TOPICS IN IWASAWA THEORY

Ralph Greenberg

October 31, 2006

1 Ideal class groups.

The ideal class group of a number field $F$ is defined as the quotient group $Cl_F = \mathcal{F}_F / \mathcal{P}_F$, where $\mathcal{F}_F$ denotes the group of fractional ideals of $F$ and $\mathcal{P}_F$ denotes the subgroup of principal fractional ideals. It has been an object of intense study since the nineteenth century. One of the fundamental theorems of algebraic number theory is that $Cl_F$ is a finite, abelian group. The fact that it is abelian is obvious, but the finiteness was first proved by Kummer for the number field $F = \mathbb{Q}(\mu_p)$, where $p$ is any prime and $\mu_p$ denotes the group of $p$-th roots of unity.

If $F$ is any number field, we denote the order of $Cl_F$ by $h_F$, the class number of $F$. If $p$ is a prime, then $Cl_F[p^\infty]$ denotes the $p$-primary subgroup of $Cl_F$ and $h_F^{(p)}$ denotes its order. Iwasawa’s papers in the 1950s concern the growth of $h_F^{(p)}$ where the $F_n$’s are a sequence of number fields such that

$$F = F_0 \subset F_1 \subset F_2 \subset ... \subset F_n \subset ...$$

and $F_n$ is a cyclic extension of $F$ of degree $p^n$ for all $n \geq 0$. Here $p$ is a fixed prime. One of Iwasawa’s main theorems shows that there is some degree of regularity in the behavior of $h_F^{(p)}$. We will discuss this and other theorems of Iwasawa concerning $Cl_F[p^\infty]$ in chapter 2. In the first three sections of this chapter, we just consider a single finite extension $F'/F$. Although some of the results will be more general, the most interesting ones will concern the case where $F'/F$ is a cyclic extension, especially a cyclic $p$-extension. These results will already show some close relationships between $Cl_F[p^\infty]$ and $Cl_F[p^\infty]$ under various hypotheses. Results of this kind were undoubtedly part of the original inspiration behind Iwasawa’s work.
The first two sections of this chapter discuss the kernels and images of two natural homomorphisms between the ideal class groups \( Cl_F \) and \( Cl_{F'} \) of those number fields:

\[
N_{F'/F} : Cl_{F'} \to Cl_F, \quad J_{F'/F} : Cl_F \to Cl_{F'}
\]  

(1)

Class field theory provides the main tool for studying \( N_{F'/F} \). Under rather mild assumptions, one can prove surjectivity. Under more stringent assumptions, one can obtain some useful results about the kernel. The map \( J_{F'/F} \) is more difficult to study. It involves the structure of the unit group \( O_F^\times \), as a Galois module.

The third section concerns “genus theory,” which shows the influence of the ramified primes on \( \dim_{\mathbb{F}_p}(Cl_{F'}[p]) \) when \( F'/F \) is a cyclic \( p \)-extension. We won’t attempt to prove the most general or precise results, just enough for certain applications later on.

The fourth section concerns the so-called “reflection principle.” We consider a number field \( F \) containing \( \mu_p \), where \( p \) is a prime, and a group \( \Delta \) of automorphisms of \( F \). It is assumed that \( p \) doesn’t divide \( |\Delta| \). One can regard \( Cl_F[p] \) as a representation space for \( \Delta \) over the field \( \mathbb{F}_p \). It can be decomposed as a direct sum of the irreducible representations of \( \Delta \) over \( \mathbb{F}_p \), each with a certain multiplicity. These irreducible representations occur in pairs in a certain way. The reflection principle shows that the corresponding multiplicities for each such pair are somehow related. The idea is that one can study cyclic, unramified extensions of \( F \) of degree \( p \) by both class field theory and by Kummer theory.

The final topic in this chapter deals with a certain object which can be viewed as a generalization of the ideal class group, or, more precisely, the Pontryagin dual of \( Cl_F[p^\infty] \). It is defined as the subgroup of a Galois cohomology group consisting of cocycle classes which are unramified at all primes of \( F \). These groups are certainly closely related to ideal class groups, but over extensions of the field \( F \). It is natural to ask how various results extend to these more general objects. Section 5 will discuss some general properties of these groups. Section 6 deals with an important special case associated to one dimensional representations of \( \text{Gal}(F(\mu_p^\infty)/F) \). The behavior of these groups is intimately related to classical Iwasawa theory, as we will explain near the end of chapter 2. These last two sections will also help to make the transition to the second half of this book, where we describe even more far-reaching generalizations of the objects studied in the classical theory.
1.1 The norm map.

Consider an arbitrary finite extension $F'/F$ of number fields. We first recall the definition of two basic homomorphisms studied in algebraic number theory:

$$
N_{F'/F} : \mathcal{F}_F' \rightarrow \mathcal{F}_F, \quad J_{F'/F} : \mathcal{F}_F' \rightarrow \mathcal{F}_F.
$$

The second map $J_{F'/F}$ is defined simply by mapping an element $I \in \mathcal{F}_F$ to $I\mathcal{O}_{F'}$, the fractional ideal of $F'$ generated by $I$. The map $J_{F'/F}$ is injective, but not surjective if $[F' : F] > 1$. To define the first map, it is sufficient to define $N_{F'/F}(P')$ for every prime ideal $P'$ of $F'$ since $\mathcal{F}_{F'}$ is the free abelian group on the set of those prime ideals. For any such $P'$, let $P = P' \cap \mathcal{O}_F$, the prime ideal of $\mathcal{O}_F$ lying below $P'$, and let $f(P'/P)$ denote the residue field degree $[\mathcal{O}_{F'}/P'] : \mathcal{O}_F/P]$. Then define

$$
N_{F'/F}(P) = P^{f(P'/P)}
$$

If $[F' : F] > 1$, then the map $N_{F'/F}$ is neither injective nor surjective.

We will also let $N_{F'/F}$ denote the norm map from $F'$ to $F$ as defined in field theory. One basic result is that if $\alpha' \in F'$ and $\alpha = N_{F'/F}(\alpha')$, then the corresponding fractional ideals satisfy

$$
N_{F'/F}(\alpha'\mathcal{O}_{F'}) = \alpha\mathcal{O}_F
$$

and, consequently, we have the inclusion $N_{F'/F}(\mathcal{P}_{F'}) \subset \mathcal{P}_F$. One can then define the map $N_{F'/F}$ in (1) to be the homomorphism induced by $N_{F'/F}$ on the quotient groups $\text{Cl}_{F'}$ and $\text{Cl}_F$. That is, if $c' \in \text{Cl}_{F'}$ and $I'$ is any ideal in $c'$, then $N_{F'/F}(c') \subset \text{Cl}_F$ is defined to be the class of the ideal $N_{F'/F}(I')$.

The image of the map $N_{F'/F} : \text{Cl}_{F'} \rightarrow \text{Cl}_F$ is clearly the subgroup of $\text{Cl}_F$ generated by the classes of the ideals $P_{I'}^{f(P'/P)}$ (using the notation above). Most of our arguments in this section will be based on properties of the Artin isomorphism

$$
\text{Art}_{H/F} : \text{Cl}_F \rightarrow \text{Gal}(H/F),
$$

where $H$ denotes the Hilbert class field of $F$. The existence of this isomorphism is a special case of the Artin reciprocity law, and is discussed briefly in an appendix. We will just recall the definition of this map and the properties that we will need.

If $P$ is any prime ideal of $F$, let $\sigma_P \in \text{Gal}(H/F)$ denote the Frobenius automorphism for $P$ (or, more precisely, for any one of the prime ideals of
$H$ lying above $P$). Then we can define a homomorphism

$$\text{Frob}_{H/F} : \mathcal{F}_F \to \text{Gal}(H/F)$$

by putting $\text{Frob}_{H/F}(P) = \sigma_P$ for every prime ideal $P$ of $F$. As discussed in the appendix, this map is surjective and its kernel is precisely $\mathcal{P}_F$. The Artin isomorphism is then defined by $\text{Art}_{H/F}(c) = \text{Frob}_{H/F}(I)$ for every $c \in \text{Cl}_F$, where $I$ is any element of $c$.

We first consider the image of the norm map. Surjectivity requires only a mild assumption about $F'/F$.

**Proposition 1.1.1.** If $H \cap F' = F$, then $N_{F'|F} : \text{Cl}_{F'} \to \text{Cl}_F$ is surjective.

One immediate consequence is that if $F' \cap H = F$, then $h_F$ divides $h_{F'}$. Another consequence is that the map $N_{F'|F} : \text{Cl}_{F'}[p^\infty] \to \text{Cl}_F[p^\infty]$ will be surjective too. One can just assume that $[F' \cap H : F]$ is prime to $p$ for that assertion to hold.

**Proof.** The proof depends on the following commutative diagram from class field theory:

$$
\begin{array}{ccc}
\text{Cl}_{F'} & \longrightarrow & \text{Gal}(H'/F') \\
\downarrow N_{F'|F} & & \downarrow R_{F'|F} \\
\text{Cl}_F & \longrightarrow & \text{Gal}(H/F)
\end{array}

(4)

Here $H'$ denotes the Hilbert class field of $F'$. Note that $H \subset H'F' \subset H'$. The right vertical map is the restriction map $g \to g|_H$, where $g \in \text{Gal}(H'/F')$. The horizontal maps are the isomorphisms $\text{Art}_{H'/F'}$ and $\text{Art}_{H/F}$. The left vertical map is the norm map $N_{F'|F}$, as indicated.

The commutativity of (4) follows from the definitions. If $P'$ is any prime ideal of $F'$ and $P$ is the prime ideal of $F$ lying below $P'$, then let $\sigma_{P'} \in \text{Gal}(H'/F')$ and $\sigma_P \in \text{Gal}(H/F)$ denote the corresponding Frobenius automorphisms. Then, on the one hand, we have the following well-known property: $\sigma_{P'}|_H = \sigma_P|_{I'(P'/P)}$. Comparing this with (2), we see that

$$\text{Frob}_{H'/F'}(I')|_H = \text{Frob}_{H/F}(N_{F'/F}(I'))$$

for all $I' \in \mathcal{F}_{F'}$. The commutativity of (4) follows from this.

The restriction map $R_{F'/F} : \text{Gal}(H'/F') \to \text{Gal}(H/F)$ is surjective because of the hypothesis that $H \cap F' = F$. The surjectivity of the map $N_{F'/F}$ then follows from the above commutative diagram.
One can give an alternative proof based on the Chebotarev density theorem, applied to any finite Galois extension of $F$ containing $HF'$. Under the assumptions of the proposition, one can show that if $c \in Cl_F$, then there exist infinitely many prime ideals $P \in c$ such that $f(P'P) = 1$ for at least one prime ideal $P'$ of $F'$ lying above $P$. If $c'$ is the class of $P'$, then $N_{F'/F}(c') = c$.

Without the assumption that $F' \cap H = F$, the above proof shows that $N_{F'/F}(Cl_{F'})$ is precisely the inverse image of $Gal(H/H \cap F')$ under the map $Art_{H/F}$. Hence, if $H \cap F' \neq F$, then $N_{F'/F}$ is not surjective. Also, if $H \subset F'$, then $N_{F'/F}$ is the zero-map.

Since it will be very useful in the next chapter, we state a corollary for the $p$-primary subgroups of the class groups. We will use the notation

$$A_F = Cl_F[p^\infty], \quad A_{F'} = Cl_{F'}[p^\infty]$$

(5)

Let $L$ denote the maximal $p$-extension of $F$ contained in $H$, which we will refer to as the $p$-Hilbert class field of $F$. Thus, we have a canonical isomorphism $Art_{L/F} : A_F \rightarrow Gal(L/F)$. The following result is easily deduced from proposition 1.1.1. Alternatively, there is a diagram just like (4) which gives the result by the same argument.

**Corollary 1.1.2.** If $L \cap F' = F$, then the map $N_{F'/F} : A_{F'} \rightarrow A_F$ is surjective.

Suppose that $F'/F$ is a $p$-extension and let $G = Gal(F'/F)$. Let $I_1, \ldots, I_r$ denote the inertia subgroups of $G$ for all the primes of $F'$ which are ramified in the extension $F'/F$. It is clear that $L \cap F' = F$ if and only if $G$ is generated by those inertia subgroups. If one assumes that $F'/F$ is a cyclic $p$-extension, then $G$ has a unique maximal subgroup, namely $G_p$ (assuming that $[F' : F] > 1$). In that case, $F' \cap L = F$ if and only if $I_j \not\subset G_p$ for at least one $j$, $1 \leq j \leq r$. But this just means that $I_j = G$ for at least one $j$, or, equivalently, that there exists at least one prime which is totally ramified in $F'/F$.

Concerning the kernel of the norm map, diagram (4) shows that $\ker(N_{F'/F})$ is just the inverse image under $Art_{H'/F'}$ of $\ker(R_{F'/F})$, which is obviously $Gal(H'/HF')$. The following result gives a simple description of this kernel under certain stringent hypotheses on the extension $F'/F$. It is actually a result in the “genus theory” of cyclic extensions - a topic that we will pursue further in section 1.3. If $F'/F$ is a Galois extension, then we will continue to denote $Gal(F'/F)$ by $G$. There is a natural action of $G$ on $Cl_{F'}$, and so we
can regard $\text{Cl}_{F'}$ as a module for the group ring $\mathbb{Z}[G]$. We will use a multiplicative notation for the class group in this chapter, and so, if $\theta \in \mathbb{Z}[G]$ and $c' \in \text{Cl}_{F'}$, we will denote the action of $\theta$ on $c'$ by $(c')^\theta$. Thus, the image of $\text{Cl}_{F'}$ under $\theta$ will be denoted by $\text{Cl}_{F'}^\theta$. We will switch to an additive notation in chapter 2.

**Proposition 1.1.3.** Suppose that $F'/F$ is a finite Galois extension and that $G = \text{Gal}(F'/F)$ is cyclic. Assume also that at most one prime of $F$ is ramified in $F'/F$. Then

$$\ker(N_{F'/F}) = \text{Cl}_{F'}^{\sigma^{-1}}$$

where $\sigma$ denotes a generator of $G$.

**Proof.** The kernel of $R_{F'/F} : \text{Gal}(H'/F') \rightarrow \text{Gal}(H'/F)$ is $\text{Gal}(H'/HF')$. The extension $HF'/F$ is clearly abelian. Let $K$ denote the maximal abelian extension of $F$ contained in $H'$. Then $HF' \subseteq K$. Under the hypotheses of the proposition, we will first show that $K = HF'$.

If no prime of $F$ is ramified in $F'/F$, then $H'/F$ is an unramified extension and so we obviously have $K = H = HF'$. If there is one prime $v$ of $F$ ramified in $F'/F$, let $I$ denote the corresponding inertia subgroup of $\text{Gal}(K/F)$ (which is the same for all primes of $K$ lying above $v$). Then $K^I$ is the maximal extension of $F$ contained in $K$ which is unramified at that one prime, and therefore everywhere unramified. Thus we have $K^I = H$ and so $I = \text{Gal}(K/H)$. But we also have that $I \cap \text{Gal}(K/F') = 1$, since $K/F'$ is an unramified extension. This means that $K = HF'$, as stated.

Now we can describe $K$ in another way. Note that $H'$ is a Galois extension of $F$. This is easy to verify just using the definition of the Hilbert class field, and is left to the reader. Let $\tilde{G} = \text{Gal}(H'/F)$ and $\tilde{N} = \text{Gal}(H'/F')$. We then have an exact sequence

$$1 \rightarrow N \rightarrow \tilde{G} \rightarrow G \rightarrow 1$$

Since $N$ is abelian, there is a natural action of $G$ on $N$. Let $\sigma$ be as above, a generator of $G$. Choose an element $\tilde{\sigma} \in \tilde{G}$ such that $\tilde{\sigma}|_{F'} = \sigma$. If $\eta \in N$, then $\sigma$ acts on $\eta$ as follows: $\eta^\sigma = \tilde{\sigma}\eta\tilde{\sigma}^{-1}$. Considering $N$ as a $\mathbb{Z}[G]$-module (for which we will use an exponential notation), we then have that $\eta^{\sigma^{-1}} = \tilde{\sigma}\eta\tilde{\sigma}^{-1}\eta^{-1}$. This is a commutator in $\tilde{G}$, and so we have $N^{\sigma^{-1}} \subset D(\tilde{G})$, where $D(\tilde{G})$ denotes the commutator subgroup of $\tilde{G}$. In fact, we have

$$D(\tilde{G}) = N^{\sigma^{-1}}$$
To see this, note that $N^{\sigma-1}$ is a normal subgroup of $\tilde{G}$. Consider the exact sequence

$$1 \to N/N^{\sigma-1} \to \tilde{G}/N^{\sigma-1} \to \tilde{G}/N \to 1$$

Clearly, $N/N^{\sigma-1}$ is contained in the center of $\tilde{G}/N^{\sigma-1}$. The quotient group $\tilde{G}/N$ is cyclic. It follows that $\tilde{G}/N^{\sigma-1}$ is abelian. Hence $D(\tilde{G}) \subset N^{\sigma-1}$, and so the two subgroups do coincide.

By definition, $K$ is the subfield of $H'$ corresponding to $D(\tilde{G})$, and so we have

$$\text{Gal}(H'/K) = N^{\sigma-1}$$

We have shown before that $K = HF'$ and so we also have

$$\text{Gal}(H'/K) = \ker(\text{Gal}(H'/F') \to \text{Gal}(H/F)) = \ker(R_{F'/F})$$

Since $\text{Art}_{H'/F'} : Cl_{F'} \to N$ is a $G$-equivariant isomorphism, the commutative diagram (4) then implies that the kernel of the norm map $N_{F'/F} : Cl_{F'} \to Cl_F$ is precisely $Cl_{F'}^{\sigma-1}$, as asserted. □

Now we turn to the important case where $F'/F$ is a $p$-extension. The following result is a consequence of propositions 1.1.1 and 1.1.3 and will be a first and quite useful step for the results in the next chapter. Its proof provides a simple illustration of some of the ideas which play a role in studying the behavior of ideal class groups in $\mathbb{Z}_p$-extensions. It asserts that, under certain stringent assumptions, $A_{F'} \neq 1 \iff A_F \neq 1$.

**Proposition 1.1.4.** Let $p$ be a prime. Suppose that $F'/F$ is a Galois extension and that $G = \text{Gal}(F'/F)$ is a cyclic $p$-group. Assume also that exactly one prime of $F$ is ramified in $F'/F$ and that this prime is totally ramified. Then $p$ divides the class number of $F'$ if and only if $p$ divides the class number of $F$.

**Proof.** Proposition 1.1.1 implies that $h_F$ divides $h_{F'}$. This makes one part of the above proposition obvious: If $p$ divides $h_F$, then $p$ divides $h_{F'}$. To prove the other part, we study the norm map $N_{F'/F} : A_{F'} \to A_F$. We know that this map is surjective by corollary 1.1.2. Proposition 1.1.3 determines its kernel because $A_{F'}$ is a direct summand of $Cl_{F'}$ as a $\mathbb{Z}[G]$-module. That kernel is $A_{F'}^{\sigma-1}$, where $\sigma$ again denotes a generator for $G$. Therefore we obtain an isomorphism

$$A_{F'}/A_{F'}^{\sigma-1} \to A_F$$

(6)
The other part of the proposition is easily deduced from (6). Assume that $h_{F'}$ is divisible by $p$. Then the $p$-group $G$ is acting on the nontrivial $p$-group $A_{F'}$ and therefore the subgroup of elements fixed by the action of $G$ will also be nontrivial. That is, if we consider $\sigma - 1$ as the endomorphism of $A_{F'}$ defined by mapping $a \in A_{F'}$ to $a^{\sigma - 1} = \sigma(a) a^{-1}$, then its kernel will be nontrivial. It follows that the image $A_{F'}^{\sigma - 1}$ of that endomorphism is a proper subgroup of $A_{F'}$. Hence, (6) implies that $A_F$ must be nontrivial. Therefore, $h_F$ is indeed divisible by $p$.

**Remark 1.1.5.** Our proof of the above proposition uses the cyclicity of $G$. However, it suffices to assume that $G$ is a $p$-group. This follows easily from the case where $F'/F$ is cyclic of degree $p$, using the fact that the composition factors for a finite $p$-group are cyclic of order $p$. The ramification assumption for $F'/F$ implies that the same assumption holds for each intermediate extension. However, one can also give the following direct proof.

Suppose that $F'/F$ is a $p$-extension in which exactly one prime is ramified. We assume that this prime is totally ramified in $F'/F$. The assertion that $p|h_F \implies p|h_{F'}$ is again obvious from corollary 1.1.2, and so we just consider the converse. We will show that if $A_{F'} \neq 1$, then $A_F \neq 1$. Let $L'$ denote the $p$-Hilbert class field of $F'$. Clearly, $L'/F$ is Galois, and $\text{Gal}(L'/F)$ is a $p$-group. Now assume that $A_{F'} \neq 1$ and so $[L' : F'] > 1$. Let $P$ be the unique ramified prime in $F'/F$, let $Q$ denote any prime of $L'$ lying above $P$, and let $I_Q$ denote the inertia subgroup of $\text{Gal}(L'/F)$ for $Q$, which is determined by $P$ up to conjugacy. Since $e(Q/P) = [F'/F] < [L' : F']$, $I_Q$ is a proper subgroup of $\text{Gal}(L'/F)$. Thus there exists a maximal subgroup $M$ of $\text{Gal}(L'/F)$ which contains $I_Q$. Maximal subgroups of a $p$-group have index $p$ and are normal. The nontrivial inertia subgroups of $\text{Gal}(L'/F)$ are conjugate to $I_Q$ and hence also contained in $M$. Therefore, the fixed field $(L')^M$ is an unramified extension of $F$ and $\text{Gal}((L')^M/F) \cong \mathbb{Z}/p\mathbb{Z}$. This proves that $A_F \neq 1$.

**Remark 1.1.6.** Suppose that $p = 2$ and that the assumptions in proposition 1.1.4 are satisfied. If $[F'/F] = 2$, then the unique prime $v$ of $F$ which is ramified in the extension $F'/F$ could be an infinite prime, which would then be totally ramified. In that case, if $v'$ denotes the prime of $F'$ lying above $v$, then the hypothesis means that $F_v = \mathbb{R}$, $F'_{v'} = \mathbb{C}$, and that $F'$ is a quadratic extension of $F$ which is unramified at all other primes of $F$, finite or infinite. If one assumes only that exactly one finite prime of $F$ is ramified in $F'/F$, and
that this prime is totally ramified, then the argument can easily be adapted to prove the analogous statement for the “strict” class numbers of $F$ and $F'$, i.e. that they are either both even or both odd. Recall that the strict class group $\mathcal{C}l^{\text{str}}_F$ of a number field $F$ is the quotient group $\mathcal{F}_F/P_F^{\text{str}}$, where $P_F^{\text{str}}$ denotes the group of principal fractional ideals which are generated by a totally positive element of $F$. (An element $\alpha \in F$ is totally positive if its image under every embedding $F \to \mathbb{R}$ is positive.) If $H^{\text{str}}$ denotes the maximal abelian extension of $F$ unramified at all the finite primes of $F$, then one can use the corresponding Artin isomorphism $\text{Art}_{H^{\text{str}}/F} : \mathcal{C}l^{\text{str}}_F \to \text{Gal}(H^{\text{str}}/F)$ to prove the analogues of 1.1.1 - 1.1.4.

**Remark 1.1.7.** One can extract some information about the structure of $A_{F'}$ in the situation of proposition 1.1.4. As an illustration, let us assume that $F'/F$ is cyclic of degree $p$ and that $|A_{F'}| = p$, in addition to the ramification assumption. For brevity, let $\tau = \sigma - 1$, considered as an endomorphism of $A_{F'}$. According to (6), $A_{F'}/A_{F'}^\tau$ will then be cyclic of order $p$. Let $|A_{F'}| = p^m$, where $m \geq 1$. Then one can easily show that each of the subquotients $A_{F'}^j/A_{F'}^{j+1}$ will also be cyclic of order $p$ for $0 \leq j \leq m - 1$ and that $A_{F'}^{p^m}$ is trivial. One can regard $\tau$ as an element of the group ring for $G$ over $\mathbb{Z}$ or over $\mathbb{F}_p$. In $\mathbb{F}_p[G]$, one can easily verify that $\tau^p = 0$. Hence, in $\mathbb{Z}[G]$, we have $\tau^p \in p\mathbb{Z}[G]$. It follows that $A_{F'}^{p^m} \subseteq A_{F'}^{p}$. This implies that

$$\dim_{\mathbb{F}_p}(A_{F'}/[p]) = \dim_{\mathbb{F}_p}(A_{F'}/A_{F'}^{p^m}) \leq p.$$ 

One possibility is that $\dim_{\mathbb{F}_p}(A_{F'}/[p]) = 1$. Thus $A_{F'} \cong \mathbb{Z}/p^m\mathbb{Z}$. The automorphism group of $A_{F'}$ is then isomorphic to $(\mathbb{Z}/p^m\mathbb{Z})^\times$. Thus $\sigma(a) = a^s$ for all $a \in A_{F'}$, where $s$ is an integer not divisible by $p$. The order of $s$ modulo $p^m$ must be 1 or $p$. Thus $s^p \equiv 1 \pmod{p^m}$. Now we have

$$A_{F'} = A_{F'}^{p^m} = A_{F'}^p,$$

which means that either $m = 1$ (and so $G$ acts trivially on $A_{F'}$) or $m > 1$ and $p|(s - 1)$. Thus, if $m > 1$ and $p$ is odd, then it follows that $p^2||(s^p - 1)$ and therefore $m = 2$. Hence, for odd $p$, we must have $m \leq 2$. This kind of argument gives no information if $p = 2$. Indeed, it is conceivable that $A_{F'}$ is cyclic of order $2^m$, for any $m \geq 1$, and that $\sigma(a) = a^{-1}$ for $a \in A_{F'}$.

Another possibility is that $A_{F'}$ is an elementary abelian $p$-group. Then $m = \dim_{\mathbb{F}_p}(A_{F'})$ and we have $1 \leq m \leq p$. The endomorphism $\tau$ is a nilpotent linear mapping on the $\mathbb{F}_p$-vector space $A_{F'}$. Suppose that $c'$ is in $A_{F'}$, but
not in $A_{F'}$. Then it is clear that $c'$ generates $A_{F'}$ as a module over the group ring $\mathbb{F}_p[G]$. One then has an isomorphism

$$A_{F'} \cong \mathbb{F}_p[G]/(\tau^m)$$

of $\mathbb{F}_p[G]$-modules.

One gets a better picture of the possibilities by considering $A_{F'}$ as a module over the group ring $\mathbb{Z}_p[G]$. Choosing $c' \in A_{F'}$ as above, $A_{F'}$ is generated by $c', (c')^\tau, (c')^{\tau^2}, \ldots$ as a group and hence $c'$ is a generator for $A_{F'}$ as a $\mathbb{Z}_p[G]$-module. That is, $A_{F'}$ is a cyclic $\mathbb{Z}_p[G]$-module. Therefore, we have $A_{F'} \cong \mathbb{Z}_p[G]/I$, where $I$ is an ideal in $\mathbb{Z}_p[G]$. The requirement that $[A_{F'} : A_{F'}] = p$ just imposes a simple condition on $I$, namely that the image of $I$ in $\mathbb{Z}_p[G]/(\tau)\mathbb{Z}_p[G] \cong \mathbb{Z}_p$ has index $p$. There are actually infinitely many such ideals and, although one can get strong restrictions on the structure of $A_{F'}$ from this point of view, one cannot bound the index of $I$. Thus, even under the stringent assumptions we have made about $A_F$ and $F'/F$, there would seem to be no bound on $|A_{F'}|$ in general.

