Algebraic Number Theory
Math 514B Spring 2008

Problem Set 10 (The last one)
Due: Thursday, May 1st

1. Let L/K be a finite abelian extension, and $\{\mathbf{H}^{\mathfrak{m}}(L/K)\} = \{N_{L/K}(\mathbf{I}_L^{\mathfrak{m}})i(K_{\mathfrak{m},1})\}$ be its class group.

   a. Show that the class group is nonempty.

   b. Show that for any representative $\mathbf{H}^{\mathfrak{m}}$ in the the class group $\{\mathbf{H}^{\mathfrak{m}}(L/K)\}$, the Artin map induces the isomorphism $\varphi_{L/K} : \frac{\mathbf{I}_L^{\mathfrak{m}}}{\mathbf{H}^{\mathfrak{m}}} \cong \mathrm{Gal}(L/K)$.

2. Fix positive integers m and n. Denote $L = \mathbb{Q}(\zeta_m)$ and $K = \mathbb{Q}(\zeta_n)$ as cyclotomic fields, and $\mathfrak{m} = (m)p_\infty$ and $\mathfrak{n} = (n)p_\infty$ as moduli of $\mathbb{Q}$.

   a) Show that $\mathfrak{n}|\mathfrak{m}$ if and only if K is a subfield of L.

   b) Say that n divides m. Show that $\mathbf{H}^{\mathfrak{m}} = \mathbf{I}^{\mathfrak{m}} \bigcap i(\mathbb{Q}_{\mathfrak{n},1})$ is a congruence subgroup mod $\mathfrak{m}$, and that the Artin map $\varphi_{L/\mathbb{Q}}$ induces the isomorphism

$$\frac{\mathbf{I}^{\mathfrak{m}}}{i(\mathbb{Q}_{\mathfrak{m},1})} \cong \mathrm{Gal}(L/\mathbb{Q}) \qquad \text{while} \qquad \frac{\mathbf{I}^{\mathfrak{m}}}{\mathbf{H}^{\mathfrak{m}}} \cong \mathrm{Gal}(K/\mathbb{Q}).$$

3. Fix a rational prime p and n, a divisor of $p-1$. Denote L as the unique subfield of $\mathbb{Q}(\zeta_p)$ of degree n, $\mathfrak{m} = (p)p_\infty$ as a modulus of $\mathbb{Q}$, and

$$\mathbf{H}^{\mathfrak{m}} = \{(\alpha) \in i(\mathbb{Q}_{\mathfrak{m}}) | \alpha^{(p-1)/n} \equiv^* 1 \mod \mathfrak{m}\}.$$

   a) Show that $\mathbf{H}^{\mathfrak{m}}$ is a congruence subgroup modulo $\mathfrak{m}$.

   b) Show that the Artin map induces the isomorphism $\mathbf{I}^{\mathfrak{m}}/\mathbf{H}^{\mathfrak{m}} \cong \mathrm{Gal}(L/\mathbb{Q})$.

4. Let K be a number field, and $\mathfrak{m}$ be a modulus of K. We call an extension L of K a *ray class field* modulo $\mathfrak{m}$ if

   i. a prime of K that does not divide $\mathfrak{m}$ is unramified in L, and

   ii. the ray class group of K is the Galois group of L/K, i.e.

$$\varphi_{L/K} : \frac{\mathbf{I}^{\mathfrak{m}}}{i(K_{\mathfrak{m},1})} \cong \mathrm{Gal}(L/K).$$

   Moreover, when $\mathfrak{m}$ is the trivial modulus, we call L a *Hilbert class field*.

   a) Show that the ray class field, hence the Hilbert class field is unique.

   b) Show that the Hilbert class field is always a subfield of the ray class field.

5. Fix p and q as distinct odd primes. Denote $K = \mathbb{Q}(\sqrt{p^*q^*})$ and $L = \mathbb{Q}(\sqrt{p^*}, \sqrt{q^*})$ where $p^* = (-1)^{(p-1)/2}p$ and $q^* = (-1)^{(q-1)/2}q$.

   a) Show that no finite prime of K ramifies in L.

   b) Show that the infinite primes ramify if and only if $p = q = 3 \bmod 4$.

   c) Show that if not both p and q are congruent to 3 modulo 4, then K does not have class number 1.