Introduction To Iwasawa Theory

July 14, 2016

This notes is based on partIII course 'Introduction To Iwasawa Theory' given by Prof.J.H.Coates in 2011. For comments and corrections, please email zc231@cam.ac.uk.

Contents

1 Cyclotomic Extensions

1.1 Cyclotomic Extension of $\mathbb{Q}$

We shall study Z_p-extensions of $\mathbb{Q}$. For $m > 1$, let μ_m denote the group of m-th roots of unity in $\bar{\mathbb{Q}}$. Let $\mathbb{Z}_p = \lim \leftarrow \mathbb{Z}/p^n\mathbb{Z}$ be the p-adic integer and $\mathbb{Z}_p^*$ be the group of units.

Recall from local fields that

$$\mathbb{Z}_p^* = \begin{cases} \mu_{p-1} \times (1 + p\mathbb{Z}_p) & \text{if } p > 2, \\ \mu_2 \times (1 + 4\mathbb{Z}_2) & \text{if } p = 2. \end{cases}$$

Recall that for each n we have an isomorphism

$$Gal(\mathbb{Q}(\mu_{p^n})/\mathbb{Q}) \cong (\mathbb{Z}/p^n\mathbb{Z})^*$$

via

$$(\zeta \mapsto \zeta^{a_n}) \mapsto a_n.$$

Taking inverse limit, we have an isomorphism

$$G = Gal(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \to Aut(\mu_{p^\infty}) = \mathbb{Z}_p^*$$

via

$$\sigma(\zeta) = \zeta^{\chi_p(\sigma)} \ \forall \zeta \in \mu_{p^\infty} \text{ and } \sigma \in G$$

where χ_p is the p-th cyclotomic character. The above is an isomorphism because it is an isomorphism at each finite level and so the image is dense. But it is also closed. Therefore we conclude that

$$Gal(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \cong \Delta \times \Gamma,$$

where Δ is cyclic of order $p-1$ if p is odd and is cyclic of order 2 if $p = 2$, and $\Gamma \cong Z_p$ because $1 + p\mathbb{Z}_p \cong Z_p$ for $p > 2$ and $1 + 4\mathbb{Z}_p \cong Z_2$.

Definition 1.1. *$\mathbb{Q}[p^\infty]$ is the fixed field of Δ. So $Gal(\mathbb{Q}[p^\infty]/\mathbb{Q}) = \Gamma$.*

Lemma 1.2. *The fixed field of Γ is $\mathbb{Q}(\mu_p)$ is p is odd and is $\mathbb{Q}(\mu_4)$ if $p = 2$. Also, $\mathbb{Q}[p^\infty]$ is a real subfield of $\mathbb{Q}(\mu_{p^\infty})$.*

Proof. The group Δ permutes the p-th root of unity when $p > 2$ and performs complex conjugation when $p = 2$. The first result follows by computing the degree of extension and the second result is immediate from this observation. □

Lemma 1.3. *$\mathbb{Q}[p^\infty]$ is the unique Z_p extension of $\mathbb{Q}$.*

Proof. Z_p is a pro-p group and so the extension is a union of finite p extensions. But each abelian extension is cyclotomic by using Class Field Theory. Therefore it is the one we constructed. □

Definition 1.4. *$\mathbb{Q}[p^n]$ is the fixed field of $p^n\Gamma$ in $\mathbb{Q}[p^\infty]$ for each n. The Galois group $Gal(\mathbb{Q}[p^n]/\mathbb{Q}) = \Gamma/p^n\Gamma \cong \mathbb{Z}/p^n\mathbb{Z}$. We call it the* **$n$-th layer** *of $\mathbb{Q}[p^\infty]$.*

Exercise 1.5. *For each $n \geq 1$, $\mathbb{Q}[2^n] = \mathbb{Q}\left(\cos\frac{\pi}{2^{n+1}}\right)$. We can also write $\mathbb{Q}[2^n] = \mathbb{Q}(\alpha_n)$ where $\alpha_1 = \sqrt{2}$ and $\alpha_n = \sqrt{2+\alpha_{n-1}}$ for all $n \geq 2$.*

Lemma 1.6. *p is totally ramified in $\mathbb{Q}[p^n]$ for all $n \geq 1$ and no other prime ramifies.*

Proof. Consider each finite level. □

Definition 1.7. *We denote $h(p^n)$ the class number of $\mathbb{Q}[p^n]$.*

Lemma 1.8. *If $m \leq n$ then $h(p^m)|h(p^n)$.*

Proof. Let $m \leq n$ and let L_n, L_m be the Hilbert Class field for $\mathbb{Q}[p^n], \mathbb{Q}[p^m]$ respectively. Then by Class field theory, $h(p^n) = [L_n : \mathbb{Q}[p^n]]$.

Now $L_m \cap \mathbb{Q}[p^n] = \mathbb{Q}[p^m]$ because $L_m/\mathbb{Q}[p^m]$ is unramified but $\mathbb{Q}[p^n]/\mathbb{Q}[p^m]$ is totally ramified at p. Also, Recall from Galois theory that if $L/K \cap L$ is Galois, then LK/K is Galois and $Gal(LK/K) \cong Gal(L/K \cap L)$. Therefore,

$$Gal(L_m\mathbb{Q}[p^n]/\mathbb{Q}[p^n]) \cong Gal(L_m/\mathbb{Q}[p^m]).$$

But $L_m\mathbb{Q}[p^n]$ is abelian and unramified over $\mathbb{Q}[p^n]$ and so is contained in L_n. Therefore, by tower law we conclude that $h(p^m)\big|h(p^n)$. □

Recall from group theory that:

Lemma 1.9. *Let G be a finite p group, and H be any subgroup of G with $H \neq G$. Then there exists a normal subgroup $G' \subset G$ such that $G' \supset H$ and $|G/G'| = p$.*

Theorem 1.10. *$h(p^n)$ is prime to p for all $n \geq 0$.*

Proof. Let M be the p-Hilbert class field of $\mathbb{Q}[p^n]$. Then $Gal(M/\mathbb{Q}[p^n])$ is the p-primary subgroup of C_n. Suppose $h(p^n)$ is not coprime to p Then $M \neq \mathbb{Q}[p^n]$. By class field theory, M is Galois over $\mathbb{Q}$ and let G be the Galois group of M over $\mathbb{Q}$. Then we know G is a finite p-group. Let $I \subset G$ be the inertia group of $\mathfrak{P}/p$ where $\mathfrak{P}$ is a prime in M above p.

Since $M \neq \mathbb{Q}[p^n]$ we have $I \neq G$. Then by the previous lemma we have some normal subgroup G' such that G' contains I. Let R be the fixed field of G' inside M and $R/\mathbb{Q}$ is Galois. But $I \subset G'$ implies $R/\mathbb{Q}$ is unramified at p, also we know that $M/\mathbb{Q}$ can only ramify at p. Combing these we conclude that $R/\mathbb{Q}$ is unramifed everywhere. So R is contained in the Hilbert class field of $\mathbb{Q}$, which is $\mathbb{Q}$, but by the previous lemma $R/\mathbb{Q}$ has degree p, which gives a contradiction. □

Definition 1.11. *Let $H(p)$ be the set of primes which divide $h(p^n)$ for some n. By the previous theorem, we know p does not belong to $H(p)$.*

Definition 1.12. *Let $\mathbb{Q}[cyc]$ be the composite of $\mathbb{Q}[p^\infty]$ for all prime p. Then the Galois group is*

$$Gal(\mathbb{Q}[cyc]/\mathbb{Q}) = \prod_p \mathbb{Z}_p = \hat{\mathbb{Z}} = \varprojlim_n \mathbb{Z}/n\mathbb{Z}.$$

We define the n-th layer $\mathbb{Q}[n]$ by $Gal(\mathbb{Q}[n]/\mathbb{Q}) = \mathbb{Z}/n\mathbb{Z}$. Note that such field is unique by Chinese remainder theorem. For each n, let $C[n]$ be the ideal class group of $\mathbb{Q}[n]$ and $h(n)$ be the class number.

Lemma 1.13. *If $m|n$ then $h(m)|h(n)$.*

Proof. The proof is similar to Lemma 1.8. We can assume $n = mp^r$ for some r and use an inductive argument. In other words, if it is true for $n = mp^r$ then it is true for all $m|n$. Then run the same argument as in Lemma 1.8. □

1.2 Cyclotomic Extension of Number Fields

Throughout the section, p is a fixed prime number.

Definition 1.14. *Let F be a number field. Define F^{cyc} to be the composite field of $\mathbb{Q}[p^\infty]$ and F inside $\bar{\mathbb{Q}}$. We call F^{cyc} the* **cyclotomic $\mathbb{Z}_p$ extension** *of F.*

Remark 1.15. *The Galois group $Gal(F^{cyc}/F) \cong \mathbb{Z}_p$. To see this, observe that $F \cap \mathbb{Q}[p^\infty]$ is a subfield of $\mathbb{Q}[p^\infty]$ and so is the m-th layer of $\mathbb{Q}[p^\infty]$ for some m. So we have*

$$Gal(\mathbb{Q}[p^\infty]/F \cap \mathbb{Q}[p^\infty]) = p^m\mathbb{Z}_p \cong \mathbb{Z}_p$$

and hence $Gal(F^{cyc}/F) \cong Gal(\mathbb{Q}[p^\infty]/F \cap \mathbb{Q}[p^\infty]) \cong \mathbb{Z}_p$.

Example 1.16. *Let $p = 37$ and $F = \mathbb{Q}(\mu_{37})$. Then $F^{cyc} = F\mathbb{Q}[37^\infty] = \mathbb{Q}(\mu_{37^\infty})$.*

Definition 1.17. *Let F be a number field. Denote F_n the unique subfield of F^{cyc} such that $[F_n : f] = p^n$. Let A_n be the p-primary subgroup of the ideal class group of F_n.*

Recall that if v is a finite place of F, F_v is the completion of F with respect to v, and U_v is the group of unit of the ring of integers, then we have an exact sequence

$$0 \to U_v \to F_v^* \to \mathbb{Z} \to 0.$$

Let k_v be the residue field and q_v be the size of k_v. If p_v is the prime below v, then $q_v = p_v^{f_v}$.

We know $U_v = \mu_{q_v-1} \times U_v^1$, where $U_v^1 = \{u \in U_v : u \equiv 1 \bmod v\}$. U_v^1 is a $\mathbb{Z}_{p_v}$ module. By local class field theory, if F_v^{ab} is the maximal abelian extension of F_v, and I_v is the inertia group of $Gal(F_v^{ab}/F_v)$ then $I_v \cong U_v$.

Lemma 1.18. *Take any prime $p \neq p_v$ then any pro-p quotient of U_v by a closed subgroup must be a finite group of order dividing $q_v - 1$.*

Proof. U_v^1 is pro-p_v and if we want the pro-p quotient then it is zero in the quotient. Hence the quotient is a quotient of μ_{q_v-1} which is a cyclic group of order dividing $q_v - 1$. □

Theorem 1.19. *Let F be a number field and K/F any abelian extension with Galois group of the form*

$$Gal(K/F) \cong \mathbb{Z}_p^d$$

topologically for some integer $d \geq 1$. If v is a prime of F which is ramified in K/F, then v must lie above p.

Proof. Take any v which does not divide p. Let J_v be the inertia group of v in K/F. If we localise at v then by local class field theory we know that if I_v is the inertia group of v in F_v^{ab}/F then $I_v \cong U_v$. But K/F is also abelian so J_v is a quotient of I_v and hence a quotient of U_v.

Now J_v is also pro-p because the Galois group is topologically $\mathbb{Z}_p^d$. Then J_v is a pro-p quotient of U_v, which by the previous lemma J_v is finite of order dividing $q_v - 1$. This implies J_v is trivial because it is a subgroup of $\mathbb{Z}_p^d$ (it has no non-trivial finite subgroup) and so v is unramified. □

2 Iwasawa Module

Throughout the section, Γ is a profinite group which is topologically isomorphic to $\mathbb{Z}_p$. We shall always write Γ multiplicatively.

Definition 2.1. *$\Gamma_n = \Gamma^{p^n}$, which is isomorphic to $p^n\mathbb{Z}_p$. Pick a topologically generator γ of Γ so we have $\Gamma = \gamma^{\mathbb{Z}_p}$. Then Γ_n has generator $\gamma_n = \gamma^{p^n}$.*

Definition 2.2. *For each $n \geq 0$ define $\omega_n = \gamma^{p^n} - 1 \in \mathbb{Z}_p[\Gamma_n] \subset \mathbb{Z}_p[\Gamma]$, which depends on the choice of γ. Further, define*

$$\omega_n W = \{\omega_n w : w \in W\}.$$

This is independent of the choice of γ (easy check). $\omega_n W$ is a Γ submodule of W such that Γ_n acts trivially on $W/\omega_n W$ because

$$\gamma^{p^n} w = w + (\gamma^{p^n} - 1)w = w + \omega_n w.$$

2.1 Construction of Iwasawa Module

Fix a prime p, let F be a number field. Let F_∞/F be a Galois extension. Note that every Galois group is profinite. For example

$$Gal(F/K) = \varprojlim_x Gal(K(x)/K).$$

We also have a Galois extension M_∞ of F such that $M_\infty \supset F_\infty$ and $Gal(M_\infty/F_\infty)$ is abelian and pro-p.

