Introduction to Iwasawa Theory

Yi Ouyang
Department of Mathematical Sciences
Tsinghua University
Beijing, China **100084**
Email: youyang@math.tsinghua.edu.cn

Contents

Chapter 1

Modules up to pseudo-isomorphism

Let A be a commutative noetherian integrally closed domain. Let K be the quotient field of A. Let $P(A) = \{\wp \in \mathrm{Spec}(A) \mid \mathrm{ht}\,\wp = 1\}$ be the set of prime ideals of A of height 1. Then for every $\wp \in P(A)$, $A_\wp$ is a discrete valuation ring.

Theorem 1.1.

$$A = \bigcap_{\wp \in P(A)} A_\wp.$$

Proof. See [7, Theorem 11.5, page 81]. This is a well known theorem about normal noetherian domains. □

For an A-module M, we let

$$M^+ := \mathrm{Hom}_A(M, A).$$

Thus there is a pairing

$$M^+ \times M \to A, \qquad (\alpha, m) \mapsto \alpha(m)$$

which induces a homomorphism of A-modules $\varphi_M : M \to M^{++}$.

Definition 1.2. An A-module M is called *reflexive* if the canonical map

$$\begin{aligned} \varphi_M : M &\longrightarrow M^{++} = \mathrm{Hom}_A(\mathrm{Hom}_A(M, A), A) \\ m &\longmapsto (\varphi_M(m) : \alpha \mapsto \alpha(m)) \end{aligned}$$

is an isomorphism.

Remark. M^+ is always torsion free, thus M is reflexive implies that M is torsion free.

Assume M is a finitely generated torsion free A-module, then

$$M \hookrightarrow M_\wp \hookrightarrow M_\wp \otimes_{A_\wp} K = M \otimes_A K := V$$

and

$$M^+ \hookrightarrow (M^+)_\wp \hookrightarrow (M^+)_\wp \otimes_{A_\wp} K = M^+ \otimes_A K = V^\wedge$$

where $V^\wedge = \mathrm{Hom}_K(V, K)$ is the dual of V. One has

$$M^+ = \{\lambda \in V^\wedge \mid \lambda(m) \in A \text{ for all } m \in M\},$$

$$(M^+)_\wp = \{\lambda \in V^\wedge \mid \lambda(m) \in A_\wp \text{ for all } m \in M_\wp\} = (M_\wp)^+,$$

where $M_\wp$ is regarded as an $A_\wp$-module.

Lemma 1.3. *Let M be a finitely generated torsion free A-module, then*

(1) $M^+ = \bigcap_{\wp \in P(A)} M_\wp^+$.

(2) $M^{++} = \bigcap_{\wp \in P(A)} M_\wp$.

(3) M is reflexive if and only if $M = \bigcap_{\wp \in P(A)} M_\wp$.

Proof. (1) $\subseteq$ is trivial. If $\lambda \in \bigcap_{\wp \in P(A)} M_\wp^+$, then for all $m \in M$, $\lambda(m) \in A_\wp$ for $\wp \in P(A)$, hence $\lambda(m) \in A$ and $\lambda \in M^+$.

(2) since $M_\wp = M_\wp^{++}$ for $\mathrm{ht}\, \wp = 1$ ($A_\wp$ is a discrete valuation ring).

(3) follows from (2). □

Corollary 1.4. *If M is a finitely generated A-module, then M^+ is reflexive.*

Definition 1.5. A finitely generated A-module M is called *pseudo-null* if the following two equivalent conditions are fulfilled:

(1) $M_\wp = 0$ for all prime ideals $\wp$ in A of height $\mathrm{ht}(\wp) \leq 1$, i.e., $\mathrm{Supp}(M) = \{\wp \in \mathrm{Spec}(A) \mid M_\wp \neq 0\} \subseteq \{\wp \in \mathrm{Spec}(A) \mid \mathrm{ht}(\wp) \geq 2\}$.

(2) If $\wp$ is a prime ideal with $\mathrm{ann}_A(M) \subseteq \wp$, then $\mathrm{ht}(\wp) \geq 2$. Recall that $\mathrm{ann}_A(M) = \{a \in A \mid aM = 0\}$.

Remark. (i) For the equivalence of the two conditions: $M_\wp = 0$ if and only if there exists $s \in A \backslash \wp$, such that $sM = 0$, which is equivalent to $\mathrm{ann}_A(M) \nsubseteq \wp$.

(ii) A pseudo-null module is torsion since $M_{(0)} = M \otimes_A K = 0$.

(iii) If A is a Dedekind domain, then M is pseudo-null if and only if $M = 0$.

(iv) If A is a 2-dimensional noetherian integrally closed local ring with finite residue field, then M is pseudo-null if and only if M is finite.

Indeed, let $\mathfrak{m}$ be the maximal ideal of A, if M is finite, there exists $r \in \mathbb{N}$ such that $\mathfrak{m}^r M = 0$, thus $\mathrm{Supp}(M) \subseteq \{\mathfrak{m}\}$. On the other hand, if $\mathrm{Supp}(M) \subseteq \{\mathfrak{m}\}$,then there exists $r \in \mathbb{N}$ such that $\mathfrak{m}^r M = 0$, thus $\mathfrak{m}^r \subseteq \mathrm{ann}_A(M)$, therefore M is a finitely generated $A/\mathfrak{m}^r$-module, hence finite.

Definition 1.6. Let $f : M \to N$ be a homomorphism of finitely generated A-modules M and N. f is called a *pseudo-isomorphism* if both $\ker f$ and $\operatorname{coker} f$ are pseudo-null, equivalently, if the induced homomorphisms

$$f_\wp : M_\wp \longrightarrow N_\wp$$

are isomorphisms for all $\wp \in P(A) \bigcup \{0\}$. We write a pseudo-isomorphism f as $f : M \xrightarrow{\approx} N$ or $f : M \sim N$.

Lemma 1.7. *Let M be a finitely generated A-torsion module, if $0 \neq \alpha \in A$ such that $\operatorname{Supp}(A/\alpha A)$ is disjoint to $\operatorname{Supp}(M) \cap P(A)$, then*

$$\alpha : M \longrightarrow M, \quad m \longmapsto \alpha m$$

is a pseudo-isomorphism.

Proof. This is clear since α is a unit of $A_\wp$ for every $\wp \in \operatorname{Supp}(M) \cap P(A)$. □

From now on, we set

$T_A(M)$: the torsion submodule of M;
$F_A(M) = M/T_A(M)$: the maximal torsion free quotient of M.

Proposition 1.8. *Let M be a finitely generated A-module. Then*
(1) There exists a pseudo-isomorphism

$$f : M \xrightarrow{\approx} T_A(M) \bigoplus F_A(M).$$

(2) There exists $\{\wp_i\}_{i \in I} \subseteq P(A)$, $n_i \in \mathbb{N}$, and a pseudo-isomorphism

$$g : T_A(M) \xrightarrow{\approx} \bigoplus_{i \in I} A/\wp_i^{n_i}$$

where $\{\wp_i, n_i\}$ are uniquely determined by $T_A(M)$ up to re-numbering.

Proof. (1) Let $\{\wp_1, \cdots, \wp_h\} = \operatorname{Supp}(M) \cap P(A)$. If $h = 0$, then $T_A(M)$ is pseudo-null, the homomorphism

$$f : M \xrightarrow{(0,\mathrm{can})} T_A(M) \bigoplus F_A(M)$$

is a pseudo-isomorphism.

If $h > 0$, let

$$S = \bigcap_{i=1}^{h} A \backslash \wp_i = A \Big\backslash \bigcup_{i=1}^{h} \wp_i.$$

then $S^{-1}A$ is a semi-local Dedekind domain with maximal ideals $S^{-1}\wp_i$, $i = 1, \cdots, h$. Thus $S^{-1}A$ is a principal ideal domain by the approximation theorem,

and $S^{-1}T_A(M)$ is a direct summand of $S^{-1}M$ and is the torsion module of $S^{-1}M$. Since M is finitely generated, then

$$\mathrm{Hom}_{S^{-1}A}(S^{-1}M, S^{-1}T_A(M)) = S^{-1}\,\mathrm{Hom}_A(M, T_A(M)).$$

Thus there exists $f_0 : M \to T_A(M)$ and $s_0 \in S$ such that

$$\frac{f_0}{s_0} : S^{-1}M \longrightarrow S^{-1}T_A(M)$$

is the projection of $S^{-1}M$ onto $S^{-1}T_A(M)$, hence

$$\frac{f_0}{s_0}|_{S^{-1}T_A(M)} = \mathrm{Id}_{S^{-1}T_A(M)}\,.$$

Thus there exists $s_1 \in S$, $f_1 = s_1 f_0$ such that $f_1|_{T_A(M)} = s_1 s_0\,\mathrm{Id}_{T_A(M)}$. Let

$$f = (f_1, \mathrm{can}) : M \longrightarrow T_A(M) \oplus F_A(M)$$

by the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & T_A(M) & \longrightarrow & M & \longrightarrow & F_A(M) & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f_1|_{T_A(M)}} & & \downarrow{\scriptstyle f} & & \| & & \\ 0 & \longrightarrow & T_A(M) & \longrightarrow & T_A(M) \oplus F_A(M) & \longrightarrow & F_A(M) & \longrightarrow & 0 \end{array}$$

By Lemma 1.7, $f_1|_{T_A(M)}$ is a pseudo-isomorphism, the snake lemma implies that f is also a pseudo-isomorphism.

(2) By the structure theorem of finitely generated modules over a principal ideal domain, there exists an isomorphism

$$g_0 : S^{-1}T_A(M) \xrightarrow{\cong} S^{-1}E = S^{-1}\left(\bigoplus_{i=1}^{h}\bigoplus_{j=1}^{r_i} A/\wp_i^{n_{ij}}\right)$$

for some uniquely determined

$$E = \bigoplus_{i=1}^{h}\bigoplus_{j=1}^{r_i} A/\wp_i^{n_{ij}}.$$

Using

$$\mathrm{Hom}_{S^{-1}A}(S^{-1}T_A(M), S^{-1}E) = S^{-1}\,\mathrm{Hom}_A(T_A(M), E),$$

again we obtain $g : T_A(M) \to E$ and $s \in S$, such that $g = sg_0$. Again using the previous lemma, g is a pseudo-isomorphism. □

Remark. (i) If M, N are torsion modules, then $f : M \xrightarrow{\approx} N$ implies that there exists $g : N \xrightarrow{\approx} M$.

In general, this is not true. For example, let $A = \mathbb{Z}_p[[T]] = \Lambda$, $N = \Lambda$ and $M = \ker(N \to \mathbb{Z}/p\mathbb{Z})$. Then $M \overset{\approx}{\to} N$ but $N \overset{\not\approx}{\to} M$.