1.2 The map $J_{F'/F}$

The map $J_{F'/F}$ is induced from the natural homomorphism

$$J_{F'/F} : \mathcal{F}_F \to \mathcal{F}_{F'}$$

defined in section 1. It is obvious that $J_{F'/F}(\mathcal{P}_F) \subset \mathcal{P}_{F'}$. We obtain a homomorphism from $\text{Cl}_F$ to $\text{Cl}_{F'}$, as follows. If $c \in \text{Cl}_F$ and $I$ is an ideal in $c$, define $J_{F'/F}(c)$ to be the ideal class in $\text{Cl}_{F'}$ represented by $J_{F'/F}(I)$. Since $J_{F'/F}(\mathcal{P}_F) \subset \mathcal{P}_{F'}$, the map $J_{F'/F}$ is well-defined. The map $J_{F'/F}$ is easily seen to be injective, but $J_{F'/F}$ can have a nontrivial kernel and this can be quite difficult to study.

The kernel of $J_{F'/F}$ has been studied rather extensively in the case where $F'/F$ is an unramified abelian extension (i.e., $F' \subset H$, where $H$ denotes the Hilbert class field of $F$). Here are a few of the known results:

1. If $F'/F$ is a cyclic unramified extension of degree $p$, then $\text{ker}(J_{F'/F})$ is nontrivial.
2. $\text{Ker}(J_{H/F}) = \text{Cl}_F$. 

10
3. If $F'/F$ is any abelian, unramified extension, then $|\ker(J_{F'/F})|$ is divisible by $[F' : F]$.

The first result is known as “Hilbert’s Theorem 94.” We will prove this below. The second is the famous “Principal Ideal Theorem.” As one consequence, it is easy to show (using proposition 1.2.1 below) that if $L$ is the $p$-Hilbert class field of $F$, then $\ker(J_{L/F}) = A_F$, the $p$-primary subgroup of $\text{Cl}_F$. The third result is a generalization of both (1) and (2) proved in 1992 by Suzuki.

There are no really general results for the case where $F'/F$ is ramified. Later in this section we will give some interesting examples of ramified cyclic extensions $F'/F$ of degree $p$ such that $\ker(J_{F'/F})$ is nontrivial.

Except for proposition 1.2.1, all the results in this section will concern a finite Galois extension $F'/F$. We will always let $G = \text{Gal}(F'/F)$. Our first two results are quite simple, based just on the definitions.

**Proposition 1.2.1.** Let $n = [F' : F]$. Then

$$ (N_{F'/F} \circ J_{F'/F})(c) = c^n $$

for all $c \in \text{Cl}_F$. Consequently, if $c \in \ker(J_{F'/F})$, then the order of $c$ divides $n$. In particular, if $(h_F, n) = 1$, then $J_{F'/F}$ is injective.

**Proof.** The proposition follows immediately from the identity

$$ N_{F'/F}(J_{F'/F}(I)) = I^n. \tag{7} $$

which holds for all $I \in \mathcal{F}_F$. It suffices to verify this identity if $I$ is a prime ideal $P$ of $F$. But, in that case, using (2), the identity amounts to the familiar fact that

$$ \sum_{P'/P} e(P'/P) f(P'/P) = n $$

where the sum runs over all the prime ideals $P'$ of $F'$ lying above $P$, $e(P'/P)$ denotes the corresponding ramification index, and $f(P'/P)$ is the residue field degree defined before. Alternatively, one can easily verify the identity if $I \in \mathcal{P}_F$. It then follows for any $I$ since $\mathcal{F}_F$ is torsion-free and the index $[\mathcal{F}_F : \mathcal{P}_F]$ is finite.

**Proposition 1.2.2.** Suppose that $F'/F$ is a finite Galois extension. Consider the mapping $N_G : \text{Cl}_{F'} \to \text{Cl}_F$, defined by $N_G(c') = \prod_{\sigma \in G} \sigma(c')$. Then

$$ J_{F'/F} \circ N_{F'/F} = N_G \tag{8} $$
In particular, if \( F' \cap H = F \), then \( \text{im}(J_{F'/F}) = \text{im}(N_G) \).

**Proof.** Suppose that \( I' \in \mathcal{F}_{F'} \) and let \( I = N_{F'/F}(I') \). Then we have

\[
 IO_{F'} = \prod_{\sigma \in G} \sigma(I') \tag{9}
\]

It suffices to verify (9) if \( I' \) is a prime ideal \( P' \) of \( F' \), which is straightforward. Alternatively, one can first consider the case where \( I' \in \mathcal{P}_{F'} \). Suppose that \( I' = \alpha' \mathcal{O}_{F'} \). Then

\[
 N_{F'/F}(\alpha') = \prod_{\sigma \in G} \sigma(\alpha')
\]

and the identity (9) then follows from (3). One can prove (9) for any \( I' \in \mathcal{F}_{F'} \) by using the facts that \( \mathcal{F}_{F'} \) is torsion-free and that \( \mathcal{P}_{F'} \) has finite index.

Therefore, if \( c' \) denotes the class of \( I' \) in \( Cl_{F'} \), then it follows that the images of \( c' \) under the maps \( J_{F'/F} \circ N_{F'/F} \) and \( N_G \) are the same, namely just the class of \( IO_{F'} \) in \( Cl_{F'} \). Finally, if \( F' \cap H = F \), then proposition 1.1.1 shows that \( N_{F'/F}(Cl_{F'}) = Cl_{F} \). It then follows that \( J_{F'/F}(Cl_{F}) = N_G(Cl_{F'}) \) as stated.

If \( F'/F \) is a Galois extension, then \( \ker(J_{F'/F}) \) is somehow related to the way \( G = \text{Gal}(F'/F) \) acts on the unit group \( \mathcal{O}_{F'}^\times \) of \( F' \). This comes from the following observation: Suppose that \( c \in \ker(J_{F'/F}) \) and that \( I \) is an ideal in \( c \). That is, \( I \in \mathcal{F}_{F} \) and it generates a principal fractional ideal in \( F' \). Let \( \alpha' \) be a generator for \( I' = IO_{F'} \). The ideal \( I' \) is invariant under the action of \( G \) and so it is clear that the map

\[
 \phi : G \to \mathcal{O}_{F'}^\times
\]

defined by \( \phi(g) = g(\alpha')/\alpha' \) defines a 1-cocycle on \( G \) with values in \( \mathcal{O}_{F'}^\times \). Its cocycle class \( [\phi] \) is determined by \( c \), the map \( c \mapsto [\phi] \) is a homomorphism, and if \( [\phi] \) is trivial, then it is easy to see that \( I \in \mathcal{P}_{F} \) and hence \( c \) is trivial. Thus, in this way, one defines an injective homomorphism

\[
 \ker(J_{F'/F}) \longrightarrow H^1(F'/F, \mathcal{O}_{F'}^\times).
\]

However, principal ideals \( I' \) which are invariant under the action of \( G \) may also arise as products of ramified primes. Such ideals also define a cocycle class in \( H^1(F'/F, \mathcal{O}_{F'}^\times) \), exactly as above. These observations are behind the
following useful result. To simplify the notation, we will identify \( \mathcal{P}_F \) and \( \mathcal{F}_F \) with their images under the injective homomorphism \( J_{F' / F} \).

**Proposition 1.2.3.** Suppose that \( F' / F \) is a finite Galois extension. We have an exact sequence

\[
0 \to \ker(J_{F' / F}) \to \mathcal{P}^G_{F'}/\mathcal{P}_F \to \mathcal{F}^G_{F'}/\mathcal{F}_F \to \text{Cl}^G_{F'}/\text{Cl}_F (\text{Cl}_F)
\]

Furthermore, we have isomorphisms

\[
\mathcal{P}^G_{F'}/\mathcal{P}_F \cong H^1(F'/F, \mathcal{O}^*_{F'}), \quad \mathcal{F}^G_{F'}/\mathcal{F}_F \cong \prod_{i=1}^t \mathbb{Z}/e_i \mathbb{Z}
\]

where \( t \) denotes the number of primes of \( F \) which are ramified in \( F' / F \) and \( e_1, \ldots, e_t \) denote the corresponding ramification indices.

**Proof.** The exact sequence results by applying the snake lemma to the following commutative diagram

\[
\begin{array}{cccccc}
1 & \to & \mathcal{P}_F & \to & \mathcal{F}_F & \to & \text{Cl}_F & \to & 1 \\
& & \downarrow & & \downarrow & & \downarrow & & \\
1 & \to & \mathcal{P}^G_{F'} & \to & \mathcal{F}^G_{F'} & \to & \text{Cl}^G_{F'} & \to & 1
\end{array}
\]

(10)

The first two vertical maps are injective, and so one obtains an injective map: \( \ker(J_{F' / F}) \to \mathcal{P}^G_{F'}/\mathcal{P}_F \). Explicitly, this map can be defined as follows: If an ideal \( I \) of \( F \) becomes principal in \( F' \), \( I \mathcal{O}_{F'} = (\alpha') \), say, then its ideal class (which is in \( \ker(J_{F' / F}) \)) is mapped to the coset of \( (\alpha') \) in \( \mathcal{P}^G_{F'}/\mathcal{P}_F \).

Consider the exact sequence \( 1 \to \mathcal{O}^*_{F'} \to F'^* \to \mathcal{P}_{F'} \to 1 \), where the map \( F'^* \to \mathcal{P}_{F'} \) is defined by mapping an element of \( F'^* \) to the principal ideal it generates. The maps are \( G \)-equivariant and so one obtains the following exact sequence of Galois cohomology groups (mostly \( H^0 \)’s).

\[
1 \to \mathcal{O}^*_{F'} \to F'^* \to \mathcal{P}^G_{F'} \to H^1(F'/F, \mathcal{O}^*_{F'}) \to 1
\]

To justify the 1 at the end, we use Hilbert’s theorem 90 which states that \( H^1(F'/F, (F')^*) \) is trivial. The isomorphism \( \mathcal{P}^G_{F'}/\mathcal{P}_{F'} \cong H^1(F'/F, \mathcal{O}^*_{F'}) \) follows immediately because the image of \( F'^* \) in \( \mathcal{P}^G_{F'} \) is \( J_{F' / F}(\mathcal{P}_{F'}) \) (which we are denoting by \( \mathcal{P}_{F'} \)). This isomorphism is just as mentioned before: If \( (\alpha') \in \mathcal{P}^G_{F'} \), then one maps it to the class of the 1-cocycle \( g \to g(\alpha')/\alpha' \).
It remains to show that $\mathcal{F}_{F'}^G / \mathcal{F}_F$ is isomorphic to $\prod_{i=1}^t \mathbb{Z}/e_i\mathbb{Z}$. To see this, let $I'$ be any fractional ideal of $F'$. Then $I' \in \mathcal{F}_{F'}^G$ if and only if the prime ideal factorization of $I'$ satisfies the following condition: primes which are conjugate under the action of $G$ occur with the same exponent. This means that $I$ can be represented uniquely as a product (with integer exponents) of the ideals

$$Q_P = \prod_{P' | P} P'$$

Note that $\mathcal{F}_{F'/F}(P) = \mathcal{O}_{F'} / Q_{P'}$, where $e_P$ denotes the ramification index of $P$ in $F'/F$. Thus, we can regard $\mathcal{F}_{F'}^G$ as the free abelian group generated by the ideals $Q_P$, and $\mathcal{F}_F$ then corresponds to the subgroup generated by the ideals $Q_{P'}$. It is therefore clear that the quotient group is indeed isomorphic to $\prod_{i=1}^t \mathbb{Z}/e_i\mathbb{Z}$.

As we will now show, Dirichlet’s unit theorem has some implications concerning the cohomology group $H^1(F'/F, \mathcal{O}_{F'}^\times)$. We will assume that $F'/F$ is a cyclic extension. One can regard $\mathcal{O}_{F'}^\times$ as a $\mathbb{Z}[G]$-module. Its structure is difficult to study. However, the vector space

$$V_{\mathcal{O}_{F'}^\times} = \mathcal{O}_{F'}^\times \otimes_{\mathbb{Z}} \mathbb{Q}$$

can be regarded as a $\mathbb{Q}[G]$-module and its structure can be completely determined. In particular, this will allow us to determine the “Herbrand quotient” which is defined by

$$h(F'/F, \mathcal{O}_{F'}^\times) = |H^2(F'/F, \mathcal{O}_{F'}^\times)| / |H^1(F'/F, \mathcal{O}_{F'}^\times)|$$

The next result shows that, under certain assumptions, this ratio is $1/[F' : F]$.

**Proposition 1.2.4.** Suppose that $F'/F$ is a cyclic extension of degree $n$. If $n$ is even, assume that the real primes of $F$ are unramified in $F'/F$. Then

$$|H^1(F'/F, \mathcal{O}_{F'}^\times)| = n|H^2(F'/F, \mathcal{O}_{F'}^\times)|$$

There is a surjective homomorphism $\mathcal{O}_{F'}^\times / (\mathcal{O}_{F'}^\times)^n \rightarrow H^2(F'/F, \mathcal{O}_{F'}^\times)$. In particular, if $F'/F$ has prime degree $p$, then

$$1 \leq \dim_{F_p}(H^1(F'/F, \mathcal{O}_{F'}^\times)) \leq s + 1$$

where $s = \dim_{F_p}(\mathcal{O}_{F'}^\times / (\mathcal{O}_{F'}^\times)^n)$.
Proof. The proof depends on properties of the Herbrand quotient which we now recall. We assume that $G$ is a finite cyclic group which acts on a finitely generated, abelian group $L$. Thus, $L$ is a finitely generated $\mathbb{Z}[G]$-module. Then the cohomology groups $H^i(G, L)$ for $i \geq 1$ are finite. The Herbrand quotient $h(G, L) = |H^2(G, L)|/|H^1(G, L)|$ has the following properties:
(1) If $L$ is finite, then $h(G, L) = 1$.
(2) Suppose that $0 \to L_1 \to L \to L_2 \to 0$ is an exact sequence of finitely generated $\mathbb{Z}[G]$-modules. Then $h(G, L) = h(G, L_1)h(G, L_2)$.

Consider the $\mathbb{Q}$-vector space $V = L \otimes \mathbb{Z} \mathbb{Q}$, which is a representation space over $G$ over $\mathbb{Q}$ of dimension $d = \text{rank}_\mathbb{Z}(L)$. One can regard $L/L_{\text{tors}}$ as a $\mathbb{Z}$-lattice in $V$ which is invariant under the action of $G$. One deduces from (1) and (2) that $h(G, L)$ depends only on the isomorphism class of $V$, not on the choice of the $G$-invariant $\mathbb{Z}$-lattice $L$. This observation together with the following lemma will make it easy to compute $h(F'/F, \mathcal{O}_E^\times)$.

**Lemma 1.2.5.** Suppose that $F'/F$ satisfies the assumptions in the above proposition. Let $W$ denote the regular representation for $G$ over $\mathbb{Q}$, let $W_0 = W^G$, which is the trivial representation (of dimension 1), and let $W_1 = W/W_0$. Let $r = \text{rank}_\mathbb{Z}(\mathcal{O}_E^\times)$. Then

$$V_{\mathcal{O}_E^\times} \cong W_0^r \times W_1^{r+1}$$

as representation spaces for $G$.

**Proof.** One fact that we will use is that a cyclic group of order $m$ has a unique faithful, irreducible representation defined over $\mathbb{Q}$. Its dimension is $\phi(m)$. As a consequence of this, one can easily see that if $G$ is a finite cyclic group, then a representation space for $G$ over $\mathbb{Q}$ is determined (up to isomorphism) by the quantities $\dim \mathbb{Q}(V^H)$, where $H$ varies over all the subgroups of $G$.

Consider $V = V_{\mathcal{O}_E^\times}$. If $H$ is any subgroup of $G$, let $E = F^H$. Then $\dim \mathbb{Q}(V^H)$ is equal to the rank of the group of units of $E$ since $\mathcal{O}_E^\times = (\mathcal{O}_F^\times)^H$, and so $\mathcal{O}_E^\times \otimes \mathbb{Q} \cong V^H$. Let $r_1$ denote the number of real primes of $F$, $r_2$ the number of complex primes of $F$. Then $r = r_1 + r_2 - 1$. The real primes of $F$ are unramified in $F'/F$, and hence in $E/F$. This is obvious if $n$ is odd and is true by assumption if $n$ is even. Thus, if $m = [E : F]$, then

$$\dim \mathbb{Q}(V^H) = mr_1 + mr_2 - 1 = r + (m - 1)(r + 1)$$

On the other hand, we have $\dim \mathbb{Q}(W_0^H) = 1$ and $\dim \mathbb{Q}(W_1^H) = m - 1$. Hence, $(W_0^r \times W_1^{r+1})^H$ also has dimension $r + (m - 1)(r + 1)$, which implies the stated isomorphism. ■
The above lemma is valid without the assumption that $G$ is cyclic. If $G$ is an arbitrary finite group $G$, then it is still true that a representation space $V$ for $G$ over $\mathbb{Q}$ is determined by the quantities $\dim_{\mathbb{Q}}(V^H)$. This follows from the fact that the isomorphism class of $V$ is determined by its character which, in turn, is determined just by its restrictions to all cyclic subgroups of $G$. Those restrictions are determined by the $\dim_{\mathbb{Q}}(V^H)$’s. It suffices to know these quantities for all cyclic subgroups $H$. The proof then proceeds exactly as above.

Returning to the proof of proposition 1.2.4, we can compute $h(F'/F, \mathcal{O}_{F'}^\times)$ by considering any $G$-invariant $\mathbb{Z}$-lattice in $V$. According to lemma 1.2.5, we can choose such a lattice $L$ so that

$$L \cong L_o \times L_1^{r+1}$$

where $L_o = \mathbb{Z}$, with a trivial action of $G$, and $L_1 = I_G$, the augmentation ideal in the group ring $\mathbb{Z}[G]$. The trivial homomorphism $G \to \{1\}$ defines a ring homomorphism $\mathbb{Z}[G] \to \mathbb{Z}$ and $I_G$ is defined to be the kernel of that homomorphism. Now

$$H^1(G, \mathbb{Z}) = 0, \quad H^2(G, \mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$$

and so $h(G, E_o) = n$. It is obvious that $h(G, \mathbb{Z}[G]) = 1$. The exact sequence

$$0 \longrightarrow I_G \longrightarrow \mathbb{Z}[G] \longrightarrow \mathbb{Z} \longrightarrow 0$$

shows that $h(G, E_o)h(G, E_1) = 1$, and so we have $h(G, E_1) = 1/n$. This can also be verified directly.

These observations imply that $h(F'/F, \mathcal{O}_{F'}^\times) = n^n/n^{r+1} = 1/n$, which is precisely the first statement in the proposition. For the second part, note that

$$H^2(F'/F, \mathcal{O}_{F'}^\times) \cong \mathcal{O}_{F'}^\times / \mathcal{N}_{F'/F}(\mathcal{O}_{F'}^\times)$$

and $(\mathcal{O}_{F'}^\times)^n \subset \mathcal{N}_{F'/F}(\mathcal{O}_{F'}^\times) \subset \mathcal{O}_{F'}^\times$. To prove the final statement, note that if $n = p$ is prime, then both $H^1(F'/F, \mathcal{O}_{F'}^\times)$ and $H^2(F'/F, \mathcal{O}_{F'}^\times)$ have exponent $p$, and so their orders determine their dimensions as $\mathbb{F}_p$-vector spaces. Thus, $h(F'/F, \mathcal{O}_{F'}^\times) = p$ implies that $\dim_{\mathbb{F}_p}(H^1(F'/F, \mathcal{O}_{F'}^\times))$ is bounded above by $\dim_{\mathbb{F}_p}(H^2(F'/F, \mathcal{O}_{F'}^\times)) + 1$, which in turn is bounded above by $s + 1$. \[\blacksquare\]

**Remark 1.2.6.** Suppose that $F'/F$ is any cyclic extension of degree $p$, where $p$ is an odd prime. Proposition 1.2.1 implies that if $c \in \ker(J_{F'/F})$,
then $c^p = 1_{\text{Cl}_F}$, and so $\ker(J_{F'/F})$ is an $\mathbf{F}_p$-vector space. Propositions 1.2.3 and 1.2.4 give the following inequality:

$$\dim_{\mathbf{F}_p}(\ker(J_{F'/F})) \leq s + 1$$

where $s$ is as in proposition 1.2.4. Explicitly, we have $s = r$ if $\mu_p \not\subset F$ and $s = r + 1$ if $\mu_p \subset F$. Thus, we have a simple bound on $|\ker(J_{F'/F})|$ just in terms of the rank $r$ of the unit group of $F$.

Now suppose that $p = 2$, i.e., that $F'/F$ is any quadratic extension. The inequality for $\dim_{\mathbf{F}_p}(\ker(J_{F'/F}))$ given above is still valid. It can even be improved if some of the infinite primes of $F$ are ramified in $F'/F$. Suppose that $t_\infty$ infinite primes of $F$ are ramified in $F'/F$. In lemma 1.2.5, one then has $V \cong W_0^r \times W_1^{r+1-t_\infty}$ and so the Herbrand quotient for the $G$-module $\mathcal{O}_{F'}^\times$ turns out to be

$$h(F'/F, \mathcal{O}_{F'}^\times) = 2^r/2^{r+1-t_\infty} = 2^{t_\infty-1}$$

Thus,

$$\dim_{\mathbf{F}_p}(\ker(J_{F'/F})) \leq \dim_{\mathbf{F}_p}(H^1(F'/F, \mathcal{O}_{F'}^\times)) \leq s + 1 - t_\infty$$

Note that if $p = 2$, then $s = r + 1 = r_1 + r_2$. If $F$ is totally real and $F'$ is totally complex, then $t_\infty = r_1$ and $r_2 = 0$, in which case one finds that $\dim_{\mathbf{F}_p}(H^1(F'/F, \mathcal{O}_{F'}^\times)) \leq 1$.

We now discuss other implications of the above propositions in various special cases.

**Remark 1.2.7.** Assume that $F'/F$ is an unramified Galois extension. Then proposition 1.2.3 implies that $\ker(J_{F'/F}) \cong H^1(F'/F, \mathcal{O}_{F'}^\times)$. If we assume in addition that $F'/F$ is a cyclic extension, then proposition 1.2.4 implies that $\ker(J_{F'/F})$ has order divisible by $n = [F' : F]$, and hence is nontrivial if $n > 1$. Hilbert’s theorem 94 is a consequence. This argument is essentially the same as Hilbert’s original proof.

**Remark 1.2.8.** Consider a Galois extension $F'/F$ of degree $n$ and a prime $p$ such that $p \nmid n$. As before, we let $A_F = \text{Cl}_F[p^\infty]$, $A_{F'} = \text{Cl}_{F'}[p^\infty]$. We will consider the maps $N_{F'/F}$ and $J_{F'/F}$ just on those subgroups. Proposition 1.2.1 implies that the composite map

$$A_F \xrightarrow{J_{F'/F}} A_{F'} \xrightarrow{N_{F'/F}} A_F$$

17
is the isomorphism $a \to a^n$ for $a \in A_F$. Therefore, $J_{F'/F}$ is injective and
$J_{F'/F}(A_F)$ is a direct factor in the $\mathbb{Z}[G]$-module $A_{F'}$ isomorphic to $A_F$. More
precisely, we have

$$A_{F'} \cong J_{F'/F}(A_F) \times \ker(N_{F'/F} : A_{F'} \to A_F)$$

as $\mathbb{Z}[G]$-modules. Now $G$ acts trivially on the first factor $J_{F'/F}(A_F)$. For
the second factor, we have $\ker(N_{F'/F} : A_{F'} \to A_F) = \ker(N_G : A_{F'} \to A_{F'})$,
which we denote by $M$. It is clear that $M$ satisfies $M^G = 1$, $M_G = 1$. Hence
we have

$$A_F \cong A_{F'}^G, \quad (A_{F'})_G \cong A_F$$

where the first isomorphism is induced by $J_{F'/F}$ and the second is induced
by $N_{F'/F}$.

**Remark 1.2.9.** Assume that $F'/F$ is a cyclic $p$-extension and that exactly
one prime of $F$ is ramified in $F'/F$ (which we will assume to be a finite
prime if $p = 2$). Let $\sigma$ be a generator of $G = \text{Gal}(F'/F)$. According to (6)
in the proof of proposition 1.1.4, if we regard $\tau = \sigma - 1$ as an endomorphism
of $A_{F'}$, then $\text{coker}(\tau) \cong A_F$. Now $\text{ker}(\tau) = A_{F'}^G$ has the same order as
$\text{coker}(\tau)$. Thus, under the above assumptions, $A_F$ and $A_{F'}^G$ have the same orders. Therefore, if $J_{F'/F}$ happens to be injective, then we must have $A_{F'}^G = J_{F'/F}(A_F)$.

Under the same assumptions, one can instead apply proposition 1.2.3 to
prove that equality. We have $t = 1$ and therefore

$$\dim_{\mathbb{F}_p}(H^1(F'/F, \mathcal{O}_{F'}^\times)) - \dim_{\mathbb{F}_p}(\ker(J_{F'/F})) = 0 \text{ or } 1$$

If we make the assumption that $J_{F'/F}$ is injective, then $H^1(F'/F, \mathcal{O}_{F'}^\times)$
would be cyclic of order $p$, $H^2(F'/F, \mathcal{O}_{F'}^\times)$ would be trivial, and the map

$$\mathcal{P}_{F'}^G / \mathcal{P}_F \to \mathcal{F}_{F'}^G / \mathcal{F}_F$$

would be surjective. The last statement means that $\mathcal{F}_{F'}^G = \mathcal{F}_F \mathcal{P}_{F'}^G$. According
to a result to be proved in the next section (proposition 1.3.4), the vanishing
of $H^2(F'/F, \mathcal{O}_{F'}^\times)$ implies that every class in $\text{Cl}_{F'}^G$ contains an ideal in $\mathcal{F}_{F'}^G$.
Thus, in a different way, we again see that $J_{F'/F}(A_F) = A_{F'}^G$ under the
assumption that $J_{F'/F}$ is injective.

The above argument does not require class field theory and gives another
proof of part of proposition 1.1.4, namely the implication: $p \mid h_{F'} \Rightarrow p \mid h_F$. 

18
For if $p \mid h_{F'}$, then $A^G_{F'}$ will be nontrivial. However, $\ker(J_{F'/F}) \subseteq A_F$ and so, if $A_F$ is trivial, then $J_{F'/F}$ would be injective and hence $A^G_{F'} = J_{F'/F}(A_F)$ would be trivial too. Therefore, it must be that $p|h_F$.

