

Iwasawa's Theorem

MARIOS MAGIOLADITIS

SEMINAR ON IWASAWA THEORY OF ELLIPTIC CURVES

INSTITUTE FOR EXPERIMENTAL MATHEMATICS (IEM)
UNIVERSITY OF DUISBURG-ESSEN
JUNE 2008

Seminar on Iwasawa Theory of Elliptic Curves, Sommersemester 2008.
Organiser: Gabor Wiese.

Lecture **6. Iwasawa's Theorem** was given on the 5th of June 2008 in the Institute for Experimental Mathematics University of Duisburg-Essen, Campus Essen.

Marios Magioladitis

Homepage: <http://www.iem.uni-due.de/~magiolad>

E-mail: magiolad@iem.uni-due.de

References

- [1] Lawrence Washington, *Introduction to Cyclotomic Fields*

Chapter 1

Basic facts

In the following K will always be a number field, p a prime number and \mathbb{Z}_p the additive group of p -adic integers. Moreover, $\Lambda = \mathbb{Z}_p[[T]]$.

We state, without proof, the following results found in §13.2 of [1].

1. $f \in \Lambda \Rightarrow \Lambda/(f)$ is infinite.
2. Λ is a Noetherian ring.
3. (p, T) is the unique maximal ideal of Λ .

Definition 1.1. *The extension K_∞/K is called \mathbb{Z}_p -extension of K if*

$$\text{Gal}(K_\infty/K) \simeq \mathbb{Z}_p.$$

Definition 1.2. *Let Γ be a topological group. We say that γ is a topological generator of Γ if $\langle \gamma \rangle$ is dense in Γ .*

Example 1.3. *Take Γ the multiplicative topological group isomorphic to the additive group \mathbb{Z}_p . Let γ correspond to $1 \in \mathbb{Z}_p$ under the above isomorphism. $\langle 1 \rangle = \mathbb{Z}$ and is dense in \mathbb{Z}_p . Thus, γ is a topological generator of Γ .*

Definition 1.4. *Let G be a topological group. The **commutator subgroup** of G is the closure of*

$$\{aba^{-1}b^{-1} \mid a, b \in G\}$$

Remark 1.5. *Let G a topological group and G' its commutator subgroup. We have that G/G' is abelian.*

Definition 1.6. Let M, M' be two Λ -modules.

We say that M is **pseudo-isomorphic** to M' , written

$$M \sim M',$$

if it exists homomorphism $\phi : M \rightarrow M'$ with $|\ker(\phi)|, |\operatorname{coker}(\phi)| < \infty$ i.e. there is an exact sequence of Λ -modules

$$0 \rightarrow A \rightarrow M \rightarrow M' \rightarrow B \rightarrow 0,$$

with A, B finite Λ -modules.

Remark 1.7. $M \sim M'$ doesn't imply $M' \sim M$ in general.

Remark 1.8. Let M, M' be two fin. generated Λ -torsion Λ -modules then

$$M \sim M' \Leftrightarrow M' \sim M.$$

Theorem 1.9. Let M be a fin. generated Λ -module. Then,

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

where $r, s, t, k_i, m_j \in \mathbb{Z}$ and f_j is distinguished and irreducible.

Proof. Theorem 13.12 of [1] (page 271)

□

Chapter 2

Iwasawa's Theorem

In this chapter we prove the following

Theorem 2.1. *Let K_∞/K be a \mathbb{Z}_p -extension. Let*

$$h(K_n) = p^{e_n} \cdot r$$

where $p \nmid r$. Then there exist integers $\lambda \geq 0$, $\mu \geq 0$, ν all independent of n , and integer n_0 s.t.

$$e_n = \lambda n + \mu p^n + \nu, \forall n \geq n_0$$

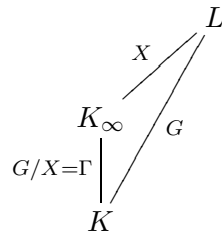
Let $\Gamma = \text{Gal}(K_\infty/K) \simeq \mathbb{Z}_p$ and let γ_0 be a topological generator of Γ . Let L_n be the maximal unramified abelian p -extension of K_n and $L := \cup L_n$. Let $X_n := \text{Gal}(L_n/K_n)$ and $X := \text{Gal}(L/K_\infty)$. Let $G := \text{Gal}(L/K)$.