(ii) If the exact sequence of finitely generated A-torsion modules

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

satisfies that the associated sets of prime ideals of height 1 of M' and M'' are disjoint. Then $M \overset{\approx}{\to} M' \oplus M''$.

Proposition 1.9. *Let M be a finitely generated torsion free A-module. Then there exists an injective pseudo-isomorphism of M onto a reflexive A-module M'.*

Proof. Consider the homomorphism $\varphi_M : M \to M^{++}$. One notes that:

(1) $M_\wp \cong M^{++}_\wp$ for $\operatorname{ht}\wp \leq 1$. In particular, $\ker\varphi_M \otimes_A K = 0$, hence $\ker\varphi_M$ is torsion. As M is torsion free, $\ker\varphi_M = 0$;

(2) M^{++} is reflexive. □

Proposition 1.10. *Let A be an n-dimensional regular local ring, $2 \leq n < \infty$. Let $\{p_1, \cdots, p_n\}$ be a regular system of parameters generating the maximal ideal of A. Let $p_0 := 0$. Then for a finitely generated A-module M, the following two assertions are equivalent:*

(1) For every $i = 0, \cdots, n-2$, the $A/(p_0, \cdots, p_i)$-module $M/(p_0, \cdots, p_i)M$ is reflexive.

(2) M is a free A-module.

In particular, a reflexive A-module M over a 2-dimensional regular local ring A is free.

Proof. We only need to show (1)⇒ (2).

From (1), M is reflexive, hence torsion free. Let $\varphi : A^r \twoheadrightarrow M$ be a minimal free presentation of M. Consider the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A^r & \xrightarrow{p_1} & A^r & \longrightarrow & (A/p_1)^r & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle\varphi} & & \downarrow{\scriptstyle\varphi} & & \downarrow{\scriptstyle\tilde{\varphi}} & & \\ 0 & \longrightarrow & M & \xrightarrow{p_1} & M & \longrightarrow & M/p_1M & \longrightarrow & 0 \end{array}$$

Assume M/p_1 is a free A/p_1-module, then by Nakayama Lemma and the minimality of r, $\tilde{\varphi}$ is an isomorphism. Hence $p_1 : \ker\varphi \to \ker\varphi$ is an isomorphism. By Nakayama again, $\ker\varphi = 0$. We get M is a free A-module. Thus we only need to show

(*) M/p_1 is a free A/p_1-module

Note that

(i) A/p_1 is a regular local ring of dimension $n-1$;

(ii) Let $\tilde{p}_i = p_i + p_1 A$, then $\{\tilde{p}_2, \cdots, \tilde{p}_n\}$ is a regular system of parameter of A/p_1.

Thus (1) holds for $(A/p_1, M/p_1)$. By induction, we only need to check (*) for $n = 2$. In this case, A/p_1 is regular of dimension 1, hence a discrete valuation ring and an integral domain. Thus $\mathrm{Hom}_A(M^+, A/p_1)$ is torsion free, therefore

$$M/p_1 = M^{++}/p_1 = \mathrm{Hom}_A(M^+, A) \otimes A/p_1 \hookrightarrow \mathrm{Hom}_A(M^+, A/p_1)$$

is also torsion free over the discrete valuation ring A/p_1, which must be free. □

Theorem 1.11 (Structure Theorem)**.** *Let A be a 2-dimensional regular local ring and M be a finitely generated A-module. Then there exists finitely many primes $\wp_i$ of height 1, natural numbers n_i for each i, nonnegative integer r and a pseudo-isomorphism*

$$f : M \xrightarrow{\approx} A^r \oplus \bigoplus_{i \in I} (A/\wp_i^{n_i}),$$

$\wp_i$, n_i and r are uniquely determined by

$$r = \dim_K M \otimes_A K, \quad \{\wp_i | i \in I\} = \mathrm{Supp}\, M \cap P(A).$$

Chapter 2

Iwasawa modules

In this chapter, we let K be a finite extension of $\mathbb{Q}_p$ and let $\mathcal{O}$ be the ring of integers of K, let π be a uniformizing parameter of $\mathcal{O}$. Let $k = \mathcal{O}/(\pi)$ be the residue field of $\mathcal{O}$. Then k is a finite extension of $\mathbb{F}_p$. As a convention, we write $\Lambda = \mathbb{Z}_p[[T]]$.

For $f(T) = a_0 + a_1 T + \cdots + a_i T^i + \cdots \in \mathcal{O}[[T]]$, $f \neq 0$, set

$$\mu(f) = \min\{\mathrm{ord}_\pi(a_i)\}, \quad \lambda(f) = \min\{i : \mathrm{ord}_\pi(a_i) = \mu(f)\}.$$

Lemma 2.1 (Division Lemma)**.** *Suppose $f = a_0 + a_1 T + \cdots \in \mathcal{O}[[T]]$ but $\pi \nmid f$, i.e. $\mu(f) \not= 0$. Let $n = \lambda(f)$. Then any $g \in \mathcal{O}[[T]]$ can be uniquely written as*

$$g = qf + r$$

where $q \in \mathcal{O}[[T]]$, and $r \in \mathcal{O}[T]$ is a polynomial of degree at most $n-1$.

Proof. First we show the uniqueness. If $qf + r = 0$, we need to show that $q = r = 0$. If not, we may assume that $\pi \nmid q$ or $\pi \nmid r$. But $0 = qf + r \mod \pi$ implies that $\pi \mid r$ and therefore $\pi \mid qf$. Since $\pi \nmid f$, we have $\pi \mid q$, contradiction!

For the existence, we have two proofs.

First proof: We let $\tau_n = \tau$ be the $\mathcal{O}$-linear map

$$\sum_{i=0}^{\infty} b_i T^i \longmapsto \sum_{i=n}^{\infty} b_i T^{i-n}.$$

Note that

(i) $\tau(T^n h) = h$ for $h \in \mathcal{O}[[T]]$.

(ii) $\tau(h) = 0$ if and only if h is a polynomial of degree $\leq n-1$.

Write $f = \pi P(T) + T^n U(T)$, where $P(T)$ is a polynomial of degree at most $n-1$ and $U(T)$ is a unit in $\mathcal{O}[[T]]$. For any $g \in \mathcal{O}[[T]]$, let

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

Then

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

and

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

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

Second proof: Note that $k[[T]]$ is a discrete valuation ring, it has a simple division algorithm. We let $\bar{g}(T)$ be the reduction of $g(T)$ modulo π. Since $\bar{f}(T) = T^n \cdot (\text{unit})$ in $k[[T]]$, we have

$$\bar{g}(T) = \bar{q}(T)\bar{f}(T) + \bar{r}(T)$$

for suitable $\bar{q}(T) \in k[[T]]$ and $\bar{r}(T) \in k[T]$ of degree $\leq n-1$. Let $q_1(T) \in \mathcal{O}[[T]]$, $r_1(T) \in \mathcal{O}[T]$ (of the same degree of $\bar{r}(T)$) be liftings of $\bar{q}(T)$ and $\bar{r}(T)$ respectively. Then

$$g(T) = f(T)q_1(T) + r_1(T) + \pi g_1(T)$$

for some $g_1(T) \in \mathcal{O}[[T]]$. Apply the same procedure for g_1, we get

$$\begin{aligned}g(T) &= f(T)q_1(T) + r_1(T) + \pi(f(T)q_2'(T) + r_2'(T) + \pi g_2(T))\\ &= f(T)q_2(T) + r_2(T) + \pi^2 g_2(T)\end{aligned}$$

where $q_2 = q_1 \mod \pi$, $r_2 = r_1 \mod \pi$. Repeat the process, we get

$g(T) = f(T)q_n(T)+r_n(T)+\pi^n g_n(T)$, $q_{n+1} = q_n \mod \pi^n$, $r_{n+1} = r_n \mod \pi^n$.

By taking the limits, the desired result is obtained. □

Corollary 2.2. *If $\pi \nmid f \in \mathcal{O}[[T]]$ (i.e., $\mu(f) = 0$), then $\mathcal{O}[[T]]/(f)$ is a free $\mathcal{O}$-module of rank $n = \lambda(f)$ with basis $\{T^i : i < n\}$.*

Definition 2.3. A *distinguished polynomial* (or *Weierstrass polynomial*) $F(T) \in \mathcal{O}[T]$ is a polynomial of the form

$$F(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_0, \quad a_i \in (\pi).$$

We note that an Eisenstein polynomial is an irreducible distinguished polynomial.

Corollary 2.4. *Let F be a distinguished polynomial, then*

$$\mathcal{O}[T]/F\mathcal{O}[T] \xrightarrow{\cong} \mathcal{O}[[T]]/F\mathcal{O}[[T]].$$

Theorem 2.5 (Weierstrass Preparation Theorem)**.** *Let $f \in \mathcal{O}[[T]]$, $f \neq 0$. Then f can be uniquely written as*

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

where $\mu = \mu(f)$, $P(T)$ is a distinguished polynomial of degree $n = \lambda(f)$, $U(T)$ is a unit in $\mathcal{O}[[T]]$. As a consequence, $\mathcal{O}[[T]]$ is a factorial domain.

Proof. One may assume $\pi \nmid f$. Write $f = a_0 + a_1 T + \cdots + a_n T^n + \cdots$ with $\pi \nmid a_n$ and $\pi \mid a_i$ for $i < n$. By the division lemma, $T^n = q(T)f(T) + r(T)$ with $\deg r < n$ and $q(T) \in \mathcal{O}[[T]]$. One has $r(T) = 0 \mod \pi$. Therefore $f(T)q(T) = T^n - r(T) := P(T) = T^n \mod \pi$, we have $q(T)a_n = 1 \mod \pi$ and $q(T) := \frac{1}{U(T)} \in (\mathcal{O}[[T]])^{\times}$. Thus in this case $f(T) = U(T)P(T)$. The uniqueness follows from the division lemma, since $T^n = U(T)^{-1} f(T) + (T^n - P(T))$. □

Remark. For $\pi \nmid f$, then $\mathcal{O}[[T]]/(f(T)) \cong \mathcal{O}[T]/(P(T))$. Thus $P(T)$ is the characteristic polynomial of the linear transformation $T : \mathcal{O}[[T]]/(f) \to \mathcal{O}[[T]]/(f)$.