**Remark 1.2.10.** This remark should be compared with remark 1.1.7. In contrast, under certain assumptions, we will obtain a lower bound on $A'_F$ instead of an upper bound. We will assume that $F'/F$ is a cyclic extension of degree $p$ in which at least one prime of $F$ is ramified, that $p|h_F$, and that the map $J_{F'/F}$ is injective. Proposition 1.2.2 would then imply that $N_G(A_{F'}) \cong A_F$. Now it is obvious that

$$A^G_{F'}[p] \subseteq \ker(N_G|_{A_{F'}})$$

and, since $p|h_F$, it is clear that $A^G_{F'}[p] \neq 1$. Hence the map $N_G|_{A_{F'}}$ has a nontrivial kernel. It follows that $|A_{F'}| > |A_F|$. This growth could be either “vertical” or “horizontal”. We will discuss two extreme cases. As in remark 1.1.7, we will illustrate the idea by assuming that $|A_F| = p$. Let $|A_{F'}| = p^m$. As we’ve just explained, we have $m \geq 2$.

First assume that $A_{F'}$ is a cyclic group. Thus, $A_{F'} \cong \mathbb{Z}/p^m\mathbb{Z}$. If $p$ is odd, then the automorphism group of $A_{F'}$ has only one subgroup of order $p$. The action of $G$ may be trivial or through that subgroup. In either case, one finds that $[A_{F'} : N_G(A_{F'})] = p$. Hence we must have $m = 2$ if $p$ is odd. However, for $p = 2$, we can’t prove anything more than the inequality $m \geq 2$.

Now assume that $A_{F'}$ is an elementary abelian $p$-group. Then one would have $\dim_{F_p}(A_{F'}) \geq p$. To see this, we will use some elementary facts about the group ring $F_p[G]$, where $G$ is a cyclic group of order $p$. As before, we let $\tau = \sigma - 1$, where $\sigma$ is a generator of $G$. The ideal $(\tau)$ of $F_p[G]$ is maximal with residue field $k_p$. We have $\tau^p = 0$. The distinct proper ideals of $F_p[G]$ are $(\tau^i)$, where $1 \leq i \leq p$. It follows that

$$(\tau^{p-1}) = F_p[G]^{(N_G)} = (N_G), \text{ where } N_G = \sum_{g \in G} g$$

Thus, if $M$ is an $F_p[G]$-module such that $\dim_{F_p}(M) = i < p$, then $\tau^i$ annihilates $M$ and hence so does $N_G$. Thus, if $N_G(M) \neq 0$, then $\dim_{F_p}(M) \geq p$. We can just apply this fact to $M = A_{F'}$. Our assumptions imply that $|N_G(A_{F'})| = p$.

**Remark 1.2.11.** We will describe two interesting examples where $F'/F$ is a ramified cyclic extension of degree $p$ and $J_{F'/F}$ has a nontrivial kernel, one
rather subtle, the other rather straightforward. We take $F = \mathbb{Q}(\mu_p)$ and assume that $p|h_F$. It is known that the divisibility $p|h_F$ holds for infinitely many primes $p$ (the so-called “irregular primes”). The exact divisibility $p|h_F$ probably holds for infinitely many $p$'s, but this is not known. The first irregular prime is $p = 37$ which does indeed satisfy the assumption. The first prime for which $p^2|h_F$ is $p = 157$. Recall that $p$ is totally ramified in $F/\mathbb{Q}$. Let $P$ denote the unique prime ideal of $F$ lying over $p$.

**Example 1.** Consider $F' = F(\sqrt[p]{\alpha})$, an extension of $F$ of degree $p$ which is ramified just at $P$. By proposition 1.1.1, we know that $p|h_F$. For all primes $p < 1000$ satisfying the assumption that $p|h_F$, it turns out that $p^2 \nmid h_F$. We cannot explain this here. It is a consequence of a rather difficult calculation due to McCallum and Sharifi. Actually, it seems reasonable to believe that this same statement will be true for any prime $p$ satisfying $p|h_F$. And so, let us assume that we have $|A_{F'}| = |A_F| = p$ in the rest of this remark. The map $N_{F'/F}: A_{F'} \rightarrow A_F$, which is certainly surjective, would then be an isomorphism. As pointed out in remark 1.2.10, it follows that $J_{F'/F}$ has a non-trivial kernel. In fact, it is clear that $\ker(J_{F'/F}) = A_F$ in this example.

**Example 2.** This is a much simpler example. Let $I$ be a nonprincipal ideal whose class $c \in \mathcal{C}l_F$ has order $p$. Then $I^p = (\alpha)$, where $\alpha \in F^\times$. Now we let $F' = F(\sqrt[p]{\alpha})$. Let $I' = J_{F'/F}(I)$. Then $I' = \sqrt[p]{\alpha}O_{F'}$ since both ideals have the same $p$-th power. Hence $c \in \ker(J_{F'/F})$. We again have $\ker(J_{F'/F}) = A_F$. Note that the field $F'$ just defined is a cyclic extension of $F$ of degree $p$, but is not uniquely determined by the class $c$, or even by the ideal $I$. For example, one can choose a different generator $\alpha \eta$ for the ideal $I^p$, where $\eta \in O_F^\times$. Under our assumptions, $F$ has only one unramified, cyclic extension of degree $p$, namely the $p$-Hilbert class field $L$ of $F$, and so it is clear that we can obtain a ramified extension $F'/F$ in this way. One sees easily that the only prime that can be ramified is $P$. We will return to this kind of example in section 4, showing that one can arrange for $F' = F(\sqrt[p]{\alpha})$ to be Galois over $\mathbb{Q}$. Of course, it is easy to verify that $L$ is Galois over $\mathbb{Q}$. As we will then see, the Galois groups $\text{Gal}(F'/\mathbb{Q})$ and $\text{Gal}(L/\mathbb{Q})$ will have different structures, making it obvious that $F' \neq L$.

The final results in this section concern an important special class of fields.

**Definition 1.2.12.** An algebraic extension $F$ of $\mathbb{Q}$ is called a CM-field if $F$ is totally complex and contains a totally real subfield $F_+$ such that $[F:F_+] = 2$. 
The simplest examples of CM-fields are complex, abelian extensions of $\mathbb{Q}$. For example, let $m \geq 3$ and let $\zeta_m$ denote a primitive $m$-th root of unity. Then $F = \mathbb{Q}(\zeta_m)$ is a CM-field and $F_+ = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$ is its maximal totally real subfield. The letters CM stand for “complex multiplication,” referring to the fact that the endomorphism ring of an abelian variety with complex multiplication is an order in a CM field. In particular, the endomorphism ring of an elliptic curve $E$ is either just $\mathbb{Z}$ or an order in an imaginary quadratic field. In the latter case, we say that $E$ has complex multiplication.

Let $\Delta = \text{Gal}(F/F_+)$, a group of order 2. Thus, $\Delta = \{1, \delta\}$, where $\delta$ denotes complex conjugation. (To be more precise, $\delta$ is the automorphism of $F$ obtained by choosing any embedding $F \to \mathbb{C}$ and restricting complex conjugation to the image of $F$.) The group $\Delta$ has two characters: the trivial character $\epsilon_0$, and the nontrivial character $\epsilon_1$. Let $\epsilon$ denote either of these two characters. Suppose that $A$ is an abelian group and that $\Delta$ acts on $A$. We let $A^{(\epsilon)}$ denote the maximal subgroup of $A$ on which $\Delta$ acts by the character $\epsilon$. That is, $A^{(\epsilon_0)} = A^\Delta$ and $A^{(\epsilon_1)}$ is the kernel of the endomorphism $N_\Delta = 1 + \delta$. If we assume that $A$ is finite and has odd order, then it is easy to see that we have the direct product decomposition $A \cong A^{(\epsilon_0)} \times A^{(\epsilon_1)}$. This is also true just under the assumption that $A$ is a torsion group and has odd exponent. In general, it is clear that $A^{(\epsilon_1)} \cap A^{(\epsilon_0)} = A[2]^\Delta$, and this will be nontrivial precisely when $A[2]$ is nontrivial. Also, it is easy to see that $2A \subseteq A^{(\epsilon_0)} + A^{(\epsilon_1)}$.

Suppose that $F'/F$ is a finite Galois extension and that both $F$ and $F'$ are CM-fields. Then one can show that $F_+/F_+$ is Galois and that $F' = F F'_+$. Thus $\text{Gal}(F'/F_+)$ can be identified with $\Delta = \text{Gal}(F/F_+)$ and then we have

$$\text{Gal}(F'/F_+) \cong \Delta \times G$$

Thus, both $\Delta$ and $G$ act on the groups $\text{Cl}_F$, $\mathcal{O}_{F'}^\times$, $\mathcal{P}_F$, and $\mathcal{F}_F$, and the actions commute with each other. There is also an action of $\Delta$ on $H^1(F'/F, \mathcal{O}_{F'}^\times)$. All of the maps and isomorphisms in proposition 1.2.3 are $\Delta$-equivariant.

One useful consequence of this is the following result.

**Proposition 1.2.13.** Suppose that $F'/F$ is a finite Galois extension, that both $F$ and $F'$ are CM-fields, and that $n = [F' : F]$ is odd. Let $\mu_{F'}$ denote the group of roots of unity in $F'$. Then

$$H^i(F'/F, \mathcal{O}_{F'}^\times)^{(\epsilon_1)} \cong H^i(F'/F, \mu_{F'})$$

21
for $i \geq 0$. If $n$ is even, then there is a homomorphism

$$H^i(F'/F, \mu_{F'}) \longrightarrow H^i(F'/F, \mathcal{O}_{F'}^{\times})^{(c_1)}$$

whose kernel and cokernel are of exponent 2.

Proof. Suppose that $A$ is any abelian group which has an action of the group $\Delta \times G$, where $G$ is a finite group and $\Delta$ has order 2. Let $\epsilon$ be one of the two characters of $\Delta$, and $\epsilon'$ the other. For any $i \geq 0$, $\Delta$ acts on the cohomology group $H^i(G, A)$. This is induced by the action of $\Delta$ on $G$ by inner automorphisms, which is trivial, and by the action of $\Delta$ on $A$. Clearly, $A^{(\epsilon)}$ is a $G$-invariant subgroup of $A$. It is also clear that $\Delta$ acts on $H^i(G, A^{(\epsilon)})$ by the character $\epsilon$. Therefore, we have a map

$$H^i(G, A^{(\epsilon)}) \longrightarrow H^i(G, A)^{(\epsilon)}.$$ (11)

This map is obviously an isomorphism when $i = 0$. For $i \geq 1$, the kernel is a quotient of $H^{i-1}(G, A/A^{(\epsilon)})$ and the cokernel is a subgroup of $H^i(G, A/A^{(\epsilon)})$. Now $\Delta$ acts on $A/A^{(\epsilon)}$ by the character $\epsilon'$. Therefore, $\Delta$ acts on the kernel and cokernel of (11) by both $\epsilon$ and $\epsilon'$ and therefore those groups have exponent 2. But $H^i(G, A^{(\epsilon)})$ and $H^i(G, A)^{(\epsilon)}$ are also killed by $|G|$ if $i \geq 1$ and hence (11) will be an isomorphism if $G$ has odd order.

Now take $A = \mathcal{O}_{F'}^{\times}$. By assumption, $G = \text{Gal}(F'/F)$ has odd order. Note that

$$(\mathcal{O}_{F'}^{\times})^{(c_1)} = \ker(N_{F'/F} : \mathcal{O}_{F'}^{\times} \rightarrow \mathcal{O}_{F}^{\times}) = \mu_{F'}$$

The first equality is clear by definition. The second follows from the fact that $\mathcal{O}_{F}^{\times}$ and $\mathcal{O}_{F'}^{\times}$ have the same rank. The statements in the proposition follow immediately.

The above proposition allows us to prove that $\ker(J_{F'/F}) \subset A_{F}^{(c_0)}$ under certain hypotheses.

Proposition 1.2.14. Suppose that $F'/F$ is a finite $p$-extension, where $p$ is an odd prime, and that both $F$ and $F'$ are CM-fields. Suppose that either (i) $F$ does not contain $\mu_p$ or (ii) $F' = F(\mu_{p^m})$ for some integer $m$. Then the map

$$A_{F}^{(c_1)} \rightarrow A_{F'}^{(c_1)}$$

induced by $J_{F'/F}$ is injective. Thus, $\ker(J_{F'/F}) \subset A_{F}^{(c_0)}$.

Note that $A_F^{(c_0)} \cong A_{F_{\mu_p}}$ and that the final conclusion in the proposition implies that $\ker(J_{F'/F}) \cong \ker(J_{F'_{\mu_p}/F_{\mu_p}})$.
Proof. First note that the both the map \( \ker (J_{F'/F}) \rightarrow \mathcal{P}^G_{F'} / \mathcal{P}_F \) and the isomorphism \( \mathcal{P}^G_{F'}/\mathcal{P}_F \cong H^1(F'/F, \mathcal{O}'_{F'}) \) are \( \Delta \)-equivariant. The first map is injective. Therefore, by proposition 1.2.13, it is enough to show that \( H^1(F'/F, \mu_{F'}) = 1 \). In case (i), the \( p \)-primary subgroup of \( \mu_F = \mu_{F'}^G \) is trivial. Since \( G \) is a \( p \)-group, it follows that the \( p \)-primary subgroup of \( \mu_{F'} \) is trivial, and hence so is \( H^1(F'/F, \mu_{F'}) \). In case (ii), we can assume that the \( p \)-primary subgroup of \( \mu_{F'} \) is \( \mu_{p^n} \). The assumption means that \( G \) acts faithfully on this group. The proposition is then a consequence of the following lemma.

Lemma 1.2.15. Let \( p \) be an odd prime. Suppose that \( G \) and \( A \) are cyclic \( p \)-groups and that \( G \) acts faithfully on \( A \). Then \( H^i(G, A) = 1 \) for all \( i \geq 1 \). The statement is true for \( p = 2 \) if \( G \) is a cyclic 2-group of order at least 4.

Proof. Since \( G \) is cyclic, the cohomology is periodic. It is enough to verify the statement for \( i = 1, 2 \). Since \( A \) is finite, the Herbrand quotient is trivial, and so it is enough to consider \( i = 1 \). Suppose that \( |G| = p^n \) and that \( |A| = p^n \). We can identify \( A \) with \( \mathbb{Z}/p^n \mathbb{Z} \) and \( \text{Aut}(A) \) with \( (\mathbb{Z}/p^n \mathbb{Z})^\times \), which we regard as a quotient group of \( \mathbb{Z}_{p}^\times \). That is, any automorphism of \( A \) can be realized as multiplication by a \( p \)-adic unit. Let \( \sigma \) be a generator of \( G \). Suppose that \( \sigma \) acts on \( A \) as multiplication by \( s \in \mathbb{Z}_{p}^\times \). Note that \( s \equiv 1 \pmod{p \mathbb{Z}_p} \) if \( p \) is odd and \( s^2 \equiv 1 \pmod{8 \mathbb{Z}_2} \) if \( p = 2 \). In either case, \( s \) is not a root of unity. The norm map \( N_G \) on \( A \) is multiplication by \( \Phi(s) \), where \( \Phi(x) \) is the cyclotomic polynomial \( 1 + x + ... + x^{p-1} \). If \( \tau \) denotes the endomorphism of \( A \) defined by \( \sigma - 1 \), then \( \tau \) acts on \( A \) as multiplication by \( s - 1 \).

Let \( a = \text{ord}_p(\Phi(s)) \) and \( b = \text{ord}_p(s - 1) \), where \( \text{ord}_p \) denotes the \( p \)-adic valuation, normalized so that \( \text{ord}_p(p) = 1 \). We can assume that \( n \geq 1 \) if \( p \) is odd. By assumption, \( n \geq 2 \) if \( p = 2 \). The lemma (for \( i = 1 \)) asserts that \( \ker (N_G) = \text{im}(\tau) \) and this is equivalent to the equality \( a + b = m \). But \( \Phi(x)(x - 1) = x^{p^n} - 1 \), and so one must just verify that

\[
\text{ord}_p(s^{p^n} - 1) = m
\]

This is true because \( G \) acts faithfully on \( A \), which implies that

\[
\text{ord}_p(s^{p^n} - 1) \geq m, \quad \text{ord}_p(s^{p^n} - 1) < m
\]

But one sees easily that \( \text{ord}_p(s^{p^n} - 1) = \text{ord}_p(s^{p^n} - 1) + 1 \) for \( n \geq 1 \) if \( p \) is odd and for \( n \geq 2 \) if \( p = 2 \). It follows that \( \text{ord}_p(s^{p^n} - 1) = m \).
Remark 1.2.15. We have stated the lemma to include $p = 2$. In that case, the argument shows that the kernel of the map $A_F^{(c_1)} \rightarrow A_{F'}^{(c_1)}$ is of exponent 2. Thus, $\Delta$ acts on that kernel by $e_0$ too.

1.3 Genus theory

Let $F'/F$ be an arbitrary cyclic extension and let $\sigma$ be a generator of $G = \text{Gal}(F'/F)$. The group $\text{Cl}_{F'}/\text{Cl}_{F'}^{-1}$ is sometimes called the “genus group” for $F'/F$ (or the group of “genera”). We will denote it by $G_{F'/F}$. The proof of proposition 1.1.3 shows that $G_{F'/F} \cong \text{Gal}(K/F')$, where $K$ is the maximal abelian extension of $F$ contained in the Hilbert class field $H$ of $F'$. The field $K$ is often referred to as the “genus field for $F'/F$.” Note that if one assumes that exactly one prime of $F$ is ramified in $F'/F$ and that this prime is totally ramified, then propositions 1.1.1 and 1.1.3 imply that $G_{F'/F} \cong \text{Cl}_F$. In general, the norm map induces a homomorphism $G_{F'/F} \longrightarrow \text{Cl}_F$. We denote its kernel by $G_{F'/F}^{(0)}$. Under the assumption that there exists at least one totally ramified prime for $F'/F$, we have an exact sequence

$$1 \longrightarrow G_{F'/F}^{(0)} \longrightarrow G_{F'/F} \longrightarrow \text{Cl}_F \longrightarrow 1$$

Furthermore, one sees easily that every element of $G_{F'/F}^{(0)}$ has order dividing $[F':F]$. Hence if $F'/F$ is a $p$-extension, then $G_{F'/F}^{(0)}$ is a $p$-group.

The reader may be familiar with genus theory for quadratic fields, which has its roots in the theory of binary quadratic forms developed by Gauss and others at the beginning of the 19-th century. If $F'$ is a quadratic extension of $\mathbb{Q}$ and $\sigma$ is the nontrivial automorphism of $F'$, then one sees easily that $\sigma(c) = c^{-1}$ for $c \in \text{Cl}_{F'}$. Thus, $G_{F'/\mathbb{Q}} = \text{Cl}_{F'/\mathbb{Q}}$. Its structure is described in the following proposition.

Proposition 1.3.1. Suppose that $[F':\mathbb{Q}] = 2$. Let $t$ denote the number of finite primes which are ramified in $F'/\mathbb{Q}$.

1. If $F'$ is an imaginary quadratic field, then $G_{F'/\mathbb{Q}} \cong (\mathbb{Z}/2\mathbb{Z})^{t-1}$.

2. Suppose that $F'$ is a real quadratic field.

   If $-1 \in \mathcal{N}_{F'/\mathbb{Q}}(F'^\times)$, then $G_{F'/\mathbb{Q}} \cong (\mathbb{Z}/2\mathbb{Z})^{t-1}$.

   If $-1 \not\in \mathcal{N}_{F'/\mathbb{Q}}(F'^\times)$, then $G_{F'/\mathbb{Q}} \cong (\mathbb{Z}/2\mathbb{Z})^{t-2}$. 

24
**Remark 1.3.2.** The two cases which occur in part (2) of this proposition can be distinguished by using the following fact for a real quadratic field $F'$.

**Fact.** We have $-1 \in \mathcal{N}_{F'/Q}(F'^\times)$ if and only if every odd prime $\ell$ ramified in $F'/Q$ satisfies $\ell \equiv 1 \pmod{4}$.

This is a consequence of “Hasse’s Norm Theorem” which states that if $F'/F$ is a cyclic extension of number fields and if $\alpha \in F'^\times$ is a local norm at all primes of $F$, then $\alpha$ is a global norm for the extension $F'/F$. However, if $\alpha \in \mathcal{O}_F^\times$, there seems to be no simple criterion for predicting when $\alpha \in \mathcal{N}_{F'/F}(\mathcal{O}_F^\times)$. In particular, one cannot predict when $-1 \in \mathcal{N}_{F'/Q}(\mathcal{O}_F^\times)$ (i.e., when $H^2(F'/F, \mathcal{O}_F^\times) = 0$). A sufficient condition is $t = 1$. For then, proposition 1.2.3 implies that $\dim_{F_2}(H^1(F'/F, \mathcal{O}_F^\times)) \leq 1$. Proposition 1.2.4 implies that $H^1(F'/F, \mathcal{O}_F^\times) \cong \mathbb{Z}/2\mathbb{Z}$ and that indeed $H^2(F'/F, \mathcal{O}_F^\times) = 0$.

We will prove proposition 1.3.1 later, deducing it from propositions 1.3.4 and 1.3.5. The analogous result for cyclic extensions of $Q$ of odd prime degree is somewhat simpler and we will prove this first. We will give two proofs to illustrate two different approaches to genus theory.

**Proposition 1.3.3.** Suppose that $F'$ is a cyclic extension of $Q$ of degree $p$, where $p$ is an odd prime. Let $t$ denote the number of primes which are ramified in $F'/Q$. Then

$$G_{F'/Q} \cong (\mathbb{Z}/p\mathbb{Z})^{t-1}$$

**Proof.** Let $K$ be the genus field for $F'/Q$. Suppose that $\ell_1, ..., \ell_t$ are the primes which are ramified in $F'/Q$. If $\ell$ is any one of these primes, let $I_\ell$ denote the corresponding inertia subgroup of $\text{Gal}(K/Q)$. It is clear that $I_\ell \cap \text{Gal}(K/F') = 1$ and hence that $I_\ell$ must be cyclic of order $p$. It is also clear that $\text{Gal}(K/Q)$ is generated by $I_{\ell_1}, ..., I_{\ell_t}$. This implies that $\text{Gal}(K/F') \cong (\mathbb{Z}/p\mathbb{Z})^u$ for some $u \leq t - 1$.

To see that $u = t - 1$, one explicitly constructs the field $K$. Using either some elementary facts about ramification theory or local class field theory, one can verify that if $\ell$ is any one of the primes ramified in $F'/Q$, then either $\ell = p$ or $\ell \equiv 1 \pmod{p}$. In both cases, there is a unique cyclic extension of $Q$ of degree $p$ in which only the prime $\ell$ is ramified: a subfield of $Q(\mu_p^\times)$ if $\ell = p$, a subfield of $Q(\mu_\ell)$ if $\ell \equiv 1 \pmod{p}$. For each $\ell_i$, $1 \leq i \leq t$, let $K_i$ denote the field just described.

25
The Kronecker-Weber theorem (which states that every finite abelian extension of $\mathbb{Q}$ is contained $\mathbb{Q}(\mu_m)$ for some $m$) implies that $F' \subset K_1...K_t$. Note also that the inertia subgroup $I_i$ of $\text{Gal}(K_1...K_t/\mathbb{Q})$ for any one of the $\ell_i$’s is of order $p$ and that $I_i \cap \text{Gal}(K_1...K_t/F')$ is trivial. This implies that $K_1...K_t \subset K$. But it is easy to see that $\text{Gal}(K_1...K_t/F') \cong (\mathbb{Z}/p\mathbb{Z})^{t-1}$. Comparing this with the inequality $u \leq t - 1$, it follows that indeed $u = t - 1$ and that the field $K$ coincides with the compositum $K_1...K_t$.

A second proof for proposition 1.3.3 can be given by studying the subgroup of $\text{Cl}_{F'}$ generated by the classes of the primes $\lambda_1,...,\lambda_t$ of $F'$ lying above $\ell_1,...,\ell_t$. For $1 \leq i \leq t$, let $c_i$ denote the class of $\lambda_i$. Each of these classes has order 1 or $p$ and is invariant under the action of $G$. One shows that this subgroup is precisely $\text{Cl}_{F'}^G$ and is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^{t-1}$. This can be proved directly, but we will justify it later as an easy consequence of proposition 1.3.5. Consider the endomorphism $\tau = \sigma - 1$ of $\text{Cl}_{F'}$, where $\sigma$ is a generator of $\text{Gal}(F'/\mathbb{Q})$. Then $\ker(\tau) = C_{F'}^G$, and $\text{coker}(\tau) = G_{F'/\mathbb{Q}}$ have the same order. Since $\tau$ annihilates $G_{F'/\mathbb{Q}}$, $N_G$ acts on that group simply as multiplication by $p$. But $N_G$ also annihilates $G_{F'/\mathbb{Q}}$ and so that group is an elementary abelian $p$-groups and therefore is indeed isomorphic to $(\mathbb{Z}/p\mathbb{Z})^{t-1}$.

Returning to cyclic extensions $F'$ of an arbitrary base field $F$, the situation is somewhat complicated by the fact that $\mathcal{O}_F^\times$ can be infinite. The genus group $G_{F'/F} = (\text{Cl}_{F'})^G$ has the same order as $(\text{Cl}_{F'})^G = C_{F'}^G$, the subgroup of $G$-invariant ideal classes. One obtains information about $\text{Cl}_{F'}$ by studying either of these groups. Both approaches will be useful in later chapters (where we apply “genus theory” to towers of cyclic extensions). Our arguments will take the second approach, studying the subgroup $C_{F'}^G$. To be more precise, we will study the possibly smaller subgroup $C_{F'}^{[G]}$, consisting of ideal classes which contain a $G$-invariant ideal. Obviously, we have

$$C_{F'}^{[G]} \cong \mathcal{F}_{F'}^G/\mathcal{P}_{F'}^G$$

and so $C_{F'}^G/C_{F'}^{[G]} \cong \text{coker}(\mathcal{F}_{F'}^G \to C_{F'}^{[G]})$, which is the subject of the next proposition.

**Proposition 1.3.4.** Suppose that $F'/F$ is a finite cyclic extension. Then there is an isomorphism

$$\text{coker}(\mathcal{F}_{F'}^G \to C_{F'}^{[G]}) \cong (\mathcal{O}_F^\times \cap N_{F'/F}(F'^\times))/N_{F'/F}(\mathcal{O}_F^\times)$$

26
In particular, if \( H^2(F'/F, \mathcal{O}_F^\times) = \mathcal{O}_F^\times / \mathcal{N}_{F'/F}^\times(\mathcal{O}_F^\times) = 1 \), then every class in \( \text{Cl}_{F'}^G \) contains a \( G \)-invariant ideal.

**Proof.** Consider the exact sequence

\[
1 \to \mathcal{P}_{F'} \to \mathcal{F}_{F'} \to \text{Cl}_{F'} \to 1
\]

This induces the following exact sequence of cohomology groups

\[
\mathcal{F}_{F'}^G \to \text{Cl}_{F'}^G \to H^1(F'/F, \mathcal{P}_{F'}) \to H^1(F'/F, \mathcal{F}_{F'})
\]

However, \( H^1(F'/F, \mathcal{F}_{F'}) = 0 \). To see this, let \( \mathcal{F}_{F',P} \) denote the group of fraction ideals of \( F' \) generated by the primes lying above \( P \), where \( P \) is any prime ideal of \( F \). Note that \( \mathcal{F}_{F',P} \) is invariant under the action of \( G \) and that \( \mathcal{F}_{F'} \) is isomorphic to a direct sum of these subgroups. For each \( P \), one has an isomorphism \( \mathcal{F}_{F',P} \cong \text{Ind}_D^G(\mathbb{Z}) \), where \( D \) is the decomposition subgroup of \( G \) for any one of the prime ideals of \( F' \) lying above \( P \) and \( \mathbb{Z} \) is given a trivial action of \( D \). Then by Shapiro’s lemma, one has

\[
H^1(F'/F, \mathcal{F}_{F',P}) \cong H^1(D, \mathbb{Z}) = \text{Hom}(D, \mathbb{Z}) = 0
\]

The assertion that \( H^1(F'/F, \mathcal{F}_{F'}) = 0 \) follows from this.

