



EÖTVÖS LORÁND UNIVERSITY

FACULTY OF SCIENCES

DEPARTMENT OF ALGEBRA AND NUMBER THEORY

# Cyclotomic Field Extensions and Iwasawa Theory

*Supervisor:*

Dr. Zabradi Gergely

Associate Professor

*Author:*

Ritoprovo Roy

Pure Mathematics, MSc

*Budapest, 2023*

# Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
1.1	Cyclotomic Fields . . . . .	2
1.2	Proof of Motivating Theorem . . . . .	3
1.3	A Few Basic Results . . . . .	5
<b>2</b>	<b>The Main Elements and Conjectures of Iwasawa Theory</b>	<b>8</b>
2.1	Herbrand-Ribet Theorem . . . . .	8
2.2	The Cyclotomic Tower . . . . .	8
2.3	The Main Conjecture . . . . .	10
2.4	The theorem of Iwasawa . . . . .	10
<b>3</b>	<b>Conclusion</b>	<b>13</b>
	<b>Acknowledgements</b>	<b>16</b>

# Chapter 1

## Introduction

### 1.1 Cyclotomic Fields

We start with a special case of Fermat's Last Theorem to motivate the explanation for cyclotomic fields.

**Theorem 1.** *Suppose  $p$  is an odd prime and  $p$  does not divide the class number of the field  $\mathbb{Q}(\zeta_p)$ , where  $\zeta_p$  is the  $p^{\text{th}}$  root of unity. Then*

$$x^p + y^p = z^p, \quad (xyz, p) = 1$$

*has no solutions in  $\mathbb{Q}$ .*

Factoring the Fermat's expression we get

$$\prod_{i=0}^{p-1} (x + \zeta_p^i y) = z^p$$

and this naturally leads us to consider the ring  $\mathbb{Z}[\zeta_p]$ . We state some basic results for this ring throughout the chapter.

**Proposition 1.**  *$\mathbb{Z}[\zeta_p]$  is the ring of algebraic integers in the field  $\mathbb{Q}(\zeta_p)$ . Hence  $\mathbb{Z}[\zeta_p]$  is a Dedekind domain (so we have a unique factorisation into prime ideals etc.)*

The proposition below will be needed with much importance to prove the motivating theorem of this chapter

**Proposition 2.** *Let  $\epsilon$  be a unit of  $\mathbb{Z}[\zeta_p]$ . Then there exists  $\epsilon_1 \in \mathbb{Q}(\zeta_p + \zeta_p^{-1})$  and  $r \in \mathbb{Z}$  such that  $\epsilon = \zeta^r \epsilon_1$ .*

*Remark.* Take any embedding of  $\mathbb{Q}(\zeta_p)$ , into the complex numbers. Complex conjugation acts as automorphism sending  $\zeta_p \rightarrow \zeta_p^{-1}$ . The fixed field is  $\mathbb{Q}(\zeta_p + \zeta_p^{-1}) = \mathbb{Q}(\cos \frac{2\pi}{p})$  and is called the maximal real subfield of  $\mathbb{Q}(\zeta_p)$ . The proposition then implies that any unit of  $\mathbb{Z}[\zeta_p]$  maybe expressed as root of unit times a real unit. This result is plausible since the field  $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$  has  $\frac{(p-1)}{2}$  real embeddings and no complex embeddings into  $\mathbb{C}$ , while  $\mathbb{Q}(\zeta_p)$  has no real embeddings and  $\frac{(p-1)}{2}$  pairs of complex embeddings. Therefore the  $\mathbb{Z}$ -rank of the unit groups of each field is  $\frac{(p-3)}{2}$ , so the units of  $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$  are of finite index in those of  $\mathbb{Q}(\zeta_p)$ .

We now state an important lemma.

**Lemma 1.** *If  $\alpha$  is an algebraic integer all of whose conjugates have absolute value 1, then  $\alpha$  is a root of unity.*

## 1.2 Proof of Motivating Theorem

We now outline the proof for the motivating theorem.