Corollary 2.6. *There are only finitely many $x \in \mathbb{C}_p$, $|x| < 1$ such that $f(x) = 0$.*

Proof. This is an easy exercise. □

Lemma 2.7. *Let P be a distinguished polynomial. If $\frac{g(T)}{P(T)} \in \mathcal{O}[[T]]$, $g(T) \in \mathcal{O}[T]$, then $\frac{g(T)}{P(T)} \in \mathcal{O}[T]$.*

Proof. Let $g(T) = P(T)f(T)$, $f \in \mathcal{O}[[T]]$. For any root $x \in \mathbb{C}_p$ of $P(T)$, $0 = P(x) = x^n +$ multiple of π, one has $|x| < 1$, hence $f(x)$ converges and $g(x) = 0$. Continue this process, we get $P(T) \mid g(T)$ as polynomials, hence $f(T) \in \mathcal{O}[T]$. □

Let $\Gamma = \mathbb{Z}_p = \varprojlim_n \mathbb{Z}/p^n\mathbb{Z}$. As a profinite group, Γ is compact and procyclic. Let γ be a topological generator of Γ, i.e., $\Gamma = \overline{\langle \gamma \rangle}$. Let $\Gamma_n = \overline{\langle \gamma^{p^n} \rangle}$ be the unique closed subgroup of index p^n of Γ, then Γ/Γ_n is cyclic of order p^n generated by $\gamma + \Gamma_n$. One has an isomorphism

$$\begin{aligned} \mathcal{O}[\Gamma/\Gamma_n] &\xrightarrow{\sim} \mathcal{O}[T]/\left((1+T)^{p^n} - 1\right) \\ \gamma \mod \Gamma_n &\longmapsto (1+T) \mod (1+T)^{p^n} - 1 \end{aligned}$$

Moreover, if $m \geq n \geq 0$, the natural map $\Gamma/\Gamma_m \to \Gamma/\Gamma_n$ induces a natural map $\phi_{m,n} : \mathcal{O}[\Gamma/\Gamma_m] \to \mathcal{O}[\Gamma/\Gamma_n]$, which is compatible with the isomorphism. We let

$$\mathcal{O}[[\Gamma]] = \varprojlim_n \mathcal{O}[\Gamma/\Gamma_n] = \varprojlim_n \mathcal{O}[T]/\left((1+T)^{p^n} - 1\right).$$

Note that $\mathcal{O}$ is a topological ring, compact and complete with π-adic topology, so are the rings $\mathcal{O}[\Gamma/\Gamma_n]$, thus $\mathcal{O}[[\Gamma]]$ is endowed with the product topology of π-adic topology, it is also compact and π-complete. The ring $\mathcal{O}[[\Gamma]]$ is called the *Iwasawa algebra* and its modules are called *Iwasawa modules*.

Theorem 2.8. *One has a topological isomorphism*

$$\mathcal{O}[[T]] \longrightarrow \mathcal{O}[[\Gamma]], \quad T \longmapsto \gamma - 1$$

where $\mathcal{O}[[T]]$ is a compact topological ring complete with (π, T)-topology.

Proof. Write $\omega_n(T) = (1+T)^{p^n} - 1$. ω_n is a distinguished polynomial. Moreover,

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

thus $\omega_n(T) \in (p, T)^{n+1}$ for $n \geq 0$.

By Corollary 2.4, for every $n \in \mathbb{N}$, we have a projection

$$\mathcal{O}[[T]] \twoheadrightarrow \mathcal{O}[[T]]/(\omega_n) \xrightarrow{\sim} \mathcal{O}[T]/(\omega_n) \xrightarrow{\sim} \mathcal{O}[\Gamma/\Gamma_n]$$

which is compatible with the transition map. By the universal property of projective limits, then we have a continuous homomorphism

$$\epsilon : \quad \mathcal{O}[[T]] \to \mathcal{O}[[\Gamma]], \quad T \mapsto \gamma - 1.$$

On one hand $\ker \epsilon \subseteq \bigcap_n (\omega_n) \subseteq \bigcap_n (p, T)^{n+1} = 0$, thus ϵ is injective. On the other hand, $\mathcal{O}[[T]]$ is compact, hence the image is closed, it is also dense since at every level the map is surjective, hence ϵ is also surjective. □

From now on let $\mathcal{O} = \mathbb{Z}_p$ and $\Lambda = \mathbb{Z}_p[[T]]$. Let $\mathfrak{m} = (p, T)$ be the maximal ideal of Λ. We identify $\mathbb{Z}_p[[\Gamma]]$ and Λ by the above Theorem, though we should keep in mind that this isomorphism depends on the choice of the topological generator γ of Γ. Write $\omega_n(T) = (1+T)^{p^n} - 1$ and $\nu_{n,e}(T) = \omega_n(T)/\omega_e(T)$.

Lemma 2.9. *If f and g are relatively prime to each other, then $|\Lambda/(f, g)| < \infty$.*

Proof. Let $h \in (f, g)$ be of minimal degree. we show that $h = p^s$(up to $\mathbb{Z}_p^*$). If not, $h = p^s H$ for $\deg H \geq 1$. By the division algorithm, $f = Hq + r$, thus $p^s r \in (f, g)$, contradiction! □

Proposition 2.10. *The prime ideals of Λ are*

$$(0), \quad \mathfrak{m} = (p, T), \quad (p), \quad (P)$$

where P are irreducible distinguished polynomials in Λ.

Proof. First all in the list are prime ideals. Let $\wp$ be a prime ideal of Λ and $h \in \wp$ be of minimal degree. Then $h = p^s H$ with $H = 1$ or distinguished (up to $\mathbb{Z}_p^*$). If $H \neq 1$, then it must be irreducible by minimality. Then $(f) \subseteq \wp$ where $f = p$ or an irreducible distinguished polynomial. If $(f) = \wp$, we are done. If

not, there exists $g \in \wp$ such that f, g are relatively prime. By the above lemma, $|\Lambda/\wp| \leq |\Lambda/(f,g)| < \infty$. Therefore $p^N \in \wp$ for $N \gg 0$, which implies $p \in \wp$ since $\wp$ is prime; also there exists a pair $i < j$, such that $T^i - T^j \in \wp$, as $1 - T^{j-i}$ is a unit, $T^i \in \wp$, hence $T \in \wp$. Thus $(p, T) \subseteq \wp$. □

Theorem 2.11 (Structure Theorem for Iwasawa modules)**.** *For any finitely generated Λ-module M,*

$$M \xrightarrow{\approx} \Lambda^r \oplus \bigoplus_{i=1}^{s} \Lambda/p^{m_i} \oplus \bigoplus_{j=1}^{t} \Lambda/F_j^{n_j}$$

where $r = \operatorname{rank} M$, $m_i (i = 1, \cdots s)$, F_j and n_j $(j = 1, \cdots, t)$ are uniquely determined by M.

Definition 2.12. $F_M = \prod_{j=1}^{t} F_j^{n_j}$ is called the *characteristic polynomial* of M.

If M is a torsion module, we define the *Iwasawa invariants* of M by

$$\lambda(M) = \sum_{i=1}^{s} m_i, \quad \mu(M) = \sum_{j} n_j \deg F_j = \deg F_M.$$

Remark. The isomorphism of $\mathbb{Z}_p[[\Gamma]]$ and $\mathbb{Z}_p[[T]]$ depends on the choice of γ. Therefore if a finitely generated Iwasawa module M is considered as a Λ-module, the corresponding F_j and F_M depend on the choice of γ, but $\lambda(M)$ and $\mu(M)$ are independent invariants.

Lemma 2.13 (Topological Nakayama's Lemma)**.** *Let M be a compact Λ-module. Then the following are equivalent:*

(1) M is finitely generated over Λ;

(2) M/TM is a finitely generated $\mathbb{Z}_p$-module;

(3) $M/(p,T)M$ is a finitely dimensional $\mathbb{F}_p$-vector space.

Proof. (1) $\Rightarrow$ (2) $\Rightarrow$ (3) are easy. Assuming (3), let $x_1, \cdots, x_n$ generate $M/(p,T)M$ as $\mathbb{F}_p$-vector space. Let $N = \Lambda x_0 + \cdots + \Lambda x_n \subseteq M$, then

$$\frac{M}{N} = \frac{N + (p,T)M}{N} = (p,T)\frac{M}{N}.$$

Thus $M/N = (p,T)^n M/N$ for all $n > 0$.

Consider a small neighborhood U of 0 in M/N. Since $(p,T)^n \to 0$ in Λ, for any $z \in M/N$, there exists a neighborhood U_z of z and some n_z such that $(p,T)^{n_z} U_z \subseteq U$. But M/N is compact, then $(p,T)^n M/N \subseteq U$ for $n \gg 0$, hence $M/N = \cap (p,T)^n M/N = 0$ and $M = N$ is finitely generated over Λ. □

Theorem 2.14. *Let X be a compact Λ-module. Then*

(1) $X = 0 \Leftrightarrow X/TX = 0 \Leftrightarrow X/\mathfrak{m}X = 0$.

(2) X is a finitely generated Λ-module $\Leftrightarrow$ X/TX is a finitely generated $\mathbb{Z}_p$-module $\Leftrightarrow$ $X/\mathfrak{m}X$ is a finite dimensional $\mathbb{F}_p$-vector space. Moreover, for

a finitely generated Λ-module X, the minimal number of generators of X is $\dim_{\mathbb{F}_p}(X/\mathfrak{m}X)$.

(3) If X/TX is finite, then X is a torsion Λ-module.

(4) If we replace T by any distinguished polynomial in (1), (2) and (3), the corresponding assertions still hold.

Proof. (1) and (2) are Nakayama's Lemma.

For (3), by (2), X is a finitely generated Λ-module. Let $x_1, \cdots, x_d$ be a set of generators. Suppose X/TX has exponent p^k, then $p^k x_i \in TX$ for $1 \leq i \leq d$. Write

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

and let $A = (p^k \delta_{ij} - T a_{ij}(T))_{i,\, j}$ and $g(T) = \det A$. Then $g(T)x_i = 0$ for all $i = 1, \cdots, d$ but $g(0) = p^{dk} \neq 0$, hence X is torsion.

(4) follows similarly. □

Lemma 2.15. *Let g be a distinguished polynomial of degree d prime to ω_n/ω_e for every $n > e$. Then for $n \gg 0$,*

$$|\Lambda/(g, \omega_n)| = p^{dn+O(1)}.$$

Proof. We know $\Lambda/(g, \omega_n)$ is finite for $n \gg 0$ by Lemma 2.9. Write $V = \Lambda/(g(T))$. Since $T^d = pQ(T) \mod g$, by induction, then for $k \geq d$, $T^k = p \cdot \text{poly.} \mod g$. Therefore for $p^n \geq d$,

$$(1+T)^{p^n} = 1 + p \cdot \text{poly.} \mod g$$

and

$$\begin{aligned}
(1+T)^{p^{n+1}} &= (1 + p \cdot \text{poly.})^p = 1 + p^2 \cdot \text{poly.} \mod g, \\
\frac{\omega_{n+2}(T)}{\omega_{n+1}(T)} &= \frac{(1+T)^{p^{n+2}} - 1}{(1+T)^{p^{n+1}} - 1} \\
&= (1+T)^{(p-1)p^{n+1}} + \cdots + (1+T)^{p^{n+1}} + 1 \\
&= p(1 + p \cdot \text{poly.}) \mod g.
\end{aligned}$$

Thus $\frac{\omega_{n+2}(T)}{\omega_{n+1}(T)}$ acts as $p \cdot$ unit on V for $p^n \geq d$.