Therefore, \( \text{coker}(\mathcal{F}_{F'}^G \to \text{Cl}_{F'}^G) \cong H^1(F'/F, \mathcal{P}_{F'}) \). Using the injectivity of the map \( \mathcal{F}_{F'/F} : \mathcal{P}_F \to \mathcal{P}_{F'} \) and the assumption that \( G \) is cyclic, generated by \( \sigma \), we see that

\[
H^1(F'/F, \mathcal{P}_{F'}) \cong \ker(\mathcal{N}_{F'/F} : \mathcal{P}_{F'} \to \mathcal{P}_F)/\mathcal{P}_{F'}^{\sigma-1}
\]

We also have

\[
\ker(\mathcal{N}_{F'/F} : \mathcal{P}_{F'} \to \mathcal{P}_F) = \{ (\alpha) \in \mathcal{P}_{F'} \mid \mathcal{N}_{F'/F}(\alpha) \in \mathcal{O}_F^\times \}
\]

and

\[
\mathcal{P}_{F'}^{\sigma-1} = \{ (\alpha^{\sigma-1}) \mid \alpha \in F'^\times \} = \{ (\alpha) \in \mathcal{P}_{F'} \mid \mathcal{N}_{F'/F}(\alpha) \in \mathcal{N}_{F'/F}(\mathcal{O}_F^\times) \}
\]

Hence, it is clear that \( \mathcal{N}_{F'/F} \) defines an isomorphism

\[
H^1(F'/F, \mathcal{P}_{F'}) \to (\mathcal{O}_F^\times \cap \mathcal{N}_{F'/F}(F'^\times))/\mathcal{N}_{F'/F}(\mathcal{O}_F^\times),
\]

proving the proposition.  \( \blacksquare \)
It is sufficient to concentrate on the $p$-primary subgroups of the ideal class groups, where $p$ is a fixed prime. As before, we will let $A_F$ and $A_{F'}$ denote the $p$-primary subgroups of $Cl_F$ and $Cl_{F'}$, respectively. According to remark 1.2.8, the groups $(A_{F'})_G$ and $A_{F'}^\mathcal{G}$ are both isomorphic to $A_F$ if $p \nmid [F' : F]$. This is valid for an arbitrary Galois extension and ramification plays no role. The isomorphisms are quite simple, given by the maps $N_{F'/F}$ and $J_{F'/F}$. We will concentrate in the rest of this section on the case where $F'/F$ is a cyclic extension whose degree is a power of $p$, first considering the case of degree $p$.

Proposition 1.3.5. Suppose that $F'/F$ is a cyclic extension of degree $p$. Then

$$t - s - 1 \leq \dim_{\mathbb{F}_p}(\mathcal{O}_{F'}^{(G)}) \leq t - u$$

where $t$ is the number of distinct prime ideals of $F$ which are ramified in $F'/F$, $s = \dim_{\mathbb{F}_p}(\mathcal{O}_F^G/(\mathcal{O}_{F'}^G)^p)$, and $u = \min(t, 1)$.

Proof. We will use the exact sequence in proposition 1.2.3. Note that $G$ acts trivially on all the groups occurring there, that $N_G$ annihilates them and acts simply as multiplication by $p$. Hence those groups are all vector spaces over $\mathbb{F}_p$. The image of the map

$$\mathcal{F}_{F'}^G / \mathcal{F}_F \longrightarrow Cl_{F'}^G / J_{F'/F}(Cl_F)$$

is $Cl_{F'}^G / J_{F'/F}(Cl_F)$. Thus we have the following relationship between orders of groups

$$|Cl_{F'}^G| \cdot |J_{F'/F}(Cl_F)|^{-1} = p^t \cdot |H^1(F'/F, \mathcal{O}_{F'}^\times)|^{-1} \cdot |\ker(J_{F'/F})|$$

Obviously, $|Cl_{F'}| = |\ker(J_{F'/F})| \cdot |J_{F'/F}(Cl_F)|$. Together with proposition 1.2.4 (assuming, for $p = 2$, that the hypothesis there for the infinite primes is satisfied), we then obtain the following formula

$$|Cl_{F'}^G| = p^{-1} \cdot |Cl_{F'}| \cdot |H^2(F'/F, \mathcal{O}_{F'}^\times)|^{-1}$$

On the other hand, proposition 1.3.4 shows that

$$|H^2(F'/F, \mathcal{O}_{F'}^\times)| = p^v \cdot |Cl_{F'}^G / Cl_{F'}^{[G]}|$$

where $p^v = [\mathcal{O}_{F'}^\times : \mathcal{O}_{F'}^\times \cap N_{F'/F}(F_{F'}^\times)]$. Thus, we obtain the formula

$$|Cl_{F'}^G| = p^{t-1-v} \cdot |Cl_{F'}|$$

28
Therefore, \(|G_{F'/F}^\circ| = p^{t-1-v}\). Since \(v \geq 0\), one immediately obtains the upper bound on \(\dim_{\mathbb{F}_p}(G_{F'/F}^\circ)\). To obtain the lower bound, we use the fact that \(|H^2(F'/F, \mathcal{O}_{F'}^\times)|\) is divisible by \(p^v\). That implies that \(v \leq s\) according to proposition 1.2.4.

If \(p = 2\), the assumptions in proposition 1.2.4 may fail to be satisfied. There may also be some infinite primes of \(F\) ramified in \(F_\infty\). One then has to slightly modify the above calculation. If \(t_\infty\) denotes the number of such primes, then according to a remark 1.2.6, the Herbrand quotient \(h(F'/F, \mathcal{O}_{F'}^\times) = 2^{t_\infty-1}\). Hence, in the above argument, we get

\[
|Cl_{F'}^G| = p^{t-(1-t_\infty)-v} \cdot |Cl_F| = p^{t+t_\infty-1-v}
\]

One then has the lower bound \(t+t_\infty-s-1\) on the \(p\)-rank of \(Cl_{F'}^G\), which again implies the stated result. Note that \(t + t_\infty\) is the total number of ramified primes in the extension \(F'/F\). ■

We return now to the special cases mentioned at the beginning of this section, where we take \(F = \mathbb{Q}\). The facts that \(h_{\mathbb{Q}} = 1\) and the unit group \(\mathbb{Z}^\times\) has order 2 simplify things considerably.

First we complete the alternative proof of proposition 1.3.3. Thus, assume that \(F''\) is a cyclic extension of \(\mathbb{Q}\) of degree \(p\), where \(p\) is an odd prime. Obviously, we have \(H^2(F''/F, \mathcal{O}_{F''}^\times) = 0\), and so proposition 1.3.4 shows that \(Cl_{F''}^G\) is generated by the classes containing ramified primes. Thus \(Cl_{F''}^G \cong (\mathbb{Z}/p\mathbb{Z})^u\) for some \(u \leq t\), where \(t\) denotes the number of ramified primes in \(F'/\mathbb{Q}\). But the classes of these ramified primes are not independent. One obtains essentially one nontrivial relationship because \(P_{F''}^G/P_{\mathbb{Q}} \cong H^1(F''/F, \mathcal{O}_{F''}^\times)\) is a group of order \(p\), as follows from proposition 1.2.3 and the vanishing of \(H^2(F'/F, \mathcal{O}_{F'}^\times)\). Hence \(u = t - 1\).

Thus we see that \(Cl_{F''}^G \cong (\mathbb{Z}/p\mathbb{Z})^{t-1}\). This implies that \(G_{F''}/\mathbb{Q} = Cl_{F''}/Cl_{F''}^{t-1}\) has order equal to \(p^{t-1}\). Now if we regard \(Cl_{F''}\) as a \(\mathbb{Z}[G]\)-module, it is clear that \(N_G \in \text{Ann}(Cl_{F''})\). Also, \(N_G\) acts as multiplication by \(p\) on \(G_{F''}/\mathbb{Q}\). Therefore, \(G_{F''}/\mathbb{Q}\) has exponent \(p\) and must be indeed be isomorphic to \((\mathbb{Z}/p\mathbb{Z})^{t-1}\).

We now prove proposition 1.3.1. Assume first that \(F'\) is imaginary quadratic. Then \(N_{F'/\mathbb{Q}}(\alpha) > 0\) for all \(\alpha \in F'^\times\), and so proposition 1.3.4 implies that \(Cl_{F'}^G\) is again generated by the classes of the ramified primes. Also, there is essentially just a single nontrivial relation between those classes.
because \( H^1(F'/F, \mathcal{O}_{F'}^\times) \cong \mathbb{Z}/2\mathbb{Z} \), which is easily verified directly since \( \mathcal{O}_{F'}^\times \) is just finite. Hence \( Cl_{F'}^G \cong (\mathbb{Z}/2\mathbb{Z})^{t-1} \).

If \( F' \) is a real quadratic field and \(-1 \notin \mathcal{N}_{F'/\mathbb{Q}}(F'^{\times})\), then the classes of the ramified primes generate \( Cl_{F'}^G \), just as in the case of an imaginary quadratic field. But this time \( H^1(F'/F, \mathcal{O}_{F'}^\times) \cong (\mathbb{Z}/2\mathbb{Z})^2 \) by proposition 1.2.3. Therefore, there will be two independent relations between those ideal classes, and so \( Cl_{F'}^G \cong (\mathbb{Z}/2\mathbb{Z})^{t-2} \). Note that we must have \( t \geq 2 \), as we pointed out earlier.

If \(-1 \in \mathcal{N}_{F'/\mathbb{Q}}(\mathcal{O}_{F'}^\times)\), then \( H^2(F'/F, \mathcal{O}_{F'}^\times) = 0 \) and the argument is the same as in the case where \( F'/\mathbb{Q} \) is cyclic of odd prime degree. But if \(-1 \notin \mathcal{N}_{F'/\mathbb{Q}}(F'^{\times})\), but \(-1 \notin \mathcal{N}_{F'/\mathbb{Q}}(\mathcal{O}_{F'}^\times)\), then the classes of the ramified primes generate a subgroup of index 2 in \( Cl_{F'}^G \). Also, \( H^2(F'/F, \mathcal{O}_{F'}^\times) \cong \mathbb{Z}/2\mathbb{Z} \) and \( H^1(F'/F, \mathcal{O}_{F'}^\times) \cong (\mathbb{Z}/2\mathbb{Z})^2 \). Thus, this subgroup is isomorphic to \( (\mathbb{Z}/2\mathbb{Z})^{t-2} \). It follows that \( Cl_{F'}^G \cong (\mathbb{Z}/2\mathbb{Z})^{t-1} \).

In all these cases, \( Cl_{F'}^G = Cl_{F'}[2] \) and \( \mathcal{G}_{F'/\mathbb{Q}} = Cl_{F'/\mathbb{Q}}/Cl_{F'}^G \) are elementary abelian 2-groups of the same order, and so must be isomorphic, proving proposition 1.3.1.

Proposition 1.3.4 has some useful consequences if \( F \) and \( F' \) are CM-fields.

**Corollary 1.3.6.** Suppose that \( F'/F \) is a finite \( p \)-extension, where \( p \) is an odd prime, and that both \( F \) and \( F' \) are CM-fields. Let \( \epsilon_1 \) be the nontrivial character of \( \Delta = \text{Gal}(F'/F_{+}) \cong \text{Gal}(F/F_{+}) \). Suppose that either \((i)\) \( F \) does not contain \( \mu_p \) or \((ii)\) \( F' = F(\mu_{p^m}) \) for some integer \( m \). Then

\[
H^2(F'/F, \mathcal{O}_{F'}^\times)^{\langle \epsilon_1 \rangle} \cong H^2(F'/F, \mu_{p^m}) = 1
\]

and every class in \( \left( A_{F'}^{\langle \epsilon_1 \rangle} \right)^{G} \) contains a \( G \)-invariant ideal.

**Proof.** The argument is similar to that for proposition 1.2.14. One uses proposition 1.2.13 for \( i = 2 \) instead of \( i = 1 \). The isomorphism in proposition 1.3.4 is \( \Delta \)-equivariant and hence preserves the \( \epsilon_1 \)-components of the groups in question. In case \((i)\), \( H^2(F'/F, \mu_{p^m}) \) obviously vanishes. In case \((ii)\), one can apply lemma 1.2.15 to see that that group vanishes.

**Corollary 1.3.7.** Suppose that the assumptions in corollary 1.3.6 are satisfied. Let \([F' : F] = p^n\). Consider the following set of primes of \( F_{+} \):

\[
S = \{ v \mid v \text{ splits in } F/F_{+} \text{ and } v \text{ is ramified in } F'/F_{+} \}
\]
For each $v$ in this set, let $p^{\alpha_v}$ denote its ramification index in $F'_v/F_v$. Then

$$(A_{F'}^{(c_1)})^G/J_{F'/F}(A_{F'}^{(c_1)}) \cong \prod_{v \in S} \mathbb{Z}/p^{\alpha_v} \mathbb{Z}$$

In particular, if every prime of $F_+$ lying in $S$ is totally ramified in $F'_v/F_v$, then $(A_{F'}^{(c_1)})^G$ contains a subgroup isomorphic to $(\mathbb{Z}/p^n \mathbb{Z})^{|S|}$.

**Proof.** We will apply proposition 1.2.3. The homomorphisms and isomorphisms in that proposition are all $\Delta$-equivariant. Since $G = \text{Gal}(F'/F)$ is a $p$-group, all the groups occurring there are actually finite $p$-groups. Since $p$ is odd, the exactness of the sequence and the two isomorphisms are still valid if we take the $\epsilon_1$-components of the groups. Note also that since $\text{Cl}_{F'}^G/J_{F'/F}(\text{Cl}_F)$ is a $p$-group, it is isomorphic to $A_{F'}^G/J_{F'/F}(A_F)$. The $\epsilon_1$-component of that group is $(A_{F'}^{(c_1)})^G/J_{F'/F}(A_F)$. Corollary 1.3.6 implies that the map

$$(\mathcal{F}_{F'}^G/\mathcal{F}_F)^{(c_1)} \longrightarrow (A_{F'}^{(c_1)})^G/J_{F'/F}(A_{F'}^{(c_1)})$$

is surjective. In fact, it is an isomorphism because $H^2(F'/F, \mathcal{O}_{F'})^{(c_1)} = 1$. Finally, the definition of $S$ implies that for every $v \in S$, there are two primes of $F$ lying above $v$ which are permuted by $\Delta$. They both have ramification index $p^{\alpha_v}$ in $F'/F$. Using the final isomorphism in proposition 1.2.3, we obtain

$$(\mathcal{F}_{F'}^G/\mathcal{F}_F)^{(c_1)} \cong \prod_{v \in S} \mathbb{Z}/p^{\alpha_v} \mathbb{Z}$$

and so the stated isomorphism in the corollary follows. The particular case is immediate.

\[ \square \]

### 1.4 The reflection principle

Let $p$ be a prime. Suppose that $F$ is a number field which contains $\mu_p$. As before, let $L$ denote the $p$-Hilbert class field of $F$. The idea to be pursued in this section is that a cyclic unramified extension $K$ of $F$ of degree $p$ is related to the ideal class group of $F$ in two different ways. One comes from class field theory, the other from Kummer theory. Briefly,

1. Class field theory shows that there is a canonical surjective homomorphism $\text{Cl}_F \rightarrow \text{Gal}(K/F)$. This arises as the composition of the Artin isomorphism $\text{Cl}_F[p^\infty] \rightarrow \text{Gal}(L/F)$ with the restriction map $\text{Gal}(L/F) \rightarrow \text{Gal}(K/F)$. 

31
Thus $\text{Gal}(K/F)$ can be identified with a certain quotient group of $\text{Cl}_F[p^\infty]$ of order $p$.

2. Kummer theory shows that $K = F(\sqrt[p]{\alpha})$, where $\alpha \in F^\times$. Since $K/F$ is unramified, it is clear that $\alpha \mathcal{O}_F = I^p$, where $I \in \mathcal{F}_F$. Let $c$ denote the class of $I$ in $\text{Cl}_F$. Then $c$ has order 1 or $p$. It is easy to see that the subgroup of $\text{Cl}_F$ generated by $c$ is uniquely determined by the extension $K/F$. This follows from the fact that the subgroup of $F^\times/(F^\times)^p$ generated by the coset $\alpha(F^\times)^p$ is determined by $K$.

The class $c$ defined in (2) can be trivial. This would be true if and only if $K = F(\sqrt[p]{\eta})$, where $\eta \in \mathcal{O}_F^\times$. Note also that if $\alpha \in F^\times$ is such that $\alpha \mathcal{O}_F = I^p$, then the Kummer extension $F(\sqrt[p]{\alpha})/F$ can only be ramified at primes of $F$ dividing $p$, but is not necessarily unramified.

Suppose that $A$ is a subset of $F^\times$ containing $(F^\times)^p$. Kummer theory gives an isomorphism

$$\kappa_A : A/(F^\times)^p \to \text{Hom}(\text{Gal}(F(\sqrt{A})/F), \mu_p)$$

(12)

Here we let $F(\sqrt{A})$ denote the extension of $F$ generated by \{\sqrt[p]{\alpha} | \alpha \in A\}. The map $\kappa_A$ is easy to define. For each $\alpha \in A$, let $\alpha' \in F(\sqrt{A})$ satisfy $\alpha'^p = \alpha$. Then one defines a cocyle $\phi$ with values in $\mu_p$ by $\phi(g) = g(\alpha')/\alpha'$ for all $g \in \text{Gal}(F(\sqrt{A})/F)$. It is easy to show that the cocyle class $[\phi]$ is determined by the coset of $\alpha$ in $A/(F^\times)^p$. The Kummer isomorphism $\kappa_A$ is defined by mapping that coset to $[\phi]$. Injectivity is straightforward to verify. Surjectivity is a consequence of Hilbert’s theorem 90.

Suppose that $\Delta$ is a group of automorphisms of $F$ and that $A$ is invariant under the action of $\Delta$. The extension $F(\sqrt{A})$ is then a Galois extension of the fixed field $F^\Delta$. It follows that $\Delta$ acts (by inner automorphisms) on $\text{Gal}(F(\sqrt{A})/F)$. Now $\Delta$ also acts on $\mu_p$, which is given by a homomorphism (or character) $\omega : \Delta \to \mathbb{F}_p^\times$. Hence one has a natural action of $\Delta$ on $\text{Hom}(\text{Gal}(F(\sqrt{A})/F), \mu_p)$. One can then verify that the map $\kappa_A$ is $\Delta$-equivariant. In particular, suppose that $A/(F^\times)^p$ is cyclic. The action of $\Delta$ on that group is given by a character $\psi : \Delta \to \mathbb{F}_p^\times$. The action of $\Delta$ on $\text{Gal}(F(\sqrt{A})/F)$ must then be given by the character $\varphi = \omega \psi^{-1}$.

There is a theorem of Kummer concerning the class numbers of the CM-field $F = \mathbb{Q}(\mu_p)$ and its maximal real subfield $F_\mathbb{R}$. We will denote the class number of $F_\mathbb{R}$ by $h_\mathbb{R}$, often call the “second factor” in $h_F$. In fact, proposition
1.1.1 implies that $h_F^+ | h_F$. The quotient $h_F/h_F^+$ is called the “first factor” and is denoted by $h_F^-$. By using class number formulas, Kummer showed that if $p|h_F^+$, then $p|h_F^-$. As our first illustration of the reflection principle, we will prove the following more general statement. It concerns a CM-field $F$ and we will use the same notation $h_F^\pm$.

**Proposition 1.4.1.** Suppose that $F$ is a CM-field containing $\mu_p$ where $p$ is an odd prime. Let $k$ be the largest integer such that $\mu_{p^k} \subset F$. Assume that $F(\mu_{p^{k+1}})/F$ is ramified for at least one prime of $F$. If $p|h_F^+$, then $p|h_F^-$. Since $F/F_+$ is ramified at the infinite primes of $F$, we know that $h_F^+ | h_F$ and so $h_F^-$ is an integer. One can also state the conclusion this way: $p|h_F$ if and only if $p|h_F^-$. 

**Proof.** Let $\Delta = \text{Gal}(F/F_+)$ and let $\delta$ denote its nontrivial element. As in section 1.2, we let $\epsilon_0, \epsilon_1$ denote the two characters of $\Delta$. In the notation defined above, we have $\epsilon_1 = \omega$. Since $p$ is odd, we have a direct product decomposition

$$Cl_F[p^\infty] = Cl_F[p^\infty]^{(\epsilon_1)} \times Cl_F[p^\infty]^{(\epsilon_0)}$$

(13)

Remark 1.2.8 implies that $Cl_F[p^\infty]^{(\epsilon_0)} \cong Cl_{F_+}[p^\infty]$ which has order $h_F^{(p)}$, the power of $p$ dividing $h_F^+$. Hence the order of $Cl_F[p^\infty]^{(\epsilon_1)}$ is equal to the power of $p$ dividing $h_F^-$. Thus, we must show that $Cl_F[p^\infty]^{(\epsilon_0)} \neq 1 \implies Cl_F[p^\infty]^{(\epsilon_1)} \neq 1$.

Assume that $Cl_F[p^\infty]^{(\epsilon_0)} \neq 1$. Hence there exists an unramified, cyclic extension of $F_+$ of degree $p$. Let $K$ be the compositum of that field and $F$. Thus, $K/F$ is an unramified, cyclic extension of degree $p$, and $K/F_+$ is abelian (in fact, cyclic) of degree $2p$. We have $K = F(\sqrt[p]{\alpha})$ for some $\alpha \in F^\times$. As mentioned above, $\alpha$ determines an ideal $I$ satisfying $P = (\alpha)$ and the corresponding ideal class $c \in Cl_F[p]$.

Let $\Delta = \text{Gal}(F/F_+)$ and let $\delta$ denote its nontrivial element. As in section 1.2, we let $\epsilon_0, \epsilon_1$ denote the two characters of $\Delta$. In the notation defined above, we have $\epsilon_1 = \omega$. Taking $A$ to be the subgroup of $F^\times$ generated by $\alpha$ and $(F^\times)^p$, so that $K = F(\sqrt[p]{A})$, note that $\Delta$ acts on $\text{Gal}(K/F)$ by $\epsilon_0$. Therefore, by (12), it follows that $\Delta$ acts on the cyclic group $A/(F^\times)^p$ by $\epsilon_1$. This means that $\delta(\alpha) = \alpha^{-1}\beta^p$, where $\beta \in F^\times$. Therefore, $\delta(I) = I^{-1}(\beta)$ and hence $\delta(c) = c^{-1}$. That is, $c \in Cl_F[p]^{(\epsilon_1)}$ in the notation of section 2. We must prove that $c \neq 1$.

If $c = 1$, then we would have $I = (\gamma)$, where $\gamma \in F^\times$. Thus, $\alpha = \gamma^p \eta$, where $\eta \in \mathcal{O}_F^\times$. We then see that $\delta(\eta) = \eta^{-1}\nu^p$, where $\nu \in \mathcal{O}_F^\times$. Now we make
the following observation: For either character \( \epsilon \) of \( \Delta \), the obvious map

\[
(\mathcal{O}_F^\times)^{(\epsilon)} \longrightarrow (\mathcal{O}_F^\times/(\mathcal{O}_F^\times)^p)^{(\epsilon)}
\]

is surjective. This is easily verified using the facts that \( |\Delta| = 2 \) and that \( p \) is odd. As a consequence, we see that \( \eta = \zeta^p \), where \( \xi \in \mathcal{O}_F^\times \) and \( \delta(\zeta) = \zeta^{-1} \). This means that \( N_{F/F_p}(\zeta) = 1 \) and hence \( \zeta \) is a root of unity in \( F \). However,

\[
K = F(\sqrt[p]{\alpha}) = F(\sqrt[p]{\eta}) = F(\sqrt[p]{\zeta})
\]

and since this extension is nontrivial, it must be \( F(\mu_{p+1}) \), a contradiction to our assumption since \( K/F \) is unramified. Thus, \( c \neq 1 \) and so \( Cl_F[p]^{(\epsilon_1)} \) is indeed nontrivial. \( \blacksquare \)

The argument just given shows more. One can adapt it to obtain the following inequality

\[
\dim_{F_p}(Cl_F[p]^{(\epsilon_0)}) \leq \dim_{F_p}(Cl_F[p]^{(\epsilon_1)})
\]

under the assumptions of the proposition. Proposition 1.4.2 below will be a refinement of this inequality.

Consider the following situation. Suppose that \( F \) is any number field containing \( \mu_p \) and let \( \Delta \) be a group of automorphisms of \( F \) such that \( p \nmid |\Delta| \). Let \( \varphi \) be any irreducible character of \( \Delta \) over \( \mathbb{Q}_p \) by which we mean the character of an irreducible representation \( \rho : \Delta \to \text{Aut}_{\mathbb{Q}_p}(V_\varphi) \), where \( V_\varphi \) is a finite-dimensional vector space over \( \mathbb{Q}_p \). Let \( d_\varphi = \dim_{\mathbb{Q}_p}(V_\varphi) \), the degree of the character \( \varphi \).

One of the irreducible characters of \( \Delta \) is \( \omega \), giving the action of \( \Delta \) on \( \mu_p \). This description defines a homomorphism \( \Delta \to \mathbb{F}_p^\times \), but the reduction map \( \mathbb{Z}_p^\times \to \mathbb{F}_p^\times \) has a canonical splitting identifying \( \mathbb{F}_p^\times \) with the group of \( \mu_{p-1} \) of \( (p-1) \)-st roots of unity in \( \mathbb{Z}_p^\times \). Thus, we can identify \( \omega \) with a character of \( \Delta \) with values in \( \mathbb{Z}_p^\times \), the character of a 1-dimensional representation space \( V_\omega \). We can make such an identification whenever we have a homomorphism \( \Delta \to \mathbb{F}_p^\times \).

Let \( \psi \) be the character of \( \Delta \) corresponding to the representation space

\[
V_\psi = \text{Hom}(V_\varphi, V_\omega),
\]

which is easily seen to be irreducible over \( \mathbb{Q}_p \). Of course, we also have \( V_\varphi \cong \text{Hom}(V_\psi, V_\omega) \). We refer to \( \psi \) as the \( \omega \)-dual of \( \varphi \). Note that \( \varphi \) and \( \psi \)
have the same degree. If they are 1-dimensional, then we have the simple relationship \( \varphi \psi = \omega \).

We will let \( \text{Irr}_\Delta(\mathbb{Q}_p) \) denote the set of irreducible characters of \( \Delta \) over \( \mathbb{Q}_p \). If \( \varphi \in \text{Irr}_\Delta(\mathbb{Q}_p) \), the idempotent for \( \varphi \) in the group ring \( \mathbb{Q}_p[\Delta] \) is defined by

\[
e_\varphi = \frac{1}{|\Delta|} \sum_{\delta \in \Delta} \varphi(\delta)^{-1} \delta
\]  

(15)

Note that \( e_\varphi \in \mathbb{Z}_p[\Delta] \) since \( (p, |\Delta|) = 1 \). The group ring \( \mathbb{Z}_p[\Delta] \) is a direct product of the ideals generated by the \( e_\varphi \)'s for \( \varphi \in \text{Irr}_\Delta(\mathbb{Q}_p) \).

