Genus theory

Let L/K be a cyclic extension of number fields of degree n. Let $\langle\sigma\rangle$ be the Galois group of L over K (so σ has order n). Let Prin_K denote the group of non-zero principal fractional ideals of K, let I_K denote the group of all non-zero fractional ideals of K, and let $\mathrm{Cl}_K := I_K/\mathrm{Prin}_K$ denote the class group of K (and similarly with K replaced by L). The goal of this exercise is to consider the two short exact sequences

$$1 \to \mathcal{O}_L^\times \to L^\times \to \mathrm{Prin}_L \to 1$$

and

$$1 \to \mathrm{Prin}_L \to I_L \to \mathrm{Cl}_L \to 1,$$

and to compute the first several terms in the Galois cohomology long exact sequences of these two short exact sequences.

One basic tool will be Hilbert's Theorem 90, which says that $H^1(\langle\sigma\rangle, L^\times) = 1$. Another will be the computation of $h_{2/1}(\mathcal{O}_L^\times)$, which was made in class.

1. Show that $H^1(\langle\sigma\rangle, I_L)$ is trivial.

2. By considering the cohomology long exact sequences attached to the two short exact sequences above, obtain the following isomorphism and exact sequences:
(a) $\mathrm{Prin}_L^{\sigma=1}/\mathrm{Prin}_K \cong H^1(\langle\sigma\rangle, \mathcal{O}_L^\times)$.
(b) $1 \to \mathrm{Prin}_L^{\sigma=1}/\mathrm{Prin}_K \to I_L^{\sigma=1}/\mathrm{Prin}_K \to \mathrm{Cl}_L^{\sigma=1} \to H^1(\langle\sigma\rangle, \mathrm{Prin}_L) \to 1$.
(c) $1 \to H^1(\langle\sigma\rangle, \mathrm{Prin}_L) \to H^2(\langle\sigma\rangle, \mathcal{O}_L^\times) \to H^2(\langle\sigma\rangle, L^\times)$.

3. Organize the results of problem (2) into a single exact sequence

$$1 \to H^1(\langle\sigma\rangle, \mathcal{O}_L^\times) \to I_L^{\sigma=1}/\mathrm{Prin}_K \to \mathrm{Cl}_L^{\sigma=1} \to H^2(\langle\sigma\rangle, \mathcal{O}_L^\times) \to H^2(\langle\sigma\rangle, L^\times).$$

Using the explicit formulas for cohomology of a cyclic group, rewrite this in the form

$$1 \to H^1(\langle\sigma\rangle, \mathcal{O}_L^\times) \to I_L^{\sigma=1}/\mathrm{Prin}_K \to \mathrm{Cl}_L^{\sigma=1} \to H^2(\langle\sigma\rangle, \mathcal{O}_L^\times) \to \mathcal{O}_K^\times/\left(\mathcal{O}_K^\times \cap N(L^\times)\right) \to 1.$$

(Here $N(L^\times)$ denotes the image in $K^\times$ of the norm map $N : L^\times \to K^\times$, so $\mathcal{O}_K^\times \cap N(L^\times)$ is the subgroup of $\mathcal{O}_K^\times$ which are norms of elements of L. Note that this is in general a weaker condition than being a norm of an element of $\mathcal{O}_L$; indeed an element of $\mathcal{O}_K^\times$ is a norm of an element of $\mathcal{O}_L$ if and only if it is a norm of an element of $\mathcal{O}_L^\times$, and this is typically a much more restrictive condition than being a norm from $L^\times$.)

4. Let Δ denote the discriminant of L over K. If $\wp$ is a prime of K, let $e_\wp$ denote the ramification degree of $\wp$, and write $\wp^{1/e_\wp}$ to denote the unique prime of L whose $e_\wp$th power is equal to $\wp$. (So $\wp^{1/e_\wp} = \wp$ unless $\wp \mid \Delta$.)
(a) Show that $I_L^{\sigma=1} = I_K \cdot \prod_{\wp|\Delta} \wp^{\frac{1}{e_\wp}\mathbf{Z}}$, and hence that

$$I_L^{\sigma=1}/I_K \cong \prod_{\wp|\Delta} \wp^{\frac{1}{e_\wp}\mathbf{Z}/\mathbf{Z}}.$$

(b) Deduce that there is a short exact sequence

$$1 \to \mathrm{Cl}_K \to I_L^{\sigma=1}/\mathrm{Prin}_K \to \prod_{\wp|\Delta} \wp^{\frac{1}{e_\wp}\mathbf{Z}/\mathbf{Z}} \to 1.$$

5. From problems (3) and (4), and the formula for $h_{2/1}(\mathcal{O}_L^\times)$ proved in class, deduce the following formula:

$$|\,\mathrm{Cl}_L^{\sigma=1}\,| = \frac{|\,\mathrm{Cl}_K\,| \prod_v e_v}{n[\mathcal{O}_K^\times : \mathcal{O}_K^\times \cap N(L^\times)]}.$$

Here the product is taken over all places v (including the archimedean places) and e_v denotes the ramification index of the place v (hence $e_v = 1$ if v is not ramified, and so the product really need only be taken over the ramified places).