For $n_0 > e$, $p^n \geq d$ and $n \geq n_0$, then $\omega_{n+2}V = \frac{\omega_{n+2}(T)}{\omega_{n+1}(T)}(\omega_{n+1}V) = p\omega_{n+1}V$, and

$$\begin{aligned}
|V/\omega_{n+2}V| &= |V/pV| \cdot |pV/p\omega_{n+1}V| = |V/pV| \cdot |V/\omega_{n+1}V| \\
&= p^{d(n-n_0+1)} |V/\omega_{n_0+1}V| = p^{nd+c}.
\end{aligned}$$

This finishes the proof. □

Lemma 2.16. *For a Λ-module M, let $M_\Gamma = M/TM$ and $M^\Gamma = M^{\gamma=1}$. If there is exact sequence*

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0,$$

then there is a long exact sequence

$$0 \to M'^\Gamma \to M^\Gamma \to M''^\Gamma \to M'_\Gamma \to M_\Gamma \to M''_\Gamma \to 0.$$

Proof. Apply the snake lemma to the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \gamma-1} & & \downarrow{\scriptstyle \gamma-1} & & \downarrow{\scriptstyle \gamma-1} & & \\ 0 & \longrightarrow & M' & \longrightarrow & M & \longrightarrow & M'' & \longrightarrow & 0 \end{array}$$

with exact rows. □

Remark. If replacing γ by γ^{p^n}, we shall have corresponding results.

Proposition 2.17. *Let M be a finitely generated torsion Λ-module such that $M/\omega_n M$ is finite for all $n \geq 0$. Then for $n \gg 0$, $|M/\omega_n M| = p^{\mu(M)p^n + \lambda(M) + O(1)}$ where $\lambda(M)$ and $\mu(M)$ are Iwasawa invariants.*

Proof. By the above lemma, we can replace M by a torsion Λ-module of the form $\bigoplus_{i=1}^s (\Lambda/p^{k_i}) \oplus \bigoplus_{j=1}^t (\Lambda/f_j(T)^{m_j})$. Now just apply Lemma 2.15. □

Chapter 3

$\mathbb{Z}_p$-extensions

Definition 3.1. A $\mathbb{Z}_p$-extension is a Galois extension K_∞/K whose Galois group is isomorphic to the ring of p-adic integers $\mathbb{Z}_p$.

Proposition 3.2. *There are exactly one sub-extension K_n of K inside K_∞ with Galois group* $\mathrm{Gal}(K_n/K) \cong \mathbb{Z}/p^n\mathbb{Z}$ *cyclic of order p^n.*

Proof. This follows easily from the fundamental theorem of Galois Theory, as the only closed subgroups of $\mathbb{Z}_p$ are 0 and $p^n\mathbb{Z}_p$ for $n \in \mathbb{N}$. □

Proposition 3.3. *Let K be a number field, then $\mathbb{Z}_p$-extensions over K are unramified outside p.*

Proof. Let v be a prime of K not lying above p. We need to show the inertia subgroup I of v is 0. if not, $I = p^n\mathbb{Z}_p$ for some $n \in \mathbb{N}$. By local class field theory, $U_{K_v} \twoheadrightarrow I = p^n\mathbb{Z}_p$ is surjective, but $U_{K_v} =$ finite groups $\times\, \mathbb{Z}_\ell^a$ for $a \in \mathbb{N}$ and $\ell \neq p$, this is impossible. □

Lemma 3.4. *Let K be a number field. Then there exists at least one prime ramified in K_∞/K, and there exists $n \geq 0$ such that every prime which is ramified in K_∞/K is totally ramified in K_∞/K_n.*

Proof. This is an easy exercise. □

Suppose K is a number field. Let $E = \mathcal{O}_K^\times$ be the group of global units. Let

$$E_1 = \{x \in E \mid x \equiv 1 \mod \wp \text{ for all } \wp \mid p\}.$$

Let $U_{1,\wp}$ be the group of local units congruent to 1 mod $\wp$. Then we have an injective diagonal map

$$\psi : E \to U = \prod_{\wp \mid p} U_\wp, \quad \epsilon \mapsto (\epsilon, \cdots, \epsilon)$$

such that $\psi(E_1) \subseteq U_1 = \prod_{\wp \mid p} U_{1,\wp}$.

Lemma 3.5. *(1)* $\overline{\psi(E_1)} = U_1 \cap \overline{K^\times \prod_{v\nmid p} U_v}$.

(2) $\overline{\psi(E)} = U \cap \overline{K^\times \prod_{v\nmid p} U_v}$.

Proof. (1). $\subseteq$ is easy. For $\supseteq$, we write $U_n = \prod_{v|p} U_{n,v}$, where $U_{n,v}$ is the group of local units congruent to 1 mod v^n, then

$$\overline{K^\times \prod_{v\nmid p} U_v} = \bigcap_n (K^\times \prod_{v\nmid p} U_v U_n), \quad \overline{\psi(E_1)} = \bigcap_n \psi(E_1) U_n.$$

It suffices to show that $U_1 \cap K^\times \prod_{v\nmid p} U_v U_n \subseteq \psi(E_1)U_n$. For any element $xu'u_n \in U_1 \cap K^\times \prod_{v\nmid p} U_v U_n$ where $x \in K^\times$, $u' \in \prod_{v\nmid p} U_v$ and $u_n \in U_n$, we have $x \in E_1$ and for $v \nmid p$, $(xu')_v = 1$. Then $xu'u_n = \psi(x)u_n \in \psi(E_1)U_n$.

The proof of (2) is similar to (1). □

Conjecture 3.6 (Leopoldt Conjecture)**.** $\operatorname{rank}_{\mathbb{Z}} E_1 = \operatorname{rank}_{Z_p} E_1 \otimes_{\mathbb{Z}} \mathbb{Z}_p = \operatorname{rank}_{\mathbb{Z}_p} \overline{\psi(E)}$.

Leopoldt Conjecture is true for abelian number fields.

Let $\delta = \operatorname{rank}_{\mathbb{Z}} E_1 - \operatorname{rank}_{Z_p} E_1 \otimes_{\mathbb{Z}} \mathbb{Z}_p$. Then $\delta \geq 0$ and $\delta = 0$ if Leopoldt Conjecture holds.

Example 3.7. Note that $7, 13$ are independent over $\mathbb{Z}$, but $\log_3 13/\log_3 7 \in \mathbb{Z}_3$, thus $\langle 7, 13\rangle_{\mathbb{Z}_3} = \langle 7\rangle_{\mathbb{Z}_3}$.

Theorem 3.8. *Let $\tilde{K}$ be the composite of all $\mathbb{Z}_p$-extensions of K inside K^{ab}. Then*

$$\operatorname{Gal}(\tilde{K}/K) \cong \mathbb{Z}_p^{r_2+1+\delta}$$

where r_2 is the number of complex embeddings of K and δ is the Leopoldt defection.

Proof. Since $\tilde{K}/K$ is unramified outside p, we first consider the maximal abelian extension F of K unramified outside p. Let H be the maximal unramified abelian extension of K inside F, i.e. the Hilbert class field of K. Write J_k the group of ideles of K and I_K the ideal class group of K. By Class field theory, then

$$\operatorname{Gal}(F/K) = J_K / \overline{K^\times \prod_{v\nmid p} U_v},$$

$$\operatorname{Gal}(H/K) \cong I_K = J_K / K^\times \prod_v U_v.$$

Write $V = \overline{K^\times \prod_{v\nmid p} U_v}$. We have

$$\operatorname{Gal}(F/H) = K^\times \prod_v U_v / V = UV/V \cong U/(U \cap V).$$

Note that $U = U_1 \times$ (finite group), then $U/U \cap V$ and $U_1/(U_1 \cap V)$ differ by a finite group. Note that $U_1 \cong$ (finite group) $\times \mathbb{Z}_p^{[K:\mathbb{Q}]}$, then by Lemma 3.5

$$U_1/U_1 \cap V = U_1/\overline{\psi(E_1)} \cong \text{finite} \times \mathbb{Z}_p^{r_2+1+\delta}.$$

Thus

$$K^\times \prod_v U_v/\overline{K^\times \prod_{v\nmid p} U_v} \cong \text{finite} \times \mathbb{Z}_p^{r_2+1+\delta}$$

and hence

$$\frac{\mathrm{Gal}(F/K)}{\mathbb{Z}_p^{r_2+1+\delta}} = \text{finite}.$$

Suppose the quotient is of order N. Write $J' = \mathrm{Gal}(F/K) = J_k/V$. Then

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

thus $NJ' \cong \mathbb{Z}_p^{r_2+1+\delta}$ as $\mathbb{Z}_p$-modules. Let $J'_N = \{x \in J' \mid Nx = 0\}$, then $J'/J'_N \cong NJ'$. J'_N is a finite group with order $\leq N$: otherwise, there exist distinct elements $x, x' \in J'_N$ with the same image at $J'/\mathbb{Z}_p^{r_2+1+\delta}$, then $x - x' \in \mathbb{Z}_p^{r_2+1+\delta}$ and $N(x - x') = 0$, contradiction!

By definition, the fixed field of J'_N must be $\tilde{K}$ and we get the Theorem. □

Theorem 3.9 (Iwasawa)**.** *Let $K = K_0 \subseteq \cdots \subseteq K_n \subseteq K_\infty$ be a tower of $\mathbb{Z}_p$-extensions. Let p^{e_n} be the exact p-power dividing $h(K_n)$, the order of ideal class group of K_n. Then there exist integers $\lambda \geq 0$, $\mu \geq 0$ and ν such that*

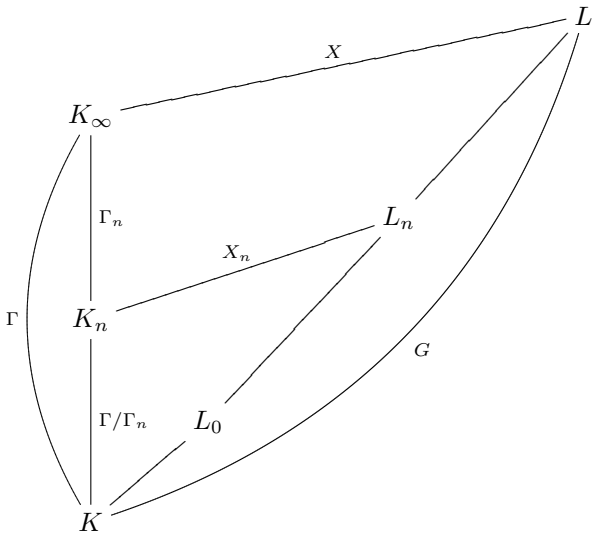
$$e_n = \lambda n + \mu p^n + \nu$$

for n sufficiently large.

