FORMALIZATION OF IWASAWA THEORY IN LEAN

JZ PAN

Contents

1. Introduction

1.1. **Iwasawa's theorem on growth of class groups.** The first goal of this project is formalize the proof of Iwasawa's theorem on growth of class groups in a $\mathbb{Z}_p$-extension tower in LEAN.

Definition 1.1. Let K be a field, p be a prime.

(i) An extension K_∞/K is called a $\mathbb{Z}_p$-extension, if it is Galois with $\Gamma = \mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$ as topological groups.

(ii) If K_∞/K is a $\mathbb{Z}_p$-extension, then for any $n \geq 0$, define $K_n := K_\infty^{\Gamma^{p^n}}$.

Theorem 1.2 (Iwasawa's theorem)**.** *Let K be a number field, p be a prime, K_∞/K be a $\mathbb{Z}_p$-extension. Then there exist integers λ, μ, ν such that for all sufficiently large n, $\mathrm{ord}_p(\#\mathrm{Cl}(K_n)) = \mu p^n + \lambda n + \nu$.*

Proof. This comes from Theorem 5.6, Proposition 4.16, and Proposition 5.7. □

2. Preliminaries in commutative algebra

2.1. **Random.**

Proposition 2.1. *Let A be a Noetherian ring and M be a finitely generated A-module. Then there exists a chain of submodules of M*

$$0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$$

such that for each $1 \le i \le n$, $M_i/M_{i-1} \cong A/\mathfrak{p}_i$ *for some prime ideal* $\mathfrak{p}_i \in \mathrm{Spec}(A)$.

Proof. When $M = 0$ we take $n = 0$ and there is nothing to prove. When $M \neq 0$ we have $\mathrm{Ass}(M) \neq \varnothing$ and we can take $\mathfrak{p}_1$ be any element in $\mathrm{Ass}(M)$ and we obtain $M_1 := A/\mathfrak{p}_1 \hookrightarrow M$. If $M_1 \neq M$, do the same for M/M_1 to get $M_2/M_1 \cong A/\mathfrak{p}_2 \hookrightarrow M/M_1$. Since M is a Noetherian A-module, the chain $M_1 \subset M_2 \subset \cdots$ must stop after a finite number of steps. □

Theorem 2.2 (Krull's Hauptidealsatz)**.** *Let* A *be a Noetherian ring. If* $\mathfrak{a} = (a_1, \cdots, a_n)$ *is an ideal of* A *generated by* n *elements, and* $\mathfrak{p}$ *is a minimal prime over-ideal of* $\mathfrak{a}$*, then* $\mathrm{ht}(\mathfrak{p}) \le n$.

Conversely, if $\mathfrak{p}$ *is a prime ideal of* A *of height* $\le n$*, then there exists an ideal* $\mathfrak{a}$ *of* A *generated by* n *elements, such that* $\overline{\mathfrak{p}}$ *is a minimal prime in* $A/\mathfrak{a}$.

(This is WIP in #23778.)

Proof. If $\mathfrak{p}$ is a minimal prime over-ideal of $\mathfrak{a}$, then $\mathfrak{a}A_\mathfrak{p} \subset \mathfrak{p}A_\mathfrak{p}$, and $\mathfrak{p}(A_\mathfrak{p}/\mathfrak{a}A_\mathfrak{p})$, which is the only maximal ideal of $A_\mathfrak{p}/\mathfrak{a}A_\mathfrak{p}$, is also a minimal prime ideal. Therefore $A_\mathfrak{p}/\mathfrak{a}A_\mathfrak{p}$ is Artinian, and so $\mathfrak{a}A_\mathfrak{p}$ is an open ideal. It follows that $\mathrm{ht}(\mathfrak{p}) = \dim(A_\mathfrak{p}) \le n$.

Conversely, if $\mathfrak{p}$ is a prime ideal of height $\le n$, then $\dim(A_\mathfrak{p}) \le n$, so there exists an *ideal of definition* $IA_\mathfrak{p}$ of $A_\mathfrak{p}$ (i.e. an open ideal with respect to $\mathfrak{p}A_\mathfrak{p}$-adic topology), generated by n elements. Clearing their denominators we may assume that the generators take the form $\frac{x_1}{s}, \cdots, \frac{x_n}{s}$ for some $x_1, \cdots, x_n \in I$ and $s \in A \setminus \mathfrak{p}$. Since $\mathfrak{p}^N A_\mathfrak{p} \subset IA_\mathfrak{p} \subset \mathfrak{p}A_\mathfrak{p}$ for some integer $N \ge 1$, we obtain $\mathfrak{p}^N \subset I \subset \mathfrak{p}$, and $IA_\mathfrak{p} = (x_1, \cdots, x_n)A_\mathfrak{p}$ (hence we may replace I by $(x_1, \cdots, x_n)$), and that $\mathfrak{p}$ is a minimal prime over-ideal of I (since if $I \subset \mathfrak{p}' \subset \mathfrak{p}$ for some prime ideal $\mathfrak{p}'$, then $\mathfrak{p}^N \subset \mathfrak{p}'$, hence $\mathfrak{p} \subset \mathfrak{p}'$, so $\mathfrak{p} = \mathfrak{p}'$). □

Theorem 2.3. *Let* A *be a Noetherian domain. Then* A *is a UFD if and only if every prime ideal of height* 1 *is principal (recall that a prime ideal* $\mathfrak{p}$ *is of height* 1 *if* $\mathfrak{p} \neq 0$ *and there is no prime ideal lies in between* 0 *and* $\mathfrak{p}$*).*

(We only need "⇒" in our project.)

Proof. "⇒": Let $\mathfrak{p}$ be a prime ideal of height 1, and let $a \in \mathfrak{p}$ be a non-zero element. Factor a into a product of irreducible elements (= prime elements) $a = p_1 \cdots p_r$. Then by $a \in \mathfrak{p}$ we obtain $p_i \in \mathfrak{p}$ for some i, since $(\mathfrak{p}_i) \neq 0$ is a prime ideal contained in $\mathfrak{p}$, we have $\mathfrak{p} = (p_i)$.

"⇐": It suffices to show that every irreducible element is prime. Let $p \in A$ be irreducible, and $\mathfrak{p}$ be a prime ideal of A minimal containing p. Then $\mathfrak{p}$ is of height 1 by Krull's Hauptidealsatz (Theorem 2.2), so $\mathfrak{p} = (\pi)$ is principal. Since $p \in \mathfrak{p} = (\pi)$, $\pi \mid p$, and since p is irreducible, $p = u\pi$ for some unit u, therefore p is prime (which generates $\mathfrak{p}$). □

Theorem 2.4. *A regular local ring is a UFD.*

Lemma 2.5 (Nakayama lemma, pro-p version)**.** *Suppose* $\Lambda \cong \mathbb{Z}_p[[T]]$*,* X *is a pro-*p Λ*-module,* $x_1, \cdots, x_t \in X$ *such that their images in* X/TX *generate* X/TX *as a* $\Lambda/(T)$*-module. Then* $x_1, \cdots, x_t$ *generate* X *as a* Λ*-module.*

Similar result holds when T is replaced by a topologically nilpotent element. Also for several variable formal power series.

Proof. Let $Y := \Lambda x_1 + \cdots + \Lambda x_t$ be the Λ-submodule of X generated by $x_1, \cdots, x_t$. Then by the image of Y in X/TX is X/TX, we know that $Y + TX = X$. Note that Y is compact, so it is closed in X, so $Z := X/Y$ is a pro-p abelian group, and the image of TX in Z is TZ. On the other hand, by $Y + TX = X$, the image of TX in Z is also Z, so $TZ = Z$. Since T is topologically nilpotent in Λ, for any open subgroup U of Z, there exists $N \ge 0$ such that for any $n \ge N$, $T^n Z \subset U$. But by $TZ = Z$ we know that $T^n Z = Z$ for any $n \ge 0$. Therefore Z must be zero. □

2.2. Noetherian integrally closed domain.

Proposition 2.6. *For a Noetherian local domain* A *of dimension one, the following are equivalent.*

- A *is integrally closed.*
- *The maximal ideal of* A *is principal.*
- A *is a discrete valuation ring.*
- A *is a regular local ring.*

(Mathlib: `IsDiscreteValuationRing.TFAE` *and* `tfae_of_isNoetherianRing_of_isLocalRing_of_isDomain`*.)*

Proof. Omitted. □

Definition 2.7. An integral domain A is called a *Krull domain* if it satisfies the following properties:

- $A_\mathfrak{p}$ is a discrete valuation ring for all height one primes $\mathfrak{p}$ of A,
- $A = \bigcap_{\mathfrak{p}\in \mathrm{Spec}(A), \mathrm{ht}(\mathfrak{p})=1} A_\mathfrak{p}$ inside $\mathrm{Frac}(A)$,
- any nonzero element of A is contained in only a finitely many height one primes of A.

