TOPICS IN IWASAWA THEORY

Ralph Greenberg

Table of contents

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 $F = \mathbf{Q}(\mu_p)$, where p is any prime and μ_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 $h_{F_n}^{(p)}$ 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 $h_{F_n}^{(p)}$. We will discuss this and other theorems of Iwasawa concerning $Cl_{F_n}[p^\infty]$ 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:

$$N_{F'/F} : Cl_{F'} \to Cl_F, \qquad J_{F'/F} : Cl_F \to Cl_{F'} \tag{1}$$

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 $\mathcal{O}_{F'}^\times$ as a Galois module.

The third section concerns *"genus theory."* which shows the influence of the ramified primes on $\dim_{\mathbf{F}_p}(Cl_{F'}[p])$ 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 μ_p, where p is a prime, and a group Δ of automorphisms of F. It is assumed that p doesn't divide $|\Delta|$. One can regard $Cl_F[p]$ as a representation space for Δ over the field $\mathbf{F}_p$. It can be decomposed as a direct sum of the irreducible representations of Δ over $\mathbf{F}_p$, 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 $\mathrm{Gal}(F(\mu_{p^\infty})/F)$. 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:

$$\mathcal{N}_{F'/F} : \mathcal{F'}_F \to \mathcal{F}_F, \qquad \mathcal{J}_{F'/F} : \mathcal{F}_F \to \mathcal{F}_{F'}$$

The second map $\mathcal{J}_{F'/F}$ 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 $\mathcal{J}_{F'/F}$ is injective, but not surjective if $[F' : F] > 1$. To define the first map, it is sufficient to

define $\mathcal{N}_{F'/F}(P')$ 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

$$\mathcal{N}_{F'/F}(P') = P^{f(P'/P)} \tag{2}$$

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

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

$$\mathcal{N}_{F'/F}(\alpha' \mathcal{O}_{F'}) = \alpha \mathcal{O}_F \tag{3}$$

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

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

$$\mathrm{Art}_{H/F} : Cl_F \to \mathrm{Gal}(H/F),$$

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 $\sigma_P \in \mathrm{Gal}(H/F)$ 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

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

by putting $\mathrm{Frob}_{H/F}(P) = \sigma_P$ 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 $\mathrm{Art}_{H/F}(c) = \mathrm{Frob}_{H/F}(I)$ for every $c \in Cl_F$, 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 $N_{F'/F} : Cl_{F'} \to Cl_F$ is surjective.*

One immediate consequence is that if $F' \cap H = F$, then h_F divides $h_{F'}$. Another consequence is that the map $N_{F'/F} : Cl_{F'}[p^\infty] \to Cl_F[p^\infty]$ 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:

$$\begin{array}{ccc} Cl_{F'} & \longrightarrow & \mathrm{Gal}(H'/F') \\ \Big\downarrow{\scriptstyle N_{F'/F}} & & \Big\downarrow{\scriptstyle R_{F'/F}} \\ Cl_F & \longrightarrow & \mathrm{Gal}(H/F) \end{array} \tag{4}$$

Here H' denotes the Hilbert class field of F'. Note that $H \subset HF' \subset H'$. The right vertical map is the restriction map $g \to g|_H$, where $g \in \mathrm{Gal}(H'/F')$. The horizontal maps are the isomorphisms $\mathrm{Art}_{H'/F'}$ and $\mathrm{Art}_{H/F}$. 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 $\sigma_{P'} \in \mathrm{Gal}(H'/F')$ and $\sigma_P \in \mathrm{Gal}(H/F)$ denote the corresponding Frobenius automorphisms. Then, on the one hand, we have the following well-known property: $\sigma_{P'}|_H = \sigma_P^{f(P'/P)}$. Comparing this with (2), we see that

$$\mathrm{Frob}_{H'/F'}(I')|_H = \mathrm{Frob}_{H/F}(\mathcal{N}_{F'/F}(I'))$$

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

The restriction map $R_{F'/F} : \mathrm{Gal}(H'/F') \to \mathrm{Gal}(H/F)$ 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 $\mathrm{Gal}(H/H \cap F')$ under the map $\mathrm{Art}_{H/F}$. 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

$$A_F = Cl_F[p^\infty], \qquad A_{F'} = Cl_{F'}[p^\infty] \tag{5}$$

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 $\mathrm{Art}_{L/F} : A_F \to \mathrm{Gal}(L/F)$. 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 $N_{F'/F} : A_{F'} \longrightarrow A_F$ is surjective.*

Suppose that F'/F is a p-extension and let $G = \mathrm{Gal}(F'/F)$. Let $I_1, ..., I_r$ 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 $\mathrm{Art}_{H'/F'}$ of $\ker(R_{F'/F})$, which is obviously $\mathrm{Gal}(H'/HF')$. 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 $\mathrm{Gal}(F'/F)$ by G. There is a natural action of G on $Cl_{F'}$, and so we can regard $Cl_{F'}$ as a module for the group ring $\mathbf{Z}[G]$. We will use a multiplicative notation for the class group in this chapter, and so, if $\theta \in \mathbf{Z}[G]$ and $c' \in Cl_{F'}$, we will denote the action of θ on c' by $(c')^\theta$. Thus, the image of $Cl_{F'}$ under θ will be denoted by $Cl_{F'}^\theta$. 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 $G = \mathrm{Gal}(F'/F)$ is cyclic. Assume also that at most one prime of F is ramified in F'/F. Then*

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

where σ denotes a generator of G.

Proof. The kernel of $R_{F'/F} : \mathrm{Gal}(H'/F') \to \mathrm{Gal}(H/F)$ is $\mathrm{Gal}(H'/HF')$. 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 $\mathrm{Gal}(K/F)$ (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 $I = \mathrm{Gal}(K/H)$. But we also have that $I \cap \mathrm{Gal}(K/F') = 1$, 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 $\widetilde{G} = \mathrm{Gal}(H'/F)$ and $N = \mathrm{Gal}(H'/F')$. We then have an exact sequence

$$1 \to N \to \widetilde{G} \to G \to 1$$

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

$$D(\widetilde{G}) = N^{\sigma-1}$$

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

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

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

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

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

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

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

Since $\mathrm{Art}_{H'/F'} : Cl_{F'} \to N$ 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 $\mathbf{Z}_p$-extensions. It asserts that, under certain stringent assumptions, $A_{F'} \neq 1 \Longleftrightarrow A_F \neq 1$.

Proposition 1.1.4. *Let p be a prime. Suppose that F'/F is a Galois extension and that $G = \mathrm{Gal}(F'/F)$ 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 $\mathbf{Z}[G]$-module. That kernel is $A_{F'}^{\sigma-1}$, where σ again denotes a generator for G. Therefore we obtain an isomorphism

$$A_{F'}/A_{F'}^{\sigma-1} \longrightarrow A_F \tag{6}$$

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 $p|h_F \Longrightarrow p|h_{F'}$ 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 $\mathrm{Gal}(L'/F)$ 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 $\mathrm{Gal}(L'/F)$ 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 $\mathrm{Gal}(L'/F)$. Thus there exists a maximal subgroup M of $\mathrm{Gal}(L'/F)$ which contains I_Q. Maximal subgroups of a p-group have index p and are normal. The nontrivial inertia subgroups of $\mathrm{Gal}(L'/F)$ are conjugate to I_Q and hence also contained in M. Therefore, the fixed field $(L')^M$ is an unramified extension of F and $\mathrm{Gal}((L')^M/F) \cong \mathbf{Z}/p\mathbf{Z}$. 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 $F_v = \mathbf{R}$, $F'_{v'} = \mathbf{C}$, 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 Cl_F^{str} of a number field F is the quotient group $\mathcal{F}_F/\mathcal{P}_F^{tp}$, where $\mathcal{P}_F^{tp}$ 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 $F \to \mathbf{R}$ is positive.) If H^{str} denotes the maximal abelian extension of F unramified at all the finite primes of F, then one can use the corresponding Artin isomorphism $\mathrm{Art}_{H^{str}/F} : Cl_F^{str} \to \mathrm{Gal}(H^{str}/F)$ 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 $A_{F'}^{\tau^j}/A_{F'}^{\tau^{j+1}}$ will also be cyclic of order p for $0 \leq j \leq m-1$ and that $A_{F'}^{\tau^m}$ is trivial. One can regard τ as an element of the group ring for G over $\mathbf{Z}$ or over $\mathbf{F}_p$. In $\mathbf{F}_p[G]$, one can easily verify that $\tau^p = 0$. Hence, in $\mathbf{Z}[G]$, we have $\tau^p \in p\mathbf{Z}[G]$. It follows that $A_{F'}^{\tau^p} \subseteq A_{F'}^{p}$. This implies that

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

One possibility is that $\dim_{\mathbf{F}_p}\big(A_{F'}[p]\big) = 1$. Thus $A_{F'} \cong \mathbf{Z}/p^m\mathbf{Z}$. The automorphism group of $A_{F'}$ is then isomorphic to $(\mathbf{Z}/p^m\mathbf{Z})^{\times}$. 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

$$A_{F'}^{\tau} = A_{F'}^{s-1} = A_{F'}^{p}$$

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

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

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

One gets a better picture of the possibilities by considering $A_{F'}$ as a module over the group ring $\mathbf{Z}_p[G]$. 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 $\mathbf{Z}_p[G]$-module. That is, $A_{F'}$ is a cyclic $\mathbf{Z}_p[G]$-module. Therefore, we have $A_{F'} \cong \mathbf{Z}_p[G]/I$, where I is an ideal in $\mathbf{Z}_p[G]$. The requirement that $[A_{F'} : A_{F'}^{\tau}] = p$ just imposes a simple condition on I, namely that the image

of I in $\mathbf{Z}_p[G]/(\tau)\mathbf{Z}_p[G] \cong \mathbf{Z}_p$ 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

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

defined in section 1. It is obvious that $\mathcal{J}_{F'/F}(\mathcal{P}_F) \subset \mathcal{P}_{F'}$. We obtain a homomorphism from Cl_F to $Cl_{F'}$ as follows. If $c \in Cl_F$ and I is an ideal in c, define $J_{F'/F}(c)$ to be the ideal class in $Cl_{F'}$ represented by $\mathcal{J}_{F'/F}(I)$. Since $\mathcal{J}_{F'/F}(\mathcal{P}_F) \subset \mathcal{P}_{F'}$, the map $J_{F'/F}$ is well-defined. The map $\mathcal{J}_{F'/F}$ 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* $\ker(J_{F'/F})$ *is nontrivial.*

2. $\mathrm{Ker}(J_{H/F}) = Cl_F$.

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 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 $G = \mathrm{Gal}(F'/F)$. 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 $c \in Cl_F$. 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

$$\mathcal{N}_{F'/F}(\mathcal{J}_{F'/F}(I)) = I^n. \tag{7}$$

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 $N_G : Cl_{F'} \to Cl_{F'}$ 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 $\mathrm{im}(J_{F'/F}) = \mathrm{im}(N_G)$.

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

$$I\mathcal{O}_{F'} = \prod_{\sigma \in G} \sigma(I') \tag{9}$$

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

$$\mathcal{N}_{F'/F}(\alpha') = \prod_{\sigma \in G} \sigma(\alpha')$$

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 $I\mathcal{O}_{F'}$ 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 $G = \mathrm{Gal}(F'/F)$ 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 α' be a generator for $I' = I\mathcal{O}_{F'}$. 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 $c \to [\phi]$ 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 $\mathcal{J}_{F'/F}$.

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

$$0 \longrightarrow \ker(J_{F'/F}) \longrightarrow \mathcal{P}_{F'}^G/\mathcal{P}_F \longrightarrow \mathcal{F}_{F'}^G/\mathcal{F}_F \longrightarrow Cl_{F'}^G/J_{F'/F}(Cl_F)$$

Furthermore, we have isomorphisms

$$\mathcal{P}_{F'}^G/\mathcal{P}_F \cong H^1(F'/F, \mathcal{O}_{F'}^{\times}), \qquad \mathcal{F}_{F'}^G/\mathcal{F}_F \cong \prod_{i=1}^{t} \mathbf{Z}/e_i\mathbf{Z}$$

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

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

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{P}_F & \longrightarrow & \mathcal{F}_F & \longrightarrow & Cl_F & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow{\scriptstyle J_{F'/F}} & & \\ 1 & \longrightarrow & \mathcal{P}_{F'}^G & \longrightarrow & \mathcal{F}_{F'}^G & \longrightarrow & Cl_{F'}^G & & \end{array} \tag{10}$$

The first two vertical maps are injective, and so one obtains an injective map: $\ker(J_{F'/F}) \to \mathcal{P}_{F'}^G/\mathcal{P}_F$. 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 (α') in $\mathcal{P}_{F'}^G/\mathcal{P}_F$.

Consider the exact sequence $1 \to \mathcal{O}_{F'}^\times \to F'^\times \to \mathcal{P}_{F'} \to 1$, where the map $F'^\times \longrightarrow \mathcal{P}_{F'}$ is defined by mapping an element of $F'^\times$ 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).

$$1 \longrightarrow \mathcal{O}_F^\times \longrightarrow F^\times \longrightarrow \mathcal{P}_{F'}^G \longrightarrow H^1(F'/F, \mathcal{O}_{F'}^\times) \longrightarrow 1$$

To justify the 1 at the end, we use Hilbert's theorem 90 which states that $H^1(F'/F, (F')^\times)$ is trivial. The isomorphism $\mathcal{P}_{F'}^G/\mathcal{P}_F \cong H^1(F'/F, \mathcal{O}_{F'}^\times)$ follows immediately because the image of $F^\times$ in $\mathcal{P}_{F'}^G$ is $\mathcal{J}_{F'/F}(\mathcal{P}_F)$ (which we are denoting by $\mathcal{P}_F$). This isomorphism is just as mentioned before: If $(\alpha') \in \mathcal{P}_{F'}^G$, 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 $\prod_{i=1}^t \mathbf{Z}/e_i\mathbf{Z}$. 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 $\mathcal{J}_{F'/F}(P) = P\mathcal{O}_{F'} = Q_P^{e_P}$, 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 $Q_P^{e_P}$. It is therefore clear that the quotient group is indeed isomorphic to $\prod_{i=1}^t \mathbf{Z}/e_i\mathbf{Z}$. ∎

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 $\mathbf{Z}[G]$-module. Its structure is difficult to study. However, the vector space

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

can be regarded as a $\mathbf{Q}[G]$-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 $\mathcal{O}_F^{\times}/(\mathcal{O}_F^{\times})^n \longrightarrow H^2(F'/F, \mathcal{O}_{F'}^{\times})$. In particular, if F'/F has prime degree p, then

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

where $s = \dim_{\mathbf{F}_p}\left(\mathcal{O}_F^{\times}/(\mathcal{O}_F^{\times})^p\right)$.

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 $\mathbf{Z}[G]$-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 $\mathbf{Z}[G]$-modules. Then $h(G, L) = h(G, L_1)h(G, L_2)$.*

Consider the $\mathbf{Q}$-vector space $V = L \otimes_{\mathbf{Z}} \mathbf{Q}$, which is a representation space over G over $\mathbf{Q}$ of dimension $d = \mathrm{rank}_{\mathbf{Z}}(L)$. One can regard L/L_{tors} as a $\mathbf{Z}$-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 $\mathbf{Z}$-lattice L. This observation together with the following lemma will make it easy to compute $h(F'/F, \mathcal{O}_{F'}^{\times})$.

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

$$V_{\mathcal{O}_{F'}^\times} \cong W_o^r \times W_1^{r+1}$$

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 $\mathbf{Q}$. 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 $\mathbf{Q}$ is determined (up to isomorphism) by the quantities $\dim_{\mathbf{Q}}(V^H)$, where H varies over all the subgroups of G.

Consider $V = V_{\mathcal{O}_{F'}^\times}$. If H is any subgroup of G, let $E = F')^H$. Then $\dim_{\mathbf{Q}}(V^H)$ is equal to the rank of the group of units of E since $\mathcal{O}_E^\times = (\mathcal{O}_{F'}^\times)^H$, and so $\mathcal{O}_E^\times \otimes \mathbf{Q} \cong V^H$. 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

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

On the other hand, we have $\dim_{\mathbf{Q}}(W_o^H) = 1$ and $\dim_{\mathbf{Q}}(W_1^H) = m-1$. Hence, $(W_o^r \times W_1^{r+1})^H$ 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 $\mathbf{Q}$ is determined by the quantities $\dim_{\mathbf{Q}}(V^H)$. 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 $\dim_{\mathbf{Q}}(V^H)$'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 $\mathbf{Z}$-lattice in V. According to lemma 1.2.5, we can choose such a lattice L so that

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

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

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

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

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

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 $h(F'/F, \mathcal{O}_{F'}^{\times}) = n^r/n^{r+1} = 1/n$, 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 $\mathbf{F}_p$-vector spaces. Thus, $h(F'/F, \mathcal{O}_{F'}^{\times}) = p$ implies that $\dim_{\mathbf{F}_p}\big(H^1(F'/F, \mathcal{O}_{F'}^{\times})\big)$ is bounded above by $\dim_{\mathbf{F}_p}\big(H^2(F'/F, \mathcal{O}_{F'}^{\times})\big) + 1$, which in turn is bounded above by $s + 1$. ■

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 $c^p = 1_{Cl_F}$, 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:

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

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 $\dim_{\mathbf{F}_p}\big(\ker(J_{F'/F})\big)$ 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_∞ infinite primes of F are ramified in F'/F. In lemma 1.2.5, one then has $V \cong W_o^r \times W_1^{r+1-t_\infty}$ 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,

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

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 $\dim_{\mathbf{F}_p}\big(H^1(F'/F, \mathcal{O}_{F'}^{\times})\big) \leq 1$.

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

$$A_F \overset{J_{F'/F}}{\longrightarrow} A_{F'} \overset{N_{F'/F}}{\longrightarrow} A_F$$

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 $\mathbf{Z}[G]$-module $A_{F'}$ isomorphic to A_F. More precisely, we have

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

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

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

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 σ be a generator of $G = \mathrm{Gal}(F'/F)$. According to (6) in the proof of proposition 1.1.4, if we regard $\tau = \sigma - 1$ as an endomorphism of $A_{F'}$, then $\mathrm{coker}(\tau) \cong A_F$. Now $\ker(\tau) = A_{F'}^G$ has the same order as $\mathrm{coker}(\tau)$. 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

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

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 $Cl_{F'}^G$ 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: $p \mid h_{F'} \Rightarrow p \mid h_F$. For if $p \mid h_{F'}$, then $A_{F'}^G$ 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 $A_{F'}^G = J_{F'/F}(A_F)$ 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

$$A_{F'}^G[p] \;\subseteq\; \ker\big(N_G\big|_{A_{F'}}\big)$$

and, since $p|h_F$, it is clear that $A_{F'}^G[p] \neq 1$. Hence the map $N_G\big|_{A_{F'}}$ 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, $A_{F'} \cong \mathbf{Z}/p^m\mathbf{Z}$. 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 $\dim_{\mathbf{F}_p}(A_{F'}) \geq p$. To see this, we will use some elementary facts about the group ring $\mathbf{F}_p[G]$, where G is a cyclic group of order p. As before, we let $\tau = \sigma - 1$, where σ is a generator of G. The ideal (τ) of $\mathbf{F}_p[G]$ is maximal with residue field F_p. We have $\tau^p = 0$. The distinct proper ideals of $\mathbf{F}_p[G]$ are (τ^i), where $1 \leq i \leq p$. It follows that

$$(\tau^{p-1}) \;=\; \mathbf{F}_p[G]^G \;=\; (N_G), \quad \textit{where} \;\; N_G = \sum_{g \in G} g$$

Thus, if M is an $\mathbf{F}_p[G]$-module such that $\dim_{\mathbf{F}_p}(M) = i < p$, then τ^i annihilates M and hence so does N_G. Thus, if $N_G(M) \neq 0$, then $\dim_{\mathbf{F}_p}(M) \geq p$. 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 $F = \mathbf{Q}(\mu_p)$ 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 $F/\mathbf{Q}$. Let P denote the unique prime ideal of F lying over p.

Example 1. Consider $F' = F(\sqrt[p]{p})$, 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 $N_{F'/F} : A_{F'} \to A_F$, 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 $c \in Cl_F$ has order p. Then $I^p = (\alpha)$, where $\alpha \in F^\times$. Now we let $F' = F(\sqrt[p]{\alpha})$. Let $I' = \mathcal{J}_{F'/F}(I)$. Then $I' = \sqrt[p]{\alpha}\mathcal{O}_{F'}$ 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 $\eta \in \mathcal{O}_F^\times$. 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 $\mathbf{Q}$. Of course, it is easy to verify that L is Galois over $\mathbf{Q}$. As we will then see, the Galois groups $\mathrm{Gal}(F'/\mathbf{Q})$ and $\mathrm{Gal}(L/\mathbf{Q})$ 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 $\mathbf{Q}$ 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 $\mathbf{Q}$. For example, let $m \geq 3$ and let ζ_m denote a primitive m-th root of unity. Then $F = \mathbf{Q}(\zeta_m)$ is a CM-field and $F_+ = \mathbf{Q}(\zeta_m + \zeta_m^{-1})$ 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 $\mathbf{Z}$ or an order in an imaginary quadratic field. In the latter case, we say that E has complex multiplication.

Let $\Delta = \mathrm{Gal}(F/F_+)$, a group of order 2. Thus, $\Delta = \{1, \delta\}$, where δ denotes complex conjugation. (To be more precise, δ is the automorphism of F obtained by choosing any embedding $F \to \mathbf{C}$ and restricting complex conjugation to the image of F.) The group Δ has two characters: the trivial character ϵ_0, and the nontrivial character ϵ_1. Let ϵ denote either of these two characters. Suppose that A is an abelian group and that Δ acts on

A. We let $A^{(\epsilon)}$ denote the maximal subgroup of A on which Δ acts by the character ϵ. 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 $F' = FF'_+$. Thus $\mathrm{Gal}(F'/F'_+)$ can be identified with $\Delta = \mathrm{Gal}(F/F_+)$ and then we have

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

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

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

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

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

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

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

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 Δ acts on $A/A^{(\epsilon)}$ by the character ϵ'. Therefore, Δ acts on the kernel and cokernel of (11) by both ϵ and ϵ' 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, $G = \mathrm{Gal}(F'/F)$ has odd order. Note that

$$(\mathcal{O}_{F'}^\times)^{(\epsilon_1)} = \ker(\mathcal{N}_{F'/F'_+} : \mathcal{O}_{F'}^\times \to \mathcal{O}_F^\times) = \mu_{F'}$$

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 $\ker(J_{F'/F}) \subset A_F^{(\epsilon_0)}$ 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 μ_p or (ii) $F' = F(\mu_{p^m})$ for some integer m. Then the map*

$$A_F^{(\epsilon_1)} \to A_{F'}^{(\epsilon_1)}$$

induced by $J_{F'/F}$ is injective. Thus, $\ker(J_{F'/F}) \subseteq A_F^{(\epsilon_0)}$.

Note that $A_F^{(\epsilon_0)} \cong A_{F_+}$ and that the final conclusion in the proposition implies that $\ker(J_{F'/F}) \cong \ker(J_{F'_+/F_+})$.

Proof. First note that the both the map $\ker(J_{F'/F}) \to \mathcal{P}_{F'}^G/\mathcal{P}_F$ and the isomorphism $\mathcal{P}_{F'}^G/\mathcal{P}_F \cong H^1(F'/F, \mathcal{O}_{F'}^\times)$ are Δ-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 μ_{p^m}. 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 $|A| = p^m$. We can identify A with $\mathbf{Z}/p^m\mathbf{Z}$ and $\mathrm{Aut}(A)$ with $(\mathbf{Z}/p^m\mathbf{Z})^\times$, which we regard as a quotient group of $\mathbf{Z}_p^\times$. That is, any automorphism of A can be realized as multiplication by a p-adic unit. Let σ be a generator of G. Suppose that σ acts on A as multiplication by $s \in \mathbf{Z}_p^\times$. Note that $s \equiv 1 \pmod{p\mathbf{Z}_p}$ if p is odd and $s^2 \equiv 1 \pmod{8\mathbf{Z}_2}$ 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 $1 + x + ... + x^{p^n-1}$. If τ denotes the endomorphism of A defined by $\sigma - 1$, then τ acts on A as multiplication by $s - 1$.

Let $a = \mathrm{ord}_p\big(\Phi(s)\big)$ and $b = \mathrm{ord}_p(s-1)$, where ord_p denotes the p-adic valuation, normalized so that $\mathrm{ord}_p(p) = 1$. 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 $\ker(N_G) = \mathrm{im}(\tau)$ 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

$$\mathrm{ord}_p(s^{p^n} - 1) = m$$

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

$$\mathrm{ord}_p(s^{p^n} - 1) \geq m, \qquad \mathrm{ord}_p(s^{p^{n-1}} - 1) < m$$

But one sees easily that $\mathrm{ord}_p(s^{p^n} - 1) = \mathrm{ord}_p(s^{p^{n-1}} - 1) + 1$ for $n \geq 1$ if p is odd and for $n \geq 2$ if $p = 2$. It follows that $\mathrm{ord}_p(s^{p^n} - 1) = m$ ∎

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 $A_F^{(\epsilon_1)} \to A_{F'}^{(\epsilon_1)}$ is of exponent 2. Thus, Δ acts on that kernel by ϵ_0 too.

1.3 Genus theory

Let F'/F be an arbitrary cyclic extension and let σ be a generator of $G = \mathrm{Gal}(F'/F)$. The group $Cl_{F'}/Cl_{F'}^{\sigma-1}$ is sometimes called the "genus group" for F'/F (or the group of *"genera"*). We will denote it by $\mathcal{G}_{F'/F}$. The proof of proposition 1.1.3 shows that $\mathcal{G}_{F'/F} \cong \mathrm{Gal}(K/F')$, 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 $\mathcal{G}_{F'/F} \cong Cl_F$. In general, the norm map induces a homomorphism $\mathcal{G}_{F'/F} \longrightarrow Cl_F$. We denote its kernel by $\mathcal{G}^{(o)}_{F'/F}$. Under the assumption that there exists at least one totally ramified prime for F'/F, we have an exact sequence

$$1 \longrightarrow \mathcal{G}^{(o)}_{F'/F} \longrightarrow \mathcal{G}_{F'/F} \longrightarrow Cl_F \longrightarrow 1$$

Furthermore, one sees easily that every element of $\mathcal{G}^{(o)}_{F'/F}$ has order dividing $[F' : F]$. Hence if F'/F is a p-extension, then $\mathcal{G}^{(o)}_{F'/F}$ 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 $\mathbf{Q}$ and σ is the nontrivial automorphism of F', then one sees easily that $\sigma(c) = c^{-1}$ for $c \in Cl_{F'}$. Thus, $\mathcal{G}_{F'/\mathbf{Q}} = Cl_{F'}/Cl^2_{F'}$. Its structure is described in the following proposition.

