Math 249B. Homework 9

1. Let K be a number field, and fix a finite set of non-archimedean places $v_1, \dots, v_r$ and integers $e_1, \dots, e_r \geq 1$. Show that there is a maximal finite abelian extension K'/K unramified away from ∞ and the v_i's with inertia group at v_i of exponent e_i (which includes the case of ramification degree equal to e_i). Describe the corresponding subgroup of $\mathbf{A}_K^\times/K^\times$. Hint: $(\mathscr{O}_{v_i}^\times)^{e_i}$ is open in $\mathscr{O}_{v_i}^\times$.

2. (*i*) Using class field theory, prove that $\mathbf{Q}(\zeta_5)/\mathbf{Q}(\sqrt{5})$ is the maximal finite abelian extension of $\mathbf{Q}(\sqrt{5})$ that is unramified away from 5∞ and has degree prime to 5. What if we omit the degree condition?

(*ii*) Use local class field theory and the structure of $\mathbf{Q}_p^\times$ to show that $\mathbf{Q}_p$ has exactly p totally ramified degree-p abelian extensions when $p > 2$.

(*iii*) Let K be a local field with residue field of size q. Use local class field theory to prove that any tamely ramified *abelian* finite extension of K has ramification degree dividing $q-1$ (regardless of the degree of the total extension, so most of the extension is unramified).

3. Let K be an imaginary quadratic field. In HW8 you saw that its $\mathbf{Z}_p$-rank is 2. Let L/K be the field generated by the $\mathbf{Z}_p$-extensions of K, so $\mathrm{Gal}(L/K) \simeq \mathbf{Z}_p^2$.

(*i*) Prove $L/\mathbf{Q}$ is Galois, and construct a $\mathbf{Z}_p$-linear action of $\mathrm{Gal}(K/\mathbf{Q})$ on $\mathrm{Gal}(L/K)$ (using $\mathrm{Gal}(L/\mathbf{Q})$).

(*ii*) Using that $\mathbf{Q}$ has $\mathbf{Z}_p$-rank 1(and not 2), prove that the action by $\mathrm{Gal}(K/\mathbf{Q})$ on $\Gamma \simeq \mathbf{Z}_p^2$ has its nontrivial element acting with eigenvalues $\{1, -1\}$. Deduce that for each sign $\varepsilon = \pm 1$ there is a unique quotient $\Gamma^\varepsilon \simeq \mathbf{Z}_p$ of Γ on which the non-trivial element of $\mathrm{Gal}(K/\mathbf{Q})$ acts by ε. Show that the corresponding field K^1/K is the cyclotomic $\mathbf{Z}_p$-extension; the field K^{-1}/K is called the *anti-cyclotomic* $\mathbf{Z}_p$-extension.

4. This exercise encapsulates most the the arithmetic content of the book "Primes of the form $x^2 + ny^2$", up to the issue of using elliptic functions to explicitly compute class fields of imaginary quadratic fields.

(*i*) Fix a squarefree $n > 1$ with $n \equiv 2, 3 \bmod 4$, so $K = \mathbf{Q}(\sqrt{-n})$ has $\mathscr{O}_K = \mathbf{Z}[\sqrt{-n}]$ and the discriminant is $-4n$. Consider primes $p \nmid 2n$, (i.e., primes unramified in K). Prove that $p = x^2 + ny^2$ with $x, y \in \mathbf{Z}$ if and only if $-n$ is a square mod p (i.e., p splits in K) and the two primes over p in $\mathscr{O}_K$ are *principal*.

(*ii*) Continuing with (*i*), given that p is a square mod n, so $p\mathscr{O}_K = \mathfrak{p}\mathfrak{p}'$, how can we tell when $\mathfrak{p}$ (or equivalently $\mathfrak{p}' = \overline{\mathfrak{p}}$) is principal? By the Hilbert/Artin principal ideal theorem, it is equivalent to say that $\mathfrak{p}$ splits completely in the Hilbert class field H of K! But given that p is already split in K (as p is a square mod n), this condition on $\mathfrak{p}$ says exactly that p is totally split in the Galois (generally not abelian) extension $H/\mathbf{Q}$! Since p is unramified in H (as H/K is unramified everywhere), being totally split amounts to having its common residual degree at all primes over p in $\mathscr{O}_H$ equal to 1.

Fix a lift of complex conjugation from K to H and let H^+ be its fixed field, so $H = K \otimes_{\mathbf{Q}} H^+$. (Beware that H^+ may not be Galois over $\mathbf{Q}$.) Prove that $H/\mathbf{Q}$ is totally split at a prime p if and only if $K/\mathbf{Q}$ is split at p and H^+ is unramified at p with a place of residual degree 1 at p. Deduce that if $\alpha \in \mathscr{O}_{H^+}$ is a primitive element for H^+ over $\mathbf{Q}$ with minimal polynomial $f \in \mathbf{Z}[X]$, so the inclusion $\mathbf{Z}[\alpha] \subseteq \mathscr{O}_{H^+}$ is an equality locally at all primes away from $\mathrm{disc}(f)$ (why?), then for $p \nmid 2n \cdot \mathrm{disc}(f)$,

$$p = x^2 + ny^2 \text{ for some } x, y \in \mathbf{Z} \Leftrightarrow -n \text{ is a square } \bmod p \text{ and } f(t) \equiv 0 \bmod p \text{ has a solution.}$$

(*iii*) Prove that for $p \neq 2, 23$, $p = x^2 + 23y^2$ for some $x, y \in \mathbf{Z}$ if and only if p is a square mod 23 and $t^3 - t - 1 \equiv 0 \bmod p$ has a solution. (Hint: Exercise 4 in HW2.)

Remark The preceding technique required n to be squarefree and $\equiv 2, 3 \bmod 4$ so that $\mathbf{Z}[\sqrt{-n}]$ is integrally closed. To allow general non-square $n > 1$, there is a similar argument to be made except that one has to replace the Hilbert class field of $\mathbf{Q}(\sqrt{-n})$ with another class field of $\mathbf{Q}(\sqrt{-n})$ attached to the order $\mathbf{Z}[\sqrt{-n}]$ in its ring of integers.

In general, if K is a number field then for any order $\mathscr{O} \subseteq \mathscr{O}_K$ (say with conductor $\mathfrak{c}$) the group $\mathrm{Pic}(\mathscr{O})$ (which we saw is always finite in Math 248A) admits an adelic description as quotient of $\mathbf{A}_K^\times/K^\times$ modulo an open subgroup (generalizing the case $\mathscr{O} = \mathscr{O}_K$ that we already know and love). Thus, by class field theory we get a finite abelian extension $K_\mathscr{O}/K$ equipped with a canonical isomorphism $\mathrm{Gal}(K_\mathscr{O}/K) \simeq \mathrm{Pic}(\mathscr{O})$ (and it is unramified away from $\mathfrak{c}$ but is generally not a ray class field!). This is called the *ring class field* over K attached to $\mathscr{O}$; in case $\mathscr{O} = \mathscr{O}_K$ it is the Hilbert class field of K.