$\mathbb{Z}_p$-extensions

Based on *Chapter 13 of Introduction to Cyclotomic Extensions* by Lawrence C. Washington

Alexandre Daoud
alex.daoud@cantab.net

Contents

Throughout this document, we shall fix a prime p. Unless otherwise stated, K shall refer to a number field. If $\mathfrak{p}$ is a prime of K, we shall denote by $K_\mathfrak{p}$ the completion of K at $\mathfrak{p}$. When $\mathfrak{p}$ is non-archimedean, we denote by $\mathcal{O}_{K,\mathfrak{p}}$ its ring of integers, $U_{K,\mathfrak{q}}$ for its unit group and $U_{K,\mathfrak{p}}^{(n)}$ for the n^{th} unit group of $\mathcal{O}_{K,\mathfrak{p}}$, $n > 0$. By $v_\mathfrak{p}$ we shall mean the $\mathfrak{p}$-adic valuation on K and $K_\mathfrak{p}$ and similarly for the $\mathfrak{p}$-adic absolute value $|\cdot|_\mathfrak{p}$. By $\mathbb{F}_{K_\mathfrak{p}}$, we shall mean the residue field of $K_\mathfrak{p}$. When it is evident which number field we are working in, we shall drop K from the subscript.

1 Basic Properties of $\mathbb{Z}_p$-extensions

Definition 1.1. Let K_∞/K be a Galois extension. We say that K_∞/K is a $\mathbb{Z}_p$**-extension** if $\mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$ as topological groups.

Proposition 1.2. *Let K_∞/K be a $\mathbb{Z}_p$-extension. Then for each $n \in \mathbb{N}$ is a unique intermediate field $K \subseteq K_n \subseteq K_\infty$ such that $[K^n : K] = p^n$. Moreover, these are exactly all intermediate fields of K_∞/K.*

Proof. By the Fundamental Theorem of Galois Theory, the intermediate extensions of L of K_∞/K are in one-to-one correspondence with the closed subgroups C_L of $\mathbb{Z}_p$. Moreover, $[L : K] = [\mathbb{Z}_p : C_L]$. Hence it suffices to determine the closed subgroups of $\mathbb{Z}_p$. Let $S \subseteq \mathbb{Z}_p$ be a non-zero closed subgroup. Fix $x \in S$ such that $v_p(x)$ is minimal. Clearly, $x\mathbb{Z} \subseteq S$. But S is closed and so $x\mathbb{Z}_p \subseteq S$. By the choice of x, we necessarily then have that $S = x\mathbb{Z}_p = p^n\mathbb{Z}_p$. □

Proposition 1.3. *Let K_∞/K be a $\mathbb{Z}_p$-extension and $\mathfrak{q}$ a prime of K not lying over p. Then K_∞/K is unramified at $\mathfrak{q}$.*

Proof. Let $I_\mathfrak{q} \subseteq \mathrm{Gal}(K_\infty/K)$ denote the inertia group for $\mathfrak{q}$. Let $\mathfrak{q}_\infty$ be a prime of K_∞ lying over $\mathfrak{q}$ and denote by $\overline{K_\infty}$ the completion of K_∞ at $\mathfrak{q}_\infty$. Since we have a continuous surjection

$$\pi : \mathrm{Gal}(\overline{K_\infty}/K_\mathfrak{p}) \twoheadrightarrow \mathrm{Gal}(\mathbb{F}_{\overline{K_\infty}}/\mathbb{F}_{K_\mathfrak{q}})$$

given by the reduction map and $I_\mathfrak{q} = \pi^{-1}(\{1\})$, it follows that $I_\mathfrak{q}$ is closed in $\mathbb{Z}_p$. Hence $I_\mathfrak{q} = 0$ or $I_\mathfrak{q} = p^n\mathbb{Z}_p$ for some $n \geq 1$. In the former case, we are done so assume that there exists some $n \geq 1$ such that $I_\mathfrak{q} = p^n\mathbb{Z}_p$. Then $I_\mathfrak{q}$ is infinite. Since $|I_\mathfrak{q}| = 1$ or 2 when $\mathfrak{q}$ is archimedean, we must have that $\mathfrak{q}$ is non-archimedean.

By Local Class Field Theory, the local Artin map induces a continuous surjective homomorphism

$$[-, \overline{K_\infty}/K_\mathfrak{q}] : U_{K,\mathfrak{q}} \longrightarrow\!\!\!\!\!\rightarrow I_\mathfrak{q}$$

Let q be the rational prime lying under $\mathfrak{q}$. Then the logarithm map induces a surjective homomorphism

$$\log : U_{K,\mathfrak{q}} \to \mathcal{O}_{K,\mathfrak{q}}$$

Since this map has finite kernel A and $\mathcal{O}_{K,\mathfrak{q}}$ is a free $\mathbb{Z}_q$-module of rank $m = [K : \mathbb{Q}]$, we then have the isomorphism

$$U_{K,\mathfrak{q}} \cong A \times \mathbb{Z}_q^m$$

Composing this with the local Artin map gives a continuous surjective homomorphism

$$A \times \mathbb{Z}_q^m \twoheadrightarrow p^n\mathbb{Z}_p$$

But $p^n\mathbb{Z}_p$ is torsion-free as a $\mathbb{Z}_p$-module so we in fact have a continuous surjective homomorphism $\mathbb{Z}_q^m \twoheadrightarrow p^n\mathbb{Z}_p$. This induces a continuous surjective homomorphism

$$\mathbb{Z}_q^m \twoheadrightarrow p^n\mathbb{Z}_p/p^{n+1}\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$$

But $\mathbb{Z}_q^m$ has no closed subgroups of index p. Hence $I_\mathfrak{q} = 0$ and so K_∞/K is unramified outside p. □

Proposition 1.4. *Let K_∞/K be a $\mathbb{Z}_p$-extension and K_n the intermediate fields. Then at least one prime of K ramifies in K_∞ and there exists $n \in \mathbb{N}$ such that every prime of K_n which ramifies in K_∞/K_n is totally ramified.*

Proof. Recall that the Hilbert class field of K is the maximal unramified abelian extension of K and is of finite degree over K. Since K_∞/K is an infinite extension, it follows that at least one prime of K must ramify in K_∞.

By Proposition 1.3, the only possible primes of K that could ramify in K_∞ are exactly those that lie over p. Denote them $\mathfrak{p}_1, \ldots, \mathfrak{p}_m$ and let $I_1, \ldots, I_m$ be their corresponding inertia groups. Then

$$\bigcap_{j=1}^{m} I_j = p^n\mathbb{Z}_p$$

for some $n \geq 1$. Now, the fixed field of $p^n\mathbb{Z}_p$ and by the Galois correspondence we have that $\mathrm{Gal}(K_\infty/K_n) \subseteq I_j$ for all j. It then follows that all the primes above each $\mathfrak{p}_j$ are totally ramified in K_∞/K_n. □

Example 1.5. Let K be a number field and and $\overline{\mathbb{Q}}$ an algebraic closure of $\mathbb{Q}$. We can construct a $\mathbb{Z}_p$-extension of K in the following way. Let μ_{p^∞} be the group of all p-power roots of unity in $\overline{\mathbb{Q}}$. Then $K(\mu_{p^\infty})/K$ is Galois and we have a continuous injective homomorphism

$$\phi : \mathrm{Gal}(K(\mu_{p^\infty})/K) \to \mathbb{Z}_p^\times$$

defined in the following way. Given $\sigma \in \mathrm{Gal}(K(\mu_{p^\infty})/K)$ and $n \geq 0$, there exists a $u_n \in \mathbb{Z}$ such that $\sigma(\zeta) = \zeta^{u_n}$ for all $\zeta \in \mu_{p^n}$. Such a u_n is uniquely determined modulo p^n and is coprime to p and so $u_{n+1} \equiv u_n \pmod{p^n}$. We then set

$$\phi(\sigma) = \lim_{n\to\infty} u_n$$

and so $\mathrm{Gal}(K(\mu_{p^\infty})/K)$ is isomorphic to an infinite closed subgroup of $\mathbb{Z}_p^\times$. Such a closed subgroup has finite torsion so, quotienting out by an appropriate subgroup of $\mathrm{Gal}(K(\mu_{p^\infty})/K)$ yields a quotient group isomorphic to $\mathbb{Z}_p$. The corresponding fixed field of this subgroup, denoted K_∞, is called the **cyclotomic $\mathbb{Z}_p$-extension** of K. Note that $K_\infty = K\mathbb{Q}_\infty$

2 Determining the amount of $\mathbb{Z}_p$-extensions

Let K be a number field of degree n. Let $\sigma_1, \ldots, \sigma_n$ be the n distinct embeddings of K into an algebraic closure of K. Let r_1 denote the number of real embeddings and r_2 the number of pairs of complex embeddings. We are interested in how many $\mathbb{Z}_p$-extensions of K there are.

Proposition 2.1. *Let $\mathfrak{p}$ denote a finite prime of K lying above p. Define*

$$U = \prod_{\mathfrak{p}/p} U_{\mathfrak{p}}^{(0)}, \quad U^{(1)} = \prod_{\mathfrak{p}/p} U_{\mathfrak{p}}^{(1)}$$

and consider the diagonal embedding map

$$\begin{aligned} i : \mathcal{O}_K^\times &\to U \\ \varepsilon &\mapsto (\varepsilon, \dots, \varepsilon) \end{aligned}$$

If $E_1 = i^{-1}(U^{(1)})$ then E_1 is a $\mathbb{Z}$-module of rank $r_1 + r_2 - 1$. Moreover, $\overline{E_1}$ (as a subspace of $U^{(1)}$) is a $\mathbb{Z}_p$-module of rank no more than $r_1 + r_2 - 1$.

Proof. Recall that we have an isomorphism

$$U_{\mathfrak{p}}^{(0)} \big/ U_{\mathfrak{p}}^{(1)} \cong \mathbb{F}_{\mathfrak{p}}^\times$$

From which it follows that E_1 has finite index in $\mathcal{O}_K^\times$. By Dirichlet's Unit Theorem, $\mathcal{O}_K^\times$ is a $\mathbb{Z}$-module of rank $r_1 + r_2 - 1$ whence so is E_1. Now, for large enough n, the logarithm map induces an isomorphism of topological groups

$$\log_{\mathfrak{p}} : U_{\mathfrak{p}}^{(n)} \to \mathfrak{p}^n \mathcal{O}_{\mathfrak{p}}$$

so that $U_{\mathfrak{p}}^{(n)}$ is a free $\mathbb{Z}_p$-module of rank $[K_{\mathfrak{p}} : \mathbb{Q}_p]$. We also have, for each $n \geq 1$, an isomorphism

$$U_{\mathfrak{p}}^{(n)} \big/ U_{\mathfrak{p}}^{(n+1)} \cong \mathbb{F}_{\mathfrak{p}}$$

Then $U^{(1)}$ is a free $\mathbb{Z}_p$-module of rank $[K : \mathbb{Q}] = \sum_{\mathfrak{p}/p} [K_{\mathfrak{p}} : \mathbb{Q}_p]$. This then implies that $\overline{E_1}$ is a $\mathbb{Z}_p$-module. Since E_1 has $\mathbb{Z}$-rank $r_1 + r_2 - 1$, $\overline{E_1}$ can have $\mathbb{Z}_p$-rank no larger than $r_1 + r_2 - 1$ as claimed. □

Conjecture 2.2 (Leopoldt)**.** *$\overline{E_1}$ is a finitely generated $\mathbb{Z}_p$-module of rank $r_1 + r_2 - 1$.*

Remark. Leopoldt's conjecture is known to be true in the case that K is an abelian extension.