Lemma 2.8. *Let A be a domain, S be a subset of $\mathrm{Spec}(A)$ such that $A_\mathfrak{p}$ is integrally closed for all $\mathfrak{p} \in S$ and $\bigcap_{\mathfrak{p}\in S} A_\mathfrak{p} = A$ inside $\mathrm{Frac}(A)$. Then A itself is integrally closed.*
(Generalization of `IsIntegrallyClosed.of_localization_maximal`. #24588)

```
#check isIntegrallyClosed_of_isLocalization
#check PrimeSpectrum.localization_comap_injective
#check PrimeSpectrum.localization_comap_range
```

Proof. Suppose $x \in \mathrm{Frac}(A)$ is integral over A. Then it's also integral over $A_\mathfrak{p}$ for all $\mathfrak{p} \in \mathrm{Spec}(A)$. Hence $x \in A_\mathfrak{p}$ for all $\mathfrak{p} \in S$. So $x \in \bigcap_{\mathfrak{p}\in S} A_\mathfrak{p} = A$. □

Proposition 2.9. *A Noetherian ring is a Krull domain if and only if it is an integrally closed domain.*

Proof. "⇒": Lemma 2.8.
"⇐": Let $\mathfrak{p}$ be a height one prime of A. Then $A_\mathfrak{p}$ is integrally closed (`isIntegrallyClosed_of_isLocalization`). We have $\mathrm{Spec}(A_\mathfrak{p}) = \{0, \mathfrak{p}A_\mathfrak{p}\}$ hence $A_\mathfrak{p}$ is also a Noetherian local domain of dimension one. Now by Proposition 2.6, $A_\mathfrak{p}$ is a DVR.
??? ???
□

2.3. **Semilocal PID.**

Lemma 2.10. *Let A be a semilocal ring, M be an A-module such that for any maximal ideal $\mathfrak{m}$ of A, $M_\mathfrak{m}$ is a finitely generated $A_\mathfrak{m}$-module. Then M is a finitely generated A-module.*

Proof. Suppose $M_{\mathfrak{m}_i}$ is generated by $\{x_{i,1}, \cdots, x_{i,n_i}\}$ for each maximal ideal $\mathfrak{m}_i$ of A. Let $y_{i,k}$ be a numerator of $x_{i,k}$, which is in A.
We prove that $\bigcup_i \{y_{i,1} \cdots, y_{i,n_i}\}$ is a finite set (Since A is semilocal) of generators of M. Let N be the A-submodule of M generated by $\bigcup_i \{y_{i,1} \cdots, y_{i,n_i}\}$.
By local property (`Submodule.eq_top_of_localization_maximal`), it suffices to show that $N_{\mathfrak{m}_i} = M_{\mathfrak{m}_i}$ for all maximal ideals $\mathfrak{m}_i$ of A. It's clear that $N_{\mathfrak{m}_i} \subseteq M_{\mathfrak{m}_i}$, so we only need to show that $M_{\mathfrak{m}_i} \subseteq N_{\mathfrak{m}_i}$.
In other words, need to prove that $M_{\mathfrak{m}_i} \subseteq \mathrm{span}_{A_{\mathfrak{m}_i}} f_i(\bigcup_i \{y_{i,1} \cdots, y_{i,n_i}\})$ where $f_i : M \to M_{\mathfrak{m}_i}$ is the localization map. It is enough to show the set of generators of $M_{\mathfrak{m}_i}$ is contained in right hand side.
Take any x in the set of generators of $M_{\mathfrak{m}_i}$. It remains to show that the image of a numerator of x under f_i is in the generators of right hand side by `Submodule.mem_of_numerator_image_mem` and `Submodule.mem_span`. i.e. $f_i(y) \in f_i(\bigcup_i \{y_{i,1} \cdots, y_{i,n_i}\})$ for some numerator y of x.
We take y as some $y_{i,k}$ as above. By definition of $y_{i,k}$, we have $f_i(y_{i,k})$ in right hand side. □

Lemma 2.11. *Let A be a semilocal (i.e. only finitely many maximal ideals) integral domain which is not a field, such that for every maximal ideal $\mathfrak{p}$ of A, $A_\mathfrak{p}$ is a PID. Then A itself is a PID.*

Proof. It's known that a semilocal Dedeking domain is a PID (`IsPrincipalIdealRing.of_finite_primes`). So we only need to show A is a Dedekind domain.
Let I be any ideal of A. Apply Lemma 2.10 to I we know that I is finitely generated. Hence A is a Noetherian ring.
Let $\mathfrak{p} \neq 0$ be a prime ideal of A. Choose a maximal ideal $\mathfrak{m}$ containing $\mathfrak{p}$. Then $0 \neq \mathfrak{p}A_\mathfrak{m} \subset \mathfrak{m}A_\mathfrak{m}$. Since $A_\mathfrak{m}$ is a PID (hence DVR), we have $\mathrm{Spec}(A_\mathfrak{m}) = \{0, \mathfrak{m}A_\mathfrak{m}\}$, so know that $\mathfrak{p}A_\mathfrak{m} = \mathfrak{m}A_\mathfrak{m}$, hence $\mathfrak{p} = \mathfrak{m}$ is maximal.
It's known that if the localizations of a domain at all maximal ideals are integrally closed, then the domain itself is integrally closed (`IsIntegrallyClosed.of_localization_maximal`). Hence our A is integrally closed. This completes the proof. □

3. Structure of module up to pseudo-isomorphism

3.1. **Characteristic ideal.**

Proposition 3.1. *Let A be a Noetherian ring, M be a finitely generated torsion A-module. Then for any height one prime $\mathfrak{p}$ of A, $M_\mathfrak{p}$ is an $A_\mathfrak{p}$-module of finite length. Moreover, there are only finitely many height one primes $\mathfrak{p}$ of A such that $M_\mathfrak{p} \neq 0$.*

Proof. By Proposition 2.1, we may let $0 = M_0 \subset M_1 \subset \cdots \subset M_n = M$ be a filtration of M such that for each $1 \leq i \leq n$, $M_i/M_{i-1} \cong A/\mathfrak{p}_i$ for some prime ideal $\mathfrak{p}_i$ of A. Note that if $\mathfrak{p}, \mathfrak{q}$ are prime ideals of A, then $(A/\mathfrak{p})_\mathfrak{q} \neq 0$ if and only if $\mathfrak{p} \subset \mathfrak{q}$. Therefore by M is torsion A-module, we obtain that $\mathrm{ht}(\mathfrak{p}_i) \geq 1$ for all $1 \leq i \leq n$, and if $\mathfrak{p}$ is a height one prime, then $M_\mathfrak{p} \neq 0$ if and only if $\mathfrak{p}_i \subset \mathfrak{p}$ for some i, by height considerations this means that $\mathfrak{p}_i = \mathfrak{p}$ for some i, hence such $\mathfrak{p}$ are only finitely many.

To prove $\ell_{A_\mathfrak{p}}(M_\mathfrak{p}) < \infty$, we only need to show that if $\mathfrak{p}, \mathfrak{q}$ are prime ideals of A such that $\mathrm{ht}(\mathfrak{p}) \geq 1$ and $\mathrm{ht}(\mathfrak{q}) = 1$, then $(A/\mathfrak{p})_\mathfrak{q}$ is an $A_\mathfrak{q}$-module of finite length. In fact, by height considerations we know that $(A/\mathfrak{p})_\mathfrak{q} \neq 0$ if and only if $\mathfrak{p} = \mathfrak{q}$, in this case $(A/\mathfrak{q})_\mathfrak{q} = A_\mathfrak{q}/\mathfrak{q}A_\mathfrak{q} = k(\mathfrak{q})$ is the residue field of $\mathfrak{q}$, which is an $A_\mathfrak{q}$-module of length one.

(*Another proof without using Proposition 2.1.* Note that $M_\mathfrak{p} = 0$ for all minimal prime ideals of A, therefore if $\mathfrak{p}$ is of height one such that $M_\mathfrak{p} \neq 0$, then $\mathfrak{p}$ is a minimal element in $\mathrm{Supp}(M)$, hence $\mathfrak{p} \in \mathrm{Ass}(M)$ which is a finite set. So there are only finitely many height one primes $\mathfrak{p}$ of A such that $M_\mathfrak{p} \neq 0$.

Suppose $\mathfrak{p}$ is a height one prime such that $M_\mathfrak{p} \neq 0$. To prove that $M_\mathfrak{p}$ is an $A_\mathfrak{p}$-module of finite length, we only need to prove that the ring $A_\mathfrak{p}/\mathrm{Ann}_{A_\mathfrak{p}}(M_\mathfrak{p})$ is Artinian. Note that $\mathrm{Ann}_{A_\mathfrak{p}}(M_\mathfrak{p}) = \mathrm{Ann}_A(M)_\mathfrak{p}$, hence $A_\mathfrak{p}/\mathrm{Ann}_{A_\mathfrak{p}}(M_\mathfrak{p}) = (A/\mathrm{Ann}_A(M))_\mathfrak{p}$ whose prime ideals are one-to-one correspondence to prime ideals of A between $\mathrm{Ann}_A(M)$ and $\mathfrak{p}$, i.e. prime ideals in $\mathrm{Supp}(M)$ which is contained in $\mathfrak{p}$. Such ideal can only be $\mathfrak{p}$ itself, since M is torsion, every prime ideal in $\mathrm{Supp}(M)$ has height ≥ 1. Hence $A_\mathfrak{p}/\mathrm{Ann}_{A_\mathfrak{p}}(M_\mathfrak{p})$ is Artinian.) □

In particular, this allows us to define the *characteristic ideal* of M.

