1 \textbf{\textit{\(Z_p\)}-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 \(Z_p\)-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

\[ X = X_{F_\infty/F} = \lim_{\leftarrow n} Cl_{F_n}[p^\infty] \]

as a module over the formal power series ring \(\Lambda = Z_p[[T]]\). 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 \(\Lambda\)-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 \(F = Q(\mu_p)\) for an odd prime \(p\) and \(F_\infty = Q(\mu_p^\infty)\). Then \(F_\infty/F\) is a \(Z_p\)-extension. The \(n\)-th layer is \(F_n = Q(\mu_p^{n+1})\). 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.

1.1 \textbf{\textit{Introductory remarks about \(Z_p\)-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 “\(\Gamma\)-extensions” by Iwasawa, but later he adopted the more descriptive term “\(Z_p\)-extensions.” Let \(p\) be a fixed prime. A Galois extension \(K/F\) is called a \(Z_p\)-extension if the topological group \(\text{Gal}(K/F)\) is isomorphic to the additive group \(\mathbb{Z}_p\) of \(p\)-adic integers.

Except for the trivial subgroup, all the closed subgroups of \(\mathbb{Z}_p\) have finite index. Such a closed subgroup is of the form \(p^n\mathbb{Z}_p\) for some nonnegative integer \(n\) and the corresponding quotient group is cyclic of order \(p^n\). Thus, if \(K/F\) is a \(Z_p\)-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 \(\text{Gal}(F_n/F) = \mathbb{Z}/p^n\mathbb{Z}\) for all \(n\). Clearly \(K = \bigcup_{n \geq 0} F_n\). If one chooses any
\( \gamma_0 \in \text{Gal}(K/F) \) such that \( \gamma_0|_{F_1} \) is nontrivial, then the infinite cyclic subgroup generated by \( \gamma_0 \) is dense in \( \text{Gal}(K/F) \). We therefore say that \( \text{Gal}(K/F) \) is a topologically cyclic group and that the element \( \gamma_0 \) is a topological generator of \( \text{Gal}(K/F) \). We will often use the notation \( F_\infty \) for a \( \mathbb{Z}_p \)-extension of \( F \).

Let \( F \) be any number field and let \( p \) be a fixed prime. One important example of a \( \mathbb{Z}_p \)-extension of \( F \) is quite easy to construct. Let \( \mu_{p^\infty} \) 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

\[
\chi : \text{Gal}(F(\mu_{p^\infty})/F) \to \mathbb{Z}_p^\times.
\]

This homomorphism is injective. Consequently, \( \text{Gal}(F(\mu_{p^\infty})/F) \) is isomorphic to an infinite closed subgroup of \( \mathbb{Z}_p^\times \). Such a group has a finite torsion subgroup and the corresponding quotient group will be isomorphic to \( \mathbb{Z}_p \). Therefore, \( F(\mu_{p^\infty}) \) contains a unique subfield \( F_\infty \) such that \( \text{Gal}(F_\infty/F) \cong \mathbb{Z}_p \).

We refer to \( F_\infty \) as the cyclotomic \( \mathbb{Z}_p \)-extension of \( F \). In particular, we will let \( \mathbb{Q}_\infty \) denote the cyclotomic \( \mathbb{Z}_p \)-extension of \( \mathbb{Q} \). The cyclotomic \( \mathbb{Z}_p \)-extension of an arbitrary number field \( F \) is then \( F_\infty = \mathbb{Q}_\infty \).

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

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

**Proof.** Let \( \Gamma = \text{Gal}(F_\infty/F) \). Let \( I_v \) denote the inertia subgroup of \( \text{Gal}(F_\infty/F) \) corresponding to a prime \( v \) of \( F \). If \( v \) is ramified in \( F_\infty/F \), then \( I_v \) is nontrivial. Hence \( I_v \) must be finite. 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 \( F_\infty/F \). If \( v \) is nonarchimedian, but lies over \( l \), where \( l \neq p \), then \( v \) is tamely ramified in \( F_\infty/F \). 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 \( F_\infty/F \).

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, \( F_\infty/F \) must be ramified for at least one prime. ■
The existence and ramification properties of $\mathbb{Z}_p$-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 $F = \mathbb{Q}$ as the base field, then it is not hard to prove that there is only one $\mathbb{Z}_p$-extension, the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty$ which was constructed above. To see this, one can use the Kronecker-Weber theorem which asserts that the maximal abelian extension $\mathbb{Q}^{ab}$ of $\mathbb{Q}$ is generated by all the roots of unity. Proposition 2.1.1 then implies that any $\mathbb{Z}_p$-extension of $\mathbb{Q}$ must be ramified only at $p$ and therefore contained in $\mathbb{Q}(\mu_{p^\infty})$, and so must be $\mathbb{Q}_\infty$. The cyclotomic $\mathbb{Z}_p$-extension of an arbitrary number field $F$ is $F_\infty = F\mathbb{Q}_\infty$.

If $F$ is a totally real number field, then it should again be true that the cyclotomic $\mathbb{Z}_p$-extension is the only $\mathbb{Z}_p$-extension of $F$. This can be proved if $F \subset \mathbb{Q}^{ab}$, 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 $\mathbb{Z}_p$-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 $\mathbb{Z}_p$-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 $\mathbb{Z}_p$-extension of a number field $F$. Let $h_n$ denote the class number of $F_n$ and let $h_n^{(p)} = p^{e_n} \mu^n$ denote the largest power of $p$ dividing $h_n$. Then there exists integers $\lambda$, $\mu$, and $\nu$ 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 $\lambda$ and $\mu$ will be nonnegative. We will refer to them as the Iwasawa invariants for $F_\infty/F$, 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 $\mathbb{Z}_p$-extension of $F$ and suppose that only one prime of $F$ is ramified in $F_\infty/F$. 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 $\text{Gal}(F_\infty/F)$ for the
one ramified prime \( v \). It is clear that \( v \) must be totally ramified in \( F_\infty/F \). Otherwise, \( F_\infty^{I_v} \) would be a nontrivial, unramified, cyclic \( p \)-extension of \( F \), contradicting 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 \( \mathbb{Q}_n \), the \( n \)-th layer in the cyclotomic \( \mathbb{Z}_p \)-extension \( \mathbb{Q}_\infty/\mathbb{Q} \). Also, if we take \( F = \mathbb{Q}(\mu_p) \), where \( p \) is any odd regular prime, then it follows that the class number of \( \mathbb{Q}(\mu_p^n) \) will not be divisible by \( p \) for all \( n \geq 1 \). The class number of \( \mathbb{Q}(\mu_2^n) \) 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 \( \mathbb{Z}_p \)-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 \( L_\infty \) is an abelian extension of \( F_\infty \). Let \( X = \text{Gal}(L_\infty/F_\infty) \). 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

\[
X \cong \lim_{\leftarrow n} \text{Gal}(L_n/F_n) \cong \lim_{\leftarrow n} A_n
\]

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

\[
R_{F_n/F_m} : \text{Gal}(L_m/F_m) \rightarrow \text{Gal}(L_n/F_n), \quad N_{F_m/F_n} : A_m \rightarrow A_n
\]

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 \( \text{Art}_{L_n/F_n} \) 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 \( L_\infty \) could be described more directly as the maximal, abelian pro-\( p \) extension of \( F_\infty \) which is unramified at all primes of \( F_\infty \). The adjective ”pro-\( p \)” refers to the fact that \( X = \text{Gal}(L_\infty/F_\infty) \) 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 \( L_\infty \) as the pro-\( p \) Hilbert class field of \( F_\infty \).

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

$$1 \rightarrow X \rightarrow \text{Gal}(L_\infty/F) \rightarrow \Gamma \rightarrow 1$$

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

$$x^\gamma = \tilde{\gamma}x\tilde{\gamma}^{-1}$$  \hspace{1cm} (1)$$

for all $x \in X$. Continuity means that the map $\Gamma \times X \rightarrow X$ defined by $(\gamma, x) \rightarrow x^\gamma$ 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 $\gamma x$ instead of $x^\gamma$. More generally, we can regard $X$ as a module for the group ring $\mathbb{Z}[\Gamma]$ and will write $\theta x$ if $\theta \in \mathbb{Z}[\Gamma]$ and $x \in X$. In particular, for any $n \geq 0$, we will denote the element $\gamma^p - 1$ in this group ring by $\omega_n$. Then $\omega_n x$ corresponds to an element of $X$ which could be written in multiplicative notation as $\tilde{\gamma}^p x(\tilde{\gamma}^p)^{-1}x^{-1}$, a commutator in $\text{Gal}(L_\infty/F_n)$. In fact, we have the following basic result.

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

**Proof.** Let $G_n = \text{Gal}(L_\infty/F_n)$ and $\Gamma_n = \text{Gal}(F_\infty/F_n)$. 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 $\omega_n$ 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 $\gamma^p$ generates a dense, infinite cyclic subgroup $\Gamma'_n$ of $\Gamma_n$. There is a surjective homomorphism from $G_n$ to $\Gamma_n$. The inverse image of $\Gamma'_n$ 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 $L_\infty/F_\infty$. But the proof is obviously more general and would apply whenever $L_\infty$ is an abelian, pro-$p$ extension of $F_\infty$ which is Galois over $F$. Under that assumption, $X = \text{Gal}(L_\infty/F_\infty)$ would again have a continuous action of $\Gamma$. Here is an interesting and important example. Let $\Sigma$ be any subset of the primes of $F$. Let $\Sigma_\infty$ be the set of primes of $F_\infty$ lying above those in $\Sigma$. Define $M^\Sigma_\infty$ to be the maximal, abelian, pro-$p$ extension of $F_\infty$ which
is ramified only at the primes in $\Sigma_\infty$. It is easy to verify that $M_\infty^\Sigma$ is Galois over $F$ and so the analogue of proposition 2.1.3 would apply. The field $L_\infty$ considered above is the special case where $\Sigma$ is empty.