Let $\mathbb{I}_K$ be the idèle group of K and $\mathcal{C}_K = \mathbb{I}_K / K^\times$ the idèle class group. Let $\mathbb{D}_K$ be the connected component of the identity of $\mathbb{I}_K$.

Lemma 2.3. *We have an isomorphism*

$$\mathbb{D}_K \cong (\mathbb{R}_{\geq 0}^\times)^{r_1} \times (\mathbb{C}^\times)^{r_2}$$

Proof. Recall that non-archimedean fields are totally disconnected and therefore so are their unit groups. Since the cartesian product of totally disconnected spaces is totally disconnected, it follows that $\mathbb{D}_K$ is topologically isomorphic to the connected components of the archimidean completions of K. □

Lemma 2.4. *Let F be a local field of characteristic 0 with residue field $\mathbb{F}$ such that* $\operatorname{char}(\mathbb{F}) = p$. *Then $U_F \cong U_F^{(1)} \oplus \mathbb{F}_p^\times$.*

Proof. Recall that we have an isomorphism

$$U_F / U_F^{(1)} \cong \mathbb{F}^\times$$

so that we have an exact sequence

$$0 \longrightarrow U_F^{(1)} \longrightarrow U_F \longrightarrow \mathbb{F} \longrightarrow 0$$

The Teichmüller lift provides a right splitting of this exact sequence so the Splitting Lemma implies the Lemma. □

Theorem 2.5. *Suppose that* $\operatorname{rank}_{\mathbb{Z}_p}(\overline{E_1}) = r_1 + r_2 - 1 - \delta$. *Then there exist* $r_2 + 1 + \delta$ *independent* $\mathbb{Z}_p$*-extensions of* K. *In particular, if* K' *is the compositum of all* $\mathbb{Z}_p$*-extensions of* K *then* $\mathrm{Gal}(K'/K) \cong \mathbb{Z}_p^{r_2+1+\delta}$.

Proof. Throughout this proof, we shall use the placeholder A to mean a certain finite group whose exact structure can be ignored. Let L be the maximal abelian extension of K which is unramified outside of p. By Proposition 1.3, $K' \subseteq L$. By class field theory, there exists a closed subgroup $K^\times \subseteq H \subseteq \mathbb{I}_K$ such that the global Artin map induces an isomorphism

$$[-, L/K] : \mathcal{C}_K / H \cong \mathrm{Gal}(L/K)$$

and such that $\mathcal{C}_K/H$ is totally disconnected. Given an archimedean prime $\mathfrak{q}$ of K, let $U_\mathfrak{q} = K_\mathfrak{q}^\times$. Furthermore, define the groups

$$U' = \prod_{\mathfrak{p}/p} U_\mathfrak{p}, \quad U'' = \prod_{\mathfrak{q}\nmid p} U_\mathfrak{q}, \quad U = U' \times U''$$

We will identify these groups with their images in $\mathbb{I}_K$. Also note that U is an open subgroup of $\mathbb{I}_K$. Now, since L/K is unramified outside of p, $U'' \subseteq H$. By Lemma we have that $\mathbb{D}_K \subseteq U'' \subseteq H$. But L is the maximal such extension so, necessarily, $H = \overline{K^\times U''}$.

Now define $J' = \mathcal{C}_K/H = \mathrm{Gal}(L/K)$ and

$$J'' = K^\times U/H = U'H/H = U'/(U' \cap H)$$

Letting $U^{(1)} = \prod_{\mathfrak{p}/p} U_{K,\mathfrak{p}}^{(1)}$ as before, Lemma 2.4 implies that $U' = U^{(1)} \times A$. Then

$$J'' \cong A \times U^{(1)}/(U^{(1)} \cap H)$$

Now let $\psi : E_1 \to U^{(1)}$ denote the embedding of E_1 into $\mathbb{I}_K$. Note that $\psi(\varepsilon)_\mathfrak{q} = 1$ when $\mathfrak{q} \nmid p$.

We first require the following Lemma:

Lemma 2.6. $U_1 \cap H = U_1 \cap \overline{K^\times U''} = \overline{\psi(E_1)}$

Proof. Fix $\varepsilon \in E_1$. Observe that

$$\psi(\varepsilon) = \varepsilon \left(\frac{\psi(\varepsilon)}{\varepsilon} \right) \in K^\times U''$$

since $(\psi(\varepsilon)/\varepsilon)_\mathfrak{p} = 1$ when $\mathfrak{p}/p$. By definition, $\psi(\varepsilon) \in U^{(1)}$. Passing to the closure, we get one inclusion.

To prove the other inclusion, denote $U^{(n)} = \prod_{\mathfrak{p}/p} U_{\mathfrak{p}}^{(n)}$. Then since $\mathbb{I}_K$ is a topological group, we have that

$$\overline{K^\times U''} = \bigcap_{n\geq 1} K^\times U'' U^{(n)}$$

Similarly, we have

$$\overline{\psi(E_1)} = \bigcap_{n\geq 1} \psi(E_1) U^{(n)}$$

It thus suffices to show that

$$U^{(1)} \cap K^\times U'' U^{(n)} \subseteq \psi(E_1) U^{(n)}$$

To this end, fix $x \in K^\times, u'' \in U''$ and $u \in U^{(n)}$ and suppose that $xu''u \in U^{(1)}$. Then, clearly, $xu'' \in U^{(1)}$. Now, $(u'')_{\mathfrak{p}} = 1$ for $\mathfrak{p}/p$ so $x \in U_{\mathfrak{p}}^{(1)}$ for such primes. Since $(U_1)_{\mathfrak{q}} = 1$ for $\mathfrak{q} \nmid p$ and u'' is a unit at such primes, it follows that x is a unit everywhere so $x \in E_1 \subseteq \mathcal{O}_K^\times$. But then $xu'' \in \psi(E_1)$ and so $xu''u \in \psi(E_1)U_n$ which completes the proof of the Lemma. □

We are now in a position to prove the Theorem. As before, $U^{(1)} \cong A \times \mathbb{Z}_p^{[K:\mathbb{Q}]}$. Hence

$$U_1/(U_1 \cap H) = U_1/\overline{\psi(E_1)} \cong A \times \mathbb{Z}_p^{r_1+1+\delta}$$

so we have a similar isomorphism for J''. But

$$J'/J'' \cong \mathcal{C}_K/U \cong C_K$$

where C_K is the finite ideal class group of K. Hence $J'/\mathbb{Z}_p^{r_2+1+\delta} \cong A$. Let N be cardinality of the finite group A. Then

$$N\mathbb{Z}_p^{r_2+1+\delta} \subseteq NJ' \subseteq \mathbb{Z}_p^{r_2+1+\delta}$$

so that $NJ' \cong \mathbb{Z}_p^{r_2+1+\delta}$ as a $\mathbb{Z}_p$-module. Let J'_N be the N-torsion subgroup of J'. Then we have isomorphisms

$$J'/J'_N \cong NJ' \cong \mathbb{Z}_p^{r_2+1+\delta}$$

Now suppose that J'_N has order larger than N. By the Pigeonhole Principle, there would exist distinct $x, y \in J'_N$ such that $[x] = [y]$. But the difference $[x] - [y]$ is also killed by N and so $\mathbb{Z}_p^{r_2+1+\delta}$ would have non-trivial N-torsion which it doesn't. Hence $|J'_N| \leq N$. In particular, it has finite cardinality so its fixed field is necessarily K' and the Theorem is proven. □

Corollary 2.7. *Let $K(1)$ be the Hilbert class field of K and L the maximal abelian extension of K unramified outside of p. Then*

$$\mathrm{Gal}(L/K(1)) \cong \left(\prod_{\mathfrak{p}/p} U_{K,\mathfrak{p}} \right) \Big/ \overline{\mathcal{O}_K^\times}$$

Proof. In the notation of the previous proof, $J' \cong \mathrm{Gal}(L/K)$. The closed subgroup J'' corresponds to $K(1)$ by class field theory and so $\mathrm{Gal}(L/K(1)) \cong J'' \cong U'/(U' \cap H)$. The same proof as for Lemma 2.6 shows that $U' \cap H = \overline{\psi(\mathcal{O}_K^\times)}$ as desired. □

3 Λ-modules

Let K be a finite extension of $\mathbb{Q}_p$, $\mathcal{O}$ its ring of integers and π a uniformiser generating the unique maximal ideal $\mathfrak{p}$ of $\mathcal{O}$.

Proposition 3.1 (Division Algorithm). *Let $f, g \in \mathcal{O}[[T]]$ with $f = \sum_{i=0}^{\infty} a_i T^i$. Suppose that $a_i \in \mathfrak{p}$ for $0 \leq i \leq n-1$ but $a_n \in \mathcal{O}^\times$. Then there exist unique $q \in \mathcal{O}[[T]]$ and $r \in \mathcal{O}[T]$ such that $g = qf + r$ and $\deg(r) \leq n-1$.*

Proof. We first prove uniqueness which amounts to showing that if $qf + r = 0$ then $q = r = 0$. Suppose that $q, r \neq 0$. Without loss of generality, we may assume that either $\pi \nmid r$ or $\pi \nmid q$. Reducing modulo π shows that, necessarily, $\pi | r$ so we have that $\pi \nmid q$ but $\pi \mid fq$. But $\pi \nmid f$ so we must have that $\pi \mid q$ which is a contradiction.