Remark. The ideals in $\mathcal{O}_L$ which are invariant under σ, but which don't have a non-trivial ideal of $\mathcal{O}_K$ as a factor, are classically called *ambig ideals*. (This comes from the German, and is sometimes translated as *ambiguous ideals*, although the translator of Hilbert claims that this translation doesn't capture the correct sense.) In more modern terms, these are essentially the same thing as the elements of the quotient group $I_L^{\sigma=1}/I_L$, and so, by problem (3) (a), are described by the ramified primes. (Problem (4) (a) is essentially a modern formulation of Hilbert's Theorem 93.)

The elements of $\mathrm{Cl}_L^{\sigma=1}$ are similarly called the *ambig ideal classes*. The formula of problem (5) is a form of what is traditionally called the *ambiguous class number formula*.

Remark. The formula of problem (5) is probably the best one can do in general, because while we have a simple formula for $h_{2/1}(\mathcal{O}_L^\times)$, it doesn't seem reasonable to expect formulas for H^1 and H^2 individually in general. However, in the case when $K = \mathbf{Q}$ and L is a quadratic extension, we *can* compute the individual H^1 and H^2, and can correspondingly obtain more information. Thus from now we suppose that we in this situation, i.e. that $K = \mathbf{Q}$ and that L is a quadratic extension.

6. If L is a quadratic extension of $\mathbf{Q}$, show that $\mathrm{Cl}_L^{\sigma=1}$ is precisely the 2-torsion subgroup of Cl_L.

7. Suppose that L is imaginary quadratic.

(a) Show that $H^1(\langle\sigma\rangle, \mathcal{O}_L^\times)$ and $H^2(\langle\sigma\rangle, \mathcal{O}_L^\times)$ both have order 2.

(b) Show that $H^1(\langle\sigma\rangle, \mathrm{Prin}_L)$ is trivial (or equivalently, that $H^2(\langle\sigma\rangle, \mathcal{O}_L^\times) \to H^2(\langle\sigma\rangle, K^\times)$ is injective, or equivalently again, that the term $[\mathcal{O}_K^\times : \mathcal{O}_K^\times \cap N(L^\times)]$ in the ambiguous class number formula is equal to 2).

(c) Using the ambiguous class number formula (or, better, the exact sequences that give rise to it), show that $\mathrm{Cl}_L[2]$ has rank equal to one less than the number of primes dividing the discriminant of L, and that it is generated by the classes of the ramified primes.

8. Suppose now that L is real quadratic, with discriminant Δ.

(a) Show (by direct computation) that $H^1(\mathcal{O}_L^\times)$ has order two or four, and that $H^2(\mathcal{O}_L^\times)$ has order one or two, depending on whether or not the norm of a fundamental unit of L is equal to -1 or 1.

(b) Using Fermat's result on writing an integer as a sum of integer squares, show that -1 is the norm of an element of L (i.e. $-1 \in N(L^\times)$) if and only if the discriminant Δ of L is not divisible by any prime that is congruent to -1 mod 4.

(c) Show that if Δ is divisible by exactly one prime (so that $L = \mathbf{Q}(\sqrt{p})$ with $p = 2$ or $p \equiv 1 \bmod 4$), then a fundamental unit in $\mathcal{O}_L$ has norm -1, and Cl_L has odd order. (We did this in class, but remind yourself how the argument goes.)

(d) Show that if Δ is divisible by at least one prime congruent to -1 mod 4, then $\mathrm{Cl}_L[2]$ has rank equal to two less than the number of primes dividing Δ, and that it is generated by the classes of the ramified primes. In particular, if $\Delta = pq$ for two primes $p \equiv q \equiv -1 \bmod 4$, then Cl_L has odd order, and hence the two ramified primes are both principal. Illustrate this phenomenon with some examples (e.g. $p = 3$ and $q = 7$, or $p = 11$ and $q = 19$).