If $\Sigma$ 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 $\Sigma_n$ denote the primes of $F_n$ lying above those in $\Sigma$. Let $M_n^\Sigma$ denote the maximal, abelian, pro-$p$ extension of $F_n$ which is ramified only at the primes in $\Sigma_n$. Then, $M_\infty^\Sigma$ is the maximal abelian extension of $F_n$ contained in $M_\infty^\Sigma$. If we let $X_\Sigma = \text{Gal}(M_\infty^\Sigma/F_\infty)$, then we have
\[
\text{Gal}(M_\infty^\Sigma/M_n^\Sigma) = \omega_n X_\Sigma, \quad \text{Gal}(M_n^\Sigma/F_\infty) \cong X_\Sigma/\omega_n X_\Sigma
\]
for any $n \geq 0$.

As proposition 2.1.2 illustrates, various questions about $\mathbb{Z}_p$-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 $\mathbb{Z}_p$-extension $F_\infty/F$ 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 $\Gamma$ 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 $\mathbb{Z}_p$-extension $F_\infty/F$. Then, with the notation as above, we have canonical isomorphisms
\[
X/\omega_n X \cong \text{Gal}(L_n/F_n) \cong A_n
\]
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 $F_\infty/F$. 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 $\mathbb{Z}_p$-extension $F_\infty/F_n$ and it is totally ramified. Let $K_n$ denote the maximal abelian extension of $F_n$ contained in $L_\infty$. Proposition 2.1.3 implies that we have the isomorphism
\[
X/\omega_n X \rightarrow \text{Gal}(K_n/F_\infty)
\]
induced by the restriction map $x \rightarrow x|_{K_n}$ for $x \in X$. 

6
Let $I_n$ denote the inertia subgroup of $\text{Gal}(K_n/F_n)$ for $v_n$. It is clear that $L_n$ is the subfield of $K_n$ fixed by $I_n$ and $F_\infty$ is the subfield fixed by $\text{Gal}(K_n/F_\infty)$. Since these two subgroups of $\text{Gal}(K_n/F_n)$ have trivial intersection, it follows that $K_n = L_n F_\infty$. Since $v_n$ is totally ramified in $F_\infty/F_n$, we have $L_n \cap F_\infty = F_n$ and therefore the restriction map

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

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 $\mathbb{Z}_p$-extension satisfying RamHyp(1) to proving an analogous formula for the growth of the quotients $X/\omega_nX$ of $X$. We do this in the next two sections where we begin the study of the structure and properties of $\Gamma$-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.

### 1.2 The structure of $\Gamma$-modules.

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

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

$$X = \lim_{\leftarrow} X_i$$

where $X_i$ is a finite, abelian $p$-group for each index $i \in I$. It is easy to make $X$ into a $\mathbb{Z}_p$-module. Each $X_i$ is a $(\mathbb{Z}/p^{t_i}\mathbb{Z})$-module for some $t_i > 0$. The canonical homomorphism $\mathbb{Z}_p \to \mathbb{Z}/p^{t_i}\mathbb{Z}$ makes each $X_i$ into a $\mathbb{Z}_p$-module. The projective limit $X$ then inherits the structure of a $\mathbb{Z}_p$-module (since the maps defining the projective limit will be $\mathbb{Z}_p$-modules homomorphisms). It is a topological $\mathbb{Z}_p$-module in the sense that the map $\mathbb{Z}_p \times X \to X$ defined by $(z, x) \mapsto zx$ (where $z \in \mathbb{Z}_p$ and $x \in X$) is continuous. Conversely, it is not hard to see that any compact, topological $\mathbb{Z}_p$-module is an abelian, pro-$p$ group. One way to prove this is to consider the Pontryagin dual $S = \text{Hom}(X, \mathbb{Q}_p/\mathbb{Z}_p)$, which is a discrete abelian group and also a topological
$\mathbb{Z}_p$-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 $\mathbb{Z}_p$-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 $\Gamma$. As above, we have $X = \varprojlim X_i$, where the $X_i$’s are finite, abelian $p$-groups and $i$ varies over an appropriate 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 $\gamma$ in some subgroup of finite index in $\Gamma$. This means that the orbit of $Y_i$ under the action of $\Gamma$ is finite. Hence $Y_i$ contains an open subgroup which is $\Gamma$-invariant. This implies that we can assume without loss of generality that each $Y_i$ is already $\Gamma$-invariant and so

$$X = \varprojlim X_i,$$

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

It will be important for us to view $X$ as a module over the ring $\Lambda = \mathbb{Z}_p[[T]]$, the formal power series ring over $\mathbb{Z}_p$ in the variable $T$. One sees easily that $\Lambda$ is a local ring, $m = (p, T)$ is its maximal ideal, and $\Lambda$ is complete in its $m$-adic topology. Also $\Lambda/m^t$ is finite (of order $p^{(t+1)/2}$) for any $t$.

Let $\gamma_0$ denote a topological generator for $\Gamma$, as in section 2.1. Roughly speaking, we will make $X$ into a $\Lambda$-module by regarding $T$ as the endomorphism $\gamma_0^{-1}$.

For each $i \in I$, we have $p^{a_i}X_i = 0$ for some $a_i > 0$. Also, $\gamma_0 - 1$ defines an endomorphism of $X_i$ which has a nontrivial kernel if $X_i$ is nontrivial. Consequently, $(\gamma_0 - 1)X_i$ is a proper subgroup of $X_i$ if $X_i \neq 0$. It follows that $(\gamma_0 - 1)^b X_i = 0$ for some $b_i > 0$. Thus, we can regard $X_i$ as a module over the finite ring $\mathbb{Z}_p[T]/(p^{a_i}, T^{b_i})$, where we let $T$ act on $X_i$ as the endomorphism $\gamma_0 - 1$. However, we obviously have $\mathbb{Z}_p[T]/(p^{a_i}, T^{b_i}) \cong \mathbb{Z}_p[[T]]/(p^{a_i}, T^{b_i})$, and so we can regard $X_i$ as a $\Lambda$-module which is annihilated by the ideal $(p^{a_i}, T^{b_i})$. Taking $t_i = a_i + b_i$, it is obvious that $m^{t_i} \subset (p^{a_i}, T^{b_i})$ and so each $X_i$ can be regarded as a module over $\Lambda/m^{t_i}$. Regarding the $X_i$’s as $\Lambda$-modules, it is clear that the maps defining the projective limit are $\Lambda$-module homomorphisms. Thus $X$ becomes a topological $\Lambda$-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 $\Lambda$-module, then $X$ is also a compact $\mathbb{Z}_p$-module and hence is an abelian, pro-$p$ group. To make $X$ into a $\Gamma$-module, note that $\Gamma$ can be identified as a topological group with a subgroup of $\Lambda^\times$. 

8
by the continuous homomorphism $\gamma(z) \to (1 + T)^z$ for all $z \in \mathbb{Z}_p$. Here we define

$$(1 + T)^z = \sum_{i=0}^{\infty} \binom{z}{i} T^i,$$

where $\binom{z}{i} = \frac{1}{i!} \prod_{j=1}^{i} (z - j + 1)$.

It is not difficult to prove that the coefficients of the above power series are in $\mathbb{Z}_p$, the constant term is 1, and so the power series is indeed invertible in $\Lambda$. Thus, $X$ admits a continuous action of $\Gamma$ from which the $\Lambda$-module structure on $X$ arises by letting $T$ act as $\gamma_0 - 1$, just as above. If $X$ is finitely generated as a $\Lambda$-module, then it is clear that $X$ is compact and that the quotients $X/m^nX$ are finite $\Lambda$-modules for all $n \geq 0$. In this case, we have

$$X \cong \lim_{\leftarrow n} X/m^nX,$$

an inverse limit of a sequence of finite $\Lambda$-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 $R/m^t$ is finite for all $t > 0$. In particular, $k = R/m$ is a finite field. Let $p$ be its characteristic. Now $R = \lim_{\leftarrow t} R/m^t$, where the finite rings $R/m^t$ 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 $R/m^{t_n}$ 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 $(r, x) \mapsto rx$ 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 $\bar{x}_i$ denote the image of $x_i$ under the natural map $X \to X/mX$. Then $x_1, \ldots, x_d$ is a generating set for the $R$-module $X$ if and only if $\bar{x}_1, \ldots, \bar{x}_d$ is a generating set for the $k$-vector space $X/mX$.