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

1. *If F' is an imaginary quadratic field, then $\mathcal{G}_{F'/\mathbf{Q}} \cong (\mathbf{Z}/2\mathbf{Z})^{t-1}$.*
2. *Suppose that F' is a real quadratic field.*
   If $-1 \in \mathcal{N}_{F'/\mathbf{Q}}(F'^{\times})$, then $\mathcal{G}_{F'/\mathbf{Q}} \cong (\mathbf{Z}/2\mathbf{Z})^{t-1}$.
   If $-1 \notin \mathcal{N}_{F'/\mathbf{Q}}(F'^{\times})$, then $\mathcal{G}_{F'/\mathbf{Q}} \cong (\mathbf{Z}/2\mathbf{Z})^{t-2}$.

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 $-1 \in \mathcal{N}_{F'/\mathbf{Q}}(F'^{\times})$ *if and only if every odd prime ℓ ramified in $F'/\mathbf{Q}$ 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 α 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 $-1 \in \mathcal{N}_{F'/\mathbf{Q}}(\mathcal{O}_{F'}^{\times})$ (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 $\dim_{\mathbf{F}_2}\left(H^1(F'/F, \mathcal{O}_{F'}^{\times})\right) \leq 1$. Proposition 1.2.4 implies that $H^1(F'/F, \mathcal{O}_{F'}^{\times}) \cong \mathbf{Z}/2\mathbf{Z}$ 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 $\mathbf{Q}$ 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 $\mathbf{Q}$ of degree p, where p is an odd prime. Let t denote the number of primes which are ramified in $F'/\mathbf{Q}$. Then*

$$\mathcal{G}_{F'/\mathbf{Q}} \cong (\mathbf{Z}/p\mathbf{Z})^{t-1}$$

Proof. Let K be the genus field for $F'/\mathbf{Q}$. Suppose that $\ell_1, ..., \ell_t$ are the primes which are ramified in $F'/\mathbf{Q}$. If ℓ is any one of these primes, let I_ℓ denote the corresponding inertia subgroup of $\mathrm{Gal}(K/\mathbf{Q})$. It is clear that $I_\ell \cap \mathrm{Gal}(K/F') = 1$ and hence that I_ℓ must be cyclic of order p. It is also clear that $\mathrm{Gal}(K/\mathbf{Q})$ is generated by $I_{\ell_1}, ..., I_{\ell_t}$. This implies that $\mathrm{Gal}(K/F') \cong (\mathbf{Z}/p\mathbf{Z})^u$ 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 ℓ is any one of the primes ramified in $F'/\mathbf{Q}$, then either $\ell = p$ or $\ell \equiv 1 \pmod{p}$. In both cases, there is a unique cyclic extension of $\mathbf{Q}$ of degree p in which only the prime ℓ is ramified: a subfield of $\mathbf{Q}(\mu_{p^2})$ if $\ell = p$, a subfield of $\mathbf{Q}(\mu_\ell)$ if $\ell \equiv 1 \pmod{p}$. For each ℓ_i, $1 \leq i \leq t$, let K_i denote the field just described.

The Kronecker-Weber theorem (which states that every finite abelian extension of $\mathbf{Q}$ is contained $\mathbf{Q}(\mu_m)$ for some m) implies that $F' \subset K_1...K_t$. Note also that the inertia subgroup I_i of $\mathrm{Gal}(K_1...K_t/\mathbf{Q})$ for any one of the ℓ_i's is of order p and that $I_i \cap \mathrm{Gal}(K_1...K_t/F')$ is trivial. This implies that $K_1...K_t \subset K$. But it is easy to see that $\mathrm{Gal}(K_1...K_t/F') \cong (\mathbf{Z}/p\mathbf{Z})^{t-1}$. 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 $Cl_{F'}$ 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 λ_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 $Cl_{F'}^G$ and is isomorphic to $(\mathbf{Z}/p\mathbf{Z})^{t-1}$. 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 $Cl_{F'}$, where σ is a generator of $\mathrm{Gal}(F'/\mathbf{Q})$. Then $\ker(\tau) = Cl_{F'}^G$ and $\mathrm{coker}(\tau) = \mathcal{G}_{F'/\mathbf{Q}}$ have the same order. Since τ annihilates $\mathcal{G}_{F'/\mathbf{Q}}$, N_G acts on that group simply as multiplication by p. But N_G also annihilates $\mathcal{G}_{F'/\mathbf{Q}}$ and so that group is an elementary abelian p-groups and therefore is indeed isomorphic to $(\mathbf{Z}/p\mathbf{Z})^{t-1}$.

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 $\mathcal{G}_{F'/F} = (Cl_{F'})_G$ has the same order as $(Cl_{F'})^G = Cl_{F'}^G$, the subgroup of G-invariant ideal classes. One obtains information about $Cl_{F'}$ 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 $Cl_{F'}^G$. To be more precise, we will study the possibly smaller subgroup $Cl_{F'}^{[G]}$ consisting of ideal classes which contain a G-invariant ideal. Obviously, we have

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

and so $Cl_{F'}^G / Cl_{F'}^{[G]} \cong \mathrm{coker}\big(\mathcal{F}_{F'}^G \to Cl_{F'}^G\big)$, 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*

$$\mathrm{coker}\big(\mathcal{F}_{F'}^G \to Cl_{F'}^G\big) \cong \big(\mathcal{O}_F^\times \cap \mathcal{N}_{F'/F}(F'^\times)\big)/\mathcal{N}_{F'/F}(\mathcal{O}_{F'}^\times)$$

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

Proof. Consider the exact sequence

$$1 \to \mathcal{P}_{F'} \to \mathcal{F}_{F'} \to Cl_{F'} \to 1$$

This induces the following exact sequence of cohomology groups

$$\mathcal{F}_{F'}^G \to Cl_{F'}^G \to H^1(F'/F, \mathcal{P}_{F'}) \to H^1(F'/F, \mathcal{F}_{F'})$$

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 $\mathcal{F}_{F',P} \cong \mathrm{Ind}_D^G(\mathbf{Z})$, where D is the decomposition subgroup of G for any one of the prime ideals of F' lying above P and $\mathbf{Z}$ is given a trivial action of D. Then by Shapiro's lemma, one has

$$H^1(F'/F, \mathcal{F}_{F',P}) \cong H^1(D, \mathbf{Z}) = \mathrm{Hom}(D, \mathbf{Z}) = 0$$

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

Therefore, $\mathrm{coker}(\mathcal{F}_{F'}^G \to Cl_{F'}^G) \cong H^1(F'/F, \mathcal{P}_{F'})$. Using the injectivity of the map $\mathcal{J}_{F'/F} : \mathcal{P}_F \to \mathcal{P}_{F'}$ and the assumption that G is cyclic, generated by σ, 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

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

and

$$\mathcal{P}_{F'}^{\sigma-1} = \big\{(\alpha^{\sigma-1}) \;\mid\; \alpha \in F'^\times\big\} = \big\{(\alpha) \in \mathcal{P}_{F'} \;\mid\; \mathcal{N}_{F'/F}(\alpha) \in \mathcal{N}_{F'/F}(\mathcal{O}_{F'}^\times)\big\}$$

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. ■

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 $A_{F'}^G$ 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*

$$t - s - 1 \;\leq\; \dim_{\mathbf{F}_p}\big(\mathcal{G}_{F'/F}^{(o)}\big) \;\leq\; t - u$$

where t is the number of distinct prime ideals of F which are ramified in F'/F, $s = \dim_{\mathbf{F}_p}\big(\mathcal{O}_F^\times/(\mathcal{O}_F^\times)^p\big)$, 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 $\mathbf{F}_p$. 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

$$|Cl_{F'}^{[G]}| = p^{t-1} \cdot |Cl_F| \cdot |H^2(F'/F, \mathcal{O}_{F'}^\times)|^{-1}$$

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

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

Therefore, $|\mathcal{G}_{F'/F}^{(o)}| = p^{t-1-v}$. Since $v \geq 0$, one immediately obtains the upper bound on $\dim_{\mathbf{F}_p}\big(\mathcal{G}_{F'/F}^{(o)}\big)$. 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_∞. One then has to slightly modify the above calculation. If t_∞ 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 $F=\mathbf{Q}$. The facts that $h_{\mathbf{Q}}=1$ and the unit group $\mathbf{Z}^\times$ 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 $\mathbf{Q}$ 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 $Cl_{F'}^G\cong(\mathbf{Z}/p\mathbf{Z})^u$ for some $u\le t$, where t denotes the number of ramified primes in $F'/\mathbf{Q}$. But the classes of these ramified primes are not independent. One obtains essentially one nontrivial relationship because $\mathcal{P}_{F'}^G/\mathcal{P}_{\mathbf{Q}}\cong H^1(F'/F,\mathcal{O}_{F'}^\times)$ 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 $Cl_{F'}^G\cong(\mathbf{Z}/p\mathbf{Z})^{t-1}$. This implies that $\mathcal{G}_{F'/\mathbf{Q}}=Cl_{F'}/Cl_{F'}^{\sigma-1}$ has order equal to p^{t-1}. Now if we regard $Cl_{F'}$ as a $\mathbf{Z}[G]$-module, it is clear that $N_G\in\mathrm{Ann}(Cl_{F'})$. Also, N_G acts as multiplication by p on $\mathcal{G}_{F'/\mathbf{Q}}$. Therefore, $\mathcal{G}_{F'/\mathbf{Q}}$ has exponent p and must be indeed be isomorphic to $(\mathbf{Z}/p\mathbf{Z})^{t-1}$.

We now prove proposition 1.3.1. Assume first that F' is imaginary quadratic. Then $\mathcal{N}_{F'/\mathbf{Q}}(\alpha)>0$ 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 $H^1(F'/F,\mathcal{O}_{F'}^\times)\cong\mathbf{Z}/2\mathbf{Z}$, which is easily verified directly since $\mathcal{O}_{F'}^\times$ is just finite. Hence $Cl_{F'}^G\cong(\mathbf{Z}/2\mathbf{Z})^{t-1}$.

If F' is a real quadratic field and $-1\notin\mathcal{N}_{F'/\mathbf{Q}}(F'^\times)$, then the classes of the ramified primes generate $Cl_{F'}^G$, just as in the case of an imaginary quadratic field. But this time $H^1(F'/F,\mathcal{O}_{F'}^\times)\cong(\mathbf{Z}/2\mathbf{Z})^2$ by proposition 1.2.3. Therefore, there will be two independent relations between those ideal classes, and so $Cl_{F'}^G\cong(\mathbf{Z}/2\mathbf{Z})^{t-2}$. Note that we must have $t\ge2$, as we pointed out earlier.

If $-1\in\mathcal{N}_{F'/\mathbf{Q}}(\mathcal{O}_{F'}^\times)$, then $H^2(F'/F,\mathcal{O}_{F'}^\times)=0$ and the argument is the same as in the case where $F'/\mathbf{Q}$ is cyclic of odd prime degree. But if $-1\in\mathcal{N}_{F'/\mathbf{Q}}(F'^\times)$, but $\notin\mathcal{N}_{F'/\mathbf{Q}}(\mathcal{O}_{F'}^\times)$, then the classes of the ramified primes generate a subgroup of index 2 in $Cl_{F'}^G$. Also, $H^2(F'/F,\mathcal{O}_{F'}^\times)\cong\mathbf{Z}/2\mathbf{Z}$ and

$H^1(F'/F, \mathcal{O}_{F'}^\times) \cong (\mathbf{Z}/2\mathbf{Z})^2$. Thus, this subgroup is isomorphic to $(\mathbf{Z}/2\mathbf{Z})^{t-2}$. It follows that $Cl_{F'}^G \cong (\mathbf{Z}/2\mathbf{Z})^{t-1}$.

In all these cases, $Cl_{F'}^G = Cl_{F'}[2]$ and $\mathcal{G}_{F'/\mathbf{Q}} = Cl_{F'}/Cl_{F'}^2$ 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 ϵ_1 be the nontrivial character of $\Delta = \mathrm{Gal}(F'/F'_+) \cong \mathrm{Gal}(F/F_+)$. Suppose that either (i) F does not contain μ_p or (ii) $F' = F(\mu_{p^m})$ for some integer m. Then*

$$H^2(F'/F, \mathcal{O}_{F'}^\times)^{(\epsilon_1)} \cong H^2(F'/F, \mu_{F'}) = 1$$

and every class in $\left(A_{F'}^{(\epsilon_1)}\right)^G$ 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 Δ-equivariant and hence preserves the ϵ_1-components of the groups in question. In case *(i)*, $H^2(F'/F, \mu_{F'})$ 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^{a_v} denote its ramification index in F'_+/F_+. Then

$$(A_{F'}^{(\epsilon_1)})^G / J_{F'/F}(A_F^{(\epsilon_1)}) \cong \prod_{v \in S} \mathbf{Z}/p^{a_v}\mathbf{Z}$$

In particular, if every prime of F_+ lying in S is totally ramified in F'_+/F_+, then $(A_{F'}^{(\epsilon_1)})^G$ contains a subgroup isomorphic to $(\mathbf{Z}/p^n\mathbf{Z})^{|S|}$.

Proof. We will apply proposition 1.2.3. The homomorphisms and isomorphisms in that proposition are all Δ-equivariant. Since $G = \mathrm{Gal}(F'/F)$ 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 ϵ_1-components of the groups. Note also that since $Cl^G_{F'}/J_{F'/F}(Cl_F)$ is a p-group, it is isomorphic to $A^G_{F'}/J_{F'/F}(A_F)$. The ϵ_1-component of that group is $(A^{(\epsilon_1)}_{F'})^G/J_{F'/F}(A^{(\epsilon_1)}_F)$. Corollary 1.3.6 implies that the map

$$(\mathcal{F}^G_{F'}/\mathcal{F}_F)^{(\epsilon_1)} \longrightarrow (A^{(\epsilon_1)}_{F'})^G/J_{F'/F}(A^{(\epsilon_1)}_F)$$

is surjective. In fact, it is an isomorphism because $H^2(F'/F, \mathcal{O}^\times_{F'})^{(\epsilon_1)} = 1$. 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 Δ. They both have ramification index p^{a_v} in F'/F. Using the final isomorphism in proposition 1.2.3, we obtain

$$(\mathcal{F}^G_{F'}/\mathcal{F}_F)^{(\epsilon_1)} \cong \prod_{v\in S} \mathbf{Z}/p^{a_v}\mathbf{Z}$$

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

1.4 The reflection principle

Let p be a prime. Suppose that F is a number field which contains μ_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 $Cl_F \to \mathrm{Gal}(K/F)$. This arises as the composition of the Artin isomorphism $Cl_F[p^\infty] \to \mathrm{Gal}(L/F)$ with the restriction map $\mathrm{Gal}(L/F) \to \mathrm{Gal}(K/F)$. Thus $\mathrm{Gal}(K/F)$ can be identified with a certain quotient group of $Cl_F[p^\infty]$ 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 Cl_F. Then c has order 1 or p. It is easy to see that the subgroup of 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 $\eta \in \mathcal{O}^\times_F$. 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

$$\kappa_A : \ A/(F^\times)^p \longrightarrow \mathrm{Hom}\big(\mathrm{Gal}(F(\sqrt[p]{A})/F), \mu_p\big) \tag{12}$$

Here we let $F(\sqrt[p]{A})$ denote the extension of F generated by $\{\sqrt[p]{\alpha} \mid \alpha \in A\}$. The map κ_A is easy to define. For each $\alpha \in A$, let $\alpha' \in F(\sqrt[p]{A})$ satisfy $\alpha')^p = \alpha$. Then one defines a cocyle ϕ with values in μ_p by $\phi(g) = g(\alpha')/\alpha'$ for all $g \in \mathrm{Gal}(F(\sqrt[p]{A})/F)$. It is easy to show that the cocyle class $[\phi]$ is determined by the coset of α in $A/(F^\times)^p$. The Kummer isomorphism κ_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 Δ is a group of automorphisms of F and that A is invariant under the action of Δ. The extension $F(\sqrt[p]{A})$ is then a Galois extension of the fixed field F^Δ. It follows that Δ acts (by inner automorphisms) on $\mathrm{Gal}(F(\sqrt[p]{A})/F)$. Now Δ also acts on μ_p which is given by a homomorphism (or character) $\omega : \Delta \to \mathbf{F}_p^\times$. Hence one has a natural action of Δ on $\mathrm{Hom}\big(\mathrm{Gal}(F(\sqrt[p]{A})/F), \mu_p\big)$. One can then verify that the map κ_A is Δ-equivariant. In particular, suppose that $A/(F^\times)^p$ is cyclic. The action of Δ on that group is given by a character $\psi : \Delta \to \mathbf{F}_p^\times$. The action of Δ on $\mathrm{Gal}(F(\sqrt[p]{A})/F)$ 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 $F = \mathbf{Q}(\mu_p)$ and its maximal real subfield F_+. We will denote the class number of F_+ by h_F^+, 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 μ_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 $\Delta = \mathrm{Gal}(F/F_+)$ and let δ denote its nontrivial element. As in section 1.2, we let ϵ_0, ϵ_1 denote the two characters of Δ. In the notation defined above, we have $\epsilon_1 = \omega$. Since p is odd, we have a direct product decomposition

$$Cl_F[p^\infty] = Cl_F[p^\infty]^{(\epsilon_1)} \times Cl_F[p^\infty]^{(\epsilon_0)} \tag{13}$$

Remark 1.2.8 implies that $Cl_F[p^\infty]^{(\epsilon_0)} \cong Cl_{F_+}[p^\infty]$ which has order $h^{(p)}_{F_+}$, 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 $Cl_F[p^\infty]^{(\epsilon_0)} \neq 1 \Longrightarrow Cl_F[p^\infty]^{(\epsilon_1)} \neq 1$.

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, α determines an ideal I satisfying $I^p = (\alpha)$ and the corresponding ideal class $c \in Cl_F[p]$.

Let $\Delta = \mathrm{Gal}(F/F_+)$ and let δ denote its nontrivial element. As in section 1.2, we let ϵ_0, ϵ_1 denote the two characters of Δ. In the notation defined above, we have $\epsilon_1 = \omega$. Taking A to be the subgroup of $F^\times$ generated by α and $(F^\times)^p$, so that $K = F(\sqrt[p]{A})$, note that Δ acts on $\mathrm{Gal}(K/F)$ by ϵ_0. Therefore, by (12), it follows that Δ acts on the cyclic group $A/(F^\times)^p$ by ϵ_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 nake the following observation: For either character ϵ of Δ, the obvious map

$$(\mathcal{O}_F^\times)^{(\epsilon)} \longrightarrow \left(\mathcal{O}_F^\times/(\mathcal{O}_F^\times)^p\right)^{(\epsilon)}$$

is surjective. This is easily verified using the facts that $|\Delta| = 2$ and that p is odd. As a consequence, we see that $\eta = \zeta\xi^p$, where $\xi \in \mathcal{O}_F^\times$ and $\delta(\zeta) = \zeta^{-1}$. This means that $\mathcal{N}_{F/F_+}(\zeta) = 1$ and hence ζ 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 $F(\mu_{p^{k+1}})$, a contradiction to our assumption since K/F is unramified. Thus, $c \neq 1$ and so $Cl_F[p]^{(\epsilon_1)}$ is indeed nontrivial. ∎

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

$$\dim_{\mathbf{F}_p}\bigl(Cl_F[p]^{(\epsilon_0)}\bigr) \leq \dim_{\mathbf{F}_p}\bigl(Cl_F[p]^{(\epsilon_1)}\bigr) \tag{14}$$

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 μ_p and let Δ be a group of automorphisms of F such that $p \nmid |\Delta|$. Let φ be any irreducible character of Δ over $\mathbf{Q}_p$, by which we mean the character of an irreducible representation $\rho : \Delta \to \mathrm{Aut}_{\mathbf{Q}_p}(V_\varphi)$, where V_φ is a finite-dimensional vector space over $\mathbf{Q}_p$. Let $d_\varphi = \dim_{\mathbf{Q}_p}(V_\varphi)$, the degree of the character φ.

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

Let ψ be the character of Δ corresponding to the representation space

$$V_\psi = \mathrm{Hom}(V_\varphi, V_\omega),$$

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

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

$$e_\varphi = \frac{1}{|\Delta|}\sum_{\delta\in\Delta} \varphi(\delta)^{-1}\delta \tag{15}$$

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

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

$$U = \prod_{\varphi\in\mathrm{Irr}_\Delta(\mathbf{Q}_p)} U^{(\varphi)} \tag{16}$$

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

$$U^{(\varphi)} = e_\varphi U = \{a \in U \mid \delta(a) = \varphi(\delta)a \text{ for all } \delta \in \Delta\} \tag{17}$$

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

In particular, suppose that U is an elementary abelian p-group. We can regard U as a representation space for Δ over $\mathbf{F}_p$. Suppose that it is irreducible. Then $U = U^{(\varphi)}$ for a unique $\varphi \in \mathrm{Irr}_\Delta(\mathbf{Q}_p)$. Conversely, if $\varphi \in \mathrm{Irr}_\Delta(\mathbf{Q}_p)$, one can find a $\mathbf{Z}_p$-lattice $T_\varphi \subset V_\varphi$ which is Δ-invariant. Then $U = T_\varphi/pT_\varphi$ is irreducible and satisfies $U = U^{(\varphi)}$. We denote this space by W_φ. One has $\dim_{\mathbf{F}_p}(W_\varphi) = d_\varphi$. It is not hard to see that this construction $V_\varphi \rightsquigarrow W_\varphi$ defines a 1-1 correspondence between the sets of irreducible representations for Δ over $\mathbf{Q}_p$ and over $\mathbf{F}_p$. Also, if V is any finite-dimensional representation space for Δ and T is a Δ-invariant $\mathbf{Z}_p$-lattice in V, then T/pT is isomorphic to a direct sum of the W_φ's, V is isomorphic to a direct sum of the V_φ'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 Δ over $\mathbf{F}_p$ plays a role, specifically the $\mathbf{F}_p$-dimension of the φ-component for an irreducible character φ. As we will discuss later, the multiplicity of W_φ in $\mathcal{O}_F^\times/(\mathcal{O}_F^\times)^p$ can be determined, in principle, and hence so can the dimension of $(\mathcal{O}_F^\times/(\mathcal{O}_F^\times)^p)^{(\varphi)}$.

Proposition 1.4.2. *Suppose that Δ 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 φ is an irreducible character for Δ over $\mathbb{Q}_p$ and that ψ is the ω-dual of φ. Then*

$$\dim_{\mathbf{F}_p}\big(Cl_F[p]^{(\psi)}\big) \le \dim_{\mathbf{F}_p}\big(Cl_F[p]^{(\varphi)}\big) + \dim_{\mathbf{F}_p}\big((\mathcal{O}_F^\times/(\mathcal{O}_F^\times)^p)^{(\varphi)}\big)$$

Proof. Let $E = F^\Delta$. Then $\Delta = \mathrm{Gal}(F/E)$. Consider the ψ-component $Cl_F[p^\infty]^{(\psi)}$ in the Δ-decomposition of $Cl_F[p^\infty]$. The $\mathbf{F}_p$-dimensions of $Cl_F[p]^{(\psi)}$ and $Cl_F[p^\infty]^{(\psi)}/pCl_F[p^\infty]^{(\psi)}$ are equal. Denote this dimension by r_ψ. The Artin map for L/F then determines an extension K_ψ/F such that $K_\psi \subseteq L$, K_ψ/E is a Galois extension, and $\mathrm{Gal}(K_\psi/E) \cong Cl_F[p]^{(\psi)}$ as $\mathbf{F}_p$-representation spaces for Δ. Each is isomorphic to a direct sum of r_ψ/d_ψ copies of W_ψ.

Now $K_\psi = F(\sqrt[p]{A_\varphi})$ for a certain subgroup A_φ of $F^\times$ which contains $(F^\times)^p$ and is Δ-invariant. The $\mathbf{F}_p$-representation space $A_\varphi/(F^\times)^p$ has dimension r_ψ and is a direct sum of r_ψ/d_ψ copies of W_φ. This follows from (12) and is the reason we use the subscript φ. The fact that K_ψ/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

$$A_\varphi/(F^\times)^p \longrightarrow Cl_F[p] \tag{18}$$

which is easily seen to be Δ-equivariant. Thus the image of (18) is a subgroup of $Cl_F[p]^{(\varphi)}$ and hence its $\mathbf{F}_p$-dimension is bounded above by $\dim_{\mathbf{F}_p}\left(Cl_F[p]^{(\varphi)}\right)$.

The kernel of (18) is of the form $B_\varphi/(F^\times)^p$, where B_φ is some subgroup of A_φ. 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

$$\left(\mathcal{O}_F^\times/(\mathcal{O}_F^\times)^p\right)^{(\varphi)} \longrightarrow \left(F^\times/(F^\times)^p\right)^{(\varphi)} \tag{19}$$

and hence $\dim_{\mathbf{F}_p}\left(B_\varphi/(F^\times)^p\right) \leq \dim_{\mathbf{F}_p}\left((\mathcal{O}_F^\times/(\mathcal{O}_F^\times)^p)^{(\varphi)}\right)$. 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 $\left(\mathcal{O}_F^\times/(\mathcal{O}_F^\times)^p\right)^{(\epsilon_1)}$ is cyclic and is generated by the coset of a primitive p^k-th root of unity ζ. However, since $F(\sqrt[p]{\zeta})$ is assumed to be ramified, the image of the coset of ζ under the map (19) isn't contained in A_{ϵ_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*

$$\dim_{\mathbf{F}_3}(Cl_{\mathbf{Q}(\sqrt{d})}[3]) \leq \dim_{\mathbf{F}_3}(Cl_{\mathbf{Q}(\sqrt{-3d})}[3]) \leq \dim_{\mathbf{F}_3}(Cl_{\mathbf{Q}(\sqrt{d})}[3]) + 1$$

Proof. In this case, we consider the biquadratic field $F = \mathbf{Q}(\sqrt{d}, \sqrt{-3d})$, a CM-field with maximal real subfield $F_+ = \mathbf{Q}(\sqrt{d})$. The first inequality follows from proposition 1.4.1. To prove the second inequality, we consider

$\Delta = \mathrm{Gal}(F/\mathbf{Q})$, a group with four characters. The nontrivial characters are ψ, φ, and ω. They factor through the quotient groups of Δ corresponding to the three quadratic fields $E_\psi = \mathbf{Q}(\sqrt{-3d})$, $E_\varphi = F_+$, and $E_\omega = \mathbf{Q}(\mu_3)$, respectively. We denote the trivial character by ϵ_0. Consider the Δ-decomposition of $Cl_F[3^\infty]$:

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

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

$$Cl_F[3^\infty]^{(\psi)} \cong Cl_{F_\psi}[3^\infty], \quad Cl_F[3^\infty]^{(\varphi)} \cong Cl_{F_\varphi}[3^\infty], \quad Cl_F[3^\infty]^{(\omega)} \cong Cl_{F_\omega}[3^\infty].$$

The ω-component is also trivial. Proposition 1.4.3 gives an inequality for the 3-ranks of the other two Δ-components. The unit group $\mathcal{O}_F^\times$ has a very simple structure, namely μ_3 and the fundamental unit of E_φ generate a subgroup of index a power of 2. It follows that $\dim_{\mathbf{F}_3}\big((\mathcal{O}_F^\times/(\mathcal{O}_F^\times)^3)^{(\varphi)}\big) = 1$. One obtains

$$\dim_{\mathbf{F}_3}\big(Cl_F[3]^{(\psi)}\big) \leq \dim_{\mathbf{F}_3}(Cl_F[3]^{(\varphi)}) + 1$$

and the second inequality in the proposition then follows. ■

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

In principle, the isomorphism class of $V_{\mathcal{O}_F^\times}$, and hence the multiplicities of each of the V_φ's in that representation space for Δ, can always be determined. One could take a Galois extension F' of $\mathbf{Q}$ containing F. Then Δ is a subquotient of $\Delta' = \mathrm{Gal}(F'/\mathbf{Q})$ and $V_{\mathcal{O}_F^\times} \cong V_{\mathcal{O}_{F'}^\times}^{\mathrm{Gal}(F'/F)}$ as representation spaces for Δ. The action of Δ on that subspace can be studied in terms of the representation space $V_{\mathcal{O}_{F'}^\times}$ for $\mathrm{Gal}(F'/\mathbf{Q})$. Therefore, it seems sufficient to consider a finite Galois extension of $\mathbf{Q}$ and so we will simply assume that

$F/\mathbf{Q}$ is Galois. The following theorem is rather well-known. After recalling the proof, we will describe how to determined the multiplicity of V_φ in $V_{\mathcal{O}_F^\times}$.