Definition 3.2. Let A be a Noetherian ring, M be a finitely generated torsion A-module. The *characteristic ideal* of M, denoted by $\mathrm{char}_A(M)$, or simply $\mathrm{char}(M)$ if there is no risk of confusion, is defined to be

$$\mathrm{char}_A(M) := \prod_{\substack{\mathfrak{p} \in \mathrm{Spec}(A) \\ \mathrm{ht}(\mathfrak{p})=1}} \mathfrak{p}^{\ell_{A_\mathfrak{p}}(M_\mathfrak{p})}.$$

Proposition 3.3. *Let A be a Noetherian ring. Let $0 \to M' \to M \to M'' \to 0$ be a short exact sequence of finitely generated A-modules. Then M is A-torsion if and only if M' and M'' are A-torsion. If M is A-torsion, then* $\mathrm{char}_A(M) = \mathrm{char}_A(M')\,\mathrm{char}_A(M'')$.

Proof. Since localization is exact, for any prime ideal $\mathfrak{p}$ of A, the $0 \to M'_\mathfrak{p} \to M_\mathfrak{p} \to M''_\mathfrak{p} \to 0$ is exact. Let $\mathfrak{p}$ runs over all minimal prime ideals of A, we obtain that M is A-torsion if and only if M' and M'' are A-torsion. Also, we have $\ell_{A_\mathfrak{p}}(M_\mathfrak{p}) = \ell_{A_\mathfrak{p}}(M'_\mathfrak{p}) + \ell_{A_\mathfrak{p}}(M''_\mathfrak{p})$, hence $\mathrm{char}_A(M) = \mathrm{char}_A(M')\,\mathrm{char}_A(M'')$ holds. □

3.2. **Pseudo-null module.**

Definition 3.4. Let A be a Noetherian ring.

(i) A finitely generated A-module M is called a *pseudo-null* A-module, if $M_\mathfrak{p} = 0$ for all prime ideals $\mathfrak{p}$ of A of height ≤ 1.

(ii) An A-linear homomorphism $f : M \to N$ between finitely generated A-modules is called a *pseudo-isomorphism* (*pis* for short), if its kernel and cokernel are pseudo-null A-modules.

(iii) Two finitely generated A-modules M, N are called *pseudo-isomorphic* (*pis* for short), denoted by $M \sim_{\mathrm{pis}} N$ or simply $M \sim N$, if there exists a pseudo-isomorphism from M to N.

Remark 3.5. We warn the reader that $M \sim N$ not necessarily implies $N \sim M$.

Proposition 3.6. *Let A be a Noetherian ring, M be a finitely generated A-module.*

(i) *If A is of Krull dimension ≤ 1, then M is pseudo-null if and only if $M = 0$.*

(ii) *If A is of Krull dimension 2, is a local ring with finite residue field, then M is pseudo-null if and only if the cardinality of M is finite.*

Proof. (i) Clear.

(ii) Let $\mathfrak{m}$ be the maximal ideal of A. If M is finite, then there exists $r \in \mathbb{N}$ such that $\mathfrak{m}^r M = 0$, hence $\mathrm{supp}(M) \subset \{\mathfrak{m}\}$. On the other hand, if $\mathrm{supp}(M) \subset \{\mathfrak{m}\}$, then there exists $r \in \mathbb{N}$ such that $\mathfrak{m}^r M = 0$, hence $\mathfrak{m}^r \subset \mathrm{Ann}_A(M)$, therefore M is a finitely generated $A/\mathfrak{m}^r$-module, which must be finite. □

Proposition 3.7. *Let A be a Noetherian ring, M, N be finitely generated torsion A-modules.*

(i) *If M is pseudo-null, then* $\mathrm{char}_A(M) = 0$.

(ii) *If $M \sim N$, then* $\mathrm{char}_A(M) = \mathrm{char}_A(N)$.

Proof. Clear from definition and Proposition 3.3. □

3.3. **Structure theorem.**

Definition 3.8. Let A be a Noetherian ring. We say that the height one localization of A is PID (?), if

$$\text{For any finitely many height one primes } \mathfrak{p}_1, \cdots, \mathfrak{p}_r \text{ of } A, \text{ let } S := A \setminus \bigcup_{i=1}^r \mathfrak{p}_i, \text{ then } S^{-1}A \text{ is a PID.} \tag{3.1}$$

Lemma 3.9. *Let A be a Noetherian ring and let M, N be finitely generated torsion A-modules. Let $\Sigma = \{\mathfrak{q}_1, \cdots, \mathfrak{q}_r\} = \{\mathfrak{q} \in \operatorname{Supp}(M) \cup \operatorname{Supp}(N) \mid \operatorname{ht}(\mathfrak{q}) = 1\}$ (by Proposition 3.1 this is a finite set). Let $S := A \setminus \bigcup_{i=1}^r \mathfrak{q}_i$ which is a multiplicative subset of A. Let $f : M \to N$ be an A-module homomorphism. Then f is a pseudo-isomorphism if and only if $S^{-1}f : S^{-1}M \to S^{-1}N$ is an isomorphism.*

Proof. Since the height one support of $\ker(f)$ and $\operatorname{coker}(f)$ are contained in Σ, and since $S^{-1}\ker(f) = \ker(S^{-1}f)$, $S^{-1}\operatorname{coker}(f) = \operatorname{coker}(S^{-1}f)$ (localization is exact), we only need to prove that if M is a finitely generated torsion A-module whose height one support is contained in Σ, then $S^{-1}M = 0$ if and only if M is pseudo-null (equivalently, $M_{\mathfrak{q}} = 0$ for all $\mathfrak{q} \in \Sigma$): "⇒": Clear. "⇐": For all $\mathfrak{q} \in \Sigma$, $M_{\mathfrak{q}} = 0$ means that $\operatorname{Ann}(M) \not\subset \mathfrak{q}$, since $\mathfrak{q}$ are prime ideals, we have $\operatorname{Ann}(M) \not\subset \bigcup_{\mathfrak{q}\in\Sigma} \mathfrak{q}$, so $S^{-1}M = 0$. □

Proposition 3.10 (Structure theorem of finitely generated torsion A-modules)**.** *Let A be a Noetherian ring satisfying (3.1) and let M be a finitely generated torsion A-module. Then there exist height one primes $\mathfrak{p}_1, \cdots, \mathfrak{p}_s$ of A and positive integers $k_1, \cdots, k_s$, such that there exists a pseudo-isomorphism $M \to \bigoplus_{i=1}^s A/\mathfrak{p}_i^{k_i}$. Moreover, the sequence $(\mathfrak{p}_i^{k_i})_{i=1}^s$ is unique up to ordering.*

Proof. Let $\Sigma = \{\mathfrak{q}_1, \cdots, \mathfrak{q}_r\} = \{\mathfrak{q} \in \operatorname{Supp}(M) \mid \operatorname{ht}(\mathfrak{q}) = 1\}$ (by Proposition 3.1 this is a finite set), and let $S = A \setminus \bigcup_{i=1}^r \mathfrak{q}_i$. Then $S^{-1}M$ is a finitely generated $S^{-1}A$-module, and is torsion (for example, since $\operatorname{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}A) = S^{-1}\operatorname{Hom}_A(M, A) = 0$).

Note that the prime ideals $\mathfrak{P}$ of $S^{-1}A$ are one-to-one correspondence to prime ideals $\mathfrak{p}$ of A satisfying $\mathfrak{p} \cap S = \varnothing$ (i.e. $\mathfrak{p} \subset \bigcup_{i=1}^r \mathfrak{q}_i$, i.e $\mathfrak{p} \subset \mathfrak{q}_i$ for some i), by $\mathfrak{P} = S^{-1}\mathfrak{p}$ and $\mathfrak{p} = \mathfrak{P} \cap A$. In particular, $S^{-1}A$ is of dimension ≤ 1.

By structure theorem of finitely generated torsion modules over a PID, there exist primes $\mathfrak{p}_1, \cdots, \mathfrak{p}_s$ of A satisfying $\mathfrak{p}_i \cap S = \varnothing$, and positive integers $k_1, \cdots, k_s$, such that there exists an isomorphism $g : S^{-1}M \xrightarrow{\sim} \bigoplus_{i=1}^s S^{-1}(A/\mathfrak{p}_i^{k_i})$ of $S^{-1}A$-modules. Since $S^{-1}M$ is torsion, the $\mathfrak{p}_i$'s must be of height one. Since $\operatorname{Hom}_{S^{-1}A}(S^{-1}M, \bigoplus_{i=1}^s S^{-1}(A/\mathfrak{p}_i^{k_i})) = S^{-1}\operatorname{Hom}_A(M, \bigoplus_{i=1}^s A/\mathfrak{p}_i^{k_i})$, by multiplying an element of S to g if necessary (this doesn't change the fact that g is an isomorphism), we may find an A-linear map $f : M \to \bigoplus_{i=1}^s A/\mathfrak{p}_i^{k_i}$ such that $g = S^{-1}f$. Now by (i) we know that f is a pseudo-isomorphism.

