

GALOIS GROUPS AND GREENBERG'S CONJECTURE

by

David C. Marshall

A Dissertation Submitted to the Faculty of the
DEPARTMENT OF MATHEMATICS

In Partial Fulfillment of the Requirements
For the Degree of

DOCTOR OF PHILOSOPHY

In the Graduate College

THE UNIVERSITY OF ARIZONA

2000

ACKNOWLEDGEMENTS

I would like to express a great many thanks to my advisor William McCallum. His unique ability to convey his wonderful intuition and insight contributed largely to the completion of this project.

I would like to thank as well the rest of the Number Theory Group at the University of Arizona, including Doug Ulmer, Dinesh Thakur, and Minhyong Kim, for the many courses, seminars, and conversations that occurred over the last several years. I consider myself lucky to have been part of such an active group.

I would also like to thank Ralph Greenberg. Much of this work was a result of some enlightening conversations that occurred during our stay at the Park City Mathematics Institute. I would like to thank him as well for many useful comments and corrections on early drafts of this document.

Finally, I wish to thank my family for all the support they have given during my educational pursuits; especially my wife, Susan, whose help during the final stages of this project were so valuable. I only hope I can be as much help to her as she now embarks on the difficult road I have just finished traveling.

TABLE OF CONTENTS

LIST OF TABLES	5
LIST OF FIGURES	6
ABSTRACT	7
CHAPTER 1. INTRODUCTION	8
1.1. Infinite Galois Groups	8
1.2. The Maximal pro- p , S -ramified Extension	9
1.2.1. Koch's Examples	9
1.2.2. A Linearization in the Case $K = \mathbb{Q}(\zeta_p)$, $S = \{p\}$	10
1.3. Greenberg's Conjecture	11
1.3.1. The Statement	11
1.3.2. Greenberg's Conjecture for Cyclotomic Fields	12
1.3.3. The Main Result	13
1.3.4. Greenberg's Conjecture and \mathcal{G}	14
CHAPTER 2. BACKGROUND	16
2.1. Cyclotomic Fields and Vandiver's Conjecture	16
2.1.1. Cyclotomic Fields and Class Numbers	16
2.1.2. Vandiver's Conjecture	18
2.2. \mathbb{Z}_p -extensions and Iwasawa's Theorem	19
2.2.1. Iwasawa's Theorem	20
2.2.2. \mathbb{Z}_p -extensions of $\mathbb{Q}(\zeta_p)$	21
2.3. The Maximal Pro- p , p -ramified Extension of $\mathbb{Q}(\zeta_p)$	25
2.3.1. Generators and Relations	25
2.3.2. The Structure of \mathcal{G}^{ab}	28
2.4. An Auxiliary Λ -module	31
CHAPTER 3. PROOF OF MAIN RESULTS	33
3.1. An Equivalent Formulation	34
3.2. Visible Torsion	38
3.3. A Unit Theorem	41
CHAPTER 4. FURTHER CONSIDERATIONS	43
4.1. Free Pro- p Galois Groups	43
4.2. A Computational Approach	45
4.3. Some Open Problems	47

TABLE OF CONTENTS—*Continued*

REFERENCES 49

LIST OF TABLES

TABLE 2.1. Experimental and predicted indexes of irregularity	24
---	----

LIST OF FIGURES

FIGURE 1.1. Field diagram 1 12
FIGURE 3.1. Field diagram 2. 39

ABSTRACT

We consider the structure of a certain infinite Galois group over $\mathbb{Q}(\zeta_p)$, the cyclotomic field of p -th roots of unity. Namely, we consider the Galois group of the maximal p -ramified pro- p -extension. Very little is known about this group. It has a free pro- p presentation in terms of g generators and s relations where g and s may be explicitly computed in terms of the p -rank of the class group of $\mathbb{Q}(\zeta_p)$.

The structure of the relations in the Galois group are shown to be very closely related to the relations in a certain Iwasawa module. The main result of this dissertation shows this Iwasawa module to be torsion free for a large class of cyclotomic fields. The result is equivalent to verifying Greenberg's pseudo-null conjecture for the given class of fields.

As one consequence, we provide a large class of examples of cyclotomic fields which do not admit free pro- p -extensions of maximal rank.

Chapter 1

INTRODUCTION

In this chapter we introduce a problem concerning the structure of a certain infinite Galois group. We then describe the relationship between this group's structure and a conjecture of Greenberg on the structure of a certain Iwasawa module. The main result of this dissertation is a proof of this conjecture for a certain class of number fields. Finally, we speculate on what this means about the Galois group structure. Details concerning most remarks follow in subsequent chapters.

1.1 Infinite Galois Groups

One of the most important outstanding problems in number theory is the determination of all Galois groups over \mathbb{Q} , the rational numbers. This is known as the *inverse Galois problem*. For example, it was shown by Shafarevich that all finite solvable groups occur as Galois groups over \mathbb{Q} (see [20] for a proof). For more details on the current techniques and results on this problem see [25].

Since the Galois group of an infinite extension of a number field is equal to the projective limit of all Galois groups of finite sub-extensions, a convenient way to package the inverse Galois problem is to study (and try to determine) $G_{\mathbb{Q}} = \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, the absolute Galois group of \mathbb{Q} (here $\overline{\mathbb{Q}}$ denotes a fixed algebraic closure of \mathbb{Q}). Although the full group structure is far from known, various techniques have been successful in making progress on the problem. We briefly describe a few of them here.

One approach taken is to try to understand $G_{\mathbb{Q}}$ via its representations, referred to as *Galois representations*. Note that via the Galois correspondence, a finite image of a representation of $G_{\mathbb{Q}}$ is a Galois group over \mathbb{Q} . This is currently a very active field due in part to the fact that very interesting Galois representations arise naturally in the study of modular forms and abelian varieties. For example, the absolute Galois group acts on the set of p -power torsion points on an elliptic curve E/\mathbb{Q} . This action can be extended to the Tate module

$$T_p(E) = \varprojlim_n E[p^n].$$

Since $E[p^n] \simeq (\mathbb{Z}/p^n\mathbb{Z})^2$, tensoring $T_p(E)$ with the field \mathbb{Q}_p we obtain a 2-dimensional \mathbb{Q}_p -vector space, and so we have a representation

$$\rho : G_{\mathbb{Q}} \longrightarrow \text{GL}_2(\mathbb{Q}_p).$$

Such representations have been studied and used extensively (see for example [22] for the role they play in the proof of Fermat's last theorem).

Secondly, there is what I call the direct approach. This amounts to chipping away at $G_{\mathbb{Q}}$ by determining large subgroups or large quotients. This is done by choosing number fields and extensions so as to take advantage of certain “extra structure” they might contain. For example

Example 1: A natural quotient of $G_{\mathbb{Q}}$ to consider is $G_{\mathbb{Q}}^{ab}$, the maximal abelian quotient of $G_{\mathbb{Q}}$. This group is the Galois group of the maximal abelian extension \mathbb{Q}^{ab} of \mathbb{Q} . The Kronecker-Weber theorem tells us that every finite abelian extension of \mathbb{Q} is contained in some cyclotomic field $\mathbb{Q}(\zeta_n)$, and hence \mathbb{Q}^{ab} is just the field generated by all roots of unity. Using this, one may then easily prove

$$G_{\mathbb{Q}}^{ab} := G_{\mathbb{Q}}/[G_{\mathbb{Q}}, G_{\mathbb{Q}}] \simeq \prod_p (\mathbb{Z}_p)^{\times},$$

where $[G_{\mathbb{Q}}, G_{\mathbb{Q}}]$ is the closure of the commutator subgroup of $G_{\mathbb{Q}}$, and $(\mathbb{Z}_p)^{\times}$ denotes the multiplicative group of invertible p -adic integers. The “extra structure” in this example is the commutativity.

1.2 The Maximal pro- p , S -ramified Extension

A common type of “extra structure” imposed on an extension of fields is *restricted ramification*. Let S denote a finite set of primes of a number field K (usually chosen to contain the infinite primes, as well as those above some fixed rational prime p). Then one may consider the Galois group of the maximal extension K_S/K unramified outside the set of primes in S (or just “ S -ramified”), denoted G_S .

One may add further structure by looking at just the *pro- p part* of such an extension for some prime p , i.e. the maximal p -ramified pro- p -extension $K_S(p)/K$. The corresponding Galois group, $G_S(p)$, is just the maximal pro- p quotient of G_S .

1.2.1 Koch’s Examples

Explicit descriptions of infinite Galois groups are unlikely to take a form as simple as that appearing in Example 1. Rather, based on cohomological techniques, a description in terms of generators and relations is more likely.

The following examples are due to Koch. The details may be found in Chapter 3, Section 2.6 of [15]. Let K be a number field and S a finite set of primes of K . For each place v in S , we can embed $K_S(p)$ into its completion at a place above v , and we get a corresponding homomorphism of Galois groups

$$\phi_v : G_v(p) \longrightarrow G_S(p),$$

where $G_v(p)$ is the local Galois group; i.e. $G_v(p)$ is the Galois group of $K_S(p)_w/K_v$ where w is a place of $K_S(p)$ above the place v . Using this, one may transfer known local relations in $G_v(p)$ to relations in $G_S(p)$, but in general there may still be unknown

relations in $G_S(p)$. Under certain favorable circumstances it is known that all relations in $G_S(p)$ come from local relations and a complete description of $G_S(p)$ may be given.

Example 2: Let $K = \mathbb{Q}$, $p \neq 2$, and $S = \{p, q\}$, where q is a prime congruent to ± 3 modulo 8. Then $G_S(p)$ has a presentation as a pro- p group with two generators $\{s, t\}$ and a single relation

$$t^{q-1}(t^{-1}, s^{-1}) = 1$$

(where (a, b) denotes the commutator $a^{-1}b^{-1}ab$).

Example 3: Let $K = \mathbb{Q}(\sqrt{-23})$, $p = 3$, and $S = \{\wp_1, \wp_2, q, \wp\}$ where \wp_1 and \wp_2 are the primes of K above 3, q is a prime not congruent to 1 modulo 9, and \wp is a prime of K which is not principal. Then $G_S(3)$ has a presentation as a pro-3 group with 4 generators s_q, s_\wp, t_q, t_\wp , and two relations

$$t_q^{q-1}(t_q^{-1}, s_q^{-1}) = 1,$$

and

$$t_q^{N(\wp)-1}(t_\wp^{-1}, s_\wp^{-1}) = 1.$$

1.2.2 A Linearization in the Case $K = \mathbb{Q}(\zeta_p)$, $S = \{p\}$

The Galois group we wish to consider is of the form $G_S(p)$ but seems, at the moment, immune to the techniques used in obtaining the examples from the last section. Let p be an odd prime and let $K = \mathbb{Q}(\zeta_p)$. Let $S = \{p\}$, where we continue to write p for the unique prime of K above p . To be consistent with the notation used later we will write Ω for the field $K_S(p)$, i.e. the maximal p -ramified pro- p -extension of K , and let \mathcal{G} denote the Galois group of Ω/K .

The group \mathcal{G} has a minimal free presentation

$$1 \longrightarrow R \longrightarrow F_g \longrightarrow \mathcal{G} \longrightarrow 1,$$

where F_g is the free pro- p group on g generators, and R is the normal closure of a topologically finitely generated subgroup. Elements of R give the relations in \mathcal{G} , and we let s denote the minimal number of relations which topologically generate a subgroup whose normal closure is R .

In Section 2.3.1 we give explicit descriptions of the numbers g and s in terms of the p -rank of the ideal class group of K . For example, if p is a regular prime the value of s is shown to be zero, and so the group \mathcal{G} is just a free pro- p group. For irregular primes s is always positive, and so \mathcal{G} is not free. For example, when $p = 37$ the group \mathcal{G} will be defined by 20 generators and a single relation.

The completed group ring $\mathbb{Z}_p[[F_g]]$ admits a derivation (the so called Fox derivative, see Section 4.2) denoted D whose image lands in the augmentation ideal of $\mathbb{Z}_p[[F_g]]$ (see Sections 2.2.1 and 2.4).

In Section 2.4 we will introduce a module Z over the group ring $\mathbb{Z}_p[[\Gamma]]$ where $\Gamma \simeq \mathbb{Z}_p^r$ is the Galois group of a certain sub-extension of Ω/K (the compositum of all \mathbb{Z}_p -extensions of K). The module Z will in fact be a certain quotient of the augmentation ideal of $\mathbb{Z}_p[[\mathcal{G}]]$. This module will have a two-step free resolution

$$0 \longrightarrow \mathbb{Z}_p[[\Gamma]]^s \xrightarrow{\phi} \mathbb{Z}_p[[\Gamma]]^g \longrightarrow Z \longrightarrow 0,$$

where ϕ is induced from the derivation D . More precisely, if w_1, \dots, w_s constitute a minimal set of generating relations for \mathcal{G} in F_g , then ϕ may be completely described in terms of the elements $D(w_i)$. It is this “linearization” of the free presentation of \mathcal{G} that supplies the bridge between the structure of \mathcal{G} and Greenberg’s conjecture.

1.3 Greenberg’s Conjecture

In this section we describe a conjecture of Greenberg concerning the structure of a certain Galois group as a module over an Iwasawa algebra Λ . We describe cases in which the conjecture is known to be true as well as give a reformulation of the conjecture for cyclotomic base fields. It is in this context that the conjecture provides information about the Galois group structures discussed in the previous section. The main result of this thesis will be stated here as well.

1.3.1 The Statement

Let K be a number field and p a prime number. By a *multiple \mathbb{Z}_p -extension of K* we mean a Galois extension K_∞/K with Galois group isomorphic to \mathbb{Z}_p^d , where d is a positive integer (when $d = 1$ we call the extension K_∞/K simply a \mathbb{Z}_p -extension). We consider the multiple \mathbb{Z}_p -extension obtained as follows:

Let K_∞ be the compositum of all \mathbb{Z}_p -extensions of K . Then K_∞/K is a Galois extension with Galois group isomorphic to \mathbb{Z}_p^r for some positive integer r . Let Γ denote this Galois group and $\mathbb{Z}_p[[\Gamma]]$ the corresponding Iwasawa algebra (see Section 2.2). It is well known that this algebra is isomorphic (non-canonically) to the power series ring $\Lambda = \mathbb{Z}_p[[T_1, T_2, \dots, T_r]]$.

