Math 249B. Homework 3

1. Let K be a global field. This exercise explains the important but slightly subtle method for expressing generalized ideal class groups in adelic terms. Fix a modulus $\mathfrak{m}$ of K.

(i) Let $U_{\mathfrak{m}} \subseteq \mathbf{A}_K^\times$ be the subgroup of ideles $(x_v) \in \mathbf{A}_K^\times$ such that $x_v \equiv 1 \bmod \mathfrak{m}_v$ for all v and $x_v \in \mathscr{O}_v^\times$ for all $v \nmid \infty$. Prove that this is an open subgroup and that $U_{\mathfrak{m}} \subseteq U_{\mathfrak{m}'}$ if $\mathfrak{m}'|\mathfrak{m}$ (the converse can fail due to residue fields with order 2). Also 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 $\mathbf{A}_K^\times$.

(ii) Prove that for all global fields K, the collection of subgroups $K^\times U_{\mathfrak{m}}/K^\times \subseteq \mathbf{A}_K^\times/K^\times$ 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 (iv) 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.)

(iii) 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, 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 $\prod_{v\nmid\infty} \mathfrak{p}_v^{\mathrm{ord}_v(x_v)}$ is well-defined and an isomorphism of groups.

(iv) By §9 in the handout on absolute values from Math 248A, 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 $\mathfrak{m}|\mathfrak{m}'$. This will be the key to translating the classical "ideal class" formulation of class field theory into the idelic version.

2. 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 §8 in Ch. VI in Lang's *Algebra* (3rd ed.) for details on this.

This exercise addresses a very important situation when Kummer theory explicitly describes all exponent-n finite abelian extensions of a global field subject to controlled ramification.

(i) Assume that K as above 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 over 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 (which can always be arranged for $A = \mathscr{O}_{K,S}$ by increasing S a little bit!) 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 $n^{\rho+1}$.

3. 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 (see Theorem 8.3 and the discussion preceding it in Ch. VI of Lang's "Algebra") to prove that there are infinitely many isomorphism classes of cylic p-extensions of K unramified away from ∞. Deduce that $G^{\mathrm{ab}}_{K,\infty}/pG^{\mathrm{ab}}_{K,\infty}$ is *infinite*.

Comparing with Exercise 2(*iv*), this shows that in characteristic $p > 0$ the study of finite cyclic extensions with p-power degree is rather more subtle than the study of finite cyclic extensions with degree not divisible by p. One of the great miracles of class field theory is that the formulations (but not the proofs!) of the main results are the same in all characteristics, not requiring special contortions to handle the p-part in characteristic p.