Math 249B. Homework 8

1. Let L/K be an extension of fields (not necessarily algebraic) and fix an embedding $K_s \to L_s$ over $K \to L$. Consider the induced continuous map $G_L \to G_K$ of absolute Galois groups (defined by $\sigma \mapsto \sigma|_{K_s}$), as well as the induced map $G_L^{\mathrm{ab}} \to G_K^{\mathrm{ab}}$ between topological abelianizations.

(*i*) Prove that the closed kernel $G_L \to G_K$ of the map corresponds to the Galois extension LK_s/L inside of L_s, and deduce that the map of Galois groups is injective if and only if every finite Galois extension L'/L is contained in LK' for some finite Galois extension K'/K inside of L'. Show in particular that in such cases if we let $K'_0 = K' \cap L$ then $K' \otimes_{K'_0} L \simeq L'$ and $\mathrm{Gal}(L'/L) \simeq \mathrm{Gal}(K'/K'_0)$.

(*ii*) Prove an analogous result for injectivity of $G_L^{\mathrm{ab}} \to G_K^{\mathrm{ab}}$ (using finite abelian extensions).

(*iii*) Verify using Krasner's Lemma that the criteria in (*i*) and (*ii*) hold when K is a global field and $L = K_v$ for a non-archimedean place v. Also treat the trivial archimedean case. (The subtlety of the Grunwald-Wang theorem is that one cannot always arrange that $K'_0 = K$ in (*ii*).)

2. Let p be a prime. Define the *$\mathbf{Z}_p$-rank* of a field k to be the maximal r such that $G_k := \mathrm{Gal}(k_s/k)$ (or equivalently, G_k^{ab}) admits $\mathbf{Z}_p^r$ as a topological quotient (if this maximum is finite). This exercise builds up to using global class field theory to canonically describe the maximal such quotient when k is a number field.

(*i*) Show that if $k'_1, \dots, k'_r$ are $\mathbf{Z}_p$-extensions of k then the composite field $K = k'_1 \cdots k'_r \subseteq k_{\mathrm{ab}}$ satisfies $\mathrm{Gal}(K/k) \simeq \mathbf{Z}_p^\rho$ (as topological groups) for some $\rho \le r$; if $\rho = r$ we say that the k'_i's are *independent* $\mathbf{Z}_p$-extensions. Deduce that k has finite $\mathbf{Z}_p$-rank if and only if there are finitely many $\mathbf{Z}_p$-extensions $k'_1, \dots, k'_r$ of k such that every $\mathbf{Z}_p$-extension is contained in their compositum, in which case the least such r is the $\mathbf{Z}_p$-rank of k.

(*ii*) If k'/k is an abelian extension such that $\mathrm{Gal}(k'/k)$ contains $\mathbf{Z}_p$ as a closed (equivalently, open) subgroup of finite index, show that $\mathrm{Gal}(k'/k)_{\mathrm{tors}}$ is finite and that there is a unique $\mathbf{Z}_p$-extension of k contained in k' (it corresponds to the fixed field of the torsion in the Galois group). Hint: $\mathbf{Z}_p$ contains no nontrivial torsion.

(*iii*) Show that the hypotheses in (*ii*) are satisfied for any local or global field k and any prime $p \ne \mathrm{char}(k)$ when $k' = k(\zeta_{p^\infty})$; the resulting $\mathbf{Z}_p$-extension is called the *cyclotomic* $\mathbf{Z}_p$-extension. Prove that it is the only one when k is a local field with residue field of size q that is a power of a prime $p' \ne p$, in which case it is unramified. (To dispose of wild ramification you will find it useful to first prove that there is no nontrivial *continuous* homomorphism to $\mathbf{Z}_p$ from a pro-ℓ group for a prime $\ell \ne p$, nor from a finite group. To handle tame ramification first prove that the maximal tame extension k_t/k has Galois group $\widehat{\mathbf{Z}} \ltimes (\prod_{\ell \ne p'} \mathbf{Z}_\ell)$ in which $1 \in \widehat{\mathbf{Z}}$ acts by conjugation on $\prod_{\ell \ne p'} \mathbf{Z}_\ell$ via the qth-power map.)

(*iv*) Deduce from (*iii*) that if k is a global field with $\mathrm{char}(k) \ne p$ then a $\mathbf{Z}_p$-extension is unramified at all non-archimedean places $v \nmid p$ (so it is everywhere unramified when $\mathrm{char}(k) > 0$). By considering the structure of $\mathbf{A}_k^\times/(k^\times \prod_{v \nmid \infty p} \mathscr{O}_v^\times)$ (especially remembering the adelic description of the *finite* class group in the number field case), use global class field theory to prove that if k is a global function field with $\mathrm{char}(k) \ne p$ then the only $\mathbf{Z}_p$-extension is the one arising from the finite constant field whereas if k is a number field then the maximal quotient of G_k^{ab} of the form $\mathbf{Z}_p^r$ is the quotient of $(\prod_{v|p} \mathscr{O}_v^\times)/\overline{\mathscr{O}_k^\times}$ by a finite torsion subgroup.