To prove the existence of q and r, define the $\mathcal{O}$-linear shift operator

$$\begin{aligned} \tau = \tau_n : \mathcal{O}[[T]] &\to \mathcal{O}[[T]] \\ \sum_{i=0}^{\infty} b_i T^i &\mapsto \sum_{i=n}^{\infty} b_i T^{i-n} \end{aligned}$$

which satisfies the following two properties

1. $\tau(T^n h(T)) = h(T)$ for all $h(T) \in \mathcal{O}[[T]]$
2. $\tau(h(T)) = 0 \iff h(T) \in \mathcal{O}[T]$ with $\deg(h(T)) \leq n-1$

We can always write

$$f(T) = \pi P(T) + T^n U(T)$$

where $P(T) \in \mathcal{O}[T]$ has $\deg(P) \leq n-1$ and $U(T) = \tau(f(T))$. Now, since $a_n \in \mathcal{O}^\times$, it follows that $U(T)$ is a unit in $\mathcal{O}[[T]]$. Define

$$q(T) = \frac{1}{U(T)} \sum_{j=0}^{\infty} (-1)^j \pi^j \left(\tau \circ \frac{P}{U}\right)^j \circ \tau(g)$$

We note that the π^j factor ensures that this is a well-defined power series over $\mathcal{O}$. Since

$$qf = \pi q P + T^n q U$$

it follows that

$$\tau(qf) = \pi\tau(qP) + \tau(T^n qU) = \pi\tau(qP) + qU$$

Now,

$$\begin{aligned} \pi\tau(qP) &= \pi \left(\tau \circ \frac{P}{U}\right) \circ \left(\sum_{j=0}^{\infty} (-1)^j \pi^j \left(\tau \circ \frac{P}{U}\right)^j \circ \tau(g)\right) \\ &= \tau(g) - qU \end{aligned}$$

so that

$$\tau(qf) = \tau(g)$$

By the second property of τ it then follows that $g = qf + r$ for some $r \in \mathcal{O}[T]$ such that $\deg(r) \leq n-1$. $\square$

Definition 3.2. Let $P(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0 \in \mathcal{O}[T]$. We say that $P(T)$ is **distinguished** if $a_i \in \mathfrak{p}$ for $0 \leq i \leq n-1$.

Theorem 3.3 (p-adic Weierstrass Preparation)**.** *Let $f(T) = \sum_{i=0}^{\infty} a_i T^i \in \mathcal{O}[[T]]$ and suppose that $a_i \in \mathfrak{p}$ for $0 \leq i \leq n-1$ but $a_n \notin \mathfrak{p}$ for some n. Then f can be written uniquely in the form $f(T) = p(T)U(T)$ where $U(T) \in \mathcal{O}[[T]]$ is a unit and $P(T)$ is a distinguished polynomial of degree n.*

Moreover, if $f(T) \in \mathcal{O}[[T]]$ is non-zero then we may uniquely write

$$f(T) = \pi^\mu P(T)U(T)$$

with P a distinguished polynomial of degree n, $U(T) \in \mathcal{O}[[T]]$ a unit and $\mu \geq 0$.

Proof. The second part follows immediately from the first part upon factoring out a large enough power of π from the coefficients of $f(T)$.

In order to prove the first statement, let $g(T) = T^n$. By the division algorithm, there exist unique $q \in \mathcal{O}[[T]]$ and $r \in \mathcal{O}[T]$ with $\deg(r) \leq n-1$ and

$$T^n = q(T)f(T) + r(T)$$

Since

$$q(T)f(T) \equiv q(T)(a_n T^n + o(T^{n+1})) \pmod{\pi}$$

whence $r(T) \equiv 0 \pmod{\pi}$. Hence $P(T) = T^n - r(T)$ is a distinguished polynomial of degree n. Denote by q_0 the constant term of $q(T)$. Comparing coefficients of T^n, we see that

$$q_0 a_n \equiv 1 \pmod{\pi}$$

and so $q_0 \in \mathcal{O}^\times$ whence $q(T)$ is a unit in $\mathcal{O}[[T]]$. Define $U(T) = 1/q(T)$. Then $f(T) = P(T)U(T)$ as desired.

To prove uniqueness, note that any distinguished polynomial of degree n can be written as $P(T) = T^n - r(T)$. Transforming the equation $f(T) = P(T)U(T)$ back to

$$T^n = U(T)^{-1}f(T) + r(T)$$

allows us to apply the uniqueness statement of the division algorithm to see that $U(T)$ and $r(T)$ are unique. □

Corollary 3.4. *Let $\mathbb{C}_p$ be the complex p-adics*[1] *and $f(T) \in \mathcal{O}[[T]]$ non-zero. Then there are only finitely many $x \in \mathbb{C}_p$ such that $|x|_p < 1$ and $f(x) = 0$.*

Proof. Fix $x \in \mathbb{C}_p$ such that $|x|_p < 1$ and $f(x) = 0$. By the p-adic Weierstrass Preparation Theorem we can write $f(T) = \pi^\mu P(T)U(T)$ for some $\mu \geq 0$, $P(T)$ distinguished and $U(T) \in \mathcal{O}[[T]]$. But $U(T)$ is a unit so $U(x) \neq 0$ and so, necessarily, $P(x) = 0$. Hence there can only be finitely many such x. □

Proposition 3.5. *Let $P(T) \in \mathcal{O}[T]$ be distinguished and $g(T) \in \mathcal{O}[T]$ arbitrary. If $g(T)/p(T) \in \mathcal{O}[[T]]$ then, in fact, $g(T)/P(T) \in \mathcal{O}[T]$.*

[1] Recall that the complex p-adics are the completion of the algebraic closure of $\mathbb{Q}_p$ which are themselves algebraically closed.

Proof. Write $g(T) = f(T)P(T)$ for some $f(T) \in \mathcal{O}[[T]]$. Let $x \in \mathbb{C}_p$ be a root of $P(T)$. Then

$$0 = P(x) = x^n + z(x)\pi$$

for some polynomial $z(x) \in \mathcal{O}[T]$. Hence $|x|_p < 1$ whence $f(x)$ converges so that $g(x) = 0$. Now, dividing by $T - x$ and expanding the ring as necessary we can continue this process to see that $P(T)$ divides $g(T)$ as polynomials and so $f(T) \in \mathcal{O}[T]$. □

From now on, let $\Lambda = \mathbb{Z}_p[[T]]$.

Proposition 3.6. *Λ is a unique factorisation domain and is Noetherian. It's irreducible elements are p and the irreducible distinguished polynomials. The units are precisely the power series whose constant term is 1.*

Proof. Everything follows immediately from the p-adic Weierstrass Theorem except the Noetherian statement which follows from the formal Hilbert Basis Theorem and the fact that $\mathbb{Z}_p$ is Noetherian (it's a PID). □

Lemma 3.7. *Let $f, g \in \Lambda$ be coprime. Then $(f, g)\Lambda$ is of finite index in Λ.*

Proof. Fix $h \in (f, g)$ of minimal degree. The necessarily $h = p^s H$ for some $s \geq 0$ and either $H = 1$ or H a distinguished polynomial. Suppose that $H \neq 1$. Since f and g are coprime, we may assume that H does not divide f. By the division algorithm we have

$$f = Hq + r$$

for some q and r with $\deg r < \deg H = \deg h$. Hence

$$p^s f = hq + p^s r$$

Then $p^s r \in (f, g)$ and $\deg(p^s r) < \deg(h)$ which contradicts the minimality of $\deg(h)$. Hence $H = 1$ and $h = p^s$. Without loss of generality, we may assume that f is coprime to p and is distinguished. Indeed, if this were not the case then we could just use g or divide by a unit. Since $h = p^s$ and f and g are coprime, it follows that $(p^s, f) \subseteq (f, g)$. By the division algorithm, any element of Λ is congruent modulo f to a polynomial of degree less than $\deg(f)$. There are only finitely many such polynomials modulo p^s whence (p^s, f) has finite index in Λ. Hence so does (f, g) as claimed. □

Lemma 3.8. *Let $f, g \in \Lambda$ be coprime. Then*

1. *The map*

$$\begin{aligned} \phi : \Lambda/(fg) &\to \Lambda/(f) \oplus \Lambda/(g) \\ [h]_{fg} &\mapsto ([h]_f, [h]_g) \end{aligned}$$

   is an injection with finite cokernel.

2. *There exists an injective map*

$$\psi : \Lambda/(f) \oplus \Lambda/(g) \to \Lambda/(fg)$$

   with finite cokernel.

Proof.

Part 1: Suppose that $\phi([h]_{fg}) = 0$. Then $h \equiv 0 \pmod{f}$ and $h \equiv 0 \pmod{g}$ so that $f \mid h$ and $g \mid h$. But f and g are coprime and Λ is a UFD and so $fg \mid h$ whence $[h] = 0$.

To see that this map has finite cokernel, we first observe that by Lemma 3.7 we can choose finitely many representatives $r_1, \ldots, r_n$ for $\Lambda/(f,g)$. We claim that

$$\{ ([0]_f, [r_i]_g) \mid 1 \leq i \leq n \}$$

is a set of coset representatives for $\operatorname{coker}\phi$. To this end, fix an equivalence class $\overline{m} \in \operatorname{coker}\phi$. Suppose that $m = ([a]_f, [b]_g) \in \Lambda/(f) \oplus \Lambda/(g)$. We need to show that there exists some $1 \leq i \leq n$ such that

$$([a]_f, [b]_g) \sim ([0]_f, [r_i]_g) \iff ([a]_f, [b - r_i]_g) \sim 0 \iff ([a]_f, [b - r_i]_g) \in \operatorname{im}\phi$$

Now, $a - b \equiv -r_k \pmod{(f,g)}$ for some $1 \leq k \leq n$. Hence $a - b + r_k \in (f,g)$ and so $a - b + r_k = Af + Bg$ for some $A, B \in \Lambda$. Define

$$c = a - Af = b - r_k + Bg$$

Then $\phi([c]) = ([a]_f, [b - r_k]_g)$ so taking $i = k$ works.

Part 2: Denote $Let M = \operatorname{im}\phi$ and $N = \Lambda/(f) \oplus \Lambda/(g)$. By Part 1, we have that $\Lambda/(fg) \cong M$ and $M \subseteq N$. Let $P \in \Lambda$ be a distinguished polynomial that is coprime to fg. Since M has finite index in N, the Pigeohole principle implies that

$$(P^i)(x,y) \equiv (P^j)(x,y) \pmod{M}$$

for some $i < j$. Observe that $1 - P^{j-i} \in \Lambda^\times$ so the above congruence then implies that $(P^i)(x,y) \in N$. Hence for large enough i, say k, we have that $P^k N \subseteq M$. We claim that $\psi = P^k$ is the desired injection with finite cokernel. Indeed, suppose that $\psi(x,y) = 0$. Then $f \mid P^k x$ and $g \mid P^k y$. But $\gcd(P^k, fg) = 1$ and so $f \mid x$ and $g \mid y$ whence $(x,y) = 0$. Hence ψ is injective. Now, (P^k, fg) has finite index in Λ and thus its image has finite index in $\Lambda/(fg)$. But $(P^k, fg) \subseteq \operatorname{im}\psi$ which implies that $\operatorname{coker}\psi$ is finite.