Conversely, if $(\mathfrak{p}_i^{k_i})_{i=1}^s$ is such that there exists a pseudo-isomorphism $M \to \bigoplus_{i=1}^s A/\mathfrak{p}_i^{k_i}$, then enlarging S if necessary, by Lemma 3.9, its localization $S^{-1}M \to \bigoplus_{i=1}^s S^{-1}(A/\mathfrak{p}_i^{k_i})$ is an isomorphism of $S^{-1}A$-module, hence by structure theorem of finitely generated torsion modules over a PID, the $(\mathfrak{p}_i^{k_i})_{i=1}^s$ is unique up to ordering. □

Proposition 3.11. *Let A be a Noetherian ring satisfying (3.1). Let M, N be finitely generated torsion A-modules. Then the followings are equivalent:*

(a) *There exists a pseudo-isomorphism $M \to N$.*
(b) *For any height one prime $\mathfrak{p}$ of A, we have $M_{\mathfrak{p}} \cong N_{\mathfrak{p}}$.*

In particular, if there exists a pseudo-isomorphism $M \to N$, then there also exists a pseudo-isomorphism $N \to M$.

Proof. (a)⇒(b): Clear.

(b)⇒(a): Let $\Sigma = \{\mathfrak{q}_1, \cdots, \mathfrak{q}_r\} = \{\mathfrak{q} \in \operatorname{Supp}(M) \cup \operatorname{Supp}(N) \mid \operatorname{ht}(\mathfrak{q}) = 1\}$ (by Proposition 3.1 this is a finite set), and let $S = A \setminus \bigcup_{i=1}^r \mathfrak{q}_i$. Since $M_{\mathfrak{p}} \cong N_{\mathfrak{p}}$ for all height one primes $\mathfrak{p}$ of A, the $S^{-1}M$ and $S^{-1}N$, being finitely generated torsion modules over a PID $S^{-1}A$, are isomorphic. Say $g : S^{-1}M \xrightarrow{\sim} S^{-1}N$ is an isomorphism of $S^{-1}A$-modules. Since $\operatorname{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}N) = S^{-1}\operatorname{Hom}_A(M, N)$, by multiplying an element of S to g if necessary (this doesn't change the fact that g is an isomorphism), we may find an A-linear map $f : M \to N$ such that $g = S^{-1}f$. Now by Lemma 3.9 we know that f is a pseudo-isomorphism. □

3.4. **Noetherian regular domain.**

Proposition 3.12. *A Noetherian regular domain (more generally, a Noetherian integrally closed domain) satisfies* (3.1).

Proof. If A is a Noetherian regular domain (more generally, a Noetherian integrally closed domain), then for each height one prime $\mathfrak{p}$ of A, $A_{\mathfrak{p}}$ is a PID. For any finitely many height one primes $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ of A, let $S := A \setminus \bigcup_{i=1}^{r} \mathfrak{p}_i$, then $S^{-1}A$ is a semilocal integral domain, whose maximal ideals are $S^{-1}\mathfrak{p}_1, \cdots, S^{-1}\mathfrak{p}_r$, and we have $(S^{-1}A)_{S^{-1}\mathfrak{p}_i} = A_{\mathfrak{p}_i}$, therefore by (i) we know that $S^{-1}A$ is a PID. □

4. Structure of Iwasawa module

4.1. **Iwasawa algebra.** Let p be a prime, Γ be a topological abelian group, isomorphic to $\mathbb{Z}_p$ as a topological abelian group, and let $\gamma \in \Gamma$ be a topological generator of Γ (i.e. the subgroup $\{\gamma^n \mid n \in \mathbb{Z}\}$ is dense in Γ). For each $n \geq 0$ let $\Gamma_n := \Gamma/\Gamma^{p^n}$.

Definition 4.1. The *Iwasawa algebra* is defined as the completed group algebra

$$\Lambda := \mathbb{Z}_p[[\Gamma]] := \varprojlim_n \mathbb{Z}_p[\Gamma_n],$$

where the transition map $\mathbb{Z}_p[\Gamma_{n+1}] \to \mathbb{Z}_p[\Gamma_n]$ is induced by the natural projection $\Gamma_{n+1} \to \Gamma_n$. Each $\mathbb{Z}_p[\Gamma_n]$ is a free $\mathbb{Z}_p$-module of rank p^n, we endow it with the p-adic topology, and endow Λ with the subspace topology of the product topology of $\prod_{n=0}^{\infty} \mathbb{Z}_p[\Gamma_n]$.

Proposition 4.2. *Let A be a ring, $\mathfrak{a}$ be an ideal of A. Let M, N be two A-modules, and $\varphi : M \to N$ be an A-module homomorphism. Then φ is continuous if we endow M, N with $\mathfrak{a}$-adic topology.*

In particular, if φ is an A-module isomorphism, then it is a homeomorphism of topological spaces if we endow M, N with $\mathfrak{a}$-adic topology.

Proof. Let $x \in M$ and $y := \varphi(x) \in N$. Let U be any open neighborhood of y in N. Then there exists some n such that $y + \mathfrak{a}^n N \subset U$. Take $V = x + \mathfrak{a}^n M$ then it is an open neighborhood of x in M, and we have $\varphi(V) = y + \varphi(\mathfrak{a}^n M) = y + \mathfrak{a}^n \varphi(M) \subset y + \mathfrak{a}^n N \subset U$. Therefore φ is continuous. □

Proposition 4.3. *For each $n \geq 0$, there is an isomorphism of $\mathbb{Z}_p$-algebras*

$$\mathbb{Z}_p[\Gamma_n] \xrightarrow{\sim} \mathbb{Z}_p[T]/\big((1+T)^{p^n} - 1\big), \qquad \gamma \mapsto 1 + T.$$

They are all free $\mathbb{Z}_p$-modules of finite rank, we endow them with p-adic topology. By Proposition 4.2 we know that it is a homeomorphism of topological spaces.

Proof. We have $\Gamma/\Gamma^{p^n} \cong \mathbb{Z}/p^n\mathbb{Z}$ as an abelian group, and the image of $\gamma \in \Gamma$ in it is a generator of it. By abuse of notation we still denote the image of $\gamma \in \Gamma$ in it by γ. Then $\mathbb{Z}[\Gamma/\Gamma^{p^n}]$ as a $\mathbb{Z}$-module is free of rank p^n and $\{\gamma^k\}_{0 \leq k \leq p^n - 1}$ is a basis of it. Now it's easy to see that as a $\mathbb{Z}_p$-module homomorphism, $\mathbb{Z}_p[\Gamma/\Gamma^{p^n}] \xrightarrow{\sim} \mathbb{Z}_p[T]/\big((1+T)^{p^n} - 1\big)$, $\gamma^k \mapsto (1+T)^k$ is well-defined and is a $\mathbb{Z}_p$-module isomorphism, and preserves multiplication. Therefore it is an isomorphism of $\mathbb{Z}_p$-algebras. □

Proposition 4.4. *There is an isomorphism of topological rings $\mathbb{Z}_p[[T]] \xrightarrow{\sim} \Lambda$ sending $1 + T$ to γ, where $\mathbb{Z}_p[[T]]$ is endowed with (p, T)-adic topology.*

Proof. We prove that there is a natural isomorphism of $\mathbb{Z}_p$-algebras

$$\varprojlim_n \mathbb{Z}_p[T]/\big((1+T)^{p^n} - 1\big) \xrightarrow{\sim} \mathbb{Z}_p[[T]],$$

and which is a homeomorphism of topological spaces, where the topology of the left hand side is the subspace topology of the product topology of the topology defined in Proposition 4.3, and the topology of the right hand side it the (p, T)-adic topology. From which we can obtain the isomorphism of topological rings $\Lambda \xrightarrow{\sim} \mathbb{Z}_p[[T]]$ given by $\gamma \mapsto 1 + T$.

For simplicity of notation, denote $\varphi_n(T) := (1+T)^{p^n} - 1$. It's easy to see that for each $n \geq 1$ and for all $1 \leq i \leq p^n - 1$, we have $\binom{p^n}{i} \in p^n\mathbb{Z}$, hence $\varphi_n(T) \in T^{p^n} + p^n\mathbb{Z}[T]_{\deg \leq p^n - 1}$, in particular $\varphi_n(T)$ is a distinguished polynomial of degree p^n.