Let $X = Gal(M_\infty/F_\infty)$. It has a natural structure as a $\mathbb{Z}_p$ module. We write X additively. Let $G = Gal(F_\infty/F)$. Then we have an exact sequence

$$0 \to X \to Gal(M_\infty/F) \to G \to 0.$$

Remark 2.3. *There is a continuous left action of G on X. Let $x \in X$ and $g \in G$. We define the action $g \circ x = \tilde{g}x\tilde{g}^{-1}$. It is easy to check this defines an action and it is continuous.*

We now define the **Iwasawa Algebra** of G.

Definition 2.4.

$$\Lambda(G) = \varprojlim_U \mathbb{Z}_p[G/U]$$

where U is open normal. So G/U is finite (each open subgroup of a profinite group has finite index).

Remark 2.5. *$\Lambda(G)$ is a compact $\mathbb{Z}_p$ algebra.*

Lemma 2.6. *Let W be any compact $\mathbb{Z}_p$ module with a continuous left action of G. Then W has a natural structure as a left $\Lambda(G)$ module extending the action of G.*

Proof. We can define

$$W = \varprojlim_U (W)_U$$

where $(W)_U$ is the largest quotient of W on which U acts trivially. Then this induces an action of G/U on $(W)_U$. Hence the result follows by considering the limit. □

Definition 2.7. *For each $n \geq 0$, let M_n be the maximal abelian extension of F_n contained in M_∞. It is clear that*

$$F_\infty \subset M_0 \subset M_1 \subset \cdots M_\infty = \bigcup_{n \geq 0} M_n.$$

Lemma 2.8. *For all $n \geq 0$, we have $Gal(M_\infty/M_n) = \omega_n X$. Hence, by Galois theory, $Gal(M_n/F_\infty) = X/\omega_n X$.*

Proof. Since M_n is the maximal abelian extension of F_n inside M_∞. We must show that $\omega_n X$ is the closure of the commutator subgroup of $Gal(M_\infty/F_n)$. We also have an exact sequence

$$0 \to X \to Gal(M_\infty/F_n) \to \Gamma_n \to 0.$$

Pick a lift τ_n of γ_n in $Gal(M_\infty/F_n)$ (remember that γ_n lies in $Gal(F_\infty/F_n)$). Then each element in $Gal(M_\infty/F_n)$ can be written as αx where $\alpha = \tau_n^a$ and $x \in X$. Then compute the commutator,

$$\begin{aligned}
[\alpha x, \beta y] &= \alpha x \beta y x^{-1} \alpha^{-1} y^{-1} \beta^{-1} \\
&= (\alpha x \alpha^{-1})(\alpha \beta y x^{-1} \alpha^{-1} \beta^{-1})(\beta y^{-1} \beta^{-1}) \\
&= (\alpha \circ x)((\alpha\beta) \circ (yx^{-1}))(\beta \circ y^{-1}) \\
&= \alpha \circ x + (\alpha\beta) \circ (y - x) - \beta \circ y \\
&= (1 - \beta)\alpha \circ x + (\alpha - 1)\beta \circ y,
\end{aligned}$$

where we used the fact that X is abelian so that $\alpha^{-1}\beta^{-1} = \beta^{-1}\alpha^{-1}$ and we wrote X additively.

Now take $\beta = 1$ and $\alpha = \tau_n$ so $\alpha - 1 = \omega_n$. Then we conclude $\omega_n x$ lies in the commutator subgroup as y is arbitrary.

Conversely, for any $\alpha = \tau_n^a - 1$ we have, by Taylor expansion,

$$\alpha - 1 = \tau_n^a - 1 = \sum_{r=1}^{\infty} \binom{a}{r} (\tau_n - 1)^r.$$

So $(\alpha - 1)\beta \circ y$ lies in $\omega_n X$ and the same holds for $(\beta - 1)\alpha \circ x$. Therefore, we conclude that $\omega_n X$ is the commutator subgroup and the result follows. □

Corollary 2.9. *If $Gal(M_0/F_\infty)$ is a finitely generated Z_p module, then X is finitely generated as $\Lambda(\Gamma)$ module.*

Proof. It is a fact that $\Lambda(\Gamma)$ is a complete local ring with maximal ideal $\langle p, \gamma - 1\rangle = \mathfrak{m}$. Recall from Nakayama's lemma that if W is a $\Lambda(\Gamma)$ module, with $W/\mathfrak{m}W$ finite dimensional as $\Lambda(\Gamma)/\mathfrak{m}$ vector space, then W is finitely generated as a $\Lambda(\Gamma)$ module. But

$$X/(\gamma - 1)X = Gal(M_0/F_\infty)$$

and so

$$X/\mathfrak{m}X = Gal(M_0/F_\infty)/pGal(M_0/F_\infty).$$

Hence the result follows by using Nakayama's lemma. □

2.2 Identification of Iwasawa Algebra

Recall that $\Lambda(\Gamma)$ is defined as the inverse limit of $\mathbb{Z}_p[\Gamma/\Gamma_n]$. We will identify this with the ring $R = \mathbb{Z}_p[[T]]$ in this section.

Lemma 2.10. *Let $f(T) \in R$. Then $f(T)$ is a unit in R if and only if $f(0) \in \mathbb{Z}_p^*$.*

Proof. See Local Fields. □

Definition 2.11. *A polynomial $q(T) \in \mathbb{Z}_p[T]$ is distinguished if it is of the form*

$$q(T) = T^n + a_{m-1}T^{m-1} + \cdots + a_0, a_i \in p\mathbb{Z}_p.$$

Proposition 2.12. [Weierstrass Preparation Lemma] *Every power series $f(T) \in R$ can be uniquely written in the form of $f(T) = p^\mu q(T)u(T)$ where $\mu \geq 0$, $q(T)$ is distinguished and $u(T)$ is a unit in R.*

Proof. □

Corollary 2.13. *For each $f(T) \in R$, $f(\alpha) = 0$ for finitely many $\alpha \in \mathbb{Z}_p$.*

Proof. By using Weierstrass preparation lemma, $f(\alpha) = 0$ if and only if $q(\alpha) = 0$. But q is a polynomial so it has finitely many roots. □

Definition 2.14. *For each $n \geq 0$, define $\omega_n(T) = (1+T)^{p^n} - 1$.*

Lemma 2.15. *$\omega_n(T)$ is distinguished for all $n \geq 0$. Moreover, $\omega_n(T) \in \mathfrak{m}^{n+1}$ for all $n \geq 0$.*

Proof. It is clear that $\omega_n(T)$ is distinguished by expanding the bracket. Also,

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

and so

$$\frac{\omega_n(T)}{\omega_{n-1}(T)} \equiv T^{p^{n-1}(p-1)} + \cdots + T^{p^{n-1}} \pmod{p}.$$

Therefore, the quotient lies in $\langle p, T\rangle = \mathfrak{m}$. But $\omega_0(T) = T$ which lies in $\mathfrak{m}$ and so by induction $\omega_n(T) \in \mathfrak{m}^{n+1}$. □

Lemma 2.16.

$$R = \varprojlim_n \mathbb{Z}[T]/\omega_n(T)\mathbb{Z}_p[T].$$

Proof. We shall define $\theta_n : R \longmapsto \mathbb{Z}_p[T]/\omega_n(T)\mathbb{Z}_p[T]$. Let $f = \omega_n g + r$. Note f is a limit of the cauchy sequence in $\mathbb{Z}_p[T]$, and we apply division algorithm to each term in the sequence and take limit. Then define

$$\theta_n(f) = r + \omega_n \mathbb{Z}_p[T].$$

Taking limit we define θ_∞.

It is injective because if the image is 0 then by definition of θ_n, f lies in the idea generated by ω_n for all n, and hence $\mathfrak{m}^{n+1}$ by the previous lemma. But

$$\bigcap_{n\geq 0} \mathfrak{m}^n = 0$$

and so $f = 0$.

Now each θ_n is surjective and hence the image $\theta_\infty(R)$ is dense. But it is also closed, so the map $\theta_\infty(R)$ is surjective. □

Theorem 2.17. *For each choice of topological generator of Γ, there is a unique continuous $\mathbb{Z}_p$ algebra isomorphism*

$$\lambda : \Lambda(\Gamma) \cong R \text{ with } \lambda(\gamma) = 1 + T.$$

Proof. Define for each n,

$$\lambda_n : \mathbb{Z}_p[\Gamma/\Gamma_n] \longmapsto \mathbb{Z}_p[T]/\omega_n(T)\mathbb{Z}_p[T]$$

via

$$\lambda_n(\gamma + \Gamma_n) = 1 + T + \omega_n(T)\mathbb{Z}_p[T].$$

It is clear that this is an isomorphism for each n. Then the result follows from the previous lemma and the definition of $\Lambda(\Gamma)$. □

3 The Asymptotic Formulae

Fix a prime p. Recall that F is a number field, F_∞/F is any $\mathbb{Z}_p$ extension, and

$$\Gamma = Gal(F_\infty/F) \cong \mathbb{Z}_p.$$

F_n is the unique subfield such that $[F_n : F] = p^n$. A_n is the p-primary part of the ideal class group of F_n. In this section, we are going to deduce an asymptotic formulae for the size of A_n for n large enough. **Throughout the section, R will denote the ring $\mathbb{Z}_p[[T]]$.**

Recall from Theorem 1.19 that the only primes which can ramify are those above p. Let v be a prime above p and J_v be the inertia group of v in F_∞/F. So $J_v = \Gamma_{n_v}$ for some $n_v \geq 0$. Further, F_∞/F_{n_v} is totally ramified at all primes above v.

Definition 3.1. *Define n_0 to be the maximum of n_v where v runs over all primes in F which ramify in F_∞/F. Write s to be the number of primes of F_{n_0} which ramify in F_∞.*

Example 3.2. *$F = \mathbb{Q}$ then $F_\infty = \mathbb{Q}^{cyc}$. The prime p is totally ramified and so $n_0 = 0$ and $s = 1$.*

Definition 3.3. *If W is any $\mathbb{Z}_p$ module, write $r_{\mathbb{Z}_p}(W)$ to be the dimension of $W \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ over $\mathbb{Q}_p$.*

Recall from the previous setting that M_∞ is the maximal abelian p-extension of F_∞ and M_n is the maximal abelian extension of F_n contained in M_∞. Let L_n be the maximal unramified abelian p-extension of F_n. We have proved in the previous section that

$$Gal(M_n/F_\infty) = X/\omega_n X, \text{ where } \omega_n = \gamma^{p^n} - 1.$$

Now let $n \geq n_0$. Then each prime which ramify in F_∞/F_n must be totally ramified. Let $w_1, \ldots, w_s$ be primes of F_n which ramify in F_∞.

Lemma 3.4. *Let J_i be the inertia group of w_i in M_n/F_n, then $J_i \cong \mathbb{Z}_p$.*

Proof. w_i is totally ramified in F_∞/F_n and the extension M_n/F_∞ is unramified. Therefore, $J_i \cap X = \{0\}$. Since M_n/F_n is abelian, the inertia subgroup of w_i in F_∞/F_n is the quotient of J_i. Thus, by the above observation, the inertia subgroup of w_i in F_∞/F_n is isomorphic to J_i. But F_∞/F_n is totally ramified at w_i, so

$$J_i \cong \Gamma_n \cong p^n\mathbb{Z}_p \cong \mathbb{Z}_p.$$

□

Theorem 3.5. *X is a finitely generated $\Gamma(\Lambda)$ module and*

$$r_{\mathbb{Z}_p}(X/\omega_n X) \leq s - 1 \ \forall n \geq 0.$$

Proof. L_n is the maximal unramified extension of F_n inside M_n. This is because M_n/F_n is an abelian p-extension. Then

$$Gal(M_n/L_n) = \langle J_1, \ldots, J_s \rangle.$$

Then $r_{\mathbb{Z}_p}(Gal(M_n/L_n)) \leq s$ for all $n \geq n_0$ and so $r_{\mathbb{Z}_p}(Gal(M_n/F_n)) \leq s$ because L_n/F_n is a finite extension. But $Gal(F_\infty/F_n) = \Gamma_n \cong \mathbb{Z}_p$. So we conclude that

$$r_{\mathbb{Z}_p}(Gal(M_n/F_\infty)) \leq s - 1 \ \forall n \geq n_0.$$

In particular, the $\mathbb{Z}_p$ rank of $Gal(M_0/F_\infty)$ is finite and so by Corollary 2.9, X is a finitely generated $\Lambda(\Gamma)$-module. □

Definition 3.6. *Let W be an R-module, and let*

$$t_R(W) = \{w \in W : rw = 0 \text{ for some } r \in R\}.$$

We say W is R-torsion if $W = t_R(W)$ and we say W is R-torsion free if $t_R(W) = \{0\}$.

Theorem 3.7. *Any finitely generated R-module with $r_{\mathbb{Z}_p}(W/\omega_n W)$ bounded as n tends to infinity is always R-torsion.*

Proof. Recall from structure theorem that if W is any finitely generated R-module and W is torsion free then we have an exact sequence

$$0 \to W \to R^d \to D \to 0$$

where $d \geq 0$ and D is a finite R-module.

