Math 249B. Homework 1

1. Let F be a field with $\mathrm{char}(F) \neq 2$. Prove that 16 is an 8th power in F if and only if one of 2, -2, or -1 is a square in F. (Hint: $(1+\sqrt{-1})^2 = 2\sqrt{-1}$). Using this, prove that for $K = \mathbf{Q}(\sqrt{7})$, 16 is an 8th power in each completion K_v but it is not an 8th power in K.

2. (*i*) If H is a subgroup of finite index in a group G, prove that there is a *normal* subgroup $N \subseteq G$ of finite index with $N \subseteq H \subseteq G$. (Hint: If $\{g_i\}$ is a finite set of representatives for the coset space G/H then show that $N := \cap g_i H g_i^{-1}$ works.)

(*ii*) Read about profinite groups in §1 of Ch. V in "Algebraic Number Theory" by Cassels-Fröhlich (typo in the Example above Theorem 2: $\widehat{\mathbf{Z}}_p$ there should just be $\widehat{\mathbf{Z}}$). Observe as a consequence of Theorem 1 and its corollaries that closed subgroups of profinite groups (with the subspace topology) are profinite, and likewise for quotients of profinite groups by closed normal subgroups (with the quotient topology). In particular, if G is profinite then its maximal Hausdorff abelian quotient $G^{\mathrm{ab}} = G/\overline{[G,G]}$ is profinite.

3. When trying to generalize Dirichlet's theorem on primes in arithmetic progressions to number fields, one is led to first ask how to make sense of an "arithmetic progression of prime ideals". Can we generalize $(\mathbf{Z}/n\mathbf{Z})^\times$ to number fields K and relate prime ideals to elements in such a generalization? The naive guess $(\mathscr{O}_K/n\mathscr{O}_K)^\times$ is not fruitful. The right approach is to identify $(\mathbf{Z}/n\mathbf{Z})^\times$ with a "generalized ideal class group" (for $\mathbf{Q}$) in which we kill not all principal ideals but only those admitting a generator satisfying a congruential condition "mod n" (and a positivity condition in $\mathbf{Q}_\infty = \mathbf{R}$). The following gives first steps in this direction.

Let K be a global field. A *modulus* for K 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, $e_v = 0$ for all but finitely many v, $e_v \in \{0,1\}$ for real v, and $e_v = 0$ for all complex v. (The symbol $\mathfrak{p}_v$ is just pure notation, especially for archimedean v; we are simply assigning a non-negative integral weight to each place, subject to vanishing almost everywhere and funny-looking conditions at archimedean places.) We write $\mathfrak{m}|\mathfrak{m}'$ if $e_v \leq e_v'$ for all v, and we write $\mathfrak{m}_v$ to denote the v-part $\mathfrak{p}_v^{e_v}$ for each v. The *support* $\mathrm{supp}(\mathfrak{m})$ of a modulus $\mathfrak{m}$ is the finite set of v such that $e_v > 0$.

For $a_v \in K_v^\times$, we write $a_v \equiv 1 \bmod \mathfrak{m}_v$ to denote a "congruential" condition on a_v whose precise meaning depends on whether v is archimedean or not: for $v \nmid \infty$ it means $\|a_v - 1\|_v \leq q_v^{-e_v}$ when $e_v > 0$ (*e.g.*, for $e_v = 1$ it says that a_v is a 1-unit), for $v|\infty$ it means $a_v > 0$ in K_v if $e_v > 0$ (in which case K_v is *uniquely* isomorphic to $\mathbf{R}$, so the positivity condition on a_v is well-defined), and it means nothing if $e_v = 0$. Finally, in the global setting with $a \in K^\times$, we say $a \equiv 1 \bmod \mathfrak{m}$ if $a \equiv 1 \bmod \mathfrak{m}_v$ for all places v. In particular, this imposes no local condition at $v \notin \mathrm{supp}(\mathfrak{m})$ and forces $a \in \mathscr{O}_v^\times$ for non-archimedean $v \in \mathrm{supp}(\mathfrak{m})$.

The *generalized ideal class group* $\mathrm{Cl}_{\mathfrak{m}}(K)$ *with modulus* $\mathfrak{m} = \prod \mathfrak{p}_v^{e_v}$ 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 $v \notin \mathrm{supp}(\mathfrak{m})$ (i.e., it consists of formal products $\prod \mathfrak{p}_v^{n_v}$ with $n_v \in \mathbf{Z}$, $n_v = 0$ for all but finitely many v, and $n_v = 0$ for all $v \in \mathrm{supp}(\mathfrak{m})$) and $P_K(\mathfrak{m})$ is the subgroup of elements $\prod \mathfrak{p}_v^{\mathrm{ord}_v(a)}$ for $a \in K^\times$ satisfying $a \equiv 1 \bmod \mathfrak{m}$. If K is a number field then in the special case $\mathfrak{m} = 1$ (i.e., $e_v = 0$ 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 a finite non-empty set S of places of K containing the archimedean places, construct a multiplicative bijection between the set of moduli $\mathfrak{m}$ of K with $\mathrm{supp}(\mathfrak{m}) \cap S = \emptyset$ and the set of nonzero ideals of $\mathscr{O}_{K,S}$.

(*ii*) 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 $(\mathbf{Z}/N\mathbf{Z})^\times \simeq \mathrm{Cl}_{\mathfrak{m}\infty}(K)$. Characters of generalized ideal class groups are a natural (and useful!) generalization of Dirichlet characters; they have associated L-functions, as we will see later.

(*iii*) Show that $K = \mathbf{Q}(\sqrt{3})$ has class number 1 but narrow ideal class group of order 2. (Hint: $2 - \sqrt{3}$ is a fundamental unit of $\mathscr{O}_K$ but it is totally positive.) When is $\mathrm{Cl}_{\infty_1\infty_2}(K) \not\simeq \mathrm{Cl}(K)$ for real quadratic K?

(*iv*) 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. Generalized ideal class groups play a crucial role in the classical formulation of class field theory (and presumably are the reason for the very name of the theory).