Proposition 1.4.4. *Suppose that F is a finite Galois extension of $\mathbf{Q}$ and let $\Delta = \mathrm{Gal}(F/\mathbf{Q})$. Let v be an infinite prime of F and let Δ_v denote the decomposition subgroup of Δ for v. Suppose that ϵ_0 is the trivial character of Δ_v and φ_0 is the trivial character of G. Let $V_{\mathcal{O}_F^\times} = \mathcal{O}_F^\times \otimes_{\mathbf{Z}} \mathbf{Q}_p$. Then*

$$V_{\mathcal{O}_F^\times} \oplus V_{\varphi_0} \cong \mathrm{Ind}_{\Delta_v}^{\Delta}(\epsilon_0)$$

as representations spaces for Δ.

Proof. The isomorphism will be proved by showing that the two representations of Δ 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 $\mathbf{R}$ or to $\mathbf{C}$. In either case, one defines a log map from $F_v^\times$ onto $\mathbf{R}$. One then identifies $\mathcal{O}_F^\times/\mu_F$ with a $\mathbf{Z}$-lattice in a certain subspace of $\prod_{v|\infty} \mathbf{R}$ of codimension 1. This map is Δ-equivariant. The $\mathbf{R}$-vector space $\prod_{v|\infty} \mathbf{R}$ is just the permutation representation determined by the action of Δ on the set of infinite primes of F. This is isomorphic to $\mathrm{Ind}_{\Delta_v}^{\Delta}(\epsilon_0)$, considered as an $\mathbf{R}$-representation space for Δ. Thus, one has an injective map

$$\mathcal{O}_F^\times \otimes_{\mathbf{Z}} \mathbf{R} \longrightarrow \mathrm{Ind}_{\Delta_v}^{\Delta}(\epsilon_0)$$

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

Obviously $m_{\varphi_0}(V_{\mathcal{O}_F^\times}) = 0$. If $\varphi \neq \varphi_0$, then $m_\varphi(V_{\mathcal{O}_F^\times})$ is just the multiplicity of φ in $\mathrm{Ind}_{\Delta_v}^{\Delta}(\epsilon_0)$. Now $V_\varphi \otimes_{\mathbf{Q}_p} \overline{\mathbf{Q}}_p$ may be reducible, a direct sum of absolutely irreducible representations spaces, each occurring with a certain multiplicity. Suppose that ξ is the character of one of the direct summands, a representation space V_ξ for Δ over $\overline{\mathbf{Q}}_p$, and let s_ξ denote the corresponding multiplicity. The quantity s_ξ is the Schur index for ξ over $\mathbf{Q}_p$ and actually depends only on φ and not on the choice of ξ. All the characters ξ occurring in φ are conjugate over $\mathbf{Q}_p$. If $m_\xi\big(\mathrm{Ind}_{\Delta_v}^{\Delta}(\epsilon_0)\big)$ denotes the multiplicity of V_ξ in $\mathrm{Ind}_{\Delta_v}^{\Delta}(\epsilon_0)$, then $m_\varphi(V_{\mathcal{O}_F^\times}) = m_\xi\big(\mathrm{Ind}_{\Delta_v}^{\Delta}(\epsilon_0)\big)/s_\xi$, assuming that $\varphi \neq \varphi_0$.

One can determine $m_\xi\big(\mathrm{Ind}_{\Delta_v}^{\Delta}(\epsilon_0)\big)$ by using the Frobenius reciprocity law. Let $d_\xi = \dim_{\overline{\mathbf{Q}}_p}(V_\xi)$. Note that Δ_v has order 1 or 2. Let d_ξ^+ and d_ξ^- denote the multiplicities of ϵ_0 and ϵ_1 (if Δ_v has order 2), respectively, when we regard V_ξ as a representation space for Δ_v. Thus, $d_\xi = d_\xi^+ + d_\xi^-$. According to the Frobenius reciprocity law, the multiplicity of ξ in $\mathrm{Ind}_{\Delta_v}^{\Delta}(\epsilon_0)$ coincides with the multiplicity of ϵ_0 in $\xi|_{\Delta_v}$. That is, we have $m_\xi\big(\mathrm{Ind}_{\Delta_v}^{\Delta}(\epsilon_0)\big) = d_\xi^+$.

If F is totally real, then $d_\xi^+ = d_\xi$. If F is a CM-field, then any irreducible character ξ 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 Δ is abelian, and φ is an irreducible character for Δ over $\mathbf{Q}_p$, then each ξ occurring in φ is 1-dimensional and occurs with multiplicity 1. In that case, we have $m(\varphi)(V_{\mathcal{O}_F^\times}) = 1$ or 0, depending on whether φ is even or odd.

We now consider the field $F = \mathbf{Q}(\mu_p)$ and $\Delta = \mathrm{Gal}(F/\mathbf{Q})$. The irreducible characters of Δ over $\mathbf{F}_p$ are the powers ω^i, $0 \le i \le p-2$.

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

$$\dim_{\mathbf{F}_p}\big(Cl_F[p]^{(\omega^j)}\big) \le \dim_{\mathbf{F}_p}\big(Cl_F[p]^{(\omega^i)}\big) \le \dim_{\mathbf{F}_p}\big(Cl_F[p]^{(\omega^j)}\big) + 1.$$

Also, the ω^0 and ω^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, $1 \le i \le p-2$, 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 $\dim_{\mathbf{F}_p}\big(Cl_F[p]^{(\omega^j)}\big) \le \dim_{\mathbf{F}_p}\big(Cl_F[p]^{(\omega^i)}\big)$.

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

We will return frequently to the field $F = \mathbf{Q}(\mu_p)$ 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 Δ-decomposition of $Cl_F[p]$? There is an

important criterion for the nontriviality of the ω^i-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 $F = \mathbf{Q}(\mu_p)$. Then*

$$Cl_F[p]^{(\omega^i)} \neq 1 \iff p|B_j$$

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 $F = \mathbf{Q}(\mu_p)$ 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 $Cl_F[p]^{(\omega^i)} \neq 1$ 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 $p|B_j$ for an even j in the stated range, then $Cl_F[p]^{(\omega^i)} \neq 1$ for $i = p - j$.

As an example, let $p = 37$, the first irregular prime. Then $37|B_{32}$, but $37 \nmid B_j$ for the other even values of j, $2 \leq j \leq 34$. The Herbrand-Ribet theorem then asserts that $Cl_F[37]^{(\omega^5)} \neq 1$ and that the ω^i-component is trivial for the other odd values of i. For an even character ω^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 $p \nmid h_{F_+}$.

In general, it seems reasonable to conjecture that $Cl_F[p^\infty]^{(\omega^i)}$ is a cyclic group, or equivalently, that $\dim_{F_p}\left(Cl_F[p]^{(\omega^i)}\right) = 1$, 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 $F = \mathbf{Q}(\mu_p)$. Then $p \nmid h_{F_+}$.*

This conjecture has been verified for all $p < 16,000,000$. For all of these primes, it turns out that the nontrivial components $Cl_F[p^\infty]^{(\omega^i)}$ 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 $\mathbf{Z}_p[\Delta]$-module. It follows immediately from the above remarks.

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

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 $X = \mathrm{Gal}(M/F)$. Note that the p-Hilbert class field L of F is contained in M. Also, M is obviously a Galois extension of F^Δ and so Δ acts on X. The next result concerns the Δ-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 $\mathcal{O}_F[\frac{1}{p}]$. 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 Δ 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*

$$\dim_{F_p}\big((X/X^p)^{(\psi)}\big) = \dim_{\mathbf{F}_p}\big(A'_F[p]^{(\varphi)}\big) + \dim_{\mathbf{F}_p}\big((\mathcal{O}_{F,S_p}^\times/(\mathcal{O}_{F,S_p}^\times)^p)^{(\varphi)}\big)$$

.

Proof. We first make the following observation. Suppose $\alpha \in \mathbf{F}^\times$. Then $F(\sqrt[p]{\alpha}) \subset M$ if and only if $p|\mathrm{ord}_v(\alpha)$ 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 α'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

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

These isomorphisms are Δ-equivariant.

Now we also have the following exact sequence

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

where the map f is induced by the inclusion $\mathcal{O}^\times_{F,S_p} \to \mathbf{F}^\times$ 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 $g\big(a(F^\times)^p\big) = c$. The fact that g is a well-defined, surjective homomorphism is easily verified. Also, α represents a coset in the kernel of g if and only if $\alpha = \beta^p\eta$, where $\eta \in \mathcal{O}^\times_{F,S_p}$, which proves the exactness.

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

$$(X/X^p)^{(\psi)} \cong Hom(A/(F^\times)^p, \mu_p)^{(\psi)} \cong Hom\big(A/(F^\times)^p)^{(\varphi)}, \mu_p\big)$$

Now $A/(F^\times)^p)^{(\varphi)} \cong \big(\mathcal{O}^\times_{F,S_p}/(\mathcal{O}^\times_{F,S_p})^p\big)^{(\varphi)} \times A'_F[p]^{(\varphi)}$. Proposition 1.4.6 then follows. ■

Returning to the case where $F = \mathbf{Q}(\mu_p)$ and $\Delta = \mathrm{Gal}(F/\mathbf{Q})$, 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*

$$\dim_{\mathbf{F}_p}\big((X/X^p)^{(\omega^j)}\big) = \dim_{\mathbf{F}_p}\big(Cl_F[p]^{(\omega^i)}\big),$$

$$\dim_{\mathbf{F}_p}\big((X/X^p)^{(\omega^i)}\big) = \dim_{\mathbf{F}_p}\big(Cl_F[p]^{(\omega^j)}\big) + 1.$$

Also, $\dim_{\mathbf{F}_p}\big((X/X^p)^{(\omega^1)}\big) = \dim_{\mathbf{F}_p}\big((X/X^p)^{(\omega^0)}\big) = 1.$

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, $\dim_{\mathbf{F}_p}\big((\mathcal{O}^\times_{F,S_p}/(\mathcal{O}^\times_{F,S_p})^p)^{(\varphi)}\big) = 1$ 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 $L/\mathbf{Q}$ is Galois, $\mathrm{Gal}(L/F)$ is cyclic or order p, and $\Delta = \mathrm{Gal}(F/\mathbf{Q})$ acts on $\mathrm{Gal}(L/F)$ by the character ω^i. Now the corresponding j is even and $\omega^j\omega^i = \omega$. The character ω^j is the only nontrivial, even character of Δ for which $(X/pX)^{(\omega^j)}$ is nontrivial. Furthermore, $(X/pX)^{(\omega^j)}$ is cyclic of order p. Thus, there is a unique subfield N of M such that $N/\mathbf{Q}$ is Galois, $\mathrm{Gal}(N/F)$ is cyclic or order p, and $\Delta = \mathrm{Gal}(F/\mathbf{Q})$ acts on $\mathrm{Gal}(N/F)$ by the character ω^j. Also, $N = F(\sqrt[p]{\alpha})$, where α is in the group A defined in the proof of proposition 1.4.7. The coset of α in$A/(F^\times)^p$ is contained in $\left(A/(F^\times)^p\right)^{(\omega^i)}$. It follows that the fractional ideal (α) 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 ω^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 $\mathbf{Z}_p$. 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 $\mathrm{Gal}(H/F)$ is $\mathrm{Hom}(\mathrm{Gal}(H/F), \mathbf{Q}/\mathbf{Z})$. This can be viewed as a subgroup of the Galois cohomology group $H^1(G_F, \mathbf{Q}/\mathbf{Z})$, where we are letting G_F act trivially on $\mathbf{Q}/\mathbf{Z}$. To be precise,

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

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

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

Given such a D, the subgroup $D[p^n]$ (for any $n \geq 0$) is isomorphic to $(\mathbf{Z}/p^n\mathbf{Z})^d$ as a group and has a certain action of G_F. That action corresponds to a homomorphism $G_F \longrightarrow GL_d(\mathbf{Z}/p^n\mathbf{Z})$. 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:

$$T = \varprojlim_n D[p^n]$$

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

If we start instead with such a finite-dimensional $\mathbf{Q}_p$-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 $\mathbf{Z}_p$-module T of rank $d = \dim_{\mathbf{Q}_p}(V)$ 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 $\rho : G_F \longrightarrow GL_d(R)$. 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 ρ"*. For example, if ρ_D is as described

above, then we can take $R = \mathbf{Z}_p$. We denote the extension cut out by ρ_D by $F(D)$. Thus, $\mathrm{Gal}(F(D)/F)$ is isomorphic to a subgroup of $GL_d(\mathbf{Z}_p)$, namely $\mathrm{im}(\rho_D)$. Now ρ_D is a continuous map, $\mathrm{Gal}(F(D)/F)$ is compact, and hence $\mathrm{im}(\rho_D)$ is a closed subgroup of $GL_d(\mathbf{Z}_p)$. 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 represention of G_F on $D[p^n]$, where we take $R = \mathbf{Z}/p^n\mathbf{Z}$. This is the reduction modulo p^n of ρ_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 $Ram(D)$ 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 $v \in Ram(D)$ 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 $Ram(D)$ 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 $H^1_{unr}(F, D)$. 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 $I_{F_v} = \mathrm{Gal}(\overline{F}_v/F_v^{unr})$, where F_v^{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

$$H^1(F, *),\ H^1(F_v, *),\quad \textit{and}\quad H^1(F_v^{unr}, *)$$

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

$$H^1_{unr}(F, D) = \ker\big(H^1(F, D) \longrightarrow \prod_v H^1(F_v^{unr}, D)\big).$$

where v runs over all the primes of F in the product. That is, if $\phi : G_F \longrightarrow D$ is a 1-cocycle, then its class $[\phi]$ is in $H^1_{unr}(F, D)$ 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 $H^1_{unr}(F, D)$.

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

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

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

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

$$\ker\big(H^i(F, D[p^n]) \longrightarrow H^i(F, D)\big) \cong H^{i-1}(F, D)/p^n H^{i-1}(F, D) \tag{20}$$

If we take $i = 1$, then $H^0(F, D) = D^{G_F}$ is a $\mathbf{Z}_p$-submodule of D. The Pontryagin dual $\widehat{D}$ of D is isomorphic to $\mathbf{Z}_p^d$; the Pontryagin dual of D^{G_F} is a quotient of $\widehat{D}$. Hence it follows that $H^0(F, D) \cong (\mathbf{Q}_p/\mathbf{Z}_p)^e \times C$, where C is finite and $0 \leq e \leq d$. The subgroup $(\mathbf{Q}_p/\mathbf{Z}_p)^e$ 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

$$H^1(F, D[p^n]) \longrightarrow H^1(F, D)[p^n] \tag{21}$$

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

$$H^1_{unr}(F, D[p^n]) \longrightarrow H^1_{unr}(F, D)[p^n] \tag{22}$$

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

$$H^1(F, D[p^n]) \longrightarrow \prod_v H^1(F_v^{unr}, D[p^n]), \qquad H^1(F, D) \longrightarrow \prod_v H^1(F_v^{unr}, D)$$

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 $D[p^n] \subset D$.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^1_{unr}(F, D[p^n]) & \longrightarrow & H^1(F, D[p^n]) & \longrightarrow & G^1(F, D[p^n]) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \alpha_n} & & \downarrow{\scriptstyle \beta_n} & & \downarrow{\scriptstyle \gamma_n} & & \\ 0 & \longrightarrow & H^1_{unr}(F, D)[p^n] & \longrightarrow & H^1(F, D)[p^n] & \longrightarrow & G^1(F, D)[p^n] & & \end{array} \tag{23}$$

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 $\mathrm{coker}(\alpha_n)$, we apply the snake lemma, obtaining the following useful exact sequence.

$$\ker(\gamma_n) \longrightarrow \mathrm{coker}(\alpha_n) \longrightarrow \mathrm{coker}(\beta_n) \tag{24}$$

But $\mathrm{coker}(\beta_n) = 0$, as pointed out in part 1. We can study $\ker(\gamma_n)$ factor-by-factor on the entire direct products (over v) which contain $G^1(F, D[p^n])$ and $G^1(F, D)$.

Suppose that v is any prime of F. Consider the map

$$\gamma_{n,v} : \ H^1(F_v^{unr}, D[p^n]) \longrightarrow H^1(F_v^{unr}, D)$$

An identical argument to the one for (21), applied to F_v^{unr} instead of F, shows that

$$|\ker(\gamma_{n,v})| \ \leq \ [H^0(F_v^{unr}, D) : H^0(F_v^{unr}, D)_{div}]$$

and hence is finite and bounded. Also, if $v \notin Ram(D)$, then I_{F_v} acts trivially on D, $H^0(F_v^{unr}, D) = D$, a divisible group, and hence the index is then 1. That is, $|\ker(\gamma_{n,v})| = 1$ if $v \notin Ram(D)$. 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 $\mathrm{coker}(\alpha_n)$ is finite and has bounded order.

Finiteness of $H^1_{unr}(F, D[p])$. To finish the proof, we will take $n = 1$. It obviously now suffices to prove that $H^1_{unr}(F, D[p])$ is finite. Let $F' = F(D[p])$, a finite Galois extension of F. Let $G = \mathrm{Gal}(F'/F)$. 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 $H^1_{unr}(F, D[p])$ under the restriction map is clearly contained in $H^1_{unr}(F', D[p])$. The kernel is finite and therefore it is enough to prove the finiteness of $H^1_{unr}(F', D[p])$. Now $G_{F'}$ acts trivially on $D[p]$. Hence $H^1(F', D[p]) = \mathrm{Hom}(G_{F'}, D[p])$ and

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

where L' is the p-Hilbert class field of F'. The finiteness of $H^1_{unr}(F, D[p])$ follows from the fact that $\mathrm{Gal}(L'/F') \cong Cl_{F'}[p^\infty]$, 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 $H^1_{unr}(F, D)$ is a cofinitely generated $\mathbf{Z}_p$-module. Consequently, $H^1_{unr}(F, D)_{div} \cong (\mathbf{Q}_p/\mathbf{Z}_p)^r$ for some $r \geq 0$ and $H^1_{unr}(F, D)/H^1_{unr}(F, D)_{div}$ 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 $\mathbf{Z}_p$-module. Consider its Pontryagin dual $X = \mathrm{Hom}\big(H^1_{unr}(F, D), \mathbf{Q}_p/\mathbf{Z}_p\big)$. We must show that X is a finitely generated $\mathbf{Z}_p$-module. This implies that $X \cong \mathbf{Z}_p^r \oplus X_{tors}$ and that X_{tors} 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 $\mathbf{Z}_p$-module and hence will be a compact $\mathbf{Z}_p$-module. The following lemma then completes the proof.

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

Proof. One direction is obvious. For the other direction, where we assume that $\widetilde{x}_1, \ldots, \widetilde{x}_d$ generate X/pX, one can give a quick proof that $x_1, \ldots, x_d$ generate X by using the compactness of $\mathbf{Z}_p$. 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 $X_n = X/p^n X$. 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. finite. The maps $\pi_n : X \to X_n$ are surjective. Hence the induced maps $X/pX \to X_n/pX_n$ are also surjective. It follows from the finite case that the images of $x_1, \ldots, x_d$ under the map π_n must generate X_n. Let Y be the $\mathbf{Z}_p$-submodule submodule of X generated by $x_1, \ldots, x_d$. Since Y is the image of $\mathbf{Z}_p^d$ 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 $H^1_{unr}(F, D[p^n]) \longrightarrow H^1_{unr}(F, D)[p^n]$ 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 $D^{I_{F_v}}$ be divisible for all primes v. For then, $\ker(\gamma_{n,v}) = 0$ for all such v and therefore $\ker(\gamma_n) = 0$. Now if $v \notin Ram(D)$, then $D^{I_{F_v}} = D$ which is a divisible group. However, it could easily happen that $D^{I_{F_v}}$ fails to be divisible for some $v \in Ram(D)$. 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

$$H^1_{U-unr}(F, D) = \ker\big(H^1(F, D) \longrightarrow \prod_{v \in U} H^1(F_v^{unr}, D)\big).$$

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

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

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

Here is an important special case. Suppose that S contains $Ram(D)$. 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 $\mathrm{Gal}(F_S/F)$. 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 $\phi \in H^1_{U-unr}(F, D)$, 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

$$H^1_{U-unr}(F, D) = \ker\big(H^1(F, D) \longrightarrow H^1(F_S, D)\big) \cong H^1(F_S/F, D),$$

the last isomorphism following from the inflation-restriction sequence. Consequently, it follows that $H^1(F_S/F, D)$ is a cofinitely generated $\mathbf{Z}_p$-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 $\mathbf{Q}_p$-vector space of common dimension d, *(ii)* the action of G_F on V_p factors through $\mathrm{Gal}(F_{S \cup S_p}/F)$, 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 $\mathbf{Q}$ and is independent of the choice of p. For each prime p, choose a Galois-invariant $\mathbf{Z}_p$-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 $(\mathbf{Q}/\mathbf{Z})^d$ 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*

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

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 $\mathbf{Z}[G]$-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

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

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

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

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

$$H^i(G, C) \longrightarrow H^i(G, nC) \longrightarrow H^i(G, C)$$

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:

$$0 \to H^1(F'/F, D(F')) \longrightarrow H^1(F,D) \longrightarrow H^1(F',D)^G \longrightarrow H^2(F'/F, D(F'))$$

where we let $D(F') = D^{G_{F'}} = H^0(F',D)$. Any subgroup C of D is a cofinitely generated $\mathbf{Z}_p$-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

$$\begin{array}{ccccccccc} 0 & \longrightarrow & H^1_{unr}(F,D) & \longrightarrow & H^1(F,D) & \longrightarrow & G^1(F,D) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle a_{F'/F}} & & \downarrow{\scriptstyle b_{F'/F}} & & \downarrow{\scriptstyle c_{F'/F}} & & \\ 0 & \longrightarrow & H^1_{unr}(F',D)^G & \longrightarrow & H^1(F',D)^G & \longrightarrow & G^1(F',D)^G & & \end{array} \tag{25}$$

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

$$\ker(c_{F'/F}) \longrightarrow \operatorname{coker}(a_{F'/F}) \longrightarrow \operatorname{coker}(b_{F'/F}) \tag{26}$$

Now $\operatorname{coker}(b_{F'/F})$ is finite and is trivial if $p \nmid n$. To prove the finiteness, or triviality, of $\operatorname{coker}(a_{F'/F})$, 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

$$c_{v'/v} : \ H^1(I_{F_v}, D) \longrightarrow H^1(I_{F_{v'}}, D) \tag{27}$$

The kernel is $H^1(I_{v'/v}, D^{I_{v'}})$, where $I_{v'/v} = I_{F_v}/I_{F_{v'}}$, 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 $I_{v'} = I_{F_v}$ 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 Δ 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 $\mathbf{Z}_p$-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 ρ_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

$$H^1_{unr}(F', D) = \mathrm{Hom}(\mathrm{Gal}(L'/F'), D)$$

where L' is the p-Hilbert class field of F'. This group is obviously finite. ■

Returning to the trivial Galois module $D = \mathbf{Q}_p/\mathbf{Z}_p$, 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 $R_{F'/F} : \mathrm{Gal}(L'/F') \to \mathrm{Gal}(L/F)$ which, in turn, is equivalent to the injectivity of the map

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

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

$$H^1_{unr}(F', \mathbf{Q}_p/\mathbf{Z}_p)^G \cong \mathrm{Hom}_G(A_{F'}, \mathbf{Q}_p/\mathbf{Z}_p) \cong \mathrm{Hom}((A_{F'})_G, \mathbf{Q}_p/\mathbf{Z}_p)$$

If F'/F is cyclic, then $(A_{F'})_G$ is the genus group $\mathcal{G}_{F'/F}$ and so we have

$$\widehat{\mathcal{G}_{F'/F}} \;\cong\; H^1_{unr}(F', \mathbf{Q}_p/\mathbf{Z}_p)^G.$$

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

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

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

$$\widehat{\mathcal{G}^{(o)}_{F'/F}} \;\cong\; \mathrm{coker}\big(H^1_{unr}(F, \mathbf{Q}_p/\mathbf{Z}_p) \longrightarrow H^1_{unr}(F', \mathbf{Q}_p/\mathbf{Z}_p)^G\big).$$

In general, one can study $\mathrm{coker}\big(H^1_{unr}(F, D) \longrightarrow H^1_{unr}(F', D)^G\big)$ 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 Δ of automorphisms of F and that the order of Δ is prime to p. Let $E = F^\Delta$. Suppose that φ is an irreducible character of Δ over $\mathbf{Q}_p$. Thus, V_φ is an Artin representation space for G_E and the action of G_E factors through $\mathrm{Gal}(F/E)$. We denote the corresponding D by D_φ. We then have the following result.

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

$$H^1_{unr}(E, D_\varphi) \cong \mathrm{Hom}_\Delta(Cl_F[p^\infty]^{(\varphi)}, D_\varphi)$$

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

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

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

We also have a canonical isomorphism

$$\mathrm{Art}_{L/F} : Cl[p^\infty] \to \mathrm{Gal}(L/F)$$

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

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

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

In the special case where φ is 1-dimensional, we have

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

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

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

$$H^1_{triv}(F, D) = \ker\big(H^1(F, D) \to \prod_v H^1(F_v, D)\big)$$

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

We will now give an example from the theory of elliptic curves to illustrate the possibility that $H^1_{triv}(F, D)$ can be infinite. Of course, it would then follow that $H^1_{unr}(F, D)$ 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 $E(\overline{\mathbf{Q}})$ of order dividing p^n. As a group, $E[p^n] \cong (\mathbf{Z}/p^n\mathbf{Z})^2$ and there is a natural action of G_F on this group. We will consider

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

which is the p-primary subgroup of $E(\overline{\mathbf{Q}})$.