□

Proposition 3.9. *Let $\mathfrak{p}$ be a non-zero prime ideal of Λ. Then $\mathfrak{p}$ is one of (p), (p,T), or $(P(T))$ for any irreducible distinguished polymomial. Moreover, (p,T) is the unique maximal ideal of Λ and so Λ is a Noetherian local ring.*

Proof. Since Λ is a UFD with irreducibles $p, P(T)$ and T, it follows that the ideals that they are generate are prime ideals. Let $h \in \mathfrak{p}$ be of minimal degree. Then by the p-adic Weierstrass preparation theorem, $h = p^s H$ for some $s \geq 0$ and H either 1 or a distinguished polynomial. Since $\mathfrak{p}$ is prime, either $p \in \mathfrak{p}$ or $H \in \mathfrak{p}$. If $1 \neq H$ then H must be irreducible by minimality of its degree. Hence in either case, $(f) \subseteq \mathfrak{p}$ where f is either p or an irreducible distinguished polynomial. If $(f) = \mathfrak{p}$ then $\mathfrak{p}$ is one of the listed prime ideals and we are done.

Next, suppose that $\mathfrak{p} \neq (f)$. Then there exists $g \in \mathfrak{p}$ such that $f \nmid g$. Now, f is irreducible so, necessarily, f and g are coprime. Then (f,g) has finite index in Λ by Lemma 3.7. But $(f,g) \subseteq \mathfrak{p}$ so that $\mathfrak{p}$ has finite index in λ. Observe that $\Lambda/\mathfrak{p}$ is a finite $\mathbb{Z}_p$-module and so $p^N \in \mathfrak{p}$ for large enough N. Since $\mathfrak{p}$ is prime we then have that $p \in \mathfrak{p}$. Moreover, $T^i \equiv T^j \pmod{\mathfrak{p}}$ for some $i < j$. Since $1 - T^{j-i} \in \Lambda^\times$ it then follows that $T^i \in \mathfrak{p}$ whence $T \in \mathfrak{p}$. We thus see that $(p,T) \subseteq \mathfrak{p}$. But $\Lambda/(p,T) \equiv \mathbb{F}_p$ which is a field and so (p,T) is maximal and $(p,T) = \mathfrak{p}$. □

Lemma 3.10. *Let $f \in \Lambda$ such that $f \notin \Lambda^\times$. Then $\Lambda/(f)$ is infinite.*

Proof. If $f = 0$ then we are done so assume that $f \neq 0$. We may assume, without loss of generality, that $f = p$ or f is a distinguished polynomial. If $f = p$ then $\Lambda/(f) \cong \mathbb{F}_p[[T]]$ which is infinite.

If f is a distinguished polynomial, fix $g \in \Lambda$. By the division algorithm, we can find unique $q \in \mathbb{Z}_p[[T]]$ such that $g = fq + r$. Then $g \equiv r \pmod{(f)}$. Since r is unique and depends on g, we see that $\Lambda/(f)$ has the same cardinalty as Λ. In particular, it is an infinite subring of $\mathbb{Z}_p[T]$. □

Definition 3.11. Let M and M' be Λ-modules. We say that M and M' are **pseudo-isomorphic** and write $M \sim M'$ if there exists a homomorphism $M \to M'$ with finite kernel and cokernel.

Proposition 3.12. *Let $f, g \in \Lambda$ be coprime. Then*

$$\Lambda/(fg) \sim \Lambda/(f) \oplus \Lambda/(g), \qquad \Lambda/(f) \oplus \Lambda/(g) \sim \Lambda/(fg)$$

Proof. This is a restatement of Lemma . □

We aim to prove the following Theorem:

Theorem 3.13. *Let M be a finitely generated Λ-module. Then*

$$M \sim \Lambda^r \oplus \left(\bigoplus_{i=1}^{s} \Lambda/(p^{n_i}) \right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda/(f_j(T)^{m_j}) \right)$$

for some $r, s, t, n_i, m_j \in \mathbb{Z}$ and f_j irreducible distinguished polynomials.

Suppose M is a finitely generated Λ-module so that we have an exact sequence

$$\Lambda^n \xrightarrow{\ \phi\ } M \longrightarrow 0$$

for some $n \geq 1$. Then the images of the generators of Λ^n under ϕ are generators for M, label them $u_1, \ldots, u_n$. Let $R = \ker \phi$. Note that the elements of R correspond to relations

$$\lambda_1 u_1 + \cdots + \lambda_n u_n = 0$$

with $\lambda_i \in \Lambda$. Since Λ is Noetherian, R is finitely generated and so M is a finitely presented Λ-module. That is to say, we have an exact sequence

$$\Lambda^m \xrightarrow{\ R\ } \Lambda^n \xrightarrow{\ \phi\ } M \longrightarrow 0$$

where R is now the so-called presentation matrix of M. We have the following standard row and column operations which correspond to changing the generators of R and M:

Operation A. *We may permute the rows or columns of R.*

Operation B. *We may add a multiple of a row (respectively column) to another row (respectively column). A special case of this operation is the following. If $\lambda' = q\lambda + r$ then we can perform the operation*

$$\begin{pmatrix} \vdots & & \vdots & \\ \lambda & \cdots & \lambda' & \cdots \\ \vdots & & \vdots & \end{pmatrix} \to \begin{pmatrix} \vdots & & \vdots & \\ \lambda & \cdots & r & \cdots \\ \vdots & & \vdots & \end{pmatrix}$$

Operation C. *We may multiply any row or column by an element of* $\Lambda^\times$*.*

Since we are working up to pseudo-isomorphism, we also have the following operations for which we provide a proof that they change the generators of R:

Operation 1. *If R contains a row $(\lambda_1, p\lambda_2, \dots, p\lambda_n)$ with $p \nmid \lambda_1$. Then we may change R to the matrix R' whose first row is $(\lambda_1, \lambda_2, \dots, \lambda_n)$ and the remaining rows are the rows of R with the first element multiplied by p:*

$$\begin{pmatrix} \lambda_1 & p\lambda_2 & \cdots \\ \alpha_1 & \alpha_2 & \cdots \\ \beta_1 & \beta_2 & \cdots \end{pmatrix} \to \begin{pmatrix} \lambda_1 & \lambda_2 & \cdots \\ p\alpha_1 & \alpha_2 & \cdots \\ p\beta_1 & \beta_2 & \cdots \end{pmatrix}$$

As a special case, if $\lambda_2 = \cdots = \lambda_n = 0$ then we may multiply $\alpha_1, \beta_1, \cdots$ by an arbitrary power of p.

Proof. In R we have the relation

$$\lambda_1 u_1 + p(\lambda_2 u_n + \cdots + \lambda_n u_n) = 0$$

Define M' to be the Λ-module $M \oplus v\Lambda$ where $v \in M$ is a new generator modulo the relations

$$(-u_1, pv) = 0, \quad (\lambda_2 u_2 + \cdots + \lambda_n u_n, \lambda_1 v) = 0$$

Let $\phi : M \to M'$ be the natural map. We claim that ϕ is a pseudo-isomorphism. Suppose that $\phi(m) = 0$. Then $(m, 0)$ lies in the module of relations of M' and so

$$(m, 0) = a(-u_1, pv) + b(\lambda_2 u_2 + \cdots + \lambda_n u_n, \lambda_1 v)$$

for some $a, b \in \Lambda$. Hence $ap = -b\lambda_1$. Since $p \nmid \lambda_1$, it follows that $p \mid b$. Similarly, $\lambda_1 \mid a$. Then in the M-component we have

$$\begin{aligned} m &= -\frac{a}{\lambda_1}(\lambda_1 u_1) - \frac{a}{\lambda_1} p(\lambda_2 u_2 + \cdots + \lambda_n u_n) \\ &= -\frac{a}{\lambda_1}(0) = 0 \end{aligned}$$

so ϕ is injective. Now consider the elements pv and $\lambda_1 v$ in M'. It is clear that these elements lie in the image of M under ϕ. Then the ideal (p, λ_1) annihilates $M'/\phi(M)$. $M'/\phi(M)$ therefore has the natural structure of a finitely-generated $\Lambda/(p, \lambda_1)$-module. Since $\gcd(p, \lambda_1) = 1$, the ideal (p, λ_1) has finite index in Λ. It then follows that $M'/\phi(M)$ is finite. Hence ϕ is a pseudo-isomorphism as claimed.

The module M' has generators $v, u_2, \dots, u_n$ and any relation $\alpha u_1 + \cdots + \alpha_n u_n = 0$ becomes $p\alpha_1 v + \alpha_2 u_2 + \cdots + \alpha_n u_n = 0$ so that the first column of the presentation matrix is multiplied by p. We furthermore have the relation $\lambda_1 v + \lambda_2 u_2 + \dots \lambda_n u_n = 0$ so the presentation matrix takes the claimed form. ☐

Operation 2. *If all the elements in the first column of R are divisible by p^k for some $k \geq 1$ and if there is a row $(p^k\lambda_1, \dots, p^k\lambda_n)$ such that $p \nmid \lambda_1$ then we may change to the matrix R' which is the same as R except that $(p^k\lambda_1, \dots, p^k\lambda_n)$ is replaced by $(\lambda_1, \dots, \lambda_n)$:*

$$\begin{pmatrix} p^k\lambda_1 & p^k\lambda_2 & \cdots \\ p^k\alpha_1 & \alpha_2 & \cdots \end{pmatrix} \to \begin{pmatrix} \lambda_1 & \lambda_2 & \cdots \\ p^k\alpha_1 & \alpha_2 & \cdots \end{pmatrix}$$

Proof. Define M' to be the Λ-module $M = v\Lambda$ where $v \in M$ is a new generator modulo the relations

$$(p^k u_1, -p^k v) = 0, \quad (\lambda_2 u_2 + \cdots + \lambda_n, \lambda_1 v) = 0$$

Let $\phi : M \to M'$ be the natural map. As before, the fact that $p \nmid \lambda_1$ implies that ϕ is injective. The fact that (p^k, λ_1) annihilates $M'/\phi(M)$ implies that ϕ has finite cokernel so that ϕ is a pseudo-isomorphism. Since we have the relation $p^k(u_1 - v) = 0$ in M' and the fact that p^k divides every element of the first column of R, it follows that

$$M' = M'' \oplus (u_1 - v)\Lambda$$

where M'' is the Λ-module generated by $v, u_2, \ldots, u_n$ and the relations $(\lambda_1, \ldots, \lambda_n)$ and R. Observe that, since $u_1 - v$ is killed by p^k, we have that $(u_1 - v)\Lambda = \Lambda/(p^k)$ which is in the form given in the Theorem. We are thus free to just work with M'' which clearly has R' as its presentation matrix. □

Operation 3. *If R contains a row $(p^k\lambda_1, \ldots, p^k\lambda_n)$ and for some λ with $p \nmid \lambda$ we have that $(\lambda\lambda_1, \ldots, \lambda\lambda_n)$ is also a relation then we may change R to R' where R' is the same as R except that $(p^k\lambda_1, \ldots, p^k\lambda_n)$ is replaced by $(\lambda_1, \ldots, \lambda_n)$.*

Proof. Define the module $M' = M/(\lambda_1 u_1 + \cdots + \lambda_n u_n)\Lambda$ and let $\phi : M \to M'$ be the natural surjection. The kernel of ϕ is clearly annihilated by the ideal (p^k, λ) of Λ and so $\ker\phi$ has the natural structure of a $\Lambda/(p^k, \lambda)$-module. But $\Lambda/(p^k, \lambda)$ is finite and $\ker\phi$ is finitely generated since M is and so $\ker\phi$ is finite and M is pseudo-isomorphic to M'. □

Definition 3.14. Let M be a finitely generated Λ-module and R its relation matrix. We call the operations $A, B, C, 1, 2, 3$ on R **admissible**.