Let Y be any finitely generated R-module with $r_{\mathbb{Z}_p}(W/\omega_n W)$ bounded, and set $W = Y/t_R(Y)$ so $t_R(W) = 0$. Then we have the above exact sequence. Let f, g, h be the multiplication by ω_n map on W, R^d, D respectively. By snake's lemma, we have

$$0 \to 0 \to 0 \to \ker h \to W/\omega_n W \to (R/\omega_n R)^d \to D/\omega_n D \to 0$$

because W and R^d are both torsion free. Since $D/\omega_n D$ is finite and so we conclude

$$r_{\mathbb{Z}_p}(W/\omega_n W) = d r_{\mathbb{Z}_p}(R/\omega_n R) = dp^n.$$

But this is bounded as n tends to infinity, so we conclude that $d = 0$ which implies $W = 0$. Hence, $Y = t_R(Y)$. □

Corollary 3.8. *X is R-torsion.*

Proof. Straight from Theorem 3.5 and Theorem 3.7. □

Definition 3.9. *For all $m \leq n$ define*

$$v_{m,n} = \frac{\omega_n}{\omega_m} = \frac{(1+T)^{p^n}-1}{(1+T)^{p^m}-1} \in R.$$

Throughout the section, we will write $Y = Gal(M_\infty/L_{n_0}F_\infty)$.

Theorem 3.10. *For all $n \geq n_0$ we have $Gal(L_n/F_n) = X/v_{n_0,n}Y$. In particular, $Gal(M_\infty/L_nF_\infty) = v_{n_0,n}Y$.*

Proof. Let $n \geq n_0$. L_n is the maximal unramified extension of F_n inside M_n and so is the maximal unramified abelian extension of F_n inside M_∞. Therefore, L_n is the fixed field of a closed subgroup H of $Gal(M_\infty/F_n)$ which is generated by the commutator subgroup of $Gal(M_\infty/F_n)$ and the inertia group of primes of F_n which ramify in M_∞. Let $w_1, \ldots, w_s$ be those primes in F_{n_0} which ramify in F_∞.

Let J_i be the inertia subgroup of w_i in M_∞/F_{n_0}. We have $Gal(M_\infty/F_{n_0}) = J_iX = XJ_i$. Since everything is abelian and F_∞/F_{n_0} is totally ramified so $J_i \cap X = \{0\}$ and so the image of J_i in Γ_{n_0} is Γ_{n_0}. Fix a topological generator $\gamma^{p^{n_0}}$ for Γ_{n_0}. Pick $\sigma_i \in J_i$ which maps to $\gamma^{p^{n_0}}$. Since $XJ_1 = XJ_i$ for $i = 2, 3, \ldots, s$. We have $\sigma_i = x_i\sigma_1$ for some x_i, $i = 2, 3, \ldots, s$. Hence L_{n_0} is the fixed field of the group generated by $\omega_{n_0}X, J_1, x_2, \ldots, x_s$. Therefore,

$$\begin{aligned} Gal(L_{n_0}/F_{n_0}) &= Gal(M_\infty/F_{n_0})/Gal(M_\infty/L_{n_0}) \\ &= XJ_1/\langle \omega_{n_0}X, J_1, x_2, \ldots, x_s\rangle \\ &= X/\langle \omega_{n_0}X, x_2, \ldots, x_s\rangle. \end{aligned}$$

Hence

$$Y = Gal(M_\infty/L_{n_0}F_\infty) \cong \langle \omega_{n_0}X, x_2, \ldots, x_s\rangle$$

because $Gal(L_{n_0}F_\infty/F_\infty) = Gal(L_{n_0}/F_{n_0})$.

For $n \geq n_0$, the inertia group of w_i will just be $J_i^{p^{n-n_0}}$ because w_i is totally ramified. Observe that

$$(x\sigma_1)^{k+1} = x(\sigma_1 x\sigma_1^{-1})(\sigma^2 x\sigma_1^{-2})\cdots(\sigma_1^{-k}x\sigma_1^k)\sigma_1^{k+1}$$

Recall that $\alpha x\alpha^{-1} = \alpha \circ x$. Writing X additively we have

$$\begin{aligned} (x\sigma_1)^{k+1} &= ((1+\sigma_1+\cdots+\sigma^k)\circ x)\sigma_1^{k+1} \\ &= \frac{\sigma_1^{k+1}-1}{\sigma_1-1}x\sigma_1^{k+1} \end{aligned}$$

Now recall that γ corresponds to $1+T$ in the identification of $\Lambda(\Gamma)$ with R. Since σ_1 maps to $\gamma^{p^{n_0}}$ so it corresponds to $(1+T)^{p^{n_0}}$. Thus, putting $k+1=p^{n-n_0}$, we have

$$\sigma_i^{p^{n-n_0}} = (x_i\sigma_1)^{p^{n-n_0}} = \frac{\sigma_1^{p^n}-1}{\sigma_1-1} x\sigma_1^{p^{n-n_0}} = (v_{n_0,n}x)\sigma^{p^{n-n_0}}.$$

Hence by a similar argument, we have

$$\begin{aligned} Gal(L_n/F_n) &= XJ_1^{p^{n-n_0}}/\langle \omega_n X, J_1^{p^{n-n_0}}, v_{n_0,n}x_i : i=2,\dots,s\rangle \\ &= X/\langle \omega_n X, v_{n_0,n}x_i : i=2,\dots,s\rangle \\ &= X/v_{n_0,n}Y. \end{aligned}$$

Further, we conclude

$$Gal(M_\infty/L_nF_\infty) = v_{n_0,n}Y \text{ because } Gal(L_n/F_n) = Gal(L_nF_\infty/F_\infty).$$

□

Proposition 3.11. *Let Y be a finitely generated R-module. Then $r_{\mathbb{Z}_p}(Y)$ is finite if and only if Y is R-torsion.*

Proof. Suppose Y is not R-torsion. Then let $W = Y/t_R(Y)$ so $W \neq 0$. Then we have an exact sequence that

$$0 \to W \to R^d \to D \to 0$$

where $d>0$ and D is finite. Then we conclude

$$r_{\mathbb{Z}_p}(W) = dr_{\mathbb{Z}_p}(R) = \infty$$

because $r_{\mathbb{Z}_p}(R)=\infty$ and so $r_{\mathbb{Z}_p}(R)=\infty$.

Conversely assume that Y is R-torsion then we have an exact sequence

$$0 \to E \to Y \to D \to 0$$

where E is a direct sum of the form R/f_iR and D is finite. By Weierstrass preparation lemma, we may write $f = p^\mu q(T)u(T)$ where $\mu \geq 0$, $q(T)$ is distinguished and $u(T)$ is a unit. Observe that we have an injection

$$0 \to R/p^\mu q(T)R \to R/p^\mu R \oplus R/q(T)R$$

with finite cokernel (it is not hard to check the cokernel has size less than p^μ).

If $f = p^\mu$ then $R/p^\mu R \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = 0$. If $f = q(T)$ for some distinguished polynomial $q(T)$ with $\deg q = \lambda$ then

$$R/q(T)R = \mathbb{Z}_p[[T]]/q(T)\mathbb{Z}_p[[T]] \cong \mathbb{Z}_p^\lambda.$$

So $r_{\mathbb{Z}_p}(R/q(T)R) = \lambda$. Therefore, using

$$r_{\mathbb{Z}_p}(\oplus_{i=1}^m R/f_i R) = \sum_{i=1}^m R/f_i R$$

and the above observation, we conclude that

$$r_{\mathbb{Z}_p}(Y) \leq \sum_{i=1}^m \lambda_i < \infty.$$

□

Lemma 3.12. *Let $f(T)$ be a power series in R. Then R/fR has no non-zero finite submodule.*

Proof. Suppose D is a finite submodule of R/fR. Let $d(T) \in D$. If $d \neq 0$, then let $b(T)$ be a lift of $d(T)$ in R and so $b(T) \neq 0$. Consider the maximal ideal $\mathfrak{m} = \langle T, p \rangle$. Since D is finite, so there exists n such that

$$\mathfrak{m}^{n+1} D = \mathfrak{m}^n D.$$

Then by Nakayama's lemma we have $\mathfrak{m}^n D = 0$.

Write $f(T) = p^\mu q(T) u(T)$ by Weierstrass preparation. Since $\mathfrak{m}^n D = 0$, we have $T^n D = 0$ and so $T^n b(T) \in \langle f(T) \rangle$. So $p^\mu \big| b(T)$. Similarly, $p^n b \in \langle f(T) \rangle$ and so $q(T) \big| b$. Therefore, $f(T) \big| b(T)$ and so $d(T) = 0$ which is a contradiction. □

Now we prove the main theorem:

Theorem 3.13. *Let Y be any finitely generated R-torsion module such that there exists an integer such that $Y/v_{n_0,n}Y$ is finite for all $n \geq n_0$. Then there exists integers $\lambda, \mu \geq 0$ and τ, not depending on n such that*

$$|Y/v_{n_0,n}Y| = p^{\lambda_n + \mu p^n + \tau}$$

for all $n \geq n_1$ where n_1 is some integer with $n_1 \geq n_0$.

Proof. We shall firstly discuss the case for $Y = R/fR, f \neq 0$. Suppose $f = p^{\mu}$. Then we claim that

$$|Y/v_{n_1,n}Y| = p^{\mu(p^n - p^{n_1})} = p^{\mu p^n + \tau}.$$

We have

$$Y/v_{n_1,n}Y = \frac{R/p^{\mu}R}{v_{n_1,n}R/p^{\mu}R} \cong R/\langle p^{\mu}, v_{n_1,n}\rangle.$$

But observe that $v_{n_1,n}$ is monic and so

$$R/v_{n_1,n}R \cong \mathbb{Z}_p^{p^{n-n_1}}.$$

So

$$Y/v_{n_1,n}Y = (\mathbb{Z}/p^{\mu}\mathbb{Z})^{p^{n-n_1}}$$

and the claim follows.

Now assume that $f = q(T)$ which is a distinguished polynomial of degree λ. Pick n_1 such that $p^{n_1} \geq \lambda$ and $v_{n_1,n}$ and $q(T)$ are coprime. We claim that for all $n \geq n_1 + 1$ we have

$$|Y/v_{n_1,n}Y| = p^{\lambda n + \tau}$$

for some integer τ. Firstly we check that for such n, $\omega_n \in \langle p^2, q(T)\rangle$. Indeed, apply division algorithm to ω_{n_1} we have

$$\omega_{n_1} = q(T)g(T) + r(T), \deg r(T) < \lambda, g(T) \neq 0.$$

Now reduce this modulo p and use the fact that $\deg r(T) < \lambda$, we conclude that $r(T) \equiv 0 \pmod{p}$. Therefore, $\omega_{n_1} \in \langle q(T), p\rangle$.

Now if $\omega_{n-1} = p\alpha(T) + q(T)\beta(T)$, then

$$\omega_n = (1 + \omega_{n-1})^p - 1 = (1 + p\alpha(T) + q\beta(T))^p - 1 \in \langle p^2, q(T)\rangle.$$

So by using an inductive argument we conclude that $\omega_n \in \langle p^2, q(T)\rangle$.

We have

$$\frac{v_{n_1,n+1}}{v_{n_1,n}} = \frac{\omega_{n+1}}{\omega_n} = (1+T)^{p^n(p-1)} + \cdots + (1+T)^{p^n} + 1.$$

But for each n,

$$(1+T)^{p^n} \equiv 1 + p^2\alpha_n \pmod{q(T)}.$$

So we conclude that

$$\frac{v_{n_1,n+1}}{v_{n_1,n}} = (1 + p^2\alpha_{p-1}) + \cdots + (1 + p^2\alpha_1) + 1 \equiv p + p^2\theta_n \pmod{q(T)}.$$

Further, $p + p^2\theta_n = p(1 + p\theta_n)$ and $1 + p\theta_n$ is a unit in R. Therefore,

$$\frac{v_{n_1,n+1}}{v_{n_1,n}} \equiv p \cdot \text{ unit } \pmod{q(T)}.$$

Using the fact that $q(T)$ and $v_{n_1,n}$ are coprime, we conclude that

$$v_{n_1,n+1}Y = pv_{n_1,n}Y.$$

Therefore,

$$|Y/v_{n_1,n+1}Y| = |Y/pY|\,|pY/pv_{n_1,n}Y| = |Y/pY|\,|Y/v_{n_1,n}Y| = p^{\lambda}\,|Y/v_{n_1,n}Y|\,.$$

Now by induction on n, we have

$$|Y/v_{n_1,n+1}Y| = p^{\lambda(n-n_1-1)}\,|Y/v_{n_1,n_1+1}Y|\,.$$

The result follows by observing that $Y/v_{n_1,n_1+1}Y$ is an R quotient module and so the size must be a power of p.