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

$$\kappa : E(F) \otimes_{\mathbf{Z}} (\mathbf{Q}_p/\mathbf{Z}_p) \to H^1(G_F, E[p^\infty])$$

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

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

$$\kappa_v : E(F_v) \otimes_{\mathbf{Z}} (\mathbf{Q}_p/\mathbf{Z}_p) \to H^1(F_v, E[p^\infty])$$

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

$$\begin{array}{ccc} E(F) \otimes_{\mathbf{Z}} (\mathbf{Q}_p/\mathbf{Z}_p) & \longrightarrow & E(F_v) \otimes_{\mathbf{Z}} (\mathbf{Q}_p/\mathbf{Z}_p) \\ \downarrow \kappa & & \downarrow \kappa_v \\ H^1(F, E[p^\infty]) & \longrightarrow & H^1(F_v, E[p^\infty]) \end{array} \tag{28}$$

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 $G_{F_v} \to G_F$ (corresponding to a fixed embedding $\overline{F} \hookrightarrow \overline{F}_v$.

Now it turns out that $E(F_v) \otimes_{\mathbf{Z}} (\mathbf{Q}_p/\mathbf{Z}_p) = 0$ if $v \nmid p$. This is a consequence of the following fact:

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

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

$$E(F_v) \otimes_{\mathbf{Z}} (\mathbf{Q}_p/\mathbf{Z}_p) \cong (\mathbf{Q}_p/\mathbf{Z}_p)^{[F_v:\mathbf{Q}_p]}$$

if $v \mid p$. It is then clear from diagram (28) that the kernel of the map

$$E(F) \otimes_{\mathbf{Z}} (\mathbf{Q}_p/\mathbf{Z}_p) \longrightarrow \prod_{v|p} E(F_v) \otimes_{\mathbf{Z}} (\mathbf{Q}_p/\mathbf{Z}_p)$$

is a subgroup of $H^1_{triv}(\mathbf{Q}, E[p^\infty])$. But this kernel is obviously infinite if

$$r \;>\; \sum_{v|p} [F_v : \mathbf{Q}_p] \;=\; [F : \mathbf{Q}].$$

This can certainly happen. For example, one could take $F = \mathbf{Q}$ and E to be an elliptic curve whose Mordell-Weil group has rank ≥ 2. If r is that rank, then $H^1_{triv}(\mathbf{Q}, E[p^\infty])$ contains a subgroup isomorphic to $(\mathbf{Q}_p/\mathbf{Z}_p)^{r-1}$.

This is an example that we alluded to at the end of remark 1.5.6. We can associate a compatible system $\mathcal{V}$ of p-adic representations with E by defining $V_p(E) = T_p(E) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$, 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 $\mathcal{D}_\mathcal{V} \cong E(\overline{\mathbf{Q}})_{tors}$. The above discussion shows that $H^1_{unr}(F, \mathcal{D}_\mathcal{V})$ contains a subgroup isomorphic to $(\mathbf{Q}/\mathbf{Z})^{r-1}$.

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 $\overline{\mathbf{Q}}$. The extension $F(\mu_{p^\infty})/F$ is an infinite Galois extension and one can define a continuous homomorphism

$$\chi : \mathrm{Gal}(F(\mu_{p^\infty})/F) \to \mathbf{Z}_p^\times$$

in the following way. Let $g \in \mathrm{Gal}(F(\mu_{p^\infty})/F)$. 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 χ are easily verified. One refers to χ as the "p-power cyclotomic character," regarding it often as a character of G_F which factors through the quotient group $\mathrm{Gal}(F(\mu_{p^\infty})/F)$.

The character χ gives the action of G_F on $T = \varprojlim \mu_{p^n}$, which is a free $\mathbf{Z}_p$-module of rank 1. The G_F-module T with this action is often denoted by $\mathbf{Z}_p(1)$. It is a Galois-invariant $\mathbf{Z}_p$-lattice in the vector space $V = T \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$, which is often denoted by $\mathbf{Q}_p(1)$. The quotient V/T is isomorphic to μ_{p^∞}.

In this section, we want to discuss one-dimensional representations of G_F over $\mathbf{Q}_p$ arising from powers of χ. In particular, we will consider the powers χ^n, where $n \in \mathbf{Z}$, 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

$$\psi : \mathrm{Gal}(F(\mu_{p^\infty})/F) \to \mathbf{Z}_p^\times$$

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

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

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

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

Assume that χ is surjective. That is, we assume that χ defines an isomorphism $\mathrm{Gal}(F(\mu_{p^\infty})/F) \cong \mathbf{Z}_p^\times$. Then it is not hard to see that an arbitrary ψ can be uniquely expressed in the form

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

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

$$\mathrm{Hom}\big(\mathrm{Gal}(F(\mu_{p^\infty})/F), \mathbf{Z}_p^\times\big) \longrightarrow \mathbf{Z}_p^\times$$

defined by sending ψ to $\psi(g_o)$. The compact-open topology then coincides with the topology transferred from $\mathbf{Z}_p^\times$. To see that $\{\chi^n \mid n \in \mathbf{Z}\}$ is a dense subgroup of $\mathrm{Hom}(\mathrm{Gal}(F(\mu_{p^\infty})/F), \mathbf{Z}_p^\times)$, 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 $\mathbf{Z}_p$ as $k \to \infty$. Then $\chi^{n_k} \to \psi$ in the compact-open topology on $\mathrm{Hom}\big(\mathrm{Gal}(F(\mu_{p^\infty})/F), \mathbf{Z}_p^\times\big)$.

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

Proposition 1.6.1. *Assume that p is odd, that χ 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 $s \in \mathbf{Z}_p$. Then*

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

for any $k \geq 1$. Assume that $s_1,\ s_2 \in \mathbf{Z}_p$ 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 $H^1_{unr}(F, D_{\psi_1})[p^k] \cong H^1_{unr}(F, D_{\psi_2})[p^k]$.

Proof. First note that G_F acts on $D_\psi[p]$ by the character ω^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 $H^0(F_v^{unr}, D_\psi) = 0$. If v is an infinite prime, then $H^0(F_v, D_\psi) = 0$ 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 $F(\mu_{p^\infty})/F$ and hence I_{F_v} acts trivially on D_ψ. Therefore, $H^0(F_v^{unr}, D_\psi) = D_\psi$. Thus, for all primes v of F, $H^0(F_v^{unr}, D_\psi)$ 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 $u \in 1 + p\mathbf{Z}_p$. 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 $(\mathbf{Z}/p^k\mathbf{Z})$-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 $H^1_{unr}(F, D_\psi)[p] \cong H^1_{unr}(F, D_{\omega^i})[p]$. Thus, $\dim_{\mathbf{F}_p}\big(H^1_{unr}(F, D_\psi)[p]\big)$ depends only on i.*

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

Corollary 1.6.3. *Under the assumptions of proposition 1.6.1, we have*

$$H^1_{unr}(F, D_{\chi^{n_1}})[p^k] \cong H^1_{unr}(F, D_{\chi^{n_2}})[p^k]$$

if $n_1, n_2 \in \mathbf{Z}$ *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 $\psi = \psi_o$, which corresponds to $s = 0$, then $H^1_{unr}(F, D_{\psi_o})$ is the Pontryagin dual of $Cl_F[p^\infty]$. It turns out that $H^1_{unr}(F, D_\psi)$ is finite for s close to 0 in $\mathbf{Z}_p$, 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 ψ. Obviously, F_∞ is a subfield of $F(\mu_{p^\infty})$ and $\mathrm{Gal}(F_\infty/F) \cong \mathrm{im}(\psi)$ which is isomorphic to $\mathbf{Z}_p$. We will let Γ denote $\mathrm{Gal}(F_\infty/F)$. One often refers to F_∞ as the cyclotomic $\mathbf{Z}_p$-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_∞/F. It is clear that all other non-archimedian primes are unramified since the same is true for $F(\mu_{p^\infty})/F$. Applying the snake lemma to (23) gives us the following extension of (24), where we use the same notation for the maps and take $D = D_\psi$:

$$\ker(\beta_n) \longrightarrow \ker(\gamma_n) \longrightarrow \mathrm{coker}(\alpha_n) \longrightarrow \mathrm{coker}(\beta_n) \tag{29}$$

in the notation of those diagrams. We have $\mathrm{coker}(\beta_n) = 0$, 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 $ord_p(s) = k \geq 0$, 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 $D_\psi[p^n]$, $H^1(F, D_\psi[p^n]) = \mathrm{Hom}(G_F, D_\psi[p^n])$, and a 1-cocycle ϕ is in $\ker(\beta_n)$ if and only if ϕ is the coboundary of an element of $D[p^{2n}]$. Since the action of G_F on $D[p^{2n}]$ factors through $\Gamma = \mathrm{Gal}(F_\infty/F)$, any $\phi \in \ker(\beta_n)$ will also factor through Γ and hence through Γ/Γ^{p^n}. We will denote the fixed field for Γ^{p^n} by F_n, a cyclic extension of F of degree p^n. Thus, it follows that

$$\ker(\beta_n) = \mathrm{Hom}(\mathrm{Gal}(F_n/F), D_\psi[p^n]) \tag{30}$$

if $n = ord_p(s) + 1$. It remains to study $\ker(\gamma_n)$ and the image of the map $\ker(\beta_n) \longrightarrow \ker(\gamma_n)$ 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 $\mathrm{coker}(\alpha_n)$ would obviously be nontrivial and that would imply that $H^1_{unr}(F, D_\psi) \neq 0$.

Since ψ 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 $v|p$, we are assuming that the inertia subgroup of $\mathrm{Gal}(F_\infty/F)$ is the entire group and hence $H^0(F_v^{unr}, D_\psi) = H^0(F, D_\psi)$ 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

$$\mathrm{im}\Big(H^1(F_{S_p}/F, D_\psi[p^n]) \to \prod_{v|p} H^1(F_v^{unr}, D[p^n])\Big) \bigcap \prod_{v|p} \ker(\gamma_{n,v})$$

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_∞/F. Let $\psi = \langle\chi\rangle^s$, where $s \in \mathbf{Z}_p$, $s \neq 0$.*

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

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

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

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

Proof. If there is just one prime $v \in S_p$, then the map $\ker(\beta_n) \longrightarrow ker(\gamma_n)$ 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)*, $\mathrm{coker}(\alpha_n) = 0$ and we have an isomorphism

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

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

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

$$H^1(F_v, D_\psi[p^n]) \longrightarrow H^1(F_v^{unr}, D_\psi) \tag{31}$$

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^{unr} and $F_v(\mu_{p^\infty})$ 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 $F_v^\times/(F_v^\times)^p \cong (\mathbf{Z}/p^n/Z)^2$. It follows that $\phi = \phi^{unr}\phi^{cyc}$, where ϕ^{unr} and ϕ^{cyc} are elements of $H^1(F_v, D_\psi[p^n])$ which factor through $\mathrm{Gal}(F_v^{unr})/F_v)$ and $\mathrm{Gal}(F_v(\mu_{p^\infty})/F_v)$, 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

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

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

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

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

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 $\mathrm{Gal}(M_n/F) \cong (\mathbf{Z}/p^n\mathbf{Z})^2$. 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 $H^1_{unr}(F, D_{\langle\chi\rangle^s})$ contains a subgroup

of order p^n. Thus, the order of $H^1_{unr}(F, D_{\langle\chi\rangle^s})$ will be unbounded as $s \to 0$ in $\mathbf{Z}_p$. 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:

$$\kappa : F^\times \otimes_{\mathbf{Z}} (\mathbf{Q}_p/\mathbf{Z}_p) \to H^1(F, \mu_{p^\infty})$$

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

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

Leopoldt's Conjecture. *$H^1_{unr}(F, \mu_{p^\infty})$ 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 $H^1(F, \mu_{p^\infty})$ associated to $b = \sqrt[p^n]{a}$. 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 $F_v(\sqrt[p^n]{a})/F_v$ 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 $F = \mathbf{Q}$, p is an odd prime, and $\psi = \chi^n$ for some $n \in \mathbf{Z}$ such that $n \not\equiv 0 \pmod{p-1}$. 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 $H^1_{unr}(\mathbf{Q}, D_{\chi^n})[p] = 0$. 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 $H^1_{unr}(\mathbf{Q}, D_{\omega^i}) = 0$. But this is true according to proposition 1.5.8 since, by assumption, $Cl_{\mathbf{Q}(\mu_p)}[p^\infty]^{(\omega^i)} = 0$. If $n \equiv 0 \pmod{p-1}$, then $H^1_{unr}(\mathbf{Q}, D_{\chi^n})[p] = 0$. This follows from part *(i)* of proposition 1.6.4.

If p is an irregular prime, then $Cl_{\mathbf{Q}(\mu_p)}[p^\infty]^{(\omega^i)} \neq 0$ for at least one odd value of i. Thus, for any such i, it follows that $H^1_{unr}(\mathbf{Q}, D_{\chi^n}) \neq 0$ for any integer $n \equiv i \pmod{p-1}$. In a later chapter, we will prove that the group $H^1_{unr}(\mathbf{Q}, D_{\chi^n})$ 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

$$m_1 \equiv m_2 \not\equiv 0 \pmod{p-1} \implies \frac{B_{m_1}}{m_1} \equiv \frac{B_{m_2}}{m_2} \pmod{p\mathbf{Z}_p}$$

which are known as the Kummer congruences. We have expressed them as congruences modulo $p\mathbf{Z}_p$ since the quantities B_m/m are p-integral, and hence in $\mathbf{Z}_p$, 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 $H^1_{unr}(\mathbf{Q}, D_{\chi^n}) \neq 0$ 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 $H^1_{unr}(\mathbf{Q}, D_{\chi^n})$ is equal to the power of p dividing $\zeta(n)$.*

In chapter 2, we will show that the groups $H^1_{unr}(\mathbf{Q}, D_{\chi^n})$ can be studied by an analogue of proposition 1.5.7 for the infinite Galois extension $\mathbf{Q}(\mu_{p^\infty})/\mathbf{Q}$. It turns out that the kernel and cokernel are actually trivial. This fact will allow us to relate the structure of the finite groups $H^1_{unr}(\mathbf{Q}, D_{\chi^n})$, for all n,

to the structure of the Galois group of a certain extension of $\mathbf{Q}(\mu_{p^\infty})$, the analogue of the p-Hilbert class field.

For $n \equiv 1 \pmod{p-1}$, one has $H^1_{unr}(\mathbf{Q}, D_{\chi^n})[p] \cong H^1_{unr}(\mathbf{Q}, D_\omega)[p] = 0$ and hence $H^1_{unr}(\mathbf{Q}, D_{\chi^n}) = 0$. 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 $\mathrm{ord}_p(B_m) = -1$. Thus,

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

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 $\mathrm{ord}_p\big(\zeta(n)\big) \to -\infty$. 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

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

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 poswer of p as $\zeta(n)$. Assume that $k \geq 1$. The refined Kummer congruences, stated in terms of values of $\zeta_p(s)$, are

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

where it is assume 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 $n \in \mathbf{Z}$ is fixed. We will consider the compatible system $\mathcal{V} = \{V_p\}$ where, for each prime p, V_p is 1-dimensional and $G_{\mathbf{Q}}$ acts by χ^n, where χ is the p-power cyclotomic character. The Mazur-Wiles theorem implies that if n is odd and negative, then the finite group $H^1_{unr}(\mathbf{Q}, D_{\chi^n})$ is trivial for all but finitely many

primes p. It follows that $H^1_{unr}(\mathbf{Q}, \mathcal{D}_\mathcal{V})$ 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 $H^1_{unr}(\mathbf{Q}, D_{\omega^{1-m}}) = 0$. 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 $H^1_{unr}(\mathbf{Q}, D_{\chi^n}) = 0$ 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 $H^1_{unr}(\mathbf{Q}, D_{\chi^n})$ is finite, although this is expected to be so. Furthermore, we have

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

and, if $p > n$, the Herbrand-Ribet theorem implies that this group is nontrivial if and only if $p | B_{p-n}$. 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 $H^1_{unr}(\mathbf{Q}, D_{\chi^n}) = 0$ for all p.

2 $\mathbf{Z}_p$-extensions and ideal class groups.

This chapter will present the theorems of Iwasawa concerning the growth of $Cl_{F_n}[p^\infty]$, where F_n varies over the layers in a $\mathbf{Z}_p$-extension of a number field F. The main theorem was proved by Iwasawa in the mid 1950s and concerns the growth of the orders of these groups. However, we will also prove results of Iwasawa concerning their group structure. A key ingredient in the proof is to consider the inverse limit

$$X = X_{F_\infty/F} = \varprojlim_n Cl_{F_n}[p^\infty]$$

as a module over the formal power series ring $\Lambda = \mathbf{Z}_p[[T]]$. The inverse limit X is defined by the norm maps N_{F_m/F_n} for $m \geq n \geq 0$. It turns out to be a finitely generated, torsion Λ-module. We will be able to partially describe the structure of such modules, enough for a proof of the theorem. Finally, in the last section, we discuss the special case where $F = \mathbf{Q}(\mu_p)$ for an odd prime p and $F_\infty = \mathbf{Q}(\mu_{p^\infty})$. Then F_∞/F is a $\mathbf{Z}_p$-extension. The n-th layer is $F_n = \mathbf{Q}(\mu_{p^{n+1}})$. There is a lot that we can say about the various invariants and modules introduced in this chapter, a topic which will be continued in later chapters. We will also discuss the relationship between $X_{F_\infty/F}$ and the unramified cohomology groups associated to powers of the cyclotomic character, continuing the topic of section 1.6.

2.1 Introductory remarks about $\mathbf{Z}_p$-extensions.

The theorem of Iwasawa alluded to above concerns a certain type of infinite extension K of a number field F. These infinite extensions were originally referred to as "Γ-extensions" by Iwasawa, but later he adopted the more descriptive term "$\mathbf{Z}_p$-extensions." Let p be a fixed prime. A Galois extension K/F is called a $\mathbf{Z}_p$-extension if the topological group $\mathrm{Gal}(K/F)$ is isomorphic to the additive group $\mathbf{Z}_p$ of p-adic integers.

Except for the trivial subgroup, all the closed subgroups of $\mathbf{Z}_p$ have finite index. Such a closed subgroup is of the form $p^n\mathbf{Z}_p$ for some nonnegative integer n and the corresponding quotient group is cyclic of order p^n. Thus, if K/F is a $\mathbf{Z}_p$-extension, the finite extensions of F which are contained in K form a tower $F = F_0 \subset F_1 \subset \cdots \subset F_n \subset \cdots$ of Galois extensions of F such that $\mathrm{Gal}(F_n/F) = \mathbf{Z}/p^n\mathbf{Z}$ for all n. Clearly $K = \bigcup_{n\geq 0} F_n$. If one chooses any

$\gamma_o \in \mathrm{Gal}(K/F)$ such that $\gamma_o|_{F_1}$ is nontrivial, then the infinite cyclic subgroup generated by γ_o is dense in $\mathrm{Gal}(K/F)$. We therefore say that $\mathrm{Gal}(K/F)$ is a topologically cyclic group and that the element γ_o is a topological generator of $\mathrm{Gal}(K/F)$. We will often use the notation F_∞ for a $\mathbf{Z}_p$-extension of F.

Let F be any number field and let p be a fixed prime. One important example of a $\mathbf{Z}_p$-extension of F is quite easy to construct. Let μ_{p^∞} denote the group of p-power roots of unity. The extension $F(\mu_{p^\infty})/F$ is an infinite Galois extension. At the beginning of section 1.6, we defined a continuous homomorphism

$$\chi : \mathrm{Gal}(F(\mu_{p^\infty})/F) \to \mathbf{Z}_p^\times.$$

This homomorphism is injective. Consequently, $\mathrm{Gal}(F(\mu_{p^\infty})/F)$ is isomorphic to an infinite closed subgroup of $\mathbf{Z}_p^\times$. Such a group has a finite torsion subgroup and the corresponding quotient group will be isomorphic to $\mathbf{Z}_p$. Therefore, $F(\mu_{p^\infty})$ contains a unique subfield F_∞ such that $\mathrm{Gal}(F_\infty/F) \cong \mathbf{Z}_p$. We refer to F_∞ as the cyclotomic $\mathbf{Z}_p$-extension of F. In particular, we will let $\mathbf{Q}_\infty$ denote the cyclotomic $\mathbf{Z}_p$-extension of $\mathbf{Q}$. The cyclotomic $\mathbf{Z}_p$-extension of an arbitrary number field F is then $F_\infty = F\mathbf{Q}_\infty$.

It is easy to show that the primes of F which are ramified in the cyclotomic $\mathbf{Z}_p$-extension F_∞/F are precisely the primes lying over p. For an arbitrary $\mathbf{Z}_p$-extension, we have the following result.

Proposition 2.1.1. *Suppose that F_∞/F is a $\mathbf{Z}_p$-extension. If v is a prime of F which is ramified in the extension F_∞/F, then v lies over p. At least one such prime must be ramified in F_∞/F.*

Proof. Let $\Gamma = \mathrm{Gal}(F_\infty/F)$. Let I_v denote the inertia subgroup of $\mathrm{Gal}(F_\infty/F)$ corresponding to a prime v of F. If v is ramified in F_∞/F, then I_v is nontrivial. Hence I_v must be infinite. If v is an archimedian prime of F, then I_v would be of order 1 or 2, and so must be trivial. Consequently, archimedian primes of F split completely in F_∞/F. If v is nonarchimedian, but lies over l, where $l \neq p$, then v is tamely ramified in F_∞/F. It is known in general that if v is tamely ramified in any abelian extension of F, then its ramification index must divide $N(v)-1$, where $N(v)$ denotes the cardinality of the residue field for v. This can be proved either by using properties of ramification groups or by using local class field theory. (See reference.) Thus, I_v would be finite. Therefore, I_v must be trivial and v must be unramified in F_∞/F.

For the final assertion, we just remark that the maximal unramified, abelian extension of F (the Hilbert class field of F) has finite degree over F. Thus, F_∞/F must be ramified for at least one prime. ■

The existence and ramification properties of $\mathbf{Z}_p$-extensions of any number field F will be discussed in considerable detail in chapter 3. We will just make a few remarks now. If we take $F = \mathbf{Q}$ as the base field, then it is not hard to prove that there is only one $\mathbf{Z}_p$-extension, the cyclotomic $\mathbf{Z}_p$-extension $\mathbf{Q}_\infty$ which was constructed above. To see this, one can use the Kronecker-Weber theorem which asserts that the maximal abelian extension $\mathbf{Q}^{ab}$ of $\mathbf{Q}$ is generated by all the roots of unity. Proposition 2.1.1 then implies that any $\mathbf{Z}_p$-extension of $\mathbf{Q}$ must be ramified only at p and therefore contained in $\mathbf{Q}(\mu_{p_\infty})$, and so must be $\mathbf{Q}_\infty$. The cyclotomic $\mathbf{Z}_p$-extension of an arbitrary number field F is $F_\infty = F\mathbf{Q}_\infty$.

If F is a totally real number field, then it should again be true that the cyclotomic $\mathbf{Z}_p$-extension is the only $\mathbf{Z}_p$-extension of F. This can be proved if $F \subset \mathbf{Q}^{ab}$, but is an open question in general (a special case of "Leopoldt's Conjecture"). If F is not totally real, then it turns out that there are infinitely many distinct $\mathbf{Z}_p$-extensions of F. We will discuss this matter in detail in chapter 3. In particular, theorem 3.3 gives a quantitative statement about the existence of $\mathbf{Z}_p$-extensions of an arbitrary number field F.

One of the main results to be proved in this chapter is the following famous theorem of Iwasawa.

Iwasawa's Growth Formula. *Suppose that $F_\infty = \bigcup_{n\geq 0} F_n$ is a $\mathbf{Z}_p$-extension of a number field F. Let h_n denote the class number of F_n and let $h_n^{(p)} = p^{e_n}$ denote the largest power of p dividing h_n. Then there exists integers λ, μ, and ν such that $e_n = \lambda n + \mu p^n + \nu$ for all sufficiently large n.*

Iwasawa's growth formula will be proved in section 2.4, based largely on the results of section 2.2 and 2.3. The integers λ and μ will be nonnegative. We will refer to them as the Iwasawa invariants for F_∞/F, often denoting them by $\lambda(F_\infty/F)$ and $\mu(F_\infty/F)$. Several interpretations of them will be given as we proceed.

Proposition 1.1.4 implies one very simple special case of Iwasawa's theorem, namely the following useful result.

Proposition 2.1.2. *Suppose that F is a number field and that p does not divide the class number of F. Let $F_\infty = \bigcup_{n\geq 0} F_n$ be a $\mathbf{Z}_p$-extension of F and suppose that only one prime of F is ramified in F_∞/F. Then p does not divide the class number of F_n for any $n \geq 0$. Therefore, Iwasawa's growth formula is valid with $\lambda = \mu = \nu = 0$.*

Proof. Suppose that I_v denotes the inertia subgroup of $\mathrm{Gal}(F_\infty/F)$ for the

one ramified prime v. It is clear that v must be totally ramified in F_∞/F. Otherwise, $F_\infty^{I_v}$ would be a nontrivial, unramified, cyclic p-extension of F, contradictict the assumption that $p \nmid h_F$. Hence. for each $n \geq 0$, the hypotheses in proposition 1.1.4 are satisfied for the extension F_n/F. Therefore, the class number of F_n is not divisible by p. ■

In particular, this result applies if F has only one prime lying above p and $p \nmid h_F$. For example, p doesn't divide the class number of $\mathbf{Q}_n$, the n-th layer in the cyclotomic $\mathbf{Z}_p$-extension $\mathbf{Q}_\infty/\mathbf{Q}$. Also, if we take $F = \mathbf{Q}(\mu_p)$, where p is any odd regular prime, then it follows that the class number of $\mathbf{Q}(\mu_{p^n})$ will not be divisible by p for all $n \geq 1$. The class number of $\mathbf{Q}(\mu_{2^n})$ is 1 for $n \leq 2$ and is odd for $n > 2$, again by proposition 2.1.2.

Now suppose that $F_\infty = \bigcup_{n\geq 0} F_n$ is any $\mathbf{Z}_p$-extension of F. For every $n \geq 0$, let L_n denote the p-Hilbert class field of F_n. Let $L_\infty = \bigcup_{n\geq 0} L_n$. Then L_∞ is an abelian extension of F_∞. Let $X = \mathrm{Gal}(L_\infty/F_\infty)$. This group will arise frequently in this book and will sometimes be denoted by $X_{F_\infty/F}$. We then have canonical isomorphisms of topological groups

$$X \;\cong\; \varprojlim_n \mathrm{Gal}(L_n/F_n) \;\cong\; \varprojlim_n A_n$$

where the inverse limits are defined by the restriction and norm maps

$$R_{F_m/F_n} :\; \mathrm{Gal}(L_m/F_m) \longrightarrow \mathrm{Gal}(L_n/F_n), \qquad N_{F_m/F_n} :\; A_m \longrightarrow A_n$$

for $m \geq n \geq 0$. The first isomorphism is just a consequence of the definition of the Galois group for an infinite Galois extension. The second isomorphism is defined by using the inverses of the Artin maps Art_{L_n/F_n} for $n \geq 0$. The compatibility of the maps defining the two inverse limits then follows from the commutative diagram (4) in the proof of proposition 1.1.1 for the fields $F = F_n$, $F' = F_m$, $m \geq n$. The field L_∞ could be described more directly as the maximal, abelian pro-p extension of F_∞ which is unramified at all primes of F_∞. The adjective "pro-p" refers to the fact that $X = \mathrm{Gal}(L_\infty/F_\infty)$ is a projective limit of finite p-groups. The equivalence of this description and the one above is not difficult to prove, and is left to the reader. We refer to L_∞ as the pro-p Hilbert class field of F_∞.