Given $0 \neq f \in \Lambda$, let $f(T) = p^\mu P(T)U(T)$ be its Weierstrasas factorisation for some $\mu \geq 0, P(T)$ distinguished and $U(T) \in \Lambda^\times$. We define the **Weierstrass degree** of f to be

$$\deg_w(f) = \begin{cases} \infty & \text{if } \mu > 0 \\ \deg P(T) & \text{if } \mu = 0 \end{cases}$$

We then define

$$\deg^{(k)}(R) = \min \deg_w(a'_{ij})$$

for $i, j \geq k$ where (a_{ij}) ranges over all relation matrices obtained from R via admissible operations which leave the first $(k-1)$ rows unchanged.

Finally, if R is in the form

$$\begin{pmatrix} \lambda_{11} & & 0 & 0 & \cdots & 0 \\ & \ddots & & & & \\ 0 & & \lambda_{r-1,r-1} & 0 & \cdots & 0 \\ * & \cdots & * & * & \cdots & * \\ * & \cdots & * & * & \cdots & * \end{pmatrix} = \begin{pmatrix} D_{r-1} & 0 \\ A & B \end{pmatrix}$$

with each λ_{kk} distinguished and

$$\deg \lambda_{kk} = \deg_w \lambda_{kk} = \deg^{(k)}(R)$$

for $1 \leq k \leq r-1$ then we say that R is in $(r-1)$-form.

Lemma 3.15. *Let M be a finitely generated Λ-module with presentation matrix R. Suppose that R is in $(r-1)$-form and $B \neq 0$. Then R may be transformed via admissible operations into R' which is in r-normal form and has the same first $(r-1)$ diagonal elements as R.*

Proof. By the special case of Operation 1, we can assume that for any N we have $p^N \mid \lambda_{i,j}$ for all $i \geq r$ and $j \leq r-1$ so that $p^N \mid A$. Choose an N large enough so that $p^N \nmid B$. By Operation 2, we may knock off enough powers of p from the matrix formed by A and B so that $p \nmid B$. Furthermore, we may assume that B contains an entry λ_{ij} such that

$$\deg_w \lambda_{ij} = \deg^{(r)}(R) < \infty$$

If $\lambda_{ij} = P(T)U(T)$ for some unit $U \in \Lambda^\times$, we may simply multiply the j^{th} column by λ_{ij} so we can ssume that λ_{ij} is distinguished. Indeed, the first $r-1$ rows have 0 in the j^{th} column so they do not change. Operation A allows us to assume that $\lambda_{ij} = \lambda_{rr}$. This is again because of the 0 entries.

By the division algorithm and the special case of B, we may assume that λ_{rj} is a polynomial satisfying

$$\deg \lambda_{rj} < \deg \lambda_{rr}$$

when $j \neq r$ and

$$\deg \lambda_{rj} < \deg \lambda_{jj}$$

for $j < r$. But λ_{rr} has minimal Weierstrass degree in B so we must have that $p \mid \lambda_{rj}$ for some $j > r$. By applying Operation 1, we can assume that $p^N \mid \lambda_{rj}$ for some $j < r$ and large N. Now suppose that $\lambda_{rj} \neq 0$ for some $j > r$. Operation 1 allows us to remove the power of p from λ_{rj}, leaving the 0s above it unchanged. Then

$$\deg_w \lambda_{rj} = \deg \lambda_{rj} < \deg \lambda_{rr} = \deg_w \lambda_r r$$

which is a contradiction. Hence $\lambda_{jr} = 0$ for all $j > r$.

Similarly, suppose that $\lambda_{rj} \neq 0$ for some $j < r$. Using Operation 1, we can assume that $p \nmid \lambda_{rj}$. But then

$$\deg_w \lambda_{rj} \leq \deg \lambda_{rj} < \deg \lambda_{jj} = \deg_w \lambda_{jj}$$

Since $\deg_w \lambda_{jj} = \deg^{(j)}(R)$, this contradicts the minimality of $\deg_w \lambda_{jj}$ so we must have that $\lambda_{rj} = 0$ for all $j < r$. This proves the claim. ☐

Theorem 3.16. *Let M be a finitely generated Λ-module. Then*

$$M \sim \Lambda^r \oplus \left(\bigoplus_{i=1}^{s} \Lambda/(p^{n_i}) \right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda/(f_j(T)^{m_j}) \right)$$

for some $r, s, t, n_i, m_j \in \mathbb{Z}$ and f_j irreducible distinguished polynomials.

Proof. Let R be the presentation matrix of M. Then, in the notation of Lemma 3.15, we have that $r = 1$. We can repeatedly apply Lemma 3.15 to bring R into the form

$$\begin{pmatrix} \lambda_{11} & & 0 \\ & \ddots & \\ & & \lambda_{rr} \\ A & & 0 \end{pmatrix}$$

where each λjj is distinguished and $\deg \lambda_{jj} = \deg^{(j)}(R)$ for $j \leq r$. Applying the division algorithm, we may assume that λ_{ij} are polynomial and

$$\deg \lambda_{ij} < \deg \lambda_{jj}$$

for $i \neq j$. Now suppose that $\lambda_{ij} \neq 0$ for $i \neq j$. Since $\deg_w \lambda_{jj}$ is minimal, we must have that $p \mid \lambda_{ij}$. We thus have a non-zero relation $(\lambda_{i1}, \ldots, \lambda_{ir}, 0, \ldots, 0)$ divisible by p. Let $\lambda = \lambda_{11} \ldots \lambda_{rr}$. Then $p \nmid \lambda$ since the λ_{ii} are distinguished and

$$\left(\lambda \frac{1}{p} \lambda_{i1}, \ldots, \lambda \frac{1}{p} \lambda_{ir}, 0, \ldots, 0\right)$$

is also a relation since $\lambda_{jj} u_j = 0$. Operation 3 allows us to assume that there exists some j for which $p \nmid \lambda_{ij}$. Hence

$$\deg_w \lambda_{ij} \leq \deg \lambda_{ij} < \deg \lambda_{jj} = \deg^{(j)}(R)$$

which is a contradiction. Hence $\lambda_{ij} = 0$ for all i, j with $i \neq j$ and so $A = 0$. Hence in terms of Λ-modules we have

$$\Lambda/(\lambda_{11}) \oplus \cdots \oplus \Lambda/(\lambda_{rr}) \oplus \Lambda^{n-r}$$

Adding in the factors $\Lambda/(p^k)$ from Operation 2 yields the form desired except that the λ_{ii} are not necessarily irreducible. But applying Lemma 3 yields the desired result. $\square$

4 Iwasawa's Class Number Formula

Definition 4.1. Let G be a topological group. We say that an element $\gamma \in G$ is a **topological generator** of G if the subgroup generated by γ is dense in G.

Example 4.2. Consider the additive group of $\mathbb{Z}_p$. Then $1 \in \mathbb{Z}_p$ is a topological generator of $\mathbb{Z}_p$. Indeed, the subgroup generated by 1 which is dense in $\mathbb{Z}$ with respect to the p-adic topology of $\mathbb{Z}_p$

Definition 4.3. Let Γ be a profinite group isomorphic to $\mathbb{Z}_p$ and γ a topological generator of Γ. Let $\Gamma^{p^n} = \overline{\langle \gamma^{p^n} \rangle}$ be the unique closed subgroup of index p^n in Γ. then $\Gamma_n = \Gamma / \Gamma^{p^n}$ is a cyclic group of order p^n with generator $\gamma + \Gamma^{p^n}$ and we have an isomorphism

$$\begin{aligned} \mathbb{Z}_p[\Gamma_n] &\to \mathbb{Z}_p[T]/((1+T)^{p^n} - 1) \\ [\gamma] &\mapsto [1+T] \end{aligned}$$

Moreover, for $0 \leq n \leq m$, the natural map $\Gamma_m \to \Gamma_n$ induces a natural map $\mathbb{Z}_p[\Gamma_m] \to \mathbb{Z}_p[\Gamma_n]$. We then define the **Iwasawa algebra** to be

$$\mathbb{Z}_p[[\Gamma]] = \varprojlim_n \mathbb{Z}_p[\Gamma_n] \cong \varprojlim \mathbb{Z}_p[T]/((1+T)^{p^n} - 1)$$

Theorem 4.4. *We have a topological isomorphism*

$$\begin{aligned} \Lambda &\to \mathbb{Z}_p[\Gamma] \\ T &\mapsto \gamma - 1 \end{aligned}$$

Proof. Write $\omega_n(T) = (1+T)^{p^n} - 1$. Then ω_n is distinguished and

$$\frac{\omega_{n+1}(T)}{\omega_n(T)} = (1+T)^{p^n(p-1)} + \cdots + (1+T)^{p^n} + 1 \in (p, T)$$

By induction on n, it then follows that $\omega_n(T) \in (p,T)^{n+1}$. Now, the division algorithm implies that we have a continuous surjection

$$\Lambda \to \Lambda/(\omega_n) \cong \mathbb{Z}_p[T]/(\omega_n) \cong \mathbb{Z}_p[\Gamma_n]$$

which is compatible with the transition maps $\mathbb{Z}_p[\Gamma_m] \to \mathbb{Z}_p[\Gamma_n]$. By the universal property of the inverse limit, this continuous map factors through the continuous map

$$\begin{aligned} \varepsilon : \Lambda &\to \mathbb{Z}_p[[\Gamma]] \\ T &\mapsto \gamma - 1 \end{aligned}$$

Observe that

$$\ker \varepsilon \subseteq \bigcap_n (\omega_n) \subseteq \bigcap_n (p,T)^{n+1} = 0$$

by Krull's intersection theorem. Hence ε is injective. Now, Λ and $\mathbb{Z}_p[[\Gamma]]$ are both profinite. In particular, Λ is compact and $\mathbb{Z}_p[[\Gamma]]$ is Hausdorff. Since ε is continuous, $\operatorname{im}\varepsilon$ is compact in $\mathbb{Z}_p[[\Gamma]]$ and is thus closed as a compact subspace of a Hausdorff space. On the other hand, $\operatorname{im}\varepsilon$ is dense in $\mathbb{Z}_p[[\Gamma]]$ since it is surjective on each finite level of the inverse system. It then follows that ε is surjective.