We first treat the case for  $p = 3$ . If  $3 \nmid x$  then  $x^3 \equiv \pm 1 \pmod{9}$  and similarly for  $y$  and  $z$ . Therefore  $x^3 + y^3 \equiv -2, 0, 2 \pmod{9}$  but  $z^3 \equiv \pm 1$ . Similarly we treat the case for  $p = 5$  by considering modulo 25. However this method fails from  $p = 7$  and onwards.

Assume  $p \geq 5$  and suppose that  $x^p + y^p = z^p$ ,  $p \nmid xyz$ . Suppose  $x \equiv y \equiv -z \pmod{p}$ . Then  $-2z^p \equiv x^p$ , which is impossible since  $p \nmid 3z$ . Therefore we may rewrite the equation as  $x^p + (-z^p) = (-y^p)$  and assume  $x, y$  and  $z$  are relatively prime.

**Lemma 2.** *The ideals  $(x + \zeta_p^i)$ ,  $i \in [p - 1]$  are pairwise relatively prime.*

**Lemma 3.** *Let  $\alpha \in \mathbb{Z}[\zeta_p]$ . Then*

$$\alpha^p \equiv r \pmod{p}$$

where  $r \in \mathbb{Q}$ .

**Lemma 4.** *Suppose  $\alpha = a_0 + a_1\zeta + \dots + a_{p-1}\zeta^{p-1}$  with  $a_i \in \mathbb{Z}$  and atleast one  $a_i = 0$ . If  $n \in \mathbb{Z}$  and  $n$  divides  $\alpha$ , then  $n$  divides each  $a_j$ .*

We now conclude the proof of the theorem. Consider the equation

$$\prod_{i=0}^{p-1} (x + \zeta_p^i) = (z)^p$$

as an equality of ideals. Since the ideals  $(x + \zeta_p^i)$ ,  $0 \leq i \leq p-1$ , are pairwise relatively prime by lemma 2, each of them must be  $p^{\text{th}}$  power of an ideal and hence

$$\prod_{i=0}^{p-1} (x + \zeta_p^i) = A_i^p$$

Since we have assumed that the class number of  $\mathbb{Q}(\zeta_p)$  is assumed to be not divisible by  $p$ , the ideal  $A_i$  must be principal, say  $A_i = (\alpha_i)$ . Consequently we have the relation  $(x + \zeta_p^i) = (\alpha_i)^p$ , so  $(x + \zeta_p^i) = u \cdot \alpha_i^p$ , where  $u$  is an unit.

Let  $i = 1$  and we omit the other subscripts. We see that  $x + \zeta_p = \epsilon \alpha^p$ . By proposition 2, we get that  $\epsilon = \zeta^r \epsilon_1$  for some integer  $r$  and where  $\bar{\epsilon}_1 = \epsilon_1$ . Lemma 3 says that we have a rational integer  $a$  such that  $\alpha^r \equiv a \pmod{p}$ . Therefore  $x + \zeta y = \zeta^r \epsilon_1 \alpha^p \equiv \zeta^r \epsilon_1 a \pmod{p}$ . Also  $x + \zeta^{-1} y = \zeta^{-r} \epsilon_1 \bar{\alpha}^p \equiv \zeta^{-r} \epsilon_1 \bar{a} = \zeta^{-r} \epsilon_1 a \pmod{p}$ . We obtain from here

$$\begin{aligned} \zeta^{-r}(x + \zeta y) &\equiv \zeta^r(x + \zeta^{-1}y) \pmod{p} \quad \text{or,} \\ x + \zeta y - \zeta^{2r}x - \zeta^{2r-1}y &\equiv 0 \pmod{p} \end{aligned}$$

If  $1, \zeta, \zeta^{2r}, \zeta^{2r-1}$  are all distinct, then by Lemma 4 we have  $p$  divides  $x$  and  $y$ , a contradiction. Hence they are not distinct. Our only possibilities are

- $1 = \zeta^{2r}$ . Then the second relation above gives me,

$$\begin{aligned} x + \zeta y - x - \zeta^{-1}y &\equiv 0 \pmod{p} \\ \implies \zeta y - \zeta^{p-1}y &\equiv 0 \pmod{p} \\ \implies y &\equiv 0 \pmod{p} \end{aligned}$$

a contradiction.

