum_{v\nmid\infty} \mathrm{ord}_v(x_v)v$ is well-defined and an isomorphism of groups.

(*v*) By §9 in the handout on absolute values, for any *finite* set of places S the image of K in $\prod_{v\in S} K_v$ is dense. Deduce that the natural map

$$\mathbf{A}_{K,\mathfrak{m}}^\times/K_{\mathfrak{m}}^\times U_{\mathfrak{m}} \to \mathbf{A}_K^\times/K^\times U_{\mathfrak{m}}$$

is an isomorphism. (It is hard to make the inverse explicit!) By using the inverse, we thereby obtain a natural isomorphism

$$\mathbf{A}_K^\times/K^\times U_{\mathfrak{m}} \simeq \mathrm{Cl}_{\mathfrak{m}}(K)$$

that is hard to make explicit. Check that the resulting surjections $\mathbf{A}_K^\times \twoheadrightarrow \mathrm{Cl}_{\mathfrak{m}}(K)$ (that are hard to make explicit) are compatible with the natural maps $\mathrm{Cl}_{\mathfrak{m}'}(K) \twoheadrightarrow \mathrm{Cl}_{\mathfrak{m}}(K)$ when $\mathfrak{m}|\mathfrak{m}'$. In Math 776, this will be the key to translating the classical "ideal class" formulation of class field theory into the idelic version.