Thus far, we have shown that ε is an isomorphism of groups and is continuous. It remains to show that ε is a homeomorphism. But this immediate since it is a continuous bijection from a compact space to a Hausdorff space. □

We want to prove the following Theorem:

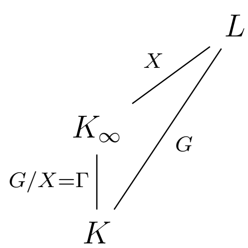
Theorem 4.5. *Let K_∞/K be a $\mathbb{Z}_p$-extension with intermediate fields K_n. Let p^{e_n} be the exact power of p dividing the class number of K_n. Then there are integers $\lambda \geq 0, \mu \geq 0$ called the* ***Iwasawa invariants*** *of K_∞/K and an integer v (all independently of n) and an integer n_0 such that*

$$e_n = \lambda n + \mu p^n + v$$

for all $n \geq n_0$.

Proof. Denote $\Gamma = \mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$ and fix a topological generator γ_0 of Γ. Denote by L_n the maximal unramified abelian p-extension of K_n. By class field theory, L_n is a subfield of the Hilbert class field of K_n whose Galois group over K_n is the ideal class group of K_n. Then $\mathrm{Gal}(L_n/K_n) \cong A_n$ where A_n is the p-Sylow subgroup of the ideal class group of K_n.

Define $L = \bigcup_{n\geq 1} L_n$ and $X = \mathrm{Gal}(L/K_\infty)$. Since each L_n is Galois over K_n and maximal, it follows that L is Galois over K. Denote $G = \mathrm{Gal}(L/K)$ so that we have the following diagram of Galois extensions:



□

The proof shall involve the following ideas. We shall give X the stucture of a Γ-module so that X is a Λ-module. We will then show that X is finitely generated as a Λ-module and has Λ-torsion. By the structure theorem, X will thus be pseudo-isomorphic to a direct sum of modules of the form $\Lambda/(p^k)$ and $\Lambda/(P(T)^k)$. These modules are easy to work with at the n^{th} level. We can then transfer the result back to X across the pseudo-isomorphism.

We first assume that all primes in K_∞/K which ramify in fact ramify totally. This can be achieved by applying Lemma 1.4 to K to obtain an intermediate extension K_m/K of K_∞/K satisfying the desired properties so we may replace K by K_m.

Under this assumption, it follows that $K_{n+1} \cap L_n = K_n$ for all n. Hence

$$\mathrm{Gal}(L_nK_{n+1}/K_n) \cong \mathrm{Gal}(L_n/K_n) \times \mathrm{Gal}(K_{n+1}/K_n)$$

Quotienting both sides by $\mathrm{Gal}(L_n/K_n)$ we get that

$$\mathrm{Gal}(L_nK_{n+1}/K_{n+1}) \cong \mathrm{Gal}(L_n/K_n)$$

This is a quotient of $X_{n+1} = \mathrm{Gal}(L_{n+1}/K_{n+1})$ since $L_nK_{n+1} \subseteq L_{n+1}$. We thus have a natural surjective map $X_{n+1} \to X_n$ which corresponds to the norm map on ideal class groups $A_{n+1} \to A_n$. Observe that $X_n \cong \mathrm{Gal}(L_nK_\infty/K_\infty)$ so that

$$\varprojlim_n X_n \cong \mathrm{Gal}\left(\left(\bigcup_{n\geq 1} L_nK_\infty\right)/K_\infty\right) = \mathrm{Gal}(L/K_\infty) = X$$

Now since X_n is an abelian p-group, it has the natural structure of a $\mathbb{Z}_p$-module. Let $\Gamma_n = \Gamma/\Gamma^{p^n} \cong \mathrm{Gal}(K_n/K)$. Given $\gamma \in \Gamma_n$, let $\widetilde{\gamma} \in \mathrm{Gal}(L_n/K)$ be an extension of γ to L_n. Define a Γ_n-action on X_n by setting

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

This action is well-defined since any other extension of γ to L_n differs from $\widetilde{\gamma}$ by an element of $X_n = \mathrm{Gal}(L_n/K_n)$. Hence X_n is a $\mathbb{Z}_p[\Gamma_n]$-module. Passing to the limit gives X the structure of a ($\mathbb{Z}_p[[\Gamma]] \cong \Lambda$)-module. Explicitly, the action of $\mathbb{Z}_p[[G]]$ on X is

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

where $\widetilde{\gamma}$ is an extension of $\gamma \in \Gamma$ to G.

Now denote the primes that ramify in K_∞/K as $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$. For each i, let $\mathfrak{P}_i$ be a prime of L lying over $\mathfrak{p}_i$ and I_i the inertia subgroup of G relative to $\mathfrak{P}_i$. Since L/K_∞ is unramified, it follows that $I_i \cap X = 1$ for all i. Hence the inclusion $I_i \to G$ induces an injective homomorphism $I_i \to G/X = \Gamma$ for all i. But K_∞/K is totally ramified at $\mathfrak{p}_i$ so, in fact, this homomorphism is surjective and we thus have isomorphisms $\Gamma \cong I_i$ for each i. In other words, $G = I_iX = XI_i$ for all i.

Now let $\sigma_i \in I_i$ map to $\gamma_0 \in \Gamma$. Then σ_i is a topological generator of I_i. Moreover since $I_i \subseteq XI_1$, there exists $a_i \in X$ such that $\sigma_i = a_i\sigma_1$.

Lemma 4.6. *Let G' be the closure of the commutator subgroup of G. Then*

$$G' = X^{\gamma_0 - 1} = TX$$

Proof. Since we have an isomorpism $\Gamma \cong I_1$ and also an inclusion $I_1 \subseteq G$, we can lift $\gamma \in \Gamma$ to the corresponding element of I_1 in order to define the action of Γ on X. To ease notation, we identify Γ with I_1 and write the action as

$$x^\gamma = \gamma x \gamma^{-1}$$

for $x \in X$ and $\gamma \in \Gamma$. Now fix $a, b \in G$ and write $a = \alpha x$, $b = \beta y$ for some $\alpha, \beta \in \Gamma$ and $x, y \in X$. Then

$$\begin{aligned}
aba^{-1}b^{-1} &= \alpha x \beta y x^{-1} \alpha^{-1} y^{-1} \beta^{-1} \\
&= x^\alpha \alpha \beta y x^{-1} \alpha^{-1} y^{-1} \beta^{-1} \\
&= x^\alpha (y x^{-1})^{\alpha\beta} (\alpha\beta) \alpha^{-1} y^{-1} \beta^{-1} \\
&= x^\alpha (y x^{-1})^{\alpha\beta} (y^{-1})^\beta && (\Gamma \text{ is abelian}) \\
&= x^\alpha x^{-\alpha\beta} y^{\alpha\beta} y^{-\beta} \\
&= x^{\alpha(1-\beta)} y^{(\alpha-1)\beta}
\end{aligned}$$

Now set $\beta = 1$ and $\alpha = \gamma_0$. Then $y^{\gamma_0 - 1} \in G'$ and so $X^{\gamma_0 - 1} \subseteq G'$. Now suppose that β is arbitrary. Then there exists $c \in \mathbb{Z}_p$ such that $\beta = \gamma_0^c$. Then

$$1 - \beta = 1 - \gamma_0^c = 1 - (1+T)^c = 1 - \sum_{n=0}^{\infty} \binom{c}{n} T^n \in T\Lambda$$

Now since $\gamma_0 - 1 = T$, it follows that $(x^\alpha)^{1-\beta} \in X^{\gamma_0 - 1}$. By a similar argument, $(y^\beta)^{1-\alpha} \in X^{\gamma_0 - 1}$. Now, X is compact Hausdorff and $X^{\gamma_0-1} = TX$ is the image of the compact space X under the continuous map $x \mapsto Tx$ and so $X^{\gamma_0 - 1}$ is closed in X. It then follows that $G' \subseteq X^{\gamma_0 - 1}$ □

Lemma 4.7. *Let Y_0 be the $\mathbb{Z}_p$-module of X generated by the set $\{ a_i \mid 2 \le i \le s \}$ and by $X^{\gamma_0 - 1} = TX$. Set $Y_n = v_n Y_0$ where*

$$v_n = 1 + \gamma_0 + \gamma_0^2 + \cdots + \gamma_0^{p^n - 1} = \frac{(1-T)^{p^n} - 1}{T}$$

Then $X_n \cong X/Y_n$ for all $n \in \mathbb{N}$.

Proof. First suppose that $n = 0$. We have that $K \subseteq L_0 \subseteq L$. Recall that L_0 is the maximal unramified p-extension of K. Since L/K is a p-extension, L_0/K is the maximal unramified abelian subextension of L/K. Hence $\mathrm{Gal}(L/L_0)$ is the closed subgroup of G generated by G' and all the inertia groups I_i. In other words, $\mathrm{Gal}(L/L_0)$ is the closure of the group generated by X^{γ_0-1}, I_1 and $\{ a_i \mid 2 \le i \le s \}$. Then

$$\begin{aligned}
X_0 = \mathrm{Gal}(L_0/K) = G/\mathrm{Gal}(L/L_0) &= XI_1/\mathrm{Gal}(L/L_0) \\
&= X/\overline{\langle X^{\gamma_0 - 1}, a_2, \ldots, a_s \rangle} \\
&= X/Y_0
\end{aligned}$$

Now, for the general case, replace K with K_n and γ_0 with $\gamma_0^{p^n}$. Then we may replace σ_i with $\sigma_i^{p^n}$. Now,

$$\begin{aligned}
\sigma_i^{k+1} = (a_i \sigma_1)^{k+1} &= a_1 \sigma_1 a_i \sigma_1^{-1} \sigma_1^2 a_i \sigma_1^{-2} \cdots \sigma_1^k a_i \sigma^{-k} \sigma_1^{k+1} \\
&= a_1^{1 + \sigma_1 + \sigma_1^2 + \cdots + \sigma_1^k} \sigma_1^{k+1}
\end{aligned}$$

Hence $\sigma_i^{p^n} = (v_n a_i) \sigma_i^{p^n}$ so a_i is replaced by $v_n a_i$. Furthermore, $X^{\gamma_0 - 1}$ is replaced by $(\gamma_0^{p^n} - 1)X = v_n X^{\gamma_0 - 1}$. Hence Y_0 becomes $v_n Y_n$ as desired. □

Lemma 4.8 (Nakayama)**.** *Let X be a compact Hasudorff Λ-module. Then*

1. *If $(p,T)X = X$ then $X = 0$*
2. *If $X/(p,T)X$ is finite then X is finitely generated by a set of representatives of $X/(p,T)X$ and has Λ-torsion.*

Proof. We first claim that

$$\bigcap_{n\geq 1}(p,T)^n X = 0$$

To this end, fix an open neighbourhood U of 0 in X. Since the action of Λ on X is continuous and $(p,T)^n \to 0$, it follows that for each $x \in X$, there exists an open neighbourhood U_x of x and an integer $n(x)$ such that

$$(p,T)^{n(x)}U_x \subseteq U$$

Now, X is compact so the open cover $\{\, U_x \,\}_{x\in X}$ of X admits a finite subcover. It then follows that there must exist some integer n and an open neighbourhood U_x of x such that $(p,T)^n U_x \subseteq U$. Now, $(p,T)X = X$ implies that $(p,T)^n X = X$ and so $X \subseteq U$ for all U. But X is Hausdorff so $X = 0$.