- $1 = \zeta^{2r-1} \implies \zeta = \zeta^{2r}$ , and then our equation becomes,

$$\begin{aligned} (x - y)(1 - \zeta) &\equiv 0 \pmod{p} \\ \implies x - y &\equiv 0 \pmod{p} \quad (\text{By Lemma 4}) \\ \implies x &\equiv y \pmod{p} \end{aligned}$$

which contradicts the choice of  $x$  and  $y$  made at the beginning of the proof.

- $\zeta = \zeta^{2r-1}$ . Then equation becomes

$$\begin{aligned} x - \zeta^2 x &\equiv 0 \pmod{p} \\ \implies x &\equiv 0 \pmod{p} \end{aligned}$$

a contradiction. And hence the proof of the theorem is complete.

### 1.3 A Few Basic Results

In this section we prove some basic results on cyclotomic fields.

**Proposition 3.** *The discriminant of  $\mathbb{Q}(\zeta_{p^n})$  is*

$$\pm p^{p^{n-1}(pn-n-1)}$$

where we have

- $p^{p^{n-1}(pn-n-1)}$  if  $p^n = 4$
- $-p^{p^{n-1}(pn-n-1)}$  if  $p \equiv 3 \pmod{4}$

We note that this proposition implies that  $p$  divides the discriminant if and only if  $p$  divides  $m$ .

**Proposition 4.** *If  $(m, n) = 1$  then  $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$*

**Theorem 2.**  *$\deg(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \phi(n)$  and  $\text{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$ , with  $a \equiv (\text{mod } n)$  corresponding to the map  $\zeta_n \rightarrow \zeta_n^a$ .*

**Theorem 3.**  *$\mathbb{Z}[\zeta_n]$  is the ring of algebraic integers of  $\mathbb{Q}(\zeta_n)$ .*

We can now compute the discriminant of  $\mathbb{Q}(\zeta_n)$ . The above mentioned result can be written as

$$\frac{\log |d(K E)|}{\deg(K E/\mathbb{Q})} = \frac{\log |d(K)|}{\deg(K/\mathbb{Q})} + \frac{\log |d(E)|}{\deg(E/\mathbb{Q})}$$

Therefore  $n = \prod p^{a_i}$  we have,

$$\begin{aligned} \frac{\log |d(KE)|}{\deg(KE/\mathbb{Q})} &= \sum_i p_i^{a_i-1} (p_i a_i - a_i - 1) \frac{\log(p_i)}{\phi(p_i^{a_i})} \\ &= \sum_i \left( a_i - \frac{1}{p_i - 1} \right) (\log(p_i)) \\ &= \log(n) - \sum_{p|n} (\log(p))/(p-1) \end{aligned}$$

we obtain the following,

**Proposition 5.**  $d(\mathbb{Q}(\zeta_n)) = (-1)^{\phi(n)/2} \frac{n^{\phi(n)}}{\prod_{p|n} p^{\phi(n)/(p-1)}}$

Yet another important result is

**Proposition 6.** *Suppose  $n$  has at least two distinct prime factors. Then  $1 - \zeta_n$  is a unit of  $\mathbb{Z}[\zeta_n]$  and  $\prod_{0 < j < n, (j,n)=1} (1 - \zeta_n^j) = 1$ .*

We go on to define an irreducible polynomial for  $\zeta_n$ .

**Definition 1.** The  $n^{\text{th}}$  cyclotomic polynomial is defined

$$\Phi_n(X) = \prod_{(j,n)=1} (X - \zeta_n^j)$$

Since  $\deg(\mathbb{Q}(\zeta_n)/\mathbb{Q}) = \phi(n) = \deg(\Phi_n(X))$ , it follows that  $\Phi_n(X)$  is the irreducible polynomial for  $\zeta_n$ . Also,  $\Phi_n(X) \in \mathbb{Z}[X]$  since the coefficients are rational algebraic integers. In addition we observe

$$X^n - 1 = \prod_{d|n} \Phi_d(X)$$

Our aim was to investigate splitting of primes in cyclotomic fields. We need the following useful result.