So we have checked the case when $Y = R/fR$. Now for general case, consider the exact sequence

$$0 \to E \to Y \to D \to 0$$

where E is a direct sum of the form R/fR and D is finite, because Y is assumed to be torsion. So in fact what we checked above is for E. Now let f, g, h be the map of left action by $v_{n_1,n}$ on E, Y, D respectively. Then by snake's lemma, we have

$$0 \to \ker f \to \ker g \to \ker h \to E/v_{n_1,n}E \to Y/v_{n_1,n}Y \to D/v_{n_1,n}D \to D.$$

By previous work, we know $E/v_{n_1,n}E$ is finite. We claim that $\ker f = 0$. This is because if $E/v_{n_1,n}E$ is finite then so is $\ker f$. But by previous lemma we know E has no non-zero finite submodule and so $\ker f = 0$. Then $\ker g$ injects into $\ker h$. But $\ker h$ has size bounded by the size of D, which is finite and so as n increases, $\ker g$ stabilises and is constant for n large enough. Then by using the exact sequence and previous work for E, the result follows by using the fact that the size of D is a power of p because it is a finite R-module. □

Corollary 3.14. *There exists integers $\lambda, \mu \geq 0$ and τ such that*

$$|A_n| = p^{\lambda n + \mu p^n + \tau}$$

where A_n is the p-primary part of the ideal class group of F_n.

Proof. Recall $X = Gal(M_\infty/F_\infty), Y = Gal(M_\infty/L_{n_0}F_\infty)$ and Y is a R-submodule of X. So Y is torsion and finitely generated. By class field theory and Theorem 3.10, for all $n \geq n_0$ we have,

$$A_n \cong Gal(L_n/F_n) = X/v_{n_0,n}Y$$

where L_n is the maximal abelian unramified p extension of F_n. Consider the exact sequence

$$0 \to Y/v_{n_0,n}Y \to X/v_{n_0,n}Y \to X/Y \to 0.$$

So using previous theorem and the fact that $X/Y \cong Gal(L_{n_0}/F_{n_0})$ which is a p group, we conclude

$$|A_n| = |X/Y|\,|Y/v_{n_0,n}Y| = p^{\lambda n+\mu p^n+\tau}.$$

□

Theorem 3.15. *Let F_∞/F be an arbitrary $\mathbb{Z}_p$ extension such that there is a unique prime of F_∞ above p and the prime is totally ramified. Then*

$$X/\omega_n X \cong A_n \ \forall n \geq 0.$$

In particular, $X/\omega_n X$ is finite for all $n \geq 0$.

Proof. By assumption we have $n_0 = 0$. We have

$$Gal(M_n/F_\infty) \cong X/\omega_n X, Gal(L_n/F_n) \cong A_n.$$

Also, $L_n \cap F_\infty = F_n$. Hence,

$$Gal(M_n/F_\infty) = Gal(F_\infty L_n/F_\infty) = Gal(L_n/F_n) = A_n.$$

□

Corollary 3.16. *With the same setting as in previous theorem, $A_0 = 0$ if and only if $A_n = 0$ for all $n \geq 0$.*

Proof. One direction is clear. Now suppose $A_0 = 0$, then $X/\omega_0 X = X/TX = 0$ by previous theorem. Then by Nakayama's lemma, $X = 0$ and so $A_n = 0$ for all $n \geq 0$. □

Definition 3.17. *Let A_∞ be the p-primary part of the ideal class group of F_∞, which is the inductive limit of A_n. We define the inclusion map by $i_n : A_n \mapsto A_\infty$.*

Example 3.18. *If $F = \mathbb{Q}(\mu_{37})$ and $p = 37$ then $F_\infty = F^{cyc} = F(\mu_{37^\infty})$. We have $A_\infty = \mathbb{Q}_{37}/\mathbb{Z}_{37}$.*

The main theorem we are now going to prove is the following,

Theorem 3.19. **[Iwasawa]** *Let F_∞/F be any $\mathbb{Z}_p$ extension. Then the size of $\ker i_n$ is bounded, independent of n.*

To prove this, we need several lemmas.

Theorem 3.20. *For all $n \geq n_0$, we have isomorphism of Γ-module.*

$$\phi_n : A_n \cong Gal(L_n/F_n) \cong X/v_{n_0,n}Y,$$

$$i_{m,n} : A_m \longmapsto A_n, m \leq n,$$
$$N_{m,n} : A_n \longmapsto A_m, m \leq n,$$

where $i_{m,n}$ is the inclusion map in the system of direct limit and $N_{m,n}$ is the norm map. We further define the surjection

$$\theta_{m,n}X/v_{n_0,n}Y \longmapsto X/v_{n_0,m}Y$$

via

$$\theta_{m,n}(x + v_{n_0,n}Y) = x + v_{n_0,m}Y.$$

Finally, define the map

$$\phi_{m,n} : X/v_{n_0,m}Y \longmapsto X/v_{n_0,n}Y$$

by

$$\phi_{m,n}(x + v_{n_0,m}Y) = v_{m,n}x + v_{n_0,n}Y.$$

Then we have two commutative diagrams, which are

$$\phi_n \circ N_{m,n} = \theta_{m,n} \circ \phi_m$$

and

$$\phi_n \circ i_{m,n} = \phi_{m,n} \circ \phi_m.$$

Proof. The proof uses some property of **Artin symbol** so we shall omit the proof. □

Corollary 3.21.

$$X \cong \varprojlim_n A_n$$

as Γ-modules.

Proof. Write

$$M_\infty = \bigcup_{n\geq 0} L_n, F_\infty = \bigcup_{n\geq 0} F_n,$$

then we have

$$X = Gal(M_\infty/F_\infty) = \lim_{\leftarrow} Gal(L_n/F_n) = \lim_{\leftarrow} A_n$$

where the limit commutes with the Galois group by using the previous theorem (the one with norm map). □

Corollary 3.22.

$$A_\infty = \lim_{n\to\infty} X/v_{n_0,n}Y.$$

Proof. Use the second commutative diagram in the previous theorem. □

Now we can prove Iwasawa's theorem (Theorem 3.19).

Proof. Throughout the proof, assume $n \geq m \geq n_0$. The first step is to show that the size of $\ker i_{m,n}$ is bounded, independent of n. Consider the exact sequence

$$0 \to Y/v_{n_0,m}Y \to X/v_{n_0,m}Y \to X/Y \to 0.$$

Consider the maps $\phi_{m,n}$ from $X/v_{n_0,m}Y$ to itself and $v_{m,n}$ from X/Y to itself. Define the map $\eta_{m,n}$ from $Y/v_{n_0,m}Y$ to $Y/v_{n_0,n}$ such that the diagram commutes. Then applying snake's lemma we have

$$0 \to \ker \eta_{m,n} \to \ker \phi_{m,n} \to \ker v_{m,n}.$$

But recall the commutative diagram from Theorem 3.20, we conclude that $\ker i_{m,n} \cong \ker \phi_{m,n}$. Hence we have

$$|\ker i_{m,n}| \leq |\ker \eta_{m,n}| \cdot |X/Y|$$

because $\ker v_{m,n}$ is contained in X/Y.

By structure theory we have

$$0 \to E \to Y \to D \to 0$$

where E is a direct sum of the form R/f_iR and D is finite. By Weierstrass preparation lemma, we can take $f_i = p^\mu$ or q^k where q is an irreducible distinguished polynomial. We claim that the map from $E/v_{n_0,m}E$ to $E/v_{n_0,m}E$ by multiplying by $v_{m,n}$ is injective for all $m \leq n$. It suffices to check this for each f_i individually.

When $f_i = p^\mu, \mu \geq 1$. Then $(v_{m,n}, p^\mu) = 1$ as $v_{m,n}$ is distinguished. Then

$$E = R/p^\mu R \text{ and } E/v_{n_0,m}E = R/\langle p^\mu, v_{n_0,m}\rangle R.$$

If $v_{m,n}(\alpha + \langle p^\mu, v_{n_0,m}\rangle) = 0$ in $E/v_{n_0,n}E$, then

$$v_{m,n}\alpha = p^\mu x + v_{n_0,n}y \text{ for some } x, y \in R.$$

But $v_{m,n}\big|v_{n_0,n}$ and $(v_{m,n}, p^\mu) = 1$ so $v_{m,n}\big|x$. Let $x = v_{m,n}x'$, we have

$$\alpha = p^\mu x' + v_{n_0,m}y$$

and so $\alpha \in \langle p^\mu, v_{n_0,m}\rangle$. Hence $\alpha = 0$ in $E/v_{n_0,m}E$.

When $f_i = q^k, k \geq 1$ where q is an irreducible distinguished polynomial. Let $\lambda = k \deg q$. claim $E/v_{n_0,E}$ is finite. Consider the exact sequence

$$0 \to E \to Y \to D \to 0.$$

We know that $Y/v_{n_0,n}Y$ is finite and D is finite, so the claim follows by using snake's lemma. Since $E/v_{n_0,n}E$ is finite and $E \cong \mathbb{Z}_p^\lambda$. Also, we claim that $(v_{n_0,n}, q) = 1$. Suppose not, then q divides $v_{n_0,n}$ as q is irreducible. Then q^{k-1} will be in the kernel of the map from E to itself given by multiplication by $v_{n_0,n}$. The cokernel is finite and this implies that the kernel should be zero, because R/fR has no non-zero finite submodule.

Similarly, $(v_{m,n}, q) = 1$. Then by the same argument as in the previous case, we deduce that the map

$$v_{m,n} : E/v_{n_0,m}E \longmapsto E/v_{n_0,n}E$$

is injective.

Now consider the exact sequence

$$E/v_{n_0,m}E \to Y/v_{n_0,n}Y \to D/v_{n_0,m}D \to 0.$$

We have $v_{m,n}$ from $E/v_{n_0,m}E$ to $E/v_{n_0,n}E$ and $\eta_{m,n}$ from $Y/v_{n_0,m}Y$ to $Y/v_{n_0,n}$. Define the map $\rho_{m,n}$ from $D/v_{n_0,m}D$ to $D/v_{n_0,n}D$ such that the diagram commutes. The by snake's lemma we conclude that the size of $\ker \eta_{m,n}$ is finite because D is finite. Therefore, recall the previous step that

$$|\ker i_{m,n}| \leq |\ker \eta_{m,n}| \cdot |X/Y|,$$

we conclude that $|\ker i_{m,n}|$ is bounded, independent of n.

Finally, we have

$$\ker i_m = \bigcup_{n \geq m} \ker i_{m,n}$$

and

$$\ker i_{m,n} \subseteq \ker i_{m,n+1}.$$

Use the fact that $\ker i_{m,n}$ has an upper bound independent of n, we conclude that $\ker i_m$ is bounded, independent of n. $\square$

4 Iwasawa Module With Ramification

In this section, we shall modify what we did before so that we allow a certain set of primes which ramify in F_∞.

4.1 Identification of The Galois Group

Definition 4.1. *Let F_∞/F be any $\mathbb{Z}_p$ extension. Let S be the set of primes of F which ramify in F_∞. Recall from Theorem 1.19 that these primes must be above p. Let M_∞ to be the maximal abelian p extension, unramified outside primes above S. Define $X = Gal(M_\infty/F_\infty)$.*

Definition 4.2. *Let J be the idele group of F, which is the restricted direct product of F_v^* with respect to U_v. So it contains element of the form $(x_v)_v$ such that $x_v \in F_v^*, x_v \in U_v$ for all but finitely many v. We embed F into J by diagonal embedding.*

Definition 4.3. *For each set S, define*

$$U_s = \prod_{v \in S} U_v, U_s' = \prod_{v \notin S} U_v, U = U_s \times U_s'.$$

By class field theory, we have an isomorphism

$$J/F^*U \cong C, \text{ where } C \text{ is the ideal class group.}$$

Let $H = \overline{F^*U_s'}$ in the topology of J. Then

$$J/H \cong Gal(m/F)$$

where m is the maximal abelian extension of F unramified outside S.

We have an exact sequence

$$0 \to W \to J/H \to C \to 0$$

where

$$W = F^*U/\overline{F^*U_s'} = U_s\overline{F^*U_s'}/\overline{F^*U_s'} \cong U_s/U_s \cap \overline{F^*U_s'}.$$

For each finite place v, define U_v to be the unit localised at v and

$$U_{v,1} = \{x \in U_v : u \equiv 1 \pmod{v}\}.$$

By Local Fields, we know

$$U_v = \mu_{N_v - 1} \times \mathcal{O}_v$$

where N_v is the size of the residue field. Then we have

$$\mathcal{O}_v \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = F_v, r_{\mathbb{Z}_p}(U_v) = d_v = [F_v : \mathbb{Q}_p].$$

Definition 4.4. *The maximal pro-p quotient of U_s is*

$$U_{s,1} = \prod_{v \in S} U_{v,1}.$$

Theorem 4.5. *$Gal(m/F)$ is a finitely generated $\mathbb{Z}_p$-module, with*

$$r_{\mathbb{Z}_p}(Gal(m/F)) \leq d = \sum_{v \in S} d_v.$$

So $X/\omega_0 X$ is a finitely generated $\mathbb{Z}_p$-module and so X is a finitely generated $\Lambda(\Gamma)$-module.