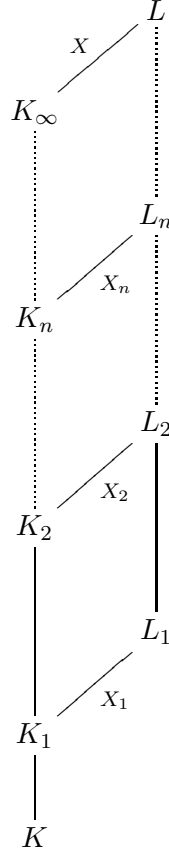
Remark 2.2. $X_n \simeq A_n = p$ -Sylow of the ideal class group of K_n .

If $h(K_n) = p^{e_n} \cdot r$, where $p \nmid r$ then

$$|X_n| = p^{e_n}.$$

We have the following diagrams.





Assumption. All primes which are ramified in K_∞/K are totally ramified.

All proofs are done under this assumption. In [1] it is shown that this assumption can easily be removed.

Let $\gamma \in \Gamma$ and $x \in X$. Then γ acts on x by

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

where $\tilde{\gamma}$ is an extension of γ to G .

The polynomial $1 + T \in \Lambda$ acts as $\gamma_0 \in \Gamma$.

Let p_1, \dots, p_s the primes which ramify in K_∞/K and fix a prime \tilde{p}_i of L lying above p_i , ($1 \leq i \leq s$).

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 in p_i ,

$$I_i \hookrightarrow G/X = \Gamma$$

is surjective, hence bijective. So

$$G = I_i X = X I_i, \quad i = 1, \dots, s.$$

Let $\sigma_i \in I_i$ map to γ_0 . Then σ_i is a topological generator of I_i . Since

$$I_i \subseteq X I_i,$$

we have

$$\sigma_i = a_i \sigma_1$$

for some $a_i \in X$.

Note that $a_1 = 1$.

Lemma 2.3. (*Assuming the "Assumption"*). *Let G' be the closure of the commutator subgroup of G . Then*

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

Proof. Lemma 13.14 of [1] (page 278). □

Let

$$Y_0 := \overline{\langle X^{\gamma_0-1}, a_2, \dots, a_n \rangle} \subset X$$

as a \mathbb{Z}_p -submodule.

Lemma 2.4. (*Assuming the "Assumption"*).

$$X_0 \simeq X/Y_0.$$

Proof. We have $K \subseteq L_0 \subseteq L$. Since L_0 is the maximal abelian unramified p -extension of K , and since L/K is a p -extension, L_0/K is the maximal unramified abelian subextension of L/K . Therefore $\text{Gal}(L/L_0)$ must be the closed subgroup of G generated by G' and all the inertia groups I_1, \dots, I_s . This implies that,

$$\text{Gal}(L/L_0) = \overline{\langle X^{\gamma_0-1}, I_1, I_2, \dots, I_s \rangle} \cong \overline{\langle X^{\gamma_0-1}, I_1, a_2, \dots, a_s \rangle}.$$

So,

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

□

Lemma 2.5. (Assuming the "Assumption"). Let

$$\nu_n := \sum_{i=0}^{p^n-1} \gamma_0^i = \frac{(1+T)^{p^n} - 1}{T}.$$

Then

$$X_n \simeq X/\nu_n Y_0, \quad \forall n \geq 0.$$

Proof. We proved the $n = 0$ case above.

For $n \geq 1$. We have that

$$X_n = \text{Gal}(L_n/K_n) = \text{Gal}(L/K_n)/\text{Gal}(L/L_n) = XI_1^n/\text{Gal}(L/L_n)$$

Replace γ_0 with $\gamma_0^{p^n}$.

Then σ_i becomes $\sigma_i^{p^n}$. Observe that

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

Therefore,

$$\sigma_i^{p^n} = (\nu_n a_i) \sigma_1^{p^n}.$$

So, a_i is replaced by $\nu_n a_i$. Finally, $X^{\gamma_0^{-1}}$ is replaced by $(\gamma_0^{p^n} - 1)X = \nu_n X^{\gamma_0^{-1}}$.