Suppose that \( U \) is any \( \mathbb{Z}_p[\Delta] \)-module. Then we have the following decomposition as a direct product of \( \mathbb{Z}_p[\Delta] \)-submodules:

\[
U = \prod_{\varphi \in \text{Irr}_\Delta(\mathbb{Q}_p)} U^{(\varphi)}
\]

(16)

where \( U^{(\varphi)} = e_\varphi U \). If \( \varphi \) is 1-dimensional, then one also has the following definition:

\[
U^{(\varphi)} = e_\varphi U = \{ a \in U \mid \delta(a) = \varphi(\delta)a \text{ for all } \delta \in \Delta \}
\]

(17)

We refer to (16) as the \( \Delta \)-decomposition of \( U \) and to the submodule \( U^{(\varphi)} \) as the \( \varphi \)-component of \( U \).

In particular, suppose that \( U \) is an elementary abelian \( p \)-group. We can regard \( U \) as a representation space for \( \Delta \) over \( \mathbb{F}_p \). Suppose that it is irreducible. Then \( U = U^{(\varphi)} \) for a unique \( \varphi \in \text{Irr}_\Delta(\mathbb{Q}_p) \). Conversely, if \( \varphi \in \text{Irr}_\Delta(\mathbb{Q}_p) \), one can find a \( \mathbb{Z}_p \)-lattice \( T_\varphi \subset V_\varphi \) which is \( \Delta \)-invariant. Then \( U = T_\varphi/pT_\varphi \) is irreducible and satisfies \( U = U^{(\varphi)} \). We denote this space by \( W_\varphi \). One has \( \dim_{\mathbb{F}_p}(W_\varphi) = d_\varphi \). It is not hard to see that this construction \( V_\varphi \sim W_\varphi \) defines a 1-1 correspondence between the sets of irreducible representations for \( \Delta \) over \( \mathbb{Q}_p \) and over \( \mathbb{F}_p \). Also, if \( V \) is any finite-dimensional representation space for \( \Delta \) and \( T \) is a \( \Delta \)-invariant \( \mathbb{Z}_p \)-lattice in \( V \), then \( T/pT \) is isomorphic to a direct sum of the \( W_\varphi \)'s, \( V \) is isomorphic to a direct sum of the \( V_\varphi \)'s, and the corresponding multiplicities are equal.

The following result is the main theorem of this section. It is an illustration of the reflection principle. The structure of \( \mathcal{O}_F^\times/(\mathcal{O}_F^\times)^p \) as a representation space for \( \Delta \) over \( \mathbb{F}_p \) plays a role, specifically the \( \mathbb{F}_p \)-dimension of the \( \varphi \)-component for an irreducible character \( \varphi \). As we will discuss later, the multiplicity of \( W_\varphi \) in \( \mathcal{O}_F^\times/(\mathcal{O}_F^\times)^p \) can be determined, in principle, and hence so can the dimension of \( (\mathcal{O}_F^\times/(\mathcal{O}_F^\times)^p)^{(\varphi)} \).

35
Proposition 1.4.2. Suppose that $\Delta$ is a group of automorphisms of a number field $F$ and that $p$ is a prime not dividing $|\Delta|$. Assume that $\mu_p \subset F$. Suppose that $\varphi$ is an irreducible character for $\Delta$ over $\mathbb{Q}_p$ and that $\psi$ is the $\omega$-dual of $\varphi$. Then

$$\dim_{\mathbb{F}_p}(\text{Cl}_F[p]^\varphi) \leq \dim_{\mathbb{F}_p}(\text{Cl}_F[p]^{(\varphi)}) + \dim_{\mathbb{F}_p}((\mathcal{O}_F^\times/(\mathcal{O}_F^\times)^p)^{(\varphi)})$$

Proof. Let $E = F^\Delta$. Then $\Delta = \text{Gal}(F/E)$. Consider the $\psi$-component $\text{Cl}_F[p^\infty]^{(\psi)}$ in the $\Delta$-decomposition of $\text{Cl}_F[p^\infty]$. The $\mathbb{F}_p$-dimensions of $\text{Cl}_F[p]^{(\psi)}$ and $\text{Cl}_F[p^\infty]^{(\psi)}/p\text{Cl}_F[p^\infty]^{(\psi)}$ are equal. Denote this dimension by $r_\psi$. The Artin map for $L/F$ then determines an extension $K_\psi/F$ such that $K_\psi \subseteq L$, $K_\psi/E$ is a Galois extension, and $\text{Gal}(K_\psi/E) \cong \text{Cl}_F[p]^{(\psi)}$ as $\mathbb{F}_p$-representation spaces for $\Delta$. Each is isomorphic to a direct sum of $r_\psi/d_\psi$ copies of $W_\psi$.

Now $K_\psi = F(\sqrt[d_\psi]{A_\varphi})$ for a certain subgroup $A_\varphi$ of $F^\times$ which contains $(F^\times)^p$ and is $\Delta$-invariant. The $\mathbb{F}_p$-representation space $A_\varphi/(F^\times)^p$ has dimension $r_\psi$ and is a direct sum of $r_\psi/d_\psi$ copies of $W_\varphi$. This follows from (12) and is the reason we use the subscript $\varphi$. The fact that $K_\psi/F$ is unramified implies that if $\alpha \in A_\varphi$, then $\alpha\mathcal{O}_F = I^p$ for some fractional ideal $I$ of $F$. Let $c$ denote the class of $I$. Of course, if $\alpha \in (F^\times)^p$, then $c = 1$. Thus, we can define in this way a homomorphism

$$A_\varphi/(F^\times)^p \longrightarrow \text{Cl}_F[p]$$

which is easily seen to be $\Delta$-equivariant. Thus the image of (18) is a subgroup of $\text{Cl}_F[p]^{(\varphi)}$ and hence its $\mathbb{F}_p$-dimension is bounded above by $\dim_{\mathbb{F}_p}(\text{Cl}_F[p]^{(\varphi)})$.

The kernel of (18) is of the form $B_\varphi/(F^\times)^p$, where $B_\varphi$ is some subgroup of $A_\varphi$. Suppose that $\alpha \in B_\varphi$. Then $c = 1$ and $I = (\gamma)$, where $\gamma \in F^\times$. Therefore, $\alpha = \gamma^p\eta$, where $\eta \in \mathcal{O}_F^\times$. This implies that $B_\varphi/(F^\times)^p$ is contained in the image of the map

$$(\mathcal{O}_F^\times/(\mathcal{O}_F^\times)^p)^{(\varphi)} \longrightarrow (F^\times/(F^\times)^p)^{(\varphi)}$$

and hence $\dim_{\mathbb{F}_p}(B_\varphi/(F^\times)^p) \leq \dim_{\mathbb{F}_p}((\mathcal{O}_F^\times/(\mathcal{O}_F^\times)^p)^{(\varphi)})$. The inequality in the proposition now follows. 

To deduce the inequality (14) from proposition 1.4.2, one needs just one additional observation. Just take $\psi = \epsilon_0$, $\varphi = \epsilon_1$. The group $(\mathcal{O}_F^\times/(\mathcal{O}_F^\times)^p)^{(\epsilon_1)}$ is cyclic and is generated by the coset of a primitive $p^k$-th root of unity $\zeta$. 

36
However, since $F(\sqrt[d]{\zeta})$ is assumed to be ramified, the image of the coset of $\zeta$ under the map (19) isn’t contained in $A_{e_1}$ and so we get the slightly better inequality (14).

Another consequence is a theorem proved in the early 1930s, due to Scholz, which is for the case $p = 3$.

**Proposition 1.4.3.** Let $d > 1$ be a squarefree integer. Then

$$\dim_{\mathbb{F}_3}(\text{Cl}_{\mathbb{Q}(\sqrt[3]{3})}[3]) \leq \dim_{\mathbb{F}_3}(\text{Cl}_{\mathbb{Q}(\sqrt[3]{-3d})}[3]) \leq \dim_{\mathbb{F}_3}(\text{Cl}_{\mathbb{Q}(\sqrt[3]{9})}[3]) + 1$$

**Proof.** In this case, we consider the biquadratic field $F = \mathbb{Q}(\sqrt{d}, \sqrt{-3d})$, a CM-field with maximal real subfield $F_+ = \mathbb{Q}(\sqrt{d})$. The first inequality follows from proposition 1.4.1. To prove the second inequality, we consider $\Delta = \text{Gal}(F/\mathbb{Q})$, a group with four characters. The nontrivial characters are $\psi$, $\varphi$, and $\omega$. They factor through the quotient groups of $\Delta$ corresponding to the three quadratic fields $E_\psi = \mathbb{Q}(\sqrt{-3d})$, $E_\varphi = F_+$, and $E_\omega = \mathbb{Q}(\mu_3)$, respectively. We denote the trivial character by $\epsilon_0$. Consider the $\Delta$-decomposition of $\text{Cl}_F[3^\infty]$:

$$\text{Cl}_F[3^\infty] = \text{Cl}_F[3^\infty]^{(\psi)} \times \text{Cl}_F[3^\infty]^{(\varphi)} \times \text{Cl}_F[3^\infty]^{(\omega)} \times \text{Cl}_F[3^\infty]^{(\epsilon_0)}$$

One can use remark 1.2.8 to identify each of these components. First of all, $\text{Cl}_F[3^\infty]^{(\epsilon_0)} \cong \text{Cl}_{\mathbb{Q}[3^\infty]}$, which is obviously trivial. Then, similarly, we have

$$\text{Cl}_F[3^\infty]^{(\psi)} \cong \text{Cl}_{F_\psi}[3^\infty], \quad \text{Cl}_F[3^\infty]^{(\varphi)} \cong \text{Cl}_{F_\varphi}[3^\infty], \quad \text{Cl}_F[3^\infty]^{(\omega)} \cong \text{Cl}_{F_\omega}[3^\infty].$$

The $\omega$-component is also trivial. Proposition 1.4.3 gives an inequality for the 3-ranks of the other two $\Delta$-components. The unit group $\mathcal{O}_F^\times$ has a very simple structure, namely $\mu_3$ and the fundamental unit of $E_\varphi$ generate a subgroup of index a power of 2. It follows that $\dim_{\mathbb{F}_3}(\mathcal{O}_F^\times/(\mathcal{O}_F^\times)^3(\varphi)) = 1$. One obtains

$$\dim_{\mathbb{F}_3}(\text{Cl}_F[3]^{(\psi)}) \leq \dim_{\mathbb{F}_3}(\text{Cl}_F[3]^{(\varphi)}) + 1$$

and the second inequality in the proposition then follows.

As we mentioned earlier, one can evaluate $\dim_{\mathbb{F}_p}(\mathcal{O}_F^\times/(\mathcal{O}_F^\times)^p(\varphi))$ in principle. That dimension is determined by the representation space $V_{\mathcal{O}_F^\times} = \mathcal{O}_F^\times \otimes_{\mathbb{Z}} \mathbb{Q}_p$ for $\Delta$ and the torsion subgroup $\mu_F$ of $\mathcal{O}_F^\times$. For the contribution from $\mu_F$, note that $\mu_F/\mu_F^p$ is an $\mathbb{F}_p$-vector space of dimension 1 and $\Delta$ acts
by $\omega$. Its contribution to the dimension is 1 if $\varphi = \omega$, and 0 otherwise. Now $T_{O_F^\varphi} = (O_F^\varphi/\mu_F) \otimes \mathbb{Z} \mathbb{Z}_p$ is a $\Delta$-invariant $\mathbb{Z}_p$-lattice in $V_{O_F^\varphi}$ and therefore the multiplicity of $W_\varphi$ in $T_{O_F^\varphi}/pT_{O_F^\varphi}$ is the same as the multiplicity of $V_\varphi$ in $V_{O_F^\varphi}$. Denote that multiplicity by $m_\varphi(V_{O_F^\varphi})$. Then the $\mathbb{F}_p$-dimension of 

\[(O_F^\varphi/(O_F^\varphi)^\varphi)(\varphi)\] 

is equal to $m_\varphi(V_{O_F^\varphi})$ if $\varphi \neq \omega$, and $m_\varphi(V_{O_F^\varphi}) + 1$ if $\varphi = \omega$.

In principle, the isomorphism class of $V_{O_F^\varphi}$, and hence the multiplicities of each of the $V_\varphi$'s in that representation space for $\Delta$, can always be determined. One could take a Galois extension $F'$ of $\mathbb{Q}$ containing $F$. Then $\Delta$ is a subquotient of $\Delta' = \text{Gal}(F'/\mathbb{Q})$ and $V_{O_F^\varphi} \cong V_{\text{Gal}(F'/F)}$ as representation spaces for $\Delta$. The action of $\Delta$ on that subspace can be studied in terms of the representation space $V_{O_F^\varphi}$, for $\text{Gal}(F'/\mathbb{Q})$. Therefore, it seems sufficient to consider a finite Galois extension of $\mathbb{Q}$ and so we will simply assume that $F/\mathbb{Q}$ is Galois. The following theorem is rather well-known. After recalling the proof, we will describe how to determined the multiplicity of $V_\varphi$ in $V_{O_F^\varphi}$.

**Proposition 1.4.4.** Suppose that $F$ is a finite Galois extension of $\mathbb{Q}$ and let $\Delta = \text{Gal}(F/\mathbb{Q})$. Let $v$ be an infinite prime of $F$ and let $\Delta_v$ denote the decomposition subgroup of $\Delta$ for $v$. Suppose that $\epsilon_0$ is the trivial character of $\Delta_v$ and $\varphi_0$ is the trivial character of $G$. Let $V_{O_F^\varphi} = O_F^\varphi \otimes \mathbb{Z} \mathbb{Q}_p$. Then

\[V_{O_F^\varphi} \oplus V_{\varphi_0} \cong \text{Ind}_{\Delta_v}^\Delta(\epsilon_0)\]

as representations spaces for $\Delta$.

**Proof.** The isomorphism will be proved by showing that the two representations of $\Delta$ have the same character. Both representations can be realized over $\mathbb{Q}$, but the character is determined by a realization over any field. The argument depends on the well-known proof of Dirichlet's unit theorem. The completions $F_v$ of $F$ at the infinite primes $v$ are either all isomorphic to $\mathbb{R}$ or to $\mathbb{C}$. In either case, one defines a log map from $F_v^\times$ onto $\mathbb{R}$. One then identifies $O_F^\varphi/\mu_F$ with a $\mathbb{Z}$-lattice in a certain subspace of $\prod_{v \mid \infty} \mathbb{R}$ of codimension 1. This map is $\Delta$-equivariant. The $\mathbb{R}$-vector space $\prod_{v \mid \infty} \mathbb{R}$ is just the permutation representation determined by the action of $\Delta$ on the set of infinite primes of $F$. This is isomorphic to $\text{Ind}_{\Delta_v}^\Delta(\epsilon_0)$, considered as an $\mathbb{R}$-representation space for $\Delta$. Thus, one has an injective map

\[O_F^\varphi \otimes \mathbb{Z} \mathbb{R} \rightarrow \text{Ind}_{\Delta_v}^\Delta(\epsilon_0)\]

and the cokernel is just the trivial representation of $\Delta$ over $\mathbb{R}$. The character
of the representation is thus determined. As we mentioned, this is sufficient to prove the stated isomorphism.

Obviously \( m_{\varphi_0}(V_{Q^\times}) = 0 \). If \( \varphi \neq \varphi_0 \), then \( m_{\varphi}(V_{Q^\times}) \) is just the multiplicity of \( \varphi \) in \( \text{Ind}^\Delta_{\Delta_0}(e_0) \). Now \( V_\varphi \otimes_{Q_p} \overline{Q_p} \) may be reducible, a direct sum of absolutely irreducible representations spaces, each occurring with a certain multiplicity. Suppose that \( \xi \) is the character of one of the direct summands, a representation space \( V_\xi \) for \( \Delta \) over \( \overline{Q_p} \), and let \( s_\xi \) denote the corresponding multiplicity. The quantity \( s_\xi \) is the Schur index for \( \xi \) over \( Q_p \), and actually depends only on \( \varphi \) and not on the choice of \( \xi \). All the characters \( \xi \) occurring in \( \varphi \) are conjugate over \( Q_p \). If \( m_\xi(\text{Ind}^\Delta_{\Delta_0}(e_0)) \) denotes the multiplicity of \( V_\xi \) in \( \text{Ind}^\Delta_{\Delta_0}(e_0) \), then \( m_\varphi(V_{Q^\times}) = m_\xi(\text{Ind}^\Delta_{\Delta_0}(e_0))/s_\xi \), assuming that \( \varphi \neq \varphi_0 \).

One can determine \( m_\xi(\text{Ind}^\Delta_{\Delta_0}(e_0)) \) by using the Frobenius reciprocity law. Let \( d_\xi = \dim_{\overline{Q_p}}(V_\xi) \). Note that \( \Delta_0 \) has order 1 or 2. Let \( d_\xi^+ \) and \( d_\xi^- \) denote the multiplicities of \( e_0 \) and \( e_1 \) (if \( \Delta_0 \) has order 2), respectively, when we regard \( V_\xi \) as a representation space for \( \Delta_0 \). Thus, \( d_\xi = d_\xi^+ + d_\xi^- \). According to the Frobenius reciprocity law, the multiplicity of \( \xi \) in \( \text{Ind}^\Delta_{\Delta_0}(e_0) \) coincides with the multiplicity of \( e_0 \) in \( \text{Ind}^\Delta_{\Delta_0}(e_0) \). That is, we have \( m_\xi(\text{Ind}^\Delta_{\Delta_0}(e_0)) = d_\xi \).

If \( F \) is totally real, then \( d_\xi = d_\xi^+ = d_\xi^- \). If \( F \) is a CM-field, then any irreducible character \( \xi \) is either totally even or totally odd, i.e., either \( d_\xi^+ = d_\xi \) or \( d_\xi^- = d_\xi \). In the important special case where \( \Delta \) is abelian, and \( \varphi \) is an irreducible character for \( \Delta \) over \( Q_p \), then each \( \xi \) occurring in \( \varphi \) is 1-dimensional and occurs with multiplicity 1. In that case, we have \( m(\varphi)(V_{Q^\times}) = 1 \) or 0, depending on whether \( \varphi \) is even or odd.

We now consider the field \( F = Q(\mu_p) \) and \( \Delta = \text{Gal}(F/Q) \). The irreducible characters of \( \Delta \) over \( F_p \) are the powers \( \omega^i \), \( 0 \leq i \leq p - 2 \).

**Proposition 1.4.5.** Suppose that \( p \) is an odd prime, that \( 2 \leq i, j \leq p - 2 \), that \( i \) is odd, and that \( i + j \equiv 1 \pmod{p - 1} \). Then

\[
\dim_{F_p}(Cl_F[p]^{(\omega^i)}) \leq \dim_{F_p}(Cl_F[p]^{(\omega^j)}) \leq \dim_{F_p}(Cl_F[p]^{(\omega^j)}) + 1.
\]

Also, the \( \omega^0 \) and \( \omega^1 \) components of \( Cl_F[p] \) are trivial.

**Proof.** First of all, note that \( i + j \equiv 1 \pmod{p - 1} \) implies that \( \omega^i \omega^j = \omega \). Suppose that \( i \) is odd, \( 1 \leq i \leq p - 2 \), and let \( \psi = \omega^j \), \( \varphi = \omega^i \). Then \( u_\varphi = 0 \) if \( i > 1 \), \( u_\varphi = 1 \) if \( i = 1 \). But when \( i = 1 \), one can observe that \( F(\mu_p^2)/F \) is a ramified extension. Thus, in all cases, we get the inequality \( \dim_{F_p}(Cl_F[p]^{(\omega^i)}) \leq \dim_{F_p}(Cl_F[p]^{(\omega^j)}) \).

39
To get the second inequality, take \( \psi = \omega^i, \varphi = \omega^j \). The structure of \( \mathcal{O}_F^\times \otimes \mathbb{Z} \mathbb{Q}_p \) is rather simple. Each nontrivial even character of \( \Delta \) occurs with multiplicity 1. That is, \( u_\varphi = 1 \) if \( j \neq 0 \), \( u_\varphi = 0 \) if \( j = 0 \). We get the second inequality as stated. If \( j = 0 \), note that \( \text{Cl}_F[p](\omega^0) = \text{Cl}_F[p]^2 \). Remark 1.2.8 identifies this group with \( \text{Cl}_\mathbb{Q}[p] \) which is trivial. Hence \( \text{Cl}_F[p](\omega^1) \) is trivial too.

We will return frequently to the field \( F = \mathbb{Q}(\mu_p) \) later in this book. It will be one of our most important examples. Proposition 1.4.5 already touches on one interesting question: what can one say about the dimensions of the various components in the \( \Delta \)-decomposition of \( \text{Cl}_F[p] \)? There is an important criterion for the nontriviality of the \( \omega^1 \)-component when \( i \) is odd, the Herbrand-Ribet theorem. It involves the Bernoulli numbers \( B_m \) which are defined by the following power series expansion

\[
\frac{t}{e^t - 1} = \sum_{m=0}^{\infty} B_m \frac{t^m}{m!}
\]

The Bernoulli numbers are nonzero rational numbers for even \( m > 0 \). It is known that \( B_m \) is \( p \)-integral if \( m \) is not divisible by \( p - 1 \). We will simply write \( p | B_m \) when \( p \) divides the numerator of \( B_m \).

**Herbrand-Ribet Theorem.** Suppose that \( p \) is an odd prime. Assume that \( i \) and \( j \) are integers in the range \( 2 \leq i, j \leq p - 2 \), that \( i \) is odd, and that \( i + j \equiv 1 \pmod{p-1} \). Let \( F = \mathbb{Q}(\mu_p) \). Then

\[
\text{Cl}_F[p](\omega^1) \neq 1 \iff p | B_j
\]

We will discuss the proof of this theorem later. It is a refinement of Kummer’s famous criterion for irregularity:

**Kummer’s Criterion.** The class number of \( F = \mathbb{Q}(\mu_p) \) is divisible by \( p \) if and only if \( p | B_j \) for at least one even \( j \) in the range \( 2 \leq j \leq p - 2 \).

To explain the connection with the Herbrand-Ribet theorem, suppose first that \( p | h_F \). Then \( \text{Cl}_F[p](\omega^1) \neq 1 \) for at least one \( i \) in the range \( 0 \leq i \leq p - 2 \). According to proposition 1.4.5, we know that \( i \neq 0 \) or 1 and that \( i \) can be taken to be odd. Herbrand proved that \( p | B_j \) where \( j = p - i \), an even integer
in the range $2 \leq j \leq p - 2$. Ribet proved that, conversely, if $p \mid B_j$ for an even $j$ in the stated range, then $Cl_F[p](\omega^j) \neq 1$ for $i = p - j$.

As an example, let $p = 37$, the first irregular prime. Then $37 \mid B_{32}$, but $37 \nmid B_j$ for the other even values of $j$, $2 \leq j \leq 34$. The Herbrand-Ribet theorem then asserts that $Cl_F[37](\omega^{32}) \neq 1$ and that the $\omega^j$-component is trivial for the other odd values of $i$. For an even character $\omega^j$, proposition 1.4.5 implies that $Cl_F[37](\omega^j) = 0$ except possibly when $j = 32$. It turns out that $Cl_F[37](\omega^{32}) = 0$ too. This is so because $p \nmid h_{F,\omega}$.

In general, it seems reasonable to conjecture that $Cl_F[p\infty](\omega^j)$ is a cyclic group, or equivalently, that $\dim_{F_p}(Cl_F[p](\omega^j)) = 1$, for all odd $i$’s. A sufficient condition for this to be so is that $Cl_F[p](\omega^j) = 0$ for all even $j$’s, as proposition 1.4.5 implies. There is no known example where an even component in $Cl_F[p]$ is nontrivial. It may never happen, an assertion often referred to as Vandiver’s conjecture. We can state it in an equivalent form as follows:

**Vandiver’s Conjecture.** Let $F = \mathbb{Q}(\mu_p)$. Then $p \nmid h_{F,\omega}$.

This conjecture has been verified for all $p < 16,000,000$. For all of these primes, it turns out that the nontrivial components $Cl_F[p\infty](\omega^j)$ are all cyclic of order $p$.

A useful consequence of Vandiver’s conjecture concerns the structure of $A_F = Cl_F[p\infty]$ as a $\mathbb{Z}_p[\Delta]$-module. It follows immediately from the above remarks.

**Proposition 1.4.6.** Suppose that $F = \mathbb{Q}(\mu_p)$. Let $\Delta = \text{Gal}(F/\mathbb{Q})$. Assume that $h_F^+$ is not divisible by $p$. Then $A_F$ is cyclic when considered as a $\mathbb{Z}_p[\Delta]$-module. That is, $A_F \cong \mathbb{Z}_p[\Delta]/I$, where $I$ is a certain ideal in $\mathbb{Z}_p[\Delta]$.

We will have a lot to say about this ideal $I$ in later chapters.

We now consider an important variation on proposition 1.4.2, a more precise illustration of the reflection principle. Suppose that $F$ is a number field, $p$ is a prime, and the hypotheses in proposition 1.4.2 are satisfied. Let $M$ denote the compositum of all abelian, $p$-extensions of $F$ which are ramified only at primes if $F$ above $p$. Let $X = \text{Gal}(M/F)$. Note that the $p$-Hilbert class field $L$ of $F$ is contained in $M$. Also, $M$ is obviously a Galois extension of $F^\Delta$ and so $\Delta$ acts on $X$. The next result concerns the $\Delta$-decomposition of $X/X^p$. Let $S_p$ denotes the set of primes of $F$ lying above $p$ and let $\mathcal{O}_{F,S_p}$ denote the ring $\mathcal{O}_{F,F^p}$. The group of $S_p$-units of $F$, which is defined to be
\( \mathcal{O}_{F,S_p}^\times \) will play a role. Also, we let \( A'_F \) denote the \( p \)-ideal class group of that ring. This is isomorphic to \( A_F/B_F \), where \( B_F \) is the subgroup of ideal classes in \( A_F \) which contain a product of primes in \( S_p \). Note that \( \Delta \) acts on both \( \mathcal{O}_{F,S_p}^\times \) and \( A'_F \).

**Proposition 1.4.7.** Suppose that the assumptions in proposition 1.4.2 are satisfied. Then

\[
\dim_{\mathbb{F}_p}((X/X^p)^{(v)}) = \dim_{\mathbb{F}_p}(A'_F[p]^{(v)}) + \dim_{\mathbb{F}_p}((\mathcal{O}_{F,S_p}^\times / (\mathcal{O}_{F,S_p}^\times )^{(p)})^{(v)})
\]

**Proof.** We first make the following observation. Suppose \( \alpha \in \mathbb{F}^\times \). Then \( F(\sqrt[p]{\alpha}) \subset M \) if and only if \( p | \text{ord}_v(\alpha) \) for all finite primes \( v \) of \( F \) such that \( v \notin S_p \). This last condition means that \( \alpha \mathcal{O}_{F,S_p} = I^p \), where \( I \) is a fractional ideal for \( \mathcal{O}_{F,S_p} \). Let \( A \subset F^\times \) denote the set of such \( \alpha \)'s. Thus the compositum of all cyclic extensions of \( F \) of degree \( p \) and unramified outside \( S_p \) is \( F(\sqrt[p]{A}) \).