Proof. We have by definition

$$r_{\mathbb{Z}_p}(U_s) = \sum_{v \in S} d_v.$$

Since the ideal class group is finite and so by using the exact sequence

$$0 \to W \to J/\overline{F^* U_s'} \to C \to 0,$$

we conclude that W and $J/\overline{F^* U_s'}$ have the same $\mathbb{Z}_p$ rank. But

$$J/\overline{F^* U_s'} \cong Gal(m/F), W \cong U_s/U_s \cap \overline{F^* U_s'}.$$

Therefore, we conclude that

$$r_{\mathbb{Z}_p}(Gal(m/F)) = r_{\mathbb{Z}_p}(W) \leq \sum_{v \in S} d_v.$$

The rest follows from the fact m is just m_0 in the previous notation and X is a finitely generated $\Lambda(\Gamma)$-module by using Nakayama's Lemma. □

Definition 4.6. *Let E be the global unit of F, i.e. the set of units in $\mathcal{O}_F$. Define*

$$E_1 = \{x \in E : x \equiv 1 \ (mod\ v) \forall v \in S\}.$$

Further, define the map $\psi_s : E_1 \longmapsto \prod_{v \in S} U_{v,1} = U_{s,1}$ by diagonal embedding.

Theorem 4.7. *In the topology of J, we have*

$$U_{s,1} \cap \overline{F^* U_s'} = \overline{\psi_s(E_1)}.$$

Proof. In the topology of J, $\overline{\psi_s(E_1)}$ means we put 1 at each place v which is not in S. Consider for each $u \in E_1$, we can write $\psi_s(u)$ as $u\frac{\psi_s(u)}{u}$. Since $u \in F^*$ and $\psi_s(u)/u \in U_s'$ because $u \in E_1$, we have $\psi_s(u) \in \overline{F^*U_s'}$. Also it is clear that $\psi_s(u) \in U_{s,1}$. So we have

$$\overline{\psi_s(E_1)} \subset U_{s,1} \cap \overline{F^*U_s'}.$$

Conversely, define

$$U_{s,n} = \prod_{v \in S} U_{v,n}$$

where

$$U_{v,n} = \{u \in E : u \equiv 1 \pmod{v^n}\}.$$

Since $\bigcap_n U_{s,n} = 1$, we have

$$\overline{\psi_s(E_1)} = \bigcap_n \psi_s(E_1)U_{s,n}, \overline{F^*U_s'} = \bigcap_n F^*U_s'U_{s,n}.$$

Let $z \in F^*U_s'U_{s,n} \cap U_{s,1}$ for some n (so it lies in $U_{s,1} \cap \overline{F^*U_s'}$) and write $z = \alpha u' u$, where $\alpha \in F^*, u' \in U_s', u \in U_{s,n}$ and $z \in U_{s,1}$. Then $\alpha u' \in U_{s,1}$ because $U_{s,n} \subset U_{s,1}$.

Now u' has entry 1 at v and $\alpha u' \in U_{s,1}$. This shows that $\alpha \equiv 1 \pmod{v}$ for all $v \in S$. Further, take any place $v \notin S$. The entry of $\alpha u'$ at $v \notin S$ is 1. But u' is a unit at $v \notin S$ so α is also a unit at $v \notin S$. Therefore, we conclude that $\alpha \in E_1$.

Finally, $\alpha u'$ has entry α at each $v \in S$ and is 1 at each $v \notin S$. So we conclude that $\alpha u' \in \psi_s(E_1)$. Therefore, $z \in \psi_s(E_1) \cap U_{s,n}$. Hence,

$$\overline{F^*U_s'} \cap U_{s,1} \subset \overline{\psi_s(E_1)}$$

and so they are the same. □

Theorem 4.8. *The Artin map gives a cononical isomorphism*

$$C \times U_s/\overline{\psi_s(E_1)} \cong Gal(m/F).$$

Proof. Use the exact sequence

$$0 \to W \to Gal(m/F) \to C \to 0$$

with

$$W = U_s/U_s \cap \overline{F^*U_s'} = U_s/\overline{\psi_s(E_1)}$$

by the previous theorem. □

Corollary 4.9.

$$r_{\mathbb{Z}_p}(Gal(m/F)) = \sum_{v \in S} d_v - r_{\mathbb{Z}_p}(\overline{\psi_s(E_1)}).$$

Proof. Clear as $r_{\mathbb{Z}_p}(U_s) = \sum_{v \in S} d_v$. □

4.2 Leopoldt Conjecture

We use the same notation as above. Let $r_1(F)$ and $r_2(F)$ be the number of real and pair of complex embeddings respectively. Then by Dirichlet's Unit Theorem, E_1 has $\mathbb{Z}$ rank $r_1(F) + r_2(F) - 1$. Also, we have

$$r_{\mathbb{Z}_p}(\overline{\psi_s(E_1)}) \leq \sum_{v \in S} d_v$$

as a consequence of Corollary 4.9. Therefore,

$$r_{\mathbb{Z}_p}(\overline{\psi_s(E_1)}) \leq \max\{r_1(F) + r_2(F) - 1, \sum_{v \in S} d_v\}.$$

[**Leopoldt Conjecture**]

$$r_{\mathbb{Z}_p}(\overline{\psi_s(E_1)}) = \max\{r_1(F) + r_2(F) - 1, \sum_{v \in S} d_v\}.$$

Definition 4.10. *The* **Leopoldt discrepancy** *is defined as*

$$\delta_s(F) = r_{\mathbb{Z}}(\psi_s(E_1)) - r_{\mathbb{Z}_p}(\overline{\psi_s(E_1)}).$$

We shall discuss two different cases. The first case is when F is arbitrary, and S contains all primes of F above p. Then, by theory in Local Fields, we have

$$\sum_{v \in S} d_v = [F : \mathbb{Q}] = r_1(F) + 2r_2(F).$$

Theorem 4.11.

$$r_{\mathbb{Z}_p}(Gal(m/F)) = r_2(F) + 1 + \delta_s(F).$$

Proof. Use Corollary 4.9, with

$$\sum_{v \in S} d_v = r_1(F) + 2r_2(F), r_{\mathbb{Z}}(\psi_s(E_1)) = r_1(F) + r_2(F) - 1.$$

□

Now let F_∞ be the composite of all $\mathbb{Z}_p$ extension of F. Clearly $F_\infty \subset m$ because F_∞/F is ableian and unramified outside p (again use Theorem 1.19).

Lemma 4.12. *$Gal(m/F_\infty)$ is torsion.*

Proof. Suppose not, then by using structure theory and fundamental theorem of Galois we can have another $\mathbb{Z}_p$ extension over F, not contained in F_∞. This contradicts the definition of F_∞. □

Corollary 4.13.

$$Gal(F_\infty/F) \cong \mathbb{Z}_p^{r_2(F)+1+\delta_s(F)}.$$

In particular, if $r_2(F) > 0$, then F has infinitely many $\mathbb{Z}_p$ extension. If $r_2(F) = 0$, then Leopoldt conjecture is true if and only if F^{cyc} is the unique $\mathbb{Z}_p$ extension of F.

Proof. Use Theorem 4.11 and the fact that F_∞ is the fixed field of the torsion subgroup. □

Let $\zeta_F(s)$ be the Dedekind zeta function of F, then

Theorem 4.14. *Let p be any prime which divides the denominator of $\zeta_F(1-n)$ for some even $n \geq 0$. Then $\delta_s(F) = 0$ for this p.*

Example 4.15. *$F = \mathbb{Q}(\theta)$ where θ is a root of $x^3 - 6x + 2$. F is real. The denominator of $\zeta_F(-3)$ is $2 \cdot 3 \cdot 5$ and so Leopoldt conjecture holds for $p = 2, 3, 5$.*

Now we discuss the second case. We assume that

$$r_1(F) = 0, \sum_{v \in S} d_v = r_2(F).$$

so $[F : \mathbb{Q}] = 2r_2(F)$.

Theorem 4.16.

$$r_{\mathbb{Z}_p}(Gal(m/F)) = 1 + \delta_s(F).$$

In particular, F has a $\mathbb{Z}_p$ extension, unramified outside S, and this is unique if and only if $\delta_s(F) = 0$.

Proof. Clear by the assumption. □

Now we take $F_\infty = F^{cyc}$. Let S be the set of primes ramified at F_∞ and suppose S contains every prime above p. Let M_∞ be the maximal abelian p-extension of F_∞, unramified outside S. Let M_n be the maximal abelian p-extension of F_n, unramified outside S. Denote $Gal(M_\infty/F_\infty)$ by X. Note the setting is the same as the first case with some more information.

We have shown that X is a finitely generated $\Lambda(\Gamma)$-module and $Gal(M_n/F_\infty) \cong X/\omega_n X$.

Theorem 4.17.

$$r_{\mathbb{Z}_p}(X/\omega_n X) = p^n r_2(F) + \delta_s(F_n),\ \forall n \geq 0.$$

Proof. By Theorem 4.11 and the fact that $r_{\mathbb{Z}_p}(Gal(F_\infty/F_n)) = 1$, we have

$$r_{\mathbb{Z}_p}(Gal(M_n/F_\infty)) = r_2(F_n) + \delta_s(F_n).$$

We check that $r_2(F_n) = p^n r_2(F)$. Indeed, $[F_n : F] = p^n$ by definition. Also, recall that $\mathbb{Q}[p^\infty]$ is a real field. Therefore,

$$r_2(F_n) = r_2(F) \cdot |\text{real embeddings}| = p^n r_2(F).$$

□

Definition 4.18. *Let W be any finitely generated R-module. Write $\mathfrak{R} = Frac(R)$. The R-rank of W is*

$$r_R(W) = dim_{\mathfrak{R}}(W \otimes_R \mathfrak{R}).$$

Lemma 4.19. *Let Y be a finitely generated torsion R-module. Then there exists $\lambda \geq 0$ such that $r_{\mathbb{Z}_p}(Y/\omega_n Y) = \lambda$ for all n large enough.*

Proof. Consider the exact sequence

$$0 \to E \to Y \to D \to 0$$

where E is a direct sum of the form R/fR. Consider the multiplication by ω_n map on each of them. Applying snake's lemma, we have

$$0 \to (E)_{\omega_n} \to (Y)_{\omega_n} \to (D)_{\omega_n} \to E/\omega_n E \to Y/\omega_n Y \to D/\omega_n D \to 0.$$

But D is finite so we have

$$r_{\mathbb{Z}_p}(Y/\omega_n Y) = r_{\mathbb{Z}_p}(E/\omega_n E).$$

As usual, we can assume $f_i = p^\mu$ or $f_i = q$ where q is a distinguished polynomial.

When $f_i = p^\mu$. Then $R/p^\mu R$ is killed by tensoring $\mathbb{Q}_p$ and so the rank is 0 for all n. When $f_i = q$, and $\lambda = \deg q$. Then $E \cong \mathbb{Z}_p^\lambda$. So we have

$$r_{\mathbb{Z}_p}(E/\omega_n E) \leq \lambda\ \forall n.$$

But since λ is constant so it stablises for large n and so it becomes a constant when n gets large. Therefore, the result follows by summing up the constant for each f_i. □

Lemma 4.20. *If $Y = W/t_R(W)$ then*

$$r_{\mathbb{Z}_p}(W/\omega_n W) = r_{\mathbb{Z}_p}(t_R(W)/\omega_n t_R(W)) + r_{\mathbb{Z}_p}(Y/\omega_n Y).$$

Proof. We have the exact sequence

$$0 \to t_R(W) \to W \to Y \to 0.$$

Since Y is torsion free, so multiplication by ω_n on Y is injective. Now consider the multiplication by ω_n map on $t_R(W), W$ and Y, and apply snake's lemma, we have

$$\begin{aligned} 0 \to (t_R(W))_{\omega_n} &\to (W)_{\omega_n} \to (Y)_{\omega_n} = 0 \\ &\to t_R(W)/\omega_n t_R(W) \to W/\omega_n W \to Y/\omega_n Y \to 0. \end{aligned}$$

The result follows by considering the $\mathbb{Z}_p$ rank of the above long exact sequence. □

Lemma 4.21. *Assume Y is any finitely generated R-module with no R-torsion and $r_R(Y) = d \geq 0$. Then*

$$r_{\mathbb{Z}_p}(Y/\omega_n Y) = dp^n, \ \forall n \geq 0.$$

Proof. Y is torsion free so we have an exact sequence

$$0 \to Y \to R^k \to D \to 0$$

where $k \geq 0$, D is finite. By considering the R-rank of the sequence, we conclude that $k = d$.

Since D is finite so we have, by using snake's lemma of multiplication by ω_n,

$$r_{\mathbb{Z}_p}(Y/\omega_n Y) = r_{\mathbb{Z}_p}(R^d/\omega_n R^d).$$

But $R/\omega_n R \cong \mathbb{Z}_p^{p^n}$ because $\deg \omega_n = p^n$. So

$$r_{\mathbb{Z}_p}(Y/\omega_n Y) = dp^n.$$

□

Theorem 4.22. *Let W be any finitely generated R-module, then there exist $d, \lambda, n_1 \geq 0$ such that*

$$r_{\mathbb{Z}_p}(W/\omega_n W) = dp^n + \lambda, \ \forall n \geq n_1.$$

Moreover, $d = r_R(W)$.

Proof. Let $Y = W/t_R(W)$ so it is torsion free. Then

$$r_{\mathbb{Z}_p}(Y/\omega_n Y) = dp^n, \forall n \geq 0$$

by Lemma 4.21. $t_R(W)$ is torsion and so by Lemma 4.19,

$$r_{\mathbb{Z}_p}(t_R(W)/\omega_n t_R(W)) = \lambda$$

for n large enough, where λ is a constant. Then apply Lemma 4.20.

