In this homework, accept the existence of the Hilbert class field of a number field \( K \). That is, assume that the maximal everywhere-unramified abelian extension \( H_K \) of \( K \) is a finite extension, with \( \text{Cl}(K) \simeq \text{Gal}(H_K/K) \) by an isomorphism that carries \([p]\) to \( \text{Frob}_p \) for each prime \( p \) of \( \mathcal{O}_K \). The aim of Exercises 1–3 is to use this to deduce some truly non-obvious facts about class numbers!

In Exercise 4(iii) you will find it useful to also accept the existence of the narrow Hilbert class field, which is a finite abelian extension \( H^+_K/K \) that is maximal for being abelian and unramified at all finite places, with \( \text{Cl}_{m\mathbb{R}}(K) \simeq \text{Gal}(H^+_K/K) \) carrying \([p]\) to \( \text{Frob}_p \) where \( m\mathbb{R} \) is the unique modulus of \( K \) supported at precisely the real places. (Of course, \( H^+_K = H_K \) if \( K \) is totally complex. In general the finite abelian group \( \text{Gal}(H^+_K/H_K) \) is of exponent 2 since it is generated by decomposition groups at real places of \( H_K \); why?)

1. (i) Let \( F'/F \) be a finite extension of fields and \( E/F \) a finite Galois extension. Explain why the “composite field” \( EF' \) over \( F \) is well-defined up to \( F \)-isomorphism (hint: first prove that the ring \( E \otimes_F F' \) is a finite product of fields, all of which are \( F \)-isomorphic to each other), and if \( E/F \) is merely finite separable but not Galois show by example with \( F = \mathbb{Q} \) and with \( F = \mathbb{F}_p(t) \) that the \( F \)-isomorphism class of a composite field \( EF' \) can admit more than one possibility.

(ii) Let \( K'/K \) be a finite extension of number fields. Prove that \( H_K K' \) is an abelian everywhere unramified extension of \( K' \) and deduce that \( H_K \subseteq H_{K'} \) over the given inclusion \( K \hookrightarrow K' \).

(iii) Deduce via field-degree considerations that \( h_K \) divides \( h_{K'}[K':K] \).

(iv) Prove that if two number fields \( K \) and \( L \) are embedded in \( \mathbb{Q} \) (so \( K \cap L \) makes sense) and if \( h_K = h_L = 1 \) then \( h_{K \cap L} = 1 \).

2. Let \( K'/K \) be a finite extension of number fields.

(i) Show that the “norm map” \( \text{Cl}(K') \to \text{Cl}(K) \) carrying \([a]\) to \([N_{K'/K}(a)]\) is a well-defined homomorphism, and by checking on classes of prime ideals prove that the diagram

\[
\begin{array}{ccc}
\text{Cl}(K') & \xrightarrow{\cong} & \text{Gal}(H_{K'/K}) \\
\downarrow{N_{K'/K}} & & \downarrow{} \\
\text{Cl}(K) & \xrightarrow{\cong} & \text{Gal}(H_K/K)
\end{array}
\]

commutes, where the horizontal maps are the natural isomorphisms (described by Frobenius elements on classes of primes) and the right vertical map is the natural “restriction” map induced by the inclusion \( H_K \subseteq H_{K'} \) from Exercise 1(ii).

(ii) Using the compatibility just proved, identify the cokernel of the norm map on class groups with the Galois group \( \text{Gal}(L/K) \) for \( L \subseteq K' \) the maximal subextension over \( K \) that is abelian and everywhere unramified over \( K \). (Hint: show \( L = H_K \cap K' \) inside of \( H_{K'} \).) In particular, deduce that this norm map is surjective (and hence \( h_K|h_{K'}\)!) when \( L = K \).

(iii) Prove that if \( K'/K \) is totally ramified at some place (perhaps archimedean in case \([K':K] = 2\)) then \( h_K|h_{K'} \). As a special case, prove that if \( F \) is a CM field and \( F^+ \) is its maximal totally real subfield (a notable example being \( F = \mathbb{Q}(\zeta_m) \) and \( F^+ = \mathbb{Q}(\zeta_m + \zeta_m^{-1}) \) with \( m > 2 \)) then \( h_{F^+}|h_F \). Can you prove such divisibility relations without class field theory?

3. The Hilbert class field tower of a number field \( K \) is the increasing tower \( \{H^{(n)}(K)\} \) of iterated Hilbert class fields: \( H^{(0)}(K) = K \) and \( H^{(n+1)}(K) = H^{H^{(n)}(K)}(K) \) for \( n \geq 0 \). In the 1960’s Golod and Shafarevich found the first examples (with imaginary quadratic \( K \)) for which this tower does not terminate.

(i) Prove that each \( H^{(n)}(K) \) is Galois and everywhere unramified over \( K \). Deduce that for \( n > 0 \) we have \( H^{(n+1)}(K) = H^{(n)}(K) \) if and only if \( H^{(n+1)}(K) \) is abelian over \( H^{(n-1)}(K) \), in which case \( H^{(n)}(K) = H^{(n)}(K) \) for all \( m \geq n \).