Now assume that $x_1, \dots, x_n$ are representatives of $X/(p,T)X$. Let $Y = \Lambda x_1 + \dots \Lambda x_n \subseteq X$. Then Y is compact since it is the image of Λ^n under the natural map. Since X is Hausdorff, Y is thus closed. It then follows that X/Y is compact Hausdorff. By Part 1, we then see that $X/Y = 0$ whence $X = Y$.

To see that X is torsion, let p^k be the exponent of $X/(p,T)X$ so that $p^k x_i \in TX$ for all $1 \leq i \leq n$. Write

$$p^k x_i = \sum_{j=1}^{m} T a_{ij}(T) x_j$$

Let $A = (p^k \delta_{ij} - T a_{ij}(T))_{i,j}$ and denote $g(A) = \det A \in \Lambda$. Then, clearly, $g(A)x_i = 0$ for all $1 \leq i \leq n$ but $g(0) = p^{kn} \neq 0$. □

Lemma 4.9. *$X = \mathrm{Gal}(L/K_\infty)$ is a finitely generated torsion Λ-module.*

Proof. Observe that $v_1 \in (p,T)$ and so $Y_0/(p,T)Y_0$ is a quotient of $Y_0/v_1Y_0 = Y_0/Y_1 \subseteq X/Y_1 = X_1$ which is finite. Hence $Y_0/(p,T)Y_0$ is finite and is thus a finitely generated torsion Λ-module by Nakayama's Lemma. But $X/Y_0 = X_0$ which is finite so X must be finitely generated and torsion too. □

We may now remove the assumption given above:

Proposition 4.10. *Let K_∞/K be a $\mathbb{Z}_p$-extension. Then X is a finitely generated Λ-module and there exists $e \geq 0$ such that*

$$X_n \cong X/v_{n,e}Y_e$$

for all $n \geq e$ where $v_{n,e} = v_n/v_e$.

Proof. By Proposition 1.4, there exists $e \geq 0$ such that every prime of K_∞/K_e that ramifies in fact ramifies totally. Then X is a finitely generated $\mathbb{Z}_p$-module by the previous Lemmata. Now if $n \geq e$ we have

$$v_{n,e} = \frac{v_n}{v_e} = 1 + \gamma_0^{p^e} + \gamma_0^{2p^e} + \cdots + \gamma_0^{p^n - p^e}$$

This replaces v_n for K_e since $\gamma_0^{p^e}$ generates $\mathrm{Gal}(K_\infty/K_e)$. Now let Y_e be the Y_0 provided by Lemma 4.7. Then $Y_n = v_{n,e}Y_e$ and $X_n \cong X/Y_n$ for all $n \geq e$ as claimed. □

Proposition 4.11. *Consider the finitely generated* Λ*-module*

$$E = \Lambda^r \oplus \left(\bigoplus_{i=1}^{s} \Lambda/(p^{k_i}) \right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda/(g_j(T)) \right)$$

where each $g_j(T)$ *is distinguished. Let* $m = \sum_i k_i$ *and* $l = \sum_j \deg g_j$*. If* $E/v_{n,e}E$ *is finite for all* n *then* $r = 0$ *and there exists* n_0 *and* c *such that*

$$|E/v_{n,e}E| = p^{mp^n + ln + c}$$

for all $n > n_0$*.*

Proof. Let V be a summand of E. We shall calculate $V/v_{n,e}V$ for each possible value of E. First suppose that $V = \Lambda$. Since $v_{n,e} \notin \Lambda^\times$, it follows that $\Lambda/(v_{n,e})$ is infinite by Lemma 3.10. But this contradicts the hypothesis that $E/v_{n,e}E$ is finite for all n. Hence $V = \Lambda$ does not occur as a summand.

Now suppose that $V = \Lambda/(p^k)$ for some k. Then

$$V/v_{n,e}V \cong \Lambda/(p^k, v_{n,e})$$

Observe that if the quotient of two distinguished polynomials is again a polynomial then the quotient is itself distinguished (or constant). Thus $v_{n,e}$ is distinguished. The division algorithm then implies that every element of $\Lambda/(p^k, v_{n,e})$ is uniquely represented by a polynomial modulo p^k of degree less than $\deg v_{n,e} = p^n - p^e$. Hence

$$|V/v_{n,e}V| = p^{k(p^n - p^e)} = p^{kp^n + c}$$

for some constant c.

Now assume that $V = \Lambda/(g(T))$ for some distinguished $g(T)$. Let $d = \deg g$. Then

$$T^d \equiv pQ(T) \pmod{g}$$

From now on, let $Q(T)$ be a placeholder for a polynomial whose exact form isn't important. If $k \geq d$ then

$$T^k \equiv pQ(T) \pmod{g}$$

So if $p^n \geq d$ we have

$$\begin{aligned}(1+T)^{p^n} &= 1 + pQ(T) + T^{p^n} \\ &\equiv 1 + pQ(T) \pmod{g}\end{aligned}$$

and thus

$$(1+T)^{p^{n+1}} \equiv 1 + p^2 Q(T) \pmod{g}$$

If we denote $P_n(T) = (1+T)^{p^n} - 1$ then we have

$$\begin{aligned} P_{n+2}(T) = (1+T)^{p^{n+2}} - 1 &= ((1+T)^{(p-1)p^{n+1}} + \cdots + (1+T)^{p^{n+1}} + 1)((1+T)^{p^{n+1}} - 1) \\ &= (1 + \cdots + 1 + p^2 Q(T))P_{n+1}(T) \\ &\equiv p(1 + pQ(T))P_{n+1}(T) \pmod{g} \end{aligned}$$

Now let ε be a placeholder for an element of $\Lambda^\times$. Then we see that P_{n+2}/P_{n+1} acts as $p\varepsilon$ on $\Lambda/(g)$ for $p^n \geq d$. Now assume that $n_0 > e$ such that $p^{n_0} > d$. Then for all $n \geq n_0$ we have

$$\frac{v_{n+2,e}}{v_{n+1,e}} = \frac{v_{n+2}}{v_{n+1}} = \frac{P_{n+2}}{P_{n+1}}$$

whence

$$v_{n+2,e}V = \frac{P_{n+2}}{P_{n+1}}(v_{n+1,e}V) = pv_{n+1,e}V$$

and so

$$|V/v_{n+2,e}V| = |V/pV| \cdot |pV/pv_{n+1,e}V|$$

Since g is coprime to p, multiplication by p is an injective endomorphism of V and so

$$|pV/pv_{n+1,e}V| = |V/v_{n+1,e}V|$$

On the other hand,

$$V/pV \cong \Lambda/(p,g) = \Lambda/(p,T^d)$$

so that $|V/pV| = p^d$. By induction on n it then follows that

$$|V/v_{n,e}V| = p^{d(n-n_0-1)}|V/v_{n_0+1,e}V|$$

for $n \geq n_0 + 1$. Hence

$$|V/v_{n,e}V| = p^{dn+c}$$

for all $n \geq n_0 + 1$ and some constant c.

The Proposition then follows upon putting together each summand. □

Corollary 4.12. *Let K_∞/K be a $\mathbb{Z}_p$-module so that X is a finitely generated Λ-module and $X_n \cong X/v_{n,e}Y_e$ for some $e \geq 0$. Then*

$$Y_e \sim X \sim \bigoplus_{i=1}^{s} \Lambda/(p^{k_i}) \oplus \bigoplus_{j=1}^{t} \Lambda/(g_j(T)) = E$$

for some distinguished irreducible polynomials g_j. Moreover, $|E/v_{n,e}E|$ is finite for all n and there exist constants n_0 and c such that for all $n \geq n_0 + 1$ we have

$$|E/v_{n,e}E| = p^{mp^n + ln + c}$$

where $m = \sum_i k_i$ and $l = \sum_j \deg g_j$.

Proof. We first observe that, since $X_e = X/Y_e$ is finite, and $Y_e \subseteq X$, we have a pseudo-isomorphism $Y_e \sim X$. Moreover, X is pseudo-isomorphic to a Λ-module of the form

$$\Lambda^r \oplus \bigoplus_{i=1}^{s} \Lambda/(p^{k_i}) \oplus \bigoplus_{j=1}^{t} \Lambda/(g_j(T))$$

by the Structure Theorem for Finitely Generated Λ-modules. Now, Lemma 3.10 implies that $\Lambda/(v_{n,e})$ is infinite. Since $Y_e/v_{n,e}Y_e$ this is not possible. Hence Λ cannot occur in the direct summand decomposition above. It remains to show that each $|E/v_{n,e}E|$ is finite. The summands of the form $\Lambda/(p^{k_i})$ were shown to always be finite in the previous proof. The only case we need to worry about is whether or not $\Lambda/(g_j, v_{n,e})$ is finite. By Lemma 3.7, this is certainly finite since g_j and $v_{n,e}$ are coprime. The rest of the Corollary then follows immediately from the Proposition. □

Corollary 4.13. *Let E be a finitely generated Λ-module of the form*

$$E = \Lambda^r \oplus \left(\bigoplus_{i=1}^{s} \Lambda/(p^{k_i}) \right) \oplus \left(\bigoplus_{j=1}^{t} \Lambda/(g_j(T)) \right)$$

If $m = \sum_i k_i$ then $m = 0$ if and only if the p-rank of $E/v_{n,e}E$ is bounded as $n \to \infty$.