We have

\[
X/X^p \cong \text{Gal}(F(\sqrt[p]{A})/F) \cong \text{Hom}(A/(F^\times)^p, \mu_p)
\]

These isomorphisms are \( \Delta \)-equivariant.

Now we also have the following exact sequence

\[
1 \longrightarrow \mathcal{O}_{F,S_p}^\times / (\mathcal{O}_{F,S_p}^\times )^{(p)} \xrightarrow{f} A/(F^\times)^p \xrightarrow{g} A'_F[p] \longrightarrow 1
\]

where the map \( f \) is induced by the inclusion \( \mathcal{O}_{F,S_p}^\times \rightarrow \mathbb{F}^\times \) and the map \( g \) is defined as follows. If \( \alpha \in A \), then write \( \alpha \mathcal{O}_{F,S_p} = I^p \) as above. Let \( c \) be the class of \( I \) in the class group for \( \mathcal{O}_{F,S_p} \). Clearly, \( c \in A'_F[p] \). We define \( g(a(F^\times)^p) = c \). The fact that \( g \) is a well-defined, surjective homomorphism is easily verified. Also, \( \alpha \) represents a coset in the kernel of \( g \) if and only if \( \alpha = \beta^p \eta \), where \( \eta \in \mathcal{O}_{F,S_p}^\times \), which proves the exactness.

The maps \( f \) and \( g \) are obviously \( \Delta \)-equivariant and the exact sequence splits because \( p \nmid |\Delta| \). We have isomorphisms

\[
(X/X^p)^{(v)} \cong \text{Hom}(A/(F^\times)^p, \mu_p)^{(v)} \cong \text{Hom}(A/(F^\times)^p)^{(v)}, \mu_p)
\]

Now \( A/(F^\times)^p)^{(v)} \cong (\mathcal{O}_{F,S_p}^\times / (\mathcal{O}_{F,S_p}^\times )^{(p)})^{(v)} \times A'_F[p]^{(v)} \). Proposition 1.4.6 then follows.

Returning to the case where \( F = \mathbb{Q}(\mu_p) \) and \( \Delta = \text{Gal}(F/\mathbb{Q}) \), we have the following result. The field \( M \) and the Galois group \( X \) are as defined above.
Corollary 1.4.8. Under the assumptions of proposition 1.4.5, we have
\[
\dim_{\mathbb{F}_p}( (X/X^p)^{(\omega^i)} ) = \dim_{\mathbb{F}_p}( Cl_F[p]^{(\omega^i)} ),
\]
\[
\dim_{\mathbb{F}_p}( (X/X^p)^{(\omega^i)} ) = \dim_{\mathbb{F}_p}( Cl_F[p]^{(\omega^j)} ) + 1.
\]
Also, \( \dim_{\mathbb{F}_p}( (X/X^p)^{(\omega^1)} ) = \dim_{\mathbb{F}_p}( (X/X^p)^{(\omega^0)} ) = 1 \).

Proof. This follows easily from proposition 1.4.7. One just notes that since the prime of \( F \) lying above \( p \) is principal, we have \( A_F \cong A_F' \). Also, \( \dim_{\mathbb{F}_p}( (\mathcal{O}^\times_{F,S_p}/(\mathcal{O}^\times_{F,S_p})^p)^{(\varphi)} ) = 1 \) if \( \varphi = \omega^j \) where \( j \) is even or if \( j = 1 \). This dimension is 0 otherwise. 

As an illustration, assume that \( h_F^{(p)} = p \) in corollary 1.4.8. Thus, \( Cl_F[p]^{(\omega^i)} \) is nontrivial for exactly one \( i \). That value of \( i \) must be odd. If \( L \) denotes the \( p \)-Hilbert class field of \( F \), then \( L/\mathbb{Q} \) is Galois, \( \text{Gal}(L/F) \) is cyclic or order \( p \), and \( \Delta = \text{Gal}(F/\mathbb{Q}) \) acts on \( \text{Gal}(L/F) \) by the character \( \omega^i \). Now the corresponding \( j \) is even and \( \omega^j \omega^i = \omega \). The character \( \omega^j \) is the only non-trivial, even character of \( \Delta \) for which \( (X/pX)^{(\omega^i)} \) is nontrivial. Furthermore, \( (X/pX)^{(\omega^i)} \) is cyclic of order \( p \). Thus, there is a unique subfield \( N \) of \( M \) such that \( N/\mathbb{Q} \) is Galois, \( \text{Gal}(N/F) \) is cyclic or order \( p \), and \( \Delta = \text{Gal}(F/\mathbb{Q}) \) acts on \( \text{Gal}(N/F) \) by the character \( \omega^j \). Also, \( N = F(\sqrt[p]{\alpha}) \), where \( \alpha \) is in the group \( A \) defined in the proof of proposition 1.4.7. The coset of \( \alpha \) in \( A/(F^x)^p \) is contained in \( (A/(F^x)^p)^{(\omega^i)} \). It follows that the fractional ideal \( (\alpha) \) for \( \mathcal{O}_F \) is of the form \( I^p \) where \( I \) is a non-principal ideal of \( \mathcal{F}_F \). This explains a remark that we made before concerning example 2 in Remark 1.2.11.

If we apply a version of Nakayama’s lemma (lemma 1.5.3 to be proved later), we can say that \( \omega^j \) is the only nontrivial, even character for which \( X^{(\omega^j)} \) is nontrivial. Furthermore, since \( (X/pX)^{(\omega^j)} \) is cyclic of order \( p \), lemma 1.5.3 implies that \( X^{(\omega^j)} \) is either a finite cyclic \( p \)-group or isomorphic to \( \mathbb{Z}_p \). Although it is quite nontrivial to prove, it turns out that \( X^{(\omega^j)} \) is finite, a consequence of a proposition to be proved in chapter 3.

1.5 Unramified Galois Cohomology

Let \( F \) be a number field and let \( p \) be a prime. We will introduce an object in this section which can be regarded as a generalization of \( Cl_F[p^\infty] \) (or, to be more precise, the Pontryagin dual of that group). Let \( H \) be the Hilbert class
field of $F$. The Pontryagin dual of $\text{Gal}(H/F)$ is $\text{Hom}(\text{Gal}(H/F), \mathbb{Q}/\mathbb{Z})$. This can be viewed as a subgroup of the Galois cohomology group $H^1(G_F, \mathbb{Q}/\mathbb{Z})$, where we are letting $G_F$ act trivially on $\mathbb{Q}/\mathbb{Z}$. To be precise,

$$H^1(G_F, \mathbb{Q}/\mathbb{Z}) = \text{Hom}(G_F, \mathbb{Q}/\mathbb{Z}) = \text{Hom}(\text{Gal}(F^{ab}/F), \mathbb{Q}/\mathbb{Z})$$

A homomorphism $\phi : \text{Gal}(F^{ab}/F) \to \mathbb{Q}/\mathbb{Z}$ factors through $\text{Gal}(H/F)$ if and only if the restrictions of $\phi$ to the inertia subgroups of $\text{Gal}(F^{ab}/F)$ corresponding to all the primes of $F$ are trivial. We denote this subgroup by $H^1_{\text{unr}}(G_F, \mathbb{Q}/\mathbb{Z})$. It can be identified with the Pontryagin dual of $C_F^I$ by using the Artin isomorphism $\text{Art}_{H/F}$.

We always assume that cocycles or homomorphisms are continuous. The topology on $\mathbb{Q}/\mathbb{Z}$ is discrete and so “continuous” means “locally constant.” Since the topology on any Galois group $G$ is compact, cocycles or homomorphisms from $G$ to a discrete group such as $\mathbb{Q}/\mathbb{Z}$ will have only finitely many values and will factor through a quotient group $G/N$ where $N$ is an open, normal subgroup of $G$.

The $p$-primary subgroup of $\mathbb{Q}/\mathbb{Z}$ is isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$, where $\mathbb{Z}_p$ denotes the $p$-adic integers and $\mathbb{Q}_p$ denotes the fraction field of $\mathbb{Z}_p$. Assume that the action of $G_F$ on $\mathbb{Q}_p/\mathbb{Z}_p$ is trivial. The $p$-primary subgroup of $H^1_{\text{unr}}(G_F, \mathbb{Q}/\mathbb{Z})$ can then be identified with $H^1_{\text{unr}}(G_F, \mathbb{Q}_p/\mathbb{Z}_p)$. This is isomorphic to $\text{Hom}(\text{Gal}(L/F), \mathbb{Q}_p/\mathbb{Z}_p)$, where $L$ denotes the $p$-Hilbert class field of $F$. We will study a natural generalization, where we replace the trivial Galois module $\mathbb{Q}_p/\mathbb{Z}_p$ by any group $D \cong (\mathbb{Q}_p/\mathbb{Z}_p)^d$ which has a continuous action of $G_F$. We consider $D$ as having the discrete topology. Note that the Pontryagin dual $\text{Hom}(D, \mathbb{Q}_p/\mathbb{Z}_p)$ of $D$ is isomorphic to $\mathbb{Z}_p^d$, a free $\mathbb{Z}_p$-module of rank $d$. We express this fact by saying that $D$ is a cofree $\mathbb{Z}_p$-module and that its $\mathbb{Z}_p$-corank is $d$.

Given such a $D$, the subgroup $D[p^n]$ (for any $n \geq 0$) is isomorphic to $(\mathbb{Z}/p^n\mathbb{Z})^d$ as a group and has a certain action of $G_F$. That action corresponds to a homomorphism $G_F \longrightarrow GL_d(\mathbb{Z}/p^n\mathbb{Z})$. We can regard $D$ as the direct limit of these finite Galois modules. We define the “Tate-module” $T$ for $D$ to be the inverse limit:

$$T = \lim_{\leftarrow} D[p^n]$$

where the map $D[p^n] \to D[p^m]$ for $m \geq n \geq 0$ is multiplication by $p^{m-n}$. Then $T$ is a free $\mathbb{Z}_p$-module of rank $d$ which has a continuous $\mathbb{Z}_p$-linear action of $G_F$. That action is given by a homomorphism $\rho_D : G_F \longrightarrow GL_d(\mathbb{Z}_p)$. We
can also define a vector space $V = T \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. This is a topological vector space over $\mathbb{Q}_p$ of dimension $d$, and so has the topology of $\mathbb{Q}_p^d$. One then has a continuous, $\mathbb{Q}_p$-linear action of $G_F$ on $V$.

If we start instead with such a finite-dimensional $\mathbb{Q}_p$-representation space $V$ for $G_F$, it is not hard to prove (using continuity and the compactness of $G_F$) that $V$ contains a free $\mathbb{Z}_p$-module $T$ of rank $d = \dim_{\mathbb{Q}_p}(V)$ which is $G_F$-invariant. One could then take $D = V/T$ as the corresponding discrete $G_F$-module.

In general, suppose that $R$ is a commutative ring and that we have a homomorphism $\rho : G_F \to GL_d(R)$. The kernel will a normal subgroup $N$ of $G_F$ and the fixed field $\overline{F}^N$ will be a certain Galois extension of $F$ which we refer to as the “the extension cut out by $\rho$”. For example, if $\rho_D$ is as described above, then we can take $R = \mathbb{Z}_p$. We denote the extension cut out by $\rho_D$ by $F(D)$. Thus, $\text{Gal}(F(D)/F)$ is isomorphic to a subgroup of $GL_d(\mathbb{Z}_p)$, namely $\text{im}(\rho_D)$. Now $\rho_D$ is a continuous map, $\text{Gal}(F(D)/F)$ is compact, and hence $\text{im}(\rho_D)$ is a closed subgroup of $GL_d(\mathbb{Z}_p)$. Such a subgroup is known to be a $p$-adic Lie group and so one could say that $F(D)/F$ is a “$p$-adic Lie extension”.

Of course, it can be an infinite extension. For any $n \geq 0$, we can consider the representation of $G_F$ on $D[p^n]$, where we take $R = \overline{\mathbb{Z}}/p^n\mathbb{Z}$. This is the reduction modulo $p^n$ of $\rho_D$. The field cut out by this representation is a finite extension of $F$, denoted by $F(D[p^n])$. Note that $F(D) = \bigcup_{n \geq 0} F(D[p^n])$. We will use the notation $\text{Ram}(D)$ for the set of primes of $F$ which are ramified in the extension $F(D)/F$. Thus, if $v$ is a prime of $F$, then $v \in \text{Ram}(D)$ if and only if the image of the inertia subgroup of $G_F$ for a prime of $\overline{F}$ lying above $v$ is nontrivial. We will say that $D$ is finitely ramified if $\text{Ram}(D)$ is a finite set.

Consider the Galois cohomology group $H^1(G_F, D)$. The subgroup of $H^1(G_F, D)$ that is referred to in the title of this section can be defined roughly as the group of “everywhere unramified cocycle classes” and will be denoted by $H^1_{\text{unn}}(F, D)$. We will make this definition more precise.

For every prime $v$ of $F$, finite or infinite, we have the natural embedding $F \hookrightarrow F_v$, where $F_v$ denotes the $v$-adic completion of $F$. This can be extended to an embedding of $\overline{F} \hookrightarrow \overline{F}_v$. The choice of this embedding will not be important. We then have the natural restriction maps $G_{F_v} \to G_F$ arising from the above embeddings. Let $I_{F_v}$ denote the inertia subgroup of $G_{F_v}$. Thus $I_{F_v} = \text{Gal}(\overline{F}_v/F_v^{\text{unr}})$, where $F_v^{\text{unr}}$ denotes the maximal unramified extension of $F_v$. We get homomorphisms

$$H^1(G_F, D) \longrightarrow H^1(G_{F_v}, D) \longrightarrow H^1(I_{F_v}, D)$$
for every \( v \). From here on, we will use the customary notation

\[
H^1(F,*) ,\ H^1(F_v,*) \text{, and } H^1(F_{\text{unr}},*)
\]

instead of  \( H^1(G_F,*) ,\ H^1(G_{F_v},*) \)  and  \( H^1(I_{F_v},D) \), where  \( * \) is any Galois module.

The “unramified Galois cohomology group” for  \( D \) over  \( F \) is defined by

\[
H^1_{\text{unr}}(F,D) = \ker(H^1(F,D) \to \prod_v H^1(F_{\text{unr}},D)).
\]

where  \( v \) runs over all the primes of  \( F \) in the product. That is, if  \( \phi : G_F \to D \) is a 1-cocycle, then its class  \( [\phi] \) is in  \( H^1_{\text{unr}}(F,D) \) if and only if  \( [\phi|_{I_{F_v}}] \) is trivial in  \( H^1(I_{F_v},D) \) for all  \( v \in U \). In particular, if  \( S \) is empty, then  \( U \) consists of all primes of  \( F \) and we denote that group simply by  \( H^1_{\text{unr}}(F,D) \).

It is not true in general that  \( H^1_{\text{unr}}(F,D) \) is finite. We will discuss several examples later to illustrate this. However, we have the following finiteness result.

**Proposition 1.5.1.** Assume that  \( D \) is finitely ramified. Then  \( H^1_{\text{unr}}(F,D)[p] \) is finite.

**Proof.** The argument involves various simple applications of fundamental theorems of group cohomology. This proof will be an opportunity to introduce such applications carefully. Later arguments of this kind will be less detailed. The proof will be given in three parts.

The map  \( H^1(F,D[p^n]) \to H^1(F,D[p^n]) \). First of all, we have an exact sequence  \( 0 \to D[p^n] \to D \to D \to 0 \) for any  \( n \geq 0 \). The map  \( D \to D \) is given by  \( x \to p^n x \) for  \( x \in D \). The kernel of this map is  \( D[p^n] \) and map is surjective because  \( D \) is a divisible group. For any  \( i \geq 1 \), we then have the following part of the corresponding cohomology exact sequence

\[
H^{i-1}(F,D) \overset{p^n}{\longrightarrow} H^{i-1}(F,D) \longrightarrow H^i(F,D[p^n]) \longrightarrow H^i(F,D) \overset{p^n}{\longrightarrow} H^i(F,D)
\]

Consequently, the map  \( H^i(F,D[p^n]) \to H^i(F,D[p^n]) \) must be surjective. Furthermore, we have

\[
\ker(H^i(F,D[p^n]) \to H^i(F,D)) \cong H^{i-1}(F,D)/p^n H^{i-1}(F,D)
\]

If we take  \( i = 1 \), then  \( H^0(F,D) = D^{GF} \) is a  \( \mathbb{Z}_p \)-submodule of  \( D \). The Pontryagin dual  \( \hat{D} \) of  \( D \) is isomorphic to  \( \mathbb{Z}_p^d \); the Pontryagin dual of  \( D^{GF} \) is
a quotient of \( \hat{D} \). Hence it follows that \( H^0(F, D) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^e \times C \), where \( C \) is finite and \( 0 \leq e \leq d \). The subgroup \((\mathbb{Q}_p/\mathbb{Z}_p)^e\) is the maximal divisible subgroup \( H^0(F, D)_{div} \) of \( H^0(F, D) \) and the corresponding quotient group \( H^0(F, D)/H^0(F, D)_{div} \) is isomorphic to \( C \). It follows that
\[
H^0(F, D)_{div} \subseteq p^n H^0(F, D) \subseteq H^0(F, D)
\]
for all \( n \) and that \( p^n H^0(F, D) = H^0(F, D)_{div} \) if \( n \) is sufficiently large. To summarize, if \( n \geq 0 \), then the map
\[
H^1(F, D[p^n]) \longrightarrow H^1(F, D)[p^n]
\]
is surjective, has finite kernel, and the order of the kernel is bounded independently of \( n \).

The map \( H^1_{unr}(F, D[p^n]) \longrightarrow H^1_{unr}(F, D)[p^n] \). We can use the subscript \( unr \) even for finite Galois modules. Consider the map
\[
H^1_{unr}(F, D[p^n]) \longrightarrow H^1_{unr}(F, D)[p^n]
\]
We already know that the kernel is finite and of bounded order since that is true for the kernel of (21). Now we consider the cokernel. We will denote the images of the following “global-to-local” maps
\[
H^1(F, D[p^n]) \longrightarrow \prod_v H^1(F_{v^{unr}}, D[p^n]), \quad H^1(F, D) \longrightarrow \prod_v H^1(F_{v^{unr}}, D)
\]
by \( G^1(F, D[p^n]) \) and \( G^1(F, D) \), respectively. By definition, \( H^1_{unr}(F, D[p^n]) \) and \( H^1_{unr}(F, D) \) are the kernels of those maps. We then have the following commutative diagram with exact rows. The vertical maps are induced by the inclusion \( D[p^n] \subset D \).
\[
0 \longrightarrow H^1_{unr}(F, D[p^n]) \longrightarrow H^1(F, D[p^n]) \longrightarrow G^1(F, D[p^n]) \longrightarrow 0
\]
Note that we can’t say that the last map in the second row is surjective.

Now the order of \( \ker(\alpha_n) \) is bounded by the order of \( \ker(\beta_n) \). For studying coker(\( \alpha_n \)), we apply the snake lemma, obtaining the following useful exact sequence.
\[
\ker(\gamma_n) \longrightarrow \text{coker}(\alpha_n) \longrightarrow \text{coker}(\beta_n)
\]
But \( \ker(\beta_n) = 0 \), as pointed out in part 1. We can study \( \ker(\gamma_n) \) factor-by-factor on the entire direct products (over \( v \)) which contain \( G^1(F, D[p]) \) and \( G^1(F, D) \).

Suppose that \( v \) is any prime of \( F \). Consider the map
\[
\gamma_{n,v} : H^1(F^\text{unr}, D[p^n]) \longrightarrow H^1(F^\text{unr}, D)
\]
An identical argument to the one for (21), applied to \( F^\text{unr} \) instead of \( F \), shows that
\[
|\ker(\gamma_{n,v})| \leq [H^0(F^\text{unr}, D) : H^0(F^\text{unr}, D)_{\text{div}}]
\]
and hence is finite and bounded. Also, if \( v \not\in \text{Ram}(D) \), then \( I_F \) acts trivially on \( D \), \( H^0(F^\text{unr}, D) = D \), a divisible group, and hence the index is then 1. That is, \( |\ker(\gamma_{n,v})| = 1 \) if \( v \not\in \text{Ram}(D) \). Since \( D \) is assumed to be finitely ramified, we can conclude that \( \ker(\gamma_n) \) is finite and of bounded order. Therefore, (24) implies that \( \ker(\alpha_n) \) is finite and has bounded order.

**Finiteness of \( H^1_{\text{unr}}(F, D[p]) \).** To finish the proof, we will take \( n = 1 \). It obviously now suffices to prove that \( H^1_{\text{unr}}(F, D[p]) \) is finite. Let \( F' = F(D[p]) \), a finite Galois extension of \( F \). Let \( G = \text{Gal}(F'/F) \). Then we have the following exact sequence, the first few terms of the inflation-restriction sequence.
\[
0 \longrightarrow H^1(F'/F, D[p]) \longrightarrow H^1(F, D[p]) \longrightarrow H^1(F', D[p])^G
\]
Since both \( G \) and \( D[p] \) are finite, obviously so is \( H^1(F'/F, D[p]) \). The image of \( H^1_{\text{unr}}(F, D[p]) \) under the restriction map is clearly contained in \( H^1_{\text{unr}}(F', D[p]) \). The kernel is finite and therefore it is enough to prove the finiteness of \( H^1_{\text{unr}}(F', D[p]) \). Now \( G_{F'} \) acts trivially on \( D[p] \). Hence \( H^1(F', D[p]) = \text{Hom}(G_{F'}, D[p]) \) and
\[
H^1_{\text{unr}}(F', D[p]) = \text{Hom}(\text{Gal}(L'/F'), D[p]),
\]
where \( L' \) is the \( p \)-Hilbert class field of \( F' \). The finiteness of \( H^1_{\text{unr}}(F, D[p]) \) follows from the fact that \( \text{Gal}(L'/F') \cong Cl_{F'}[p^{\infty}] \), which is finite.

We will refer back to various steps in this proof from time to time. Here is an important corollary.

**Corollary 1.5.2.** Assume that \( D \) is finitely ramified. Then \( H^1_{\text{unr}}(F, D) \) is a cofinitely generated \( \mathbb{Z}_p \)-module. Consequently, \( H^1_{\text{unr}}(F, D)_{\text{div}} \cong (\mathbb{Q}_p/\mathbb{Z}_p)^r \) for some \( r \geq 0 \) and \( H^1_{\text{unr}}(F, D)/H^1_{\text{unr}}(F, D)_{\text{div}} \) is finite.
Note that $H^1_{unr}(F, D)$ will be isomorphic to the direct sum of its maximal divisible subgroup and the corresponding finite quotient group.

**Proof.** Since $H^1_{unr}(F, D)$ is a $p$-primary abelian group, it is a $\mathbb{Z}_p$-module. Consider its Pontryagin dual $X = \text{Hom}(H^1_{unr}(F, D), \mathbb{Q}_p/\mathbb{Z}_p)$. We must show that $X$ is a finitely generated $\mathbb{Z}_p$-module. This implies that $X \cong \mathbb{Z}_p \oplus X_{tor}$ and that $X_{tor}$ is finite. The final part of the corollary will then follow. The Pontryagin dual of $H^1_{unr}(F, D)[p]$ is $X/pX$ and so proposition 1.5.1 implies the finiteness of that group. Furthermore, $X$ is the Pontryagin dual of a discrete $\mathbb{Z}_p$-module and hence will be a compact $\mathbb{Z}_p$-module. The following lemma then completes the proof.

**Lemma 1.5.3. (Nakayama’s lemma for compact $\mathbb{Z}_p$-modules.)** Suppose that $X$ is a compact $\mathbb{Z}_p$-module. Let $x_1, \ldots, x_d$ be in $X$. Let $\tilde{x}_1, \ldots, \tilde{x}_d$ denote their images in $X/pX$. Then $x_1, \ldots, x_d$ is a generating set for $X$ as a $\mathbb{Z}_p$-module if and only if $\tilde{x}_1, \ldots, \tilde{x}_d$ is a generating set for $X/pX$ as a vector space over $F_p = \mathbb{Z}_p/p\mathbb{Z}_p$.

**Proof.** One direction is obvious. For the other direction, where we assume that $\tilde{x}_1, \ldots, \tilde{x}_d$ generate $X/pX$, one can give a quick proof that $x_1, \ldots, x_d$ generate $X$ by using the compactness of $\mathbb{Z}_p$. It is easy to verify this if $X$ is finite, which we leave to the reader. In general, we have $X = \varprojlim X_n$, where $X_n = X/p^nX$. One uses the compactness of $X$ to verify that. Note that our assumption implies that $X/pX$ is finite. It follows easily that that $X_n$ is finite for all $n$. The maps $\pi_n : X \to X_n$ are surjective. Hence the induced maps $X/pX \to X_n/p^nX$ are also surjective. It follows from the finite case that the images of $x_1, \ldots, x_d$ under the map $\pi_n$ must generate $X_n$. Let $Y$ be the $\mathbb{Z}_p$-submodule submodule of $X$ generated by $x_1, \ldots, x_d$. Since $Y$ is the image of $\mathbb{Z}_p^d$ under a continuous map, it is compact and therefore closed. But $\pi_n(Y) = X_n$. This is true for all $n$ and so it follows that $Y$ is also dense in $X$. Hence $Y = X$, as claimed. ■

**Remark 1.5.4.** One can examine the first two parts of the proof of proposition 1.5.1 to determine when the map $H^1_{unr}(F, D[p^n]) \to H^1_{unr}(F, D)[p^n]$ is injective and/or surjective. For injectivity, it would suffice that $D^{G_F}$ be divisible. Of course, this could be true simply because $D^{G_F} = 0$. For surjectivity, it would suffice that $D^{G_v}$ be divisible for all primes $v$. For then, $\ker(\gamma_n) = 0$ for all such $v$ and therefore $\ker(\gamma_n) = 0$. Now if $v \not\in \text{Ram}(D)$, then $D^{G_v} = D$ which is a divisible group. However, it could easily happen that $D^{G_v}$ fails to be divisible for some $v \in \text{Ram}(D)$. Even if that happens,
it is still possible that $\ker(\gamma_n) = 0$.

**Remark 1.5.5.** We will also consider the following object. Suppose that $S$ is a finite set of primes of $F$. Let $U$ denote the complement of $S$. Then define

$$H^1_{U - \text{unr}}(F, D) = \ker\left(H^1(F, D) \rightarrow \prod_{v \in U} H^1(F_v^{\text{unr}}, D)\right).$$

If $S$ is empty, then this group is $H^1_{\text{unr}}(F, D)$. The proof of proposition 1.5.1 and its corollary can be applied to this group. One finds that the map

$$H^1_{U - \text{unr}}(F, D[p]) \rightarrow H^1_{U - \text{unr}}(F, D)[p]$$

has finite kernel and cokernel. In fact, if one choose $S$ so that $\text{Ram}(D) \subseteq S$, then the cokernel is trivial. Now one can still prove that $H^1_{U - \text{unr}}(F, D[p])$ is finite. As in the above proof, one can let $F' = F(D[p])$. Let $S'$ be the set of primes of $F'$ lying above the primes in $S$. Let $U'$ denote its complement. Then the image of $H^1_{U - \text{unr}}(F, D[p])$ under the restriction map is contained in $H^1_{U' - \text{unr}}(F', D[p])$, which is a subgroup of Hom($G_{F'}, D[p]$). If $\phi'$ is in that subgroup, then $\phi'$ factors through Gal($K'/F'$), where $K'$ is a cyclic extension of $F'$ of degree $p$ which is ramified only at primes in $S'$. The discriminant of such extensions $K'/Q$ is easily seen to be bounded. One can then use Hermite’s theorem (which states that there are only finitely many extensions of $Q$ with a given discriminant) to see that only finitely many such extensions $K'$ exist. Thus, $H^1_{U' - \text{unr}}(F', D[p])$ is finite and therefore so is $H^1_{U - \text{unr}}(F, D[p])$. It follows that $H^1_{U - \text{unr}}(F, D)[p]$ is finite and therefore $H^1_{U - \text{unr}}(F, D)$ is a cofinitely generated $\mathbb{Z}_p$-module.