**Proof.** It is obvious that $\bar{x}_1, \ldots, \bar{x}_d$ generate the $k$-vector space $X/mX$ if $x_1, \ldots, x_d$ generate the $R$-module $X$. Conversely, assume that $\bar{x}_1, \ldots, \bar{x}_d$
generate $X/mX$ 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 $m^tX = 0$ for some $t > 0$. We are assuming that the image of $Y$ under the canonical homomorphism $X \to X/mX$ is all of $X/mX$. Thus, $X = Y + mX$. It follows that $X = Y + m^iX$ 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 $X = mX$.
2. $X$ is a finitely generated $R$-module if and only if $X/mX$ 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, $m^tX = 0$ for some $t > 0$. But, on the other hand, $X = mX$ if and only if $X = m^iX$ for all $i > 0$. It follows that $X = 0$. ■

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

The ring $\Lambda$ is Noetherian and has Krull-dimension 2. The maximal ideal $m$ has height 2. One simple way to obtain prime ideals of height 1 is as kernels of the evaluation homomorphisms. Suppose that $\alpha \in \overline{Q}_p$ and has absolute value $< 1$. If $f(T) \in \Lambda$, then one can define $f(\alpha) \in \mathcal{O} = \mathbb{Z}_p[\alpha]$ 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 $Q_p(\alpha)$—a finite extension of $Q_p$. 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 $\alpha$ and $\alpha'$ are two such elements of $\overline{Q}_p$, then it is easy to see that the corresponding evaluation homomorphisms have the same kernel if and only if $\alpha$ and $\alpha'$ are conjugate over $Q_p$. 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 $\Lambda$ arise in this way. The exception is the ideal $(p)$. If $f(T) = \sum a_iT^i \in \Lambda$, define $\tilde{f}(T) = \sum \tilde{a}_iT^i \in \mathbb{F}_p[[T]]$, where $\tilde{a}$ denotes the image of $a \in \mathbb{Z}_p$. 

10
under the homomorphism $\mathbb{Z}_p \to F_p$. Then the map $\Lambda \to F_p[[T]]$ defined by $f(T) \to \tilde{f}(T)$ is a surjective ring homomorphism with kernel $(p)$. This makes it clear that $(p)$ is indeed a prime ideal of $\Lambda$.

Suppose that $X$ is a finitely generated, torsion $\Lambda$-module. If $I$ is any ideal of $\Lambda$, we will use the notation $X[I] = \{ x \in X \mid \alpha x = 0 \text{ for all } \alpha \in I \}$

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

Let $Y = \bigcup_{n \geq 0} X[p^n]$, which is just the $\mathbb{Z}_p$-torsion submodule of $X$. We will denote $Y$ simply by $X_{\text{tors}}$ in this chapter. Just as above, we see that $Y = X[p^t]$ for some $t > 0$. We have $Z \subset Y$. The quotient $X/Y$ is a finitely generated, torsion $\Lambda$-module and is torsion-free as a $\mathbb{Z}_p$-module. If $f(T) = \sum a_i T^i$ is a nonzero element of $\Lambda$ 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 $\Lambda$-module, then it is a quotient of the $\Lambda$-module $U^d$, where $U = \Lambda/(g(T))$. The following lemma gives the structure of $U$ as a $\mathbb{Z}_p$-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 $l = \min \{ i \mid b_i \in \mathbb{Z}_p \}$. Then $U = \Lambda/(g(T))$ is a free $\mathbb{Z}_p$-module of rank $l$.

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

Now $U/pU$ can be considered as an $F_p[[T]]$-module and is isomorphic to $F_p[[T]]/(\bar{g}(T))$, where, as earlier, $\bar{g}(T) = \sum b_i T^i$. Note that $\bar{g}(T)$ is a nonzero element of $F_p[[T]]$ and $(\bar{g}(T)) = (T^l)$. It is clear that $U/pU$ has dimension $l$ as an $F_p$-vector space and so, by lemma 1.5.3 (Nakayama’s Lemma for compact $\mathbb{Z}_p$-modules), it follows that $U$ is a finitely generated $\mathbb{Z}_p$-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 $\Lambda$-module. Then there are uniquely determined $\Lambda$-submodules $Z$ and $Y$ of $X$
with the following properties:

a. $Z$ is finite and $X/Z$ has no nonzero, finite $\Lambda$-submodules.

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

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

$$\lambda(X) = \text{rank}_{\mathbb{Z}_p}(X/Y) = \dim_{\mathbb{Q}_p}(V).$$

(2)

Then $X/Y = \mathbb{Z}_p^{\lambda(X)}$ as a $\mathbb{Z}_p$-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 $\Lambda$-module $X[p^i]/X[p^{i-1}]$ has exponent $p$ and can be considered as an $\mathbb{F}_p[[T]]$-module. It will be finitely generated and thus has finite rank. We define

$$\mu(X) = \sum_{i=1}^{t} \text{rank}_{\mathbb{F}_p[[T]]}(X[p^i]/X[p^{i-1}]).$$

(3)

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

$$\mu(X) = 0 \iff Y \text{ is finite} \iff X[p] \text{ is finite} \iff X/pX \text{ is finite}.$$  

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

We will refer to $\lambda(X)$ and $\mu(X)$ as the Iwasawa invariants for the $\Lambda$-module $X$. Another invariant which will play an important role will be a polynomial $f_X(T)$ in $\mathbb{Z}_p[T]$, which we refer to as the “characteristic polynomial” of $X$. However, this polynomial depends not just on the structure of $X$ as a $\Gamma$-module, but also on the choice of topological generator $\gamma_o$ of $\Gamma$. (In a later chapter, we will remedy this by redefining the ring $\Lambda$ in a more intrinsic way, viewing it as the “completed group algebra for $\Gamma$ over $\mathbb{Z}_p$.”) 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 $\mathbb{Q}_p$-vector space $V$ defined above. These eigenvalues are in $\mathbb{Q}_p^p$ 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 $Y = X_{\text{tors}}$ as a $\Lambda$-module. For each $i \geq 1$, define $r_i = \text{rank}_{F_p[[T]]}(X[p^i]/X[p^{i-1}]).$ Assume that $\mu(X) > 0$. This means that $r_1 > 0$. Choose $t$ so that $r_1 > 0$, but $r_{t+1} = 0$. Note that $r_1 \geq \cdots \geq r_t$. Let $r = r_1$. The finer $\mu$-invariants will be positive integers $\mu_1, \ldots, \mu_r$, consisting of $r_1 - r_2 1's, r_2 - r_3 2's, \ldots,$ and $r_t t's$. With this definition, we have

$$\mu(X) = \sum_{i=1}^{t} r_i = \sum_{j=1}^{r} \mu_j. \quad (4)$$

As a simple illustration, suppose that $X$ is a $\Lambda$-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 $F_\infty/F$ be a $\mathbb{Z}_p$-extension and let $L_\infty$ be the pro-$p$ Hilbert class field of $F_\infty$. We will prove that $X = \text{Gal}(L_\infty/F_\infty)$ is a finitely generated, torsion $\Lambda$-module in section 2.5. The integers $\lambda$ and $\mu$ 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 $F/Q$ is an abelian extension and $F_\infty$ is the cyclotomic $\mathbb{Z}_p$-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 $F = \mathbb{Q}(\mu_p)$. 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 $F_\infty/F$ satisfies RamHyp(1), then the assertion that $X$ is a finitely generated, torsion $\Lambda$-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 $\Lambda$-module follows from the following result.

**Proposition 2.2.5.** Let $X$ be a finitely generated $\Lambda$-module. Then the following statements are equivalent:
a. There exists an element \( f(T) \in m \) such that \( X/f(T)X \) is finite.

b. \( X \) contains a torsion \( \mathbb{Z}_p \)-submodule \( Y \) such that \( X/Y \) is finitely generated as a \( \mathbb{Z}_p \)-module.

c. \( X \) is a torsion \( \Lambda \)-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 \( \mathbb{Z}_p \)-torsion free. Since \( \Lambda \) 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 \( \mathbb{Z}_p \)-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 \( \beta \in p\mathbb{Z}_p \) 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 \( p^i Y = 0 \). Then for each \( i, 0 < i \leq t \), \( Y[p^i]/Y[p^{i-1}] \) can be considered as a finitely generated \( \mathbb{F}_p[[T]] \)-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 \( \mathbb{Z}_p \), it follows that \( X \) is finitely generated over \( \mathbb{Z}_p \). 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 \( \mathbb{Z}_p \)-module and its \( \mathbb{Z}_p \)-rank \( l = \deg(f(T)) \) is positive. Let \( r = \text{rank}_\Lambda(X) \). The following lemma then completes the proof of proposition 2.2.5. It implies that \( r = 0 \) if \( X/(f(T))X \) is finite. \( \blacksquare \)

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

\[
\text{rank}_{\mathbb{Z}_p}(X/f(T)X) \geq rl. \tag{5}
\]

If \( X \) is a torsion-free \( \Lambda \)-module, then equality holds.

Proof. To prove (5), we can obviously replace \( X \) by the quotient module \( X/X_{\text{tors}} \). So we can assume without loss of generality that \( X \) is a torsion-free \( \Lambda \)-module. We can also clearly assume that \( f(T) \) is not divisible by \( p \).
Now $X$ contains a $\Lambda$-submodule $Y$ which is free of rank $r$ over $\Lambda$. We have the exact sequence

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

where $Z$ is a finitely generated, torsion $\Lambda$-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 $\mathbb{Z}_p$-module of rank $rl$. Let $U$ denote the $\mathbb{Z}_p$-torsion submodule of $Z$. Then $Z/U$ is a free $\mathbb{Z}_p$-module of finite rank. This implies that $Z[f(T)]$ and $Z/f(T)Z$ have the same (finite) $\mathbb{Z}_p$-rank. Thus we see that $\text{rank}_{\mathbb{Z}_p}(X/f(T)X) = rl$. $\blacksquare$

In a later chapter, we will discuss more precise results concerning the structure of finitely generated $\Lambda$-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 $\text{dim}(R)$. 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:

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

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.