Let γ_o be a topological generator for $\Gamma = \mathrm{Gal}(F_\infty/F)$. For any $n \geq 0$, $\gamma_o^{p^n}$ is a topological generator for $\Gamma_n = \Gamma^{p^n}$, the unique subgroup of Γ of index p^n. We have $\Gamma_n = \mathrm{Gal}(F_\infty/F_n)$. Now L_∞ is a Galois extension of F and we

therefore have an exact sequence

$$1 \to X \to \mathrm{Gal}(L_\infty/F) \to \Gamma \to 1$$

of topological groups. We can then define a continuous action of Γ on X by inner automorphisms as one normally does for group extensions. Thus, if $\gamma \in \Gamma$, let $\widetilde{\gamma}$ be an automorphism of L_∞ such that $\widetilde{\gamma}|_{F_\infty} = \gamma$. One then defines

$$x^\gamma = \widetilde{\gamma} x \widetilde{\gamma}^{-1} \tag{32}$$

for all $x \in X$. Continuity means that the map $\Gamma \times X \to X$ defined by $(\gamma, x) \to x^\gamma$ for all $\gamma \in \Gamma$ and $x \in X$ is continuous. It will be somewhat more convenient to use an additive notation for X, and so we will now write γx instead of x^γ. More generally, we can regard X as a module for the group ring $\mathbf{Z}[\Gamma]$ and will write θx if $\theta \in \mathbf{Z}[\Gamma]$ and $x \in X$. In particular, for any $n \geq 0$, we will denote the element $\gamma_o^{p^n} - 1$ in this group ring by ω_n. Then $\omega_n x$ corresponds to an element of X which could be written in multiplicative notation as $\widetilde{\gamma_o}^{p^n} x (\widetilde{\gamma_o}^{p^n})^{-1} x^{-1}$, a commutator in $\mathrm{Gal}(L_\infty/F_n)$. In fact, we have the following basic result.

Proposition 2.1.3. *For each $n \geq 0$, the commutator subgroup of $\mathrm{Gal}(L_\infty/F_n)$ is $\omega_n X$. It is a closed subgroup.*

Proof. Let $G_n = \mathrm{Gal}(L_\infty/F_n)$ and $\Gamma_n = \mathrm{Gal}(F_\infty/F_n)$. We let $D(G_n)$ denote the commutator subgroup of G_n (as an abstract group). The elements of $\omega_n X$ are commutators in G_n and so $\omega_n X \subset D(G_n)$. Since X is compact and multiplication by ω_n is continuous, it follows that $\omega_n X$ is compact and hence closed. It is clearly a normal subgroup of G_n.

To prove that $D(G_n) = \omega_n X$, it is enough to show that the quotient $G_n/\omega_n X$ is abelian. Now $\gamma_0^{p^n}$ generates a dense, infinite cyclic subgroup Γ_n' of Γ_n. There is a surjective homomorphism from G_n to Γ_n. The inverse image of Γ_n' under that homomorphism is clearly abelian and dense in G_n. It follows that G_n is indeed abelian. ∎

Remark 2.1.4. We have stated the above proposition for the extension L_∞/F_∞. But the proof is obviously more general and would apply whenever L_∞ is an abelian, pro-p extension of F_∞ which is Galois over F. Under that assumption, $X = \mathrm{Gal}(L_\infty/F_\infty)$ would again have a continuous action of Γ. Here is an interesting and important example. Let Σ be any subset of the primes of F. Let Σ_∞ be the set of primes of F_∞ lying above those in Σ. Define M_∞^Σ to be the maximal, abelian, pro-p extension of F_∞ which

is ramified only at the primes in Σ_∞. It is easy to verify that M_∞^Σ is Galois over F and so the analogue of proposition 2.1.3 would apply. The field L_∞ considered above is the special case where Σ is empty.

If Σ contains all the primes of F lying above p, then we have $F_\infty \subseteq M_\infty^\Sigma$ according to proposition 2.1.1. For any $n \geq 0$, let Σ_n denote the primes of F_n lying above those in Σ. Let M_n^Σ denote the maximal, abelian, pro-p extension of F_n which is ramified only at the primes in Σ_n. Then, M_n^Σ is the maximal abelian extension of F_n contained in M_∞^Σ. If we let $X_\Sigma = \mathrm{Gal}(M_\infty^\Sigma/F_\infty)$, then we have

$$\mathrm{Gal}(M_\infty^\Sigma/M_n^\Sigma) = \omega_n X_\Sigma, \qquad \mathrm{Gal}(M_n^\Sigma/F_\infty) \cong X_\Sigma/\omega_n X_\Sigma$$

for any $n \geq 0$.

As proposition 2.1.2 illustrates, various questions about $\mathbf{Z}_p$-extensions, including the proof of the growth formula become simpler under the following hypothesis about ramification.

RamHyp(1): *Exactly one prime of F is ramified in the $\mathbf{Z}_p$-extension F_∞/F and this prime is totally ramified.*

Under this hypothesis, proposition 2.1.2 already tells us that if p does not divide the class number of F, then $X = 0$. The next proposition tells us that X, together with the action of Γ on it, determines the structure of all the groups A_n for $n \geq 0$.

Proposition 2.1.5. *Suppose that RamHyp(1) is satisfied for the $\mathbf{Z}_p$-extension F_∞/F. Then, with the notation as above, we have canonical isomorphisms*

$$X/\omega_n X \cong \mathrm{Gal}(L_n/F_n) \cong A_n$$

for all $n \geq 0$.

Proof. This is a straightforward variation on the proof of proposition 1.1.4. Let v be the unique prime of F which is ramified in F_∞/F. Let v_n denote the unique prime of F_n lying above v. Then v_n is the only prime of F_n ramified in the $\mathbf{Z}_p$-extension F_∞/F_n and it is totally ramified. Let K_n denote the maximal abelian extension of F_n contained in L_∞. Proposition 2.1.3 implies that we have the isomorphism

$$X/\omega_n X \to \mathrm{Gal}(K_n/F_\infty)$$

induced by the restriction map $x \to x|_{K_n}$ for $x \in X$.

Let I_n denote the inertia subgroup of $\mathrm{Gal}(K_n/F_n)$ for v_n. It is clear that L_n is the subfield of K_n fixed by I_n and F_∞ is the subfield fixed by $\mathrm{Gal}(K_n/F_\infty)$. Since these two subgroups of $\mathrm{Gal}(K_n/F_n)$ have trivial intersection, it follows that $K_n = L_n F_\infty$. Since v_n is totally ramified in F_∞/F_n, we have $L_n \cap F_\infty = F_n$ and therefore the restriction map

$$\mathrm{Gal}(K_n/F_\infty) \to \mathrm{Gal}(L_n/F_n)$$

is indeed an isomorphism. The second isomorphism in the proposition is just the inverse of the Artin map for the extension L_n/K_n. ■

The above proposition reduces the proof of Iwasawa's formula for a $\mathbf{Z}_p$-extension satisfying RamHyp(1) to proving an analogous formula for the growth of the quotients $X/\omega_n X$ of X. We do this in the next two sections where we begin the study of the structure and properties of Γ-modules, a topic that we will return to in Chapter 7. That study will also be the basis for proving Iwasawa's growth formula in general.

2.2 The structure of Γ-modules.

We will refer to an abelian, pro-p group X which admits a continuous action by the group Γ as a Γ-module. This means that there is a homomorphism $\Gamma \to \mathrm{Aut}(X)$ such that the map $\Gamma \times X \to X$ defined by $(\gamma, x) \to \gamma x$ is continuous. Here $\gamma \in \Gamma$, $x \in X$, and γx denotes the image of x under the automorphism given by γ.

Suppose that X is any abelian, pro-p group. Then, for some indexing set I, we have

$$X = \varprojlim_i X_i$$

where X_i is a finite, abelian p-group for each index $i \in I$. It is easy to make X into a $\mathbf{Z}_p$-module. Each X_i is a $(\mathbf{Z}/p^{t_i}\mathbf{Z})$-module for some $t_i > 0$. The canonical homomorphism $\mathbf{Z}_p \to \mathbf{Z}/p^{t_i}\mathbf{Z}$ makes each X_i into a $\mathbf{Z}_p$-module. The projective limit X then inherits the structure of a $\mathbf{Z}_p$-module (since the maps defining the projective limit will be $\mathbf{Z}_p$-modules homomorphisms). It is a topological $\mathbf{Z}_p$-module in the sense that the map $\mathbf{Z}_p \times X \to X$ defined by $(z, x) \to zx$ (where $z \in \mathbf{Z}_p$ and $x \in X$) is continuous. Conversely, it is not hard to see that any compact, topological $\mathbf{Z}_p$-module is an abelian, pro-p group. One way to prove this is to consider the Pontryagin dual $S = \mathrm{Hom}(X, \mathbf{Q}_p/\mathbf{Z}_p)$, which is a discrete abelian group and also a topological

$\mathbf{Z}_p$-module. One then sees that every element of S has finite, p-power order. It follows from this that S is a direct limit of finite $\mathbf{Z}_p$-modules S_i where i varies over some indexing set I.

Suppose now that X is an abelian, pro-p group which has a continuous action of Γ. As above, we have $X = \varprojlim X_i$, where the X_i's are finite, abelian p-groups and i varies over an appropiate indexing set I. For each $i \in I$, let $Y_i = \ker(X \to X_i)$. Thus, Y_i is an open subgroup of X. An easy continuity argument shows that $\gamma(Y_i) = Y_i$ for all γ in some subgroup of finite index in Γ. This means that the orbit of Y_i under the action of Γ is finite. Hence Y_i contains an open subgroup which is Γ-invariant. This implies that we can assume without loss of generality that each Y_i is already Γ-invariant and so

$$X = \varprojlim_i X_i,$$

where each X_i is a finite, abelian p-group with a continuous action of Γ. The maps defining the projective limit are Γ-homomorphisms.

It will be important for us to view X as a module over the ring $\Lambda = \mathbf{Z}_p[[T]]$, the formal power series ring over $\mathbf{Z}_p$ in the variable T. One sees easily that Λ is a local ring, $\mathfrak{m} = (p, T)$ is its maximal ideal, and Λ is complete in its $\mathfrak{m}$-adic topology. Also $\Lambda/\mathfrak{m} = \mathbf{F}_p$ and $\Lambda/\mathfrak{m}^t$ is finite (of order $p^{t(t+1)/2}$) for any Let γ_o denote a topological generator for Γ, as in section 2.1. Roughly speaking, we will make X into a Λ-module by regarding T as the endomorphism $\gamma_o - 1$.

For each $i \in I$, we have $p^{a_i} X_i = 0$ for some $a_i > 0$. Also, $\gamma_o - 1$ defines an endomorphism of X_i which has a nontrivial kernel if X_i is nontrivial. Consequently, $(\gamma_o - 1)X_i$ is a proper subgroup of X_i if $X_i \neq 0$. It follows that $(\gamma_o - 1)^{b_i} X_i = 0$ for some $b_i > 0$. Thus, we can regard X_i as a module over the finite ring $\mathbf{Z}_p[T]/(p^{a_i}, T^{b_i})$, where we let T act on X_i as the endomorphism $\gamma_o - 1$. However, we obviously have $\mathbf{Z}_p[T]/(p^{a_i}, T^{b_i}) \cong \mathbf{Z}_p[[T]]/(p^{a_i}, T^{b_i})$, and so we can regard X_i as a Λ-module which is annihilated by the ideal (p^{a_i}, T^{b_i}). Taking $t_i = a_i + b_i$, it is obvious that $\mathfrak{m}^{t_i} \subset (p^{a_i}, T^{b_i})$ and so each X_i can be regarded as a module over $\Lambda/\mathfrak{m}^{t_i}$. Regarding the X_i's as Λ-modules, it is clear that the maps defining the projective limit are Λ-module homomorphisms. Thus X becomes a topological Λ-module. That is, the map $\Lambda \times X \to X$ defined by $(\theta, x) \to \theta x$ for $\theta \in \Lambda,\ x \in X$ is continuous.

Conversely, if X is any compact Λ-module, then X is also a compact $\mathbf{Z}_p$-module and hence is an abelian, pro-p group. To make X into a Γ-module, note that Γ can be identified as a topological group with a subgroup of $\Lambda^\times$

by the continuous homomorphism $\gamma_o^z \longrightarrow (1+T)^z$ for all $z \in \mathbf{Z}_p$. Here we define

$$(1+T)^z = \sum_{i=0}^{\infty} \binom{z}{i} T^i, \qquad where \quad \binom{z}{i} = \frac{1}{i!} \prod_{j=1}^{i} (z-j+1).$$

It is not difficult to prove that the coefficients of the above power series are in $\mathbf{Z}_p$. the constant term is 1, and so the power series is indeed invertible in Λ. Thus, X admits a continuous action of Γ from which the Λ-module structure on X arises by letting T act as $\gamma_o - 1$, just as above. If X is finitely generated as a Λ-module, then it is clear that X is compact and that the quotients $X/\mathfrak{m}^n X$ are finite Λ-modules for all $n \geq 0$. In this case, we have

$$X \cong \varprojlim_i X/\mathfrak{m}^n X,$$

an inverse limit of a sequence of finite Λ-modules.

We proved a version of Nakayama's lemma in chapter 1, lemma 1.5.3. That proof works in a much more general context. Assume that R is a local ring with maximal ideal $\mathfrak{m}$, that R is complete in its $\mathfrak{m}$-adic topology, and that $R/\mathfrak{m}^t$ is finite for all $t > 0$. In particular, $k = R/\mathfrak{m}$ is a finite field. Let p be its characteristic. Now $R = \varprojlim R/\mathfrak{m}^t$, where the finite rings $R/\mathfrak{m}^n$ have the discrete topology, and so R is a compact, topological ring. Suppose that X is a projective limit of finite, abelian groups X_n and that each X_n is a module over the ring $R/\mathfrak{m}^{t_n}$ for some $t_n > 0$ (which implies that X_n must be a p-group). We can then regard each X_n as an R-module. Assume that the maps defining the projective limit are R-module homomorphisms. Then X itself becomes an R-module and the map $R \times X \to X$ defined by $(r, x) \to rx$ is continuous. That is, X is a compact, topological R-module. Conversely, any topological R-module X which is compact arises in the above way.

Proposition 2.2.1. Nakayama's lemma for compact R-modules. *Suppose that R and X are as above. Let $x_1, \ldots, x_d$ be a subset of X. For each i, $1 \leq i \leq d$, let $\widetilde{x}_i$ denote the image of x_i under the natural map $X \to X/\mathfrak{m}X$. Then $x_1, \ldots, x_d$ is a generating set for the R-module X if and only if $\widetilde{x}_1, \ldots, \widetilde{x}_d$ is a generating set for the k-vector space $X/\mathfrak{m}X$.*

Proof. It is obvious that $\widetilde{x}_1, \ldots, \widetilde{x}_d$ generate the k-vector space $X/\mathfrak{m}X$ if $x_1, \ldots, x_d$ generate the R-module X. Conversely, assume that $\widetilde{x}_1, \ldots, \widetilde{x}_d$

generate $X/\mathfrak{m}X$ as a k-vector space. Let Y be the R-submodule of X generated by $x_1, \ldots, x_d$. Since Y is a continuous image of R^d and R is compact, it follows that Y is compact. Therefore Y is a closed R-submodule of X. It is therefore enough to prove that Y is dense in X. This follows as before once we establish the result in the case where X is finite.

If X is finite, then $\mathfrak{m}^t X = 0$ for some $t > 0$. We are assuming that the image of Y under the canonical homomorphism $X \to X/\mathfrak{m}X$ is all of $X/\mathfrak{m}X$. Thus, $X = Y + \mathfrak{m}X$. It follows that $X = Y + \mathfrak{m}^i X$ for all $i > 0$. Taking $i = t$, we get $Y = X$. ■

Corollary 2.2.2. *Suppose that R and X are as above. Then*

1. *$X = 0$ if and only if $X = \mathfrak{m}X$.*
2. *X is a finitely generated R-module if and only if $X/\mathfrak{m}X$ is finite.*

Proof. These statements follow immediately from Nakayama's lemma. Of course, statement 1 could be proved quite directly by again reducing to the case where X is finite. Then, on the one hand, $\mathfrak{m}^t X = 0$ for some $t > 0$. But, on the other hand, $X = \mathfrak{m}X \Rightarrow X = \mathfrak{m}^t X$ for all $t > 0$. It follows that $X = 0$. ■

We will be primarily interested in the special case where R is ring Λ introduced earlier. Suitable candidates for X are provided by compact Γ-modules. In general, the examples of interest to us will be finitely generated as Λ-modules.

The ring Λ is Noetherian and has Krull-dimension 2. The maximal ideal $\mathfrak{m}$ has height 2. One simple way to obtain prime ideals of height 1 is as kernels of the evaluation homomorphisms. Suppose that $\alpha \in \overline{\mathbf{Q}}_p$ and has absolute value < 1. If $f(T) \in \Lambda$, then one can define $f(\alpha) \in \mathcal{O} = \mathbf{Z}_p[\alpha]$ since the power series obviously converges to some element of that ring. The ring $\mathcal{O}$ is a subring of the ring of integers in $\mathbf{Q}_p(\alpha)$—a finite extension of $\mathbf{Q}_p$. The map $f(T) \to f(\alpha)$ defines a surjective ring homomorphism $\Lambda \to \mathcal{O}$ and its kernel is a prime ideal of height 1. If α and α' are two such elements of $\overline{\mathbf{Q}}_p$, then it is easy to see that the corresponding evaluation homomorphisms have the same kernel if and only if α and α' are conjugate over $\mathbf{Q}_p$. Therefore, infinitely many distinct prime ideals arise in this way. In fact, it will become clear later that all but one of the prime ideals of height 1 in Λ arise in this way. The exception is the ideal (p). If $f(T) = \sum a_i T^i \in \Lambda$, define $\widetilde{f}(T) = \sum \widetilde{a}_i T^i \in \mathbf{F}_p[[T]]$, where $\widetilde{a}$ denotes the image of $a \in \mathbf{Z}_p$

under the homomorphism $\mathbf{Z}_p \to \mathbf{F}_p$. Then the map $\Lambda \to \mathbf{F}_p[[T]]$ defined by $f(T) \to \widetilde{f}(T)$ is a surjective ring homomorphism with kernel (p). This makes it clear that (p) is indeed a prime ideal of Λ.

Suppose that X is a finitely generated, torsion Λ-module. If I is any ideal of Λ, we will use the notation

$$X[I] = \{x \in X \mid \alpha x = 0 \quad \text{for all } \alpha \in I\}$$

Let $Z = \bigcup_{n \geq 0} X[\mathfrak{m}^n]$ which is a Λ-submodule of X. Since Λ is Noetherian, Z must be finitely generated and so it follows that $Z = X[\mathfrak{m}^t]$ for some $t > 0$ and that Z is finite. It is clear that any finite Λ-submodule of X is contained in Z and so we refer to Z as the maximal, finite Λ-submodule of X.

Let $Y = \bigcup_{n \geq 0} X[p^n]$, which is just the $\mathbf{Z}_p$-torsion submodule of X. We will denote Y simply by X_{tors} in this chapter. Just as above, we see that $Y = X[p^t]$ for some $t \geq 0$. We have $Z \subset Y$. The quotient X/Y is a finitely generated, torsion Λ-module and is torsion-free as a $\mathbf{Z}_p$-module. If $f(T) = \sum a_i T^i$ is a nonzero element of Λ which annihilates X, then write $f(T) = p^m g(T)$, where $g(T) \in \Lambda$ is not divisible by p. It is clear that $g(T)$ annihilates X/Y. If X/Y has d generators as a Λ-module, then it is a quotient of the Λ-module U^d, where $U = \Lambda/(g(T))$. The following lemma gives the structure of U as a $\mathbf{Z}_p$-module.

Lemma 2.2.3. *Suppose that $g(T) = \sum_{i=0}^{\infty} b_i T^i \in \Lambda$ is not divisible by p. Let $l = \min\{i \mid b_i \in \mathbf{Z}_p^\times\}$. Then $U = \Lambda/(g(T))$ is a free $\mathbf{Z}_p$-module of rank l.*

Proof. Let $I = (g(T))$. It is clear that $U = \Lambda/I$ is torsion-free as a $\mathbf{Z}_p$-module. Otherwise, there would be an element $h(T) \in \Lambda$ such that $ph(T) \in I$, but $\notin pI$). That is, $ph(T) = g(T)j(T)$ where $j(T)$ is not divisible by p. But this is not possible since (p) is a prime ideal of Λ.

Now U/pU can be considered as an $\mathbf{F}_p[[T]]$-module and is isomorphic to $\mathbf{F}_p[[T]]/(\widetilde{g}(T))$, where, as earlier, $\widetilde{g}(T) = \sum \widetilde{b}_i T^i$. Note that $\widetilde{g}(T)$ is a nonzero element of $\mathbf{F}_p[[T]]$ and $(\widetilde{g}(T)) = (T^l)$. It is clear that U/pU has dimension l as an $\mathbf{F}_p$-vector space and so, by lemma 1.5.3 (Nakayama's Lemma for compact $\mathbf{Z}_p$-modules), it follows that U is a finitely generated $\mathbf{Z}_p$-module and that l is the minimal number of generators. Since U is torsion-free, it must be free of rank l. ■

We summarize the above observations in the following proposition.

Proposition 2.2.4. *Suppose that X is a finitely generated, torsion Λ-module. Then there are uniquely determined Λ-submodules Z and Y of X*

with the following properties:

a. *Z is finite and X/Z has no nonzero, finite Λ-submodules.*

b. *Y is annihilated by a power of p and X/Y is a free $\mathbf{Z}_p$-module of finite rank.*

This proposition allows us to define certain important invariants associated with X. The $\mathbf{Z}_p$-rank of X/Y is obviously equal to $\dim_{\mathbf{Q}_p}(V)$, where V is the $\mathbf{Q}_p$-vector space $X \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$. We define

$$\lambda(X) = \mathrm{rank}_{\mathbf{Z}_p}(X/Y) = \dim_{\mathbf{Q}_p}(V). \tag{33}$$

Then $X/Y = \mathbf{Z}_p^{\lambda(X)}$ as a $\mathbf{Z}_p$-module. Now $Y = X[p^t]$ for some $t > 0$. (Even if $Y = 0$, we will take $t > 0$ in the following definitions.) For each i such that $0 < i \leq t$, the Λ-module $X[p^i]/X[p^{i-1}]$ has exponent p and can be considered as an $\mathbf{F}_p[[T]]$-module. It will be finitely generated and thus has finite rank. We define

$$\mu(X) = \sum_{i=1}^{t} \mathrm{rank}_{\mathbf{F}_p[[T]]}\big(X[p^i]/X[p^{i-1}]\big). \tag{34}$$

If X is finitely generated as a $\mathbf{Z}_p$-module, then $\mu(X) = 0$. To be precise, we have

$$\mu(X) = 0 \Leftrightarrow Y \textit{ is finite } \Leftrightarrow X[p] \textit{ is finite } \Leftrightarrow X/pX \textit{ is finite}$$

In this case, Y and Z coincide. On the other hand, it is also clear that $\lambda(X) = 0 \Leftrightarrow p^t X = 0$ for some $t > 0$

We will refer to $\lambda(X)$ and $\mu(X)$ as the Iwasawa invariants for the Λ-module X. Another invariant which will play an important role will be a polynomial $f_X(T)$ in $\mathbf{Z}_p[T]$, which we refer to as the "characteristic polynomial" of X. However, this polynomial depends not just on the structure of X as a Γ-module, but also on the choice of topological generator γ_o of Γ. (In a later chapter, we will remedy this by redefining the ring Λ in a more intrinsic way, viewing it as the "completed group algebra for Γ over $\mathbf{Z}_p$.") The definition is $f_X(T) = p^{\mu(X)} g_X(T)$, where $g_X(T)$ is the monic polynomial whose roots are precisely the eigenvalues of the linear operator $T = \gamma_o - 1$ acting on the $\mathbf{Q}_p$-vector space V defined above. These eigenvalues are in $\overline{\mathbf{Q}}_p$ and are counted according to their multiplicities so that $g_X(T)$, and hence $f_X(T)$,

has degree equal to $\lambda(X)$. Since T acts on X topologically nilpotently, it is not hard to see that the eigenvalues of T have absolute value < 1. Therefore, the nonleading coefficients of $g_X(T)$ are divisible by p.

It will be useful to have finer invariants to describe the structure of $Y = X_{tors}$ as a Λ-module. For each $i \geq 1$, define $r_i = \text{rank}_{\mathbf{F}_p[[T]]}(X[p^i]/X[p^{i-1}])$. Assume that $\mu(X) > 0$. This means that $r_1 > 0$. Choose t so that $r_t > 0$, but $r_{t+1} = 0$. Note that $r_1 \geq \cdots \geq r_t$. Let $r = r_1$. The finer μ-invariants will be positive integers $\mu_1, \ldots, \mu_r$, consisting of $r_1 - r_2$ $1's$, $r_2 - r_3$ $2's$, ..., and r_t $t's$. With this definition, we have

$$\mu(X) = \sum_{i=1}^{t} r_i = \sum_{j=1}^{r} \mu_j. \tag{35}$$

As a simple illustration, suppose that X is a Λ-module and that $Y \cong \Lambda/p^m\Lambda$, where $m \geq 0$. We then have $r = 1$ and $\mu_1 = m$. If $Y \cong (\Lambda/p\Lambda)^m$, we then have $r = m$ and $\mu_1 = \cdots = \mu_m = 1$. In both cases, we have $\mu(X) = m$.

Let F_∞/F be a $\mathbf{Z}_p$-extension and let L_∞ be the pro-p Hilbert class field of F_∞. We will prove that $X = \text{Gal}(L_\infty/F_\infty)$ is a finitely generated, torsion Λ-module in section 2.5. The integers λ and μ occurring in Iwasawa's formula turn out to be precisely the Iwasawa invariants for X: $\lambda = \lambda(X)$, $\mu = \mu(X)$. The polynomial $f_X(T)$ will also be of special interest. In the case where $F/\mathbf{Q}$ is an abelian extension and F_∞ is the cyclotomic $\mathbf{Z}_p$-extension of F, its roots are related in a certain way to the zeros of the p-adic L-functions defined by Kubota and Leopoldt. The precise relationship, which was first conjectured by Iwasawa in 1969 and proved by Mazur and Wiles in 1979, will be described in Chapter 8 together with a proof for the special case where $F = \mathbf{Q}(\mu_p)$. Closely related to this is a simple interpretation of the roots of $f_X(T)$ in terms of the unramified cohomology groups discussed in section 1.6. That interpretation will be discussed in the final section of this chapter

If F_∞/F satisfies RamHyp(1), then the assertion that X is a finitely generated, torsion Λ-module is relatively easy to prove. In this case, we already know that $X/\omega_n X$ is finite for all n. In particular, X/TX is finite. The assertion that X is finitely generated then follows immediately from the corollary to Nakayama's lemma. The assertion that X is a torsion Λ-module follows from the following result.