**Lemma 5.** *Suppose  $p \nmid n$  and let  $\mathcal{P}$  be a prime of  $\mathbb{Q}(\zeta_n)$  lying above  $p$ . Then the  $n^{\text{th}}$  roots of unity are distinct mod  $\mathcal{P}$ .*

We have to note that the result is not true for  $p \mid n$ . In  $\mathbb{Q}(\zeta_p)$  we have  $\zeta_p \equiv \text{mod } (1 - \zeta_p)$ . Assume that  $p \mid n$ , and let  $\mathcal{P}$  lie above  $p$  in  $\mathbb{Q}(\zeta_n)$ . The Frobenius automorphism of  $\mathbb{Q}(\zeta_n)$  is defined by

$$\sigma_p x \equiv x^p \text{ mod } \mathcal{P} \quad \text{for all } x \in \mathbb{Z}[\zeta_n]$$

Since  $\sigma_p \zeta_n$  is an  $n^{\text{th}}$  root of unity, the previous lemma implies that  $\sigma_p \zeta_n = \zeta_p^n$ . The order of  $\zeta_p$  is the degree of the residue class extension  $\mathbb{Z}[\zeta_n] \bmod \mathcal{P} / \mathbb{Z} \bmod p$ . Now,

$$\begin{aligned} \sigma_p^f &= 1 \\ \iff \sigma_p^f(\zeta_n) &= \zeta_n \\ \iff \zeta_n^{p^f} &= \zeta_n \\ \iff p^f &\equiv 1 \pmod{n} \end{aligned}$$

Since  $p$  is unramified in  $\mathbb{Q}(\zeta_n)$ , we know from algebraic number theory that the degree of the residue class extension multiplied by the number of primes above  $p$  equals the degree of extension  $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ . We therefore arrive at the following

**Theorem 4** (Cyclotomic Reciprocity Law). *Suppose  $p \nmid n$  and let  $f$  be the smallest positive integer such that  $p^f \equiv 1 \pmod{n}$ . Then  $p$  splits into  $g = \phi(n)/f$  distinct primes in  $\mathbb{Q}(\zeta_n)$ , each of which has residue class degree  $f$ . In particular,  $p$  splits completely  $\iff p^f \equiv 1 \pmod{n}$ .*

# Chapter 2

## The Main Elements and Conjectures of Iwasawa Theory

### 2.1 Herbrand-Ribet Theorem

We investigate Kummer's criterion deeply. We consider the action of the Galois group  $\bar{\omega}$  on  $\mathfrak{C}$ . Let  $\mathfrak{B} = \mathfrak{C}/\mathfrak{C}^p$ , which is a finite dimensional vector space over the field  $\mathbb{F}_p$ , on which the Galois group  $\bar{\omega}$  acts naturally. The action is semisimple, because the order of  $\bar{\omega}$  is prime to  $p$ . We therefore naturally arrive at the question **which characters of  $\theta^n$ , where  $n = 1, 2, \dots, p-1$ , occur in  $\mathfrak{B}$ , and what is the multiplicity of their occurrence ?**

**Theorem 5** (Herbrand-Ribet). *Let  $n$  be an odd integer with  $3 \leq n \leq p-2$ . Then  $\theta^n$  occurs in  $\mathfrak{B}$  if and only if  $p$  divides the numerator  $\zeta(n+1-p)$ .*

The occurrence is not guaranteed yet.

**Conjecture 1** (Kummer-Vandiver). *Let  $K = \mathbb{Q}(\zeta_p)^+$ , the maximal real subfield of the  $p^{\text{th}}$  cyclotomic field. Then  $p$  does not divide  $h_K$ .*

### 2.2 The Cyclotomic Tower

Let  $n$  be a natural number, and write  $\mu_{p^{n+1}}$  (respectively  $\mu_{p^\infty}$ ) for the group of all  $p^{n+1}$ -th roots of unity in some fixed algebraic closure of  $\mathbb{Q}$ .

**Definition 2.** We define the following notions

$$\mathcal{F}_n = \mathbb{Q}(\mu_{p^{n+1}}) \quad \mathcal{F}_\infty = \mathbb{Q}(\mu_{p^\infty})$$

and,

$$F_n = \mathbb{Q}(\mu_{p^{n+1}})^+ \quad F_\infty = \mathbb{Q}(\mu_{p^\infty})^+$$

be their maximal totally real subfields. We write

$$\mathcal{G} = \text{Gal}(\mathcal{F}_\infty/\mathbb{Q}) \quad G = \text{Gal}(F_\infty/\mathbb{Q})$$

For the corresponding Galois groups.