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

This is a finite set. We will say that $X$ is “pure of dimension $d$” if $\text{dim}(R/P) = d$ 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 $d = \text{dim}(R) - h$. In particular, a torsion-free $R$-module would be pure of dimension equal to $\text{dim}(R)$.

If we take $R = \Lambda$, then the Krull-dimension is 2. As explained earlier, $\Lambda$ has one prime ideal of height 2, the maximal ideal $m = (p, T)$, and infinitely many prime ideals of height 1. A nonzero, finitely generated, torsion $\Lambda$-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 \( \Lambda \)-submodules and hence is pure of dimension 1.

We have been considering \( \Lambda \)-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 \( \mathbb{Z}_p \)-module). Let \( S = \text{Hom}(X, \mathbb{Q}_p/\mathbb{Z}_p) \). 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 \( X = \text{Hom}(S, \mathbb{Q}_p/\mathbb{Z}_p) \) is an abelian, pro-\( p \) group. We can regard both \( S \) and \( X \) as \( \mathbb{Z}_p \)-modules.

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

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

Suppose that \( S \) is a discrete, \( p \)-primary abelian group with a continuous action of \( \Gamma \). We can translate our earlier results into equivalent statements about \( S \). Let \( X = \text{Hom}(S, \mathbb{Q}_p/\mathbb{Z}_p) \), which also admits a continuous action of \( \Gamma \). (This is defined on \( \text{Hom} \) in the usual way, using the given action of \( \Gamma \) on \( S \) and the trivial action on \( \mathbb{Q}_p/\mathbb{Z}_p \).) Since \( S \) is also a \( \mathbb{Z}_p \)-module, it is not hard to make \( S \) into a \( \Lambda \)-module directly (showing first that \( S \) is a direct limit of finite \( \Gamma \)-invariant subgroups). Or one can equivalently transfer the structure of \( X \) as a \( \Lambda \)-module to \( S \). Just as above, we say that \( S \) is cofinitely generated as a \( \Lambda \)-module if \( X \) is finitely generated as a \( \Lambda \)-module, cotorsion as a \( \Lambda \)-module if \( X \) is a torsion \( \Lambda \)-module. We refer to \( \text{rank}_{\Lambda}(X) \) as \( \text{corank}_{\Lambda}(S) \). If \( S \) is a cofinitely generated, torsion \( \Lambda \)-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 \( \Lambda \)-module, then \( S \) is divisible as a \( \Lambda \)-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 \( \Gamma \). Regard \( S \) as a \( \Lambda \)-module. Then

1. \( S = 0 \iff S^\Gamma = 0 \iff S[m] = 0 \).
2. \( S \) is a cofinitely generated \( \Lambda \)-module \( \iff S[m] \) is finite.
3. \( S \) is a cofinitely generated, cotorsion \( \Lambda \)-module \( \iff S[\theta] \) is finite for some \( \theta \in m \).

**Proposition 2.2.9.** Suppose that \( S \) satisfies the assumptions in proposition 2.2.8. If \( S^\Gamma \) is finite, then \( S \) is a cofinitely generated, cotorsion \( \Lambda \)-module.

**Proposition 2.2.10.** Suppose that \( S \) is a cofinitely generated, cotorsion \( \Lambda \)-module. Then \( S_{div} = (\mathbb{Q}_p/\mathbb{Z}_p)^\lambda \) as a \( \mathbb{Z}_p \)-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.

### 1.3 Growth theorems for quotients of \( \Gamma \)-modules.

Now let \( X \) be a finitely generated, torsion \( \Lambda \)-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 \( \gamma \) acting on the vector space \( V = X \otimes_{\mathbb{Z}_p} \overline{\mathbb{Q}}_p \) are \( p^n \)-th roots of unity. (Of course, the corresponding eigenvectors may be in the vector space \( V \otimes_{\mathbb{Q}_p} \overline{\mathbb{Q}}_p \) obtained by extending scalars to the algebraic closure \( \overline{\mathbb{Q}}_p \) of \( \mathbb{Q}_p \).) 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 \( \Lambda \), we can write \( \omega_n = \prod_{i=0}^{p} \phi_i \), 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 \( \phi_i \) are the numbers \( \zeta - 1 \), where \( \zeta \) is a primitive \( p^t \)-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 \( \gamma \) 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 $\Lambda$-module. Choose $n_o$ so that $X/n,n_oX$ is finite for all $n \geq n_o$. Let $\lambda = \lambda(X)$, $\mu = \mu(X)$. Then we have

$$|X/n,n_oX| = p^{\lambda n + \mu p^n + \nu}$$

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

Proof. Suppose that we have an exact sequence of torsion $\Lambda$-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

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

Choose $n_o$ sufficiently large so that the $X_2/n,n_oX_2$ 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

$$0 \longrightarrow X_1[n,n_o] \longrightarrow X_2[n,n_o] \longrightarrow X_3[n,n_o] \longrightarrow X_1/n,n_oX_1$$

$$\quad \longrightarrow X_2/n,n_oX_2 \longrightarrow X_3/n,n_oX_3 \longrightarrow 0.$$

Note that each $\phi_i$ is in $m$ and so $n,n_o \in m^t$ for $t = n - n_o + 1$. Hence, it is clear that if $n \gg n_o$, then $X_i[n,n_o] = Z_i$ for $i = 1, 2, 3$, where $Z_i$ denotes the maximal finite $\Lambda$-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

$$|X_2/n,n_oX_2| = |X_1/n,n_oX_1||X_3/n,n_oX_3|p^{-a}$$

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 $\mathbb{Z}_p$-module of finite rank.

Case (a): This is quite easy. If $X$ is finite, then $n,n_o$ annihilates $X$ for $n >> n_o$ and so $X/n,n_oX = X$ 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 $\mathbb{F}_p[[T]]$, which is a principal ideal domain. Therefore,
X is isomorphic to \( F_p[[T]]^r \times \mathbb{Z} \), where \( r \geq 0 \) and \( \mathbb{Z} \) is the \( F_p[[T]] \)-torsion submodule of \( X \). Noting that \( F_p[[T]]/(T^d) \) is finite (of order \( p^d \)) for any integer \( d > 0 \), it follows that \( \mathbb{Z} \) 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 \( \phi_i \) has degree \( p^i - p^{i-1} \). Hence \( \nu_{n,n_0} \) has degree \( p^n - b \) for \( n > n_0 \), where \( b \) is a constant. Also, \( \nu_{n,n_0} \) is not divisible by \( p \) in \( \Lambda \). It follows that \( X/\nu_{n,n_0}X \) has order \( p^{n-b} \) for \( n > n_0 \), again verifying the proposition since \( \lambda(X) = 0 \) and \( \mu(X) = 1 \).

**Case (c).** Assume that \( X \) is a free \( \mathbb{Z}_p \)-module of rank \( l \). Multiplication by \( T \) defines a \( \mathbb{Z}_p \)-linear endomorphism of \( X \). Let \( \alpha_1, \ldots, \alpha_l \) denote the eigenvalues (in \( \overline{\mathbb{Q}_p} \)) 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 \( F_p \)-vector space of dimension \( l \). The characteristic polynomial for the endomorphism \( T \) of \( X/pX \) is \( t^l \) and hence \( g(t) \equiv t^l \mod p\mathbb{Z}_p[t] \). This implies the important fact that \( |\alpha_i|_p < 1 \) for \( 1 \leq i \leq l \).

Thus, if \( f(T) \in \Lambda \), then \( f(\alpha_i) \in \overline{\mathbb{Q}_p} \) 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 \( \mathbb{Z}_p \) determines the order of the cokernel. To be precise, if some \( \alpha_i \) is a root of \( f(T) \), then \( X/f(T)X \) is infinite. Otherwise, write \( \prod_{i=1}^l f(\alpha_i) = p^u \), where \( u \in \mathbb{Z}_p^\times \). Then \( |X/f(T)X| = p^u \).