Let $\mathrm{Gal}(K_\infty/K) = \Gamma$. We fix a topological generator γ_0 of Γ.

For every $n \in \mathbb{N}$, let L_n be the maximal unramified abelian p-extension of K_n. By the maximality, L_n/K is Galois. Let $L = \bigcup_{n\geq 0} L_n$. Then L/K is also Galois. Write $X_n = \mathrm{Gal}(L_n/K_n)$, $X = \mathrm{Gal}(L/K_\infty)$ and $G = \mathrm{Gal}(L/K)$. We

have the following diagram:



For $n \gg 0$, then all primes which are ramified in K_∞/K are totally ramified in K_∞/K_n. Then for $n \gg 0$, $K_{n+1} \cap L_n = K_n$ and $X_n = \mathrm{Gal}(L_n/K_n) \cong \mathrm{Gal}(L_nK_{n+1}/K_{n+1})$, thus a quotient of X_{n+1}. Moreover $X_n \cong \mathrm{Gal}(L_nK_\infty/K_\infty)$ and

$$\varprojlim X_n = \mathrm{Gal}(\bigcup L_nK_\infty/K_\infty) = \mathrm{Gal}(L/K_\infty) = X.$$

Since X_n is an abelian p-group, there is an Z_p-action on X_n, since $\mathrm{Gal}(L_n/K)$ is Galois, X_n is also equipped with an Γ/Γ_n-action: let $\gamma \in \Gamma/\Gamma_n$, let $\tilde{\gamma}$ be any lifting of γ in $\mathrm{Gal}(L_n/K)$, then for $x \in X_n$, $x^\gamma = \tilde{\gamma}x\tilde{\gamma}^{-1}$ is independent of the choices of the lifting. Then X_n is a $\mathbb{Z}_p[\Gamma_n]$-module. Passing to the limit, we see $X = \varprojlim X_n$ is a compact $\varprojlim \mathbb{Z}_p[\Gamma_n] = \mathbb{Z}_p[[\Gamma]] = \Lambda$-module.

We make the following assumption at first:

(*) All primes ramified in K_∞/K are totally ramified.

Let $\wp_1, \cdots, \wp_s$ be primes of K which ramify in K_∞/K. Fix $\tilde{\wp}_i$ of L lying above $\wp_i$, let $I_i \subseteq G$ be the inertia group. Since L/K_∞ is unramified,

$$I_i \cap X = 1.$$

Since K_∞/K is totally ramified at $\wp_i$, $I_i \cong G/X = \Gamma$, thus

$$G = I_iX = XI_i, \qquad i = 1, \cdots, s.$$

We identify I_1 with Γ. Let σ_i be a topological generator of I_i, then $\sigma_i = a_i\sigma_1$ for some $a_i \in X$.

Lemma 3.10. *With the assumption (*). Then $G' = [G, G] = X^{\gamma_0 - 1} = TX$.*

Proof. Let $a = \alpha x$, $b = \beta y$ for $\alpha, \beta \in \Gamma$ and $x, y \in X$. Then

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

Let $\beta = 1$ and $\alpha = \gamma_0$, then $y^{\gamma_0 - 1} \in G'$, hence $X^{\gamma_0 - 1} \subseteq G'$. On the other hand, write $\beta = \gamma_0^c$ for $c \in \mathbb{Z}_p$, then

$$x^{\alpha(1-\beta)} = x^{\alpha(1-\gamma_0^c)} \in X^{\gamma_0 - 1}$$

since $1 - \gamma_0^c = 1 - (1+T)^c = 1 - \sum \binom{c}{n} T^n \in T\Lambda$. Similarly $y^{\beta(\alpha-1)} \in X^{\gamma_0 - 1}$, hence $G' \subseteq X^{\gamma_0 - 1}$. □

Lemma 3.11. *With the assumption. Let* $Y_0 = \overline{\langle TX, a_2, \cdots, a_s \rangle}$. *Let* $\nu_n = \omega_n/\omega_0 = \frac{(1+T)^{p^n} - 1}{T}$ *and let* $Y_n = \nu_n Y_0$. *Then*

$$X_n \cong X/Y_n$$

for $n \geq 0$.

Proof. For $n = 0$, L_0/K is the maximal unramified abelian p-extension of K, thus the maximal abelian unramified extension inside the Galois extension L/K, by Galois theory, $\mathrm{Gal}(L/L_0)$ is the closed subgroup generated by I_i for $1 \leq i \leq s$ and G', i.e., $\mathrm{Gal}(L/L_0) = I_1 Y_0$ and

$$X_0 = G/I_1 Y_0 = I_1 X / I_1 Y_0 = X/Y_0.$$

For general n, just replace K by K_n, γ_0 by $\gamma_0^{p^n}$ and Y_0 by Y_n. □

Theorem 3.12. *X is a finitely generated torsion Λ-module.*

Proof. First with the assumption. To show that X is finitely generated is equivalent to showing that Y_0 is finitely generated. But $Y/\nu_1 Y$ is finite and $\nu_1 \in (p, T)$, by Nakayama's Lemma, Y is a finitely generated Λ-module. Moreover Y and X are torsion by Theorem 2.14.

In general, suppose all primes ramified in K_∞/K are totally ramified in K_∞/K_e. Replace K by K_e, then for $n \geq e$,

$$X_n = X/\nu_{n,e} Y_e$$

where $\nu_{n,e} = \omega_n/\omega_e$ and Y_e is the corresponding Y_0 for the extension K_∞/K_e. Similarly we can show that Y_e is finitely generated and hence X is finitely generated. □

Lemma 3.13. *Let $M_1 \sim M_2$ be two finitely generated Λ-modules with a given pseudo-isomorphism. If $|M_1/\nu_{n,e} M_1| < \infty$ for all $n \geq e$. Then there exist some constant c and some $n_0 \geq e$, such that*

$$|M_1/\nu_{n,e} M_1| = p^c |M_2/\nu_{n,e} M_2|$$

for $n \geq n_0$.

Proof. Consider the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \nu_{n,e}M_1 & \longrightarrow & M_1 & \longrightarrow & M_1/\nu_{n,e}M_1 & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \phi'_n} & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \phi''_n} & & \\ 0 & \longrightarrow & \nu_{n,e}M_2 & \longrightarrow & M_2 & \longrightarrow & M_2/\nu_{n,e}M_2 & \longrightarrow & 0 \end{array}$$

by the snake lemma, we have an exact sequence

$$0 \to \ker \phi'_n \to \ker \phi \to \ker \phi''_n \to \operatorname{coker} \phi'_n \to \operatorname{coker} \phi \to \operatorname{coker} \phi''_n \to 0.$$

We have

(1) $|\ker \phi'_n| \leq |\ker \phi|$;
(2) $|\operatorname{coker} \phi''_n| \leq |\operatorname{coker} \phi|$;
(3) $|\operatorname{coker} \phi'_n| \leq |\operatorname{coker} \phi|$;
(4) $|\ker \phi''_n| \leq |\ker \phi||\operatorname{coker} \phi|$.

Now for $m \geq n$, we have

(a) $|\ker \phi'_n| \geq |\ker \phi'_m|$;
(b) $|\operatorname{coker} \phi''_n| \leq |\operatorname{coker} \phi''_m|$;
(c) $|\operatorname{coker} \phi'_n| \geq |\operatorname{coker} \phi'_m|$.

(3) and (c) needs a little more explanation, others are easy. For (c), let $\nu_{m,e}y \in \nu_{m,e}M_2$, let $z \in \nu_{n,e}M_2$ be a representative of $\nu_{n,e}y$ in $\operatorname{coker} \phi'_n$. Then $\nu_{n,e}y - z = \phi(\nu_{n,e}x)$ for $\nu_{n,e}x \in \nu_{n,e}M_1$ and $\nu_{m,e}y$ is represented by $\nu_{m,n}z$ in $\operatorname{coker} \phi'_m$. The proof of (3) is similar.

By (2) and (b), the sizes of $\operatorname{coker} \phi''_n$'s are non-decreasing with an upper bound $|\operatorname{coker} \phi|$, when $n \gg 0$, $|\operatorname{coker} \phi''_n|$ will be stable. Similarly the sizes of $\ker \phi'_n$ and $\operatorname{coker} \phi'_n$ will be stable when $n \gg 0$, hence also the size of $\ker \phi''_n$ by the long exact sequence. □

Proof of Theorem 3.9. By Theorem 3.12,

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

where $f_j(T)$'s are irreducible distinguished polynomials.

By the above lemma 3.13, $|X_n| = |X/\nu_{n,e}Y_0|$ is equal to $|E/\nu_{n,e}E|$ up to a bounded factor. Note that

$$|\Lambda/(p^{k_i}, \nu_{n,e}| = p^{k_i(p^n - p^e)} = p^{k_i p^n + c}.$$

We have to compute $|\Lambda/(\nu_{n,e}, f_j(T)^{m_j})|$.

Let g be a distinguished polynomial of degree d. Write $V = \Lambda/(g(T))$. As in the proof of Lemma 2.15, for $n_0 > e$, $p^n \geq d$ and $n \geq n_0$, then $\nu_{n+2,e}V = \frac{\omega_{n+2}(T)}{\omega_{n+1}(T)}(\nu_{n+1,e}V) = p\nu_{n+1,e}V$, and

$$\begin{aligned} |V/\nu_{n+2,e}V| =& |V/pV| \cdot |pV/p\nu_{n+1,e}V| = |V/pV| \cdot |V/\nu_{n+1,e}V| \\ =& p^{d(n-n_0+1)}|V/\nu_{n_0+1,e}V| = p^{nd+c}. \end{aligned}$$

Plug the above result in the case $g = F_j^{m_j}$, we have when $n \gg 0$,

$$|E/\nu_{n,e}E| = p^{\mu p^n + \lambda n + c}$$

with $\mu = \mu(E) = \sum k_i$ and $\lambda = \lambda(E) = \sum m_j \deg F_j$. □

We just showed that the module X is a finitely generated torsion Λ-module. Here we give more examples of Iwasawa modules. Hereafter we consider the following special case: $K = \mathbb{Q}(\zeta_p)$, $K_n = \mathbb{Q}(\zeta_{p^{n+1}})$ and $K_\infty = \mathbb{Q}(\zeta_{p^\infty})$. We let $\Delta = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$. Then $\mathrm{Gal}(K_\infty/\mathbb{Q}) = \Delta \times \Gamma$.