Finally, as in Lemma 4.21, $d = r_R(Y)$. But recall that

$$0 \to t_R(W) \to W \to Y \to 0$$

is exact. So $r_R(Y) = r_R(W)$ because $r_R(t_R(W)) = 0$. Hence, $d = r_R(W)$. □

Corollary 4.23. *X has $\Lambda(\Gamma)$-rank $r_2(F) + \epsilon$, where $\epsilon \geq 0$ and satisfies*

$$\delta_s(F_n) = \epsilon p^n + \lambda$$

for all n large enough.

Proof. We have, by the previous theorem that

$$r_{\mathbb{Z}_p}(X/\omega_n X) = \lambda + dp^n$$

for n large where $d = r_R(X)$. But by Theorem 4.17, we also have

$$r_{\mathbb{Z}_p}(X/\omega_n X) = r_2(F)p^n + \delta_s(F_n).$$

Therefore, we have

$$d = r_2(F) + \frac{\delta_s(F_n) - \lambda}{p^n} = r_2(F) + \epsilon.$$

□

Corollary 4.24. *$\epsilon = 0$ if and only if $\delta_s(F_n) = a$ for all sufficiently large n in which case X has $\Lambda(\Gamma)$-rank $r_2(F)$.*

Lemma 4.25. *Let F be a number field. Assume that $\mu_{p^m} \subset F$ for some $m \geq 1$, and S is the set of primes in F above p. Then F has an unramified extension L with*

$$Gal(L/F) = (\mathbb{Z}/p^m\mathbb{Z})^{\delta_s(F)}$$

where $\delta_s(F)$ is the Leopoldt discrepancy.

Proof. Write δ to be $\delta_s(F)$. Write $E_1 = E_{1,tor} \oplus V_1$ where V_1 is free of rank r as an abelian group. Pick $\eta_1, \ldots, \eta_r$ such that they form a $\mathbb{Z}$ basis for V_1 and they also generate $\overline{\psi_s(V_1)}$ as a $\mathbb{Z}_p$-module.

The maximal number of $\mathbb{Z}_p$ linearly independent elements will be $r - \delta$. In fact (this is a bit sketchy) choose notation so that $\eta_{\delta+1}, \ldots, \eta_r$ are linearly independent $\mathbb{Z}_p$ subset and pretend that they generate $\overline{\psi_s(V_1)}$ as a $\mathbb{Z}_p$-module. Then for $i = 1, \ldots, \delta$, we have

$$\eta_i = \prod_{j>\delta} \eta_j^{\alpha_{ij}}, \alpha_{ij} \in \mathbb{Z}_p.$$

Choose $\beta_{ij} \in \mathbb{Z}$ such that $\beta_{ij} \equiv \alpha_{ij} \pmod{p^m}$. Then define

$$\theta_i = \frac{\eta_i}{\prod_{j>\delta} \eta_j^{\beta_{ij}}}, i = 1, \ldots, \delta.$$

It is clear that $\theta_i \in U_{s,1}^{p^m}$. Now consider for each θ_i, we adjoin the p^m-th root of θ_i, and since μ_{p^m} lies in F, so the extension is Kummer extension (hence cyclic). Denote the extension by L_i and we have $Gal(L_i/F) = \mathbb{Z}/p^m\mathbb{Z}$.

We need to check the extension is unramified. Let v be a prime not above p. The minimal polynomial is $x^{p^m} - \theta_i$, and by standard technique of Local Fields, this is unramified at v not above p. Now take a prime v above p. Since $\theta_i \in U_{s,1}^{p^m}$. So v will split completely, by using the theorem in Local Fields that

$$L \otimes_K K_p \cong \oplus_{P|p} L_P$$

and the fact that μ_{p^m} lies in F (so that $x^{p^m} - \theta_i$ splits completely). Therefore, it is unramified everywhere. Finally, take L to be the composite field of each $L_i, i = 1, \ldots, \delta$. As the composite field of unramified extension is still unramified, so L/F is unramified and it has the correct Galois group. □

Corollary 4.26. *If $F_\infty = F^{cyc}$ and $\mu_{p^m} \in F, m \geq 1$, then $\delta_s(F_n)$ is bounded.*

Proof. By previous Lemma and the asymptotic formulae, we have

$$(p^m)^{|\delta_s(F_n)|} \leq |A_n| = p^{\lambda n + \mu p^n + \tau}.$$

□

Definition 4.27. *Let W be a finitely generated R-torsion module. Define $W(p)$ to be the p-primary submodule of W and $U = W/W(p)$.*

Remark 4.28. *W is torsion if and only if $U \cong \mathbb{Z}_p^\lambda$. This can be checked using the exact sequence*

$$0 \to E \to W \to D \to 0.$$

Lemma 4.29. *Enlarge F so that $\mu_p \subset F$ if p is odd and $\mu_4 \subset F$ if $p = 2$. Further, let $\mu_{p^{n+1}} \in F_n$ and $F_\infty = F^{cyc}$. Let L_∞ be the maximal abelian unramified p extension of F_∞ and $W = Gal(L_\infty/F_\infty)$. We know W is torsion so let $U \cong \mathbb{Z}_p^\lambda$.*

Choose $k \geq 1$ such that $p^k W(p) = 0$. If $n > k$ and $(\mathbb{Z}/p^h\mathbb{Z})^t$ is a quotient of W, then $t \leq \lambda$. Hence W has a quotient isomorphic to $(\mathbb{Z}/p^n\mathbb{Z})^{\delta_s(F_n)}$ for all $n \geq n_0$.

Proof. We have an exact sequence

$$0 \to W(p) \to W \to U \to 0.$$

Consider the multiplication by p^h map and by assumption $p^h W(p) = 0$. Also, it is injective on U. So by snake's lemma, we have

$$(U)_{p^h} = 0 \to W(p)/p^h W(p) = W(p) \to W/p^h W \to (\mathbb{Z}/p^h\mathbb{Z})^\lambda \to 0.$$

Now W has a quotient $(\mathbb{Z}/p^h\mathbb{Z})^t$, so $W/p^h W$ has a such quotient and so $t \leq \lambda$.

Let L_n be maximal abelian unramified p extension of F_n. Then by assumption and Lemma 4.25, $Gal(L_n/F_n)$ has a quotient $(\mathbb{Z}/p^{n+1}\mathbb{Z})^{\delta_s(F_n)}$. Recall that

$$Gal(L_n/F_n) \cong Gal(L_n F_\infty/F_\infty) = W/v_{n_0,n}Y$$

where $Y = Gal(F_\infty L_{n_0}/L_{n_0})$. This shows that W has a quotient isomorphic to $(\mathbb{Z}/p^{n+1}\mathbb{Z})^{\delta_s(F_n)}$ for all n. □

5 Kummer Theory

We will go through Kummer Theory and explain how it helps to study the $\Lambda(\Gamma)$-module X. Throughout the section, assume $\mu_{p^\infty} \subset F_\infty$, $\mu_{p^n} \subset F_n$.

Definition 5.1. *Let F_∞^{ab} be the maximal abelian p extension of F_∞.*

We will define the Kummer pairing,

$$\langle , \rangle : Gal(F_\infty^{ab}/F_\infty) \times F_\infty^* \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \longmapsto \mu_{p^\infty}.$$

For each n, we define

$$\langle , \rangle_n : Gal(F_\infty^{ab}/F_\infty)/p^n Gal(F_\infty^{ab}/F_\infty) \times F_\infty^*/F_\infty^{*p^n} \to \mu_{p^n}$$

by

$$\langle \sigma, \alpha \rangle = \frac{\sigma(z)}{z} \in \mu_{p^n}$$

where $z^{p^n} = \alpha$ for any choice of z. It is easy to see this is well-defined (as $\mu_{p^n} \subset F_n$). Then take the inductive limit, we have $\langle , \rangle$ defined by

$$\langle \sigma, \alpha \otimes \frac{1}{p^n} \bmod \mathbb{Z}_p \rangle = \frac{\sigma(z)}{z}.$$

We shall list the properties of the Kummer pairing.

(1) The Kummer pairing gives an isomorphism

$$\theta : Gal(F_\infty^{ab}/F_\infty) \cong Hom(F_\infty^* \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p, \mu_{p^\infty})$$

given by

$$\theta(\sigma)(a \otimes \frac{1}{p^n} \bmod \mathbb{Z}_p) = \langle \sigma, a \otimes \frac{1}{p^n} \bmod \mathbb{Z}_p \rangle.$$

(2) It also introduces an isomorphism

$$\psi : F_\infty^* \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \cong Hom(Gal(F_\infty^{ab}/F_\infty), \mu_{p^\infty})$$

given by

$$a \otimes \frac{1}{p^n} \bmod \mathbb{Z}_p \mapsto (\sigma \mapsto \frac{\sigma(z)}{z}).$$

(3) Let $\Gamma = Gal(F_\infty/F)$ and $\gamma \in \Gamma$. It is a fact that

$$\langle \gamma \circ \sigma, \gamma(a \otimes \frac{1}{p^n} \bmod \mathbb{Z}_p) \rangle = \gamma \langle \sigma, a \otimes \frac{1}{p^n} \bmod \mathbb{Z}_p \rangle.$$

Hence θ is a Γ-homomorphism.

Let $\tilde{\gamma}$ be a life of γ in $Gal(F_\infty^{ab}/F)$ and recall that the action is given by

$$\gamma \circ \sigma = \tilde{\gamma}\sigma\tilde{\gamma}^{-1}.$$

Let $z^{p^n} = a, a \in F_\infty^*$. We check that $(\tilde{\gamma}z)^{p^n} = \gamma a$. Indeed, let $(\tilde{\gamma}z)^{p^n} = a'$, then

$$\begin{aligned}
\langle \gamma \circ \sigma, a' \otimes \frac{1}{p^n} \bmod \mathbb{Z}_p \rangle &= \frac{(\gamma \circ \sigma)\tilde{\gamma}(z)}{\tilde{\gamma}(z)} \\
&= \frac{(\tilde{\gamma}\sigma\tilde{\gamma}^{-1})\tilde{\gamma}(z)}{\tilde{\gamma}(z)} \\
&= \tilde{\gamma}\left(\frac{\sigma(z)}{z}\right) \\
&= \tilde{\gamma}\langle \sigma, a \otimes \frac{1}{p^n} \bmod \mathbb{Z}_p \rangle.
\end{aligned}$$

Now use property (3), we have $a' = \gamma a$.

Let J_∞ be any extension of F_∞, contained in F_∞^{ab} and $H = Gal(F_\infty^{ab}/J_\infty)$. By duality, we have

$$Gal(J_\infty/F_\infty) = Hom(H^\perp, \mu_{p^\infty})$$

where $H^\perp$ is the orthogonal complement of H in our pairing. Hence

$$H^\perp = \{a \otimes \frac{1}{p^n} \bmod \mathbb{Z}_p : F_\infty(\sqrt[p^n]{a}) \subset J_\infty\}.$$

because $a \otimes \frac{1}{p^n} \bmod \mathbb{Z}_p$ is in $H^\perp$ if and only if

$$1 = \langle h, a \otimes \frac{1}{p^n} \bmod \mathbb{Z}_p \rangle = \frac{h(z)}{z}, \ \forall h \in H.$$

This holds if and only if z is fixed by h for all $h \in H$ and so $z \in J_\infty$.

Definition 5.2. *Let I'_∞ be the free abelian group on finite places of F_∞ which do not divide p. For example, it contains ideal of the form*

$$\prod_{v \nmid p} v^{ord_v(\alpha)} \in I'_\infty.$$

This gives a natural embedding from F_∞^* to I'_∞.

Lemma 5.3. *Let K be a number field and $\mu_{p^m} \subset K$ for some $m \geq 1$. Let $\alpha \in K^*$. Then $K(\sqrt[p^m]{\alpha})/K$ is unramified outside p if and only if $ord_v(\alpha) \equiv 0$ (mod p^m) for all v of K not dividing p.*

Proof. Let $v \nmid p$.Suppose $K(\sqrt[p^m]{\alpha})/K$ is unramified outside p. Let $z = \sqrt[p^m]{\alpha}$. The conjugates of z are of the form $z\zeta_{p^m}^i$, for i prime to p. Let $v = v_1 \dots v_k$, where $v_i \neq v_j$ as the extension is unramified.

If z lies in v then it lies in every v_i. Conversely, if z lies in some v_i, then every conjugate of z lies in v_i because v_i is ideal and the conjugates are just $z\zeta_{p^m}^i$. Now each v_i must contain some conjugate of z since the Galois group acts transitively on v_i. Therefore, each v_i must contain z and hence v contains z. Therefore, z lies in v if and only if z is contained in v_i for each i. This shows that $ord_v(z)$ is an integer and hence

$$ord_v(\alpha) = p^m ord_v(z) \equiv 0 \pmod{p^m}.$$

Conversely, suppose $ord_v(\alpha) \equiv 0 \pmod{p^m}$ for any $v \nmid p$. Consider the field localised at v, $K_v(\sqrt[p^m]{\alpha})/K_v$. Let π be a uniformliser, so $\alpha = \pi^{p^n} u$ where u is a unit and $n \geq m$. Then

$$K_v(\sqrt[p^m]{\alpha}) = K_v(\sqrt[p^m]{u}).$$

Consider the minimal polynomial $x^{p^m} - u$, this is separable and since u is a unit then the extension must be unramified (see Local Fields). □

Definition 5.4. *For each $\alpha \in F_\infty^*$, define the natural embedding*

$$\epsilon_\infty : F_\infty^* \longmapsto I'_\infty \text{ by } \epsilon_\infty(\alpha) = \langle \alpha \rangle'_\infty$$

where $\langle \alpha \rangle'_\infty = \prod_{v \nmid p} v^{ord_v(\alpha)}$.