Proposition 2.2.5. *Let X be a finitely generated Λ-module. Then the following statements are equivalent:*

a. *There exists an element $f(T) \in \mathfrak{m}$ such that $X/f(T)X$ is finite.*

b. *X contains a torsion $\mathbf{Z}_p$-submodule Y such that X/Y is finitely generated as a $\mathbf{Z}_p$-module.*

c. *X is a torsion Λ-module.*

Proof. We have already proved that *(c)* $\Rightarrow$ *(b)*. The converse *(b)*$\Rightarrow$*(c)* is rather easy. We can assume that X/Y is $\mathbf{Z}_p$-torsion free. Since Λ is Noetherian, Y is also finitely generated and has bounded exponent. Therefore, it is annihilated by p^a for some a. As for X/Y, this is a free $\mathbf{Z}_p$-module of finite rank and multiplication by T defines an endomorphism of that module. If $g(x)$ is the characteristic polynomial of this endomorphism, then $g(T)$ annihilates X/Y. Thus the nonzero element $p^a g(T)$ is an annihilator of X, proving *(c)*.

We also have *(b)* $\Rightarrow$ *(a)*. To see this, one can simply take $g(T) = T - \beta$, where $\beta \in p\mathbf{Z}_p$ is not an eigenvalue of the endomorphism of X/Y given by multiplication by T. Then $(T-\beta)(X/Y)$ has finite index in X/Y. Suppose that $p^t Y = 0$. Then for each i, $0 < i \leq t$, $Y[p^i]/Y[p^{i-1}]$ can be considered as a finitely generated $\mathbf{F}_p[[T]]$-module. the cokernel of multiplication by $T - \beta$ is clearly finite. It then follows that $(T-\beta)Y$ has finite index in Y. Consequently, by the snake lemma, one sees that $(T-\beta)X$ has finite index in X.

Finally, we prove that *(a)* $\Rightarrow$ *(c)*. If *(a)* holds and p divides $f(T)$, then X/pX is finite too. Hence, by Nakayama's lemma for the ring $\mathbf{Z}_p$, it follows that X is finitely generated over $\mathbf{Z}_p$. Hence *(b)* is true, and so *(c)* follows in this case. Thus, we can now assume that p doesn't divide $f(T)$. Then, by lemma 2.2.3, $\Lambda/(f(T))$ is a free $\mathbf{Z}_p$-module and its $\mathbf{Z}_p$-rank $l = \deg(f(T))$ is positive. Let $r = \mathrm{rank}_\Lambda(X)$. The following lemma then completes the proof of proposition 2.2.5. It implies that $r = 0$ if $X/(f(T))X$ is finite. ■

Lemma 2.2.6. *Suppose that X is a finitely generated Λ-module and that $f(T) \in \Lambda$. Let $r = \mathrm{rank}_\Lambda(X)$ and $l = \deg(f(T))$. Then*

$$\mathrm{rank}_{\mathbf{Z}_p}(X/f(T)X) \geq rl. \tag{36}$$

If X is a torsion-free Λ-module, then equality holds.

Proof. To prove (36), we can obviously replace X by the quotient module $X/X_{\Lambda-tors}$. So we can assume without loss of generality that X is a torsion-free Λ-module. We can also clearly assume that $f(T)$ is not divisible by p.

Now X contains a Λ-submodule Y which is free of rank r over Λ. We have the exact sequence

$$0 \longrightarrow Y \longrightarrow X \longrightarrow Z \longrightarrow 0$$

where Z is a finitely generated, torsion Λ-module. The snake lemma then gives an exact sequence

$$0 \longrightarrow Z[f(T)] \longrightarrow Y/f(T)Y \longrightarrow X/f(T)X \longrightarrow Z/f(T)Z \longrightarrow 0.$$

By lemma 2.2.6, $Y/f(T)Y$ is a free $\mathbf{Z}_p$-module of rank rl. Let U denote the $\mathbf{Z}_p$-torsion submodule of Z. Then Z/U is a free $\mathbf{Z}_p$-module of finite rank. This implies that $Z[f(T)]$ and $Z/f(T)Z$ have the same (finite) $\mathbf{Z}_p$-rank. Thus we see that $\text{rank}_{\mathbf{Z}_p}(X/f(T)X) = rl$. ■

In a later chapter, we will discuss more precise results concerning the structure of finitely generated Λ-modules. The results that we are proving here and in the next section will suffice for the proof of Iwasawa's growth formula. Some of the later theorems (including a couple in this chapter) involve the following standard ring-theoretic notion. Let R be a Noetherian, local, integral domain. The Krull-dimension of R is then finite. We denote it by $\dim(R)$. If P is any prime ideal of R, then we will denote its height by $\text{ht}(P)$. It is related to the Krull-dimension of R/P by the formula:

$$\text{ht}(P) + \dim(R/P) = \dim(R).$$

Let X be a finitely generated R-module. For any $x \in X$, let $\text{Ann}(x)$ denote its annihilator in R. The primes ideals of R which are associated to X form the following set.

$$\text{Ass}_R(X) = \{P \mid P = \text{Ann}(x) \quad \text{for some } x \in X\}$$

This is a finite set. We will say that X is "pure of dimension d" if $\dim(R/P) = d$ for every prime ideal $P \in \text{Ass}(X)$. Thus, X is pure if all the prime ideals in $\text{Ass}(X)$ have the same height h. The dimension will then be $d = \dim(R) - h$. In particular, a torsion-free R-module would be pure of dimension equal to $\dim(R)$.

If we take $R = \Lambda$, then the Krull-dimension is 2. As explained earlier, Λ has one prime ideal of height 2, the maximal ideal $\mathfrak{m} = (p, T)$, and infinitely many prime ideals of height 1. A nonzero, finitely generated, torsion Λ-module X is pure in the following two cases: *(a)* X is finite and hence pure

of dimension 0, *(b)* X has no nonzero, finite Λ-submodules and hence is pure of dimension 1.

We have been considering Λ-modules which are profinite and therefore compact as topological groups. It is also quite useful to consider their Pontryagin duals. Suppose that X is a pro-p abelian group (i.e. a compact $\mathbf{Z}_p$-module). Let $S = \mathrm{Hom}(X, \mathbf{Q}_p/\mathbf{Z}_p)$. One verifies easily that S is a p-primary abelian group and that the usual topology on it (the so-called "compact-open" topology) is just the discrete topology. Also, if S is any p-primary abelian group with the discrete topology, then we can regard it as a direct limit of finite abelian p-groups. Therefore, its Pontryagin dual $X = \mathrm{Hom}(S, \mathbf{Q}_p/\mathbf{Z}_p)$ is an abelian, pro-p group. We can regard both S and X as $\mathbf{Z}_p$-modules.

If X is a finitely generated $\mathbf{Z}_p$-module, we will say that S is a cofinitely generated $\mathbf{Z}_p$-module. We then define $\mathrm{corank}_{\mathbf{Z}_p}(S) = \mathrm{rank}_{\mathbf{Z}_p}(X)$, which we refer to as the $\mathbf{Z}_p$-corank of S. Note that since the Pontryagin dual of $\mathbf{Z}_p$ is $\mathbf{Q}_p/\mathbf{Z}_p$, it follows that any cofinitely generated $\mathbf{Z}_p$-module S is isomorphic to $(\mathbf{Q}_p/\mathbf{Z}_p)^l \times T$ as a $\mathbf{Z}_p$-module, where T is finite and $l = \mathrm{corank}_{\mathbf{Z}_p}(S)$. Thus, the maximal divisible subgroup S_{div} of S is isomorphic to $(\mathbf{Q}_p/\mathbf{Z}_p)^l$ and has finite index in S. If X is torsion-free as a $\mathbf{Z}_p$-module (finitely generated or not), then S is divisible. The following result is a consequence of Nakayama's lemma for compact $\mathbf{Z}_p$-modules, but also can be proved directly.

Proposition 2.2.7. *Suppose that S is a discrete, p-primary abelian group. Then S is a cofinitely generated $\mathbf{Z}_p$-module if and only if $S[p]$ is finite. If S is divisible, then* $\mathrm{corank}_{\mathbf{Z}_p}(S) = \dim_{\mathbf{F}_p}(S[p])$.

Suppose that S is a discrete, p-primary abelian group with a continuous action of Γ. We can translate our earlier results into equivalent statements about S. Let $X = \mathrm{Hom}(S, \mathbf{Q}_p/\mathbf{Z}_p)$, which also admits a continuous action of Γ. (This is defined on Hom in the usual way, using the given action of Γ on S and the trivial action on $\mathbf{Q}_p/\mathbf{Z}_p$). Since S is also a $\mathbf{Z}_p$-module, it is not hard to make S into a Λ-module directly (showing first that S is a direct limit of finite Γ-invariant subgroups). Or one can equivalently transfer the structure of X as a Λ-module to S. Just as above, we say that S is cofinitely generated as a Λ-module if X is finitely generated as a Λ-module, cotorsion as a Λ-module if X is a torsion Λ-module. We refer to $\mathrm{rank}_\Lambda(X)$ as $\mathrm{corank}_\Lambda(S)$. If S is a cofinitely generated, torsion Λ-module, then we define $\lambda(S)$ to be $\lambda(X)$, $\mu(S)$ to be $\mu(X)$. It is useful to note that if X is torsion-free as a Λ-module, then S is divisible as a Λ-module (i.e. $\theta S = S$ for every nonzero

$\theta \in \Lambda$). Here are the most useful results.

Proposition 2.2.8. *Suppose that S is a discrete, p-primary, abelian group with a continuous action of Γ. Regard S as a Λ-module. Then*

1. *$S = 0 \Longleftrightarrow S^\Gamma = 0 \Longleftrightarrow S[\mathfrak{m}] = 0$.*
2. *S is a cofinitely generated Λ-module $\Longleftrightarrow S[\mathfrak{m}]$ is finite .*
3. *S is a cofinitely generated, cotorsion Λ-module $\Longleftrightarrow S[\theta]$ is finite for some $\theta \in \mathfrak{m}$.*

Proposition 2.2.9. *Suppose that S satisfies the assumptions in proposition 2.2.8. If S^Γ is finite, then S is a cofinitely generated, cotorsion Λ-module.*

Proposition 2.2.10. *Suppose that S is a cofinitely generated, cotorsion Λ-module. Then $S_{div} = (\mathbf{Q}_p/\mathbf{Z}_p)^\lambda$ as a $\mathbf{Z}_p$-module, where $\lambda = \lambda(S)$. The quotient S/S_{div} has bounded exponent.*

The proofs are rather easy, based on corollary 2.2.2 , propositions 2.2.4 and 2.2.5.

2.3 Growth theorems for quotients of Γ-modules.

Now let X be a finitely generated, torsion Λ-module. It can of course happen that $X/\omega_n X$ is infinite for some values of n. This corresponds to the possibility that some of the eigenvalues of γ_o acting on the vector space $V = X \otimes_{\mathbf{Z}_p} \overline{\mathbf{Q}_p}$ are p^n-th roots of unity. (Of course, the corresponding eigenvectors may be in the vector space $V \otimes_{\mathbf{Q}_p} \overline{\mathbf{Q}_p}$ obtained by extending scalars to the algebraic closure $\overline{\mathbf{Q}_p}$ of $\mathbf{Q}_p$.) The order of such roots of unity is certainly bounded. (To see this, note that if p^t is the order of some such root of unity, then it is clear that $\phi(p^t) = p^t - p^{t-1} \leq \lambda(X)$. This gives a bound on t.) In the ring Λ, we can write $\omega_n = \prod_{i=0}^{n} \phi_i$, where $\phi_i = \omega_i/\omega_{i-1}$ for $i > 0$ and $\phi_0 = \omega_0 = T$. For $m \geq n \geq 0$, define $\nu_{m,n} = \prod_{n<i\leq m} \phi_i$, which we take to be 1 if $m = n$. Thus, $\omega_m = \omega_n \nu_{m,n}$. Note that the roots of the polynomial ϕ_i are the numbers $\zeta - 1$, where ζ is a primitive p^i-th root of unity.

We fix an integer n_o sufficiently large so that no p^t-th root of unity is an eigenvalue of γ_o acting on V for $t > n_o$. Then it is easy to verify that $X/\nu_{n,n_o} X$ is finite for all $n \geq n_o$. We will prove the following proposition.

Proposition 2.3.1. *Let X be a finitely generated, torsion Λ-module. Choose n_o so that $X/\nu_{n,n_o}X$ is finite for all $n \geq n_o$. Let $\lambda = \lambda(X)$, $\mu = \mu(X)$. Then we have*

$$|X/\nu_{n,no}X| = p^{\lambda n + \mu p^n + \nu}$$

for all $n \gg 0$, where ν is some integer.

Proof. Suppose that we have an exact sequence of torsion Λ-modules

$$0 \longrightarrow X_1 \longrightarrow X_2 \longrightarrow X_3 \longrightarrow 0$$

We first show that the validity of the above theorem for X_1 and X_3 implies the validity for X_2. It is easy to see that

$$\lambda(X_2) = \lambda(X_1) + \lambda(X_3), \qquad \mu(X_2) = \mu(X_1) + \mu(X_3).$$

Choose n_o sufficiently large so that the $X_2/\nu_{n,n_o}X_2$ is finite for all $n \geq n_o$. Then the same thing will be true for X_1 and X_3. The snake lemma gives

$$\begin{aligned} 0 \longrightarrow X_1[\nu_{n,n_o}] &\longrightarrow X_2[\nu_{n,n_o}] \longrightarrow X_3[\nu_{n,n_o}] \longrightarrow X_1/\nu_{n,n_o}X_1 \\ &\longrightarrow X_2/\nu_{n,n_o}X_2 \longrightarrow X_3/\nu_{n,n_o}X_3 \longrightarrow 0. \end{aligned}$$

Note that each ϕ_i is in $\mathfrak{m}$ and so $\nu_{n,n_o} \in \mathfrak{m}^t$ for $t = n - n_o + 1$. Hence, it is clear that if $n \gg n_o$, then $X_i[\nu_{n,n_o}] = Z_i$ for $i = 1, 2, 3$, where Z_i denotes the maximal finite Λ-submodule of X_i. Thus the terms in the first half stabilize for $n \gg 0$, and therefore the image of the fourth arrow will have order $|Z_1||Z_3|/|Z_2| = p^a$, say. This implies that

$$|X_2/\nu_{n,n_o}X_2| = |X_1/\nu_{n,n_o}X_1||X_3/\nu_{n,n_o}X_3|p^{-a}$$

for $n \gg 0$. It is then clear that proving proposition 3 for $X = X_1$ and $X = X_3$ implies it for $X = X_2$.

Based on this last remark and proposition 2.2.4, it is enough to consider the following three special cases: *(a)* X is finite, *(b)* X has exponent p, and *(c)* X is a free $\mathbf{Z}_p$-module of finite rank.

Case (a): This is quite easy. If X is finite, then ν_{n,n_o} annihilates X for $n >> n_o$ and so $X/\nu_{n,n_o}X = X$ has constant order $|X|$ for such n. The proposition is valid since $\lambda(X) = \mu(X) = 0$.

Case (b). If X has exponent p, then one can consider X as a finitely-generated module over $\mathbf{F}_p[[T]]$, which is a principal ideal domain. Therefore,

X is isomorphic to $\mathbf{F}_p[[T]]^r \times Z$, where $r \geq 0$ and Z is the $\mathbf{F}_p[[T]$-torsion submodule of X. Noting that $\mathbf{F}_p[[T]]/(T^d)$ is finite (of order p^d) for any integer $d > 0$, it follows that Z is finite too. Thus it is enough to just consider the special case $X = F_p[[T]]$. We then have $\lambda(X) = 0$, $\mu(X) = 1$. Note that ϕ_i has degree $p^i - p^{i-1}$. Hence ν_{n,n_o} has degree $p^n - b$ for $n > n_o$, where b is a constant. Also, ν_{n,n_o} is not divisible by p in Λ. It follows that $X/\nu_{n,n_o}X$ has order p^{p^n-b} for $n > n_o$, again verifying the proposition since $\lambda(X) = 0$ and $\mu(X) = 1$.

Case (c). Assume that X is a free $\mathbf{Z}_p$-module of rank l. Multiplication by T defines a $\mathbf{Z}_p$-linear endomorphism of X. Let $\alpha_1, \ldots, \alpha_l$ denote the eigenvalues (in $\overline{\mathbf{Q}}_p$) of this endomorphism, counting multiplicity, which are just the roots of the characteristic polynomial $g(t) = det(tI - T)$. It is clear that T acts nilpotently on X/pX, an $\mathbf{F}_p$-vector space of dimension l. The characteristic polynomial for the endomorphism T of X/pX is t^l and hence $g(t) \equiv t^l \pmod{p\mathbf{Z}_p[t]}$. This implies the important fact that $|\alpha_i|_p < 1$ for $1 \leq i \leq l$.

Thus, if $f(T) \in \Lambda$, then $f(\alpha_i) \in \overline{\mathbf{Q}}_p$ is defined Furthermore, multiplication by $f(T)$ defines an endomorphism of X which has eigenvalues $f(\alpha_1), \ldots, f(\alpha_l)$. The determinant of this endomorphism is $\prod_{i=1}^{l} f(\alpha_i)$. The determinant of a matrix over $\mathbf{Z}_p$ determines the order of the cokernel. To be precise, if some α_i is a root of $f(T)$, then $X/f(T)X$ is infinite. Otherwise, write $\prod_{i=1}^{l} f(\alpha_i) = p^a u$, where $u \in \mathbf{Z}_p^{\times}$. Then $|X/f(T)X| = p^a$.

We take $f(T) = \nu_{n,n_o} = \prod_{n_o < j \leq n} \phi_j$. The roots of $\phi_j(T)$ are the numbers $\zeta - 1$, where ζ varies over the primitive p^j-th roots of unity (in $\overline{\mathbf{Q}}_p$). Recall that $\mathrm{ord}_p(\zeta - 1) = 1/(p^j - p^{j-1})$ for all such roots of unity. Let α be any one of the α_i's. We have

$$\phi_j(\alpha) = \prod_{\zeta} (\alpha - (\zeta - 1)))$$

where the product is over all the primitive p^j-th roots of unity ζ. Our choice of n_o implies that α is not a root of ϕ_j for $j > n_o$. Obviously, if j is sufficiently large (say, $j \geq n_1$), then $\mathrm{ord}_p(\zeta - 1) < \mathrm{ord}_p(\alpha)$ for all $\alpha \in \{\alpha_1, ..., \alpha_l\}$. The number of factors in the product defining $\phi_j(\alpha)$ is $p^j - p^{j-1}$. Each of these factors has valuation equal to $\mathrm{ord}_p(\zeta - 1)$ for $j \geq n_1$. Thus, for such j, we have

$$\mathrm{ord}_p\big(\phi_j(\alpha)\big) = 1$$

and so $\mathrm{ord}_p\big(\nu_{n,n_o}(\alpha_i)\big) = n + c_i$ for $n > n_1$, where $c_i \in \mathbf{Z}$. It follows that

$|X/\nu_{n,n_o}X| = p^{ln+d}$ for $n \gg 0$, where $d \in \mathbf{Z}$. Since $\lambda(X) = l$ and $\mu(X) = 0$, we have verifies the proposition for case (c).

As we already remarked, proposition 2.3.1 follows from these separate calculations. ■

It may be worthwhile to discuss one simple case of Proposition 2.3.1 explicitly. Assume that p is odd. Suppose that $X = \mathbf{Z}_p$. The action of Γ on X would then be given by a continuous homomorphism $\kappa : \Gamma \to 1 + p\mathbf{Z}_p$. Thus $\kappa(\gamma) = 1 + \alpha$, where $\alpha \in p\mathbf{Z}_p$. (In fact, α is the eigenvalue of $T = \gamma - 1$ acting on X.) We assume that the action of Γ is nontrivial. That is, $\alpha \neq 0$. Suppose that $\mathrm{ord}_p(\alpha) = a$. Then $X/TX = X/\alpha X$ is cyclic of order p^a. Now $1 + p\mathbf{Z}_p \cong \mathbf{Z}_p$ as a topological group and the image $\kappa(\Gamma)$ will be the subgroup $1 + p^a\mathbf{Z}_p$, which is the unique subgroup of $1 + p\mathbf{Z}_p$ of index p^{a-1}. The image $\kappa(\Gamma_n)$ will be the unique subgroup of index p^{n+a-1}. That is, $\mathrm{ord}_p(\kappa(\gamma^{p^n}) - 1) = p^{n+a}$. It follows that $X/\omega_n X$ is cyclic of order p^{n+a}. This is true for *all* $n \geq 0$. Thus, in the notation of proposition 2.3.1, we have $\lambda = \lambda(X) = 1$, $\mu = \mu(X) = 0$, and $\nu = a$.

Another result which sometimes will be useful is the following proposition. Any integer n_o satisfying the property in proposition 2.3.1 will also have the property that $\mathrm{rank}_{\mathbf{Z}_p}(X/\omega_n X) = \mathrm{rank}_{\mathbf{Z}_p}(X/\omega_{n_o}X)$ for all $n \geq n_o$. The two properties are equivalent. The following result concerns the growth of the torsion subgroup of $X/\omega_n X$.

Proposition 2.3.2. *Suppose that X is a finitely generated, torsion Λ-module. Choose n_o as above. Let $\lambda_o = \mathrm{rank}_{\mathbf{Z}_p}(X/\omega_{n_o}X)$. Then, for $n \gg 0$, we have*

$$|(X/\omega_n X)_{\mathrm{tors}}| = p^{(\lambda-\lambda_o)n+\mu p^n+\nu},$$

where $\lambda = \lambda(X)$, $\mu = \mu(X)$, and ν is some integer.

Proof. Let $Y = \omega_{n_o}X$. Then $\lambda(Y) = \lambda - \lambda_o$. We have $\omega_n X = \nu_{n,n_o}Y$ for $n \geq n_o$. Also, $Y/\nu_{n,n_o}Y$ is finite for all such n. We have an exact sequence

$$0 \to Y/\nu_{n,n_o}Y \to (X/\omega_n X)_{\mathrm{tors}} \to (X/Y)_{\mathrm{tors}} \to 0$$

The result follows immediately by applying proposition 2.3.1 to Y. ■

One further result concerns the order of quotients of the form $X/(T-\beta)X$, where $\beta \in p\mathbf{Z}_p$.

Proposition 2.3.3. *Suppose that X is a finitely generated, torsion Λ-module and that $f_X(\beta) \neq 0$. Then $X/(T-\beta)X$ is finite. If X has no nonzero, finite*

Λ-*submodules, then*

$$\mathrm{ord}_p\big(|X/(T-\beta)X|\big) \;=\; \mathrm{ord}_p\big(f_X(\beta)\big).$$

If $f_X(\beta)=0$, *then* $X/(T-\beta)X$ *is infinite.*

Proof. We can write $f_X(T)=p^{\mu(X)}g_X(T)$, where $g_X(T)$ is a monic polynomial in T. Thus, $f_X(\beta)=p^{\mu(X)}g_X(\beta)$. It is clear from the proof of proposition 2.3.1 that $X/(T-\beta)X$ is finite since β is not a root of $g_X(T)$. To calculate the order of $X/(T-\beta)X$, consider the exact sequence

$$0 \longrightarrow Y \longrightarrow X \longrightarrow X/Y \longrightarrow 0$$

where Y is the $\mathbf{Z}_p$-torsion submodule of X. Thus, $Y = X[p^t]$ for some $t \geq 0$. We assume that X has no nonzero Λ-submodules. If one considers the maps induced by multiplication by p^{i-1} on X for $i \geq 1$, then one sees that $X[p^i]/X[p^{i-1}]$ is isomorphic to a Λ-submodule of X and hence also has no nonzero Λ-submodules. This means that each $X[p^i]/X[p^{i-1}]$ is free as a $\mathbf{F}_p[[T]]$-module. On the other hand, X/Y is a free $\mathbf{Z}_p$-module.

If one then applies the snake lemma as in the proof of proposition 2.3.1, one can reduce the proof to the two cases where either $X \cong \mathbf{F}_p[[T]]$ or X is a free $\mathbf{Z}_p$-module of rank l. One has $X/(T-\beta)X \cong \mathbf{F}_p$ and $\mu(X)=1$ in the first case. The proposition is valid in that case. In the second case, let $\alpha_1, ..., \alpha_l$ denote the roots of $f_X(T)=g_X(T)$. It is clear that the index of $(T-\beta)X$ in X is infinite if and only if β is equal to one of the α_i's. If we assume that $f_X(\beta) \neq 0$, then that index is finite and has the same valuation as the determinant of the operator $T-\beta$ on X, which is

$$\prod_{i=1}^{l}(\alpha_i-\beta) \;=\; \pm\, f_X(\beta),$$

proving the formula in the proposition. ■

We will now prove some results about the group-theoretic structure of the quotients of X occurring in propositions 2.3.1 and 2.3.2, starting first with the case where $\mu(X)=0$.

Proposition 2.3.4. *Let* X *be a finitely generated, torsion* Λ*-module. Choose* n_o *so that* $X/\nu_{n,n_o}X$ *is finite for all* $n \geq n_o$. *Assume that* $\mu(X)=0$. *Then, for all* $n \gg 0$, *there is an isomorphism*

$$X/\nu_{n,n_o}X \cong \prod_{i=1}^{\lambda}\mathbf{Z}/p^{n+c_i}\mathbf{Z} \times C,$$

where $c_1, \ldots, c_\lambda$ are certain integers and C is isomorphic to the maximal, finite, Λ-submodule of X.

Proof. As a $\mathbf{Z}_p$-module, we have $X \cong U \times Z$, where $U \cong \mathbf{Z}_p^\lambda$. Here Z is a Λ-submodule of X, but U is just a $\mathbf{Z}_p$-submodule. Suppose that t is chosen so that $p^t Z = 0$. Then $p^t U = p^t X$ is a Λ-submodule of X, and has finite index. Hence $\nu_{n,n_o} X \subset p^t U$ for $n \gg n_o$. Note that

$$X/\nu_{n,n_o} X \cong U/\nu_{n,n_o} X \times Z$$

as a $\mathbf{Z}_p$-module. Note that $\nu_{n,n_o} X$ is a free Z_p-module of rank λ. We will show below that

$$\nu_{n+1,n_o} X = p\nu_{n,n_o} X \tag{37}$$

for $n \geq n_1$, where n_1 is chosen in a certain way. Thus, for such n, if $U/\nu_{n,n_o} X$ is isomorphic to a direct product of cyclic groups of orders $p^{a_1}, ..., p^{a_\lambda}$, then $U/\nu_{n+1,n_o} X$ will be isomorphic to a direct product of cyclic groups of orders $p^{a_1+1}, ..., p^{a_\lambda+1}$. The proposition will then follow by induction.

First choose $n_o' \geq n_o$ so that $X' = \nu_{n_o',n_o} X \subset p^t U$. Then Γ acts continuously on the quotient group $X'/p^2 X'$. Choose $n_1 \geq n_o'$ so that the subgroup $\Gamma^{p^{n_1}}$ acts trivially on this quotient. If $i > n_1$, then $\phi_i = \sum_{j=0}^{p-1} \gamma_o^{jp^{i-1}}$ acts on $X'/p^2 X'$ as multiplication by p. A simple application of Nakayama's lemma (for $\mathbf{Z}_p$-modules) implies that $\phi_i X' = pX'$. Let $n \geq n_1$. Then, taking $i = n+1$ and multiplying by $\nu_{n,n_o'}$, we obtain the identity (6). ■

If A is any finite abelian group, its exponent is the smallest positive integer m such that $A[m] = A$, or equivalently, the least common multiple of the orders of elements in A. We will refer to $\dim_{\mathbf{F}_p}(A[p])$ as the p-rank of A. The p-rank of A is also clearly equal to $\dim_{\mathbf{F}_p}(A/pA)$.