The action of  $\mathcal{G}$  over  $\mu_{p^\infty}$  defines an injection

$$\chi : \mathcal{G} \rightarrow \mathbb{Z}_p^\times = \text{Aut}(\mu_{p^\infty})$$

which is an isomorphism since cyclotomic polynomials are irreducible. We also observe that both  $\mathcal{G}$  and  $G$  are abelian. Let  $\mathcal{L}$  (resp.  $L_\infty$ ) be the maximal abelian  $p$ -extension of  $\mathcal{F}$  (resp.  $F_\infty$ ), which is unramified everywhere.

**Definition 3.** We define

$$\mathcal{Y}_\infty = \text{Gal}(\mathcal{L}_\infty/\mathcal{F}_\infty) \quad Y_\infty = \text{Gal}(L_\infty/F_\infty)$$

Since  $\mathcal{Y}_\infty$  and  $Y_\infty$  are abelian, the Galois group acts on the inner automorphism in the following way:

Let  $\sigma \in \mathcal{G}$ , and we pick any lifting of  $\tilde{\sigma} \in \mathcal{L}_\infty$  over  $\mathbb{Q}$ . We then define

$$\sigma.y = \tilde{\sigma}y\tilde{\sigma}^{-1} \quad \text{for } y \in \mathcal{Y}_\infty$$

We now proceed to define Iwasawa Algebras

**Definition 4** (Iwasawa Algebras). The Iwasawa algebras of  $\mathcal{G}$  and  $G$  are defined by

$$\Lambda(\mathcal{G}) = \varprojlim \mathbb{Z}_p[\mathcal{G}/\mathcal{H}] \quad \Lambda(G) = \varprojlim \mathbb{Z}_p[G/H]$$

where  $\mathcal{H}$  and  $H$  runs over open subgroups of  $\mathcal{G}$  and  $G$  respectively. Since  $\mathcal{Y}_\infty$  is by construction a compact  $\mathbb{Z}_p$  module, the  $\mathcal{G}$  action on it extends by continuity and linearity to an action of the whole Iwasawa Algebra  $\Lambda(\mathcal{G})$ . Standard arguments in Iwasawa Theory show that  $\mathcal{Y}_\infty$  is a finitely generated torsion module over  $\Lambda(\mathcal{G})$ .

One can see the implication that if Vandiver's conjecture is true then  $Y_\infty = 0$ .

## 2.3 The Main Conjecture

Let  $\mathcal{M}_\infty$  be the maximal abelian  $p$ -extension of  $\mathcal{F}_\infty$ , which is unramified outside the unique prime above  $p$  in  $\mathcal{F}_\infty$ .

**Definition 5.** We define

$$\mathcal{X}_\infty = \text{Gal}(\mathcal{M}_\infty/\mathcal{F}_\infty) \quad X_\infty = \text{Gal}(M_\infty/F_\infty)$$

We now study the following important theorem

**Theorem 6** (Iwasawa). *The module  $X_\infty$  is a finitely generated torsion  $\Lambda(G)$ -module.*

We recall from the structure theory of finitely generated torsion  $\Lambda(G)$ -modules, implies that for each such module  $N$ , there is an exact sequence of  $\Lambda(G)$ -modules

$$0 \rightarrow \bigoplus_{i=1}^r \frac{\Lambda(G)}{\Lambda(G)f_i} \rightarrow N \rightarrow D \rightarrow 0$$

where  $f_i$  is a non-zero divisor, and  $D$  is finite. Then the characteristic ideal of  $N$ , which denote by  $ch_G(N)$ , is defined to be the ideal of  $\Lambda(G)$  generated by the product  $f_1 f_2 f_3 \cdots f_r$ .

**Theorem 7.** *There exists a unique pseudo-measure  $\zeta_p$  on  $G$  such that*

$$\int_G \chi(g)^k d\zeta_p = (1 - p^{k-1})\zeta(1 - k)$$

for all even integers  $k \geq 2$ .