Corollary 5.5. *If $\alpha \in F_\infty^*$, then $F_\infty(\sqrt[p^n]{\alpha})/F_\infty$ is unramified outside p if and only if $\langle \alpha \rangle'_\infty \in I'^{p^n}_\infty$, if and only if $ord_v(\alpha) \equiv 0 \pmod{p^n}$ for all $v \nmid p$.*

Proof. The second bit is clear because $\langle \alpha \rangle'_\infty \in I'^{p^n}_\infty$ if and only if $ord_v(\alpha) \equiv 0 \pmod{p^n}$ for all $v \nmid p$. Pick $m \geq n-1$ so that $\mu_{p^n} \subset F_m$. Claim that $F_\infty(\sqrt[p^n]{\alpha})/F_\infty$ is unramified outside p if and only if $F_m(\sqrt[p^n]{\alpha})/F_m$ is unramified outside p. Then the result follows by Lemma 5.3, with K replaced by F_m, which is finite over $\mathbb{Q}$.

If $F_m(\sqrt[p^n]{\alpha})/F_m$ is unramified then for any v not above p, we know that the composite field of two unramified extensions is again unramified. Therefore, $F_\infty(\sqrt[p^n]{\alpha})/F_\infty$ is unramified at any v not above p, because F_∞/F_m also ramifies at v above p.

Conversely, suppose $F_\infty(\sqrt[p^n]{\alpha})/F_\infty$ is unramified outside p. Then for any v not above p, by using tower law, the ramification degree of v in $F_\infty(\sqrt[p^n]{\alpha})/F_m$ is 1 and so it is unramified in $F_m(\sqrt[p^n]{\alpha})/F_m$. □

Theorem 5.6. *The subgroup of $F_\infty^* \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p$ corresponding to $Gal(M_\infty/F_\infty)$ in Kummer pairing consists of all elements of the form*

$$\alpha \otimes \frac{1}{p^n} \ mod\ \mathbb{Z}_p \ where\ \langle \alpha \rangle'_\infty \in I'^{p^n}_\infty.$$

Proof. By the discussion before Definition 5.2, we have

$$H^\perp = \{\alpha \otimes \frac{1}{p^n} \bmod \mathbb{Z}_p : F_\infty(\sqrt[p^n]{\alpha}) \subset M_\infty\}.$$

But M_∞ is the maximal abelian p extension of F_∞, unramified outside p. So we want $F_\infty(\sqrt[p^n]{\alpha})$ to be unramified outside p. Now apply the previous corollary. □

Definition 5.7. *Recall the map $\epsilon_\infty : F_\infty^* \longmapsto I'_\infty$. Tensor with $\mathbb{Q}_p/\mathbb{Z}_p$ we have a map*

$$\psi_\infty : F_\infty \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \longmapsto I'_\infty \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p$$

by

$$\psi_\infty(\alpha \otimes \frac{1}{p^n} \ mod\ \mathbb{Z}_p) = \langle \alpha \rangle'_\infty \otimes \frac{1}{p^n} \ mod\ \mathbb{Z}_p.$$

Remark 5.8. *The kernel of ϵ_∞ is E'_∞, the group of units of ring of integers of F_∞ localised at prime above p.*

Lemma 5.9. *The natural map*

$$E'_\infty \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \longmapsto F_\infty^* \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p$$

is injective.

Proof. We have an exact sequence

$$0 \to E'_\infty \to F_\infty^* \to Im\epsilon_\infty \to 0.$$

Note that I'_∞ is written multiplicatively. Take $\alpha \in F_\infty^*$. $\langle \alpha \rangle'_\infty = \prod_{v \nmid p} v^{ord_v(\alpha)}$. So it is clear that the mulitplication by p on $Im\epsilon_\infty$ is injective.

Consider the multiplication by p^n map on each of them. Apply snake's lemma, we have

$$(Im\epsilon_\infty)_{p^n} = 0 \to E'_\infty/p^n E'_\infty \to F_\infty^*/p^n F_\infty^*.$$

Let $n \to \infty$, and since direct limit commutes with exact sequence, we have

$$0 \to E'_\infty \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \to F_\infty^* \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p$$

and so the result follows. □

Lemma 5.10.

$$\ker \psi_\infty = \mathfrak{m}_\infty = \{\alpha \otimes \frac{1}{p^n} \ mod \ \mathbb{Z}_p : \langle\alpha\rangle'_\infty \in I'^{p^n}_\infty\}.$$

Proof.

$$\psi_\infty(\alpha \otimes \frac{1}{p^n} \bmod \mathbb{Z}_p) = \langle\alpha\rangle'_\infty \otimes \frac{1}{p^n} \bmod \mathbb{Z}_p$$

which is 0 if and only if $\langle\alpha\rangle'_\infty \in I'^{p^n}_\infty$. □

Theorem 5.11. *We have isomorphisms*

$$X \cong Hom(\mathfrak{m}_\infty, \mu_{p^\infty}), \mathfrak{m}_\infty \cong Hom(X, \mu_{p^\infty}).$$

Proof. Theorem 5.6 and duality. □

Definition 5.12. *Let A'_∞ be the p-primary subgroup of I'_∞ modulo $Im\epsilon_\infty$. Define the map ρ_∞*

$$\rho_\infty : \mathfrak{m}_\infty \longmapsto A'_\infty \text{ by } \rho_\infty(\alpha \otimes \frac{1}{p^n} \ mod \ \mathbb{Z}_p) = c(a)$$

where $\langle\alpha\rangle'_\infty = a^{p^n}$, and $c(a)$ is the representative of a in the quotient A'_∞. One way to think about A'_∞ is the ideal class group, with the primes above p removed.

Lemma 5.13. *We have an exact sequence of Γ-module,*

$$0 \to E'_\infty \otimes)_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \to \mathfrak{m}_\infty \to A'_\infty \to 0$$

where the map from $\mathfrak{m}_\infty \longmapsto A'_\infty$ is given by ρ_∞.

Proof. We check ρ_∞ is surjective. Pick any $c \in A'_\infty$ with order p^n for some n. Take any representative a of c so that a^{p^n} is principal (principal in the sense of I'_∞). In other words, $a^{p^n} \in Im\epsilon_\infty$. So $a^{p^n} = \langle\alpha\rangle'_\infty$ for some $\alpha \in F^*_\infty$. Then

$$c = \rho_\infty(\alpha \otimes \frac{1}{p^n} \bmod \mathbb{Z}_p).$$

Now suppose $\rho_\infty(\alpha \otimes \frac{1}{p^n} \bmod \mathbb{Z}_p) = 0$. Let $\langle\alpha\rangle'_\infty = a^{p^n}$. Then a is principal, i.e. $a \in Im\epsilon$. So $a = \langle\beta\rangle'_\infty$. Therefore,

$$\langle\alpha\rangle'_\infty = \langle\beta^{p^n}\rangle'_\infty$$

and so

$$\alpha = \beta^{p^n} \cdot c \text{ where } c \in E'_\infty.$$

But $\alpha \otimes \frac{1}{p^n} \bmod \mathbb{Z}_p = c \otimes \frac{1}{p^n} \bmod \mathbb{Z}_p$, because β^{p^n} is killed by tensor with $\frac{1}{p^n}$. So the kernel is indeed, $E'_\infty \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p$. □

Theorem 5.14. *We have a canonical exact sequence*

$$0 \to E_\infty \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \to \mathfrak{m}_\infty \to A_\infty \to 0.$$

Proof. The map from $\mathfrak{m}_\infty$ to A_∞ is defined by τ_∞, as follows: Let $n_0 = n_0(F_\infty/F)$ (see Definition 3.1), $\psi_1(n), \ldots, \psi_s(n)$ be the prime above p for $n \geq n_0$. Note that they are totally ramified in F_∞/F_n. Let I_n be the group generated by all finite primes of F_n. Define, for $r \geq n \geq n_0$,

$$i_{n,r} : I_n \longmapsto I_r \text{ by } i_{n,r}(\psi_j(n)) = \psi_j(r)^{p^{r-n}}.$$

Also, take any $x = \alpha \otimes \frac{1}{p^n} \bmod \mathbb{Z}_p$ in $\mathfrak{m}_\infty$. Let $\langle\alpha\rangle'_\infty = a^{p^n}$. Then define

$$\langle\alpha\rangle_n = a^{p^n} d, \text{ where } d \text{ is divisible only by the primes above } p.$$

But each prime above p are totally ramified for $n \geq n_0$. Suppose $\psi_j(n)$ is a factor of d, and then there exists r_j large enough, so that

$$i_{n,r}(\psi_j(n)) = \psi_j(r)^{p^{r-n}} = I^{p^n}$$

where I is an ideal (so it becomes a p^n-th power for r large enough). Pick r to be the maximal of r_j, and so we have

$$\langle\alpha\rangle_r = b^{p^n} \text{ for some ideal } b.$$

Define $\tau_\infty(x)$ to be $c(b)$, the class of b in A_∞.

Suppose $\tau_\infty(x) = 0$, then there exists $t \geq$ such that the class of $i_{r,t}(b)$ is principal in A_∞. Let $i_{r,t}(b) = \langle\beta\rangle_t, \beta \in F_t^*$. Then

$$\langle\beta^{p^n}\rangle_t = i_{r,t}(b^{p^n}) = i_{r,t}(\langle\alpha\rangle_r) = \langle\alpha\rangle_t.$$

So $\alpha = \beta^{p^n}\epsilon$, where $\epsilon \in E_t$, the group of unit in F_t. Then

$$x = \alpha \otimes \frac{1}{p^n} \bmod \mathbb{Z}_p = \epsilon \otimes \frac{1}{p^n} \bmod \mathbb{Z}_p$$

and so $x \in E_t \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p$. Therefore, we have the correct kernel.

Now let $z \in A_\infty$ and let z be the image of some class c in A_n for some $n \geq n_0$. Suppose c has order p^m. Let b be a representative of c and so b^{p^n} is principal. Let

$$\langle\alpha\rangle_n = b^{p^m}, x = \alpha \otimes \frac{1}{p^n} \bmod \mathbb{Z}_p.$$

Then $\tau_\infty(x)$ is the class of b (pick $r = n$) and so $\tau_\infty)(x) = z$. So τ_∞ is surjective. □

6 Twisting by Roots of Unity

Let F be a number field and p be any prime. Let $G_F = Gal(\bar{F}/F)$. Consider the action of G_F on μ_{p^∞}. Pick any $\sigma \in G_F$. Suppose $\sigma(\zeta_p) = \zeta_p^{a_1}$. Then $\sigma(\zeta_{p^2}) = \zeta_{p^2}^{a_1+a_2p}$ because the $\zeta_p = \zeta_{p^2}^p$. Continue this so we have an infinite sum $a_1 + a_2p + a_3p^2 + \cdots$. Also, if the action is non-trivial then each a_i must be prime to p. Then this gives a p-adic expansion of an element in $\mathbb{Z}_p^*$. So define

$$\chi_F : G_F \longmapsto \mathbb{Z}_p^* \text{ by } \chi_F(\sigma) = a_1 + a_2p + \cdots .$$

Equivalently, we have

$$\sigma(\zeta) = \zeta^{\chi_F(\sigma)}, \forall \zeta \in \mu_{p^\infty}.$$

Definition 6.1. *Define*

$$T_p(\mu) = \varprojlim_n \mu_{p^n} \cong \mathbb{Z}_p$$

and G_F acts on $T_p(\mu)$ by χ_F.

For $n = 0$, let $J(0) = \mathbb{Z}_p$. $J(1) = T_p(\mu)$. For $n > 0$, define

$$J(n) = \underbrace{J(1) \otimes_{\mathbb{Z}_p} \cdots \otimes_{\mathbb{Z}_p} J(1)}_{n \text{ times}}$$

with the action

$$\sigma(x_1 \otimes \cdots \otimes x_n) = \sigma(x_1) \otimes \cdots \otimes \sigma(x_n) = \chi_F(\sigma)^n(x_1 \otimes \cdots \otimes x_n).$$

For $n = -1$, define

$$J(-1) = Hom_{\mathbb{Z}_p}(J(1), \mathbb{Z}_p)$$

with action $\sigma(f)(x) = f(\sigma^{-1}x)$, in other words, G_F acts as χ_F^{-1}. For $n > 0$, define

$$J(-n) = \underbrace{J(-1) \otimes_{\mathbb{Z}_p} \cdots \otimes_{\mathbb{Z}_p} J(-1)}_{n \text{times}}$$

with G_F acts as χ_F^{-n}.