Proof. Recall that the p-rank of a finite abelian group A is the number of direct summands of p-power order of A. By tensoring with $\mathbb{Z}/p\mathbb{Z}$, the p-rank is equal to $\dim_{\mathbb{Z}/p\mathbb{Z}}(A/pA)$. With this in mind, we have

$$E/(p, v_{n,e})E = \bigoplus_{i=1}^{s} \Lambda/(p, v_{n,e}) \oplus \bigoplus_{j=1}^{t} \Lambda/(p, v_{n,e}, g_j)$$

Now, $v_{n,e}$ is a distinguished polynomial of degree $p^n - p^e$ so if $\deg v_{n,e} \geq \max \deg g_j$ then we have

$$\begin{aligned} E/(p, v_{n,e})E &= \bigoplus_{i=1}^{s} \Lambda/(p, T^{p^n - p^e}) \oplus \bigoplus_{j=1}^{t} \Lambda/(p, T^{\deg g_j}) \\ &\cong (\mathbb{Z}/p\mathbb{Z})^{s(p^n - p^e) + l} \end{aligned}$$

where $l = \sum_j \deg g_j$. This is bounded as $n \to \infty$ if and only if $s = 0$ if and only if $m = 0$. □

Lemma 4.14. *Let Y and E be Λ-modules such that $Y \sim E$ and $Y/v_{n,e}Y$ is finite for all $n \geq e$. Then there exist constants c and n_0 such that*

$$|Y/v_{n,e}Y| = p^c |E/v_{n,e}E|$$

for all $n \geq n_0$.

Proof. We have a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & v_{n,e}Y & \longrightarrow & Y & \longrightarrow & Y/v_{n,e}Y & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \phi'_n} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi''_n} & & \\ 0 & \longrightarrow & v_{n,e}E & \longrightarrow & E & \longrightarrow & E/v_{n,e}E & \longrightarrow & 0 \end{array}$$

We first claim that we have the following inequalities:

1. $|\ker \phi'_n| \leq |\ker \phi|$
2. $|\operatorname{coker} \phi'_n| < |\operatorname{coker} \phi|$
3. $|\operatorname{coker} \phi''_n| < |\operatorname{coker} \phi|$
4. $|\ker \phi''_n| < |\ker \phi| \cdot |\operatorname{coker} \phi|$

Inequality 1 is immediate. Inequality 2 follows upon multiplying the representatives of $\operatorname{coker} \phi$ by $v_{n,e}$. Inequality 3 follows from the fact that representatives of $\operatorname{coker} \phi$ give representatives of $\operatorname{coker} \phi''_n$. To prove inequality 4, first note that the Snake Lemma gives us an exact sequence

$$0 \longrightarrow \ker \phi'_n \longrightarrow \ker \phi \longrightarrow \ker \phi''_n \longrightarrow \operatorname{coker} \phi'_n \longrightarrow \operatorname{coker} \phi \longrightarrow \operatorname{coker} \phi''_n \longrightarrow 0$$

so that $|\ker \phi''_n| \leq |\ker \phi| \cdot |\operatorname{coker} \phi'_n| \leq |\ker \phi| \cdot |\operatorname{coker} \phi|$.

Now let $m \geq n \geq 0$. We claim that we have the following inequalities:

a. $|\ker \phi'_n| \geq |\ker \phi'_m|$

b. $|\operatorname{coker} \phi'_n| \geq |\operatorname{coker} \phi'_m|$

c. $|\operatorname{coker} \phi''_n| \leq |\operatorname{coker} \phi''_m|$

To prove a, first observe that $v_{m,e} = (v_{m,e}/v_{n,e})v_{n,e}$ and so $v_{m,e}Y \subseteq v_{n,e}Y$ whence $\ker \phi'_m \subseteq \ker \phi'_n$. To prove b, fix $v_{m,e}y \in v_{m,e}E$. Let $z \in v_{n,y}E$ be a representative of $[v_{n,e}y] \in \operatorname{coker} \phi'_n$. Then $v_{n,e}y - z = \phi(v_{n,e}x)$ for some $x \in Y$. Multiplying by $v_{m,e}/v_{n,e}$ we get

$$v_{m,e}y - \left(\frac{v_{m,e}}{v_{n,e}}\right) z = \phi(v_{m,e}x) = \phi'_m(v_{m,e}(x))$$

So $v_{m,e}/v_{n,e}$ times representatives of $\operatorname{coker} \phi'_n$ gives representatives of $\operatorname{coker} \phi'_m$ whence b. c is immediate from the fact that $v_{m,e}E \subseteq v_{n,e}E$.

Combining all these inequalities, we see that the orders of $\ker \phi'_n, \operatorname{coker} \phi'_n$ and $\operatorname{coker} \phi''_n$ are constant for all $n \geq n_0$ for some n_0. From the above exact sequence, we have

$$|\ker \phi'_n| \cdot |\ker \phi| \cdot |\ker \phi''_n| = |\operatorname{coker} \phi'_n| \cdot |\operatorname{coker} \phi| \cdot |\operatorname{coker} \phi''_n|$$

so that $|\ker \phi''_n|$ is also constant for all $n \geq n_0$. Now, the exact sequence

$$0 \longrightarrow \ker \phi''_n \longrightarrow Y/v_{n,e}Y \longrightarrow E/v_{n,e}E \longrightarrow \operatorname{coker} \phi''_n \longrightarrow 0$$

implies that $|Y/v_{n,e}Y| = |E/v_{n,e}E| \cdot |\ker \phi''_n| \cdot |\operatorname{coker} \phi''_n|^{-1} = p^c|E/v_{n,e}E|$ for some constant c and all $n \geq n_0$. □

We cam now finally prove the original Theorem:

Theorem 4.15. *Let K_∞/K be a $\mathbb{Z}_p$-extension with intermediate fields K_n. Let p^{e_n} be the exact power of p dividing the class number of K_n. Then there are integers $\lambda \geq 0, \mu \geq 0$ called the* ***Iwasawa invariants*** *of K_∞/K and v (independently of n) and an integer n_0 such that*

$$e_n = \lambda n + \mu p^n + v$$

for all $n \geq n_0$.

Proof. Let $e \geq 0$ be such that all primes that ramify in K_∞/K_e ramify totally. Then we have that X is a finitely generated Λ-module and $X_n \cong X/v_{n,e}Y_e$. Since $X_e = X/Y_e$ is finite (and a power of p), we have that

$$|X_n| = |X/Y_e| \cdot |Y/v_{n,e}Y| = |X/Y_e| \cdot p^c \cdot |E/v_{n,e}E| = p^{\lambda n + \mu p^n + v}$$

for all $n \geq n_0$ for some constants n_0, λ, μ and v. □

5 The 1-dimensional Main Conjectures

Definition 5.1. Let M be a finitely generated torsion Λ-module so that

$$M \sim \bigoplus_{i=1}^{s} \Lambda/(p^{k_i}) \oplus \bigoplus_{j=1}^{t} \Lambda/(f_j(T)^{g_j})$$

for some irreducible distinguished polynomials f_j. We define the **characteristic polynomial** of M to be

$$\mathrm{char}(M) = \prod_{i=1}^{s} p^{k_i} \times \prod_{j=1}^{t} f_j^{g_j}$$

Theorem 5.2 (Mazur-Wiles)**.** *Let $\mathbb{Q}_\infty$ be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. Let $F_\infty = \mathbb{Q}(\mu_{p^\infty})$ be the extension of $\mathbb{Q}$ generated by all p-power roots of unity, $\Delta = \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ and denote $\Gamma = \mathbb{Z}_p$. Recall that we have an isomorphism*

$$G = \mathrm{Gal}(F_\infty/\mathbb{Q}) \cong \Delta \times \mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) = \Delta \times \Gamma$$

Let $F_n = \mathbb{Q}(\mu_{p^n})$. Denote by E_n the group of global units of F_n and C_n the subgroup of E_n consisting of the cyclotomic units. These are both $\mathrm{Gal}(F_n/K)$-modules. We recall that the closure of E_n in $\prod_{\mathfrak{p}/p} U_{F_{n,\mathfrak{p}}}$ is a finitely generated $\mathbb{Z}_p$-module and thus so is the corresponding closure of C_n. Define

$$E_\infty = \varprojlim_{n\in\mathbb{N}} \overline{E_n}, \qquad C_\infty = \varprojlim_{n\in\mathbb{N}} \overline{C_n}$$

with respect to the norm maps. Then E_∞ and C_∞ are finitely generated $\mathbb{Z}_p[[\mathrm{Gal}(F_\infty/\mathbb{Q})]] = \Gamma[[\Delta]] = \Lambda[\Delta]$-modules.

Let A_n be the p-part of the ideal class group of F_n and denote $X_\infty = \varprojlim_{n\in\mathbb{N}} A_n$ with respect to the norm maps.

Now fix a character $\chi : \Delta \to \mathbb{Z}_p^\times$. Given a $\Lambda[\Delta]$-module M, let $M^\chi = e_\chi M$ be the χ-isotypical part of M.

From previous results, we know that X is a finitely generated torsion Λ-module whence so is X^χ. It can be shown that $(E_\infty/C_\infty)^\chi$ is also a finitely generated torsion Λ-module. Then

$$\mathrm{char}(X^\chi) = \mathrm{char}((E_\infty/C_\infty)^\chi)$$

Theorem 5.3 (Rubin)**.** *Let K be an imaginary quadratic fieled and p a rational prime that splits completely into distinct primes $\mathfrak{p}$ and $\mathfrak{p}^*$ in K. Let K_∞ be the unique $\mathbb{Z}_p$-extension of K which is ramified only at $\mathfrak{p}$. Let F_0 be an abelian extension of K such that $[F_0 : K]$ is* *prime to p and such that* F_0 *contains the Hilbert class field of* K*. Then* $\mathfrak{p}$ *is totally ramified in* K_∞/K *and* $K_\infty \cap F_0 = K$*. Let* $F_\infty = F_0 K_\infty$*. Denote*

$$\Delta = \mathrm{Gal}(F_\infty/K_\infty) = \mathrm{Gal}(F_0/K)$$
$$\Gamma = \mathrm{Gal}(K_\infty/K) = \mathrm{Gal}(F_\infty/F_0)$$

so that $\mathrm{Gal}(F_\infty/K) = \Delta \times \Gamma$*. Let* F_n *be the extension of* F_0 *of degree* p^n *in* F_∞*. If we replace* C_n *in the above Theorem with the subgroup of* E_n *consisting of the elliptic units then we again have finitely generated* Λ*-modules* $X_\infty, C_\infty, E_\infty$*.*

The images of a character $\chi : \Delta \to \overline{\mathbb{Q}_p^\times}$ *lie entirely in the ring of integers of an* n*-dimensional extension of* $\mathbb{Q}_p$ *in which case we say that* $\dim \chi = n$*. For simplicity, we assume that* $\dim \chi = 1$ *but the main conjecture in this case can be formulated perfectly analogously for arbitary dimensions.*

The rest of the statements of the previous Theorem then follow through immediately and we get

$$\mathrm{char}(X_\infty^\chi) = \mathrm{char}((E_\infty/C_\infty)^\chi)$$