Therefore, Y_0 becomes $\nu_n Y_0$ and the proof is complete. □

We above lemma allows to retrieve information about X_n from information about X .

Lemma 2.6. (*Nakayama's Lemma*). *Let X be a compact Λ -module. Then*

$$X \text{ is fin. generated over } \Lambda \Leftrightarrow X/(p, T)X \text{ is finite.}$$

If x_1, \dots, x_n generate $X/(p, T)X$ over \mathbb{Z} , then they also generate X as a Λ -module. As special case of that,

$$X/(p, T)X = 0 \Leftrightarrow X = 0.$$

Proof. Lemma 13.16 of [1] (page 279). \square

Lemma 2.7. (*Assuming the "Assumption"*). *X is finitely generated Λ -module and*

$$X_n \simeq X/\nu_n Y_0, \quad \forall n \geq 0.$$

Proof. Clearly $\nu_1 \in (p, T)$, so $Y_0/(p, T)Y_0$ is a quotient of $Y_0/\nu_1 Y_0 \subseteq X/\nu_1 Y_0 = X_1$, which is finite.

Therefore Y_0 is finitely generated. Since $X_0 = X/Y_0$ is finite, X is finitely generated. The rest come from the previous lemma. \square

We have that

$$0 \rightarrow Y_0 \hookrightarrow X \rightarrow X/Y_0 \rightarrow 0.$$

This implies that $Y_0 \sim X$.

Since X is fin. generated, by theorem 1.9, we have that

$$Y_0 \sim X \sim \Lambda^r \oplus \left(\bigoplus_{i=1}^s \Lambda/(p^{k_i}) \right) \oplus \left(\bigoplus_{j=1}^t \Lambda/(f_j(T)^{m_j}) \right),$$

where $r, s, t, k_i, m_j \in \mathbb{Z}$ and f_j is distinguished and irreducible.

We shall calculate $V/\nu_n V$ for each of the summands V on the right side.

(1) $V = \Lambda$.

$\Lambda/(\nu_n)$ is infinite. Since, $Y_0/\nu_n Y_0$ is finite and $\Lambda^r/(\nu_n) \subset Y_0/\nu_n Y_0$, it follows that $r = 0$.

(2) $V = \Lambda/(p^k)$. We have that

$$V/\nu_n V \simeq \Lambda/(p^k, \nu_n)$$

$$|V/\nu_n V| = p^{k(p^n-1)} = p^{kp^n-k}$$

(3) $V = \Lambda/(f(T)^m)$.

Let

$$g(T) := f(T)^m.$$

and let $\deg(g) := d$. g is also distinguished. Hence,

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

We have:

$$T^d = g(T) + pQ(T)$$

for some $Q(T)$ and

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

$$T^d T^{k-d} \equiv p(T^{k-d}Q(T)) \pmod{g}$$

$$T^k \equiv p(T^{k-d}Q(T)) \pmod{g}$$

for $k \geq d$. If $p^n \geq d$ then

$$(1+T)^{p^n} \equiv (1+pQ'(T)) \pmod{g}$$

for some $Q'(T)$. Then,

$$((1+T)^{p^n})^p \equiv ((1+pQ'(T)))^p \pmod{g}$$

$$(1+T)^{p^{n+1}} \equiv 1 + p^2Q''(T) \pmod{g}$$

for some $Q''(T)$. It follows that

$$\begin{aligned} P_{n+2}(T) &= (1+T)^{p^{n+2}} - 1 \\ &= \left[(1+T)^{(p-1)p^{n+1}} + \dots + (1+T)^{p^{n+1}} + 1 \right] \left[(1+T)^{p^{n+1}} - 1 \right] \\ &\equiv (1 + \dots + 1 + p^2(\text{polyn.}))(P_{n+1}(T)) \pmod{g} \\ &\equiv p(1 + p(\text{polyn.}))P_{n+1}(T) \pmod{g}. \end{aligned}$$

Note that $1 + p(\text{polyn.})$ is a unit in Λ .