Modules over the Iwasawa algebra Λ have been the subject of a large amount of research over the last thirty years beginning with Iwasawa’s beautiful theorem on the growth of the p -part of the class group in a single \mathbb{Z}_p -extension (see Section 2.2). We consider the analogous module for the multiple \mathbb{Z}_p -extension described above. For an intermediate field $K \subset F \subset K_\infty$, let $A(F)$ denote the p -primary part of the ideal class group of F . The action of $\text{Gal}(F/K)$ on $A(F)$ gives $A = \varprojlim_F A(F)$ the structure of a Λ -module. Using class field theory A is identified (as a Λ -module) with the

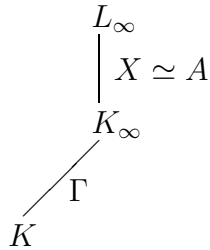


FIGURE 1.1. Field diagram 1

Galois group X of the maximal abelian unramified pro- p -extension of L_∞/K_∞ (see Figure 1.1). The Λ -module structure of X is induced from the conjugation action of Γ on X (see Section 2.2.1). The module X is known to be finitely generated and torsion.

A Λ -module M is said to be *pseudo-null* if its annihilator has height at least 2, or, equivalently, if it is torsion and $\text{Ext}_\Lambda^1(M, \Lambda) = 0$ (see Section 3.1). Greenberg has made the following conjecture (hinted at in [6] and explicitly stated in [7]).

Conjecture 1.3.1 (Greenberg). *Let K_∞ be the compositum of all \mathbb{Z}_p -extensions of a number field K with Galois group Γ . Then the Galois group X of the maximal abelian unramified pro- p -extension of K_∞ is pseudo-null as a module over $\Lambda \simeq \mathbb{Z}_p[[\Gamma]]$.*

When K is totally real and abelian, Leopoldt's conjecture is known to hold. As a consequence we have $r = 1$; i.e. K has just one \mathbb{Z}_p -extension. In this case a module over the Iwasawa algebra $\Lambda = \mathbb{Z}_p[[T]]$ is pseudo-null precisely when it is finite. This is equivalent to the Iwasawa λ invariant attached to the single \mathbb{Z}_p -extension of K (the cyclotomic \mathbb{Z}_p -extension of K) being zero (see Section 2.2). This version of the conjecture has been verified for certain real quadratic fields by Ichimura and Sumida in [8], and Kraft and Schoof in [16], for example.

1.3.2 Greenberg's Conjecture for Cyclotomic Fields

When one takes $\mathbb{Q}(\zeta_p)$, the cyclotomic field of p -th roots of unity, as the ground field K Greenberg's conjecture has a very nice reformulation.

Let M_∞ be the maximal abelian p -ramified pro- p -extension of K_∞ , and let $Y = \text{Gal}(M_\infty/K_\infty)$. The group Y may be made into a module over the Iwasawa algebra Λ in a way analogous to that of X (i.e. via the conjugation action of Γ on Y), and we let Y_{tor} denote the Λ -torsion submodule. In Section 3.1 we establish the following reformulation of Greenberg's conjecture:

$$X \text{ is pseudo-null} \Leftrightarrow Y_{tor} = 0.$$

It was shown by Greenberg (see [6]) under the assumption of Leopoldt's conjecture, and in general by Nguyen-Quang-Do (see [21]), that Y contains no non-trivial pseudo-null submodules, so in fact $Y_{tor} = 0$ if and only if Y_{tor} is pseudo-null.

The connection between the group structure of the Galois group \mathcal{G} introduced in Section 1.2.2 and Greenberg's conjecture follows from this equivalent formulation. The group Z in the linearization of the free presentation of \mathcal{G} is also a Λ -module, and in fact will be shown to be closely related to Y (see Section 2.4). In particular, we will see that

$$Y_{tor} \simeq Z_{tor},$$

and therefore Greenberg's conjecture becomes equivalent to Z being a torsion free Λ -module.

1.3.3 The Main Result

McCallum has verified Greenberg's conjecture for a certain class of cyclotomic fields, namely those of the form $K = \mathbb{Q}(\zeta_p)$, where p is a prime number exactly dividing the class number of K and the Kubota-Leopoldt p -adic L -function attached to K has valuation 1 at $s = 1$ (see [19]). Based on his work, I have tried to approach the problem in terms of the λ invariant attached to the cyclotomic \mathbb{Z}_p -extension of K , which we denote $\lambda(p)$, rather than the divisibility of the class number (the two are conjecturally quite related). Let $L_p(s, \omega^i)$ denote the Kubota-Leopoldt p -adic L -function attached to ω^i , where ω denotes the Teichmüller character. Let B_i denote the i -th Bernoulli number (see Section 2.1.1). Then I have proved

Main Result: *Let p be an odd prime and let $K = \mathbb{Q}(\zeta_p)$. Suppose K satisfies Vandiver's conjecture (i.e. $A(K)^+ = 0$) and $\lambda(p) = 1$. Then, if for each B_{1-i} divisible by p , $3 \leq i \leq p - 2$, the inequality*

$$v_p(L_p(1, \omega^{1-i})) \leq v_p(|\varepsilon_i A(K)|)$$

holds, K satisfies Greenberg's conjecture.

Remark 1. The statement of Vandiver's conjecture is given in Section 2.1.2, as well as many of its consequences. The conjecture has been verified for primes up to 12 million by the authors of [2]. Although it is not generally believed that the conjecture will hold for *all* primes, it is surely a good approximation to the truth.

Remark 2. The computations in [2] have also computed (indirectly) the λ invariant of the cyclotomic \mathbb{Z}_p -extension of $\mathbb{Q}(\zeta_p)$ for primes up to 4 million. In fact, for these primes, $\lambda(p)$ is equal to the index of irregularity of the prime p (see Section 2.1.1). In particular, there seems to be no shortage of cyclotomic fields with λ invariant 1. (Using the tables in the back of [28] we see that 165 of the first 219 irregular primes have $\lambda(p) = 1$, and in general this should be the case for approximately 30% of all primes.)

Remark 3. The assumptions of Vandiver's conjecture and $\lambda(p) = 1$ imply that $A(K) \simeq \mathbb{Z}/p^m\mathbb{Z}$ for some m (see Proposition 2.2.1), and hence there is only one

Bernoulli number B_{1-i} divisible by p for $3 \leq i \leq p-2$ (see Theorem 2.1.2). The inequality condition is equivalent to a condition on the characteristic power series of A (see Theorem 2.2.3). Under these hypothesis we know the characteristic power series to be of the form

$$g(T) = up^m + T,$$

where $u \in \mathbb{Z}_p^\times$. The inequality condition becomes equivalent to the condition that $v_p(g(p)) \leq v_p(|A(K)|)$. If $m > 1$, this condition is automatically satisfied. If $m = 1$ the condition will be satisfied provided u is not -1 modulo p . In [13] the value of u modulo p is checked for primes up to 4001, although tables are given only for $1 < p < 400$ and $3600 < p \leq 4001$. For these primes the condition is satisfied.

The proof of this result will be given in Chapter 3 and will largely follow the proof of McCallum's previous result. The hypothesis on λ at present seems hard to weaken. In Chapter 4 we will mention a computational approach to the problem which might lend itself better to λ values greater than 1 (as well as provide a simpler proof of the case $\lambda = 1$).

1.3.4 Greenberg's Conjecture and \mathcal{G}

In the previous sections of this chapter a connection was explained between the structure of the Galois group \mathcal{G} and Greenberg's conjecture for $\mathbb{Q}(\zeta_p)$. We should try to point out what exactly one problem says about the other.

Let us suppose we are able to determine the structure of \mathcal{G} by explicitly describing a minimal generating set of relations. Using the differential calculus of Fox we could then explicitly describe the map ϕ occurring in the sequence

$$0 \longrightarrow \Lambda^s \xrightarrow{\phi} \Lambda^g \longrightarrow Z \longrightarrow 0.$$

But as we have stated, Greenberg's conjecture becomes equivalent to the Λ -torsion sub-module of Z being 0, which could easily then be checked.

What, on the other hand, does knowledge of Greenberg's conjecture for K say about the structure of \mathcal{G} ? The question of the existence of free pro- p extensions (i.e., Galois extensions with free pro- p Galois groups) has been brought up by several authors (see the papers of Wingberg [29], and Yamagishi [30], [31], for example). Such extensions have been shown to be p -ramified, and therefore are contained in the maximal p -ramified pro- p extension. Greenberg's conjecture for cyclotomic fields would imply the non-existence of free pro- p extensions of maximal rank, i.e., that \mathcal{G} would have no free pro- p quotients of maximal rank (the maximal rank is $g-s$, where g and s are as in Section 1.2.2). It has been believed by some authors that such extensions should exist (see [31] for example). This consequence will be explained further in Section 4.1.

Does Greenberg's conjecture give any information about the relations in \mathcal{G} ? This is not so clear. It may give indications about the complexity of the relations (i.e. how far down in the descending central q -series they lie; see Section 2.3.2). In particular, it would imply that any relations inducing torsion in Z (via the linearization above) could not exist. In Section 4.2 we look at some Fox derivative computations to try and shed more light on this question.

Chapter 2

BACKGROUND

In this chapter we review many of the facts and constructions needed for a full understanding of both the statement of Greenberg's conjecture as well as the proof in Chapter 3 of the main result.

The main reference for Sections 2.1 and 2.2 are the text of Washington [28], as well as that of Lang [18]. For more details on the content of Section 2.4 see [21]. The content of Section 2.3 seems to be folklore, although I found no single source containing the derivations given here (Section 13.1 of [28] was helpful for the details of Section 2.3.2).

Some needed background topics have been omitted, but are used frequently here, including continuous Galois cohomology of pro-finite groups and class field theory. Details on the former subject can be found in the wonderful new text [20], as well as in [26], and for the latter one could consult [3] for example.

2.1 Cyclotomic Fields and Vandiver's Conjecture

Here we review some of the basic facts concerning class numbers of cyclotomic fields. Vandiver's conjecture is also stated. The connections between (p -primary parts of) class groups, Vandiver's conjecture, and Iwasawa's λ invariants are largely conjectural, but as we will see, for primes up to 4 million, we have

$$p\text{-rank of the class group} = i(p) = \lambda(p),$$

where $i(p)$ denotes the index of irregularity of p (see below) and $\lambda(p)$ denotes the λ invariant of the cyclotomic \mathbb{Z}_p -extension of $\mathbb{Q}(\zeta_p)$ (see Section 2.2).

2.1.1 Cyclotomic Fields and Class Numbers

We let p be an odd prime number and let ζ_p denote a fixed primitive p -th root of unity. The field $K = \mathbb{Q}(\zeta_p)$ is called the cyclotomic field of p -th roots of unity. It is a Galois extension of \mathbb{Q} with Galois group isomorphic to $(\mathbb{Z}/p\mathbb{Z})^\times$ (which is a cyclic group of order $p - 1$).

We let C denote the ideal class group of K and h the class number (i.e. $h = \#(C)$). The group C is a finite abelian group and we let A denote its p -primary part (which is just the Sylow p -subgroup).

We let K^+ denote the maximal real subfield of K . It may be obtained from \mathbb{Q} by adjoining $\zeta_p + \zeta_p^{-1}$. The class group and class number of K^+ are denoted C^+ and h^+

respectively. In Chapter 4 of [28] it is shown that the natural map

$$C^+ \longrightarrow C$$

is an injection, and so in particular one has that h^+ divides h , and we define h^- as the quotient (called the *relative class number*).

For the fields $K = \mathbb{Q}(\zeta_p)$ we are often interested in the p -divisibility of the various class numbers above. We say that a prime p is *irregular* if p divides h (otherwise we say p is regular). The first few irregular primes are 37, 59, 67, 101, 103, 131, 149, and 157. There are known to be infinitely many irregular primes, but the same statement for regular primes is still unproven.

The following result is known as the *Kummer criterion* for irregular primes (see Chapter 5 of [28] for a proof). We let B_n denote the n -th Bernoulli number, defined by the expansion

$$\frac{t}{e^t - 1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!}.$$

Theorem 2.1.1. *Let h and B_n be as above. Then p divides h if and only if p divides B_n for some $n = 2, 4, \dots, p-3$.*

The number of B_n divisible by p in the theorem is called the index of irregularity of p , denoted $i(p)$ (for the irregular primes listed above, all have $i(p) = 1$ except 157, which has index of irregularity 2). Herbrand's Theorem together with Ribet's converse, given in Theorem 2.1.2 below, provides a nice refinement of Kummer's criterion.

As above, let A denote the p -primary part of C . There is an action of the group $\Delta = \text{Gal}(K/\mathbb{Q})$ on A , making A into a module over the group ring $\mathbb{Z}_p[\Delta]$. For each i , $0 \leq i \leq p-2$, let

$$\varepsilon_i = \frac{1}{p-1} \sum_{\sigma \in \Delta} \omega^i(\sigma) \sigma^{-1},$$

where ω is the cyclotomic character. The ε_i are the orthogonal idempotents of the group ring $\mathbb{Z}_p[\Delta]$ (see Chapter 6 of [28]). These elements may be used to decompose A into eigenspaces for the action of Δ ; that is, we have

$$A \simeq \bigoplus_{i=0}^{p-2} A_i,$$

where $A_i = \varepsilon_i A$. Then for $\sigma \in \Delta$, A_i is the eigenspace with eigenvalue $\omega^i(\sigma)$. By grouping together even terms and odd terms we will also write the decomposition in the form

$$A = A^- \oplus A^+,$$

where A^- is the sum over the odd terms, and A^+ is the sum over the even (this is just the idempotent decomposition corresponding to the action of $\text{Gal}(K/K^+)$, which is a group of order 2). The subgroup A^+ is the image of the ideal class group of K^+ under the map induced by extension of ideals. Then we have

Theorem 2.1.2. $A_0 = A_1 = 0$. For i odd, $3 \leq i \leq p-2$, $A_i \neq 0$ if and only if p divides B_{p-i} .