Let E_n be the group of global units of K_n and C_n be the subgroup generated by $\zeta_{p^{n+1}}$ and $\zeta_{p^{n+1}} - 1$ as $\mathrm{Gal}(K_n/\mathbb{Q})$-module, which is called the group of *cyclotomic units*. We recall the map ψ maps E_n into the finitely generated $\mathbb{Z}_p[K_n/\mathbb{Q}]$-module $\prod_{\wp|p} U_{K_{n\wp}}$. Let $\overline{E_n} = \psi(E_n)$ and $\overline{C_n} = \overline{\psi(C_n)}$. Let

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

with the transition maps given by the norm map. Then E_∞ and C_∞ are finitely generated $\mathbb{Z}_p[[\mathrm{Gal}(K_\infty/\mathbb{Q})]] = \Lambda[\Delta]$-modules. For any character $\chi : \Delta \to \mathbb{Z}_p^\times$ and a $\Lambda[\Delta]$-module M, let $M^\chi = e_\chi M$ be the χ-part of M. Then E_∞^χ, C_∞^χ and $(E_\infty/C_\infty)^\chi$ are finitely generated Λ-modules. Recall E_n/C_n are finite for all $n \in \mathbb{N}$, and $\overline{E_n}/\overline{C_n} = \frac{E_\infty/C_\infty}{\omega_n(E/C)}$, then E_∞/C_∞ is Λ-torsion and so is $(E_\infty/C_\infty)^\chi$.

Similarly X is a $\Lambda[\Delta]$-module and X^χ is Λ-torsion. Then the Iwasawa Main Conjecture is the following theorem of Mazur-Wiles:

Theorem 3.14 (Main Conjecture)**.** *If χ is even (i.e., $\chi(-1) = 1$), $\chi \neq 1$, then*

$$(\mathrm{Char}\, X^\chi) = (\mathrm{Char}(E_\infty/C_\infty)^\chi).$$

The main conjecture has another equivalent form. By the proof of Theorem 3.8, we know for any number field K, the maximal abelian pro-p extension of K unramified outside p has $\mathbb{Z}_p$-rank $r_2(K) + 1 + \delta(K)$. In a $\mathbb{Z}_p$-extension K_∞/K, let M_n (resp. M_∞) be the maximal abelian pro-p extension of K_n (resp. K_∞) unramified outside p. Then $K_\infty \subset M_n \subset M_\infty$. Let

$$\mathfrak{X}_n = \mathrm{Gal}(M_n/K_\infty), \quad \mathfrak{X}_\infty = \mathrm{Gal}(M_\infty/K_\infty).$$

Then $\mathfrak{X}_\infty$ is a finitely generated Λ-module since $\mathfrak{X}_n = \mathfrak{X}_\infty/\omega_n\mathfrak{X}_\infty$ is finitely generated as $\mathbb{Z}_p$-module.

Back to the special case. Then $\delta(K) = 0$ and $\mathfrak{X}_\infty$ is of Λ-rank $r_2(K) + 1$, and there is an action of Δ on $\mathfrak{X}_\infty$. One can show that if χ is even, $\mathfrak{X}_\infty^\chi$ is a torsion Λ-module. On the other hand, the p-adic L-function $L_p(s, \chi)$ is given by

$$L_p(1 - s, \chi) = g((1 + T)^s - 1)$$

for some $g(T) \in \Lambda$. Then

Theorem 3.15 (Equivalent form of Main Conjecture)**.** *For χ even, $\chi \neq 1$,*

$$(\mathrm{Char}(\mathfrak{X}_\infty^\chi)) = (g(T)).$$

Chapter 4

Iwasawa theory of elliptic curves

Let K be any number field. For an elliptic curve E defined over K, the theorem of Mordell-Weil claims that the set of K-rational points $E(K)$ of E is a finitely generated abelian group, that is

$$E(K) = \mathbb{Z}^r \oplus T$$

for T the torsion group of $E(K)$ and r the rank of $E(K)$. The study of $r(E(K))$ is a major problem in the arithmetic of elliptic curve. For example, the famous Birch-Swinnerton-Dyer Conjecture claims that this rank equals the order of zeroes of $L(E, s)$, the L-function of E, at $s = 0$, and gives a conjectural relation about the leading terms of $L(E, s)$.

Let F_∞/F be a $\mathbb{Z}_p$-extension and F_n be the n-th layer. Let E be an elliptic curve defined over F. One can ask how $\operatorname{rank} E(F_n)$ varies as n varies. We shall study this question in this chapter. First let us introduce the definitions of Selmer groups and Shafarevich groups.

Let L be a field of characteristic 0 and E be an elliptic curve defined over L. Let $\overline{L}$ be an algebraic closure of L. Let $G_L = \operatorname{Gal}(\overline{L}/L)$. We write $H^i(L, -)$ for the cohomology group $H^i(G_L, -)$.

For the exact sequence

$$0 \longrightarrow E[n] \longrightarrow E \xrightarrow{[n]} E \longrightarrow 0,$$

taking the Galois cohomology, one has

$$0 \longrightarrow \frac{E(L)}{nE(L)} \xrightarrow{\kappa} H^1(L, E[n]) \longrightarrow H^1(L, E)[n] \longrightarrow 0, \tag{4.1}$$

where the Kummer map κ is defined as follows: For $b \in E(L)$, choose $a \in E(\overline{L})$ such that $na = b$, then $\kappa(b)$ is the cohomological class associated to the cocycle

$$\kappa(b)(\sigma) = a^\sigma - a, \ \forall \sigma \in G_L.$$

Let v be a place of L, then we get a local exact sequence analogue to (4.1). If we regard G_{L_v} as a subgroup of G_L, then the restriction maps from $H^1(L,-)$ to $H^1(L_v,-)$ yield the following commutative diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \frac{E(L)}{nE(L)} & \xrightarrow{\kappa} & H^1(L,E[n]) & \longrightarrow & H^1(L,E)[n] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \frac{E(L_v)}{nE(L_v)} & \xrightarrow{\kappa_\eta} & H^1(L_v,E[n]) & \longrightarrow & H^1(L_v,E)[n] & \longrightarrow & 0 \end{array}$$

The *n-th Selmer group* of E over L is the group

$$\mathrm{Sel}_E(L)[n] = \bigcap_v \ker\left(H^1(L,E[n]) \to H^1(L_v, E(\overline{L_v}))[n]\right).$$

The *Shafarevich-Tate group* of E over L is the group

$$Ш_E(L) = \bigcap_v \ker\left(H^1(L,E(\overline{L})) \to H^1(L_\eta, E(\overline{L_v}))\right).$$

Easily by diagram chasing, these two groups and the Mordell-Weil group are related by the following important fundamental exact sequence

$$0 \to E(L)/nE(L) \to \mathrm{Sel}_E(L)[n] \to Ш_E(L)[n] \to 0. \tag{4.2}$$

For every pair (n,m) such that $n \leq m$, we have the following commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \frac{E(L)}{nE(L)} & \longrightarrow & H^1(L,E[n]) & \longrightarrow & H^1(L,E)[n] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \frac{E(L)}{mE(L)} & \longrightarrow & H^1(L,E[m]) & \longrightarrow & H^1(L,E)[m] & \longrightarrow & 0 \end{array}$$

where the vertical maps are natural injections. Furthermore, the local analogue of the above diagram also holds and the restriction maps are compatible with the diagrams. Passing to the limit, we have

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(L)\otimes\mathbb{Q}/\mathbb{Z} & \xrightarrow{\kappa} & H^1(L,E(\overline{L})_{tors}) & \longrightarrow & H^1(L,E) & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & E(L_v)\otimes\mathbb{Q}/\mathbb{Z} & \xrightarrow{\kappa_v} & H^1(L_v,E(\overline{L_v})_{tors}) & \longrightarrow & H^1(L_v,E) & \longrightarrow & 0 \end{array}$$

The *Selmer group* of E over L is the group

$$\mathrm{Sel}_E(L) = \bigcap_v \ker\left(H^1(L,E(\overline{L})_{tors}) \to H^1(L_v, E(\overline{L_v}))\right).$$

One has the exact sequence

$$0 \to E(L)\otimes\mathbb{Q}/\mathbb{Z} \to \mathrm{Sel}_E(L) \to Ш_E(L) \to 0. \tag{4.3}$$

Let p be a prime number, then the p-primary Selmer group is given by

$$\begin{aligned}\mathrm{Sel}_E(L)_p =& \bigcap_v \ker\left(H^1(L, E[p^\infty]) \to H^1(L_v, E(\overline{L_v}))[p^\infty]\right)\\ =& \ker\left(H^1(L, E[p^\infty] \to \prod_v \frac{H^1(L_v, E[p^\infty])}{\mathrm{Im}\ \kappa_v}\right)\end{aligned}$$

and one has an exact sequence

$$0 \to E(L) \otimes \mathbb{Q}_p/\mathbb{Z}_p \to \mathrm{Sel}_E(L)_p \to Ш_E(L)_p \to 0.$$

Put

$$\mathcal{H}_E(L_v) = \frac{H^1(L_v, E[p^\infty])}{\mathrm{Im}\ \kappa_v},$$

Denote by $\mathcal{P}_E(L)$ the product of $\mathcal{H}_E(L_v)$ for all primes v of L. Then

$$\mathrm{Sel}_E(L)_p = \ker\left(H^1(L, E[p^\infty]) \to \mathcal{P}_E(L)\right).$$

Put

$$\mathcal{G}_E(L) = \mathrm{Im}\left(H^1(L, E[p^\infty]) \to \mathcal{P}_E(L)\right),$$

then one has an exact sequence

$$0 \to \mathrm{Sel}_E(L)_p \to H^1(L, E[p^\infty]) \to \mathcal{G}_E(L) \to 0. \tag{4.4}$$

Suppose furthermore that the extension L/F is a Galois extension. Write $G = \mathrm{Gal}(L/F)$. For every intermediate field F' of L/F, write $G(L/F') = \mathrm{Gal}(L/F')$. One has the following commutative diagram with exact rows

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \mathrm{Sel}_E(F')_p & \longrightarrow & H^1(F', E[p^\infty]) & \longrightarrow & \mathcal{G}_E(F') & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle s_{L/F'}} & & \downarrow{\scriptstyle h_{L/F'}} & & \downarrow{\scriptstyle g_{L/F'}} & & \\ 0 & \longrightarrow & \mathrm{Sel}_E(L)_p^{G(L/F')} & \longrightarrow & H^1(L, E[\phi^\infty])^{G(L/F')} & \longrightarrow & \mathcal{G}_E(L)^{G(L/F')} & & \end{array}$$

where the vertical maps $s_{L/F'}$, $h_{L/F'}$ and $g_{L/F'}$ are natural restrictions. The snake lemma then gives the exact sequence:

$$0 \to \ker s_{L/F'} \to \ker h_{L/F'} \to \ker g_{L/F'} \to \mathrm{coker}\, s_{L/F'} \to \mathrm{coker}\, h_{L/F'}. \tag{4.5}$$

Theorem 4.1 (Mazur's Control Theorem)**.** *If F_∞/F is a $\mathbb{Z}_p$-extension, assuming that E has good ordinary reduction at all primes of F lying over p. Let F_n be the n-th layer of the $\mathbb{Z}_p$ extension. Then the natural maps*

$$s_n = s_{F_\infty/F_n} : \mathrm{Sel}_E(F_n)_p \longrightarrow \mathrm{Sel}_E(F_\infty)_p^{\Gamma_n}$$

have finite kernels and cokernels, whose orders are bounded as $n \to \infty$.