(Recall that: $a_0 + Tf$ with $f \in \Lambda$ is a unit in $\Lambda \Leftrightarrow a_0 \in \mathbb{Z}_p^\times$)

Therefore, $\frac{P_{n+2}}{P_{n+1}}$ acts as $p(\text{unit})$ on $V = \Lambda/(g)$ for $p^n \geq d$.

Assume $n_0 > 0, p^{n_0} \geq d, n \geq n_0$. Then

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

and

$$\nu_{n+2}V = \frac{P_{n+2}}{P_{n+1}}(\nu_{n+1}V) = p\nu_{n+1}V.$$

Therefore,

$$|V/\nu_{n+2}V| = |V/pV| |pV/p\nu_{n+1}V| = |V/\nu_{n+1}V|$$

for $n \geq n_0$. The last equality holds because since $(g, p) = 1$, multiplication by p is injective.

We have that

$$V/pV \simeq \Lambda/(p, g) = \Lambda/(p, T^d) = \mathbb{Z}_p[[T]]/(p, T^d) = \mathbb{F}_p[[T]]/(T^d).$$

So

$$|V/pV| = p^d.$$

By induction,

$$|V/\nu_n V| = p^{d(n-n_0-1)} |V/\nu_{n_0+1} V|$$

for $n \geq n_0 + 1$.

- If $V/\nu_n V$ is infinite then V cannot occur exactly as in case 1. This happens only when $(\nu_n, f) \neq 1$.

- If $V/\nu_n V$ is finite $\forall n$,

$$|V/\nu_n V| = p^{dn+c}, \quad n \geq n_0 + 1,$$

for some constant c .

We obtain the following

Proposition 2.8. *Suppose*

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

where each g_j is distinguished (not necessarily irreducible).

Let $m := \sum_i k_i$ and $\ell := \sum_j \deg g_j$.

If $E/\nu_n E$ is finite $\forall n$, then $r = 0$ and there exist n_0 and c s.t.

$$|E/\nu_n E| = p^{mp^n + \ell n + c}, \quad \forall n > n_0.$$

We have an exact sequence

$$0 \rightarrow A \rightarrow Y_0 \rightarrow E \rightarrow B \rightarrow 0$$

where A, B are finite and E is as in the last proposition. We know $|E/\nu_n E|$, $\forall n > n_0$. It remains to obtain information for $|Y_0/\nu_n Y_0|$. At the moment, all we can conclude is that

$$e_n = mp^n + \ell n + c_n,$$

where c_n is bounded. The following lemma solves our problem.

Lemma 2.9. *(Assuming the "Assumption"). Suppose that Y and E are Λ -modules with $Y \sim E$ s.t. $Y/\nu_n Y$ is finite $\forall n \geq 0$. Then, for some constant c and for some n_0 we have that,*

$$|Y/\nu_n Y| = p^c |E/\nu_n E|, \quad \forall n \geq n_0.$$

Proof. Since $Y \sim E$, \exists homomorphism $\phi : Y \rightarrow E$ with $|\ker(\phi)|, |\operatorname{coker}(\phi)| < \infty$.

We have the following commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \nu_n Y & \longrightarrow & Y & \longrightarrow & Y/\nu_n Y & \longrightarrow & 0 \\ & & \phi'_n \downarrow & & \phi \downarrow & & \phi''_n \downarrow & & \\ 0 & \longrightarrow & \nu_n E & \longrightarrow & E & \longrightarrow & E/\nu_n E & \longrightarrow & 0 \end{array}$$

which can be written (using Snake Lemma)

$$\begin{array}{ccccccc}
0 & \longrightarrow & \ker(\phi'_n) & \longrightarrow & \ker(\phi) & \longrightarrow & \ker(\phi''_n) \\
& & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \nu_n Y & \longrightarrow & Y & \longrightarrow & Y/\nu_n Y \longrightarrow 0 \\
& & \downarrow \phi'_n & & \downarrow \phi & & \downarrow \phi''_n \\
0 & \longrightarrow & \nu_n E & \longrightarrow & E & \longrightarrow & E/\nu_n E \longrightarrow 0 \\
& & \downarrow & & \downarrow & & \downarrow \\
& & \text{coker}(\phi'_n) & \longrightarrow & \text{coker}(\phi) & \longrightarrow & \text{coker}(\phi''_n) \longrightarrow 0
\end{array}$$

There are the following inequalities:

- (i) $|\ker(\phi'_n)| \leq |\ker(\phi)|$
- (ii) $|\text{coker}(\phi'_n)| \leq |\text{coker}(\phi)|$
- (iii) $|\text{coker}(\phi''_n)| \leq |\text{coker}(\phi)|$
- (iv) $|\ker(\phi''_n)| \leq |\ker(\phi)| \cdot |\text{coker}(\phi)|$

Inequality (i) is obvious.