We take \( f(T) = \nu_{n,n_0} = \prod_{n_0 < j \leq n} \phi_j \). The roots of \( \phi_j(T) \) are the numbers \( \zeta - 1 \), where \( \zeta \) varies over the primitive \( p^j \)-th roots of unity (in \( \overline{\mathbb{Q}_p} \)). Recall that \( \text{ord}_p(\zeta - 1) = 1/(p^j - p^{j-1}) \) for all such roots of unity. Let \( \alpha \) be any one of the \( \alpha_i \)'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 \( \zeta \). Our choice of \( n_0 \) implies that \( \alpha \) is not a root of \( \phi_j \) for \( j > n_0 \). Obviously, if \( j \) is sufficiently large (say, \( j \geq n_1 \)), then \( \text{ord}_p(\zeta - 1) < \text{ord}_p(\alpha) \) for all \( \alpha \in \{\alpha_1, \ldots, \alpha_l\} \). 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 \( \text{ord}_p(\zeta - 1) \) for \( j \geq n_1 \). Thus, for such \( j \), we have

\[
\text{ord}_p(\phi_j(\alpha)) = 1
\]

and so \( \nu_{n,n_0}(\alpha_i) = n + c_i \) for \( n > n_1 \), where \( c_i \in \mathbb{Z} \). It follows that
\[ |X/\nu_{n,n,0}X| = p^{n+d} \text{ for } n \gg 0, \text{ where } d \in \mathbb{Z}. \] Since \( \lambda(X) = l \) and \( \mu(X) = 0 \), we have verified 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 \( X = \mathbb{Z}/p \). The action of \( \Gamma \) on \( X \) would then be given by a continuous homomorphism \( \kappa : \Gamma \to 1 + p\mathbb{Z}_p \). Thus \( \kappa(\gamma) = 1 + \alpha \), where \( \alpha \in p\mathbb{Z}_p \). (In fact, \( \alpha \) is the eigenvalue of \( T = \gamma - 1 \) acting on \( X \).) We assume that the action of \( \Gamma \) is nontrivial. That is, \( \alpha \neq 0 \).

Suppose that \( \text{ord}_p(\alpha) = a \). Then \( X/TX = X/\alpha X \) is cyclic of order \( p^a \).

Now \( 1 + p\mathbb{Z}_p \sim \mathbb{Z}_p \) as a topological group and the image \( \kappa(\Gamma) \) will be the subgroup \( 1 + p^a\mathbb{Z}_p \), which is the unique subgroup of index \( p^a - 1 \). That is, \( \text{ord}_p(\kappa(\gamma^{p^n}) - 1) = p^{a+n} \). It follows that \( X/\omega_nX \) is cyclic of order \( p^{a+n} \). 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 \( \text{rank}_{\mathbb{Z}_p}(X/\nu_{n,n,0}X) = \text{rank}_{\mathbb{Z}_p}(X/\nu_{n,n,0}X) \) for all \( n \geq n_o \). The two properties are equivalent. The following result concerns the growth of the torsion subgroup of \( X/\nu_{n,n}X \).

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

\[ |(X/\nu_nX)_{\text{tors}}| = p^{(\lambda - \lambda_o)n + \mu p^n + \nu}, \]

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

**Proof.** Let \( Y = \omega_{n,n}X \). Then \( \lambda(Y) = \lambda - \lambda_o \). We have \( \omega_nX = \nu_{n,n,0}Y \) for \( n \geq n_o \). Also, \( Y/\nu_{n,n,0}Y \) is finite for all such \( n \). We have an exact sequence

\[ 0 \to Y/\nu_{n,n,0}Y \to (X/\omega_nX)_{\text{tors}} \to (X/Y)_{\text{tors}} \to 0 \]

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 \( \beta \in p\mathbb{Z}_p \).

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

\[
\text{ord}_p\left(|X/(T - \beta)X|\right) = \text{ord}_p\left(f_X(\beta)\right).
\]

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 \( \beta \) is not a root of \( g_X(T) \). To calculate the order of \( X/(T - \beta)X \), consider the exact sequence

\[
0 \rightarrow Y \rightarrow X \rightarrow X/Y \rightarrow 0
\]

where \( Y \) is the \( \mathbb{Z}_p \)-torsion submodule of \( X \). Thus, \( Y = X[p^t] \) for some \( t \geq 0 \). We assume that \( X \) has no nonzero \( \Lambda \)-submodules. If one considers the maps induced by multiplication by \( p^{i-1} \) on \( X \) for \( i \geq 1 \), then one sees that \( X[p^t]/X[p^{i-1}] \) is isomorphic to a \( \Lambda \)-submodule of \( X \) and hence also has no nonzero \( \Lambda \)-submodules. This means that each \( X[p^t]/X[p^{i-1}] \) is free as a \( F_p[[T]] \)-module. On the other hand, \( X/Y \) is a free \( \mathbb{Z}_p \)-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 \( X \cong F_p[[T]] \) or \( X \) is a free \( \mathbb{Z}_p \)-module of rank \( l \). One has \( X/(T - \beta)X \cong F_p \) 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 \( \beta \) is equal to one of the \( \alpha_i \)'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. \( \square \)

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 \( \Lambda \)-module. Choose \( n_0 \) so that \( X/\nu_{n,n_0}X \) is finite for all \( n \geq n_0 \). Assume that \( \mu(X) = 0 \). Then, for all \( n \gg 0 \), there is an isomorphism

\[
X/\nu_{n,n_0}X \cong \bigoplus_{i=1}^{\lambda} \mathbb{Z}/p^{n+c_i} \mathbb{Z} \times C,
\]
where $c_1, \ldots, c_\lambda$ are certain integers and $C$ is isomorphic to the maximal, finite, $\Lambda$-submodule of $X$.

Proof. As a $\mathbb{Z}_p$-module, we have $X \cong U \times Z$, where $U \cong \mathbb{Z}_p^\lambda$. Here $Z$ is a $\Lambda$-submodule of $X$, but $U$ is just a $\mathbb{Z}_p$-submodule. Suppose that $t$ is chosen so that $p^t Z = 0$. Then $p^t U = p^t X$ is a $\Lambda$-submodule of $X$, and has finite index. Hence $\nu_{n,n_0} X \subset p^t U$ for $n \gg n_0$. Note that

$$X/\nu_{n,n_0} X \cong U/\nu_{n,n_0} X \times Z$$

as a $\mathbb{Z}_p$-module. Note that $\nu_{n,n_0} X$ is a free $\mathbb{Z}_p$-module of rank $\lambda$. We will show below that $\nu_{n+1,n_0} X = p\nu_{n,n_0} X$ (6) for $n \geq n_1$, where $n_1$ is chosen in a certain way. Thus, for such $n$, if $U/\nu_{n,n_0} X$ is isomorphic to a direct product of cyclic groups of orders $p^{a_1}, \ldots, p^{a_\lambda}$, then $U/\nu_{n+1,n_0} X$ will be isomorphic to a direct product of cyclic groups of orders $p^{a_1+1}, \ldots, p^{a_\lambda+1}$. The proposition will then follow by induction.

First choose $n_0' \geq n_0$ so that $X' = \nu_{n_0',n_0} X \subset p^i U$. Then $\Gamma$ acts continuously on the quotient group $X'/p^2 X'$. Choose $n_1 \geq n_0'$ so that the subgroup $\Gamma p^{n_1-1}$ acts trivially on this quotient. If $i > n_1$, then $\phi_i = \sum_{j=0}^{p-1} \gamma_j i n_1^{-1}$ acts on $X'/p^2 X'$ as multiplication by $p$. A simple application of Nakayama's lemma (for $\mathbb{Z}_p$-modules) implies that $\phi_i X' = p X'$. Let $n \geq n_1$. Then, taking $i = n + 1$ and multiplying by $\nu_{n,n_0'}$, 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 $\text{dim}_{\mathbb{F}_p}(A[p])$ as the $p$-rank of $A$. The $p$-rank of $A$ is also clearly equal to $\text{dim}_{\mathbb{F}_p}(A/pA)$.

**Proposition 2.3.5.** Let $X$ be a finitely generated, torsion $\Lambda$-module. Choose $n_0$ so that $X/\nu_{n,n_0} X$ is finite for all $n \geq n_0$.

1. If $\lambda(X) > 0$, then the exponent of $X/\nu_{n,n_0} X$ is equal to $p^{a+c}$ for all $n \gg 0$, where $c$ is some integer. If $\lambda(X) = 0$, then the exponent of $X/\nu_{n,n_0} X$ is bounded and becomes constant for $n \gg 0$.

2. Let $r = \text{rank}_{\mathbb{F}_p[[x]]}(X[p])$. Then the $p$-rank of $X/\nu_{n,n_0} X$ is equal to $rp^a + c$ 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 \( x \not\in Z \), the maximal finite \( \Lambda \)-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 \( \mathbb{Z}_p \)-module of rank \( \lambda(X) \). The maximal finite \( \Lambda \)-submodule of \( X/p^tX \) is of the form \( X_o/p^tX \) for a uniquely determined \( \Lambda \)-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

\[
\nu_{n,n_o}X \cap X_o = \nu_{n,n_o}X_o \quad (7)
\]

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 (7). 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 \( \Lambda \)-module. If \( x_1, \ldots, x_d \) 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 \( x_1, \ldots, x_d \) in that quotient.

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

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

since the \( \mu \)-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 \( \mathbb{F}_p \).

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 \( \Lambda \)-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 \( \coker(f_n) \) are finite and of bounded order as \( n \) varies.

**Proposition 2.3.6.** Let \( X \) be a finitely generated, torsion \( \Lambda \)-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 \( \mu \)-invariants for \( X \). For \( n \geq n_o \), let \( A_n = X/\nu_{n,n_o}X \) and let \( B_n = (\mathbb{Z}/p^n\mathbb{Z})^\lambda \times \prod_{j=1}^r (\mathbb{Z}/p^{\mu_j}\mathbb{Z})^{p^n} \). 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 \( \mu_1, \ldots, \mu_r \).

### 1.4 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 \( X/\omega_nX \) 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 \( \Lambda \)-module. Now the power of \( p \) dividing \( h_n \) is equal to \( |X/\omega_nX| \) 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 \( F_\infty/F \) be a \( \mathbb{Z}_p \)-extension and let \( L_\infty \) denote its pro-\( p \)-Hilbert class field. Then \( X = \text{Gal}(L_\infty/F_\infty) \) is a finitely generated, torsion \( \Lambda \)-module.