We first give some consequences of Mazur's Control Theorem:

Corollary 4.2. *Suppose E is an elliptic curve defined over F such that E has good, ordinary reduction at all primes lying above p. If $E(F)$ and $Ш_E(F)$ are both finite, then $\mathrm{Sel}_E(F_\infty)_p$ is Λ-cotorison. Consequently, $\mathrm{rank}_{\mathbb{Z}} E(F_n)$ is bounded as n varies.*

Proof. Let $X = \mathrm{Hom}(\mathrm{Sel}_E(F_\infty)_p, \mathbb{Q}_p/\mathbb{Z}_p)$. Then X is an Λ-module. Moreover,

$$X/TX = \mathrm{Hom}(\mathrm{Sel}_E(F_\infty)_p^\Gamma, \mathbb{Q}_p/\mathbb{Z}_p)$$

is finite since $\mathrm{Sel}_E(F)_p$ is finite, thus X is a finitely generated Λ-torsion module, hence $\mathrm{Sel}_E(F_\infty)_p$ is Λ-cotorison.

Now $X/X_{\mathbb{Z}_p\text{-tors}} \cong \mathbb{Z}_p^\lambda$, thus $(\mathrm{Sel}_E(F_\infty)_p)_{\mathrm{div}} \cong (\mathbb{Q}_p/\mathbb{Z}_p)^\lambda$ and $(\mathrm{Sel}_E(F_n)_p)_{\mathrm{div}} \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{t_n}$ for some $t_n \le \lambda$. Since $E(F_n) \otimes \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow (\mathrm{Sel}_E(F_n)_p)_{\mathrm{div}}$ through the Kummer map, we have $\mathrm{rank}\, E(F_n) \le \lambda$. □

Corollary 4.3. *Suppose E is an elliptic curve defined over F such that E has good, ordinary reduction at all primes lying above p. If $E(F_n)$ and $Ш_E(F_n)$ are finite for all n, then there exist $\lambda, \mu \ge 0$, depending only on E and F_∞/F, such that*

$$|Ш_E(F_n)_p| = p^{\lambda n + \mu p^n + O(1)}.$$

Proof. From the assumption, $\mathrm{Sel}_E(F_n)_p$ are finite. Let $X = \mathrm{Hom}(\mathrm{Sel}_E(F_\infty)_p, \mathbb{Q}_p/\mathbb{Z}_p)$. Then $|X/\omega_n X| = |\mathrm{Sel}_E(F_\infty)_p^{\Gamma_n}| < \infty$ for all n, thus X is a finitely generated torsion Λ-module. Apply Proposition 2.17, we get $|X/\omega_n X| = p^{\lambda(X)n + \mu(X)p^n + O(1)}$. The result then follows. □

Corollary 4.4. *Suppose E is an elliptic curve defined over F such that E has good, ordinary reduction at all primes lying above p. Let $r = \mathrm{corank}_\Lambda(\mathrm{Sel}_E(F_\infty)_p)$ $= \mathrm{rank}_\Lambda X$, then*

$$\mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_E(F_n)_p = rp^n + O(1).$$

Proof. Let $X = \mathrm{Hom}(\mathrm{Sel}_E(F_\infty)_p, \mathbb{Q}_p/\mathbb{Z}_p)$. Then X is a finitely generated Λ-module, say pseudo-isomorphic to $\Lambda^r \times Y \times Z$ for Y a free $\mathbb{Z}_p$-module of finite rank and Z a torsion group of bounded components. Since $X/\omega_n X$ is the Pontragin dual of $\mathrm{Sel}_E(F_\infty)_p^{\Gamma_n}$, and the size of latter one differs from $|\mathrm{Sel}_E(F_n)_p|$ by a finite bounded value, then

$$\mathrm{corank}_{\mathbb{Z}_p} \mathrm{Sel}_E(F_n)_p = \mathrm{rank}_{\mathbb{Z}_p} X/\omega_n X = rp^n + O(1).$$

□

We shall not give a complete proof of the control theorem here (cf. Greenberg [3]). One has to use the exact sequence

$$0 \to \ker s_n \to \ker h_n \to \ker g_n \to \mathrm{coker}\, s_n \to \mathrm{coker}\, h_n,$$

then to study $\ker s_n$ and $\mathrm{coker}\, s_n$, it suffices to study $\ker h_n$, $\mathrm{coker}\, h_n$ and $\ker g_n$. The first two are easy by the inflation-restrction exact sequence, but the third one needs more analysis. One needs to study the local restriction

$$r_v : \frac{H^1(F_{n,v}, E[p^\infty])}{\mathrm{Im}\ \kappa_v} \longrightarrow \frac{H^1(L_\eta, E[p^\infty])}{\mathrm{Im}\ \kappa_\eta},$$

for every place v. For $v \nmid p$, it is easy. For $v \mid p$, it is more difficult. Here we only prove Theorem 4.6, which will be key to the study of the local maps. One can use Tate's duality theorem for local fields to prove Theorem 4.6, but we give a proof using methods of Iwasawa theory.

We first have:

Lemma 4.5. *Let K be a finite extension over $\mathbb{Q}_p$ and let F/K be a finite abelian extension with Galois group Δ. Let $\chi : \Delta \to \mathbb{Z}_p^*$ be a character of Δ. Let M_F be a maximal abelian p-extension over F. Then M_F/K is Galois and*

$$\operatorname{rank}_{\mathbb{Z}_p} \operatorname{Gal}(M_F/F)^\chi = \begin{cases} [K:\mathbb{Q}_p]+1, & \text{if } \chi = 1, \\ [K:\mathbb{Q}_p], & \text{otherwise.} \end{cases}$$

Proof. M_F/K is Galois since M_F is maximal. By class field theory, the isomorphism

$$\varprojlim_n F^\times/F^{\times p^n} \longrightarrow \operatorname{Gal}(M_F/F)$$

is Δ-equivariant. Recall that

$$F^\times = \langle \pi_F \rangle \times U_F,$$

the p-completion of $\langle \pi_F \rangle$ is a copy of $\mathbb{Z}_p$, with a trivial action of Δ, the p-completion of U_F is isomorphic to $\mathcal{O}_F = \mathcal{O}_K[\Delta] \times \mu_{p^\infty}(F)$. Thus

$$\operatorname{rank}_{\mathbb{Z}_p} \operatorname{Gal}(M_F/F)^\chi = \begin{cases} [K:\mathbb{Q}_p]+1, & \text{if } \chi = 1, \\ [K:\mathbb{Q}_p], & \text{otherwise.} \end{cases}$$

□

Theorem 4.6. *Let K_v be a finite extension of $\mathbb{Q}_p$. Suppose that A is a G_{k_v}-module and that $A \cong \mathbb{Q}_p/\mathbb{Z}_p$ as a group. Then $H^1(K_v, A)$ is a cofinitely generated $\mathbb{Z}_p$-module of $\mathbb{Z}_p$-corank*

$$= [K_v:\mathbb{Q}_p] + \begin{cases} 1, & \text{if } A = \mu_{p^\infty} \text{ or } A = \mathbb{Q}_p/\mathbb{Z}_p; \\ 0, & \text{otherwise.} \end{cases}$$

Proof. G_{K_v} acts on $A \cong \mathbb{Q}_p/\mathbb{Z}_p$ through a character $\psi : G_{K_v} \to \operatorname{Aut}(\mathbb{Q}_p/\mathbb{Z}_p) \cong \mathbb{Z}_P^\times$: for any $g \in G_{K_v}$ and $a \in A$, $ga = \psi(g)a$. If $A = \mathbb{Q}_p/\mathbb{Z}_p$(i.e. $\psi = 1$) or $A = \mu_{p^\infty}$(i.e. ψ is the cyclotomic character), the theorem is easy to check following from Lemma 4.5 and Kummer theory. We suppose now A is not $\mathbb{Q}_p/\mathbb{Z}_p$ or μ_{p^∞}, there are two cases:

(1) Im ψ is finite. Let $H = \ker \psi$, then $G = G_{K_v}/H$ is finite. Let $F = \overline{K_v}^H$ be the field fixed by H, then $\operatorname{Gal}(F/K_v) = G$ is a finite abelian group. We consider the inflation-restriction sequence

$$0 \to H^1(G, A) \to H^1(K_v, A) \to H^1(H, A)^G \to H^2(G, A).$$

If $p \neq 2$, then $\mathbb{Z}_p^\times$ is pro-cyclic, G is cyclic in this case and $|H^1(G,A)| = |H^2(G,A)|$. Suppose G is generated by σ and $\psi(\sigma) = a \in A$, then $H^1(G,A) = {}_NA/(a-1)A$. Note that $a \neq 1$ and $A/(a-1)A$ is finite, so $H^1(G,A)$ and $H^2(G,A)$ are both finite. If $p = 2$, then $G = \operatorname{Im}\psi = \mathbb{Z}/2^n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/2^n\mathbb{Z}$. In each case one can verify that $H^1(G,A)$ and $H^2(G,A)$ are finite. Now H acts trivially on A, then

$$\begin{aligned} H^1(H,A) &= \operatorname{Hom}(H,A) = \operatorname{Hom}(\operatorname{Gal}(\overline{K_v}/F)^{ab}, A) \\ &= \operatorname{Hom}(\operatorname{Gal}(M_F/F), A). \end{aligned}$$

Thus $H^1(H,A)^G = \operatorname{Hom}_G(\operatorname{Gal}(M_F/F), A) = \operatorname{Hom}(\operatorname{Gal}(M_F/F)^\chi, \mathbb{Q}_p/\mathbb{Z}_p)$ where χ is the restriction of ψ at G. The theorem follows from Lemma 4.5.