This result gives a “piece by piece” picture of Kummer’s criterion. In particular, we have *the p -rank of A is at least $i(p)$* . Putting the two theorems together also gives $p|h \Leftrightarrow p|h^-$.

2.1.2 Vandiver’s Conjecture

We state Vandiver’s conjecture here and describe some of its consequences. We also give a heuristic argument as to why it should hold for most primes. The conjecture was first made by Kummer in a letter to Kronecker (see Kummer’s *Collected Works*, Vol. I, pg. 85). We retain the notation h, h^+ of the last section.

Vandiver’s Conjecture. p does not divide h^+ (i.e. $A^+ = 0$).

In Section 2.2.2 we will see that for cyclotomic fields with λ invariant equal to 1, satisfying Vandiver’s conjecture is equivalent to having a cyclic p -class group. Based on the results of the last section, such a cyclic group would have to lie completely in either A^+ or A^- . But since $p|h \Leftrightarrow p|h^-$, it must be the case that $A = A^-$, and so $A^+ = 0$. The opposite direction is part of Proposition 2.2.1.

The conjecture has many favorable consequences and the interested reader should consult [28], especially Chapters 8 and 10. The first consequence we state implies equality between the p -rank of A and $i(p)$, the index of irregularity of p .

Theorem 2.1.3. Suppose p does not divide h^+ . Then each A_i in the idempotent decomposition of A is cyclic.

This is a specific case of Theorem 10.14 of [28]. If each A_i is cyclic, then the number of non-zero terms in the idempotent decomposition (which is the index of irregularity) is exactly the p -rank of A .

The main consequences of Vandiver’s conjecture needed for the proof of our main result are given below in Theorems 2.2.3 and 2.2.5, and Proposition 2.2.1.

The following heuristic argument for why Vandiver’s conjecture should be at least a close approximation to the truth is given in [28]. Suppose we assume the values of h^+ , as p varies, are randomly distributed modulo p (which may not be a reasonable thing to do). In other words, suppose p divides h^+ with probability $1/p$. Then the number of exceptions to Vandiver’s conjecture for $p \leq x$ should approximately be

$$\sum_{p \leq x} \frac{1}{p} \sim \log \log(x).$$

Since $\log \log(4000000) \approx 2.72$, it's not that surprising that no exceptions have been found. For a more sophisticated argument, in which one obtains the approximation $1/2 \log \log(x)$, see Section 8.3 of [28].

2.2 \mathbb{Z}_p -extensions and Iwasawa's Theorem

The theory of \mathbb{Z}_p -extensions originated in Iwasawa's paper [10], although more modern treatments may be found in [11], [28], [20], and [18]. These references should be consulted for more details of what follows. Let K be a number field. As in Section 1.3.1 we define a \mathbb{Z}_p -extension K_∞/K to be a Galois extension with Galois group $\Gamma \simeq \mathbb{Z}_p$, the additive group of p -adic integers. Applying the Galois correspondence it is easily seen that such an extension is equivalent to a unique infinite tower of fields

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_\infty := \bigcup_n K_n, \quad (2.1)$$

with $\text{Gal}(K_n/K) \simeq \mathbb{Z}/p^n\mathbb{Z}$ (this tower corresponds to the chain of closed subgroups of the form $p^n\mathbb{Z}_p$). We claim such extensions are abundant. In fact, if r_2 denotes the number of pairs of complex embeddings of K into \mathbb{C} , then it is known that K has at least $r_2 + 1$ independent \mathbb{Z}_p -extensions (Leopoldt's conjecture implies exactly $r_2 + 1$). Consider the following construction.

Let ζ_{p^n} denote a primitive p^n -th root of unity. Since

$$\text{Gal}(\mathbb{Q}(\zeta_{p^{n+1}})/\mathbb{Q}(\zeta_p)) \simeq \mathbb{Z}/p^n\mathbb{Z},$$

the archetypical \mathbb{Z}_p -extension is given by

$$\mathbb{Q}(\zeta_p) \subset \mathbb{Q}(\zeta_{p^2}) \subset \cdots \subset \mathbb{Q}(\zeta_{p^n}) \subset \cdots \subset \mathbb{Q}(\zeta_{p^\infty}) := \bigcup_n \mathbb{Q}(\zeta_{p^n}).$$

We can construct a \mathbb{Z}_p -extension of $\mathbb{Q}_\infty/\mathbb{Q}$ by considering the extension $\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}$. Since $\text{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) \simeq (\mathbb{Z}/p^n\mathbb{Z})^\times$, we have

$$\begin{aligned} \text{Gal}(K_\infty/\mathbb{Q}) &\simeq \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})^\times \\ &\simeq (\mathbb{Z}_p)^\times \\ &\simeq \mathbb{Z}_p \oplus (\mathbb{Z}/p\mathbb{Z})^\times. \end{aligned}$$

Now let \mathbb{Q}_∞ be the fixed field of $(\mathbb{Z}/p\mathbb{Z})^\times$.

If K is any other number field the extension $K\mathbb{Q}_\infty/K$ will then be a \mathbb{Z}_p -extension. This particular extension is called the *cyclotomic* \mathbb{Z}_p -extension of K .

2.2.1 Iwasawa's Theorem

In this section we introduce a theorem of Iwasawa describing the growth of the p -part of the ideal class group in a \mathbb{Z}_p -extension. In particular, this allows us to introduce Iwasawa's λ invariant.

We let

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_\infty = \bigcup_n K_n \quad (2.2)$$

be a \mathbb{Z}_p -extension and let X be the Galois group of the maximal abelian unramified pro- p -extension L_∞/K_∞ . Then we have an isomorphism $X \simeq \varprojlim_n X_n$, where X_n is the Galois group of the maximal abelian unramified p -extension of K_n , say L_n . By class field theory, X_n is also isomorphic to the p -primary part of the ideal class group of K_n which we denote A_n .

The Galois group $\text{Gal}(K_n/K)$ acts on X_n as follows: let $\gamma \in \text{Gal}(K_n/K)$, and let $x \in X_n$. Extend γ to $\tilde{\gamma} \in \text{Gal}(L_n/K)$. Then γ acts on x by

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

The fact that this action is well-defined (i.e. independent of the extension of γ to $\tilde{\gamma}$) follows from X_n being abelian. Further, since X_n is a p -group we may extend this action, making X_n into a module over the group ring $\mathbb{Z}_p[\text{Gal}(K_n/K)]$. This action makes X_n and A_n isomorphic as *Galois modules*, where A_n is given the usual action of $\text{Gal}(K_n/K)$.

If we then use the compatibility of the X_n , we obtain an action of the *completed group ring*

$$\mathbb{Z}_p[[\Gamma]] := \varprojlim_n \mathbb{Z}_p[\text{Gal}(K_n/K)]$$

on the group X (as well as the group $\varprojlim_n A_n$). It is well known that $\mathbb{Z}_p[[\Gamma]]$ is non-canonically isomorphic to the power series ring $\Lambda = \mathbb{Z}_p[[T]]$, such that a topological generator γ of the completed group ring is sent to $1 + T$ (see Theorem 7.1 of [28]).

We define a *pseudo-isomorphism* of Λ -modules to be a Λ -module homomorphism with pseudo-null kernel and cokernel. (Note, for $\Lambda = \mathbb{Z}_p[[T]]$, pseudo-null is equivalent to finite.) Iwasawa proved the following result about the structure of the Λ -module X .

Theorem 2.2.1 (Iwasawa, [10]). *There is a pseudo-isomorphism of Λ -modules*

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

where each $g_j(T)$ is a monic polynomial. Further, if we take $\lambda = \sum \deg g_j$, and $\mu = \sum k_i$, then for all $n > n_0$

$$\# |X_n| = p^{\lambda n + \mu p^n + c},$$

where c and n_0 are constants that only depend on the extension K_∞/K .

The first part of the theorem follows from a general structure theorem for finitely generated Λ -modules. The formula for the order of X_n is derived by giving explicit descriptions of Λ -submodules Y_n such that

$$X_n \simeq X/Y_n.$$

The details of the full proof of the theorem can be found in Chapter 13 of [28].

The constants λ and μ are called the *Iwasawa invariants* of the extension K_∞/K . We will make use of the following theorem of Ferrero and Washington (see [4] for a proof).

Theorem 2.2.2. *Let K be an abelian extension of \mathbb{Q} . Then the Iwasawa μ -invariant of the cyclotomic \mathbb{Z}_p -extension of K is 0.*

2.2.2 \mathbb{Z}_p -extensions of $\mathbb{Q}(\zeta_p)$

In Iwasawa's theorem there are two aspects that make detailed computations potentially difficult. The first is the fact that the structure of X is given only up to *pseudo-isomorphism*, i.e. a module homomorphism with finite kernel and co-kernel. The second is the fact that the equation for the order of X_n only holds after a certain level in the \mathbb{Z}_p -tower.

When one takes the cyclotomic \mathbb{Z}_p -extension of a cyclotomic field $\mathbb{Q}(\zeta_p)$, and assumes Vandiver's conjecture, these difficulties subside. More specifically, we have the following two results.

Theorem 2.2.3. *Assume Vandiver's conjecture holds for $\mathbb{Q}(\zeta_p)$. Then, for $i = 3, 5, \dots, p-2$, one has*

$$\varepsilon_i X \simeq \mathbb{Z}_p[[T]]/f(T, \omega^{1-i})$$

where $f((1+p)^s - 1, \omega^{1-i}) = L_p(s, \omega^{1-i})$.

This is essentially Theorem 10.16 of [28]. The polynomial $f(T, \omega^{1-i})$ is called the *characteristic power series* of $\varepsilon_i X$. It has many interesting arithmetic properties. In particular, it is the subject of the so-called Main Conjecture of Iwasawa theory, relating f to the p -adic L -function $L_p(s, \omega^{1-i})$. One interpretation of Greenberg's conjecture is that there is no simple analogue of the characteristic power series in the multivariable case (since the annihilator of X would have at least *two* independent generators).

Theorem 2.2.4. *For the \mathbb{Z}_p -extension $\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}(\zeta_p)$ one has*

$$X_n \simeq X/((1+T)^{p^n} - 1)X$$

for all $n \geq 0$.

In other words, for the cyclotomic \mathbb{Z}_p -extension of $\mathbb{Q}(\zeta_p)$ we have a rather explicit description of X as well as the submodules Y_n . This is a consequence of the proof of Theorem 2.2.1. See Proposition 13.22 of [28].

The main result of this dissertation considers cyclotomic fields of p -th roots of unity for which the Iwasawa λ -invariant of the cyclotomic \mathbb{Z}_p -extension is one. For each $n \geq 0$ write K_n for the field $\mathbb{Q}(\zeta_{p^{n+1}})$ and $K_\infty = \cup_n K_n$. Recall the notation X_n for the Galois group of the maximal abelian unramified p -extension of K_n (which is isomorphic to A_n , the p -primary part of the class group of K_n). Then, in light of the results stated in this section and the last, we have the following.

Proposition 2.2.1. *Suppose $K = K_0$ satisfies Vandiver's conjecture. If the Iwasawa λ -invariant of the cyclotomic \mathbb{Z}_p -extension K_∞/K_0 is 1, then the p -primary part of the ideal class group of K_0 is cyclic, say of order p^m . Further, for all $n > 0$, we have*

$$X_n \simeq \mathbb{Z}/p^{m+n}\mathbb{Z},$$

and the natural map from $X_0 \rightarrow X_n$ is injective for all n .

Proof: For the first part of the proposition we make use of Theorem 2.2.4, which gives the isomorphism

$$X_0 \simeq X/TX,$$

where X is described in Theorem 2.2.3. Since $\lambda = 1$ we know $X = \varepsilon_i X$ for some i (recall the definition of λ in Theorem 2.2.1), and in fact we have

$$X \simeq \mathbb{Z}_p[[T]]/(T + p^m),$$

for some m , and so we immediately obtain the first part of the proposition, namely $X_0 \simeq \mathbb{Z}/p^m\mathbb{Z}$.

Similarly,

$$X_n \simeq X/((1 + T)^{p^n} - 1)X \tag{2.3}$$

will clearly be cyclic, and using the formula for the order of X_n given in Theorem 2.2.1 (with $\lambda = 1$, $\mu = 0$, and $c = m$) we have

$$X_n \simeq \mathbb{Z}/p^{m+n}\mathbb{Z}.$$

(The order could also be computed directly from (2.3).)

For the last part of the proposition, we consider the capitulation map on the p -primary part of class groups

$$A_0 \longrightarrow A_n,$$

rather than the map of Galois groups. The kernel of this map may be computed by considering the exact sequence

$$0 \longrightarrow E_n \longrightarrow K_n^\times \longrightarrow P_n \longrightarrow 0, \quad (2.4)$$

where E_n is the unit group of K_n , and P_n is the group of principal fractional ideals of K_n . An ideal class of A_0 which becomes principal in A_n may be obtained by looking at the principal ideals of K_n which are fixed by $G = \text{Gal}(K_n/K_0)$. More precisely, a principal ideal (a) of K_n which is fixed by the action of G must be of the form

$$(a) = I(\pi)^e,$$

where (π) is the unique prime in K_n/K_0 above p (and the only ramified prime in K_n/K_0), and I is an ideal from K_0 .

Since the unique ramified prime in K_n/K_0 is already principal, the ideal classes of K_0 which become principal classes in K_n are determined modulo $(K_0)^\times$ by those principal ideals of K_n fixed by G . Taking cohomology of (2.4) with respect to G , we obtain

$$0 \rightarrow E_0 \rightarrow K_0^\times \rightarrow H^0(G, P_n) \rightarrow H^1(G, E_n) \rightarrow 0,$$

and so we see that the kernel of $A_0 \rightarrow A_n$ is precisely given by

$$H^1(G, E_n) = H^1(G, E_n)^- \oplus H^1(G, E_n)^+.$$

Since all of the above maps are Δ -equivariant, Vandiver's conjecture implies

$$H^1(G, E_n)^+ = 0,$$

and so we need only consider the group $H^1(G, E_n)^-$. Since $\text{Gal}(K_n/\mathbb{Q})$ is abelian the group $\text{Gal}(K_0/\mathbb{Q})$ acts trivially on G , and hence

$$H^1(G, E_n)^- = H^1(G, E_n^-).$$

But since every unit of K_n is the product of a real unit and a root of unity (see Corollary 4.13 of [28]), $E_n^- = \mu_{p^{n+1}}$, the group of roots of unity in K_n , and $H^1(G, \mu_{p^{n+1}})$ is 0 (see Lemma 13.27 of [28] for example). \square

We state one more consequence of Vandiver's conjecture needed for Chapter 3. The maximal abelian unramified extension H of a number field K is called the *Hilbert class field* of K . The extension is finite, and it is a well known result of class field theory that the Galois group of H over K is isomorphic to the class group of K . Similarly, the maximal abelian unramified p -extension is called the p -Hilbert class field. Its Galois group is isomorphic to the p -primary part of the class group of K .