**Proof.** If a prime \( v \) of \( F \) is ramified in the \( \mathbb{Z}_p \)-extension \( F_\infty/F \), then the corresponding inertia subgroup \( I_v \) of \( \text{Gal}(F_\infty/F) \) has finite index in \( \Gamma = \text{Gal}(F_\infty/F) \). By proposition 1, there are only finitely many such \( v \)'s and so the intersection of these inertia subgroups has finite index in \( \Gamma \). 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 \( F_\infty/F_{n_o} \) 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 \( L_\infty \). Thus, \( \text{Gal}(L_\infty/K_n) = \omega_nX \). Let \( \eta \) be any prime of \( F_n \) ramified in \( F_\infty/F_n \). There are \( t \) such primes, which we denote by
η_1, \ldots, η_t. Since \( L_∞/F_∞ \) is unramified, only these primes are ramified in the extension \( K_n/F_n \). The corresponding inertia subgroups of \( \text{Gal}(K_n/F_n) \) are all isomorphic to \( \mathbb{Z}_p \) and they generate the subgroup \( \text{Gal}(K_n/L_n) \). Thus, \( \text{Gal}(K_n/L_n) \) is a finitely generated \( \mathbb{Z}_p \)-module which has rank \( \leq t \). It has finite index in \( \text{Gal}(K_n/F_n) \) since \( L_n/F_n \) is a finite extension. Therefore, \( \text{Gal}(K_n/F_n) \) is also a finitely generated \( \mathbb{Z}_p \)-module with the same rank.

It follows that \( X/ω_nX = \text{Gal}(L_∞/F_∞) \) is finitely generated as a \( \mathbb{Z}_p \)-module and has rank \( \leq t − 1 \). Nakayama’s Lemma implies that \( X \) is finitely generated as a \( \Lambda \)-module. On the other hand, lemma 2.2.6 implies that

\[
\text{rank}_{\mathbb{Z}_p}(X/ω_nX) \geq rp^n
\]

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

As the above proof might suggest, it is not always true that the quotients \( X/ω_nX \) 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 \( X/ν_{n,n_o}X \) 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 \( [L_n : F_n]/|X/ν_{n,n_o}X| \) 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 \( \text{Gal}(L_∞/F_n) \) for the primes over \( p \).

**Proposition 2.4.2.** Let \( F_∞/F \) be a \( \mathbb{Z}_p \)-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 \( X = \text{Gal}(L_∞/F_∞) \) and \( Y = \text{Gal}(L_∞/L_{n_o}F_∞) \). Then

\[
X/ν_{n,n_o}Y = \text{Gal}(L_n/F_n)
\]

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 \( L_n^* \cap F_∞ = F_n \). It therefore follows that \( \text{Gal}(L_n^*/F_n) \cong \text{Gal}(L_n^*F_∞/F_∞) \), which is clearly abelian. Thus, \( L_n^* = L_n \).

Let \( G_n = \text{Gal}(L_∞/F_n) \). 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
$L_\infty/F_n$ are the same as those ramified in $F_\infty/F_n$, and we denote them by $\eta_1, \ldots, \eta_t$. The number $t$ of such primes is independent of $n$ because $n \geq n_0$.

Each inertia subgroup for a prime of $L_\infty$ above one of the $\eta_i$'s is canonically isomorphic to $\Gamma_n$ (by the restriction map). We have $L_n^* = L^H_n$ by definition and therefore $H_n = \text{Gal}(L_\infty/L_n)$.

Let $Y_n = H_n \cap X$. Then $Y_n = \text{Gal}(L_\infty/L_n F_\infty)$. In particular, $Y$ (as defined in the proposition) is just $Y_{n_0}$. It is also clear that $X/Y_n = \text{Gal}(L_n/F_n)$. So it remains just to prove that $Y_n = \nu_{n,n_0} Y_{n_0}$ for all $n \geq n_0$.

Let $R$ denote the set of primes $\eta$ of $L_\infty$ ramified in the extension $L_\infty/F_{n_0}$. For each $\eta \in R$, let $I_\eta$ denote the corresponding inertia subgroup of $G_{n_0}$. Then, as we noted above, $I_\eta = \Gamma_{n_0} = \mathbb{Z}_\eta$. For $n \geq n_0$, the inertia subgroup of $G_n$ for $\eta$ will be $I_\eta \cap G_n$. This will be the unique subgroup of $I_\eta$ of index $p^{n-n_0}$, namely $I^{p^m}$ where we put $m = n - n_0$ for brevity.

Choose a topological generator $\gamma_{n_0}$ for $\Gamma_{n_0}$. For each $\eta \in R$, let $g_\eta$ denote the element of $I_\eta$ such that $g_\eta|_{F_\infty} = \gamma_{n_0}$. If $\eta, \eta' \in R$, then $g_\eta$ and $g_{\eta'}$ are in the same coset in $G_{n_0}/X$ 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 $(\eta, \eta')$ 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 $y^\theta$ in place of $\theta y$. We will now do a simple calculation in $G_{n_0}$ to show that $y(\eta, \eta')^{\nu_{n,n_0}} = y_n(\eta, \eta')$. This implies that $Y^{\nu_{n,n_0}} = Y_n$, from which proposition 2.4.2 follows.

Let $a = g_\eta$, $b = g_{\eta'}$, $y = ab^{-1} = y(\eta, \eta')$, and $\gamma = \gamma_{n_0}$. Note that $y_n^{\nu_{n,n_0}} = \sum_{i=0}^{p^m-1} \gamma^i$. Also, since $b|_{F_{n_0}} = \gamma$, we have $b^i y b^{-i} = y^{\gamma^i}$ for $0 \leq i < p^m$. Therefore,

$$y_{n,n_0}^{p^m} = \prod_{i=0}^{p^m-1} b^i y b^{-i} = (yb)^{p^m} b^{-p^m} = a^{p^m} b^{-p^m} = y_n(\eta, \eta')$$

as we stated above.

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

$$h_n^{(p)} = |\text{Gal}(L_n/F_n)| = |X/Y||Y/\nu_{n,n_0} Y|$$
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 \( \mathbb{Z}_p \)-extension \( F_\infty/F \). One can then take \( n_o = 0 \) in proposition 2.4.2 and so \( Y = \text{Gal}(L_\infty/L_0F_\infty) \). The Galois group \( G = \text{Gal}(L_\infty/F) \) now acts transitively on the set \( R \) occurring in the proof of proposition 2.4.2. Thus, the inertia groups \( I_\eta \)'s are conjugate in \( G \) and the elements \( g_\eta \) 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, \( G/Y = \text{Gal}(L_0F_\infty/F) \) is abelian. This implies that \( G' \subset Y \). Hence \( Y = G' = TX \). Therefore, it follows that \( Y_n = \nu_{n,0}Y = \omega_nX \) 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 \( F_\infty/F \) 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 \( \mathbb{Z}_p \)-extension just by replacing the base field \( F \) by \( F_{n_o} \).

**Proposition 2.4.4.** Suppose that RamHyp(2) is satisfied for the \( \mathbb{Z}_p \)-extension \( F_\infty/F \). 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 \( Y = \text{Gal}(L_\infty/L_0F_\infty) \) 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 \( \mathbb{Z}_p \)-extension \( F_\infty/F \). 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 $F_{\infty}/F$ be a $\mathbb{Z}_p$-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 $A_n \cong \prod_{i=1}^{\lambda} \mathbb{Z}/p^{n+c_i} \mathbb{Z} \times C$ for $n \gg 0$, where $c_1, \ldots, c_\lambda$ 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 $X/\nu_{n,n_0} Y$ for $n \gg 0$. We already have similar results for the quotients $Y/\nu_{n,n_0} Y$.

To prove part a, note that since $X$ is a finitely generated $\Lambda$-module, it is enough to consider the order of the image of $x$ in $X/\nu_{n,n_0} Y$, 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 $Y/\nu_{n,n_0} Y$ has order $p^{n+c}$ for $n \gg 0$, where $c$ is some integer. Thus, the image of $x$ in $X/\nu_{n,n_0} Y$ will have order $p^{n+c+t}$, and a follows.

For part b, note that $(X/\nu_{n,n_0} Y)/p(X/\nu_{n,n_0} Y)$ is isomorphic to $\tilde{X}/\nu_{n,n_0} \tilde{Y}$, where $\tilde{X} = X/pX$ and $\tilde{Y}$ denotes the image of $Y$ under the natural map $X \to \tilde{X}$. The result then follows from proposition 2.3.1 applied to the $\Lambda$-module $\tilde{Y}$.

The proof of part c is just a slight variation on the proof of proposition 2.3.4, using (6) for $Y$ instead of $X$. $\blacksquare$

**Remark 2.4.8.** The group $C$ occurring in the above proposition is isomorphic to the maximal, finite $\Lambda$-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 $\mu_1, \ldots, \mu_r$ be the finer $\mu$-invariants for the $\Lambda$-module $X$, which were defined in section 2.3. Then we have

$$A_n \cong (\mathbb{Z}/p^n \mathbb{Z})^\lambda \times \prod_{j=1}^{r} (\mathbb{Z}/p^{\mu_j} \mathbb{Z})^{\mu^n}$$
This follows immediately from propositions 2.4.2 and 2.3.6.