Proposition 2.3.5. *Let X be a finitely generated, torsion Λ-module. Choose n_o so that $X/\nu_{n,n_o} X$ is finite for all $n \geq n_o$.*

1. *If $\lambda(X) > 0$, then the exponent of $X/\nu_{n,n_o} X$ is equal to p^{n+c} for all $n \gg 0$, where c is some integer. If $\lambda(X) = 0$, then the exponent of $X/\nu_{n,n_o} X$ is bounded and becomes constant for $n \gg 0$.*

2. *Let $r = \mathrm{rank}_{\mathbf{F}_p[[T]]}(X[p])$. Then the p-rank of $X/\nu_{n,n_o} X$ is equal to $rp^n + c$ for $n \gg 0$, where c is some constant.*

Proof. The first statement follows immediately from proposition 2.3.4 if $\mu(X) = 0$. Note also that the proof of that proposition shows the following

(again under the assumption that $\mu(X) = 0$): Let $x \in X$. Assume that $x \notin Z$, the maximal finite Λ-submodule of X. Then the image of x in $X/\nu_{n,n_o}X$ has order p^{n+c} for all $n \gg 0$, where c is a certain integer (depending on x). We will use this observation in the general case.

In general, let p^t denote the exponent of $Y = X_{\text{tors}}$. Then p^tX is a free $\mathbf{Z}_p$-module of rank $\lambda(X)$. The maximal finite Λ-submodule of X/p^tX is of the form X_o/p^tX for a uniquely determined Λ-submodule X_o of X containing p^tX. Since $p \nmid \nu_{n,n_o}$, it is clear that $(X/X_o)[\nu_{n,n_o}] = 0$. This implies that

$$\nu_{n,n_o}X \cap X_o = \nu_{n,n_o}X_o \tag{38}$$

for any $n \geq n_o$.

Let $x \in X$. Assume that $p^tx \neq 0$. Since $\lambda(X) > 0$, the image of x in $X/\nu_{n,n_o}X$ has unbounded order as $n \to \infty$. Now $p^tx \in X_o$ and its images in $X/\nu_{n,n_o}X$ and in $X_o/\nu_{n,n_o}X_o$ have the same order for $n \geq n_o$ according to (38). This order is p^{n+c} if $n \gg 0$, for some c. Thus, the order of the image of x in $X/\nu_{n,n_o}X$ will be p^{n+c+t} for sufficiently large n. The stated result follows immediately because X is finitely generated as a Λ-module. If $x_1, ..., x_d$ is a set of generators, then the exponent of $X/\nu_{n,n_o}X$ will be the maximum of the orders of the images of $x_1, ..., x_d$ in that quotient.

We now prove the second statement. One can equivalently define r as $\text{rank}_{\mathbf{F}_p[[T]]}(X/pX)$. This follows from the exact sequence

$$0 \to X[p] \to X \to X \to X/pX \to 0$$

since the μ-invariant is additive in exact sequences, and so $\mu(X[p]) = \mu(X/pX)$. Note that

$$(X/\nu_{n,n_o}X)/p(X/\nu_{n,n_o}X) \cong X/(\nu_{n,n_o}X + pX) \cong (X/pX)/\nu_{n,n_o}(X/pX)$$

The stated result follows from proposition 2.3.1, since the order of a group of exponent p determines its dimension over $\mathbf{F}_p$. ■

If $\mu(X) > 0$, then the actual structure of the quotients $X/\nu_{n,n_o}X$ would be somewhat more complicated. We will be content to state the following result, omitting the proof. If one uses the structure theorem for Λ-modules to be proved in Chapter 5, then the result is not hard to prove. We use the following notation. Suppose that $\{A_n\}$ and $\{B_n\}$ are two sequences of groups, defined for all $n \geq n_o$, say. We will write $\{A_n\} \approx \{B_n\}$ if there exists

a sequence of group homomorphisms $f_n : A_n \to B_n$ defined for $n \geq n_o$ such that $\ker(f_n)$ and $\operatorname{coker}(f_n)$ are finite and of bounded order as n varies.

Proposition 2.3.6. *Let X be a finitely generated, torsion Λ-module. Choose n_o so that $X/\nu_{n,n_o}X$ is finite for all $n \geq n_o$. Let $\lambda = \lambda(X)$ and $\mu = \mu(X)$. Let $\mu_1, \ldots, \mu_r$ be the finer μ-invariants for X. For $n \geq n_o$, let $A_n = X/\nu_{n,n_o}X$ and let $B_n = (\mathbf{Z}/p^n\mathbf{Z})^\lambda \times \prod_{j=1}^r (\mathbf{Z}/p^{\mu_j}\mathbf{Z})^{p^n}$. Then $\{A_n\} \approx \{B_n\}$.*

Note that the group B_n in this proposition has order $p^{\lambda n + \mu p^n}$. It is also worth pointing out that knowing the sequence of groups $\{A_n\}$ (up to the equivalence relation $\approx$) is sufficient to determine the invariants $\lambda(X)$, $\mu(X)$, r, and $\mu_1, \ldots, \mu_r$.

2.4 Proof of Iwasawa's growth formula

We will prove Iwasawa's theorem in complete generality in this section. If we assume RamHyp(1), then the result follows quickly from earlier results. In this case, we know that $X/\omega_n X$ is finite for all n. As we have already pointed out, Nakayama's lemma and proposition 2.2.5 imply that X must be a finitely generated, torsion Λ-module. Now the power of p dividing h_n is equal to $|X/\omega_n X|$ by proposition 2.1.5. The growth for these quantities is then given by either proposition 2.3.1 or 2.3.2, and is just as described by Iwasawa's growth formula.

As a first step to the complete proof, we prove the following important result.

Proposition 2.4.1. *Suppose that F_∞/F be a $\mathbf{Z}_p$-extension and let L_∞ denote its pro-p-Hilbert class field. Then $X = \operatorname{Gal}(L_\infty/F_\infty)$ is a finitely generated, torsion Λ-module.*

Proof. If a prime v of F is ramified in the $\mathbf{Z}_p$-extension F_∞/F, then the corresponding inertia subgroup I_v of $\operatorname{Gal}(F_\infty/F)$ has finite index in $\Gamma = \operatorname{Gal}(F_\infty/F)$. By proposition 1, there are only finitely many such v's and so the intersection of these inertia subgroups has finite index in Γ. That is, $\bigcap_v I_v = \Gamma_{n_o}$ for some $n_o \geq 0$. Every prime of F_{n_o} which is ramified in F_∞/F_{n_o} must be totally ramified. Let t be the number of such primes.

Suppose that $n \geq n_o$. Let K_n denote the maximal abelian extension of F_n contained in L_∞. Thus, $\operatorname{Gal}(L_\infty/K_n) = \omega_n X$. Let η be any prime of F_n ramified in F_∞/F_n. There are t such primes, which we denote by

$\eta_1, \ldots, \eta_t$. Since L_∞/F_∞ is unramified, only these primes are ramified in the extension K_n/F_n. The corresponding inertia subgroups of $\mathrm{Gal}(K_n/F_n)$ are all isomorphic to $\mathbf{Z}_p$ and they generate the subgroup $\mathrm{Gal}(K_n/L_n)$. Thus, $\mathrm{Gal}(K_n/L_n)$ is a finitely generated $\mathbf{Z}_p$-module which has rank $\leq t$. It has finite index in $\mathrm{Gal}(K_n/F_n)$ since L_n/F_n is a finite extension. Therefore, $\mathrm{Gal}(K_n/F_n)$ is also a finitely generated $\mathbf{Z}_p$-module with the same rank.

It follows that $X/\omega_n X = \mathrm{Gal}(K_n/F_\infty)$ is finitely generated as a $\mathbf{Z}_p$-module and has rank $\leq t-1$. Nakayama's Lemma implies that X is finitely generated as a Λ-module. On the other hand, lemma 2.2.6 implies that

$$\mathrm{rank}_{\mathbf{Z}_p}(X/\omega_n X) \geq rp^n$$

for all n, where $r = \mathrm{rank}_\Lambda(X)$. It follows that $r = 0$. That is, X is torsion as a Λ-module. ■

As the above proof might suggest, it is not always true that the quotients $X/\omega_n X$ are finite. In a later chapter we will give some examples of this phenomenon and study it in some detail. However, as noted in proposition 2.3.1, if n_o is sufficiently large, then the quotients $X/\nu_{n,n_o}X$ will be finite for all $n \geq n_o$. In fact, as we will see in the proof of the next result, one can take n_o just as in the proof of proposition 2.4.1. It then turns out that $[L_n : F_n]/|X/\nu_{n,n_o}X|$ becomes constant for $n \gg 0$. These facts follow easily from the following proposition, which is somewhat more precise. The proof involves keeping careful track of the inertia subgroups of $\mathrm{Gal}(L_\infty/F_n)$ for the primes over p.

Proposition 2.4.2. *Let F_∞/F be a $\mathbf{Z}_p$-extension. Choose n_o so that all the primes of F_{n_o} which are ramified in F_∞/F_{n_o} are totally ramified in that extension. Let $X = \mathrm{Gal}(L_\infty/F_\infty)$ and $Y = \mathrm{Gal}(L_\infty/L_{n_o}F_\infty)$. Then*

$$X/\nu_{n,n_o}Y = \mathrm{Gal}(L_n/F_n)$$

for all $n \geq n_o$.

Proof. Let $n \geq n_o$. Let L_n^* denote the maximal unramified, extension of F_n contained in L_∞. Then L_n^*/F_n is Galois. Obviously, $L_n \subset L_n^*$. But since at least one prime of F_n is totally ramified in F_∞/F_n, we have $L_n^* \bigcap F_\infty = F_n$. It therefore follows that $\mathrm{Gal}(L_n^*/F_n) \cong \mathrm{Gal}(L_n^*F_\infty/F_\infty)$, which is clearly abelian. Thus, $L_n^* = L_n$.

Let $G_n = \mathrm{Gal}(L_\infty/F_n)$. Let H_n be the smallest closed subgroup of G_n containing all the inertia subgroups of G_n. The primes of F_n ramified in

L_∞/F_n are the same as those ramified in F_∞/F_n, and we denote them by $\eta_1, \ldots, \eta_t$. The number t of such primes is independent of n because $n \geq n_o$. Each inertia subgroup for a prime of L_∞ above one of the η_i's is canonically isomorphic to Γ_n (by the restriction map). We have $L_n^* = L_\infty^{H_n}$ by definition and therefore $H_n = \mathrm{Gal}(L_\infty/L_n)$.

Let $Y_n = H_n \bigcap X$. Then $Y_n = \mathrm{Gal}(L_\infty/L_n F_\infty)$. In particular, Y (as defined in the proposition) is just Y_{n_o}. It is also clear that $X/Y_n = \mathrm{Gal}(L_n/F_n)$. So it remains just to prove that $Y_n = \nu_{n,n_o} Y_{n_o}$ for all $n \geq n_o$.

Let R denote the set of primes η of L_∞ ramified in the extension L_∞/F_{n_o}. For each $\eta \in R$, let I_η denote the corresponding inertia subgroup of G_{n_o}. Then, as we noted above, $I_\eta = \Gamma_{n_o} = \mathbf{Z}_p$. For $n \geq n_o$, the inertia subgroup of G_n for η will be $I_\eta \bigcap G_n$. This will be the unique subgroup of I_η of index p^{n-n_o}, namely I^{p^m} where we put $m = n - n_o$ for brevity.

Choose a topological generator γ_{n_o} for Γ_{n_o}. For each $\eta \in R$, let g_η denote the element of I_η such that $g_\eta|_{F_\infty} = \gamma_{n_o}$. If η, $\eta' \in R$, then g_η and $g_{\eta'}$ are in the same coset in G_{n_o}/X and so $y(\eta, \eta') = g_\eta g_{\eta'}^{-1}$ is in X. Furthermore, the definitions imply that Y is the smallest closed subgroup of X containing all the $y(\eta, \eta')$'s, where we allow (η, η') to vary over $R \times R$. Similarly, it follows that Y_n is the smallest closed subgroup of X containing the elements $y_n(\eta, \eta') = g_\eta^{p^m} g_{\eta'}^{-p^m}$ for $(\eta, \eta') \in R \times R$, where m is as above.

The rest of this proof will be somewhat clearer if we switch to a multiplicative notation for Y. Thus, if $y \in Y$ and $\theta \in \Lambda$, we will write y^θ in place of θy. We will now do a simple calculation in G_{n_o} to show that $y(\eta, \eta')^{\nu_{n,n_o}} = y_n(\eta, \eta')$. This implies that $Y^{\nu_{n,n_o}} = Y_n$, from which proposition 2.4.2 follows.

Let $a = g_\eta$, $b = g_{\eta'}$, $y = ab^{-1} = y(\eta, \eta')$, and $\gamma = \gamma_{n_o}$. Note that $\nu_{n,n_o} = \sum_{i=0}^{p^m-1} \gamma^i$. Also, since $b|_{F_{n_o}} = \gamma$, we have $b^i y b^{-i} = y^{\gamma^i}$ for $0 \leq i < p^m$. Therefore,

$$y^{\nu_{n,n_o}} = \prod_{i=0}^{p^m-1} b^i y b^{-i} = (yb)^{p^m} b^{-p^m} = a^{p^m} b^{-p^m} = y_n(\eta, \eta')$$

as we stated above. ■

The proof of Iwasawa's growth formula can now be easily completed. Since Y is a Λ-submodule of X and X/Y is finite, we have $\lambda(Y) = \lambda(X)$ and $\mu(Y) = \mu(X)$. Also,

$$h_n^{(p)} = |\mathrm{Gal}(L_n/F_n)| = |X/Y||Y/\nu_{n,n_o} Y|$$

for $n \geq n_o$ and so proposition 2.4.2 combined with proposition 2.3.1 (applied to Y) establishes the growth formula with $\lambda = \lambda(X)$, $\mu = \mu(X)$.

Remark 2.4.3. Assume that RamHyp(1) holds for the $\mathbf{Z}_p$-extension F_∞/F. One can then take $n_o = 0$ in proposition 2.4.2 and so $Y = \mathrm{Gal}(L_\infty/L_0F_\infty)$. The Galois group $G = \mathrm{Gal}(L_\infty/F)$ now acts transitively on the set R occurring in the proof of proposition 2.4.2. Thus, the inertia groups I_η's are conjugate in G and the elements g_η form a single conjugacy class of G. Therefore, $y(\eta, \eta')$ is a commutator in G. That is, $Y \subset G'$. On the other hand, $G/Y = \mathrm{Gal}(L_0F_\infty/F)$ is abelian. This implies that $G' \subset Y$. Hence $Y = G' = TX$. Therefore, it follows that $Y_n = \nu_{n,0}Y = \omega_n X$ for all $n \geq 0$, which is essentially the content of proposition 2.1.5.

There are a number of interesting and useful consequences of proposition 2.4.2 in addition to establishing the growth formula. To state some of these, we introduce the following ramification hypothesis:

RamHyp(2): *Every prime of F which is ramified in F_∞/F is totally ramified.*

This simply means that we can take $n_o = 0$. It will simplify the statement of the following results. They could be applied to an arbitrary $\mathbf{Z}_p$-extension just by replacing the base field F by F_{n_o}.

Proposition 2.4.4. *Suppose that RamHyp(2) is satisfied for the $\mathbf{Z}_p$-extension F_∞/F. Then $X/\nu_{n,0}X$ is finite for all $n \geq 0$. That is, $f_X(\zeta - 1) \neq 0$ for all $\zeta \in \mu_{p^\infty}$, except possibly $\zeta = 1$.*

Proof. The corresponding statement for $Y = \mathrm{Gal}(L_\infty/L_0F_\infty)$ is part of proposition 2.4.2. Since $[X : Y]$ is finite, the first statement in the proposition follows. The second statement then follows from a previous remark. ■

Proposition 2.4.5. *Suppose that RamHyp(2) is satisfied for the $\mathbf{Z}_p$-extension F_∞/F. Assume that p does not divide the class numbers of F and F_1. Then p does not divide the class number of F_n for any $n \geq 0$.*

Proof. The assumption implies that $X = Y = \nu_{1,0}Y$. Now $\nu_{1,0} \in \mathfrak{m}$. Therefore, Nakayama's lemma implies that $Y = 0$. Hence $X = 0$ too. The conclusion follows from this. ■

Remark 2.4.6. If one just assumes that the power of p dividing the class numbers of F and F_1 are equal, in addition to RamHyp(2), then one has $Y = \nu_{1,0}Y$. It again follows that $Y = 0$. That is, X is finite and the power

of p dividing the class number of F_n is equal to $|X|$ for all $n \geq 0$. Examples exist where this actually happens.

If one combines propositions 2.3.4, 2.3.5, and 2.4.4, one obtains information about the group-theoretic structure of the p-primary subgroup A_n of C_{F_n}, summarized in the following proposition. We let $\lambda = \lambda(X)$, $\mu = \mu(X)$, and $r = \text{rank}_{F_p[[T]]}(X[p])$.

Proposition 2.4.7. *Let F_∞/F be a $\mathbf{Z}_p$-extension. Then*

a. The exponent of A_n will be p^{n+c} for $n \gg 0$, where c is some integer.

b. The p-rank of A_n will be $rp^n + c$, where c is some integer.

c. If $\mu = 0$, then $A_n \cong \prod_{i=1}^{\lambda} \mathbf{Z}/p^{n+c_i}\mathbf{Z} \times C$ for $n \gg 0$, where $c_1, ..., c_\lambda$ are certain integers and C is a certain finite group.

Proof. Using the notation of proposition 2.4.2, the results concern the structure of the quotients $X/\nu_{n,n_o}Y$ for $n \gg 0$. We already have similar results for the quotients $Y/\nu_{n,n_o}Y$.

To prove part a, note that since X is a finitely generated Λ-module, it is enough to consider the order of the image of x in $X/\nu_{n,n_o}Y$, where x is an element of X which is not of finite order. For some $t \geq 0$, we have $p^t x \in Y$. As pointed out at the beginning of the proof of proposition 2.3.5, the image of $p^t x$ in $Y/\nu_{n,n_o}Y$ has order p^{n+c} for $n \gg 0$, where c is some integer. Thus, the image of x in $X/\nu_{n,n_o}Y$ will have order p^{n+c+t}, and a follows.

For part b, note that $(X/\nu_{n,n_o}Y)/p(X/\nu_{n,n_o}Y)$ is isomorphic to $\widetilde{X}/\nu_{n,n_o}\widetilde{Y}$, where $\widetilde{X} = X/pX$ and $\widetilde{Y}$ denotes the image of Y under the natural map $X \to \widetilde{X}$. The result then follows from proposition 2.3.1 applied to the Λ-module $\widetilde{Y}$.

The proof of part c is just a slight variation on the proof of proposition 2.3.4, using (37) for Y instead of X. ■

Remark 2.4.8. The group C occurring in the above proposition is isomorphic to the maximal, finite Λ-submodule of X, as the proof shows. Also, one can make the following statement concerning the structure of the A_n's without the assumption that $\mu(X) = 0$. Let $\mu_1, ..., \mu_r$ be the finer μ-invariants for the Λ-module X, which were defined in section 2.3. Then we have

$$A_n \approx (\mathbf{Z}/p^n\mathbf{Z})^\lambda \times \prod_{j=1}^{r} (\mathbf{Z}/p^{\mu_j}\mathbf{Z})^{p^n}$$

This follows immediately from propositions 2.4.2 and 2.3.6.

2.5 Structure of the ideal class group of F_∞.

Suppose that $F_\infty = \bigcup_{n\geq 0} F_n$ is a $\mathbf{Z}_p$-extension of F. For brevity we will denote Cl_{F_n} by C_n. The p-primary subgroup of C_n will be denoted by A_n. For $m \geq n \geq 0$, we will denote the norm map N_{F_m/F_n} (either from C_m to C_n, or from A_m to A_n) by $N_{m,n}$. We will write $J_{n,m}$ for J_{F_m/F_n}.

The ideal class group of F_∞ can be defined as $C_\infty = \varinjlim C_n$, where the direct limit is defined by the maps $J_{n,m}$. The natural map $C_n \to C_\infty$ will be denoted by $J_{n,\infty}$. The main object of study in this section will be $A_\infty = \varinjlim A_n$, (defined by the same maps $J_{n,m}$, restricted to the A_n's). This is the p-primary subgroup of C_∞. There is a natural action of Γ on A_∞, which we can then regard as a discrete Γ-module and hence as a discrete Λ-module. Here is one important result. We denote the Iwasawa invariants λ and μ occurring in the growth formula by $\lambda(F_\infty/F)$ and $\mu(F_\infty/F)$, respectively.

Proposition 2.5.1. *The Λ-module A_∞ is cofinitely generated, cotorsion, and copure of dimension 1. In particular, if $\mu(F_\infty/F) = 0$, then $A_\infty \cong (\mathbf{Q}_p/\mathbf{Z}_p)^\lambda$ as a group, where $\lambda = \lambda(F_\infty/F)$.*

Proof. We will exploit three facts. Let $A_n^* = J_{n,\infty}(A_n)$. Then (1) $A_\infty = \bigcup_{n\geq 0} A_n^*$, (2) the groups A_n^* are isomorphic to quotients of $X = X_{F_\infty/F}$ for $n \gg 0$, and (3) X is a finitely generated, torsion Λ-module.

The assertion (1) is obviously true and (3) is just the content of proposition 2.4.1. For (2), note that the natural restriction map $X \to \mathrm{Gal}(L_n/F_n)$ is surjective when $n \gg 0$. Also, $\mathrm{Gal}(L_n/F_n)$ is canonically isomorphic to A_n for all n. Obviously, A_n^* is isomorphic to a quotient of A_n, and so (2) follows from these remarks. All of these groups have an action of Γ and can be viewed as Λ-modules. The isomorphisms will be as Λ-modules.

Since X is a finitely generated, torsion Λ-module, proposition 2.2.5 implies that $X/\theta X$ is finite for some $\theta \in \mathfrak{m}$. Since A_n^* is a quotient of X for $n \gg 0$ (as a Λ-module), $A_n^*/\theta A_n^*$ is then a quotient of $X/\theta X$. Also, note that $|A_n^*/\theta A_n^*| = |A_n^*[\theta]|$, and so we get the following inequality

$$|A_n^*[\theta]| \leq |X/\theta X|$$

for all $n \gg 0$. It follows from this that $A_\infty[\theta]$ is finite. Proposition 2.2.8 then implies that A_∞ is cofinitely generated and cotorsion as a Λ-module.

We will show that A_∞ is copure of dimension 1 as a Λ-module. This means that the Pontryagin dual of A_∞ has no nonzero, finite Λ-submodules. Such a submodule would correspond to a quotient of A_∞. Let $\widetilde{A}_\infty = A_\infty/B_\infty$ be the maximal, finite Λ-module quotient of A_∞. Thus, B_∞ is the maximal, Λ-submodule of A_∞ which is copure of dimension 1. For each $n \geq 0$, define B_n to be the inverse-image of B_∞ under the map $J_{n,\infty}$. Clearly, B_n is a $\mathrm{Gal}(F_n/F)$-invariant subgroup of A_n. We denote A_n/B_n by $\widetilde{A}_n$. There are maps $\widetilde{J}_{n,m}$, $\widetilde{J}_{n,\infty}$, and $\widetilde{N}_{m,n}$ on these quotient groups induced from the corresponding maps $J_{n,m}$, $J_{n,\infty}$, and $N_{m,n}$ for $m \geq n \geq 0$. It is clear that

$$\widetilde{J}_{n,\infty} : \widetilde{A}_n \to \widetilde{A}_\infty$$

is injective for all n and surjective for $n \gg 0$. Therefore, the maps

$$\widetilde{J}_{n,m} : \widetilde{A}_n \to \widetilde{A}_m$$

are isomorphisms for $m \geq n \gg 0$. The norm maps

$$\widetilde{N}_{m,n} : \widetilde{A}_m \to \widetilde{A}_n$$

will also be isomorphisms for $m \geq n \gg 0$. The surjectivity follows from proposition 1.1.1. In addition, the identity

$$\widetilde{N}_{m,n} \circ \widetilde{J}_{n,m}(\widetilde{a}) = \widetilde{a}^{p^{m-n}}$$

will hold for all $\widetilde{a} \in \widetilde{A}_n$. These observations imply that $\widetilde{A}_n$ is trivial for $n \gg 0$, and hence for all n. This is because, for $m > n$, the map $\widetilde{a} \to \widetilde{a}^{p^{m-n}}$ cannot be an isomorphism of $\widetilde{A}_n$ if that group is nontrivial. It follows that $\widetilde{A}_\infty = 0$ and hence A_∞ is copure of dimension 1, as claimed.

Finally, if $\mu(A_\infty) = 0$, then the Pontryagin dual of A_∞ will be a finitely generated $\mathbf{Z}_p$-module. It is pure of dimension 1 as a Λ-module, and so it must be torsion-free and hence free as a $\mathbf{Z}_p$-module. Hence A_∞ is indeed cofree as a $\mathbf{Z}_p$-module. ■

The ingredients in the above proof have some consequences relating the structure of $X = X_{F_\infty/F}$ and A_∞ as Λ-modules. For example, it follows that

$$\mathrm{Ann}(X) \subset \mathrm{Ann}(A_\infty)$$

To see this, just note that if $\theta \in \mathrm{Ann}(X)$. then θ annihilates the Λ-modules A_n^* for sufficiently large n, and so clearly $\theta \in \mathrm{Ann}(A_\infty)$. It is also not difficult

to see that $\lambda(A_\infty) \leq \lambda(X)$. Using proposition 2.3.6, one can also verify that $\mu(A_\infty) \leq \mu(X)$. The following result allows one to turn these inequalities into equalities.

Proposition 2.5.2. *Let Z be the maximal, finite Λ-submodule of X. Then* $\ker(J_{n,\infty}) \cong Z$ *for* $n \gg 0$. *In particular,* $\ker(J_{n,\infty})$ *has bounded order.*

Proof. Choose n_o so that the $\mathbf{Z}_p$-extension F_∞/F_{n_o} satisfies RamHyp(2). Let $Y = \mathrm{Gal}(L_\infty/L_{n_o}F_\infty)$ as in Proposition 2.4.2. Then we have a canonical homomorphism $\alpha_n : X \to A_n$ which is defined as the composition of the restriction map $X \to \mathrm{Gal}(L_n/F_n)$ with the inverse Artin isomorphism $\mathrm{Art}^{-1}_{L_n/F_n} : \mathrm{Gal}(L_n/F_n) \to A_n$. We then have the following commutative diagram

$$\begin{array}{ccc} X & \longrightarrow & A_n \\ \downarrow{\scriptstyle \nu_{m,n}} & & \downarrow{\scriptstyle J_{n,m}} \\ X & \longrightarrow & A_m \end{array} \tag{39}$$

for $m \geq n \geq 0$. The left vertical arrow is the map $X \to X$ defined by $x \to \nu_{m,n}x$.