It's clear that $\mathbb{Z}_p[T]_{\deg \leq p^n - 1} \xrightarrow{\sim} \mathbb{Z}_p[T]/(\varphi_n(T))$ is an isomorphism of $\mathbb{Z}_p$-modules, and the Weierstrass division (Proposition 4.7) implies that $\mathbb{Z}_p[T]_{\deg \leq p^n - 1} \xrightarrow{\sim} \mathbb{Z}_p[[T]]/(\varphi_n(T))$ is also an isomorphism of $\mathbb{Z}_p$-modules, therefore the natural ring homomorphism $\mathbb{Z}_p[T] \hookrightarrow \mathbb{Z}_p[[T]]$ induces an isomorphism of $\mathbb{Z}_p$-algebras $\mathbb{Z}_p[T]/(\varphi_n(T)) \xrightarrow{\sim} \mathbb{Z}_p[[T]]/(\varphi_n(T))$ (Corollary 4.8).

Since each $\mathbb{Z}_p[[T]]/(\varphi_n(T))$ is a free $\mathbb{Z}_p$-module of finite rank endowed with the p-adic topology, we have $\mathbb{Z}_p[[T]]/(\varphi_n(T)) \cong \varprojlim_m \mathbb{Z}_p[[T]]/(p^m, \varphi_n(T))$, where each $\mathbb{Z}_p[[T]]/(p^m, \varphi_n(T))$ is endowed with discrete topology. Therefore we have the following isomorphisms of rings as well as topological spaces:

$$\varprojlim_n \overbrace{\mathbb{Z}_p[T]/(\varphi_n(T))}^{p\text{-adic topology}} \xrightarrow{\sim} \varprojlim_n \overbrace{\mathbb{Z}_p[[T]]/(\varphi_n(T))}^{p\text{-adic topology}} \cong \varprojlim_{m,n} \overbrace{\mathbb{Z}_p[[T]]/(p^m, \varphi_n(T))}^{\text{discrete topology}}$$
$$\overset{(*)}{\cong} \varprojlim_k \overbrace{\mathbb{Z}_p[[T]]/(p,T)^k}^{\text{discrete topology}} \xrightarrow{\sim} \overbrace{\mathbb{Z}_p[[T]]}^{(p,T)\text{-adic topology}},$$

here $(*)$ holds because $\{(p^m, \varphi_n(T))\}_{m\geq 1, n\geq 1}$ and $\{(p,T)^k\}_{k\geq 1}$ are *cofinal*. In fact, for each $k \geq 1$, and for any $m \geq k$ and $n \geq k$, we have $(p^m, \varphi_n(T)) \subset (p,T)^k$; conversely, for each $m \geq 1$ and $n \geq 1$, we have $(p,T)^{p^n} \subset (p, \varphi_n(T))$, and $(p, \varphi_n(T))^m \subset (p^m, \varphi_n(T))$, therefore for any $k \geq p^n m$, we have $(p,T)^k \subset (p,T)^{p^n m} \subset (p, \varphi_n(T))^m \subset (p^m, \varphi_n(T))$. □

4.2. **Weierstrass preparation theorem.** This is WIP in #21944.

Definition 4.5. If $(A, \mathfrak{m}, k)$ is a local ring, then a polynomial $f(X) = \sum_{i=0}^n a_i X^i \in A[X]$ is called a *distinguished polynomial* if $a_n = 1$ and $a_i \in \mathfrak{m}$ for all $0 \leq i \leq n-1$.

(Mathlib: `Polynomial.IsDistinguishedAt`)

Proposition 4.6. *Let A be a ring, and let $f(X) = \sum_{n=0}^\infty a_n X^n \in A[[X]]$ be a formal power series. Then $f(X) \in A[[X]]^\times$ if and only if $a_0 \in A^\times$.*

(Mathlib: `PowerSeries.isUnit_iff_constantCoeff`)

Proof. If $f(X) \in A[[X]]^\times$, then there exists $g(X) = \sum_{n=0}^\infty b_n X^n \in A[[X]]$ such that $f(X)g(X) = 1$, therefore by considering constant term we obtain $a_0 b_0 = 1$, hence $a_0 \in A^\times$. Conversely, if $a_0 \in A^\times$, by multiplying a_0^{-1} to $f(X)$ if necessary, we may assume that $a_0 = 1$ and $f(X) = 1 - X f_1(X)$ for some $f_1(X) \in A[[X]]$. Since $A[[X]]$ is (X)-adically complete and separated, it's easy to see that $1 + \sum_{k=0}^\infty X^k f_1(X)^k$ converges (X)-adically in $A[[X]]$ and which is the inverse of $f(X)$. □

Proposition 4.7 (Weierstrass division)**.** *Let $(A, \mathfrak{m}, k)$ be a complete local ring, $g(X) = \sum_{i=0}^\infty a_i X^i \in A[[X]] \setminus \mathfrak{m}[[X]]$ be a formal power series such that not all of its coefficients are in $\mathfrak{m}$. Let $n \geq 0$ be the integer such that $a_n \in A \setminus \mathfrak{m} = A^\times$ and $a_i \in \mathfrak{m}$ for all $0 \leq i \leq n-1$. Then for any $f \in A[[X]]$, there exists a unique formal power series $q(X) \in A[[X]]$ and a unique polynomial $r(X) \in A[X]$ of degree $\leq n-1$ such that $f = gq + r$.*

Proof. Write $g(X) = \sum_{i=0}^{n-1} a_i X^i + X^n g_1(X)$ for some $g_1(X) \in A[[X]]^\times$, and $f(X) = \sum_{i=0}^{n-1} b_i X^i + X^n f_1(X)$ for some $f_1(X) \in A[[X]]$. We construct a sequence $(q_k)_{k=1}^\infty$ inductively in $A[[X]]$, such that $f - gq_k \in A[X]_{\deg \leq n-1} + \mathfrak{m}^k[[X]]$, and such that $q_{k+1}(X) - q_k(X) \in \mathfrak{m}^k[[X]]$. We construct $q_1(X) := f_1(X) g_1(X)^{-1}$. Since $a_i \in \mathfrak{m}$ for all $i \leq n-1$, we have

$$\begin{aligned} f(X) - g(X)q_1(X) &= f(X) - \left(\sum_{i=0}^{n-1} a_i X^i\right) q_1(X) - X^n f_1(X) \\ &= \sum_{i=0}^{n-1} b_i X^i - \left(\sum_{i=0}^{n-1} a_i X^i\right) q_1(X) \in A[X]_{\deg \leq n-1} + \mathfrak{m}[[X]]. \end{aligned}$$

Suppose $q_k(X)$ is constructed, then we may write $f(X) - g(X)q_k(X) = \sum_{i=0}^{n-1} b_i^{(k)} X^i + X^n s_k(X)$ for some $s_k(X) \in \mathfrak{m}^k[[X]]$, and we construct $q_{k+1}(X) := q_k(X) + s_k(X) g_1(X)^{-1}$. Then we have

$$\begin{aligned} f(X) - g(X)q_{k+1}(X) &= \sum_{i=0}^{n-1} b_i^{(k)} X^i + X^n s_k(X) - \left(\sum_{i=0}^{n-1} a_i X^i\right) s_k(X) g_1(X)^{-1} - X^n s_k(X) \\ &= \sum_{i=0}^{n-1} b_i^{(k)} X^i - \left(\sum_{i=0}^{n-1} a_i X^i\right) s_k(X) g_1(X)^{-1} \in A[X]_{\deg \leq n-1} + \mathfrak{m}^{k+1}[[X]]. \end{aligned}$$

Since $A[[X]]$ is complete and separated according to the sequence $\{\mathfrak{m}^k[[X]]\}_{k\geq 1}$ of ideals, there exists a unique limit $q(X) \in A[[X]]$ of the sequence $(q_k)_{k=1}^\infty$, which satisfies $r := f - gq \in A[X]_{\deg \leq n-1}$.