Here is an important special case. Suppose that $S$ contains $\text{Ram}(D)$. Let $F_S$ denote the maximal extension of $F$ unramified outside of $S$. Thus, the action of $G_F$ on $D$ factors through the quotient group Gal($F_S/F$). The inertia subgroups of $G_F$ for primes lying above $v \in U$ are all contained in $G_{F_S}$ and generate a dense subgroup of that group. Furthermore, if $\phi \in H^1_{U - \text{unr}}(F, D)$, then $\phi|_{G_{F_S}}$ is a homomorphism which is trivial on every inertia subgroup, and is therefore trivial. More precisely, it is clear that

$$H^1_{U - \text{unr}}(F, D) = \ker\left(H^1(F, D) \rightarrow H^1(F_S, D)\right) \cong H^1(F_S/F, D),$$

the last isomorphism following from the inflation-restriction sequence. Consequently, it follows that $H^1(F_S/F, D)$ is a cofinitely generated $\mathbb{Z}_p$-module.
Remark 1.5.6. One can define a generalization of the Pontryagin dual of the ideal class group $Cl_F$ by letting $p$ vary. Consider a compatible system of $p$-adic representations $\mathcal{V} = \{V_p\}$ of $G_F$. Thus, (i) each $V_p$ is a $\mathbb{Q}_p$-vector space of common dimension $d$, (ii) the action of $G_F$ on $V_p$ factors through $\text{Gal}(F_{S \cup S_p}/F)$, where $S$ is a fixed finite set of primes of $F$; and (iii) if $v$ is a prime of $F$, $v \notin S$, and $p$ is a prime such that $v \nmid p$, then the characteristic polynomial for the Frobenius automorphisms for $v$ acting on $V_p$ has coefficients in $\mathbb{Q}$ and is independent of the choice of $p$. For each prime $p$, choose a Galois-invariant $\mathbb{Z}_p$-lattice $T_p \subset V_p$. Then one can consider the Galois-module $\mathcal{D}_\mathcal{V} = \bigoplus_p V_p/T_p$, which is isomorphic to $(\mathbb{Q}/\mathbb{Z})^d$ as a group. One can then define $H^1_{unr}(F, \mathcal{D}_\mathcal{V})$ in the obvious way. One clearly has

$$H^1_{unr}(F, \mathcal{D}_\mathcal{V}) \cong \bigoplus_p H^1_{unr}(F, V_p/T_p)$$

Obviously, $H^1_{unr}(F, \mathcal{D}_\mathcal{V})$ is finite if and only if $H^1_{unr}(F, V_p/T_p)$ is finite for all $p$ and trivial for all but finitely many $p$. One can say little in general about the finiteness of this group. However, in remark 1.5.10, we will give an example where $H^1_{unr}(F, V_p/T_p)$ is infinite for all primes $p$. It is also possible for this group to be finite for all $p$ and nontrivial for an infinite set of $p$, as we will point out in remark 1.6.5. In the special case where each $V_p$ is the trivial representation of $G_F$, $H^1_{unr}(F, \mathcal{D}_\mathcal{V})$ is the Pontryagin dual of $Cl_F$ and so is finite.

The following result concerns Galois theory for $H^1_{unr}(\cdot, D)$. By this we mean that it shows a relationship between an object associated with $F$ and the $G$-invariant subobject of an object associated to $F'$. One example is the simple fact that $\mathcal{O}_F^\times = (\mathcal{O}_F^\times)^G$. However, Galois theory for the unramified cohomology groups is more subtle.

**Proposition 1.5.7.** Let $F'/F$ be a finite Galois extension. Then the kernel and cokernel of the restriction map

$$H^1_{unr}(F, D) \to H^1_{unr}(F', D)^G$$

are finite. If $p \nmid |F'| : F|$, then the above restriction map is an isomorphism.

**Proof.** Let $n = |G|$. First we show that if $C$ is a $\mathbb{Z}[G]$-module such that $C[n]$ and $C/nC$ are both finite, then $H^i(G, C)$ is finite for any $i \geq 1$. Multiplication by $n$ gives us two obvious exact sequences

$$0 \to C[n] \to C \to nC \to 0, \quad 0 \to nC \to C \to C/nC \to 0$$

51
The following exact sequences are part of the corresponding cohomology sequences.

\[
H^i(G, C[n]) \rightarrow H^i(G, C) \rightarrow H^i(G, nC),
\]

\[
H^{i-1}(G, C/nC) \rightarrow H^i(G, nC) \rightarrow H^i(G, C)
\]

Our assumption about \( C \) implies that \( H^i(G, C[n]) \) and \( H^{i-1}(G, C/nC) \) are both finite. The composite map

\[
H^i(G, C) \rightarrow H^i(G, nC) \rightarrow H^i(G, C)
\]

is just multiplication by \( n \) on \( H^i(G, C) \). Both maps have finite kernels and therefore \( H^i(G, C)[n] \) is finite. But \( H^i(G, C) \) is annihilated by \( |G| = n \) and therefore \( H^i(G, C) \) itself is indeed finite. Note also that if \( C[n] = 0 \) and \( nC = C \), then the argument shows that \( H^i(G, C) = 0 \).

The following exact sequence is part of the inflation-restriction sequence:

\[
0 \rightarrow H^1(F'/F, D(F')) \rightarrow H^1(F, D) \rightarrow H^1(F', D)^G \rightarrow H^2(F'/F, D(F'))
\]

where we let \( D(F') = D^G_{F'} = H^0(F', D) \). Any subgroup \( C \) of \( D \) is a cofinitely generated \( \mathbb{Z}_p \)-module. It is clear that \( C[n] \) and \( C/nC \) will be finite. Applying the remark at the beginning of the proof to \( C = D(F') \), it follows that \( H^1(F'/F, D(F')) \) and \( H^2(F'/F, D(F')) \) are both finite. Also, if \( p \nmid n \), then both these groups vanish.

Consider the following commutative diagram

\[
\begin{array}{ccc}
0 & \rightarrow & H^1_{\text{unr}}(F, D) \\
& & \downarrow a_{F'/F} \\
0 & \rightarrow & H^1_{\text{unr}}(F', D)^G \\
\end{array}
\]

\[
\begin{array}{ccc}
& & \text{c}_{F'/F} \\
\end{array}
\]

\[
\begin{array}{ccc}
& & \text{b}_{F'/F} \\
\end{array}
\]

The finiteness of \( \ker(b_{F'/F}) \) implies the finiteness of \( \ker(a_{F'/F}) \). If \( p \nmid n \), then clearly \( \ker(b_{F'/F}) = 0 \). As for the cokernel, the snake lemma gives the following exact sequence

\[
\ker(c_{F'/F}) \rightarrow \text{coker}(a_{F'/F}) \rightarrow \text{coker}(b_{F'/F})
\]

Now \( \text{coker}(b_{F'/F}) \) is finite and is trivial if \( p \nmid n \). To prove the finiteness, or triviality, of \( \text{coker}(a_{F'/F}) \), it suffices to prove the finiteness, or triviality, of \( \ker(c_{F'/F}) \).
As in the proof of proposition 1.5.1, we study \( \ker(c_{F'/F}) \) factor-by-factor. Suppose \( v \) is any prime of \( F \) and \( v' \) is a prime of \( F' \) lying above \( v \). Consider the restriction map

\[
c_{v'/v}: H^1(I_{F'v}, D) \to H^1(I_{Fv}, D)
\]

(27)

The kernel is \( H^1(I_{v'/v}, D^{I_{v'}}) \), where \( I_{v'/v} = I_{F'v}/I_{Fv} \), a group which can be identified with the inertia subgroup of \( G \) for the prime \( v' \). The kernel of \( c_{v'/v} \) for every \( v \). Furthermore, if \( v \) is unramified in \( F'/F \), then \( I_v = I_{Fv} \) and hence \( \ker(c_{v'/v}) \) is obviously trivial. Therefore, indeed, \( \ker(c_{F'/F}) \) is finite. Also, if \( p \nmid n \), then \( p \nmid |I_{v'/v}| \) for all \( v \), the kernels of the maps (27) are all trivial, and hence \( \ker(c_{F'/F}) = 0 \) in that case, as stated.

Let us now assume that the action of \( G_F \) on \( V \) factors through a finite quotient group \( \Delta \) of \( G_F \). We will refer to such a \( V \) as an Artin representation space. Let \( D = V/T \), where \( T \) is a Galois-invariant \( \mathbb{Z}_p \)-lattice as before. In this case, we have the following result.

**Corollary 1.5.8.** Suppose that \( V \) is an Artin representation space. Then \( H^1_{unr}(F, D) \) is finite.

**Proof.** Let \( F' = F(D) \), the field cut out by \( \rho_D \), which will be a finite Galois extension of \( F \). By proposition 1.5.7, it suffices to show that \( H^1_{unr}(F', D) \). But \( G_{F'} \) acts trivially on \( D \) and hence

\[
H^1_{unr}(F', D) = \text{Hom}(\text{Gal}(L'/F'), D)
\]

where \( L' \) is the \( p \)-Hilbert class field of \( F' \). This group is obviously finite. \( \blacksquare \)

Returning to the trivial Galois module \( D = \mathbb{Q}_p/\mathbb{Z}_p \), one can translate some of the results from the earlier sections rather easily. Consider corollary 1.1.2. The surjectivity of the map \( N_{F'/F} : A_{F'} \to A_F \) corresponds to the surjectivity of the map \( R_{F'/F} : \text{Gal}(L'/F') \to \text{Gal}(L/F) \) which, in turn, is equivalent to the injectivity of the map

\[
H^1_{unr}(F, \mathbb{Q}_p/\mathbb{Z}_p) \to H^1_{unr}(F', \mathbb{Q}_p/\mathbb{Z}_p)
\]

Now using the Artin isomorphism \( Art_{L'/F'} : A_{F'} \to \text{Gal}(L'/F') \), one has isomorphisms

\[
H^1_{unr}(F', \mathbb{Q}_p/\mathbb{Z}_p)^G \cong \text{Hom}_G(A_{F'}, \mathbb{Q}_p/\mathbb{Z}_p) \cong \text{Hom}((A_{F'})_G, \mathbb{Q}_p/\mathbb{Z}_p)
\]

53
If $F'/F$ is cyclic, then $(A_{F'})_G$ is the genus group $G_{F'/F}$ and so we have

$$\overline{G_{F'/F}} \cong H^1_{\text{unr}}(F', \mathbb{Q}_p/\mathbb{Z}_p)^G.$$ 

If $F'/F$ satisfies the assumptions of proposition 1.1.3, then the assertion about $\ker(N_{F'/F})$ in that proposition means that the map 

$$H^1_{\text{unr}}(F, \mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow H^1_{\text{unr}}(F', \mathbb{Q}_p/\mathbb{Z}_p)^G$$

is surjective. More generally, one can regard genus theory as an assertion about the cokernel of that map. For, by definition, if $F'/F$ is a cyclic extension, we have 

$$\overline{G_{F'/F}} \cong \text{coker}(H^1_{\text{unr}}(F, \mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow H^1_{\text{unr}}(F', \mathbb{Q}_p/\mathbb{Z}_p)^G).$$

In general, one can study $\text{coker}(H^1_{\text{unr}}(F, D) \longrightarrow H^1_{\text{unr}}(F', D)^G)$ by using (26). This involves studying the kernels of the local restriction maps (27), which is usually rather straightforward, and the image of the global-to-local map $G^1(F, D)$, which is usually a more subtle question.

Next we return to the situation considered in section 1.4. That is, we assume that we have a finite group $\Delta$ of automorphisms of $F$ and that the order of $\Delta$ is prime to $p$. Let $E = F^{\Delta}$. Suppose that $\varphi$ is an irreducible character of $\Delta$ over $\mathbb{Q}_p$. Thus, $V_{\varphi}$ is an Artin representation space for $G_E$ and the action of $G_E$ factors through $\text{Gal}(F/E)$. We denote the corresponding $D$ by $D_{\varphi}$. We then have the following result.

**Proposition 1.5.9.** Under the above assumptions, there is a canonical isomorphism 

$$H^1_{\text{unr}}(E, D_{\varphi}) \cong \text{Hom}_{\Delta}(\text{Cl}_{F'[p^\infty]}(\varphi), D_{\varphi})$$

In particular, if $d_{\varphi} = 1$, then $H^1_{\text{unr}}(E, D_{\varphi})$ is isomorphic to the Pontryagin dual of $\text{Cl}_{F'[p^\infty]}(\varphi)$.

**Proof.** We apply proposition 1.5.7 to the Galois extension $F/E$. We then have an isomorphism 

$$a_{F/E} : H^1_{\text{unr}}(E, D_{\varphi}) \rightarrow H^1_{\text{unr}}(F, D_{\varphi})^{\Delta}.$$ 

We also have a canonical isomorphism 

$$\text{Art}_{L/F} : C[l[p^\infty]] \rightarrow \text{Gal}(L/F')$$
This isomorphism commutes with the natural actions of $\Delta$ on $Cl[p^\infty]$ and on $\text{Gal}(L/F)$ (with $\Delta$ acting on $\text{Gal}(L/F)$ by inner automorphisms as usual). We can identify $H^1_{\text{unr}}(F, D_\varphi)$ with $\text{Hom}(\text{Gal}(L/F), D_\varphi)$ and then we obtain the isomorphisms

$$H^1_{\text{unr}}(F, D_\varphi)^{\Delta} \cong \text{Hom}_\Delta(\text{Gal}(L/F), D_\varphi) \cong \text{Hom}_\Delta(Cl[p^\infty], D_\varphi)$$

It is clear that a $\Delta$-equivariant homomorphism $Cl[p^\infty] \to D_\varphi$ must factor through the $\varphi$-component of $Cl[p^\infty]$ and this gives the isomorphism in the proposition.

In the special case where $\varphi$ is 1-dimensional, we have

$$\text{Hom}_\Delta(Cl_F[p^\infty](\varphi), D_\varphi) = \text{Hom}(Cl_F[p^\infty](\varphi), D_\varphi)$$

which is isomorphic to the Pontryagin dual of $Cl_F[p^\infty](\varphi)$ because $D_\varphi$ is isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$ as a group.

**Remark 1.5.10.** One can also consider the group of “locally trivial cocycle classes.” The precise definition is

$$H^1_{\text{tr} \text{-} \text{unr}}(F, D) = \ker(H^1(F, D) \to \prod_v H^1(F_v, D))$$

Obviously, $H^1_{\text{tr} \text{-} \text{unr}}(F, D)$ is a subgroup of $H^1_{\text{unr}}(F, D)$. The two groups can certainly differ. For example, let $D = \mathbb{Q}_p/\mathbb{Z}_p$ with a trivial action of $G_F$. Then $H^1_{\text{unr}}(F, \mathbb{Q}_p/\mathbb{Z}_p) = \text{Hom}(\text{Gal}(L/F), \mathbb{Q}_p/\mathbb{Z}_p)$ and $H^1_{\text{tr} \text{-} \text{unr}}(F, \mathbb{Q}_p/\mathbb{Z}_p)$ corresponds to the subgroup of homomorphisms $f : \text{Gal}(L/F) \to \mathbb{Q}_p/\mathbb{Z}_p$ which are trivial on every decomposition subgroup of $\text{Gal}(L/F)$. Obviously, $Cl_F$ is generated by the ideal classes of the prime ideals $P$ of $F$ and so $\text{Gal}(H/F)$ is generated by the Frobenius automorphisms $\sigma_P$ for those prime ideals. Consequently, the same thing is true for $\text{Gal}(L/F)$. Hence if $f(\sigma_P) = 0$ for all $P$, then $f \equiv 0$. Thus, $H^1_{\text{tr} \text{-} \text{unr}}(F, \mathbb{Q}_p/\mathbb{Z}_p) = 0$.

We will now give an example from the theory of elliptic curves to illustrate the possibility that $H^1_{\text{tr} \text{-} \text{unr}}(F, D)$ can be infinite. Of course, it would then follow that $H^1_{\text{unr}}(F, D)$ is infinite. Suppose that $E$ is an elliptic curve defined over $F$. Let $p$ be a prime. For $n \geq 0$, let $E[p^n]$ denote the elements of $E(\mathbb{Q})$ of order dividing $p^n$. As a group, $E[p^n] \cong (\mathbb{Z}/p^n\mathbb{Z})^2$ and there is a natural action of $G_F$ on this group. We will consider

$$D = E[p^\infty] = \bigcup_{n \geq 0} E[p^n]$$

55
which is the \( p \)-primary subgroup of \( E(\mathbb{Q}) \).

A famous theorem of Mordell and Weil asserts that the group of \( F \)-rational points \( E(F) \) is a finitely generated abelian group. Let \( r \) denote its rank. Consider the Kummer homomorphism

\[
\kappa : E(F) \otimes \mathbb{Z} \left( \frac{Q_p}{\mathbb{Z}_p} \right) \rightarrow H^1(G_F, E[p^\infty])
\]

Note that \( E(F) \otimes \mathbb{Z} \left( \frac{Q_p}{\mathbb{Z}_p} \right) \cong (\frac{Q_p}{\mathbb{Z}_p})^r \). The definition of \( \kappa \), which we will now give, is an imitation of classical Kummer theory. (One finds a brief discussion of that in the next section.) Let \( \alpha = a \otimes (1/p^n + \mathbb{Z}_p) \in E(F) \otimes \mathbb{Z} \left( \frac{Q_p}{\mathbb{Z}_p} \right) \), where \( a \in E(F) \). Let \( b \in E(\mathbb{Q}) \) be chosen so that \( p^n b = a \). Define a map \( \sigma : G_F \rightarrow E[p^\infty] \) by \( \sigma(g) = g(b) - b \) for all \( g \in G_F \). Then \( \sigma \) is a 1-cocycle and we define \( \kappa(a) \) to be the class \([\sigma]\) in \( H^1(F, E[p^\infty]) \) of \( \sigma \). It is not hard to verify that \( \kappa \) is injective.

Suppose that \( v \) is any prime of \( F \). Consider the local Kummer homomorphism

\[
\kappa_v : E(F_v) \otimes \mathbb{Z} \left( \frac{Q_p}{\mathbb{Z}_p} \right) \rightarrow H^1(F_v, E[p^\infty])
\]

This is defined just as above and is again an injective map. We then have a commutative diagram

\[
\begin{array}{ccc}
E(F) \otimes \mathbb{Z} \left( \frac{Q_p}{\mathbb{Z}_p} \right) & \longrightarrow & E(F_v) \otimes \mathbb{Z} \left( \frac{Q_p}{\mathbb{Z}_p} \right) \\
\downarrow \kappa & & \downarrow \kappa_v \\
H^1(F, E[p^\infty]) & \longrightarrow & H^1(F_v, E[p^\infty])
\end{array}
\]

(28)

The top horizontal map is induced by the inclusion \( E(F) \subset E(F_v) \). The bottom horizontal map is induced by the restriction map \( G_{F_v} \rightarrow G_F \) (corresponding to a fixed embedding \( F \hookrightarrow F_v \)).

Now it turns out that \( E(F_v) \otimes \mathbb{Z} \left( \frac{Q_p}{\mathbb{Z}_p} \right) = 0 \) if \( v \nmid p \). This is a consequence of the following fact:

Let \( \ell \) be an arbitrary prime. Suppose that \( F_v \) is a finite extension of \( Q_\ell \) and that \( E \) is an elliptic curve defined over \( F_v \). Then \( E(F_v) \cong \mathbb{Z}_\ell^n \times E(F_v)_{\text{tors}} \), where \( n = [F_v : Q_\ell] \).

If \( \ell \neq p \), then \( \mathbb{Z}_\ell \otimes \mathbb{Z} \left( \frac{Q_p}{\mathbb{Z}_p} \right) = 0 \). Since \( E(F_v)_{\text{tors}} \) is finite, its tensor product with \( \mathbb{Q}_p/\mathbb{Z}_p \) is also trivial. However, \( \mathbb{Z}_p \otimes \mathbb{Z} \left( \frac{Q_p}{\mathbb{Z}_p} \right) \cong \mathbb{Q}_p/\mathbb{Z}_p \), and so we have

\[
E(F_v) \otimes \mathbb{Z} \left( \frac{Q_p}{\mathbb{Z}_p} \right) \cong \left( \frac{Q_p}{\mathbb{Z}_p} \right)^{[F_v : Q_\ell]}
\]
if \( v \mid p \). It is then clear from diagram (28) that the kernel of the map
\[
E(F) \otimes \mathbb{Z} (\mathbb{Q}_p/\mathbb{Z}_p) \longrightarrow \prod_{v \mid p} E(F_v) \otimes \mathbb{Z} (\mathbb{Q}_p/\mathbb{Z}_p)
\]
is a subgroup of \( H^1_{tr,v}(\mathbb{Q}, E[p^\infty]) \). But this kernel is obviously infinite if
\[
r > \sum_{v \mid p} [F_v : \mathbb{Q}_p] = [F : \mathbb{Q}].
\]
This can certainly happen. For example, one could take \( F = \mathbb{Q} \) and \( E \) to be an elliptic curve whose Mordell-Weil group has rank \( \geq 2 \). If \( r \) is that rank, then \( H^1_{tr,v}(\mathbb{Q}, E[p^\infty]) \) contains a subgroup isomorphic to \((\mathbb{Q}_p/\mathbb{Z}_p)^r\)^{−1}.

This is an example that we alluded to at the end of remark 1.5.6. We can associate a compatible system \( V \) of \( p \)-adic representations with \( E \) by defining \( V_p(E) = \mathbb{Q}_p \otimes T_p(E) \) where \( T_p(E) \) is the \( p \)-adic Tate-module for \( E \). Then \( D = V_p(E)/T_p(E) \cong E[p^\infty] \) and \( \mathcal{D}_V \cong E(\mathbb{Q})_{tor} \). The above discussion shows that \( H^1_{unr}(F, \mathcal{D}_V) \) contains a subgroup isomorphic to \((\mathbb{Q}/\mathbb{Z})^{r-1}\).

### 1.6 Powers of the cyclotomic character.

Let \( \mu_{p^\infty} = \bigcup_{n \geq 0} \mu_{p^n} \) denote the group of \( p \)-power roots of unity in \( \overline{\mathbb{Q}} \). The extension \( F(\mu_{p^\infty})/F \) is an infinite Galois extension and one can define a continuous homomorphism
\[
\chi : \text{Gal}(F(\mu_{p^\infty})/F) \to \mathbb{Z}_p^\times
\]
in the following way. Let \( g \in \text{Gal}(F(\mu_{p^\infty})/F) \). For every \( n \geq 0 \), there exists an integer \( u_n \) such that \( g(\zeta) = \zeta^{u_n} \) for all \( \zeta \in \mu_{p^n} \). This integer \( u_n \) is uniquely determined modulo \( p^n \) and is not divisible by \( p \). The definition implies that \( u_{n+1} \equiv u_n \pmod{p^n} \) and hence that \( \{u_n\} \) converges to a certain \( p \)-adic unit \( u \). We then have \( g(\zeta) = \zeta^u \) for all \( \zeta \in \mu_{p^\infty} \). Define \( \chi(g) = u \). The stated properties of \( \chi \) are easily verified. One refers to \( \chi \) as the “\( p \)-power cyclotomic character,” regarding it often as a character of \( G_F \) which factors through the quotient group \( \text{Gal}(F(\mu_{p^\infty})/F) \).

The character \( \chi \) gives the action of \( G_F \) on \( T = \varprojlim \mu_{p^n} \), which is a free \( \mathbb{Z}_p \)-module of rank 1. The \( G_F \)-module \( T \) with this action is often denoted by \( \mathbb{Z}_p(1) \). It is a Galois-invariant \( \mathbb{Z}_p \)-lattice in the vector space \( V = T \otimes \mathbb{Q}_p \). The quotient \( V/T \) is isomorphic to \( \mu_{p^\infty} \).
In this section, we want to discuss one-dimensional representations of $G_F$ over $Q_p$ arising from powers of $\chi$. In particular, we will consider the powers $\chi^n$, where $n \in \mathbb{Z}$, but it turns out to be important to consider a more general class of representations. The prime $p$ will be assumed to be odd in most of the results. We will discuss $p = 2$ at the very end.

Consider an arbitrary continuous homomorphism 

$$\psi : \text{Gal}(F(\mu_p^\infty)/F) \to \mathbb{Z}_p^\times$$

Then $\psi$ defines a 1-dimensional representation space $V$ for $\text{Gal}(F(\mu_p^\infty)/F)$. Equivalently, we can regard $V$ as a representation space for $G_F$, where the action factors through the restriction map $G_F \to \text{Gal}(F(\mu_p^\infty)/F)$. Any $\mathbb{Z}_p$-lattice $T$ will be $G_F$-invariant and $D = V/T$ will be isomorphic to $Q_p/\mathbb{Z}_p$ as a group, but with the action of $G_F$ given by the character $\psi$. We will denote this $D$ by $D_\psi$ in the rest of this section. If $\psi$ has finite order, then corollary 1.5.8 asserts that $H^1_{\text{unr}}(F, D_\psi)$ is finite. As we will discuss in the next chapter, it is possible for $H^1_{\text{unr}}(F, D_\psi)$ to be infinite if $\psi$ has infinite order, but this can only happen for finitely many choices of $\psi$.

Since we are assuming that $p$ is odd, we have a direct product decomposition 

$$\mathbb{Z}_p^\times \cong \mu_{p-1} \times (1 + p\mathbb{Z}_p)$$

Corresponding to this decomposition, we will write $\chi = \omega \langle \chi \rangle$, where $\omega$ is a character of order $p - 1$, the composition of $\chi$ with projection to the factor $\mu_{p-1}$, and $\langle \chi \rangle$ is the composition of $\chi$ with projection to the factor $1 + p\mathbb{Z}_p$.