1.5 Structure of the ideal class group of $F_\infty$.

Suppose that $F_\infty = \bigcup_{n \geq 0} F_n$ is a $\mathbb{Z}_p$-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 $F_\infty$ can be defined as $C_\infty = \lim_{\rightarrow} C_n$, 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 $A_\infty = \lim_{\rightarrow} A_n$, (defined by the same maps $J_{n,m}$, restricted to the $A_n$’s). This is the $p$-primary subgroup of $C_\infty$. There is a natural action of $\Gamma$ on $A_\infty$, which we can then regard as a discrete $\Gamma$-module and hence as a discrete $\Lambda$-module. Here is one important result. We denote the Iwasawa invariants $\lambda$ and $\mu$ occurring in the growth formula by $\lambda(F_\infty/F)$ and $\mu(F_\infty/F)$, respectively.

**Proposition 2.5.1.** The $\Lambda$-module $A_\infty$ is cofinitely generated, cotorsion, and copure of dimension 1. In particular, if $\mu(F_\infty/F) = 0$, then $A_\infty \cong (\mathbb{Q}_p/\mathbb{Z}_p)^\lambda$ 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 $\Lambda$-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 $X \to \text{Gal}(L_n/F_n)$ is surjective when $n \gg 0$. Also, $\text{Gal}(L_n/F_n)$ 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 $\Gamma$ and can be viewed as $\Lambda$-modules. The isomorphisms will be as $\Lambda$-modules.

Since $X$ is a finitely generated, torsion $\Lambda$-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 $\Lambda$-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 $A_\infty$ is cofinitely generated and cotorsion as a $\Lambda$-module.
We will show that $A_\infty$ is copure of dimension 1 as a $\Lambda$-module. This means that the Pontryagin dual of $A_\infty$ has no nonzero, finite $\Lambda$-submodules. Such a submodule would correspond to a quotient of $A_\infty$. Let $\widetilde{A}_\infty = A_\infty/B_\infty$ be the maximal, finite $\Lambda$-module quotient of $A_\infty$. Thus, $B_\infty$ is the maximal, $\Lambda$-submodule of $A_\infty$ which is copure of dimension 1. For each $n \geq 0$, define $B_n$ to be the inverse-image of $B_\infty$ under the map $J_{n,\infty}$. Clearly, $B_n$ is a Gal($F_n/F$)-invariant subgroup of $A_n$. We denote $A_n/B_n$ by $\widetilde{A}_n$. There are maps $\tilde{J}_{n,m}$, $\tilde{J}_{n,\infty}$, and $\tilde{N}_{m,n}$ 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

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

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

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

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

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

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

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

will hold for all $\tilde{a} \in \widetilde{A}_n$. 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 $\tilde{a} \to \tilde{a}^{p^{m-n}}$ cannot be an isomorphism of $\widetilde{A}_n$ if that group is nontrivial. It follows that $\widetilde{A}_\infty = 0$ and hence $A_\infty$ is copure of dimension 1, as claimed.

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

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

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

To see this, just note that if $\theta \in \text{Ann}(X)$, then $\theta$ annihilates the $\Lambda$-modules $A_n^\ast$ for sufficiently large $n$, and so clearly $\theta \in \text{Ann}(A_\infty)$. 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 $\Lambda$-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 $\mathbb{Z}_p$-extension $F_\infty/F_{n_o}$ satisfies RamHyp(2). Let $Y = \text{Gal}(L_\infty/L_{n_o}F_\infty)$ 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 $X \to \text{Gal}(L_n/F_n)$ with the inverse Artin isomorphism $\text{Art}_{L_n/F_n}^{-1} : \text{Gal}(L_n/F_n) \to A_n$. We then have the following commutative diagram

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

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

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

where $N_{\text{Gal}(F_m/F_n)} : A_m \to A_m$ is the norm operator for $\text{Gal}(F_m/F_n)$, acting on $A_m$. If $g$ is a generator of $\text{Gal}(F_m/F_n)$, 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 $\Gamma$-homomorphism. We can lift the norm operator $N_{\text{Gal}(F_m/F_n)}$ on $A_m$ to $X$ as follows. Recall that $1 + T \in \Lambda$ acts on $X$ as $\gamma_o$. Let $\gamma_n = \gamma_o^{p^n}$, which is a topological generator for $\text{Gal}(F_\infty/F_n)$. Then $(1 + T)^{p^n}$ acts on $X$ as $\gamma_n$. Since $g = \gamma_n|_{F_m}$ generates $\text{Gal}(F_m/F_n)$, the element $\sum_{i=0}^{p^{m-n}-1}(1 + T)^i \in \Lambda$ is a lifting of $N_{\text{Gal}(F_m/F_n)}$. This element is $\omega_m/\omega_n = \nu_{m,n}$.

We then have $\alpha_m(\nu_{m,n}x) = N_{\text{Gal}(F_m/F_n)}(\alpha_m(x))$. This is indeed equal to $J_{n,m}(\alpha_n(x))$, and so diagram (8) is commutative. Now take $m \geq n \geq n_o$. 

31
Define a map
\[ j_{n,m} : x/\nu_{n,n}Y \to x/\nu_{m,n}Y \]
by \( j_{n,m}(x + \nu_{n,n}Y) = \nu_{m,n}x + \nu_{m,n}Y \). It follows that
\[ \ker(J_{n,m}) \cong \ker(j_{n,m}) \] (9)

Since \( \nu_{n,m}(\nu_{n,n}Y) = \nu_{m,n}Y \), we have
\[ \ker(j_{n,m}) = (X[\nu_{n,m}] + \nu_{n,n}Y)/\nu_{n,n}Y \cong X[\nu_{n,m}]/(X[\nu_{n,m}] \cap \nu_{n,n}Y) \]
Since \( m \geq n \geq n_0 \), 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
\[ \ker(J_{n,\infty}) \cong Z/(Z \cap \nu_{n,n}Y) \] (10)
The subgroups \( \{\nu_{n,n}Y \mid n \geq n_0\} \) form a base of neighborhoods of 0 in \( X \), and so it is also clear that \( Z \cap \nu_{n,n}Y = 0 \) for \( n \gg n_0 \), proving the stated result. \( \blacksquare \)

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 \( Q_\infty \), 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.

1.6 The base field \( F = Q(\mu_p) \).

In this section, we will continue to discuss the important example \( F = Q(\mu_p) \). 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 \( \mathbb{Z}_p \)-extension of \( F = Q(\mu_p) \) is \( F_\infty = Q(\mu_{p_\infty}) \). Earlier results in this chapter give us some rough, general picture of the structure of \( X = \text{Gal}(L_\infty/F_\infty) \), where \( L_\infty \) is the pro-\( p \) Hilbert class field of \( F_\infty \). 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 \(\mu\)-invariant \(\mu(X)\) vanishes.

III. If \(p \nmid h_{F^+}\), then \(X\) is a free \(\mathbb{Z}_p\)-module.

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

V. If \(p < 12,000,000\), then \(p \nmid h_F\) and \(\text{rank}_{\mathbb{Z}_p}(X)\) 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 \(\mathbb{Z}_p\)-extension of any abelian extension \(F\) of \(Q\).) We will give two proofs in Chapter 7. Assuming that result, the third assertion just means that the maximal finite \(\Lambda\)-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 \(L_{\infty}\) is a Galois extension of \(Q\). Thus \(X\) is a normal subgroup of \(\text{Gal}(L_{\infty}/Q)\) and so admits a continuous \(\mathbb{Z}_p\)-linear action of \(G = \text{Gal}(F_{\infty}/Q)\). If \(p \nmid h_{F^+}\), then \(X\) is a free \(\mathbb{Z}_p\)-module (according to \(III\)). The assertion that \(X\) is cyclic as a \(G\)-module then means that \(X\) is spanned as a \(\mathbb{Z}_p\)-module by \(\{gx_o \mid g \in G\}\) for some \(x_o \in X\). Now the structure of \(X\) as a \(\Lambda\)-module reflects the action of \(\Gamma = \text{Gal}(F_{\infty}/F)\) on \(X\). The finite group \(\Delta = \text{Gal}(F_{\infty}/Q_{\infty})\) (which is a subgroup of \(G\) also acts on \(X\). Since \(G\) is commutative, the actions of \(\Gamma\) and \(\Delta\) on \(X\) commute. That is, the action of \(\Delta\) on \(X\) is \(\Lambda\)-linear. Therefore, it is natural to consider \(X\) as a module for the ring \(\Lambda[\Delta]\) - the group ring for \(\Delta\) over \(\Lambda\). 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 \(\Lambda\)-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 $\mathbb{Z}_p$-extension $F_\infty/F$ is $F_n = \mathbb{Q}(\mu_{p^{n+1}})$. 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 $\Delta$-components of $X$ have no nonzero, finite $\Lambda$-submodules. In other words, for each odd $i$, the $\Lambda$-module $X^{(\omega^i)}$ is pure of dimension 1. Note that $Z$ is $\Delta$-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 $\Delta$-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 $F_\infty/F$, we have a canonical isomorphism $X/TX \cong A_F$. This isomorphism is $\Delta$-equivariant. We can decompose $X$ as a $\mathbb{Z}_p[\Delta]$-module as follows:

$$X \cong \prod_{i=0}^{p-2} X^{(\omega^i)} \tag{11}$$

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 $\Lambda$-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 $\Delta$-component $X^{(\omega_i)}$ is a free $\mathbb{Z}_p$-module if $p \nmid h_{F^+}$. Assertion $V$ then means that $\text{rank}_{\mathbb{Z}_p}(X^{(\omega_i)}) \leq 1$, assuming that $p < 12,000,000$. Thus, for those $i$'s for which $X^{(\omega_i)}$ is nontrivial, we have $X^{(\omega_i)} \cong \mathbb{Z}_p$ and the action of $\Gamma$ on $X^{(\omega_i)}$ is by a character $\langle \chi \rangle^{s_i}$, where $s_i \in \mathbb{Z}_p$.