To prove the uniqueness, suppose $q(X) \in A[[X]]$ and $r(X) \in A[X]_{\deg \leq n-1}$ such that $gq = r$, then we prove by induction that for any $k \geq 0$ we have $q, r \in \mathfrak{m}^k[[X]]$, which implies that $q = r = 0$. When $k = 0$

there is nothing to prove. Suppose $q, r \in \mathfrak{m}^k[[X]]$ for some $k \geq 0$. Then we have $(\sum_{i=0}^{n-1} a_i X^i)q(X) + X^n g_1(X)q(X) = r(X)$, since $a_i \in \mathfrak{m}$ for all $i \leq n-1$, we obtain $r(X) \in \mathfrak{m}^{k+1}[X]_{\deg \leq n-1}$. Multiply $g_1(X)^{-1}$ to both side, we obtain $(\sum_{i=0}^{n-1} a_i X^i)q(X)g_1(X)^{-1} + X^n q(X) = r(X)g_1(X)^{-1}$, therefore $q(X) \in \mathfrak{m}^{k+1}[[X]]$. □

Corollary 4.8. *Let $(A, \mathfrak{m}, k)$ be a complete local ring, $g(X) = \sum_{i=0}^{n} a_i X^i \in A[X]$ be a polynomial such that $a_n \in A \setminus \mathfrak{m}$ and $a_i \in \mathfrak{m}$ for all $i < n$. Then the natural map $A[X]/(g) \to A[[X]]/(g)$ is an isomorphism.*

Proof. Let $f \in A[[X]]$. Then by Proposition 4.7, we may find a unique formal power series $q(X) \in A[[X]]$ and a unique polynomial $r(X) \in A[X]$ of degree $\leq n-1$ such that $f = gq + r$. Then r is the unique inverse of f under the natural map $A[X]/(g) \to A[[X]]/(g)$. □

Proposition 4.9 (Weierstrass preparation theorem)**.** *Let $(A, \mathfrak{m}, k)$ be a complete local ring. Let $g(X) \in A[[X]] \setminus \mathfrak{m}[[X]]$ be a formal power series such that not all of its coefficients are in $\mathfrak{m}$. Then there is a unique distinguished polynomial $f(X) \in A[X]$ and a unique invertible formal power series $h(X) \in A[[X]]^\times$ such that $g = fh$.*

Proof. Take $f(X) = X^n$ in Proposition 4.7, we obtain $q(X) \in A[[X]]$ and $r(X) \in A[X]_{\deg \leq n-1}$ such that $X^n = g(X)q(X) + r(X)$. Since $g(X) = \sum_{i=1}^{n-1} a_i X^i + X^n g_1(X)$ with $a_i \in \mathfrak{m}$ for all $i \leq n-1$ and $g_1(X) \in A[[X]]^\times$, we have $r(X) \in \mathfrak{m}[X]_{\deg \leq n-1}$, and by the construction in (ii) we have $q(X) \in g_1(X)^{-1} + \mathfrak{m}[[X]] \subset A[[X]]^\times$. Therefore take $h(X) := q(X)^{-1} \in A[[X]]^\times$ and $f(X) := X^n - r(X)$, then $f(X)$ is a distinguished polynomial of degree n, and $g(X) = f(X)h(X)$ holds.

To prove the uniqueness, suppose $f(X)$ and $f'(X)$ are two distinguished polynomials and $u(X) \in A[[X]]^\times$ such that $f'(X) = f(X)u(X)$. Then $\overline{u}(X) \in k[[X]]^\times$ and we have $\overline{f}'(X) = X^{\deg(f')} = \overline{f}(X)\overline{u}(X) = X^{\deg(f)}\overline{u}(X) \in k[[X]]^\times$, which forces that $\deg(f) = \deg(f')$ and $\overline{u}(X) = 1$. Therefore $f'(X) - f(X) \in A[X]_{\deg \leq \deg(f)-1}$ and $f'(X) = f(X) + (f'(X) - f(X))$ is a Weierstrass division of f' by f, on the other hand, $f'(X) = f(X)u(X)$ is also a Weierstrass division of f' by f, hence by the uniqueness of Weierstrass division we have $u(X) = 1$ and $f'(X) = f(X)$.

(*Another proof.* It is possible to prove Weierstrass preparation theorem using a form of Hensel's lemma presented in https://ncatlab.org/nlab/show/Hensel's+lemma.) □

4.3. **Characteristic ideal.**

Proposition 4.10. *$\Lambda \cong \mathbb{Z}_p[[T]]$ is a Noetherian regular local ring of Krull dimension 2.*

Corollary 4.11. *Hence by Proposition 2.4, Λ is a UFD (or maybe one can check directly that the I-adic completion of a UFD is a UFD).*

Corollary 4.12. *Hence by Proposition 2.3, any height 1 prime $\mathfrak{p}$ of Λ is principal.*

(i) *If the generator of $\mathfrak{p}$ is in $p\mathbb{Z}_p[[T]]$, then we must have $\mathfrak{p} = (p)$.*

(ii) *If the generator of $\mathfrak{p}$ is not in $p\mathbb{Z}_p[[T]]$, then by Proposition 4.9 such $\mathfrak{p}$ has a unique generator which is a distinguished polynomial.*

Therefore, we have

Proposition 4.13. *If X is a finitely generated torsion Λ-module, then there exists a pseudo-isomorphism*

$$X \to \bigoplus_{i=1}^{m} \Lambda/(f_i^{b_i}) \oplus \bigoplus_{j=1}^{s} \Lambda/(p^{n_j})$$

where $f_1, \cdots, f_m$ are distinguished polynomials. The characteristic ideal $\mathrm{char}_\Lambda(X)$ is generated by $p^{\sum_{j=1}^{s} n_j} \prod_{i=1}^{m} f_i^{b_i}$ which is contained in $p^{\sum_{j=1}^{s} n_j}\mathbb{Z}_p[[T]]$ but not in $p^{1+\sum_{j=1}^{s} n_j}\mathbb{Z}_p[[T]]$.

Definition 4.14. (i) The μ-invariant of X is defined to be $\mu(X) := \sum_{j=1}^{s} n_j$, and the λ-invariant of X is defined to be $\lambda(X) := \sum_{i=1}^{m} b_i \deg f_i$.

(ii) If $f \in \mathbb{Z}_p[[T]]$ is not zero, then define $\mu(f)$ be the integer such that $f \in p^{\mu(f)}\mathbb{Z}_p[[T]]$ but $f \notin p^{1+\mu(f)}\mathbb{Z}_p[[T]]$, define $\lambda(f)$ be the leading degree of $(p^{-\mu(f)} f \bmod p) \in \mathbb{F}_p[[T]]$.

Clearly, $\mu(X)$ and $\lambda(X)$ are equal to $\mu(f)$ and $\lambda(f)$ if $\mathrm{char}_\Lambda(X) = (f)$.

Proposition 4.15. *We have $\mu(X) = \sum_{i=0}^{\infty} \mathrm{rank}_{\mathbb{F}_p[[T]]} X[p^{i+1}]/X[p^i]$, and $\lambda(X) = \mathrm{rank}_{\mathbb{Z}_p} X/X[p^\infty]$.*

.....

4.4. **Growth of coinvariant part.**

Proposition 4.16. *If X is a finitely generated torsion Λ-module such that $X/(\gamma^{p^n}-1)X$ is finite for any $n \geq 0$, then there exists some constant $\nu = \nu(X)$ such that for all sufficiently large n, $\mathrm{ord}_p(\#(X/(\gamma^{p^n}-1)X)) = \mu(X)p^n + \lambda(X)n + \nu(X)$.*

5. Arithmetic of $\mathbb{Z}_p$-extensions

5.1. **The class group of $\mathbb{Z}_p$-extension of a number field.** Let K be a number field, p be a prime, K_∞/K be a $\mathbb{Z}_p$-extension.

Definition 5.1. (i) For each $n \geq 0$ let L_n be the p^∞-Hilbert class field of K_n. That is, the maximal unramified abelian extension of K_n of exponent p^∞.

(ii) Let $X_n := \mathrm{Gal}(L_n/K_n) \cong \mathrm{Cl}(K_n)(p)$, the maximal quotient of the class group $\mathrm{Cl}(K_n)$ which is p^∞-torsion.

Definition 5.2. (i) Let $L_\infty := \bigcup_{n\geq 0} L_n = \bigcup_{n\geq 0} L_nK_\infty$, then it is an unramified abelian pro-p extension of K_∞, because each L_nK_∞/K_∞ is finite unramified abelian p-extension.

(ii) Let L'_∞ be the maximal unramified abelian pro-p extension of K_∞, that is, the compositum of all finite unramified abelian p-extensions of K_∞.

Proposition 5.3. $L'_\infty = L_\infty$.

Note that $L'_\infty = L_\infty$ is a Galois extension of K.

Proof. It is easy to see that "$\supset$" holds. As for "$\subset$", suppose E is a finite unramified abelian p-extension of K_∞, we want to prove $E \subset L_\infty$. The proof consists of the following steps:

(1) There exists an integer $n_0 \geq 0$ such that E/K_{n_0} is Galois.

(2) There exists an integer $n_1 \geq n_0$ such that $\mathrm{Gal}(E/K_{n_1})$ is abelian. So $\mathrm{Gal}(E/K_{n_1}) \cong \mathrm{Gal}(K_\infty/K_{n_1}) \times G$, where G is a finite abelian group, corresponding to some E_{n_1}/K_{n_1} finite abelian extension, so that $E = K_\infty E_{n_1}$.

(3) There exists an integer $n_2 \geq n_1$ such that $E_{n_1}K_{n_2}/K_{n_2}$ is a finite unramified abelian p-extension. Therefore $E_{n_1}K_{n_2} \subset L_{n_2}$, hence $E \subset L_{n_2}K_\infty \subset L_\infty$. □

Lemma 5.4. *Suppose X has rank r as a Λ-module, then we have*

$$\mathrm{rank}_{\mathbb{Z}_p}\left(X/((1+T^{p^n})-1)X\right) = rp^n + O(1)$$

as $n \to \infty$. This is left as an exercise. For example, if $X = \Lambda$, then $r = 1$, and $\mathrm{rank}_{\mathbb{Z}_p}\left(X/((1+T^{p^n})-1)X\right) = p^n$.