An important (deep) result regarding the Hilbert class field is that all ideal classes of K become principal classes when extended to H (and similarly, all ideal classes of p -power order become principal when extended to the p -Hilbert class field). This fact is used in Section 3.2 in conjunction with the following.

Theorem 2.2.5. *Suppose $K = \mathbb{Q}(\zeta_p)$ satisfies Vandiver's conjecture. Then the p -Hilbert class field of K is contained in the compositum of all \mathbb{Z}_p -extensions of K .*

We will restate this result in Section 2.3.2 where it follows as a consequence from the proof of Theorem 2.3.2.

Finally, we conclude with some information about the Iwasawa invariants of a cyclotomic field $K = \mathbb{Q}(\zeta_p)$. Since K is abelian over \mathbb{Q} the μ invariant is zero by Theorem 2.2.2. We denote the λ invariant by $\lambda(p)$. Let $i(p)$ denote the index of irregularity of p . Washington has given a probability argument (see the appendix to Chapter 10 of [18]) indicating that for all but finitely many primes p it should be the case that

$$i(p) \leq \lambda(p) \leq i(p) + 1.$$

Further, for most primes it should be the case that $\lambda(p) = i(p)$. This equality is known to hold for primes up to 4 million. We now consider the probability that $i(p) = k$. The following argument and table is reproduced from [28]. There are $(p-3)/2$ Bernoulli numbers to consider for a prime p , so if we assume that B_j is divisible by p with probability $\frac{1}{p}$ (i.e. the Bernoulli numbers are randomly distributed modulo p), then the probability that $i(p) = k$ is given by

$$\binom{\frac{p-3}{2}}{k} \left(1 - \frac{1}{p}\right)^{\frac{1}{2}(p-3)-k} \left(\frac{1}{p}\right)^k.$$

As $p \rightarrow \infty$, this value approaches $(\frac{1}{2})^k e^{-1/2}/k!$. In particular, this indicates that approximately $e^{-1/2} \sim 60.65\%$ of all primes should be regular (i.e. $i(p) = 0$). Table 2.1 gives the percentages for the 283145 odd primes less than 4 million (taken from the computations done for [2]) together with the predicted value above.

$i(p)$	Experimental percentage	$(\frac{1}{2})^k e^{-1/2}/k!$
0	.605866	.606531
1	.303862	.303265
2	.076014	.075816
3	.012478	.012636
4	.001558	.001580
5	.000194	.000158
6	.000025	.000013
7	.000004	.000001

TABLE 2.1. Experimental and predicted indexes of irregularity

So in particular, approximately 30% of all primes should have $\lambda(p) = 1$.

2.3 The Maximal Pro- p , p -ramified Extension of $\mathbb{Q}(\zeta_p)$

We now return to consider more closely the Galois group introduced in Section 1.2.2 in the particular case that the base field is the cyclotomic field $K = \mathbb{Q}(\zeta_p)$. We will first determine explicit formulae for the minimal number of generators and relations of \mathcal{G} . Secondly, using class field theory, we describe the structure of the maximal abelian quotient of \mathcal{G} .

2.3.1 Generators and Relations

We will make use of the machinery of continuous Galois cohomology of pro-finite groups, and so the reader may wish to consult [20]. For the duration of this section we fix the following notation:

- K : $\mathbb{Q}(\zeta_p)$
- Ω : the maximal p -ramified pro- p -extension of K .
- \mathcal{G} : $\text{Gal}(\Omega/K)$.
- Ω' : the maximal p -ramified extension of K .
- \mathcal{G}' : $\text{Gal}(\Omega'/K)$.
- $C(L)$: the ideal class group of a number field L .
- μ_p : the group of p -th roots of unity.

It is well known that the group \mathcal{G} has cohomological dimension equal to 2 (see [26]), and so has a minimal free presentation

$$1 \rightarrow R \rightarrow F_g \rightarrow \mathcal{G} \rightarrow 1,$$

where F_g is the free pro- p group on g generators and R is the normal closure of a finitely generated subgroup of F_g (the group of relations for \mathcal{G}). We denote the minimal number of (topological) generators of R by s . It is shown in [26] that the quantities g and s are given by the \mathbb{F}_p -dimensions of the vector spaces $H^i(\mathcal{G}, \mathbb{Z}/p\mathbb{Z})$ for $i = 1, 2$ respectively ($\mathbb{Z}/p\mathbb{Z}$ is given the trivial \mathcal{G} action).

Our main goal in this section is to compute the numbers g and s in terms of the p -rank of the p -primary part of $C(K)$ which we denote a . This is accomplished by computing the dimensions of the cohomology groups above. Since K contains the set μ_p , and \mathcal{G} is the maximal pro- p quotient of \mathcal{G}' , we have

$$H^i(\mathcal{G}, \mathbb{Z}/p\mathbb{Z}) \simeq H^i(\mathcal{G}', \mu_p).$$

We will compute the \mathbb{F}_p -dimensions of the latter groups.

Theorem 2.3.1. *The minimal number of generators g and relations s of the Galois group of the maximal p -ramified pro- p -extension of K are given by*

$$g = \frac{p+1}{2} + a$$

and

$$s = a.$$

The proof of this result will follow from a detailed analysis of the following exact sequence of \mathcal{G} -modules

$$1 \longrightarrow \mu_p \longrightarrow \mathcal{O}_{\Omega'}[1/p]^{\times} \xrightarrow{p} \mathcal{O}_{\Omega'}[1/p]^{\times} \longrightarrow 1.$$

The p -power map on $\mathcal{O}_{\Omega'}[1/p]^{\times}$ is surjective by the maximality of Ω' over K , i.e. since p -th roots of p -units generate p -ramified extensions. Taking cohomology of the sequence with respect to the Galois group \mathcal{G}' yields a long exact sequence which may be broken into the following pair of short exact sequences.

$$0 \longrightarrow \frac{\mathcal{O}_K[1/p]^{\times}}{(\mathcal{O}_K[1/p]^{\times})^p} \longrightarrow H^1(\mathcal{G}', \mu_p) \longrightarrow H^1(\mathcal{G}', \mathcal{O}_{\Omega'}[1/p]^{\times})[p] \longrightarrow 0 \quad (2.5)$$

$$0 \longrightarrow \frac{H^1(\mathcal{G}', \mathcal{O}_{\Omega'}[1/p]^{\times})}{pH^1(\mathcal{G}', \mathcal{O}_{\Omega'}[1/p]^{\times})} \longrightarrow H^2(\mathcal{G}', \mu_p) \longrightarrow H^2(\mathcal{G}', \mathcal{O}_{\Omega'}[1/p]^{\times})[p] \longrightarrow 0. \quad (2.6)$$

Lemma 2.3.1. *For K , Ω' , and \mathcal{G}' as above, we have*

$$H^1(\mathcal{G}', \mathcal{O}_{\Omega'}[1/p]^{\times}) \simeq C(K).$$

Proof: Consider the exact sequence of groups

$$0 \longrightarrow \mathcal{O}_{\Omega'}[1/p]^{\times} \longrightarrow (\Omega')^{\times} \longrightarrow P'_{\Omega'} \longrightarrow 0, \quad (2.7)$$

where $P'_{\Omega'}$ is the set of principal ideals of Ω' supported away from p . Taking cohomology with respect to the Galois group \mathcal{G}' , and using the fact that $H^1(\mathcal{G}', (\Omega')^{\times}) = 0$ by Hilbert's 90, we obtain the exact sequence

$$0 \longrightarrow \mathcal{O}_K[1/p]^{\times} \longrightarrow K^{\times} \longrightarrow (P'_{\Omega'})^{\mathcal{G}'} \longrightarrow H^1(\mathcal{G}', \mathcal{O}_{\Omega'}[1/p]^{\times}) \longrightarrow 0.$$

We claim the group $(P'_{\Omega'})^{\mathcal{G}'}$ may be identified with the set I'_K of ideals of K supported away from p . This is the case since Ω' contains the Hilbert class field of K and therefore all ideals of K become principal in Ω' . So we have

$$H^1(\mathcal{G}', \mathcal{O}_{\Omega'}[1/p]^{\times}) \simeq I'_K/P'_K,$$

which is the class group of K since the primes of K above p are principal. \square

We will need to continue the exact sequence of cohomology obtained from sequence (2.7) in the previous proof. The following lemma determines the next term.

Lemma 2.3.2. *With $P'_{\Omega'}$ as above, we have*

$$H^1(\mathcal{G}', P'_{\Omega'}) = 0.$$

Proof: We write F_i for an intermediate finite Galois extension of K contained in Ω' , and G_i for $\text{Gal}(F_i/K)$. Then since $\mathcal{G}' = \varprojlim_i G_i$ and $P'_{\Omega'} = \varinjlim_i P'_{F_i}$, we have

$$\begin{aligned} H^1(\mathcal{G}', P'_{\Omega'}) &= \varinjlim_i H^1(G_i, P'_{F_i}) \\ &= \varinjlim_i H^1(G_i, I'_{F_i}), \end{aligned}$$

where I'_{F_i} is the set of all ideals of F_i supported away from p . The last equality is seen as follows. Consider the exact sequence

$$0 \longrightarrow P'_{F_i} \longrightarrow I'_{F_i} \longrightarrow C'_{F_i} \longrightarrow 0,$$

where C'_{F_i} is the ideal class group of F_i away from p . Taking cohomology and direct limits we obtain

$$\cdots \rightarrow \varinjlim_i H^{j-1}(C'_{F_i}) \rightarrow \varinjlim_i H^j(P'_{F_i}) \rightarrow \varinjlim_i H^j(I'_{F_i}) \rightarrow \varinjlim_i H^j(C'_{F_i}) \rightarrow \cdots.$$

Since the Hilbert class field of each F_i is contained in the field Ω' , the extension of the C'_{F_i} are eventually 0 making each $\varinjlim_i H^j(G_i, C'_{F_i}) = 0$. The desired equality then follows.

We now show that $H^1(G_i, I'_{F_i}) = 0$. The group I'_{F_i} may be decomposed as a direct sum over the prime ideals of K , and so we obtain

$$\begin{aligned} H^1(G_i, I'_{F_i}) &\simeq \bigoplus_{\mathfrak{p}} H^1(G_i, \mathbb{Z}[I'_{\mathfrak{p}}]) \\ &\simeq \bigoplus_{\mathfrak{p}} H^1(G_i, \mathbb{Z}[G_i/D_{\mathfrak{p}}]), \end{aligned}$$

where $D_{\mathfrak{p}}$ is a decomposition group for \mathfrak{p} and $G_i/D_{\mathfrak{p}}$ is the set of cosets. But the group ring $\mathbb{Z}[G_i/D_{\mathfrak{p}}]$ is the induced module $\text{Ind}_{D_{\mathfrak{p}}}^{G_i} \mathbb{Z}$, and so Shapiro's lemma gives

$$H^1(G_i, I'_{F_i}) \simeq \bigoplus_{\mathfrak{p}} H^1(D_{\mathfrak{p}}, \mathbb{Z}),$$

and these last terms are clearly 0. \square

Lemma 2.3.3. *For Ω' and \mathcal{G}' as above, we have*

$$H^2(\mathcal{G}', \mathcal{O}_{\Omega'}[1/p]^{\times})[p] = 0.$$

Proof: We will in fact show the whole group $H^2(\mathcal{G}', \mathcal{O}_{\Omega'}[1/p]^\times)$ to be zero. Continuing the exact sequence of cohomology obtained from sequence (2.7) and using lemma 2.3.2 we have

$$0 \rightarrow H^2(\mathcal{G}', \mathcal{O}_{\Omega'}[1/p]^\times) \rightarrow H^2(\mathcal{G}', (\Omega')^\times) \rightarrow \dots \quad (2.8)$$

Using Theorem 3 of Chapter 5 of [3] for example, we may identify $H^2(\mathcal{G}', (\Omega')^\times)$ with a subgroup of the Brauer group of K , $B(K)$, and so we have an injection

$$H^2(\mathcal{G}', \mathcal{O}_{\Omega'}[1/p]^\times) \hookrightarrow B(K).$$

We will now make use of the well known exact sequence arising from the cohomology theory of ideles (see Proposition 7.3 and Section 11 of [3]).