To verify the commutativity of the above diagram, suppose that $x \in X$. The commutative diagram (4) in the proof of proposition 1.1.1 implies that

$$N_{m,n}(\alpha_m(x)) = \alpha_n(x)$$

According to proposition 1.2.2, we have

$$J_{n,m}(\alpha_n(x)) = N_{\mathrm{Gal}(F_m/F_n)}(\alpha_m(x)),$$

where $N_{\mathrm{Gal}(F_m/F_n)} : A_m \to A_m$ is the norm operator for $\mathrm{Gal}(F_m/F_n)$, acting on A_m. If g is a generator of $\mathrm{Gal}(F_m/F_n)$, then the norm operator is $\sum_{i=0}^{p^{m-n}-1} g^i$.

Now an element $\gamma \in \Gamma$ acts on A_m via its restriction $\gamma|_{F_m}$. The map $\alpha_m : X \to A_m$ then becomes a Γ-homomorphism. We can lift the norm operator $N_{\mathrm{Gal}(F_m/F_n)}$ on A_m to X as follows. Recall that $1 + T \in \Lambda$ acts on X as γ_o. Let $\gamma_n = \gamma_o^{p^n}$, which is a topological generator for $\mathrm{Gal}(F_\infty/F_n)$. Then $(1+T)^{p^n}$ acts on X as γ_n. Since $g = \gamma_n|_{F_m}$ generates $\mathrm{Gal}(F_m/F_n)$, the element $\sum_{i=0}^{p^{m-n}-1}(1+T)^i \in \Lambda$ is a lifting of $N_{\mathrm{Gal}(F_m/F_n)}$. This element is $\omega_m/\omega_n = \nu_{m,n}$.

We then have $\alpha_m(\nu_{m,n}x) = N_{Gal(F_m/F_n)}(\alpha_m(x))$. This is indeed equal to $J_{n,m}(\alpha_n(x))$, and so diagram (39) is commutative. Now take $m \geq n \geq n_o$.

Define a map

$$j_{n,m} : X/\nu_{n,n_o}Y \to X/\nu_{m,n_o}Y$$

by $j_{n,m}(x + \nu_{n,n_o}Y) = \nu_{m,n}x + \nu_{m,n_o}Y$. It follows that

$$\ker(J_{n,m}) \cong \ker(j_{n,m}) \tag{40}$$

Since $\nu_{n,m}(\nu_{n,n_o}Y) = \nu_{m,n_o}Y$, we have

$$\ker(j_{n,m}) = (X[\nu_{n,m}] + \nu_{n,n_o}Y)/\nu_{n,n_o}Y \cong X[\nu_{n,m}]/(X[\nu_{n,m}] \cap \nu_{n,n_o}Y)$$

Since $m \geq n \geq n_o$, the quotient $X/\nu_{m,n}X$ is finite, and so $X[\nu_{n,m}] \subset Z$. It is clear that we have $X[\nu_{n,m}] = Z$ when $m \gg n$, and therefore

$$\ker(J_{n,\infty}) \cong Z/(Z \cap \nu_{n,n_o}Y) \tag{41}$$

The subgroups $\{\nu_{n,n_o}Y \mid n \geq n_o\}$ form a base of neighborhoods of 0 in X, and so it is also clear that $Z \cap \nu_{n,n_o}Y = 0$ for $n \gg n_o$, proving the stated result. ■

Remark 2.5.3. The prime-to-p part of the C_n's behave quite differently. Suppose that q is a prime, $q \neq p$. Let Q_n denote the q-primary subgroup of C_n. Applying remark 1.2.8 (but for a Galois extension of p-power degree and for the q-primary subgroup of the class groups, one sees that the map $J_{n,m} : Q_n \to Q_m$ is injective and that $J_{n,m}(Q_n)$ is a direct factor Q_m for any $m \geq n$. Thus Q_∞, the direct limit of the Q_n's, will be isomorphic to the direct sum of the finite groups Q_0, $Q_1/J_{0,1}(Q_0)$, $Q_2/J_{1,2}(Q_1)$, ... The behavior of the groups $Q_n/J_{n-1,n}(Q_{n-1})$ is difficult to study. We will describe some results and conjectures about this topic in chapter 4.

2.6 The base field $F = \mathbf{Q}(\mu_p)$.

In this section, we will continue to discuss the important example $F = \mathbf{Q}(\mu_p)$. Remark 1.2.11, propositions 1.4.5 and 1.4.6, and the discussion in between, and section 1.6 already concern this field. It will be an example which we will return to periodically throughout this book. We will now illustrate some of the results of this chapter for the base field F.

The cyclotomic $\mathbf{Z}_p$-extension of $F = \mathbf{Q}(\mu_p)$ is $F_\infty = \mathbf{Q}(\mu_{p^\infty})$. Earlier results in this chapter give us some rough, general picture of the structure of $X = \mathrm{Gal}(L_\infty/F_\infty)$, where L_∞ is the pro-p Hilbert class field of F_∞. This

special case has been studied extensively, both theoretically and computationally, and so we will start with a brief summary of what is now known. We denote the maximal real subfield of F by F^+.

I. *If* $p \nmid h_F$, *then* $X = 0$.

II. *The* μ*-invariant* $\mu(X)$ *vanishes.*

III. *If* $p \nmid h_{F^+}$, *then* X *is a free* $\mathbf{Z}_p$*-module.*

IV. *If* $p \nmid h_{F^+}$, *then* X *is a cyclic* $\mathrm{Gal}(F_\infty/\mathbf{Q})$*-module.*

V. *If* $p < 12,000,000$, *then* $p \nmid h_F$ *and* $\mathrm{rank}_{\mathbf{Z}_p}(X)$ *is equal to the index of irregularity for* p.

The first assertion is an immediate consequence of proposition 2.1.2. The second is a theorem due to B. Ferrero and L. Washington (which is valid more generally for the cyclotomic $\mathbf{Z}_p$-extension of any abelian extension F of $\mathbf{Q}$.) We will give two proofs in Chapter 7. Assuming that result, the third assertion just means that the maximal finite Λ-submodule of X is trivial. That is, X is pure of dimension 1. We will justify this statement below.

The fourth result needs some explanation. The field L_∞ is a Galois extension of $\mathbf{Q}$. Thus X is a normal subgroup of $\mathrm{Gal}(L_\infty/\mathbf{Q})$ and so admits a continuous $\mathbf{Z}_p$-linear action of $G = \mathrm{Gal}(F_\infty/\mathbf{Q})$. If $p \nmid h_{F^+}$, then X is a free $\mathbf{Z}_p$-module (according to III). The assertion that X is cyclic as a G-module then means that X is spanned as a $\mathbf{Z}_p$-module by $\{gx_o \mid g \in G\}$ for some $x_o \in X$. Now the structure of X as a Λ-module reflects the action of $\Gamma = \mathrm{Gal}(F_\infty/F)$ on X. The finite group $\Delta = \mathrm{Gal}(F_\infty/\mathbf{Q}_\infty)$ (which is a subgroup of G) also acts on X. Since G is commutative, the actions of Γ and Δ on X commute. That is, the action of Δ on X is Λ-linear. Therefore, it is natural to consider X as a module for the ring $\Lambda[\Delta]$ - the group ring for Δ over Λ. The assertion in IV then means that X is a cyclic $\Lambda[\Delta]$-module when $p \nmid h_{F^+}$. We will also justify this statement below.

The assertion V is a result of elaborate calculations described in [Buhler et al]. The first such calculations were done in 1967 by Iwasawa and Sims verifying the same assertion for $p < 4001$. As we proceed, it will become clearer how such calculations could be done. It is a conjecture of Vandiver that h_F^+ is never divisible by p.

We return now to assertion III. We must explain why the maximal finite Λ-submodule Z of X is trivial if $p \nmid h_{F^+}$. By proposition 2.5.2, Z is trivial if and only if $J_{n,\infty} : A_n \to A_\infty$ is injective for all sufficiently large n. The n-th

layer in the $\mathbf{Z}_p$-extension F_∞/F is $F_n = \mathbf{Q}(\mu_{p^{n+1}})$. Each of these fields is a CM-field. For $m \geq n \geq 0$, we can apply proposition 1.2.14 to the extension F_m/F_n. $J_{n,m} : A_n \to A_m$ are injective for all $m \geq n \geq 0$. The assumptions in that proposition are clearly satisfied.

The maximal totally real subfield of F_n, which we denote by F_n^+, is a cyclic extension of F^+ of degree p^n. Only one prime of F^+ is ramified in F_n^+/F^+, namely the unique prime above p, and that prime is totally ramified. Hence, proposition 1.1.4 implies that if $p \nmid h_{F^+}$, then $p \nmid h_{F_n^+}$ for all $n \geq 0$. Therefore, in the notation of proposition 1.2.14, we have $A_n^{(\epsilon_0)} = 0$ and hence $A_n = A_n^{(\epsilon_1)}$. It follows that the maps $J_{n,m} : A_n \to A_m$ are injective. Therefore, the maps $J_{n,\infty}$ are injective, and we can then conclude that Z is trivial if $p \nmid h_{F^+}$.

In general, without the assumption that $p \nmid h_{F^+}$, one can still state that the *odd* Δ-components of X have no nonzero, finite Λ-submodules. In other words, for each odd i, the Λ-module $X^{(\omega^i)}$ is pure of dimension 1. Note that Z is Δ-invariant. We are asserting that $Z^{(\omega^i)} = 0$ if i is odd. if one examines the proof of proposition 2.5.2, one sees that the isomorphism is Δ-equivariant. Thus, one has an isomorphism

$$\ker(J_{n,\infty})^{(\omega^i)} \cong Z^{(\omega^i)}$$

for any i. If i is odd, one can again apply proposition 1.2.14 to conclude that $Z^{(\omega^i)}$ is trivial.

Assertion IV is a consequence of proposition 1.4.5 or 1.4.6. Assuming that $p \nmid h_{F^+}$, we know that $A_F^{(\omega^i)}$ is cyclic for each i. Since RamHyp(1) holds for F_∞/F, we have a canonical isomorphism $X/TX \cong A_F$. This isomorphism is Δ-equivariant. We can decompose X as a $\mathbf{Z}_p[\Delta]$-module as follows:

$$X \cong \prod_{i=0}^{p-2} X^{(\omega^i)} \tag{42}$$

We then have an isomorphism

$$X^{(\omega^i)}/TX^{(\omega^i)} \cong A_F^{(\omega^i)}$$

for each i. If i is even, then it follows from Nakayama's lemma that $X^{(\omega^i)} = 0$. If i is odd, Nakayama"s lemma implies that $X^{(\omega^i)}$ can be generated by one element as a Λ-module. Since this is valid for all i, it follows that X is a cyclic $\Lambda[\Delta]$-module, as asserted.

According to assertion III, each Δ-component $X^{(\omega^i)}$ is a free $\mathbf{Z}_p$-module if $p \nmid h_{F^+}$. Assertion V then means that $\text{rank}_{\mathbf{Z}_p}(X^{(\omega^i)}) \leq 1$, assuming that $p < 12,000,000$. Thus, for those i's for which $X^{(\omega^i)}$ is nontrivial, we have $X^{(\omega^i)} \cong \mathbf{Z}_p$ and the action of Γ on $X^{(\omega^i)}$ is by a character $\langle\chi\rangle^{s_i}$, where $s_i \in \mathbf{Z}_p$. One of the most interesting discoveries of Iwasawa was that this number s_i must be the zero of a certain analytic function, the Kubota-Leopoldt p-adic L-function $L_p(s, \omega^j)$, where $j = 1 - i$. We will prove this in a later chapter.

We now want to explain the relationship of the Λ-module X to the groups $H^1_{unr}(\mathbf{Q}, D_\psi)$, where ψ is a power of the cyclotomic character χ and D_ψ denotes the Galois module associated to ψ as defined in section 1.6. Thus, we assume that $\psi : \text{Gal}(F_\infty/\mathbf{Q}) \to \mathbf{Z}_p^\times$ is a continuous homomorphism. For each i, let $f_i(T)$ denote the characteristic polynomial for $X^{(\omega^i)}$.

Proposition 2.6.1. *Suppose that $\psi|_\Delta = \omega^i$. Then the restriction map defines an isomorphism*

$$H^1_{unr}(\mathbf{Q}, D_\psi) \longrightarrow \text{Hom}_\Gamma(X^{(\omega^i)}, D_\psi)$$

If $\psi(\gamma_o) = 1 + \beta_\psi$, then the group $\text{Hom}_\Gamma(X^{(\omega^i)}, D_\psi)$ is isomorphic to the Pontryagin dual of $X^{(\omega^i)}/(T - \beta_\psi)X^{(\omega^i)}$. The group $H^1_{unr}(\mathbf{Q}, D_\psi)$ is finite if and only if $f_i(\beta_\psi) \neq 0$. We then have

$$ord_p\big(|H^1_{unr}(\mathbf{Q}, D_\psi)|\big) = ord_p\big(f_i(\beta_\psi)\big).$$

if i is odd.

Proof. We consider the restriction map in two steps, from $G_\mathbf{Q}$ to G_F and from G_F to G_{F_∞}. Proposition 1.5.5 implies that we have an isomorphism

$$H^1_{unr}(\mathbf{Q}, D_\psi) \longrightarrow H^1_{unr}(F, D_\psi)^\Delta$$

For the second step, note that $H^0(F_\infty, D_\psi) = D_\psi$. The inflation-restriction sequence for the extension F_∞/F becomes

$$0 \longrightarrow H^1(\Gamma, D_\psi) \longrightarrow H^1(F, D_\psi) \longrightarrow H^1(F_\infty, D_\psi)^\Gamma \longrightarrow H^2(\Gamma, D_\psi)$$

We will show that $H^2(\Gamma, D_\psi) = 0$ and that $H^1(\Gamma, D_\psi)$ is usually also trivial.

For the rest of the proof, and for later arguments, it will be useful to make some general observations about $H^i(\Gamma, A)$ for any discrete, p-primary

abelian group A with a continuous action of Γ. These will be summarized in the lemma below. Let $\Gamma_n = \Gamma^{p^n}$ for $n \geq 0$. By definition, we have

$$H^i(\Gamma, A) = \varinjlim_n H^i(\Gamma/\Gamma_n, A^{\Gamma_n})$$

under the natural inflation maps. We will let N_{Γ/Γ_n} denote the norm map for the action of the finite cyclic group Γ/Γ_n on A^{Γ_n}. The kernel will be denoted simply by $\ker(N_{\Gamma/\Gamma_n})$, a subgroup of A^{Γ_n}. The image is $N_{\Gamma/\Gamma_n}(A^{\Gamma_n})$, a subgroup of A^{Γ}. First we consider $i = 2$. We have

$$H^2(\Gamma/\Gamma_n, A^{\Gamma_n})) \cong A^{\Gamma}/N_{\Gamma/\Gamma_n}(A^{\Gamma_n})$$

If $m \geq n \geq 0$, then the inflation map corresponds to the map

$$A^{\Gamma}/N_{\Gamma/\Gamma_n}(A^{\Gamma_n}) \longrightarrow A^{\Gamma}/N_{\Gamma/\Gamma_m}(A^{\Gamma_m})$$

which is defined by mapping the coset of $a \in A^{\Gamma}$ in the first group to the coset of $N_{\Gamma_n/\Gamma_m}(a)$ in the second group. But $N_{\Gamma_n/\Gamma_m}(a) = p^{m-n}a$ since a is fixed by Γ. Hence, for each such a and for sufficiently large m, the image is trivial. Thus, the direct limit is trivial. That is, $H^2(\Gamma, A) = 0$.

Now, if $i = 1$ and $m \geq n \geq 0$, then the inflation map corresponds to the homomorphism

$$\ker(N_{\Gamma/\Gamma_n})/(\gamma_o - 1)A^{\Gamma_n} \longrightarrow \ker(N_{\Gamma/\Gamma_m})/(\gamma_o - 1)A^{\Gamma_m}$$

which is defined by mapping the coset of $a \in \ker(N_{\Gamma/\Gamma_n})$ to the coset of the same a in $\ker(N_{\Gamma/\Gamma_m})$. However, if $a \in A$, then $a \in A^{\Gamma_n}$ for some n and, essentially as above, one sees that $a \in \ker(N_{\Gamma/\Gamma_m})$ for sufficiently large m. That is, $\bigcup_{n\geq 0} \left(\ker(N_{\Gamma/\Gamma_n}) = A$. On the other hand, it is clear that $\bigcup_{n\geq 0} \left((\gamma_o - 1)A^{\Gamma_n}\right) = (\gamma_o - 1)A$. We have proved most of the following basic lemma.

Lemma 2.6.2. *If A is a discrete, p-primary Γ-module, then*

$$H^1(\Gamma, A) \cong A/(\gamma_o - 1)A, \qquad H^2(\Gamma, A) = 0$$

Furthermore, if we assume that A is a divisible group, that $A[p]$ is finite, and that A^{Γ} is also finite, then $H^1(\Gamma, A) = 0$ too.

To prove the final part of this lemma, note that $A \cong (\mathbf{Q}_p/\mathbf{Z}_p)^r$ for some $r \geq 0$. We can regard $\gamma_o - 1$ as an endomorphism of that group. The kernel of that

endomorphism is A^Γ and, if that kernel is finite, then the image is a divisible group of $\mathbf{Z}_p$-corank r, and hence must also be isomorphic to $(\mathbf{Q}_p/\mathbf{Z}_p)^r$. It follows easily that $(\gamma_o - 1)A = A$, and therefore that $H^1(\Gamma, A)$ is trivial as stated.

Returning to the proof of proposition 2.6.1, the inflation-restriction sequence simplifies to

$$0 \longrightarrow D_\psi/(\gamma_o - 1)D_\psi \longrightarrow H^1(F, D_\psi) \longrightarrow H^1(F_\infty, D_\psi)^\Gamma \longrightarrow 0$$

We can use this to prove that the second step of the restriction map is also an isomorphism.

Assume first that $\psi|_\Gamma$ is nontrivial. Then the above lemma implies that we have an isomorphism $H^1(F, D_\psi) \longrightarrow H^1(F_\infty, D_\psi)^\Gamma$. Just as in the proof of proposition 1.5.5, we must consider the kernel of the restriction map $H^1(I_v, D_\psi) \to H^1(I_\eta, D_\psi)$, where v is a prime of F, η is a prime of F_∞ lying over v, and I_v, I_η are the inertia subgroups of G_F and G_{F_∞} for a prime of $\overline{\mathbf{Q}}$ lying over η. However, if $v \nmid p$, then v is unramified in F_∞/F. It follows that $I_v = I_\eta$ and the kernel of the restriction map at v is certainly trivial. There is a unique prime v of F lying above p and a unique prime η of F_∞ lying over v. Also, v is totally ramified in F_∞/F, the inertia subgroup of Γ for v is Γ itself, and hence I_v/I_η can be identified with Γ. It follows that $H^1(I_v/I_\eta, D_\psi) = 0$. Therefore, the kernel of the restriction map at v is again trivial. This proves that the restriction map

$$H^1_{unr}(F, D_\psi) \longrightarrow H^1_{unr}(F_\infty, D_\psi)$$

is an isomorphism if $\psi|_\Gamma$ is nontrivial.

Now assume that $\psi|_\Gamma$ is trivial, i.e., that $\psi = \omega^i$ for some i. The restriction map $H^1(F, D_\psi) \longrightarrow H^1(F_\infty, D_\psi)^\Gamma$ has a nontrivial kernel, namely $H^1(\Gamma, D_\psi) = \mathrm{Hom}(\Gamma, D_\psi)$. This group is isomorphic to $\mathbf{Q}_p/\mathbf{Z}_p$. However, consider the composite map

$$H^1(\Gamma, D_\psi) \longrightarrow H^1(I_v/I_\eta, D_\psi) \longrightarrow H^1(I_v, D_\psi)$$

where v is the prime of F lying above p. The first map is an isomorphism, the second map is injective. Hence, it follows that

$$\ker\big(H^1_{unr}(F, D_\psi) \longrightarrow H^1_{unr}(F_\infty, D_\psi)\big) = H^1_{unr}(F, D_\psi) \bigcap H^1(\Gamma, D_\psi) = 0$$

To show that the cokernel of the map $H^1_{unr}(F, D_\psi) \longrightarrow H^1_{unr}(F_\infty, D_\psi)^\Gamma$ is trivial, we again refer to the proof of proposition 1.5.5. In the diagram (24) and the exact sequence (25), take $F' = F_\infty$, $D = D_\psi$, and $G = \Gamma$. However, $\ker(b_{F'/F})$ is now the infinite group $H^1(\Gamma, D_\psi)$. Taking into account the above remarks about the local restriction map for $v \nmid p$, it follows that $\ker(c_{F'/F}) = H^1(I_v/I_\eta, D_\psi)$ and that the map $\ker(b_{F'/F}) \longrightarrow \ker(c_{F'/F})$ is surjective. Therefore, the map $\ker(c_{F'/F}) \longrightarrow \ker(a_{F'/F})$ is the zero-map. Also, since $G = \Gamma$, lemma 2.6.2 implies that $\mathrm{coker}(b_{F'/F}) = 0$. It then follows that $\mathrm{coker}(a_{F'/F}) = 0$.

Thus, in all cases, the map $H^1_{unr}(F, D_\psi) \longrightarrow H^1_{unr}(F_\infty, D_\psi)^\Gamma$ is an isomorphism. Combining this with the first step, we obtain the isomorphism

$$H^1_{unr}(\mathbf{Q}, D_\psi) \longrightarrow H^1_{unr}(F_\infty, D_\psi)^{\mathrm{Gal}(F_\infty/\mathbf{Q})}$$

Now $H^1_{unr}(F_\infty, D_\psi) = \mathrm{Hom}(X, D_\psi)$. Since Δ acts on D_ψ by the character $\psi|_\Delta = \omega^i$, we have

$$H^1_{unr}(F_\infty, D_\psi)^\Delta = \mathrm{Hom}(X^{(\omega^i)}, D_\psi)$$

It is then clear that $H^1_{unr}(F_\infty, D_\psi)^{\Delta\times\Gamma}$ is isomorphic to $\mathrm{Hom}_\Gamma(X^{(\omega^i)}, D_\psi)$ and this establishes the first part of proposition 2.5.1.

Since γ_o acts on D_ψ as multiplication by $1 + \beta_\psi$, and this determines the action of Γ, it follows that any element of $\mathrm{Hom}_\Gamma(X^{(\omega^i)}, D_\psi)$ must factor through the maximal quotient of $X^{(\omega^i)}$ on which γ_o acts in the same way. That quotient is $X^{(\omega^i)}/\big(\gamma_o - (1 + \beta_\psi)\big)X^{(\omega^i)}$. Conversely, any element of $\mathrm{Hom}(X^{(\omega^i)}, D_\psi)$ factoring through that quotient will be Γ-equivariant. That is,

$$\mathrm{Hom}_\Gamma(X^{(\omega^i)}, D_\psi) = \mathrm{Hom}\big(X^{(\omega^i)}/\big(\gamma_o - (1 + \beta_\psi)\big)X^{(\omega^i)}, D_\psi\big)$$

which is indeed isomorphic to the Pontryagin dual of $X^{(\omega^i)}/\big(T - \beta_\psi)\big)X^{(\omega^i)}$ since $D_\psi \cong \mathbf{Q}_p/\mathbf{Z}_p$ as a group. This proves the second statement in the proposition. It is then clear that $H^1_{unr}(\mathbf{Q}, D_\psi)$ is finite if and only if $f_i(\beta_\psi) \neq 0$. Furthermore, one can apply proposition 2.3.3 if i is odd because we know that $X^{(\omega^i)}$ has no nonzero, finite Λ-submodules. The final statement follow then follows. ■

Remark 2.6.3. It is worth discussing what happens for an arbitrary $\mathbf{Z}_p$-extension F_∞/F. We consider any number field F and let p be any prime. Let $D = D_\psi$, where $\psi \in \mathrm{Hom}(\Gamma, \mathbf{Z}_p^\times)$. Assume first that ψ has infinite

order. Then $F_\infty = F(D)$ and D^Γ is finite and nontrivial. The cokernel of the restriction map

$$H^1(F, D) \longrightarrow H^1(F_\infty, D)^\Gamma \tag{43}$$

is isomorphic to a subgroup of $H^2(\Gamma, D)$. But that group vanishes according to lemma 2.6.2 and hence the restriction map is surjective. The kernel is $H^1(\Gamma, D^{G_{F_\infty}})$. This group also vanishes because $D^{G_{F_\infty}} = D$ is divisible. For the same reason, the local restriction map $H^1(F_v^{unr}, D) \longrightarrow H^1(F_\eta^{unr}, D)$ is injective for every ramified prime v in the extension F_∞/F, where η is a prime of F_∞ lying over v. Therefore, we again get an isomorphism

$$H^1_{unr}(F, D) \longrightarrow \mathrm{Hom}_\Gamma(X, D), \tag{44}$$

where $X = X_{F_\infty/F}$. In particular, if we let $\beta = \psi(\gamma_o) - 1$, then $H^1_{unr}(F, D)$ is infinite if and only if $f_X(\beta) = 0$. On the other hand, if ψ has finite order, then corollary 1.5.8 implies that $H^1_{unr}(F, D)$ must be finite. Therefore, since $f_X(T)$ is a nonzero polynomial, it follows that $H^1_{unr}(F, D)$ is finite for all but finitely many $\psi \in \mathrm{Hom}(\Gamma, \mathbf{Z}_p^\times)$.

If ψ has finite order, then ψ is the trivial character unless $p = 2$. For $p = 2$, the character ψ could have order 1 or 2. It is not difficult to verify that the kernel of the map (44) is still finite. One uses the fact that if n is sufficiently large, then at least one prime of F_n is totally ramified in F_∞/F_n. However, the cokernel of (44) can be infinite. In particular, if ψ is trivial (and so $\beta = 0$), it is possible to have $f_X(0) = 0$ even though $H^1_{unr}(F, D)$ is finite. As an example to illustrate how this can happen, suppose that F is an imaginary quadratic field, that p splits in $F/\mathbf{Q}$, and that F_∞ is the cyclotomic $\mathbf{Z}_p$-extension of F. This situation was discussed briefly following the proof of proposition 1.6.4. For $s \in \mathbf{Z}_p$, let $\psi_s = \langle\chi\rangle^s$. Thus, ψ_s has infinite order if $s \neq 0$. Let $D_s = D_{\psi_s}$ and $\beta_s = \psi_s(\gamma_o) - 1)$. Thus, $\beta_s \to 0$ as $s \to 0$ in $\mathbf{Z}_p$. For $s \neq 0$, we have

$$H^1_{unr}(F, D_s) \cong \mathrm{Hom}(X/(T - \beta_s)X, \mathbf{Q}_p/\mathbf{Z}_p)$$

as explained above. However, under the above assumptions on F, the order of $H^1_{unr}(F, D_s)$ is unbounded as $s \to 0$ in $\mathbf{Z}_p$. It follows that $f_X(\beta_s) \to 0$ as $s \to 0$ and therefore $f_X(0) = 0$.