Proposition 5.5. *If K is any number field, K_∞/K is any $\mathbb{Z}_p$-extension, and $\mathfrak{l}$ is a prime of K not lying over p. Then $\mathfrak{l}$ is unramified in K_∞/K.*

Proof. Let $D_\mathfrak{l}$ be the decomposition subgroup of $\mathfrak{l}$ in $\Gamma := \mathrm{Gal}(K_\infty/K)$. Let $l = \mathrm{char}(\mathcal{O}_K/\mathfrak{l}) \neq p$, then $K_\mathfrak{l}/\mathbb{Q}_l$ is a finite extension, and let $(K_\infty)_\mathfrak{l} := \varinjlim (K_n)_\mathfrak{l}$, then $D_\mathfrak{l} = \mathrm{Gal}((K_\infty)_\mathfrak{l}/K_\mathfrak{l})$ is a subgroup of $\mathbb{Z}_p$.

We have $K_\mathfrak{l} \subset K_\mathfrak{l}^{\mathrm{unr}} \subset K_\mathfrak{l}^{\mathrm{ab}}$, and

$$\mathrm{Gal}(K_\mathfrak{l}^{\mathrm{unr}}/K_\mathfrak{l}) \cong \widehat{\mathbb{Z}} = \prod_{q \text{ prime}} \mathbb{Z}_q.$$

So $K_\mathfrak{l}$ has at least one $\mathbb{Z}_p$-extension, i.e. the unique unramified $\mathbb{Z}_p$-extension. If there are other $\mathbb{Z}_p$-extensions of $K_\mathfrak{l}$, then there exists a Galois extension of $K_\mathfrak{l}$ with Galois group isomorphic to $\mathbb{Z}_p^2$.

However, $\mathrm{Gal}(K_\mathfrak{l}^{\mathrm{ab}}/K_\mathfrak{l}^{\mathrm{unr}})$ doesn't have a quotient isomorphic to $\mathbb{Z}_p$, because by local class field theory, $\mathrm{Gal}(K_\mathfrak{l}^{\mathrm{ab}}/K_\mathfrak{l}^{\mathrm{unr}}) \cong \mathcal{O}_{K_\mathfrak{l}}^\times \cong (\text{a finite group}) \times \mathbb{Z}_l^{[K_\mathfrak{l}:\mathbb{Q}_l]}$ which is a finite group times a pro-l group, obviously it doesn't have a quotient isomorphic to $\mathbb{Z}_p$. So there is only one $\mathbb{Z}_p$-extension of $K_\mathfrak{l}$, note that $(K_\infty)_\mathfrak{l}/K_\mathfrak{l}$ is either trivial or a $\mathbb{Z}_p$-extension, in both cases it must be contained in $K_\mathfrak{l}^{\mathrm{unr}}$. □

Theorem 5.6 (Iwasawa)**.** *Suppose K is any number field, and K_∞/K is any $\mathbb{Z}_p$-extension. Let L_∞ be the maximal unramified abelian pro-p extension of K_∞, let $X_\infty := \mathrm{Gal}(L_\infty/K_\infty)$ which is a Λ-module, where $\Lambda := \mathbb{Z}_p[[\Gamma]]$, isomorphic to $\mathbb{Z}_p[[T]]$ by choosing a topological generator γ of Γ, and maps T to $\gamma - 1$. Then X_∞ is a finitely generated torsion Λ-module.*

Proof. Consider $\mathrm{Gal}(K_\infty/K_n) = \Gamma^{p^n}$ with topological generator γ^{p^n}. Let E_n be the maximal abelian extension of K_n contained in L_∞, so that $\mathrm{Gal}(L_\infty/E_n) = \mathrm{Gal}(L_\infty/K_n)' = (\gamma^{p^n}-1)X_\infty$. Note that $X_\infty/TX_\infty \cong \mathrm{Gal}(E_0/K_\infty)$ is a finitely generated $\mathbb{Z}_p$-module, so by Nakayama lemma (Lemma 2.5) we know that X_∞ is finitely generated Λ-module.

Recall that if $r = \mathrm{rank}_\Lambda X_\infty$, then $\mathrm{rank}_{\mathbb{Z}_p}\left(X_\infty/(\gamma^{p^n}-1)X_\infty\right) = rp^n + O(1)$ as $n \to \infty$ (Lemma 5.4). So in order to prove X_∞ is torsion (i.e. $r = 0$), we only need to prove $\mathrm{rank}_{\mathbb{Z}_p}\left(X_\infty/(\gamma^{p^n}-1)X_\infty\right)$ is bounded.

Let $\mathfrak{p}_1, \cdots, \mathfrak{p}_t$ be the primes of K which are ramified in K_∞/K. Then t is finite (by Proposition 5.5), and number of primes of K_∞ lying over $\mathfrak{p}_1, \cdots, \mathfrak{p}_t$ is also finite, because for each i, the index $[\Gamma : D_{\mathfrak{p}_i}]$ is finite. So let s_n be the number of primes of K_n which are ramified in K_∞/K_n, then s_n is bounded.

Consider E_n/K_n. Recall that L_n is the p-Hilbert class field of K_n. Then $L_n \subset L_\infty$, $K_\infty \subset L_\infty$, so $L_nK_\infty \subset E_n$. Let $I_1, \cdots, I_{s_n}$ be the inertia subgroups of $\mathrm{Gal}(E_n/K_n)$ for the ramified primes. For $1 \le j \le s_n$, $I_j \cap \mathrm{Gal}(E_n/K_\infty) = \{1\}$, because E_n/K_∞ is unramified. Therefore I_j maps injectively to a closed subgroup of Γ^{p^n} via the map $\mathrm{Gal}(E_n/K_n) \to \mathrm{Gal}(K_\infty/K_n)$, in particular, I_j is isomorphic to $\mathbb{Z}_p$.

Now we come to the key point. Let $I := I_1 \cdots I_{s_n} \subset \mathrm{Gal}(E_n/K_n)$, then $\mathrm{rank}_{\mathbb{Z}_p} I \le s_n$, and E_n^I is the maximal unramified abelian pro-p extension of K_n, so $E_n^I = L_n$, hence $\mathrm{rank}_{\mathbb{Z}_p}\mathrm{Gal}(E_n/K_n) \le s_n$, because $\mathrm{Gal}(L_n/K_n) \cong \mathrm{Cl}(K_n)(p)$ is a finite group. Therefore $\mathrm{rank}_{\mathbb{Z}_p}\mathrm{Gal}(E_n/K_\infty) \le s_n - 1$, because $\mathrm{Gal}(K_\infty/K_n) = \Gamma^{p^n}$ is of $\mathbb{Z}_p$-rank 1. Note that $\mathrm{Gal}(E_n/K_\infty) \cong X_\infty/(\gamma^{p^n}-1)X_\infty$, so $\mathrm{rank}_{\mathbb{Z}_p}\left(X_\infty/(\gamma^{p^n}-1)X_\infty\right)$ is bounded. □

5.2. **Recover the finite level of class group from infinite level.** Back to K_n and K_∞. Recall that $X_\infty := \mathrm{Gal}(L_\infty/K_\infty) = \varprojlim \mathrm{Gal}(L_n/K_n)$, and $X_n := \mathrm{Gal}(L_n/K_n) \cong \mathrm{Cl}(K_n)(p)$.

Let $\Gamma := \mathrm{Gal}(K_\infty/K) \cong \mathbb{Z}_p$, choose a topological generator γ of Γ (or equivalently, $\gamma \in \Gamma$ such that $\gamma|_{K_1}$ is nontrivial).

Proposition 5.7. *(This is incorrect ...) For each $n \ge 0$ there is an isomorphism $X_\infty/(\gamma^{p^n}-1)X_\infty \xrightarrow{\sim} X_n$.*

Proof. Let $G := \mathrm{Gal}(L_\infty/K)$. We claim that $(\gamma-1)X_\infty$ is a closed normal subgroup of G and $X_\infty/(\gamma-1)X_\infty \cong X_0 = \mathrm{Cl}(K)(p)$. We have a group extension

$$0 \to X_\infty \to G \to \Gamma \to 1,$$

which induces

$$0 \to X_\infty/(\gamma-1)X_\infty \to G/(\gamma-1)X_\infty \to \Gamma \to 1,$$

so $G/(\gamma-1)X_\infty$ is abelian, and $(\gamma-1)X_\infty$ is a closed normal subgroup. The proof of Proposition 5.8 can be easily modified to show that $(\gamma-1)X_\infty = G'$. Let $E = L_\infty^{G'}$ be the maximal abelian extension of K contained in L_∞. Let $I_{\mathfrak{P}}$ be the inertia subgroup of $\mathrm{Gal}(E/K)$ for a prime $\mathfrak{P} \mid \mathfrak{p}$, then $L_0 = E^{I_{\mathfrak{P}}}$. Let $H = \mathrm{Gal}(E/K_\infty)$ (so that $K_\infty = E^H$), then $L_0 \cap K_\infty = K$, $H \cap I_{\mathfrak{P}} = \{1\}$, so $E = L_0K_\infty$, and $\mathrm{Gal}(E/K_\infty) \xrightarrow{\sim} \mathrm{Gal}(L_0/K)$ is a natural isomorphism. Hence we conclude that $X_\infty/(\gamma-1)X_\infty \xrightarrow{\sim} X_0$.