Denote by K_v the completion of K at a place v , and $B(K_v)$ the local Brauer group. It is well known that the group $B(K_v)$ is isomorphic to the torsion group \mathbb{Q}/\mathbb{Z} via the so called *invariant* map, and one has an exact sequence

$$0 \rightarrow B(K) \rightarrow \bigoplus_v B(K_v) \xrightarrow{\sum \text{inv}} \mathbb{Q}/\mathbb{Z} \rightarrow 0. \quad (2.9)$$

For each place v of K not dividing p , the subgroup $H^2(\mathcal{G}', \mathcal{O}_{\Omega'}[1/p]^\times)$ of $B(K)$ is mapped into the group $H^2(\Omega'_v/K_v, \mathcal{O}_{\Omega'_v}) \subset B(K_v)$. Since v is an unramified place, this group is zero (see section 3 of Chapter 12 of [24]). There is only one place of K which is ramified in Ω'/K , namely the unique place of K above p . But for an $\alpha \in B(K)$, by the exactness of the sequence (2.9), it must be the case that $\sum_v \text{inv}(\alpha) = 0$. This forces the image at the place above p to also be zero, and hence we have $H^2(\mathcal{G}', \mathcal{O}_{\Omega'}[1/p]^\times)$ injecting into the zero subgroup of $\bigoplus_v B(K_v)$. \square

Proof of Theorem 2.3.1: We return now to our computations of g and s . Recall that h denotes the \mathbb{F}_p -dimension of $C(K)/pC(K)$, which is equal to the \mathbb{F}_p -dimension of $C(K)[p]$, the p -torsion of $C(K)$. An application of the unit theorem tells us that the \mathbb{F}_p -dimension of $\mathcal{O}_K[1/p]^\times/(\mathcal{O}_K[1/p]^\times)^p$ is $\frac{p-1}{2} + 1$. Since the rank of $H^1(\mathcal{G}', \mathcal{O}_{\Omega'}[1/p]^\times)[p]$ is a , (2.5) gives us

$$g = \dim_{\mathbb{F}_p} H^1(\mathcal{G}', \mu_p) = \frac{p+1}{2} + a.$$

It follows immediately from the above lemmas and sequence (2.6) that $s = a$. \square

2.3.2 The Structure of \mathcal{G}^{ab}

The proof of our main result in Chapter 3 will require the determination of the maximal abelian quotient of the Galois group \mathcal{G} , which we denote \mathcal{G}^{ab} . So \mathcal{G}^{ab} is the Galois group of the maximal abelian extension of $K = \mathbb{Q}(\zeta_p)$ contained in Ω , which we denote K^{ab} . Let A denote the p -primary part of the ideal class group of K , and assume Vandiver's conjecture holds for K .

Theorem 2.3.2. *Let \mathcal{G} be the Galois group of the maximal p -ramified pro- p -extension of $K = \mathbb{Q}(\zeta_p)$. Then \mathcal{G}^{ab} has \mathbb{Z}_p -rank $r_2 + 1$. Further, if K satisfies Vandiver's conjecture, we have*

$$\mathcal{G}_{\text{tor}}^{ab} \simeq \bigoplus_{i=2}^{p-3} \mathbb{Z}/p^{a_i}\mathbb{Z},$$

where the sum is taken over the even indices and $a_i = v_p(L_p(1, \omega^i))$.

Proof: We let J_K denote the idele group of K , i.e.

$$J_K = \{(x_v) \in \prod_v K_v^\times \mid x_v \in U_v \text{ for almost all } v\},$$

where K_v is the completion of K at a place v , and U_v denotes the local units of K_v . Through an abuse of notation we will continue to write K^\times for the diagonal embedding of K^\times in J_K and U_v for the subgroup of ideles which are units at v and 1 elsewhere. Let $U = U_p$ be the subgroup of ideles which have units at p and 1's elsewhere, and U' the product of all U_v , for $v \neq p$.

Class field theory gives a correspondence between norm subgroups of J_K/K^\times (the *idele class group* of K) and abelian extensions of K . In particular, we obtain an isomorphism

$$\mathcal{G}^{ab} \simeq \text{pro-}p \text{ completion of } J_K/(K^\times U').$$

Let \overline{E} denote the closure of the embedding of the units of K in U . We then obtain an exact sequence

$$1 \rightarrow U_1/\overline{E}_1 \rightarrow \mathcal{G}^{ab} \rightarrow A \rightarrow 1,$$

where the subscript 1 indicates we are taking units congruent to 1 modulo the prime p . (If H denotes the p -Hilbert class field of K , then this is just the exact sequence of Galois groups

$$1 \rightarrow \text{Gal}(K^{ab}/H) \rightarrow \text{Gal}(K^{ab}/K) \rightarrow \text{Gal}(H/K) \rightarrow 1,$$

where K^{ab} is the maximal abelian extension of K in Ω .) This gives the first part of the theorem, since U has \mathbb{Z}_p -rank $[K : \mathbb{Q}] = 2r_2 + r_1$ and \overline{E}_1 has \mathbb{Z}_p -rank $r_1 + r_2 - 1$ by Leopoldt's conjecture, which is known to hold for K .

We claim the torsion in \mathcal{G}^{ab} comes from U_1/\overline{E}_1 , and show this by considering an idele class (a_v) of \mathcal{G}^{ab} such that

$$(a_v)^{p^m} = \alpha(u_v) \in K^\times U'.$$

This implies α is a p^m -th power in K_p . Let \mathfrak{a} be a representative of the ideal class of A mapped to by (a_v) , so $\mathfrak{a}^{p^m} = (\alpha)$. Let $K_{m+1} = \mathbb{Q}(\zeta_{p^m})$. Then $K_{m+1}(\alpha^{1/p^m})$ is an unramified extension. Since \mathfrak{a} lies in A^- (by Vandiver's conjecture), the Kummer pairing implies the Galois group of $K_{m+1}(\alpha^{1/p^m})/K_{m+1}$ lies in A_{m+1}^+ , which is 0 ($A^+ = 0 \Rightarrow A_n^+ = 0$ for all n). Hence α must be a p^m -th power in K_{m+1} as well. This means the ideal \mathfrak{a} is principal when extended to K_{m+1} (generated by a p^m -th root of α). But the map from A to A_{m+1} is injective, and so \mathfrak{a} must have represented a principal class in A as well. Hence the torsion in \mathcal{G}^{ab} maps to 0 in A .

We now just need to determine the torsion subgroup of U_1/\overline{E}_1 . We may consider each factor of the idempotent decomposition separately. Since $\varepsilon_i E_1 = 0$ for $i = 0$ and for i odd, and each $\varepsilon_i U_1 \simeq \mathbb{Z}_p$, we obtain

$$U_1/\overline{E}_1 \simeq (\mathbb{Z}_p)^{(p+1)/2} \oplus \bigoplus_{i \text{ even}} \varepsilon_i U_1/\varepsilon_i \overline{E}_1.$$

For even i the terms $\varepsilon_i U_1/\varepsilon_i \overline{E}_1$ are equal to $\varepsilon_i U_1^+/\varepsilon_i \overline{E}_1^+$, where the superscript $+$ indicates we are looking at units in the local subfield fixed by the automorphism of order 2. Vandiver's conjecture implies the cyclotomic units C_1^+ have index prime to p in E_1^+ (see Theorem 8.2 of [28]), and so it suffices to consider the quotients $\varepsilon_i U_1^+/\varepsilon_i \overline{C}_1^+$. But Theorem 8.25 of [28] states

$$[\varepsilon_i U_1^+ : \varepsilon_i \overline{C}_1^+] = p^{v_p(L_p(1, \omega^i))},$$

and hence our claim is proved. \square

Although it is not necessary for our work here, \mathcal{G}^{ab} in fact breaks up as a direct sum

$$\mathcal{G}^{ab} \simeq \mathbb{Z}_p^{r_2+1} \oplus \text{torsion}.$$

The fixed field of the torsion subgroup is the compositum of all \mathbb{Z}_p -extensions of K .

Corollary 2.3.1. *Let*

$$1 \longrightarrow R \longrightarrow F_g \longrightarrow \mathcal{G} \longrightarrow 1$$

be a minimal free presentation of \mathcal{G} . Then the image of R is contained in the closure of the subgroup $F_g^{p^n}[F_g, F_g]$ where $n = \min\{v_p(L_p(1, \omega^i))\}$.

Proof: This follows immediately from the structure of \mathcal{G}^{ab} . \square

Corollary 2.3.2. *The p -Hilbert class field of K is contained in the compositum of all \mathbb{Z}_p -extensions of K .*

Proof: Since the compositum of all \mathbb{Z}_p -extensions is the fixed field of the torsion subgroup of \mathcal{G}^{ab} , the result will follow if the torsion subgroup is contained in the inertia subgroup for p . But this is in fact the case since, by local class field theory the image of U_1'/\overline{E}_1 will be in the inertia subgroup. Since all the torsion in \mathcal{G}^{ab} comes from U_1'/\overline{E}_1 , the result follows. \square

2.4 An Auxiliary Λ -module

We retain the notation and context of the last section. Recall the linearization of the free presentation of the Galois group \mathcal{G} described in Section 1.2.2; namely, given the minimal free presentation

$$1 \longrightarrow R \longrightarrow F_g \longrightarrow \mathcal{G} \longrightarrow 1,$$

there is a Λ -module Z (to be defined below) which fits into an exact sequence

$$0 \longrightarrow \Lambda^s \xrightarrow{\phi} \Lambda^g \longrightarrow Z \longrightarrow 0,$$

where the map ϕ is described in terms of Fox derivatives on the set F_g . We now define and describe the module Z in more detail.

Suppose G is a finite p -group, and consider the group ring $\mathbb{Z}_p[G]$. There is an *augmentation* map from $\mathbb{Z}_p[G]$ to \mathbb{Z}_p given by sending $\sum_i a_i \sigma_i$ to $\sum_i a_i$. We define the *augmentation ideal* $I(G)$ via the sequence

$$0 \longrightarrow I(G) \longrightarrow \mathbb{Z}_p[G] \longrightarrow \mathbb{Z}_p \longrightarrow 0,$$

so $I(G)$ is the subgroup generated by the elements $\sigma - 1$ for σ in G .

For a pro- p group G we may similarly define the augmentation ideal $I(G)$ of the completed group ring $\mathbb{Z}_p[[G]]$ by taking the inverse limit of the augmentation sequences

$$0 \longrightarrow I(G/U) \longrightarrow \mathbb{Z}_p[G/U] \longrightarrow \mathbb{Z}_p \longrightarrow 0,$$

where the U range over the open subgroups of finite index in G . The exactness is preserved since the $I(G/U)$ satisfy the Mittag-Leffler condition. So $I(G)$ is topologically generated by elements of the form $\sigma - 1$ as σ ranges over the elements of G .

Now let K , Ω , and \mathcal{G} be as before, and let K_∞ denote the compositum of all \mathbb{Z}_p -extensions of K (so in particular, $K_\infty \subset \Omega$). Let $\Gamma \simeq \mathbb{Z}_p^r$ denote the Galois group of K_∞/K and Λ the power series ring $\mathbb{Z}_p[[T_1, \dots, T_r]]$. Finally, let Y denote the Galois group of the maximal abelian extension of K_∞ contained in Ω .

It will be shown in the next Chapter that Greenberg's conjecture for the field K and the prime p is equivalent to the Λ -module Y being torsion free. In [21], Nguyen-Quang-Do introduces an auxiliary Λ -module Z closely related to Y , but which lends itself more easily to study. We define

$$Z := H_0(\Omega/K_\infty, I(\mathcal{G})).$$

(Here we are using group *homology*. See Chapter 4 of [3], or [21] for a brief description.) This seemingly odd definition is justified by the following theorem, in which we see that Z contains Y as a Λ -submodule with torsion free quotient. So in particular Y and Z will have isomorphic Λ -torsion submodules. The module Z will also be seen to give the linearization described above.

Theorem 2.4.1. *With notation as above, one has the following exact sequences of Λ -modules:*

$$0 \longrightarrow Y \longrightarrow Z \longrightarrow I(\Gamma) \longrightarrow 0,$$

$$0 \longrightarrow \Lambda^s \longrightarrow \Lambda^g \longrightarrow Z \longrightarrow 0.$$

Proof: We obtain the first exact sequence by considering the augmentation exact sequence for $\mathbb{Z}_p[[\mathcal{G}]]$, namely

$$0 \longrightarrow I(\mathcal{G}) \longrightarrow \mathbb{Z}_p[[\mathcal{G}]] \longrightarrow \mathbb{Z}_p \longrightarrow 0.$$

Taking homology with respect to the group $G = \text{Gal}(\Omega/K_\infty)$ we obtain

$$\cdots \rightarrow H_1(G, \mathbb{Z}_p[[\mathcal{G}]]) \rightarrow H_1(G, \mathbb{Z}_p) \rightarrow Z \rightarrow \mathbb{Z}_p[[\Gamma]] \rightarrow \mathbb{Z}_p \rightarrow 0. \quad (2.10)$$

It is shown in [3] (Chapter 4, Proposition 1) that $H_1(G, \mathbb{Z}) \simeq G^{ab}$, the maximal abelian quotient of G . Since \mathcal{G} is a pro- p group the argument may be easily applied to $H_1(G, \mathbb{Z}_p)$ with the same outcome. Further, since the map from $\mathbb{Z}_p[[\Gamma]]$ to \mathbb{Z}_p is just the augmentation map we may rewrite the sequence

$$\cdots \longrightarrow H_1(G, \mathbb{Z}_p[[\mathcal{G}]]) \longrightarrow Y \longrightarrow Z \longrightarrow I(\Gamma) \rightarrow 0$$

(recall that Y was the Galois group of the maximal abelian extension of K_∞ contained in Ω , and so $G^{ab} \simeq Y$). We need only show $H_1(G, \mathbb{Z}_p[[\mathcal{G}]]) = 0$ to complete the computation. This follows from the fact that $\mathbb{Z}_p[[\mathcal{G}]]$ is a free $\mathbb{Z}_p[[G]]$ -module.

The second exact sequence will be obtained by taking homology of the so called *resolution of Lyndon* (see [21])

$$0 \longrightarrow \mathbb{Z}_p[[\mathcal{G}]]^s \longrightarrow \mathbb{Z}_p[[\mathcal{G}]]^g \longrightarrow I(\mathcal{G}) \longrightarrow 0,$$

where g and s are respectively the minimal number of generators and relations of \mathcal{G} (see section 2.3.1). As above, we take homology with respect to the group G , obtaining

$$\cdots \longrightarrow H_1(G, I(\mathcal{G})) \longrightarrow \Lambda^s \longrightarrow \Lambda^g \longrightarrow Z \longrightarrow 0.$$

By extending the long exact sequence of homology (2.10), and using the fact that $H_2(G, \mathbb{Z}_p[[\mathcal{G}]]) = 0$ as well, we obtain the isomorphism

$$H_2(G, \mathbb{Z}_p) \simeq H_1(G, I(\mathcal{G})).$$

The vanishing of the group $H_2(G, \mathbb{Z}_p)$ is known as the *weak Leopoldt conjecture* for K_∞ , and is well known to hold in this case since K_∞ contains all p -power roots of unity (see [21], especially Theorem 1.4, Corollary 1.5, and Theorem 2.2). \square

Chapter 3

PROOF OF MAIN RESULTS

We recall our main result.