(*v*) Let k be a number field and let $\varepsilon_1, \dots, \varepsilon_{r_1+r_2-1}$ be a maximal set of multiplicatively independent units of $\mathscr{O}_k$. Using (*iv*), prove that k has finite $\mathbf{Z}_p$-rank $[k : \mathbf{Q}] - r_p(k) \le r_2 + 1$ where $r_p(k) \le r_1 + r_1 - 1$ is the maximal number of ε_i's which are $\mathbf{Z}_p$-multiplicatively independent (in the $\mathbf{Z}_p$-module quotient of $(\mathscr{O}_k \otimes_{\mathbf{Z}} \mathbf{Z}_p)^\times = \prod_{v|p} \mathscr{O}_v^\times$ by its finite torsion subgroup). Deduce that $\mathbf{Q}$ and any real quadratic field have $\mathbf{Z}_p$-rank 1 (so the cyclotomic $\mathbf{Z}_p$-extension is the only one) whereas an imaginary quadratic field has $\mathbf{Z}_p$-rank 2. *Leopoldt's conjecture* says $r_p(k) = r_1 + r_2 - 1$; it lies very deep.

3. Let L/K be a finite abelian extension of global fields. Recall that $\mathrm{N}(\mathbf{A}_L^\times) \subseteq \mathbf{A}_K^\times$ is an open subgroup (this was elementary for number fields, and to handle p-extensions in characteristic $p > 0$ it rested on the local norm index inequality in the cyclic case), and more deeply the inclusion $K^\times \mathrm{N}(\mathbf{A}_L^\times)/K^\times \subseteq \mathbf{A}_K^\times/K^\times$ has finite index.

(*i*) Say that a modulus $\mathfrak{m}$ of K is *admissible* with respect to L/K if $U_{\mathfrak{m}} \subseteq \mathrm{N}(\mathbf{A}_L^\times)$. Prove that an admissible $\mathfrak{m}$ exists and that if $\mathfrak{m}$ and $\mathfrak{m}'$ are two such then so is $\gcd(\mathfrak{m}, \mathfrak{m}')$.

(*ii*) By (i), there is a "least" admissible modulus $\mathfrak{f}_{L/K}$ for L/K which divides all others. Show that $v|\mathfrak{f}_{L/K}$ if and only if v is ramified in L (even if v is real).

(*iii*) For any modulus $\mathfrak{m}$, let $\mathrm{N}(\mathfrak{m}) = \mathrm{N}_K^L(I_L(\mathfrak{m})) \subseteq I_K(\mathfrak{m})$. Recall the general isomorphism $I_K(\mathfrak{m})/P_K(\mathfrak{m}) \simeq \mathbf{A}_K^\times/K^\times U_\mathfrak{m}$ respecting change in $\mathfrak{m}$ (including how it was constructed!). Show that if $\mathfrak{m}$ is admissible with respect to L/K (i.e., if $\mathfrak{f}_{L/K}|\mathfrak{m}$) then this isomorphism carries $P_K(\mathfrak{m})\mathrm{N}(\mathfrak{m})/P_K(\mathfrak{m})$ over to $K^\times\mathrm{N}(\mathbf{A}_L^\times)/K^\times U_\mathfrak{m}$, and deduce that there is a natural isomorphism $I_K(\mathfrak{m})/P_K(\mathfrak{m})\mathrm{N}(\mathfrak{m}) \simeq \mathbf{A}_K^\times/K^\times\mathrm{N}(\mathbf{A}_L^\times)$. In particular, using results which rest on the global norm index inequality in the cyclic case, deduce that for such $\mathfrak{m}$ the quotient $I_K(\mathfrak{m})/P_K(\mathfrak{m})\mathrm{N}(\mathfrak{m})$ has size *at least* $[L : K]$. (It is the exact size, once class field theory is proved.)

(*iv*) If $\mathfrak{m}|\mathfrak{m}'$ with $\mathfrak{m}$ admissible (so $\mathfrak{m}'$ is too), prove that the natural map

$$I_K(\mathfrak{m}')/P_K(\mathfrak{m}')\mathrm{N}(\mathfrak{m}') \to I_K(\mathfrak{m})/P_K(\mathfrak{m})\mathrm{N}(\mathfrak{m})$$

is compatible with the isomorphism from each to $\mathbf{A}_K^\times/K^\times\mathrm{N}(\mathbf{A}_L^\times)$, and so it is an *isomorphism*. (This isomorphism property was classically proved without adeles by delicate arguments with weak approximation; see Lang's "Algebraic Number Theory".)

4. Using local class field theory, compute the number of degree-p abelian extensions of a field K that is a finite extension of $\mathbf{Q}_p$. Your answer will depend on the absolute ramification degree $e = e(K/\mathbf{Q}_p)$. (Hint: to compute $[\mathscr{O}_K^\times : (\mathscr{O}_K^\times)^p]$, use the snake lemma for the p-power map acting on the short exact sequence

$$1 \to 1 + \mathfrak{m}^N \to \mathscr{O}_K^\times \to Q_N \to 1$$

with N large and *finite* cokernel Q_N.)