(2) Im ψ is infinite. Let $F_\infty = \overline{K_v}^{\ker\psi}$ and $G = \operatorname{Gal}(F_\infty/K_v)$, Note that $G \cong \operatorname{Im}\psi \hookrightarrow \mathbb{Z}_p^*$, one can write $G \cong \Delta \times \Gamma$, where Δ is a subgroup of $\mathbb{Z}/(p-1)\mathbb{Z}$ or $\mathbb{Z}/2\mathbb{Z}$ if $p = 2$. Let $F = \mathbb{F}_\infty^\Gamma$. Again we need to consider the inflation-restriction sequence

$$0 \to H^1(G,A) \to H^1(K_v,A) \to H^1(F_\infty,A)^G \to H^2(G,A).$$

First consider the spectral sequence $H^p(\Delta, H^q(\Gamma,A)) \Rightarrow H^{p+q}(G,A)$. For $n = p+q = 2$, as $\mathbb{Z}_p$ has cohomological dimension 1, $H^2(\Gamma,A) = 0$. If prime $p \neq 2$, the order of Δ is prime to p, $H^1(\Gamma,A)$ and A^γ are p-groups, hence $H^1(\Delta, H^1(\Gamma,A)) = 0$ and $H^2(\Delta, A^\Gamma) = 0$, thus $H^2(G,A) = 0$. If $p = 2$ and Δ trivial, again $H^2(G,A) = 0$; if $\Delta = \mathbb{Z}/2\mathbb{Z}$, one can get $H^2(G,A) \cong \mathbb{Z}/2\mathbb{Z}$, but easy to see it is finite. For $n = p+q = 1$, for $\Delta = 1$, easily to see $H^1(G,A) = H^1(\Gamma,A)$ is finite; for prime $p \neq 2$ or $\Delta = 1$, we have $H^1(\Delta, H^0(\Gamma,A)) = 0$ and $H^0(\Delta, H^1(\Gamma,A)) = 0$; for $p = 2$ and $\Delta \cong \mathbb{Z}/2\mathbb{Z} \neq 1$, both are again finite. Thus $H^1(G,A)$ is finite. So we have

$$\operatorname{corank}_{\mathbb{Z}_p} H^1(K_v,A) = \operatorname{corank}_{\mathbb{Z}_p} H^1(F_\infty,A)^G.$$

Let $F_n = F_\infty^{\Gamma_n}$. Fix an algebraic closure $\overline{\mathbb{Q}}_p$ of $\mathbb{Q}_p$. Let M_n be the maximal abelian pro-p extension of F_n and M_∞ be the maximal abelian pro-p extension of F_∞. Let $X = \operatorname{Gal}(M_\infty/F_\infty)$ and $X_n = \operatorname{Gal}(M_n/F_n)$. By Lemma 4.5,

$$\operatorname{Gal}(M_n/F_n)^\chi = [K_v : \mathbb{Q}_p]p^n + \begin{cases} 1, & \chi = 1; \\ 0, & \chi \neq 1. \end{cases}$$

Hence

$$\operatorname{Gal}(M_n/F_\infty)^\chi = [K_v : \mathbb{Q}_p]p^n.$$

Write ψ_Δ and ψ_Γ the restrictions of ψ on Δ and Γ. Then

$$\begin{aligned} \operatorname{corank}_{\mathbb{Z}_p} H^1(K_v,A) &= \operatorname{corank}_{\mathbb{Z}_p} H^1(F_\infty,A)^G = \operatorname{corank}_{\mathbb{Z}_p} \operatorname{Hom}(\operatorname{Gal}(\overline{\mathbb{Q}}_p/F_\infty), A)^G \\ &= \operatorname{corank}_{\mathbb{Z}_p} \operatorname{Hom}_G(X,A) = \operatorname{rank}_{\mathbb{Z}_p} X^\psi \\ &= \operatorname{rank}_{Z_p} (X^{\psi_\Delta})^{\psi_\Gamma} \\ &= \operatorname{rank}_{Z_p} \frac{X^{\psi_\Delta}}{(\gamma_0 - \psi(\gamma_0))} = \operatorname{rank}_{Z_p} \frac{X^{\psi_\Delta}}{T-b} \end{aligned}$$

where $b = \psi(\gamma_0) - 1 \in p\mathbb{Z}_p$. We need to study X, X^{ψ_Δ}. Note for $p \neq 2$, $X^{\psi_\Delta} = e_{\psi_\Delta} X$ for e_χ the idempotent element of χ.

Note that M_n is the maximal abelian sub-extension inside M_∞/F_n, thus

$$\mathrm{Gal}(M_\infty/M_n) = \overline{\mathrm{Gal}(M_\infty/F_n)'}.$$

By the exact sequence

$$1 \longrightarrow X \longrightarrow \mathrm{Gal}(M_\infty/F_n) \longrightarrow \Gamma_n \to 1$$

then any element in $\mathrm{Gal}(M_\infty/F_n)$ is of the form αx for $\alpha = \tilde{\gamma}_0^{p^n m}$ and $x \in X$. Let $\alpha x, \beta y \in \mathrm{Gal}(M_\infty/F_n)$, then

$$\alpha x \beta y x^{-1} \alpha^{-1} y^{-1} \beta^{-1} = x^{\alpha(1-\beta)} y^{(\alpha-1)\beta},$$

we have $\mathrm{Gal}(M_\infty/F_n)' = \omega_n X$. Since X is compact, $\omega_n X$ is closed and $\mathrm{Gal}(M_\infty/M_n) = \omega_n X$ and

$$\mathrm{Gal}(M_n/F_\infty) = X/\omega_n X.$$

By Nakayama Lemma, X is a finitely generated Λ-module of rank $[K_v : \mathbb{Q}_p]|\Delta|$. Moreover, $X/\omega_n X$ is Δ-equivariant,

$$\mathrm{Gal}(M_n/F_\infty)^\chi = (X/\omega_n X)^\chi = X^\chi/\omega_n X^\chi,$$

then X^χ is a finitely generated Λ-module of rank $[K_v : \mathbb{Q}_p]$.

By Class field theoy, since $p^\infty \mid [F_\infty : \mathbb{Q}_p]$, G_{F_∞} has p-adic cohomological dimension 1, hence $H^1(F_\infty, \mathbb{Q}_p/\mathbb{Z}_p)$ is a divisible group. Thus $X = H^1(F_\infty, \mathbb{Q}_p/\mathbb{Z}_p)^\wedge$ is torsion free as $\mathbb{Z}_p$-module. Thus X has no nonzero finite Λ-submodules. Let $Y = X_{\Lambda-tors}$ and $W = X/Y$. Then W is torsion free and

$$0 \longrightarrow \frac{Y}{\omega_n Y} \longrightarrow \frac{X}{\omega_n X} \longrightarrow \frac{W}{\omega_n W} \longrightarrow 0$$

is exact by snake lemma. W has Λ-rank $[K_v : \mathbb{Q}_p]|\Delta|$ and hence $W/\omega_n W$ has $\mathbb{Z}_p$-rank $K_v : \mathbb{Q}_p]|\Delta|p^n$, the same as the $\mathbb{Z}_p$-rank of $X/\omega_n X$. Therefore $Y/\omega_n Y$ is finite and must be isomorphic to a subgroup of $(X/\omega_n X)_{\mathbb{Z}_p-tors} = \mu_{p^\infty}(F_n)$.

On one hand, if $\mu_{p^\infty}(F_\infty)$ is finite, then $Y = \varprojlim_n Y/\omega_n Y$ is finite and hence $Y = 0$. On the other hand, if Y is infinite, then $Y = \varprojlim_n Y/\omega_n Y$ is pro-cyclic and therefore $\cong \mathbb{Z}_p$ as a $\mathbb{Z}_p$-module.

Suppose $W \to \Lambda^r$ is a quasi-isomorphism, then $0 \to W \to \Lambda^r \to B \to 0$ is exact and B is a finite Λ-module, by snake lemma again, $(W/\omega_n W)_{\mathbb{Z}_p-tors}$ is bounded by $\ker(\omega_n : B \to B)$, which equals B when $n \gg 0$. Therefore if $\mu_{p^\infty}(F_n)$ is unbounded, then $Y/\omega_n Y$ is also unbounded and Y is infinite. Hence if $\mu_{p^\infty} \subset F_\infty$, then $Y \cong T_p(\mu_{p^\infty})$.

Now we can finish the proof of the Theorem. We have

$$\mathrm{corank}_{\mathbb{Z}_p} H^1(K_v, A) = \mathrm{rank}_{\mathbb{Z}_p} X^{\psi_\Delta}/(T - b)$$

for $T - b$ a distinguished polynomial of degree 1. As X is quasi-isomorphic to $\Lambda^{[K_v:\mathbb{Q}_p]|\Delta|}$ if $\mu_{p^\infty} \subsetneq F_\infty$, or $T_p(\mu_{p^\infty}) \oplus \Lambda^{[K_v:\mathbb{Q}_p]|\Delta|}$. In the latter case, $\mu_{p^\infty} \subseteq F_\infty$ and ψ_Δ gives the action of Δ on μ_{p^∞}. As we assume ψ is not the cyclotomic character, $T_p(\mu_{p^\infty})^\psi = 0$ and $X^{\psi_\Delta}/(T - b)$ is of $\mathbb{Z}_p$-rank $[K_v : \mathbb{Q}_p]$.

□

Bibliography

[1] J.W.S. Cassels and A. Fröhlich, *Algebraic number theory.* Proceedings of an instructional conference organized by the London Mathematical Society (a NATO Advanced Study Institute) with the support of the Inter national Mathematical Union. Academic Press, 1967.

[2] R. Greenberg, *Iwasawa theory for elliptic curves.* Arithmetic theory of elliptic curves (Cetraro, 1997), 51-144, Lecture Notes in Math.**1716**, Springer, Berlin, 1999.

[3] R. Greenberg, *Introduction to Iwasawa theory for elliptic curves.* Arithmetic algebraic geometry (Park City, UT, 1999), 407–464, IAS/Park City Math. Ser. **9**, Amer. Math. Soc., Providence, RI, 2001.

[4] K. Iwasawa, *On* Γ*-extensions of algebraic number fields.* Bull. Amer. Math. Soc. **65**(1959), 183–226.

[5] K. Iwasawa, *On the* μ*-invariants of* $\mathbb{Z}_\ell$*-extensions.* Number Theory, Algebraic Geometry and Commutative Algebra(in honor of Y. Akizuki). Kinokuniya: Tokyo, 1973, 1-11.

[6] B. Mazur, *Rational points on Abelian varieties in towers of number fields*, Invent. Math., **1**8(1972), 183-266.

[7] H. Matsumura, *Commutative ring theory.* Translated from the Japanese by M. Reid. Cambridge Studies in Advanced Mathematics, **8**. Cambridge University Press, 1986.

[8] J. Neukirch, A. Schmidt and K. Wingberg, *Cohomology of number fields.* Grundlehren der Mathematischen Wissenschaften, **323**. Springer-Verlag, Berlin, 2000.

[9] J. H. Silverman, *The Arithmetic of Elliptic Curves.* GTM **106**, Springer-Verlag, 1986.

[10] L. Washington, *Introduction to cyclotomic fields, 2nd edition.* GTM **83**, Springer-Verlag, 1997.