Let  $I(G)$  denote the kernel of the augmentation homomorphism from  $\Lambda(G)$  to  $\mathbb{Z}_p$ . As  $\zeta_p$  is a pseudo-measure,  $I(G)\zeta_p$  is an ideal of  $\Lambda(G)$ .

**Theorem 8** (The Main Conjecture of Iwasawa). *We have*

$$ch_G(X_\infty) = I(G)\zeta_p$$

## 2.4 The theorem of Iwasawa

For each  $n \geq 0$ , we consider the local field

$$K_n = \mathbb{Q}_p(\mu_{p^{n+1}})^+$$

We write  $U_n^1$  as the group of units of  $K_n$ , which are  $\equiv 1 \pmod{\mathfrak{p}_n}$ , where  $p_n$  is the maximal ideal of the ring of integers of  $K_n$ . Let  $D_n$  be the group of cyclotomic units of  $F_n$ . Thus  $D_n$  is generated by Galois conjugates of

$$\pm \frac{\zeta_n^{-e/2} - \zeta_n^{e/2}}{\zeta_n^{-1/2} - \zeta_n^{1/2}}$$

where  $\zeta_n$  denotes the primitive  $p^{n+1}$ -th root of unity, and  $e$  is a primitive root modulo  $p$  such that  $e^{p-1} \not\equiv 1 \pmod{p^2}$ . We define  $D_n^1$  to be the subgroup of all elements of  $D_n$  which are  $\equiv 1 \pmod{\mathfrak{p}_n}$ . We let

$$C_n^1 = \bar{D}_n^{-1}$$

be the closure of  $D_n^1$  in  $U_n^1$  with respect to  $\mathfrak{p}_n$ -adic topology. Define

$$U_\infty^1 = \varprojlim U_n^1, \quad C_\infty^1 = \varprojlim C_n^1$$

where the projective limits are taken with respect to the norm maps. Of course the group  $G$  acts continuously on both these  $\mathbb{Z}_p$ -modules, endowing them with an action of  $\Lambda(G)$ .

**Theorem 9** (Iwasawa). *The  $\Lambda(G)$ -module  $U_\infty^1/C_\infty^1$  is canonically isomorphic to  $\Lambda(G)/I(G) \cdot \zeta_p$ , where  $\zeta_p$  is the  $p$ -adic zeta function, and  $I(G)$  is the augmentation ideal.*

The comparison between the Galois group  $X_\infty$  and the module  $U_\infty^1/C_\infty^1$  is provided by class field theory. Let  $V_n^1$  be the group of units of the ring of integers of  $F_n$  which are  $\equiv 1 \pmod{\mathfrak{p}_n}$ , and we define

$$E_n^1 = \bar{V}_n^{-1}, \quad E_\infty^1 = \varprojlim E_n^1$$

where the closure in  $U_n^1$  is again taken with respect to  $p$ -adic topology and projective limit with respect to norm maps. The Artin map of global class field theory gives a canonical  $\Lambda(G)$ -isomorphism

$$\text{Gal}(M_\infty/L_\infty) \cong U_\infty^1/E_\infty^1$$

as a result giving us the four term exact sequence of  $\Lambda(G)$ -modules

$$0 \rightarrow E_\infty^1/C_\infty^1 \rightarrow U_\infty^1/C_\infty^1 \rightarrow X_\infty \rightarrow Y_\infty \rightarrow 0$$

all of which are finitely generated torsion modules. But the characteristic ideal is multiplicative in exact sequences. Hence if we assume Iwasawa's theorem we have

**Proposition 7.** *The main conjecture is true if and only if  $ch_G(Y_\infty) = ch_G(E_\infty^1/C_\infty^1)$ .*

# Chapter 3

## Conclusion

We conclude this report by explaining why Kummer's criterion for irregularity is a consequence of the main conjecture. An important result of Iwasawa goes as follows