Assume that $\chi$ is surjective. That is, we assume that $\chi$ defines an isomorphism $\text{Gal}(F(\mu_p^\infty)/F) \cong \mathbb{Z}_p^\times$. Then it is not hard to see that an arbitrary $\psi$ can be uniquely expressed in the form 

$$\psi = \omega^i \langle \chi \rangle^s$$

where $0 \leq i \leq p - 2$ and $s \in \mathbb{Z}_p$. Thus, in a sense, one can regard $\psi$ as a power of $\chi$. It is actually a limit of integer powers of $\chi$. To explain what we mean, note that the group $\text{Hom}(\text{Gal}(F(\mu_p^\infty)/F), \mathbb{Z}_p^\times)$ has a natural topology on it, the compact-open topology. It is rather simple to describe in this case because $\text{Gal}(F(\mu_p^\infty)/F)$ is compact and contains a dense, cyclic subgroup. If $g_\alpha$ is a topological generator for $\text{Gal}(F(\mu_p^\infty)/F)$, then there is a bijection 

$$\text{Hom}(\text{Gal}(F(\mu_p^\infty)/F), \mathbb{Z}_p^\times) \longrightarrow \mathbb{Z}_p^\times$$

58
defined by sending \( \psi \) to \( \psi(g_0) \). The compact-open topology then coincides with the topology transferred from \( \mathbb{Z}_p^\times \). To see that \( \{ \chi^n \mid n \in \mathbb{Z} \} \) is a dense subgroup of \( \text{Hom}(\text{Gal}(F(\mu_{p^n})/F), \mathbb{Z}_p^\times) \), consider \( \psi = \omega^i \langle \chi \rangle^s \). One can take a sequence of integers \( n_k \) such that (\( i \)) \( n_k \equiv i \pmod{p - 1} \) for all \( k \) and (\( ii \)) \( n_k \to s \) in \( \mathbb{Z}_p \) as \( k \to \infty \). Then \( \chi^{n_k} \to \psi \) in the compact-open topology on \( \text{Hom}(\text{Gal}(F(\mu_{p^n})/F), \mathbb{Z}_p^\times) \).

For a fixed \( i \), the following proposition describes a kind of continuity for the behavior of \( H^1_{\text{unr}}(F, D_\psi) \) as \( s \) varies over \( \mathbb{Z}_p \). In addition to the above assumption about \( \chi \), we impose a mild ramification assumption.

**Proposition 1.6.1.** Assume that \( p \) is odd, that \( \chi \) is an isomorphism, and that every prime of \( F \) lying above \( p \) is totally ramified in \( F(\mu_p)/F \). Suppose that \( i \) is fixed, that \( 1 \leq i \leq p - 2 \), and that \( \psi = \omega^i \langle \chi \rangle^s \) for some \( s \in \mathbb{Z}_p \).

Then

\[
H^1_{\text{unr}}(F, D_\psi)[p^k] \cong H^1_{\text{unr}}(F, D_\psi[p^k])
\]

for any \( k \geq 1 \). Assume that \( s_1, s_2 \in \mathbb{Z}_p \) satisfy \( s_1 \equiv s_2 \pmod{p^{k-1}} \). Let \( \psi_1 = \omega^i \langle \chi \rangle^{s_1} \), \( \psi_2 = \omega^i \langle \chi \rangle^{s_2} \). Then \( H^1_{\text{unr}}(F, D_\psi_1)[p^k] \cong H^1_{\text{unr}}(F, D_\psi_2)[p^k] \).

**Proof.** First note that \( G_F \) acts on \( D_\psi[p] \) by the character \( \omega^i \). The assumptions imply that this character is nontrivial. Hence \( H^0(F, D_\psi) = 0 \). Also, if \( v \) is any prime of \( F \) lying above \( p \), then the assumptions imply that \( \omega^i|_{I_{F_v}} \) is nontrivial. Therefore, the action of \( I_{F_v} \) on \( D_\psi[p] \) is nontrivial and hence we have \( H^0(F_v^{\text{unr}}, D_\psi) = 0 \). If \( v \) is an infinite prime, then \( H^0(F_v, D_\psi) \) is if \( i \) is odd and \( H^0(F_v, D_\psi) = D_\psi \) if \( i \) is even. If \( v \) is any other prime of \( F \), then \( v \) is unramified in \( F(\mu_{p^n})/F \) and hence \( I_{F_v} \) acts trivially on \( D_\psi \). Therefore, \( H^0(F_v^{\text{unr}}, D_\psi) = D_\psi \). Thus, for all primes \( v \) of \( F \), \( H^0(F_v^{\text{unr}}, D_\psi) \) is a divisible group. The first part of the proposition then follows from remark 1.5.4, taking \( n = k \). The conditions which imply injectivity and surjectivity are satisfied.

If \( s_1 \equiv s_2 \pmod{p^{k-1}} \), then \( u^{s_1} \equiv u^{s_2} \pmod{p^k} \) for all \( u \in 1 + p\mathbb{Z}_p \). Therefore, for any \( g \in G_F \), we have \( \langle \chi \rangle^{s_1}(g) \equiv \langle \chi \rangle^{s_2}(g) \pmod{p^k} \). It follows that

\[
D_{\psi_1}[p^k] \cong D_{\psi_2}[p^k]
\]

as \( (\mathbb{Z}/p^k\mathbb{Z}) \)-modules with an action of \( G_F \). The second part of the proposition then follows from the first part.

In the above proposition, one can take \( k = 1 \), \( s_1 \) arbitrary and \( s_2 = 0 \). Then \( \psi_2 = \omega^i \), the character of an Artin representation. Consequently, we have the following result.
Corollary 1.6.2. Under the assumptions of proposition 1.6.1, we have
\[ H_{\text{unr}}^1(F, D_\psi)[p] \cong H_{\text{unr}}^1(F, D_{\psi'}[p]). \]
Thus, \( \dim_{F_p}(H_{\text{unr}}^1(F, D_\psi)[p]) \) depends only on \( i \).

Now suppose that \( \psi = \chi^n \), where \( n \in \mathbb{Z} \). The following corollary follows immediately from proposition 1.6.1.

Corollary 1.6.3. Under the assumptions of proposition 1.6.1, we have
\[ H_{\text{unr}}^1(F, D_{\chi^n})[p^k] \cong H_{\text{unr}}^1(F, D_{\chi^{n_2}})[p^k] \]
if \( n_1, n_2 \in \mathbb{Z} \) satisfy the congruence \( n_1 \equiv n_2 \pmod{(p - 1)p^{k-1}} \) and are not divisible by \( p - 1 \).

The case where \( \psi = \langle \chi \rangle^s \), which is excluded in proposition 1.6.1 and the above corollaries, is actually quite interesting to consider. There can be a discontinuity at \( s = 0 \). If \( \psi = \psi_0 \), which corresponds to \( s = 0 \), then \( H_{\text{unr}}^1(F, D_{\psi_0}) \) is the Pontryagin dual of \( Cl_F[p^\infty] \). It turns out that \( H_{\text{unr}}^1(F, D_\psi) \) is finite for \( s \) close to 0 in \( \mathbb{Z}_p \), but, in certain cases, its order will be unbounded as \( s \to 0 \).

In certain other cases, its order will be bounded, but larger than \( h_F^{(p)} \).

We will assume that \( s \neq 0 \). Let \( F_\infty = F(D_\psi) \) denote the field cut out by \( \psi \). Obviously, \( F_\infty \) is a subfield of \( F(\mu_{p^n}) \) and \( \text{Gal}(F_\infty/F) \cong \text{im}(\psi) \) which is isomorphic to \( \mathbb{Z}_p \). We will let \( \Gamma \) denote \( \text{Gal}(F_\infty/F) \). One often refers to \( F_\infty \) as the cyclotomic \( \mathbb{Z}_p \)-extension of \( F \). We will have more to say about it at the beginning of chapter 2. For simplicity, we will assume that the primes of \( F \) lying over \( p \) are all totally ramified in \( F_\infty/F \). It is clear that all other non-archimedean primes are unramified since the same is true for \( F(\mu_{p^n})/F \).

Applying the snake lemma to (23) gives us the following extension of (24), where we use the same notation for the maps and take \( D = D_\psi \):
\[
\ker(\beta_n) \longrightarrow \ker(\gamma_n) \longrightarrow \coker(\alpha_n) \longrightarrow \coker(\beta_n) \tag{29}
\]
in the notation of those diagrams. We have \( \coker(\beta_n) = 0 \), as explained in the first part of the proof of proposition 1.5.1. (See (21).)

Since \( s \neq 0 \), \( H^0(F, D_\psi) \) will be a finite cyclic group. Let \( p^u \) denote its order. Note that \( u \geq 1 \). If \( \text{ord}_p(s) = k \geq 0 \), then \( u = k + 1 \). It follows from (20) that \( \ker(\beta_n) \) will be cyclic and its order will be \( p^{\min(n,u)} \). If \( n = u \), then one can describe this kernel very simply. In that case, \( G_F \) acts trivially on \( D_\psi[p^n] \), \( H^1(F, D_\psi[p^n]) = \text{Hom}(G_F, D_\psi[p^n]) \), and a 1-cocycle \( \phi \) is in \( \ker(\beta_n) \) if and only if \( \phi \) is the coboundary of an element of \( D[p^{2n}] \). Since the action
of $G_F$ on $D[p^n]$ factors through $\Gamma = \Gal(F_\infty/F)$, any $\phi \in \ker(\beta_n)$ will also factor through $\Gamma$ and hence through $\Gamma/\Gamma^p$. We will denote the fixed field for $\Gamma^p$ by $F_n$, a cyclic extension of $F$ of degree $p^n$. Thus, it follows that

$$\ker(\beta_n) = \Hom(\Gal(F_n/F), D_\psi[p^n])$$

if $n = ord_p(s) + 1$. It remains to study $\ker(\gamma_n)$ and the image of the map $\ker(\beta_n) \to \ker(\gamma_n)$ in (29). That image is cyclic and not difficult to study. As we will see, it is possible for $\ker(\gamma_n)$ to be non-cyclic. If that is so, then $\coker(\alpha_n)$ would obviously be nontrivial and that would imply that $H^1_{\text{unr}}(F, D_\psi) \neq 0$.

Since $\psi$ is unramified for all $v \nmid p$, it follows from the second part of the proof of proposition 1.5.1 that $\ker(\gamma_{n,v}) = 0$ for such $v$. But for any $v \mid p$, we are assuming that the inertia subgroup of $\Gal(F_\infty/F)$ is the entire group and hence $H^0(F_v^{\text{unr}}, D_\psi) = H^0(F, D_\psi)$ will have order $p^u$. In fact, just as explained above, if $n = ord_p(s) + 1$, then $\ker(\gamma_{n,v})$ will be cyclic of order $p^n$. Suppose that there are $t$ primes of $F$ lying over $p$. Then $\ker(\gamma_n)$ could potentially have $t$ cyclic factors of order at least $p^n$. However, the actual size of $\ker(\gamma_n)$ depends on the intersection

$$\text{im}\left(\ll H^1(F_{S_p}/F, D_\psi[p^n]) \to \prod_{v \mid p} H^1(F_v^{\text{unr}}, D[p^n]) \rr \right) \cap \prod_{v \mid p} \ker(\gamma_{n,v})$$

where $S_p$ denotes the set of primes of $F$ lying above $p$. We will consider two extreme cases in the following result.

**Proposition 1.6.4.** Assume that $p$ is an odd prime and that all primes in $S_p$ are totally ramified in $F_\infty/F$. Let $\psi = \langle \chi \rangle^s$, where $s \in \Z_p$, $s \neq 0$.

(i) If $|S_p| = 1$ and $n = ord_p(s) + 1$, then $\coker(\alpha_n) = 0$. In particular, if $h_{\psi}^{(p)} = 1$, then $H^1_{\text{unr}}(F, D_\psi) = 0$.

(ii) If $p$ splits completely in $F/Q$ and $n = ord_p(s) + 1$, then

$$\Hom(\Gal(F_{S_p}/F), D_\psi[p^n]) / \Hom(\Gal(F_n/F), D_\psi[p^n]) \cong H^1_{\text{unr}}(F, D_\psi)[p^n]$$

In particular, if $F$ has a nontrivial cyclic $p$-extension which is ramified in $S_p$ and not contained in $F_\infty$, then $H^1_{\text{unr}}(F, D_\psi) \neq 0$.

**Proof.** If there is just one prime $v \in S_p$, then the map $\ker(\beta_n) \to \ker(\gamma_n)$ is surjective. This follows from the facts mentioned above: both $\ker(\beta_n)$ and
\( \ker(\gamma_{n,v}) \) have order \( p^n \), the map is injective since \( v \) is totally ramified in \( F_n/F \). Hence, in case (i), \( \ker(\alpha_n) = 0 \) and we have an isomorphism

\[
H^1_{\text{unr}}(F, D_\psi)[p^n] \cong H^1_{\text{unr}}(F, D_\psi[p^n])
\]

for \( n = \text{ord}_p(s) + 1 \). In particular, if we make the assumption that \( p \nmid h_F \), then for any \( s \in \mathbb{Z}_p \), it follows that \( H^1_{\text{unr}}(F, D_\psi)[p^n] = 0 \) for some \( n \geq 1 \) and hence \( H^1_{\text{unr}}(F, D_\psi) = 0 \).

Now assume that \( p \) splits completely in \( F/\mathbb{Q} \). Then \( F_v = \mathbb{Q}_p \) for all \( v \in S_p \). We will then show that the map

\[
H^1(F_v, D_\psi[p^n]) \longrightarrow H^1(F_v^{\text{unr}}, D_\psi)
\]

is trivial for \( n \) as stated. To see this, note that an element \( \phi \in H^1(F_v, D_\psi[p^n]) \) is just a homomorphism of order dividing \( p^n \) and factors through a cyclic extension of \( F_v \). Now both \( F_v^{\text{unr}} \) and \( F_v(\mu_{p^n}) \) contain unique cyclic extension of \( F_v \) of degree \( p^n \). The intersection of those two extensions is \( F_v \) since one is an unramified extension, the other totally ramified. Their compositum contains any cyclic extension of \( F_v \) of degree dividing \( p^n \). This follows from local class field theory since \( F_v^{\times}/(F_v^{\times})^p \cong (\mathbb{Z}/p^n/\mathbb{Z})^2 \). It follows that \( \phi = \phi^{\text{anr}} \phi^{\text{yc}} \), where \( \phi^{\text{anr}} \) and \( \phi^{\text{yc}} \) are elements of \( H^1(F_v, D_\psi[p^n]) \) which factor through \( \text{Gal}(F_v^{\text{unr}})/F_v \) and \( \text{Gal}(F_v(\mu_{p^n})/F_v) \), respectively. They are both homomorphisms of order dividing \( p^n \). The earlier argument describing \( \ker(\beta_n) \) applies without change to \( F_v \). It follows that

\[
\ker(H^1(F_v, D_\psi[p^n]) \longrightarrow H^1(F_v, D_\psi))
\]

contains \( \phi^{\text{yc}} \). On the other hand, \( \phi^{\text{anr}} \) is clearly in the kernel of the restriction map \( H^1(F_v, D_\psi) \longrightarrow H^1(F_v^{\text{unr}}, D_\psi) \). It follows that the image of \( \phi \) under the map (31) is indeed trivial, as stated.

Now the inflation map identifies \( \text{Hom}(\text{Gal}(F_{S_p}/F), D_\psi[p^n]) \) with a certain subgroup of \( H^1(F, D_\psi[p^n]) = \text{Hom}(G_F, D_\psi[p^n]) \). Under the assumption that \( v \) splits completely in \( F/\mathbb{Q} \), (31) implies that its image under \( \beta_n \) is contained in \( H^1_{\text{unr}}(F, D_\psi)[p^n] \). Conversely, since \( \ker(\gamma_{n,v}) \) is trivial for all \( v \nmid p \), if \( \phi \in \text{Hom}(G_F, D_\psi[p^n]) \) and \( \beta_n(\phi) \in H^1_{\text{unr}}(F, D_\psi)[p^n] \), then \( \phi \) factors through \( \text{Gal}(F_{S_p}/F) \). It follows that

\[
\beta_n(\text{Hom}(\text{Gal}(F_{S_p}/F), D_\psi[p^n])) = H^1_{\text{unr}}(F, D_\psi)[p^n]
\]

Thus part (ii) of the proposition now follows from (30).
As an example, suppose that $F$ is an imaginary quadratic field and that $p$ splits in $F$. Then, it turns out that for any $n \geq 1$, $F_{S_p}$ contains a subfield $M_n$ such that $\text{Gal}(M_n/F) \cong (\mathbb{Z}/p^n\mathbb{Z})^2$. It is not difficult to prove this using class field theory. Since the unit group of $F$ is finite, the structure of ray class groups is relatively easy to study. Therefore, proposition 1.6.4 implies that if $s \neq 0$, but $s \equiv 0 \pmod{p^{n-1}}$, then $H^1_{\text{unr}}(F, D(\chi_s))$ contains a subgroup of order $p^n$. Thus, the order of $H^1_{\text{unr}}(F, D(\chi_s))$ will be unbounded as $s \to 0$ in $\mathbb{Z}_p$. We have not justified the assertion that this group is finite if $s$ is sufficiently close to 0. That will become easy to verify in chapter 2.

A topic which we will discuss in detail in chapter 3 concerns the special case where $\psi = \chi$, the $p$-power cyclotomic character itself. Classical Kummer theory gives the following important isomorphism:

$$\kappa : F^\times \otimes \mathbb{Z} (\mathbb{Q}_p/\mathbb{Z}_p) \to H^1(F, \mu_{p^n})$$

The map is easily defined. Let $\alpha = a \otimes (1/p^n + \mathbb{Z}_p) \in F^\times \otimes \mathbb{Z} (\mathbb{Q}_p/\mathbb{Z}_p)$, where $a \in F^\times$. Let $b$ be a $p^n$-th root of $a$ in $\overline{\mathbb{Q}}^\times$. Define $\sigma : G_F \to \mu_{p^n}$ by $\sigma(g) = g(b)/b$ for all $g \in G_F$. Then $\sigma$ is a 1-cocycle and we define $\kappa(\alpha)$ to be the class $[\sigma]$ in $H^1(F, \mu_{p^n})$ of $\sigma$. It is not hard to verify that $\kappa$ is injective. The surjectivity is a consequence of Hilbert’s theorem 90, the fact that $H^1(F, \overline{\mathbb{Q}}^\times) = 1$, and will also be left to the reader.

Note that $H^1(F, \mu_{p^n})$ is a very big group. Indeed, it is not hard to show that $F^\times \otimes \mathbb{Z} (\mathbb{Q}_p/\mathbb{Z}_p)$ is a direct sum of a countable number of copies of $\mathbb{Q}_p/\mathbb{Z}_p$. On the other hand, there is considerable reason to believe the following important conjecture:

**Leopoldt’s Conjecture.** $H^1_{\text{unr}}(F, \mu_{p^n})$ is a finite group.

The usual way to formulate this conjecture involves the image of the unit group of $F$ in the direct product of the completions of $F$ at the primes above $p$. The connection with the units of $F$ arises from Kummer theory. If $a \in \mathcal{O}_F^\times$ and $n \geq 1$, then one can consider the cocycle class in $H^1(F, \mu_{p^n})$ associated to $b = \sqrt[n]{a}$. This cocycle class is unramified at all primes of $F$ not dividing $p$. Whether or not it is unramified at a prime $v$ dividing $p$ is related (although not quite equivalent) to whether or not $F_v(\sqrt[n]{a})/F_v$ is a ramified extension. Leopoldt’s conjecture essentially amounts to the assertion that only finitely many of these cocycle classes are unramified at all $v | p$.

Suppose now that $F = \mathbb{Q}$, $p$ is an odd prime, and $\psi = \chi^n$ for some $n \in \mathbb{Z}$ such that $n \equiv 0 \pmod{p-1}$. The assumptions in proposition 1.6.1 and its
corollaries are satisfied. These groups are trivial if \( p \) is a regular prime. To see this, it is enough to verify that \( H^1_{\text{unr}}(\mathbb{Q}, D_{\chi^n})[p] = 0 \). Choose \( i \) so that \( n \equiv i \pmod{p-1}, 1 \leq i \leq p-2 \). According to corollary 1.6.2, it suffices to show that \( H^1_{\text{unr}}(\mathbb{Q}, D_{\omega^i}) = 0 \). But this is true according to proposition 1.5.8 since, by assumption, \( \text{Cl}_{\mathbb{Q}(\mu_p)}[p^\infty]^{(\omega)} = 0 \). If \( n \equiv 0 \pmod{p-1} \), then \( H^1_{\text{unr}}(\mathbb{Q}, D_{\chi^n})[p] = 0 \). This follows from part (i) of proposition 1.6.4.

If \( p \) is an irregular prime, then \( \text{Cl}_{\mathbb{Q}(\mu_p)}[p^\infty]^{(\omega)} \neq 0 \) for at least one odd value of \( i \). Thus, for any such \( i \), it follows that \( H^1_{\text{unr}}(\mathbb{Q}, D_{\chi^n}) \neq 0 \) for any integer \( n \equiv i \pmod{p-1} \). In a later chapter, we will prove that the group \( H^1_{\text{unr}}(\mathbb{Q}, D_{\chi^n}) \) is finite for all odd, negative values of \( n \). The order of this group turns out to be closely related to values of the Riemann zeta function \( \zeta(s) \). Recall that \( \zeta(s) \) can be analytically continued to the complex plane (with a simple pole at \( s = 1 \)). Its functional equation forces \( \zeta(n) = 0 \) when \( n \) is a negative, even integer. It is known that \( \zeta(n) \) is a nonzero, rational number if \( n \) is negative and odd, closely related to one of the Bernoulli numbers. To be precise, if we write \( n = 1 - m \), where \( m \) is positive and even, then

\[
\zeta(n) = -\frac{B_m}{m}.
\]

It is useful to state the congruences

\[
m_1 \equiv m_2 \not\equiv 0 \pmod{p-1} \implies \frac{B_{m_1}}{m_1} \equiv \frac{B_{m_2}}{m_2} \pmod{p\mathbb{Z}_p}
\]

which are known as the Kummer congruences. We have expressed them as congruences modulo \( p\mathbb{Z}_p \) since the quantities \( B_m/m \) are \( p \)-integral, and hence in \( \mathbb{Z}_p \), for \( m \not\equiv 0 \pmod{p-1} \). Note that for \( 0 < m < p \), \( B_m \) is divisible by \( p \) precisely when \( B_m/m \) is divisible by \( p \). Thus, the Herbrand-Ribet theorem can be stated as follows:

**If \( n \) is an odd, negative integer, then \( H^1_{\text{unr}}(\mathbb{Q}, D_{\chi^n}) \neq 0 \) if and only if \( p \) divides the numerator of \( \zeta(n) \).**

The following much more precise result is a consequence of a theorem of Mazur and Wiles to be discussed in a later chapter. It is an illustration of the close connection between values of \( L \)-functions and certain objects defined by Galois cohomology.

**Theorem.** Suppose that \( p \) is an odd prime, that \( n \) is an odd, negative integer, and that \( n \not\equiv 1 \pmod{p-1} \). Then the order of \( H^1_{\text{unr}}(\mathbb{Q}, D_{\chi^n}) \) is equal to the power of \( p \) dividing \( \zeta(n) \).
In chapter 2, we will show that the groups $H^1_{\text{unr}}(\mathbb{Q}, D_{\chi^n})$ can be studied by an analogue of proposition 1.5.7 for the infinite Galois extension $\mathbb{Q}(\mu_{p^{\infty}})/\mathbb{Q}$. It turns out that the kernel and cokernel are actually trivial. This fact will allow us to relate the structure of the finite groups $H^1_{\text{unr}}(\mathbb{Q}, D_{\chi^n})$, for all $n$, to the structure of the Galois group of a certain extension of $\mathbb{Q}(\mu_{p^{\infty}})$, the analogue of the $p$-Hilbert class field.

For $n \equiv 1 \pmod{p - 1}$, one has $H^1_{\text{unr}}(\mathbb{Q}, D_{\chi^n})[p] \cong H^1_{\text{unr}}(\mathbb{Q}, D_\omega)[p] = 0$ and hence $H^1_{\text{unr}}(\mathbb{Q}, D_{\chi^n}) = 0$. However, assuming $n$ is also negative, the denominator of $\zeta(n)$ is then divisible by $p$. To be precise, suppose that $n = 1 - m$ where $m > 0$ and $m \equiv 0 \pmod{p - 1}$, then the Clausen-von Staudt theorem states $\text{ord}_p(B_m) = -1$. Thus,

$$\text{ord}_p(\zeta(n)) = -1 - \text{ord}_p(m)$$

and so the power of $p$ dividing the denominator of $\zeta(n)$ is unbounded. In fact, restricting to negative $n \equiv 1 \pmod{p - 1}$, as $n \to 1$ $p$-adically, we have $\text{ord}_p(\zeta(n)) \to -\infty$. This corresponds to a property of the Kubota-Leopoldt $p$-adic $L$-function $L_p(\omega^0, s)$, namely that this function has a pole at $s = 1$.

In light of the above theorem and the continuity properties described in corollary 1.6.3, it is natural to ask whether analogous continuity properties hold for the powers of $p$ dividing the values of $\zeta(s)$ at negative integers. A refinement of the Kummer congruences stated earlier provides an even more precise result. Define

$$\zeta_p(s) = (1 - \frac{1}{p^s})\zeta(s),$$

which is just the function defined by the Euler product for $\zeta(s)$ with the Euler factor for $p$ removed, analytically continued to the complex plane (except $s = 1$). Thus, if $n$ is a negative, odd integer, then $\zeta_p(n) = (1 - p^n)\zeta(n)$, which is nonzero and divisible by the same power of $p$ as $\zeta(n)$. Assume that $k \geq 1$. The refined Kummer congruences, stated in terms of values of $\zeta_p(s)$, are

$$n_1 \equiv n_2 \pmod{(p - 1)p^{k-1}} \implies \zeta_p(n_1) \equiv \zeta_p(n_2) \pmod{p^k\mathbb{Z}_p}$$

where it is assumed that $n_1$, $n_2$ are odd, negative integers and $n_1, n_2 \not\equiv 1 \pmod{p - 1}$.

**Remark 1.6.5.** We return to the discussion in remark 1.5.6. Suppose that $n \in \mathbb{Z}$ is fixed. We will consider the compatible system $\mathcal{V} = \{V_p\}$ where, for
each prime $p$, $V_p$ is 1-dimensional and $G_Q$ acts by $\chi^n$, where $\chi$ is the $p$-power cyclotomic character. The Mazur-Wiles theorem implies that if $n$ is odd and negative, then the finite group $H^1_{\text{unr}}(Q, D_{\chi^n})$ is trivial for all but finitely many primes $p$. It follows that $H^2_{\text{unr}}(Q, D_V)$ is finite. This can actually be proved just using Herbrand’s half of the Herbrand-Ribet theorem, the assertion that if $0 < m < p$, $m$ is even, and $p \nmid B_m$, then $H^2_{\text{unr}}(Q, D_{\omega^{1-m}}) = 0$. In fact, it is not necessary to assume that $m < p$. Since $B_m \neq 0$, only finitely many primes $p$ can divide $B_m$. Hence, if $n = 1 - m$, it follows that $H^1_{\text{unr}}(Q, D_{\chi^n}) = 0$ if $p \nmid B_m$.

The situation is quite different for positive, odd values of $n$. First of all, apart from the cases discussed above, it is not even known that $H^1_{\text{unr}}(Q, D_{\chi^n})$ is finite, although this is expected to be so. Furthermore, we have

$$H^1_{\text{unr}}(Q, D_{\chi^n})[p] \cong H^1_{\text{unr}}(Q, D_{\omega^n})[p]$$

and, if $p > n$, the Herbrand-Ribet theorem implies that this group is nontrivial if and only if $p \nmid B_{p-n}$. However, it seems reasonable to conjecture that this occurs for an infinite, although very sparse, set of primes $p$. For example, take $n = 3$. It turns out that $p | B_{p-3}$ for $p = 16843$ and for $p = 2124679$. For even values of $n$, positive or negative, Vandiver’s conjecture implies that $H^1_{\text{unr}}(Q, D_{\chi^n}) = 0$ for all $p$. 

66