(ii) Prove that the Hilbert class field tower terminates if and only if \( K \) is contained in a number field \( K' \) with \( h_{K'} = 1 \). In particular, if \( K \) embeds into a number field \( K' \) with class number 1 then deduce that \( K' \) can be chosen to be a solvable extension over \( K \).
4. Let $K$ be a number field and $m$ a modulus for $K$. Let $h_m(K) = \#Cl_m(K)$. In HW1, Exercise 3(iv) you showed that $Cl_m(K)$ maps onto $Cl(K)$ with finite kernel, so $h_m(K)$ is finite and in fact is a multiple of $h_K$.

(i) By using the adelic description of $Cl_m(K)$, analyze the structure of the kernel of the map $Cl_m(K) \to Cl(K)$ to deduce the following formula (which is painful to prove without the adelic viewpoint):

$$\frac{h_m(K)}{h_K} = \frac{\#(\mathcal{O}_K/\mathfrak{m}_f \cdot 2^{\#\text{supp}(\mathfrak{m}_\infty)})}{[\mathcal{O}_K^*: U(\mathfrak{m})]}$$

where $\mathfrak{m}_f$ and $\mathfrak{m}_\infty$ are respectively the “finite” and “infinite” components of $\mathfrak{m}$ and $U(\mathfrak{m})$ is the finite-index group of units $u \in \mathcal{O}_K^*$ satisfying $u \equiv 1 \mod \mathfrak{m}$ (including that $u > 0$ in $K$, for all real $v \in \text{supp}(\mathfrak{m})$).

(ii) Assume that $K$ has some real places (so $(\mathcal{O}_K^*)^{\text{tor}} = (-1)^!$). If $\text{supp}(\mathfrak{m})$ has no archimedean places (i.e., it corresponds to a nonzero ideal of $\mathcal{O}_K$) and $\mathfrak{m}_\infty$ denotes the modulus obtained by adding in the $r_1$ real places then prove that

$$\frac{h_{m\infty}(K)}{h_m(K)} = \frac{2^{r_1}}{[U(\mathfrak{m}) : U(\mathfrak{m}_\infty)]},$$

More explicitly, construct an isomorphism of groups

$$\ker(Cl_{m\infty}(K) \to Cl_m(K)) \simeq \coker(U(\mathfrak{m}) \to (-1)^r),$$

where the map in the cokernel construction is defined by forming signs of units.

(iii) Taking the special case $m = 1$, show that $h_\infty(K)/h_K$ divides $2^{r_1-1}$ with equality if and only if all elements of $\mathcal{O}_K^*$ are totally positive or totally negative and with $h_\infty(K) = h_K$ if and only if each collection of signs at the real places of $K$ is attained by some element of $\mathcal{O}_K^*$.

What does this say when $K$ is a real quadratic field? In the special case that $K$ is real quadratic with class number 1 (which conjecturally happens infinitely often) and has a totally positive fundamental unit $\varepsilon$ (e.g., $\mathbb{Q}(\sqrt{3})$ but not $\mathbb{Q}(\sqrt{2})$), use the existence of the Hilbert class field and narrow Hilbert class field to deduce that if 2 is unramified in $K$ then $K(\sqrt{-\varepsilon})/K$ must be unramified at all finite places of $K$ (including 2-adic ones) and is the narrow Hilbert class field of $K$, whereas $K(\sqrt{\varepsilon})/K$ and $K(\sqrt{-1})/K$ must be ramified at some 2-adic place of $K$. Can you predict which of $K(\sqrt{-\varepsilon})$ or $K(\sqrt{-1})$ is the narrow Hilbert class field of $K$ (i.e., even unramified at 2-adic places) when 2 is ramified in $K$ (e.g., $K = \mathbb{Q}(\sqrt{3})$)? It is very subtle how the ramification at 2-adic places of $K$ is influenced by the archimedean hypothesis on $\varepsilon$.

5. Let $k$ be a field of characteristic $p > 0$ and let $K = k((x))$ and $\mathcal{O} = k[[x]]$. Fix $f \in \mathcal{O}$, and let $f(0) \in k$ be the image of $f$ in $\mathcal{O}/\mathfrak{m} \simeq k$. (That is, $f(0)$ is the constant term in the series expansion of $f$.) The following considerations arise in the treatment (by Artin–Tate) of the $p$-part of global class field theory in characteristic $p > 0$, with $k$ a finite field.

(i) Show that if $f = h^p - h$ for some $h \in K$ then necessarily $h \in \mathcal{O}$.

(ii) Show in two ways that $f = h^p - h$ for some $h \in \mathcal{O}$ if and only if $f(0) = c^p - c$ for some $c \in k$: use Hensel’s Lemma, or reduce to the case $f(0) = 0$ (i.e., $f \in \mathfrak{m}$) and then consider $h = -\sum_{j \geq 0} j^p$. Are these two methods related?