Theorem 3.0.2. *Let p be an odd prime and suppose $K = \mathbb{Q}(\zeta_p)$ satisfies the following conditions:*

1. *Vandiver's conjecture.*
2. $\lambda(p) = 1$.
3. *for the B_{1-i} divisible by p , $v_p(L_p(1, \omega^{1-i})) \leq v_p(|\varepsilon_i A|)$.*

Let K_∞/K be the compositum of all \mathbb{Z}_p -extensions of K . Then the Galois group X of the maximal abelian unramified pro- p -extension L_∞/K_∞ is pseudo-null as a module over Λ .

The proof of this result requires the introduction of several auxiliary Λ -modules including the modules Y and Z appearing in Section 2.4. We re-establish some notation. Let M_∞ be the maximal abelian p -ramified pro- p -extension of K_∞ , and let N_∞ be the subfield of M_∞ generated by all p th power roots of p -units of K_∞ (so one has $K \subset K_\infty \subset N_\infty \subset M_\infty$). Then we have the standard Iwasawa modules

$$Y = \text{Gal}(M_\infty/K_\infty), \quad Y' = \text{Gal}(N_\infty/K_\infty).$$

The proof of Theorem 3.0.2 can be broken into three distinct parts, which we describe here.

1. Establish the equivalence

$$X \text{ is pseudo-null} \Leftrightarrow Y_{\text{tor}} = 0.$$

Nguyen-Quang-Do has shown that Y contains no non-trivial pseudo-null submodules (see [21]), so in fact $Y_{\text{tor}} = 0$ if and only if Y_{tor} is pseudo-null.

2. Show that if $Y_{\text{tor}} \neq 0$, then non-trivial elements would be visible in Y'_{tor} under the restriction map (of Galois groups).
3. Show that $Y'_{\text{tor}} = 0$

Steps 1 and 2 will be proved in the following two sections. Step 3 is a result of McCallum (see [19]) that will be stated in Section 3.3.

3.1 An Equivalent Formulation

In this section we wish to prove the following equivalent formulation of Greenberg's conjecture for cyclotomic base fields, thereby establishing part 1 above.

Theorem 3.1.1. *Suppose $K = \mathbb{Q}(\zeta_p)$, $p \geq 7$, and K_∞ is the compositum of all \mathbb{Z}_p -extensions of K . Then X is a pseudo-null Λ -module if and only if the Λ -torsion submodule of Y is trivial.*

We denote the \mathbb{Z}_p -rank of $\Gamma = \text{Gal}(K_\infty/K)$ by r . The proof will follow immediately from the following lemmas, noting that the condition $p \geq 7$ implies r is at least 4. Recall that the $\text{Ext}_\Lambda^i(\cdot, \Lambda)$ are the right derived functors associated to $\text{Hom}_\Lambda(\cdot, \Lambda)$. We abbreviate $\text{Ext}_\Lambda^i(\cdot, \Lambda)$ by $\text{Ext}^i(\cdot)$.

Lemma 3.1.1. *If $i \geq 1$, then*

$$\text{Ext}^i(I(\Gamma)) = \begin{cases} 0 & i \neq r-1 \\ \mathbb{Z}_p & i = r-1 \end{cases}$$

Proof: Taking Hom of the augmentation exact sequence for Γ ,

$$0 \longrightarrow I(\Gamma) \longrightarrow \Lambda \longrightarrow \mathbb{Z}_p \longrightarrow 0,$$

we obtain

$$\text{Ext}^i(I(\Gamma)) \simeq \text{Ext}^{i+1}(\mathbb{Z}_p). \quad (3.1)$$

We will utilize the Koszul resolution of \mathbb{Z}_p to compute $\text{Ext}^i(\mathbb{Z}_p)$. The main reference for this is Chapter 1, Section 6 of [1]. Let

$$0 \longrightarrow C_r \xrightarrow{d} C_{r-1} \xrightarrow{d} \cdots \xrightarrow{d} C_1 \xrightarrow{d} C_0 \longrightarrow 0$$

be the Koszul complex for Λ as a module over itself relative to the Λ -regular sequence $\mathbf{x} = T_1, T_2, \dots, T_r$. Let e_1, \dots, e_r be a basis for the free Λ -module Λ^r . Then

$$C_k \simeq \bigwedge^k \Lambda^r,$$

the k -th exterior power of Λ^r , and the maps d are given by

$$d(e_{i_1} \wedge e_{i_2} \wedge \cdots \wedge e_{i_k}) = \sum_{s=1}^k (-1)^{s+1} T_s e_{i_1} \wedge \cdots \wedge \widehat{e_{i_s}} \wedge \cdots \wedge e_{i_k},$$

where the hat indicates an omitted term. Let I be the ideal of Λ generated by the sequence \mathbf{x} . Then it is well known that since \mathbf{x} is a regular Λ -sequence, the Koszul complex is a free resolution for $\Lambda/I \simeq \mathbb{Z}_p$ (see Corollary 1.6.14 of [1] for example).

Let ω_r denote the unique Λ isomorphism from $\bigwedge^r \Lambda^r \rightarrow \Lambda$. Then, letting M^* denote the dual of a Λ -module M (i.e. $M^* = \text{Hom}_\Lambda(M, \Lambda)$), we define

$$\omega_k : \bigwedge^k \Lambda^r \longrightarrow \left(\bigwedge^{r-k} \Lambda^r \right)^*,$$

by setting $(\omega_k(x))(y) = \omega_r(x \wedge y)$. These maps are in fact isomorphisms, commuting with the maps d and d^* , yielding an isomorphism of the Koszul complex with its dual complex

$$0 \longrightarrow C_0^* \xrightarrow{d^*} C_1^* \xrightarrow{d^*} \cdots \xrightarrow{d^*} C_{r-1}^* \xrightarrow{d^*} C_r^* \longrightarrow 0.$$

Let $K_i = d(C_{i+1})$ (by exactness, for $i > 0$ this is also the kernel of the map from C_i of C_{i-1}). Using the fact that the Koszul complex is a free resolution of \mathbb{Z}_p we may form the short exact sequences

$$\begin{array}{ccccccccc} 0 & \longrightarrow & K_0 & \longrightarrow & C_0 & \longrightarrow & \mathbb{Z}_p & \longrightarrow & 0, \\ 0 & \longrightarrow & K_1 & \longrightarrow & C_1 & \longrightarrow & K_0 & \longrightarrow & 0, \\ & & & & \vdots & & & & \\ 0 & \longrightarrow & K_{r-1} & \longrightarrow & C_{r-1} & \longrightarrow & K_{r-2} & \longrightarrow & 0, \\ 0 & \longrightarrow & K_r & \longrightarrow & C_r & \longrightarrow & K_{r-1} & \longrightarrow & 0. \end{array} \tag{3.2}$$

Using the top sequence in (3.2) and the fact that the C_i are free (and so have zero Ext groups), we obtain the sequence

$$0 \longrightarrow \mathbb{Z}_p^* \longrightarrow C_0^* \xrightarrow{d^*} K_0^* \longrightarrow \text{Ext}^1(\mathbb{Z}_p) \longrightarrow 0.$$

But the map d^* surjects onto K_0^* , and so $\text{Ext}^1(\mathbb{Z}_p) = 0$. Similarly, for $2 \leq i \leq r$, the sequences in (3.2) may be used to establish $\text{Ext}^i(\mathbb{Z}_p) \simeq \text{Ext}^1(K_{i-2})$. By the exactness of the dual of the Koszul complex it follows that these groups are also zero for $i \leq r-1$.

The group $\text{Ext}^1(K_{r-2})$ can be computed from the second from last sequence in (3.2), from which we obtain

$$0 \longrightarrow K_{r-2}^* \longrightarrow C_{r-1}^* \xrightarrow{d^*} K_{r-1}^* \longrightarrow \text{Ext}^1(K_{r-2}) \longrightarrow 0.$$

The map d^* is not surjective in this case, and we obtain

$$\text{Ext}^1(K_{r-2}) \simeq K_{r-1}^*/d^*(C_{r-1}).$$

Since $K_r = 0$, the last sequence of (3.2) gives $K_{r-1}^* \simeq C_r^*$, and so we obtain

$$\begin{aligned} \text{Ext}^r(\mathbb{Z}_p) &\simeq \text{Ext}^1(K_{r-2}) \\ &\simeq C_r^*/d^*(C_{r-1}) \\ &\simeq C_0/d(C_1) \\ &\simeq \mathbb{Z}_p. \end{aligned}$$

Recalling the isomorphism (3.1), we obtain the desired result. \square

Lemma 3.1.2. *Let M be a finitely generated Λ -module. Then M is pseudo-null if and only if M is torsion and $\text{Ext}^1(M) = 0$.*

Proof: The main tool in the proof of this result is Grothendieck's local duality theorem relating local cohomology with certain Ext functors. The main reference is Section 3.5 of [1]. Let m denote the unique maximal ideal of Λ , and $H_m^i(M)$ the local cohomology (see Section 3.5 of [1] for a definition). We recall the facts needed here:

1. Let R be a Noetherian local ring with maximal ideal m , and let M be a finitely generated R -module of dimension d . Then $H_m^d(M) \neq 0$, and $H_m^i(M) = 0$ for $i > d$. (This is part of Theorem 3.5.7 of [1].)
2. Let (R, m) be a Cohen-Macaulay complete local ring of dimension r . Then for all finitely generated R -modules and all integers i there are isomorphisms

$$H_m^i(M) \simeq \text{Hom}_R(\text{Ext}_R^{r-i}(M, \omega_R), E),$$

and

$$\text{Ext}_R^i(M, \omega_R) \simeq \text{Hom}_R(H_m^{r-i}(M), E),$$

where ω_R is the canonical module of R , and E is the injective hull of the residue field R/m (see Theorem 3.5.8 of [1]). This is Grothendieck's local duality theorem.

The ring Λ is a regular local ring, and so is also Cohen-Macaulay (by Corollary 2.2.6 of [1]). Hence Λ satisfies the hypothesis of the above facts. Also, since Λ is in fact Gorenstein, Theorem 3.3.7 of [1] implies $\omega_\Lambda \simeq \Lambda$. Let r denote the dimension of Λ .

Let $\text{Ann}(M)$ denote the annihilator of the Λ -module M . Then

$$d := \dim(M) = r - \text{ht}(\text{Ann}(M)),$$

where $\text{ht}(I)$ denotes the height of an ideal I (see Corollary 2.1.4 of [1], using the fact that $\dim(M) = \dim(\Lambda/\text{Ann}(M))$).

If M is pseudo-null, then $d \leq r - 2$. By fact 1 above, we then see that $H_m^{r-1} = 0$, and so Grothendieck's duality gives $\text{Ext}_\Lambda^1(M, \Lambda) = 0$ as well.

Now suppose M is torsion and $\text{Ext}_\Lambda^1(M, \Lambda) = 0$. Grothendieck's duality then gives $H_m^{r-1}(M) = 0$, and since $\text{ht}(\text{Ann}(M)) \geq 1$ (since M is torsion) we have $d \leq r - 1$. But by fact 1, it cannot be the case that $d = r - 1$ (otherwise we would have $H_m^{r-1}(M) \neq 0$) and so $d \leq r - 2$. Hence $\text{ht}(\text{Ann}(M)) \geq 2$, i.e. M is pseudo-null. \square

Denote by X' the Galois group of the sub-extension of L_∞/K_∞ in which all primes above p are completely decomposed.

Lemma 3.1.3. *If Γ has \mathbb{Z}_p -rank at least 4, then $\text{Ext}^1(X') \simeq Y_{\text{tor}}$.*

Proof: Jannsen, in [14], has established a duality relating X and Y which, for $r \geq 4$, is given by the following exact sequence

$$0 \rightarrow X' \rightarrow \text{Ext}^1(Y)(1) \rightarrow \bigoplus_{\wp} \mathbb{Z}_p[[\Gamma/\Gamma_{\wp}]] \rightarrow \mathbb{Z}_p \rightarrow 0,$$

where Γ_{\wp} is the decomposition group in Γ for a prime \wp of K_{∞} above p ,

The module $\bigoplus_{\wp} \mathbb{Z}_p[[\Gamma/\Gamma_{\wp}]]$ is pseudo-null since the annihilator has height at least 4. Since both $\bigoplus_{\wp} \mathbb{Z}_p[[\Gamma/\Gamma_{\wp}]]$ and \mathbb{Z}_p have vanishing Ext^1 and Ext^2 , Jannsen's exact sequence yields

$$\text{Ext}^1(X') \simeq \text{Ext}^1(\text{Ext}^1(Y)). \quad (3.3)$$

Now recall the sequence derived in Theorem 2.4.1 relating the Λ -module structure of Y to that of Z ,

$$0 \rightarrow Y \rightarrow Z \rightarrow I(\Gamma) \rightarrow 0.$$

Taking Hom of this sequence, and using Lemma 3.1.1, we obtain $\text{Ext}^1(Y) \simeq \text{Ext}^1(Z)$, and so

$$\text{Ext}^1(\text{Ext}^1(Y)) \simeq \text{Ext}^1(\text{Ext}^1(Z)).$$

It will be shown below using the two-step free resolution of Z (also in Theorem 2.4.1) that $\text{Ext}^1(\text{Ext}^1(Z)) \simeq Z_{\text{tor}}$. Since $Z_{\text{tor}} \simeq Y_{\text{tor}}$, this yields

$$\text{Ext}^1(\text{Ext}^1(Y)) \simeq Y_{\text{tor}}.$$

Combining this with (3.3) we obtain $\text{Ext}^1(X') \simeq Y_{\text{tor}}$, as desired. \square

Lemma 3.1.4. $\text{Ext}^1(\text{Ext}^1(Z)) \simeq Z_{\text{tor}}$.