**Proposition 8.**  *$X_\infty$  has no non-zero finite  $\Lambda(\Gamma_0)$ -submodule, where  $\Gamma_0 = \text{Gal}(F_\infty/F_0)$ .*

using this proposition, it follows easily from the conjecture and the structure theory of finitely generated torsion  $\Lambda(G)$ -modules, that

$$I(G)\zeta_p = \Lambda(G)$$

if and only if

$$X_\infty = 0$$

However, we claim that the first equation above is equivalent to the assertion that all of the values

$$\zeta(-1), \zeta(-3), \dots, \zeta(4-p)$$

are  $p$ -adic units. Indeed, as we know, for any finitely generated torsion  $\Lambda(G)$ -module  $M$ , we have a decomposition

$$M = \bigoplus_{i \bmod \frac{p-1}{2}} M^{(i)}$$

where  $M^{(i)}$  denotes the submodule of  $M$  on which  $G(F_0/\mathbb{Q})$  acts via  $\theta^{2i}$ . As we mentioned earlier,  $\zeta_p$  has a simple pole with residue  $1 - p^{-1}$  at the trivial character,

from which it follows easily that

$$(I(G)\zeta_p)^{(0)} = \Lambda(G)^{(0)}$$

also by taking  $i$  to be any of  $1, 2, \dots, (p-3)/2$  we can understand

$$(I(G)\zeta_p)^{(i)} = (\Lambda(G))^{(i)}$$

if and only if  $p$  does not divide the numerator of  $\zeta(1-2i)$ . It follows that our main equation is valid if and only if all the zeta values are  $p$ -adic units.

Next we must relate the criterion  $X_\infty = 0$  to the ideal class group of  $\mathcal{F}_0 = \mathbb{Q}(\mu_p)$ . For each  $n \geq 0$ , let  $\mathcal{A}_n$  denote the  $p$ -primary part of the ideal class group of  $\mathcal{F}_n$  and we define

$$\mathcal{A}_\infty = \varinjlim \mathcal{A}_n$$

where the inductive limits is taken with respect to the natural maps coming from the inclusion of fields. There is a canonical  $\mathcal{G}$ -isomorphism

$$\mathcal{A}_\infty^- = \text{Hom}(X_\infty, \mu_{p^\infty})$$

Moreover, it is known that the natural map from  $\mathcal{A}_n^-$  to  $\mathcal{A}_\infty^-$  is an injective homomorphism and introduces the isomorphism

$$\mathcal{A}_n^- \cong (\mathcal{A}_\infty^-)^{\Gamma_n}$$

for all  $n \geq 0$ , where  $\Gamma_n = \text{Gal}(\mathcal{F}_\infty/\mathcal{F}_n)$ . But for any discrete  $p$ -primary  $\Gamma_0$ -module  $N$ ,  $N^{\Gamma_0} = 0$  if and only if  $N = 0$ . In the view of these remarks, we see that

$$\mathcal{A}_0^- \text{ if and only if } X_\infty = 0$$

To conclude the proof of Kummer's criterion, one has to prove a stronger statement that  $\mathbb{A}_0 \neq 0$  if and only if  $\mathcal{X}_\infty \neq 0$ . One direction is already shown in the last equation. To prove the other direction we assume  $\mathcal{A}_0^+ \neq 0$ , thus writing  $L_0$  for the  $p$ -Hilbert class field of  $F_0$ , we have  $L_0 \neq F_0$ , and so  $L_0 F_\infty \neq F_\infty$ , because  $F_\infty/F_0$  is totally ramified at the unique prime above  $p$ . But clearly,  $L_0 F_\infty \in M_\infty$ , and so  $X_\infty = 0$  as required.

# Bibliography

- [1] Lawrence C. Washington (1982) *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics, Springer-Verlang.
- [2] J. Coates, R. Sujatha *Cyclotomic Fields and Zeta Values*, Springer Monographs in Mathematics, Springer.
- [3] Lang, Serge *Algebraic Number Theory*, Graduate Texts in Mathematics, Springer-Verlang

# Acknowledgements

I would like to thank Professor Zabradi Gergely, my supervisor for this project, who introduced me to this topic and methods discussed here. I would also like to convey sincere thanks to Professor Istvan Agoston, for giving me this opportunity for directed studies. Last but not the least I would like to thanks Professor Arpad Toth, as his course on Multiplicative Number Theory exposed me to much of the topics in zeta functions, and algebraic number theory which is discussed here.