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 $\Lambda$-module $X$ to the groups $H^1_{\text{unr}}(\mathbb{Q}, D_\psi)$, where $\psi$ is a power of the cyclotomic character $\chi$ and $D_\psi$ denotes the Galois module associated to $\psi$ as defined in section 1.6. Thus, we assume that $\psi : \text{Gal}(F_\infty/\mathbb{Q}) \to \mathbb{Z}_p^\times$ 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

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

If $\psi(\gamma_0) = 1 + \beta_\psi$, 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 $H^1_{\text{unr}}(\mathbb{Q}, D_\psi)$ is finite if and only if $f_i(\beta_\psi) \neq 0$. We then have

$$\text{ord}_p(|H^1_{\text{unr}}(\mathbb{Q}, D_\psi)|) = \text{ord}_p(f_i(\beta_\psi)).$$

if $i$ is odd.

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

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

For the second step, note that $H^0(F_\infty, D_\psi) = D_\psi$. The inflation-restriction sequence for the extension $F_\infty/F$ 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 $\Gamma$. These will be summarized in the lemma below. Let $\Gamma_n = \Gamma^{p^n}$ for $n \geq 0$. By definition, we have

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

under the natural inflation maps. We will let $N_{\Gamma/\Gamma_n}$ denote the norm map for the action of the finite cyclic group $\Gamma/\Gamma_n$ on $A^{\Gamma_n}$. The kernel will be denoted simply by $\ker(N_{\Gamma/\Gamma_n})$, a subgroup of $A^{\Gamma_n}$, a subgroup of $A^\Gamma$. 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 $N_{\Gamma/\Gamma_m}(a)$ in the second group. But $N_{\Gamma/\Gamma_m}(a) = p^{m-n}a$ since $a$ is fixed by $\Gamma$. 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

$$\ker(N_{\Gamma/\Gamma_n})/(\gamma_0 - 1)A^{\Gamma_n} \longrightarrow \ker(N_{\Gamma/\Gamma_m})/(\gamma_0 - 1)A^{\Gamma_m}$$

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, $\bigcup_{n\geq0}(\ker(N_{\Gamma/\Gamma_n}) = A$. On the other hand, it is clear that $\bigcup_{n\geq0}((\gamma_0 - 1)A^{\Gamma_n}) = (\gamma_0 - 1)A$. We have proved most of the following basic lemma.

**Lemma 2.6.2.** If $A$ is a discrete, $p$-primary $\Gamma$-module, then

$$H^1(\Gamma, A) \cong A/(\gamma_0 - 1)A, \quad H^2(\Gamma, A) = 0$$

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

To prove the final part of this lemma, note that $A \cong (\mathbb{Q}_p/\mathbb{Z}_p)^r$ for some $r \geq 0$. We can regard $\gamma_0 - 1$ as an endomorphism of that group. The kernel of that
endomorphism is $A^\Gamma$ and, if that kernel is finite, then the image is a divisible group of $\mathbb{Z}_p$-corank $r$, and hence must also be isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^r$. 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

$$0 \rightarrow D_\psi/(\gamma_o - 1)D_\psi \rightarrow H^1(F, D_\psi) \rightarrow H^1(F, D_\psi) = 0$$

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 $H^1(F, D_\psi) \rightarrow H^1(F, D_\psi)$. Just as in the proof of proposition 1.5.5, we must consider the kernel of the restriction map $H^1(I_v, D_\psi) \rightarrow H^1(I_\eta, D_\psi)$, where $v$ is a prime of $F$, $\eta$ is a prime of $F$ lying over $v$, and $I_v, I_\eta$ are the inertia subgroups of $G_F$ and $G_{F_{\infty}}$ for a prime of $\mathbb{Q}$ lying over $\eta$. However, if $v \nmid p$, then $v$ is unramified in $F_{\infty}/F$. 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 $\eta$ of $F_{\infty}$ lying over $v$. Also, $v$ is totally ramified in $F_{\infty}/F$, the inertia subgroup of $\Gamma$ for $v = \Gamma$, and hence $I_v/I_\eta$ can be identified with $\Gamma$. 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

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

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 $H^1(F, D_\psi) \rightarrow H^1(F_{\infty}, D_\psi)\Gamma$ has a nontrivial kernel, namely $H^1(\Gamma, D_\psi) = \text{Hom}(\Gamma, D_\psi)$. This group is isomorphic to $\mathbb{Q}_p/\mathbb{Z}_p$. However, consider the composite map

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

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

$$\ker(H^1_{\text{unr}}(F, D_\psi) \rightarrow H^1_{\text{unr}}(F_{\infty}, D_\psi)) = H^1_{\text{unr}}(F, D_\psi) \cap H^1(\Gamma, D_\psi) = 0$$

37
To show that the cokernel of the map \( H^1_{unr}(F, D_\psi) \to H^1_{unr}(F, D_\psi)^\Gamma \) 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 \( \ker(b_{F'/F}) \to \ker(c_{F'/F}) \) is surjective. Therefore, the map \( \ker(c_{F'/F}) \to \ker(a_{F'/F}) \) is the zero-map. Also, since \( G = \Gamma, \) lemma 2.6.2 implies that \( \text{coker}(b_{F'/F}) = 0. \) It then follows that \( \text{coker}(a_{F'/F}) = 0. \)

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

\[
H^1_{unr}(\mathbb{Q}, D_\psi) \to H^1_{unr}(F_\infty, D_\psi)^{\text{Gal}(F_\infty/\mathbb{Q})}
\]

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

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

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

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

\[
\text{Hom}_\Gamma(X^{(\omega^i)}, D_\psi) = \text{Hom}(X^{(\omega^i)}/(\gamma_o - (1 + \beta_\psi))X^{(\omega^i)}, D_\psi)
\]

which is indeed isomorphic to the Pontryagin dual of \( X^{(\omega^i)}/(T - \beta_\psi))X^{(\omega^i)} \) since \( D_\psi \cong \mathbb{Q}_p/\mathbb{Z}_p \) as a group. This proves the second statement in the proposition. It is then clear that \( H^1_{unr}(\mathbb{Q}, D_\psi) \) 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 \( \Lambda \)-submodules. The final statement follow then follows. \( \blacksquare \)

**Remark 2.6.3.** It is worth discussing what happens for an arbitrary \( \mathbb{Z}_p \)-extension \( F_\infty/F. \) We consider any number field \( F \) and let \( p \) be any prime. Let \( D = D_\psi, \) where \( \psi \in \text{Hom}(\Gamma, \mathbb{Z}_p^\omega). \) Assume first that \( \psi \) has infinite
order. Then $F_\infty = F(D)$ and $D^F$ is finite and nontrivial. The cokernel of the restriction map

$$H^1(F, D) \longrightarrow H^1(F_\infty, D)^\Gamma$$

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 $H^1(F_{unr}, D)_v \longrightarrow H^1(F_{\eta \unr}, D)$ is injective for every ramified prime $v$ in the extension $F_\infty/F$, where $\eta$ is a prime of $F_\infty$ lying over $v$. Therefore, we again get an isomorphism

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

where $X = X_{F_\infty/F}$. In particular, if we let $\beta = \psi(\gamma_0) - 1$, then $H^1_{unr}(F, D)$ is infinite if and only if $f_X(\beta) = 0$. On the other hand, if $\psi$ 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 $\psi \in \text{Hom}(\Gamma, \mathbb{Z}_p^\times)$.

If $\psi$ has finite order, then $\psi$ is the trivial character unless $p = 2$. For $p = 2$, the character $\psi$ could have order 1 or 2. It is not difficult to verify that the kernel of the map (13) 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 $F_\infty/F_n$.

However, the cokernel of (13) can be infinite. In particular, if $\psi$ 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 $F/\mathbb{Q}$, and that $F_\infty$ is the cyclotomic $\mathbb{Z}_p$-extension of $F$. This situation was discussed briefly following the proof of proposition 1.6.4. For $s \in \mathbb{Z}_p$, let $\psi_s = \langle \chi \rangle^s$. Thus, $\psi_s$ has infinite order if $s \neq 0$. Let $D_s = D_{\psi_s}$ and $\beta_s = \psi_s(\gamma_0) - 1$). Thus, $\beta_s \to 0$ as $s \to 0$ in $\mathbb{Z}_p$. For $s \neq 0$, we have

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

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 $\mathbb{Z}_p$. It follows that $f_X(\beta_s) \to 0$ as $s \to 0$ and therefore $f_X(0) = 0$. 

39