Proof: Consider the free resolution of Z given in Theorem 2.4.1

$$0 \rightarrow \Lambda^s \xrightarrow{\phi} \Lambda^g \xrightarrow{\psi} Z \rightarrow 0.$$

By taking the dual of this exact sequence, and writing Φ for the image of $(\Lambda^*)^g$ in $(\Lambda^*)^s$ (we are writing A^* for $\text{Hom}_{\Lambda}(A, \Lambda)$), we may form the following pair of short exact sequences

$$0 \rightarrow Z^* \rightarrow (\Lambda^*)^g \rightarrow \Phi \rightarrow 0,$$

$$0 \rightarrow \Phi \rightarrow (\Lambda^*)^s \rightarrow \text{Ext}^1(Z) \rightarrow 0.$$

Now we dualize again. Using the fact that the double dual of a free module is itself once again, and $(\text{Ext}^1(Z))^* = 0$ (since $\text{Ext}^1(Z)$ is torsion), we obtain

$$0 \longrightarrow \Phi^* \longrightarrow \Lambda^g \longrightarrow (Z^*)^* \longrightarrow \text{Ext}^1(\Phi) \longrightarrow 0,$$

$$0 \longrightarrow \Lambda^s \longrightarrow \Phi^* \longrightarrow \text{Ext}^1(\text{Ext}^1(Z)) \longrightarrow 0.$$

By identifying Φ^* with its image in Λ^g , the second exact sequence gives an isomorphism between $\text{Ext}^1(\text{Ext}^1(Z))$ and the image of Φ^* in Z (via the original free resolution of Z). We claim this image is precisely Z_{tor} . Let $y \in Z_{\text{tor}}$ and let $x \in \Lambda^g$ map to y (i.e. $\psi(x) = y$). Then, x will map to 0 in $(Z^*)^*$ if and only if $\delta(\psi(x)) = 0$ for all $\delta \in Z^*$. But $\psi(x) = y$, and $\delta(y) = 0$ for all such δ since y is a torsion element. Hence x is in the kernel of the map from Λ^g to $(Z^*)^*$, i.e. $x \in \Phi^*$.

On the other hand if x is in Φ^* , then $\delta(\psi(x)) = 0$ for all $\delta \in Z^*$. But since Z is a finitely generated Λ -module, it follows that $\psi(x)$ must be in Z_{tor} . \square

Recall from Section 2.2.2 that we say two Λ -modules M and M' are *pseudo-isomorphic* if there is a Λ -module homomorphism $M \rightarrow M'$ with pseudo-null kernel and co-kernel. When this is the case, we write $M \sim M'$.

Proof of Theorem 3.1.1: Consider the natural surjection $X \rightarrow X'$. The kernel is generated (as a \mathbb{Z}_p -module) by the Frobenius automorphisms at primes above p . Therefore it is finitely generated as a module over $\bigoplus_{\varphi} \mathbb{Z}_p[[\Gamma/\Gamma_{\varphi}]]$, and so is pseudo-null. Hence $X \sim X'$, and therefore X is pseudo-null if and only if X' is. Now Lemmas 3.1.2 and 3.1.3 imply the desired equivalence. \square

3.2 Visible Torsion

We assume from now on that the λ invariant of the cyclotomic \mathbb{Z}_p -extension of K is equal to 1, as well as the boundedness condition on $v_p(L_p(1, \omega^i))$. Vandiver's conjecture then implies A , the p -class group of K , is cyclic. We now establish part 2 of our argument by proving the following theorem.

Theorem 3.2.1. *Suppose $Y_{\text{tor}} \neq 0$. Then, with the assumptions above, the map*

$$Y_{\text{tor}} \longrightarrow Y'$$

given by restricting Galois groups is not the zero map.

We will define a field F shown to be intermediate between K_{∞} and N_{∞} and consider the restriction of Y_{tor} to $\text{Gal}(F/K)$. We will be able to show that this is not the zero map, thereby proving Theorem 3.2.1.

Recall our definitions of Ω and \mathcal{G} . We take for the field F the maximal abelian extension of K contained in Ω , denoted K^{ab} . So, in particular, $\text{Gal}(K^{ab}/K) \simeq \mathcal{G}^{ab}$.

Lemma 3.2.1. *The fixed field of the torsion subgroup of \mathcal{G}^{ab} is K_{∞} .*

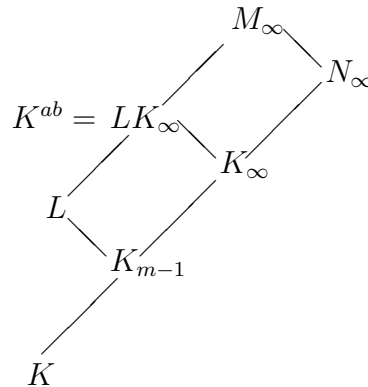


FIGURE 3.1. Field diagram 2.

Proof: This is a consequence of the proof of the structure of \mathcal{G}^{ab} . See also Theorem 13.4 in [28], where this result is a consequence. \square

In particular, since K_{∞} contains all p -power roots of unity, the extension K^{ab}/K_{∞} is a Kummer extension with Galois group isomorphic to, say, $\mathbb{Z}/p^m\mathbb{Z}$ (this is just the torsion subgroup of \mathcal{G}^{ab} , and so $p^m \leq |A|$). Let K_n denote the n -th layer of the cyclotomic \mathbb{Z}_p -extension of K (so $K_n = \mathbb{Q}(\zeta_{p^{n+1}})$) and A_n the p -primary part of the ideal class group of K_n .

Lemma 3.2.2. *The field K^{ab} is contained in N_{∞} .*

Proof: To show that K^{ab} is contained in N_{∞} , we need to show that K^{ab}/K_{∞} is generated by a p -th power root of a unit of K_{∞} .

Consider the extension K^{ab}/K_{m-1} . There is a non-canonical isomorphism

$$\mathrm{Gal}(K^{ab}/K_{m-1}) \simeq \mathrm{Gal}(K_{\infty}/K_{m-1}) \times \mathrm{Gal}(K^{ab}/K_{\infty}).$$

We let L denote the fixed field of the first factor. (So $K^{ab} = LK_{\infty}$, see Figure 3.1.) The extension L/K_{m-1} is a Kummer extension, and we may write

$$L = K_{m-1}(x^{1/p^m})$$

for some x in K_{m-1} where the ideal (x) is a p^m -th power, say $(x) = J^{p^m}$.

Since, in particular, J represents a class of order dividing p^m in A_{m-1} , Proposition 2.2.1 implies that the class of J is in the image of the map from $A = A_0$ to A_n . We let I be a representative ideal of the class that extends to J .

By Theorem 2.2.5 we know the p -Hilbert class field of K is contained in K_{∞} . This means that the class of I , and therefore J , becomes principal in K_{∞} . The extension K^{ab}/K_{∞} is also generated by a p^m -th root of x , and the ideal (x) in K_{∞} is now the p^m -th power of a *principal* ideal,

$$(x) = (y)^{p^m}.$$

The elements x and y^{p^m} then differ by a unit, i.e. $x = uy^{p^m}$. But clearly the extension LK_∞ is also generated by the p^m -th root of $x/y^{p^m} = u$, and so the field $K^{ab} = LK_\infty$ is contained in N_∞ . \square

Proof of Theorem 3.2.1: Suppose now that the Λ -torsion sub-module of Y is not zero. We then want to show that the map to the torsion sub-module of Y' given by restriction of Galois groups is not the zero map. By Lemma 3.2.2 it will suffice to show that the map from Y_{tor} to $\text{Gal}(F/K) \simeq \mathcal{G}^{ab}$ (also given by restriction of Galois groups, viewing elements of Y as elements of $\text{Gal}(M_\infty/K)$) is not the zero map.

Recall the definition $Z = H_0(\Omega/K_\infty, I(\mathcal{G}))$. Since $H_0(\mathcal{G}, I(\mathcal{G})) \simeq \mathcal{G}^{ab}$, we obtain a surjective map (via co-restriction)

$$Z \longrightarrow \mathcal{G}^{ab}.$$

In fact, we may use the derivation of the second exact sequence of Theorem 2.4.1 to obtain the commutative diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & \Lambda & \longrightarrow & \Lambda^g & \longrightarrow & Z \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \downarrow \\ 0 & \longrightarrow & \mathbb{Z}_p & \longrightarrow & \mathbb{Z}_p^g & \longrightarrow & \mathcal{G}^{ab} \longrightarrow 0 \end{array}$$

where the vertical arrows are surjective. The map from Y_{tor} to \mathcal{G}^{ab} factors through Z_{tor} (again, via corestriction), and so it suffices to show the map from Z_{tor} to \mathcal{G}^{ab} is not the zero map.

Suppose $z \in Z$ is a non-trivial torsion element with $f \cdot z = 0$, where f is an irreducible element of Λ . Let $\sigma = (\sigma_1, \dots, \sigma_g)$ be the image of 1 in Λ^g . Since the map from Λ^g to Z is surjective we choose an element $\mu = (\mu_1, \dots, \mu_g) \in \Lambda^g$ which maps to z . Then there must be an $h \in \Lambda$ such that

$$f \cdot (\mu_1, \dots, \mu_g) = h \cdot (\sigma_1, \dots, \sigma_g),$$

where f does not divide h (otherwise z would be 0). Since Λ is a UFD, and f was chosen to be irreducible, h must divide each of the μ_i . By replacing each μ_i with $\frac{\mu_i}{h}$, we may assume there is a non-trivial torsion element of $z \in Z$, mapped to by μ , with

$$f \cdot (\mu_1, \dots, \mu_g) = (\sigma_1, \dots, \sigma_g).$$

We will show that the element z does not map to 0 in \mathcal{G}^{ab} by pushing these elements down to the lower exact row and showing that μ can not map to 0.

The first two vertical arrows are simply evaluation at 0 (we are viewing elements of Λ as power series). Let w be the image of 1 in \mathbb{Z}_p^g . Then we have

$$w = f(0) \cdot \mu(0) = \sigma(0). \tag{3.4}$$

Since f is not a unit, $f(0)$ must be divisible by p , and so w is divisible by a positive power of p , say p^a (in fact w is exactly divisible by p^m since the torsion subgroup of

\mathcal{G}^{ab} is isomorphic to $\mathbb{Z}/p^m\mathbb{Z}$). But by the equality in (3.4), not all of the $\mu_i(0)$ can be divisible by p^m . This means $\mu(0)$ can not map to 0 in \mathcal{G}^{ab} and, by the commutativity of the above diagram, neither can z . \square

3.3 A Unit Theorem

Finally, we state a unit theorem proved by McCallum in [19] for certain multiple \mathbb{Z}_p -extensions. It is a generalization of a theorem of Iwasawa. Recall that N_∞ is the extension of K_∞ generated by p -power roots of p -units of K_∞ with Galois group Y' . There is a natural surjection $Y \rightarrow Y'$ of Galois groups, and in the last section we saw that if there exist non-trivial Λ -torsion elements of Y , then the Λ -torsion sub-module of Y is not mapped to zero in Y' .

The unit theorem will tell us that in fact Y_{tor} is mapped to zero because Y' is in fact Λ -torsion free. Hence the torsion sub-module of Y must have been 0 to begin with, and so by Theorem 3.1.1, our main result is proved.

Theorem 3.3.1 (McCallum, [19]). *Let K_∞/K be a multiple \mathbb{Z}_p -extension satisfying the following two conditions:*

1. K_∞ contains the p^n -th roots of unity for all $n \geq 1$.
2. K contains a unique prime above the rational prime p .

Then the Λ -module $Y' = \text{Gal}(N_\infty/K_\infty)$ is torsion free.

Conditions 1 and 2 are clearly satisfied for the fields in question. We give now a brief sketch of how the proof of Theorem 3.3.1 proceeds. All references in the following are to [19], which should be consulted for details.

First we fix some notation. For an intermediate field $K \subset F \subset K_\infty$, let $E_F = \mathcal{O}_F[1/p]^\times$, and let $U_F \subset E_F$ be the subgroup of elements which are norms from E_L for every extension L contained in K_∞ . Now define the Λ -module Y'' to be the Galois group of the extension of K_∞ obtained by adjoining all p -power roots of elements of U_F as F varies over all intermediate fields (so in particular, we have $K_\infty \subset Y'' \subset Y'$).

A fairly elementary argument shows Y'' to be Λ -torsion free (see Lemma 2.1). McCallum then proceeds to show that in fact $Y' = Y''$ by considering the kernel of the natural projection $Y' \rightarrow Y''$. Using Kummer theory, this kernel is given by (the Pontrjagin dual of)

$$\varinjlim_F (E_F/U_F) \otimes \mathbb{Q}_p/\mathbb{Z}_p. \quad (3.5)$$

To show this is 0, a filtration $U_F \subset V_F \subset V_F^{loc} \subset E_F$ is introduced as follows. Let N denote the norm map.

- $V_F^{loc} = \{x \in E_F : x_v \in N_{L_v/F_v} L_v^\times \text{ for all intermediate } L \text{ and all places } v\}$

- $V_F = \{x \in E_F : x \in N_{L/F}L^\times \text{ for all intermediate } L\}$

Each graded factor ($\varinjlim_F (E_F/V_F^{loc}) \otimes \mathbb{Q}_p/\mathbb{Z}_p$ for example) is then shown to be zero. The arguments for each factor are rather technical and we refer the interested reader to [19] for the details.

Chapter 4

FURTHER CONSIDERATIONS

In this Chapter we describe an interesting consequence of Greenberg's conjecture for cyclotomic fields regarding the existence (or non-existence) of free pro- p Galois extensions. We also consider a computational approach to establishing Greenberg's conjecture for cyclotomic fields as well as possible avenues for future research progress.

4.1 Free Pro- p Galois Groups

Let K be a field. By a *free pro- p -extension* of K we mean a Galois extension F/K whose Galois group is a free pro- p group. Such extensions arise often in number theory. The following list is taken from [31].

1. The maximal pro- p -extension of a p -adic number field not containing a primitive p -th root of unity is free.
2. The maximal unramified pro- p -extension of an algebraic function field over an algebraically closed field is free.
3. The maximal pro- p -extension of the cyclotomic \mathbb{Z}_p -extension of an algebraic number field is free.
4. The maximal p -ramified pro- p -extension of the cyclotomic \mathbb{Z}_p -extension of an algebraic number field is free if and only if the corresponding Iwasawa μ invariant is 0.

Numbers 1 and 2 are due to Shafarevich (see [27]). Numbers 3 and 4 are results of Iwasawa (see [9] and [12] respectively).