For inequality (iii): Representatives of $\text{coker}(\phi)$ give representatives for $\text{coker}(\phi''_n)$ so the inequality follows immediately.

For inequality (ii):

$$\text{coker}(\phi) \cong E/\phi(Y) \text{ and}$$

$$\text{coker}(\phi'_n) \cong \nu_n E/\phi(\nu_n Y) \cong \nu E/\nu_n \phi(Y).$$

So, the map

$$\text{coker}(\phi) \longrightarrow \text{coker}(\phi'_n)$$

$$x + \phi(Y) \longmapsto \nu_n x + \nu_n \phi(Y)$$

is well-defined and surjective.

14

because

$$E \longrightarrow \nu_n E$$

$$x \longmapsto \nu_n x$$

is surjective.

For inequality (iv): By the Snake lemma, there is a long exact sequence

$$0 \rightarrow \ker(\phi'_n) \rightarrow \ker(\phi) \rightarrow \ker(\phi''_n) \rightarrow \operatorname{coker}(\phi'_n) \rightarrow \operatorname{coker}(\phi''_n) \rightarrow 0.$$

It follows that

$$|\ker(\phi''_n)| \leq |\ker(\phi)| |\operatorname{coker}(\phi'_n)| \stackrel{(ii)}{\leq} |\ker(\phi)| |\operatorname{coker}(\phi)|.$$

Now suppose $m \geq n \geq 0$. We have the following inequalities.

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

For (a): Observe that $\nu_m = \frac{\nu_m}{\nu_n} \nu_n$. Therefore $\nu_m Y \subseteq \nu_n Y$. This implies that,

$$\ker(\phi'_m) \subset \ker(\phi'_n).$$

For (b): Let that $\nu_m y \in \nu_m E$. Let $z \in \nu_n E$ be a representative for $\nu_n y$ in $\operatorname{coker}(\phi'_n)$. Then

$$\nu_n y - z = \phi(\nu_n x), \text{ for some } x \in Y.$$

Multiply by ν_m/ν_n to obtain

$$\nu_m y - \frac{\nu_m}{\nu_n} z = \phi(\nu_m x) = \phi'_m(\nu_m x).$$

So $\frac{\nu_m}{\nu_n}$ times representatives for $\operatorname{coker}(\phi'_n)$ gives representatives for $\operatorname{coker}(\phi'_m)$ i.e. $|\operatorname{coker}(\phi'_n)| \geq |\operatorname{coker}(\phi'_m)|$.

For (c): It follows easily from $\nu_m E \subseteq \nu_n E$.

By the seven inequalities above, we conclude that $|\ker(\phi'_n)|$, $|\operatorname{coker}(\phi'_n)|$ and $|\operatorname{coker}(\phi''_n)|$ are constant for $n \geq n_0$, for some n_0 .

It remains to conclude that for $|\ker(\phi''_n)|$ as well.

By the Snake Lemma,

$$|\ker(\phi'_n)| |\ker(\phi''_n)| |\operatorname{coker}(\phi)| = |\ker(\phi)| |\operatorname{coker}(\phi'_n)| |\operatorname{coker}(\phi''_n)|.$$

It follows that $|\ker(\phi''_n)|$ must be a constant for $n \geq n_0$. After that the lemma follows easily. \square

We therefore have E as in the proposition, integers $\lambda \geq 0, \mu \geq 0, \nu$ and n_0 s.t.

$$\begin{aligned} p^{e_n} &= |X_n| = |X/Y_0| |Y_0/\nu_n Y_0| \\ &= (\text{some constant}) |E/\nu_n E| \\ &= p^{\lambda n + \mu p^n + \nu}, \quad \forall n > n_0. \end{aligned}$$

This completes the proof of the theorem.