(e) Show that if a fundamental unit in $\mathcal{O}_L$ has norm -1, then $\mathrm{Cl}_L[2]$ has rank equal to one less than the number of primes dividing the discriminant of L, and that it is generated by the classes of the ramified primes.

(f) Show that if L is real quadratic and Δ is not divisible by any $p \equiv -1 \bmod 4$ (so that -1 *is* a norm from $L^\times$, by problem (7) (b)), but the norm of a fundamental unit is 1, then $\mathrm{Cl}_L[2]$ has rank equal to one less than the number of primes dividing the discriminant of K, and it is *not* generated by the classes of the ramified primes. (These generate a subgroup of rank one less.) Give examples showing that this case can occur.

Remark. In the case when L is real quadratic, one can obtain more uniform statements by working with the *strict* class group. To this end, let $(L^\times)^+$ (bad notation, I know!) denote the elements in $L^\times$ that are *totally positive*, i.e. are positive with respect to both embeddings of L into $\mathbf{R}$. Write $(\mathcal{O}_L^\times)^+ := \mathcal{O}_L^\times \cap (L^\times)^+$, and

let Prin_L^+ denote the group of fractional ideals which are principal, admitting a totally positive generator. Define the strict class group via the short exact sequence

$$1 \to \mathrm{Prin}_L^+ \to I_L \to \mathrm{Cl}_L^+ \to 1. \tag{1}$$

There is also the short exact sequence

$$1 \to (\mathcal{O}_L^\times)^+ \to (L^\times)^+ \to \mathrm{Prin}_L^+ \to 1. \tag{2}$$

9. (a) Show that the embedding $\mathrm{Prin}_L^+ \hookrightarrow \mathrm{Prin}_L$ is an isomorphism if and only if a fundamental unit of $\mathcal{O}_L$ has norm -1.

(b) Show that the natural surjection $\mathrm{Cl}_L^+ \to \mathrm{Cl}_L$ is an isomorphism if and only if a fundamental unit of $\mathcal{O}_L^+$ has norm -1, and otherwise has a kernel of order two.

10. Show that $H^1(\langle\sigma\rangle, (L^\times)^+)$ is trivial, and that $H^2(\langle\sigma\rangle, (\mathcal{O}_L^\times)^+)$ is trivial. Deduce from this that $H^1(\langle\sigma\rangle, \mathrm{Prin}_L^+) = 1$. (Look at the long exact cohomology sequence attached to diagram (2).)

11. By taking Galois cohomology of the short exact sequence (1) defining Cl_L^+, and taking into account problem (10), show that the rank of the elementary abelian 2-group $\mathrm{Cl}_L^+[2]$ is equal to one less than the number of primes dividing the discriminant of L, and that it is generated by the classes of the ramified primes.

12. Taking into account all that you have proved, show that $\mathrm{Cl}_L[2]$ and $\mathrm{Cl}_L^+[2]$ have the same rank if the discriminant of L is not divisible by any $p \equiv -1 \bmod 4$, and that the former has rank one less than the latter otherwise.

13. Recall that for a finite abelian group A, the two-torsion subgroup $A[2]$ and the two-torsion quotient $A/2A$ are elementary abelian 2-groups of the same rank. Thus, by problem (12), the quotients $\mathrm{Cl}_L\,/2\,\mathrm{Cl}_L$ and $\mathrm{Cl}_L^+\,/2\,\mathrm{Cl}_L +$ have the same rank if the discriminant of L is not divisible by any $p \equiv -1 \bmod 4$, and that the former had rank one less than the latter otherwise. Furthermore, by (11), the rank of $\mathrm{Cl}_L^+\,/2\,\mathrm{Cl}_L^+$ is one less than the number of primes dividing the discriminant of L.

14. Suppose now that L is either imaginary or real. Let F denote the maximal everywhere unramified extension F of L which is abelian over $\mathbf{Q}$. Similarly, in the case when L is real quadratic, let F^+ denote the maximal extension of L which is unramified at all finite primes and abelian over $\mathbf{Q}$. Use the Kronecker–Weber theorem to determine F and F^+ and hence to compute $\mathrm{Gal}(F/L)$ and $\mathrm{Gal}(F^+/L)$, and show that these groups are isomorphic to $\mathrm{Cl}_L\,/2\,\mathrm{Cl}_L$ and $\mathrm{Cl}_L^+\,/2\,\mathrm{Cl}_L^+$ respectively.

15. Generalize the "strict" theory to an arbitrary cyclic extension L/K, and find a strict analogue of the ambiguous class number formula.