In general, consider L_n/K_n, the p-Hilbert class field of K_n, so that $\mathrm{Gal}(L_n/K_n) =: X_n \cong \mathrm{Cl}(K_n)(p)$. We have $\mathrm{Gal}(K_\infty/K_n) \cong \Gamma^{p^n} \cong p^n\mathbb{Z}_p$ with topological generator γ^{p^n}. We have K_∞/K_n is ramified at only one place and is totally ramified. So similarly, we get $X_\infty/(\gamma^{p^n}-1)X_\infty \xrightarrow{\sim} X_n$. □

We state a group theory result. Suppose $\mathcal{G}$ is any group, $\mathcal{X}$ is a normal abelian subgroup of $\mathcal{G}$. Then $\mathcal{G}/\mathcal{X}$ acts on $\mathcal{X}$ as follows: if $\sigma \in \mathcal{G}/\mathcal{X}$, lift σ to an element $\widetilde{\sigma}$ in $\mathcal{G}$. Then define for all $x \in \mathcal{X}$, $\sigma(x) := \widetilde{\sigma}x\widetilde{\sigma}^{-1}$. Note that $\sigma(x)x^{-1} = \widetilde{\sigma}x\widetilde{\sigma}^{-1}x^{-1} \in \mathcal{G}'$.

Assume $\mathcal{G}/\mathcal{X}$ is cyclic with a generator g, then $\mathcal{G}' = \{g(x)x^{-1} \mid x \in \mathcal{X}\}$. We write $\mathcal{X}$ additively, then $g(x)x^{-1}$ becomes $g(x) - x = (g-1)x$.

If we view $g-1$ as an element in $\mathbb{Z}[\mathcal{G}/\mathcal{X}]$, and view $\mathcal{X}$ as a $\mathbb{Z}[\mathcal{G}/\mathcal{X}]$-module, then $\{g(x)-x \mid x \in \mathcal{X}\} = (g-1)\mathcal{X}$ is a $\mathbb{Z}[\mathcal{G}/\mathcal{X}]$-submodule of $\mathcal{X}$. Hence $(g-1)\mathcal{X}$ is a normal subgroup of $\mathcal{G}$.

Proposition 5.8. $\mathcal{G}' = (g-1)\mathcal{X}$.

Proof. "$\supset$" is trivial. As for "$\subset$", we have an exact sequence

$$0 \to \mathcal{X}/(g-1)\mathcal{X} \to \mathcal{G}/(g-1)\mathcal{X} \to \mathcal{G}/\mathcal{X} \to 0,$$

and $\mathcal{G}/(g-1)\mathcal{X}$ is a central extension of $\mathcal{G}/\mathcal{X}$ (which is cyclic) by $\mathcal{X}/(g-1)\mathcal{X}$, so it is abelian, so $\mathcal{G}' \subset (g-1)\mathcal{X}$. □

Appendix A. Known results in mathlib

A.1. **Rings.**

- Commutative ring with unit `CommRing`
- Field `Field`
  - assertion that a ring is a field `IsField`
- assertion that a ring is an integral domain `IsDomain`
- assertion that a ring is PID: `IsDomain` + `IsPrincipalIdealRing`
- assertion that a ring is UFD: `IsDomain` + `UniqueFactorizationMonoid`
- Noetherian ring `IsNoetherianRing`
  - finitely many minimal prime ideals `minimalPrimes.finite_of_isNoetherianRing`
  - finitely many minimal prime over-ideals `Ideal.finite_minimalPrimes_of_isNoetherianRing`
- Artin ring `IsArtinianRing`
  - it is also Noetherian `instIsNoetherianRingOfIsArtinianRing` (instance, shouldn't need to call directly)
- Characteristic of a ring `ringChar`, exponential characteristic `ringExpChar`
  - assertion that a ring is of specific characteristic `CharZero`, `CharP`, `ExpChar`
- Krull dimension of a ring `ringKrullDim`
  - assertion that a ring is of Krull dimension $\leq n$ `Ring.KrullDimLE`
  - assertion that a ring is of Krull dimension ≤ 1 `Ring.DimensionLEOne`

A.2. **Ideals.**

- Ideal of a ring `Ideal`
  - assertion that an ideal is principal `Submodule.IsPrincipal`
  - assertion that an ideal is a prime ideal `Ideal.IsPrime`
    - `Ideal.Quotient.isDomain_iff_prime`
  - assertion that an ideal is a maximal ideal `Ideal.IsMaximal`
    - `Ideal.Quotient.maximal_ideal_iff_isField_quotient`
    - `Ideal.Quotient.field` (instance, shouldn't need to call directly)
- Height of an ideal `Ideal.height`, height of a prime ideal `Ideal.primeHeight`
  - assertion that an ideal is the whole ring or of finite height `Ideal.FiniteHeight`
- the `Type` of prime ideals of a ring $\mathrm{Spec}(R)$ `PrimeSpectrum`
- set of minimal primes `minimalPrimes`, set of minimal prime over-ideals `Ideal.minimalPrimes`

A.3. **Modules.**

- Support of a module $\mathrm{Supp}(M)$ `Module.support`
- Annihilator of a module $\mathrm{Ann}(M)$ `Module.annihilator`
- $M^* = \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Q}/\mathbb{Z})$ `CharacterModule`
- Associated primes of a module $\mathrm{Ass}(M)$ `associatedPrimes`
- Finitely generated module `Module.Finite`
- Free module `Module.Free`
- Projective module `Module.Projective`
- Injective module `Module.Injective`
- Flat module `Module.Flat`
- Torsion module `Module.IsTorsion`
- Torsion submodule `Submodule.torsion`
  - Torsion-free module `Submodule.torsion R M = ⊥`
- Noetherian module `IsNoetherian`
- Artin module `IsArtinian`
- assertion that a module is of finite length `IsFiniteLength`
  - in the statement of theorems use `IsNoetherian` + `IsArtinian` instead
  - if and only if exists composition series `isFiniteLength_iff_exists_compositionSeries`
  - length of a module $\ell_A(M)$ `Module.length`
- composition series `CompositionSeries`
  - usage:
    `∃ (s : CompositionSeries (Submodule R M)), RelSeries.head s = ⊥ ∧ RelSeries.last s = ⊤`

A.4. **Number theory.**

- assertion that a field is a number field (i.e. finite extension of $\mathbb{Q}$) `NumberField`
- ring of integers $\mathcal{O}_K$ `NumberField.RingOfIntegers`
- assertion that a ring is a Dedekind domain `IsDedekindDomain`
  - unique factorization of ideals `Ideal.uniqueFactorizationMonoid` (instance, shouldn't need to call directly)
- fraction ideals `FractionalIdeal`
  - usage: if R is a domain, K is fraction field of R, then the `Type` of fraction ideals in K is: `FractionalIdeal (nonZeroDivisors R) K`
  - $\mathrm{ord}_{\mathfrak{p}}(\mathfrak{a})$ `FractionalIdeal.count`
- ideal class group `ClassGroup`
  - finite `NumberField.RingOfIntegers.instFintypeClassGroup` (instance, shouldn't need to call directly)
  - class number `NumberField.classNumber`
- places of a number field K: `AbsoluteValue K ℝ`, `NumberField.place`
  - infinite places `NumberField.InfinitePlace`
  - real and complex places `NumberField.InfinitePlace.IsReal`, `NumberField.InfinitePlace.IsComplex`
  - r_1, r_2 `NumberField.InfinitePlace.nrRealPlaces`, `NumberField.InfinitePlace.nrComplexPlaces`
  - $r_1 + r_2 - 1$ `NumberField.Units.rank`
  - Dirichlet unit theorem `NumberField.Units.rank_modTorsion`
- assertion that a field extension is abelian `#23669`
- assertion that a field extension is cyclotomic `IsCyclotomicExtension`
  - cyclotomic field $K(\mu_n)$ `CyclotomicField`
- p-adic cyclotomic character: if $\mu_{p^\infty} \subset L$ then $\chi_{\mathrm{cyc}} : \mathrm{Aut}(L) \to \mathbb{Z}_p^\times$ `#21934`

References

[Nek06] J. Nekovář. *Selmer complexes*. Astérisque No. 310 (2006), viii+559 pp.

[NSW08] J. Neukirch, A. Schmidt, K. Wingberg. *Cohomology of number fields*. Second edition. Grundlehren Math. Wiss., 323. Springer-Verlag, Berlin, 2008. xvi+825 pp.

[Was97] L. C. Washington. *Introduction to cyclotomic fields*. Second edition. Grad. Texts in Math., 83. Springer-Verlag, New York, 1997. xiv+487 pp.