Definition 6.2. *Let W be any $\mathbb{Z}_p$-module, endowed with left action of G_F. For each $n \in \mathbb{Z}$, define*

$$W(n) = W \otimes_{\mathbb{Z}_p} J(n)$$

with G_F action on the left by

$$\sigma(w \otimes t) = \sigma(w) \otimes \sigma(t) = \chi_F(\sigma)^n \sigma(w) \otimes t$$

and we write $\sigma_n(w) = \chi_F(\sigma)^n \sigma(w)$.

Definition 6.3. *Let $\widehat{W} = Hom(W, \mathbb{Q}_p/\mathbb{Z}_p)$. Define the G_F action on $\widehat{W}$ by $(\sigma f)(x) = f(\sigma^{-1}x)$.*

Similarly, for A a discrete p-primary module, define $\widehat{A} = Hom(A, \mathbb{Q}_p/\mathbb{Z}_p)$ with action $(\sigma f)(x) = f(\sigma^{-1}x)$.

It is a fact that

$$\widehat{\widehat{W}} = W, \widehat{\widehat{A}} = A.$$

Lemma 6.4. *For $n \in \mathbb{Z}$, $\widehat{W(n)} = \widehat{W}(-n)$.*

Proof. We have

$$\widehat{W(n)} = Hom(W(n), \mathbb{Q}_p/\mathbb{Z}_p) = Hom(W \otimes_{\mathbb{Z}_p} J(n), \mathbb{Q}_p/\mathbb{Z}_p).$$

Recall that

$$Hom(A \otimes B, C) \cong Hom(A, Hom(B, C)).$$

So we have

$$\begin{aligned} \widehat{W(n)} &= Hom(W, Hom(J(n), \mathbb{Q}_p/\mathbb{Z}_p)) \\ &= Hom(W, \mathbb{Q}_p/\mathbb{Z}_p(-n)) \\ &= Hom(W, \mathbb{Q}_p/\mathbb{Z}_p)(-n). \end{aligned}$$

Note that we have a new action

$$\sigma * w = \chi_F(\sigma)^n \sigma w, w \in W(n)$$

and

$$(\sigma f)(x) = f(\sigma^{-1} * x) = \chi_F(\sigma)^{-n} f(\sigma^{-1}x).$$

Then this and $Hom(W, \mathbb{Q}_p/\mathbb{Z}_p(-n))$ have the same Galois action. □

Now suppose $F_\infty = F(\mu_{p^\infty})$. Then the Galois group is $\Delta \times \Gamma$, where $\Gamma \cong \mathbb{Z}_p$, and $\Delta \cong Gal(F_0/F)$, where

$$F_0 = \begin{cases} F(\mu_p) & \text{if } p \text{ is odd,} \\ F(\mu_4) & \text{if } p = 2. \end{cases}$$

Let M_∞ be the maximal abelian p-extension of F_∞, unramified outside p. Let $X_\infty = Gal(M_\infty/F_\infty)$. Recall the notation that

$$\mathfrak{m}_\infty = \ker\left(F_\infty^* \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \longmapsto I'_\infty \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p\right).$$

Recall that we also have the theorem

$$X_\infty \cong Hom(\mathfrak{m}_\infty, \mu_{p^\infty}).$$

Theorem 6.5. *$X_\infty = \widehat{\mathfrak{m}_\infty}(1)$ and hence $\widehat{X_\infty} = \mathfrak{m}_\infty(-1)$.*

Proof.

$$\begin{aligned} X_\infty &= Hom(\mathfrak{m}_\infty, \mu_{p^\infty}) \\ &= Hom(\mathfrak{m}_\infty, \mathbb{Q}_p/\mathbb{Z}_p(1)) \\ &= Hom(\mathfrak{m}_\infty, \mathbb{Q}_p/\mathbb{Z}_p)(1) \\ &= \widehat{\mathfrak{m}_\infty}(1). \end{aligned}$$

□

Corollary 6.6. *$\widehat{X_\infty(-n)} = \widehat{X_\infty}(n) = \mathfrak{m}_\infty(n-1)$.*

Proof.

$$\widehat{X_\infty}(n) = \mathfrak{m}_\infty(-1)(n) = \mathfrak{m}_\infty(n-1).$$

□

7 Complex Multiplication Fields

$[K : \mathbb{Q}] < \infty$. We say K is totally real if each embedding $\psi : K \longmapsto \mathbb{C}$ has $\psi(K) \subset \mathbb{R}$ and complex if $\psi(K) \not\subset \mathbb{R}$.

Definition 7.1. *We say that K is a CM field, (complex multiplication field) of it is imaginary quadratic extension of a totally real field. We shall denote K^+ be its totally real subfield and define $Gal(K/K^+) = \{1, \tau\}$.*

Example 7.2. *Let F be totally real and $K = F(\mu_{p^n})$ where $n \geq 1$ if $p > 2$ and $n \geq 2$ if $p = 2$. Then K is a CM field (using $e^{i\theta} = \cos\theta + i\sin\theta, \sin\theta = \sqrt{1 - \cos^2\theta}$).*

Lemma 7.3. *Under complex embedding $\psi : K \longmapsto \mathbb{C}$, τ corresponds to the complex conjugation.*

Proof. Let $K = K^+(\sqrt{a})$ and $\tau(\sqrt{a}) = -\sqrt{a}$. But a must be negative because K is not totally real. So $-\sqrt{a} = i\sqrt{a} = \overline{\sqrt{a}}$. □

Theorem 7.4. *Let K be any CM field. If E is the group of units, $\mu(K)$ is the group of roots of unity. and E^+ is the group of units of K^+. Then*

$$[E : \mu(K)E^+] \leq 2.$$

Proof. Define

$$\lambda : E \longmapsto E \text{ by } \lambda(\alpha) = \frac{\alpha}{\tau(\alpha)}.$$

It has the correct image because if $\alpha\beta = 1$, then

$$\frac{\alpha}{\tau(\alpha)}\frac{\beta}{\tau(\beta)} = \frac{\alpha\beta}{\tau(\alpha\beta)} = \frac{1}{\tau(1)} = 1.$$

Let $\psi : K \longmapsto \mathbb{C}$ be any embedding. Then

$$|\psi(\lambda(\alpha))| = |\psi(\alpha)\psi(\tau(\alpha^{-1}))| = 1.$$

To see this, use the previous lemma so that $\tau(\alpha) = \bar{\alpha}$. Thus we conclude that $\lambda(\alpha)$ is a root of unity. This is because the set $\{z \in \mathbb{Z} : |z| = 1\}$ is compact and E is discrete. So the intersection must be finite and so $\lambda(\alpha)$ has finite order. So we can define the map

$$\psi : E \longmapsto \mu(K)/\mu(K)^2 \text{ by } \psi(\alpha) = \lambda(\alpha) + \mu(K)^2.$$

If $\alpha \in \ker\psi$, then $\lambda(\alpha) \in \mu(K)^2$. so $\alpha = \tau)(\alpha)z^2$, where $z \in \mu(K)$. Then $z\tau(z) = 1$ and so

$$\frac{\alpha}{z} = \tau\left(\frac{\alpha}{z}\right).$$

Therefore, $\frac{\alpha}{z} \in E^+$. Hence $\alpha \in E^+\mu(K)$ and so $\ker\psi \subset E^+\mu(K)$.

Conversely, if $\alpha = \epsilon\beta$, where $\epsilon \in E^+, \beta \in \mu(K)$, then

$$\lambda(\alpha) = \frac{\alpha}{\tau(\alpha)} = \frac{\epsilon\beta}{\tau(\epsilon)\tau(\beta)} = \frac{\beta}{\tau(\beta)} = \beta^2$$

because $\tau(\beta) = \bar{\beta} = \beta^{-1}$. So $\ker\psi = E^+\mu(K)$.

Finally, $|\mu(K)/\mu(K)^2| \leq 2$ because $\mu(K)$ is a finite cyclic group. Therefore,

$$|E/E^+\mu(K)| = |E/\ker\psi| \leq |\mu(K)/\mu(K)^2| = 2.$$

□

Corollary 7.5. *For any prime p, then natural map*

$$E^+ \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \longmapsto E \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p$$

is surjective.

Proof. We have an exact sequence

$$0 \to E^+ \to E \to E/E^+ \to 0.$$

Tensor is right exact so we have

$$E^+ \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \to E \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \to (E/E^+) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \to 0.$$

But $E/E^+ \cong E/E^+\mu(K) \cdot E^+\mu(K)/E^+$, which is finite, and so is killed by tensor with $\mathbb{Q}_p/\mathbb{Z}_p$. □

Now let F be a totally real number field. $F_\infty = F(\mu_{p^\infty}), F_0 = F(\mu_p)$ if $p > 2$ and $F_0 = F(\mu_4)$ if $p = 2$. Then all F_n are CM fields. Let M_∞ be the maximal abelian p extension of F_∞, unramified outside p. Let E_n be the group of units of F_n and E_n^* be the group of units of F_n^*.

Definition 7.6. *If β is any J-module, where $J = \{1, \tau\}$. Define*

$$\beta^+ = \{b \in \beta : \tau(b) = b\}, \beta^- = \{b \in \beta : \tau(b) = -b\}.$$

Remark 7.7. *Assume p is odd. If β is also a $\mathbb{Z}_p$-module, then*

$$\beta^+ = \frac{1+\tau}{2}\beta, \beta^- = \frac{1-\tau}{2}\beta.$$

So $\beta = \beta^+ \oplus \beta^-$.

Lemma 7.8.

$$E_\infty \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p)^- = \{0\}.$$

Proof. By Corollary 7.5, we know that

$$(E_\infty \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p)^+ = E_\infty \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p.$$

□

Corollary 7.9. $\mathfrak{m}_\infty^- \cong A_\infty^-$.

Proof. Recall we have a canonical exact sequence

$$0 \to E_\infty \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \to \mathfrak{m}_\infty \to A_\infty \to 0.$$

Take $-$ of the exact sequence and use the previous lemma. □

Theorem 7.10. $\widehat{X_\infty}^+ \cong A_\infty^-(-1)$.

Proof. It is a fact that $\widehat{\beta^+} = \widehat{\beta}^+$. Recall from Theorem 6.5, that $\widehat{X_\infty} = \mathfrak{m}_\infty(-1)$. We have $\widehat{x_\infty}^+ = (m_\infty(-1))^J$. Consider the tensor $\mathfrak{m}_\infty(-1) = \mathfrak{m}_\infty \otimes_{\mathbb{Z}_p} J(-1)$, $J = \{1, \tau\}$ acts on $\mathbb{Z}_p(n)$ by $(-1)^n$. Hence,

$$(\mathfrak{m}(-1))^J = \mathfrak{m}_\infty^-(-1) = A_\infty^-(-1).$$

□

Lemma 7.11. *Assume p is odd. Let R_∞ be the maximal ablian p-extension of F_∞^+, unramified outside p. Then $R_\infty F_\infty$ is the maximal abelian extension of F_∞^+ in M_∞.*

Proof. Let U_∞ be the maximal abelian extension of F_∞^+ in M_∞. Since a composite of abelian extensions is again abelian and $(2, p) = 1$, we have

$$Gal(U_\infty/F_\infty^+) \cong Gal(U_\infty/F_\infty) \times Gal(F_\infty/F_\infty^+) = Gal(U_\infty/F_\infty) \times J.$$

Further, $Gal(U_\infty/F_\infty)$ is the maximal quotient of $Gal(M_\infty/F_\infty)$ which is fixed by J, because J acts on X_∞ by

$$\tau \circ x = \tilde{\tau} x \tilde{\tau}^{-1}$$

where $\tilde{\tau}$ is a lift of τ and so x is fixed if and only if $x\tilde{\tau} = \tilde{\tau}x$. Then $Gal(U_\infty/F_\infty) = X_\infty^+$. Therefore, the fixed field by J, U_∞^J has

$$Gal(U_\infty^J/F_\infty^+) \cong X_\infty^+.$$

Now U_∞^J is also p-extension, abelian over F_∞^+, unramified outside p. To see it is unramified outside p, suppose v ramifies for some v not above p, then it also ramifies in the extension U_∞/F_∞^+. But U_∞/F_∞ is unramified outside p, and so the ramification degree can only be 2. But it is a p-extension and $(2,p)=1$ so the ramification degree cannot be 2, which gives a contradiction. This implies that $U_\infty^J \subset R_\infty$. Thus, $F_\infty U_\infty^J \subset F_\infty R_\infty$.

Finally, $F_\infty U_\infty^J = U_\infty$ because it is a quadratic extension of U_∞^J and both of them are contained in U_∞. So $U_\infty \subset F_\infty R_\infty$. But $F_\infty R_\infty$ is also abelian, so $F_\infty R_\infty \subset U_\infty$ by maximality. Therefore, $F_\infty R_\infty = U_\infty$. □

Theorem 7.12.

$$\widehat{Gal(R_\infty/F_\infty^+)} \cong A_\infty^-(-1)$$

and

$$\widehat{Gal(R_\infty/F_\infty^+)}(-n) = A_\infty^{-1}(n-1).$$

Proof. From the proof of the previous lemma, we see that

$$Gal(R_\infty/F_\infty^+) = Gal(F_\infty R_\infty/F_\infty) \cong X_\infty^+.$$

The later part follows from

$$\widehat{W(n)} = \widehat{W}(-n).$$

□