Questions concerning the existence of free pro- p -extensions have been the subject of several papers, including [30] and [29]. Let Ω denote the maximal p -ramified pro- p -extension of K with Galois group \mathcal{G} . Since free pro- p -extensions are unramified outside p , any such extension of K will be contained in Ω (see Lemma 2.1 of [30]), and so free pro- p -extensions of K correspond to free pro- p -quotients of \mathcal{G} . We note here two results from the cited papers.

Theorem 4.1.1 (Wingberg, [29]). *If K contains the $2p$ -th roots of unity then \mathcal{G} is isomorphic to a free pro- p -product of decomposition groups and a free pro- p group. Further, \mathcal{G} is a free pro- p group if and only if the number of places of Ω above p is 1.*

For $K = \mathbb{Q}(\zeta_p)$ we saw in Section 2.3.1 that \mathcal{G} is a free pro- p group exactly when p is a regular prime (since the number of relations is equal to the p -rank of the class group of K), and hence Ω must contain just 1 prime above p .

When p is an irregular prime the group \mathcal{G} is not free, but we may look for free pro- p quotients. Let r_2 denote the number of complex places of K . Then Leopoldt's conjecture predicts $r_2 + 1$ independent \mathbb{Z}_p -extensions of K , and so the maximal rank of a free pro- p -extension of K is bounded by $r_2 + 1$. Consider the following result.

Theorem 4.1.2 (Yamagishi, [30]). *If F/K is a free pro- p -extension of maximal rank $r_2 + 1$, and Leopoldt's conjecture is true for K , then F is the unique such extension of K .*

In light of the above results, we prove the following consequence of Greenberg's conjecture.

Theorem 4.1.3. *Let p be an irregular prime and suppose $K = \mathbb{Q}(\zeta_p)$ satisfies Vandiver's conjecture and Greenberg's conjecture. Then K has no free pro- p -extension of rank $r_2 + 1$.*

Proof: Let Ω be the maximal pro- p -extension of K with Galois group \mathcal{G} . Let g and s denote the minimal number of generators and relations of \mathcal{G} , as in Section 2.3.1. So the maximal possible rank $r_2 + 1$ is equal to $g - s$. We then make use of the minimal presentation of \mathcal{G}

$$1 \longrightarrow R \longrightarrow F_g \longrightarrow \mathcal{G} \longrightarrow 1,$$

and its relation to the exact sequence of $\Lambda = \mathbb{Z}_p[[T_1, \dots, T_{r_2+1}]]$ -modules

$$0 \longrightarrow \Lambda^s \longrightarrow \Lambda^g \longrightarrow Z \longrightarrow 0$$

(see Section 1.2.2). In particular, if \mathcal{G} has a free pro- p quotient of maximal rank, then there is a corresponding sequence of Λ -modules

$$0 \longrightarrow Z_{\text{tor}} \longrightarrow Z \longrightarrow \Lambda^{r_2+1} \longrightarrow 0,$$

which splits, and so $Z \simeq \Lambda^{r_2+1} \oplus Z_{\text{tor}}$. But as we have seen, Greenberg's conjecture for K is equivalent to $Z_{\text{tor}} = 0$, and so in fact Z is free.

Recall the definition $Z = H_0(\Omega/K_\infty, I(\mathcal{G}))$. Define

$$\begin{aligned} Z_K &:= H_0(\Omega/K, I(\mathcal{G})) \\ &\simeq H_0(K_\infty/K, H_0(\Omega/K_\infty, I(\mathcal{G}))) \\ &\simeq H_0(K_\infty/K, Z). \end{aligned}$$

Since Z is a free Λ -module of rank $r_2 + 1$, and $H_0(K_\infty/K, M) = M/(T_1, \dots, T_{r_2+1})M$ for any Λ -module M , we have

$$Z_K \simeq \Lambda^{r_2+1}/(T_1, \dots, T_{r_2+1})\Lambda^{r_2+1} \simeq \mathbb{Z}_p^{r_2+1}.$$

Now, by taking homology of the augmentation exact sequence for \mathcal{G} with respect to the Galois group \mathcal{G} itself (rather than the group $\text{Gal}(\Omega/K_\infty)$ as we did in Theorem 2.4.1) we obtain the isomorphism

$$Z_K \simeq \mathcal{G}^{ab}.$$

But for irregular primes p satisfying Vandiver's conjecture the group \mathcal{G}^{ab} has non-trivial torsion and so we have a contradiction. \square

We then obtain

Corollary 4.1.1. *Let p be an irregular prime and suppose $K = \mathbb{Q}(\zeta_p)$ satisfies the three conditions of Theorem 3.0.2. Then K does not have a free pro- p -extension of rank $r_2 + 1$.*

We conclude this section with one final comment. It should be pointed out that the above corollary conflicts with the results stated (without proof) in the last section of [31].

4.2 A Computational Approach

Let p be a prime number, $K = \mathbb{Q}(\zeta_p)$, and let Γ , Λ , \mathcal{G} , and Z be as in Chapter 3. As before, the Galois group \mathcal{G} has a minimal free presentation

$$1 \longrightarrow R \longrightarrow F_g \longrightarrow \mathcal{G} \longrightarrow 1,$$

where F_g is the free pro- p group on g generators. We let s again denote the minimal number of relations which topologically generate R . If we denote the generators of F_g by x_1, \dots, x_g , then we may think of the generators of R , say w_1, \dots, w_s , as words in the x_i .

Recall also the exact sequence

$$0 \longrightarrow \Lambda^s \xrightarrow{\phi} \Lambda^g \longrightarrow Z \longrightarrow 0.$$

In Section 1.2.2 we claimed the map ϕ to be induced from a certain derivation on the completed group ring $\mathbb{Z}_p[[F_g]]$. We explain this description now as it appears in [21]. For more details on the differential calculus of Fox see his paper [5].

Let $I(F_g)$ be the augmentation ideal of $\mathbb{Z}_p[[F_g]]$. Define

$$dx_i = 1 - x_i.$$

The elements dx_i , $1 \leq i \leq g$, form a basis for the augmentation ideal as a module over the completed group ring $\mathbb{Z}_p[[F_g]]$. The map which sends $x_i \rightarrow 1 - x_i$ induces a derivation

$$D : \mathbb{Z}_p[[F_g]] \longrightarrow I(F_g),$$

defined as follows. We set $\frac{\partial x_j}{\partial x_i} = \delta_{ij}$ (the Kronecker delta), and we set $\frac{\partial x_i^{-1}}{\partial x_i} = -x_i^{-1}$. Let $w = y_1 y_2 \cdots y_m$ be a (reduced) word in the x_i (so $y_j = x_i^{\pm 1}$ for some i). Then we define

$$D(w) = \sum_{i=1}^g \frac{\partial w}{\partial x_i} dx_i,$$

where the ‘‘partial derivative’’ is given by $\frac{\partial w}{\partial x_i} = \sum_{j=1}^m y_1 \cdots y_{j-1} \frac{\partial y_j}{\partial x_i}$.

If we now look back to the construction of the free presentation of Z ,

$$0 \longrightarrow \Lambda^s \xrightarrow{\phi} \Lambda^g \longrightarrow Z \longrightarrow 0,$$

we see that the free terms come from isomorphisms

$$\begin{aligned} \Lambda^s &\simeq H_0(\Omega/K_\infty, R^{ab}) \\ \Lambda^g &\simeq H_0(\Omega/K_\infty, H_0(R, I(F_g))). \end{aligned}$$

The map $\phi : \Lambda^s \rightarrow \Lambda^g$ is induced by the derivation D by passing to the quotient. More precisely, let w_1, \dots, w_s be a minimal system of generators for R in F_g . We abuse notation and continue to denote by w_i their image in $H_0(\Omega/K_\infty, R^{ab})$. The map ϕ is then completely determined by the values

$$\phi(w_i) = \sum_{i=1}^d \frac{\partial w}{\partial \sigma_i} d\sigma_i,$$

where σ_i is the image of x_i in Γ , $d\sigma_i$ is the image of dx_i in Λ^g , and $\frac{\partial w}{\partial \sigma_i}$ is the image of $\frac{\partial w}{\partial x_i}$.

Example 4: Consider the following sample calculation. Suppose \mathcal{G} is a one-relator group; i.e. $s = 1$. As we have seen, the one relation w defining \mathcal{G} must lie in the subgroup of $F_g^p[F_g, F_g]$ of F_g . Let us suppose we know the relation to be of the form $w = x_1^p$. We then compute $D(w)$. The only non-zero partial derivative will be $\frac{\partial w}{\partial x_1}$, which is given by

$$\frac{\partial w}{\partial x_1} = 1 + x_1 + x_1^2 + \cdots + x_1^{p-1}.$$

Therefore $D(x_1^p) = (1 + x_1 + x_1^2 + \cdots + x_1^{p-1})(1 - x_1)$. If we now pass to the quotient as described above we obtain a description of the map $\Lambda \xrightarrow{\phi} \Lambda^g$ as

$$w \longrightarrow \phi(w) = (1 + (1 + T_1) + (1 + T_1)^2 + \cdots + (1 + T_1)^{p-1}, 0, \dots, 0),$$

where we have replaced σ_1 with $1 + T_1$ (and we have assumed the generator x_1 restricts to a generator of Γ). Since the polynomial is irreducible, such a relation would produce no torsion in Z .

Example 5: As a second sample calculation, suppose again that \mathcal{G} is a one-relator group with defining relation $w = x_1^{-1}x_2^{-1}x_1x_2 = [x_1, x_2]$. We then find

$$D(w) = (-x_1^{-1} + x_1^{-1}x_2^{-1})(1 - x_1) + (-x_1^{-1}x_2^{-1} + x_1^{-1}x_2^{-1}x_1)(1 - x_2).$$

If we write g for the inverse of the unit power series $1 + T_1$, and write h for the inverse of $1 + T_2$, then after passing to the quotient we may describe the map ϕ by

$$w \longrightarrow \phi(w) = (-g(1 - h), h(1 - g), 0, \dots, 0).$$

Again, we see that such a relation would produce no torsion in Z .

4.3 Some Open Problems

Finally, we describe some open problems intended as possible future research projects related to this work.

1. The most obvious direction of generalization is to consider cyclotomic fields whose p -class groups have the form

$$A \simeq (\mathbb{Z}/p^n\mathbb{Z})^2,$$

together with the appropriate assumptions (Vandiver's conjecture, $\lambda(p) = 2$, and some sort of boundedness condition on $v_p(L_p(1, \omega^i))$). The argument given in Section 3.2 breaks down if \mathcal{G} is defined by *two* independent relations and it is not clear at all that a modification should exist. Rather, it seems a new approach will be required. We describe some possibilities below.

2. The example computations in the last section indicate that a computational approach to verifying Greenberg's conjecture may be possible. For example, in the one-relator case, if it could be shown that no relation in $F_g^{p^n}[F_g, F_g]$ could produce torsion in Z , then Greenberg's conjecture would be true. Although the two example calculations only touch the surface, the existence of "product rule" and "chain rule" type formulas for the Fox derivative make such an approach plausible. This approach also avoids the need of a boundedness condition on $v_p(L_p(1, \omega^i))$.

A good understanding of the Fox derivative may also help in the case of at least two defining relations. For example, suppose w_1 and w_2 are generators of Λ^s (so $s = 2$) such that

$$\begin{aligned} \phi(w_1) &= (p, T_2, 0, 0, \dots, 0) \\ \phi(w_2) &= (0, T_1, p, 0, \dots, 0). \end{aligned}$$

Then the element $z = (T_1, 0, -T_2, 0, \dots, 0)$ is non-zero in Z , but

$$p \cdot z = T_1\phi(w_1) - T_2\phi(w_2),$$

which is 0 in Z . So z is a torsion element which maps to 0 in \mathcal{G}^{ab} . Such “hidden torsion” might be ruled out by an understanding of the Fox derivative (i.e. the map ϕ).

3. As we have already stated, it is well known that the quantities g and s are given by the \mathbb{F}_p -dimensions of $H^1(\mathcal{G}, \mathbb{Z}/p\mathbb{Z})$ and $H^2(\mathcal{G}, \mathbb{Z}/p\mathbb{Z})$ respectively. Using the cup product pairing

$$H^1(\mathcal{G}, \mathbb{Z}/p\mathbb{Z}) \times H^1(\mathcal{G}, \mathbb{Z}/p\mathbb{Z}) \longrightarrow H^2(\mathcal{G}, \mathbb{Z}/p\mathbb{Z}),$$

one might hope to extract information about the relations in \mathcal{G} . This approach has been quite successful in the case that \mathcal{G} is a Demushkin group (although \mathcal{G} is certainly *not* Demushkin in the cases we consider).

We may, for our choice of base field K , identify the cohomology group $H^1(\mathcal{G}, \mathbb{Z}/p\mathbb{Z})$ with a subgroup of $K^\times / (K^\times)^p$ (namely the subgroup consisting of elements whose p -th roots generate p -unramified extensions). The group $H^2(\mathcal{G}, \mathbb{Z}/p\mathbb{Z})$ may be identified with a quotient of the ideal class group of K . Using these identifications, the description of the cup product pairing takes on a rather “algorithmic” look based on ideal norm computations.

4. Finally, there are questions on the nature of the generators of the annihilator of X . For example, how many are there? Greenberg’s conjecture only predicts there are more than one.

Also, there is some evidence that in certain cases the generators are very special power series. For example, suppose K is an imaginary quadratic field in which p splits. K has two independent \mathbb{Z}_p -extensions, and so X is a module over the ring $\mathbb{Z}_p[[T_1, T_2]]$. The Main conjecture for elliptic curves gives the two variable p -adic L -functions attached to each of the primes above p as annihilators of X . There seems to be no reason not to believe the two functions to be independent. This example was in fact part of the motivation behind Greenberg’s conjecture.

REFERENCES

- [1] W. Bruns and J. Herzog. *Cohen-Macaulay Rings*. Cambridge Studies in Advanced Math, **39**. Cambridge University Press, Great Britain, 1993.
- [2] J. Buhler, R. Crandall, R. Ernvall, and T. Metsankyla. Irregular primes and cyclotomic invariants up to four million. *Math. Comp.* **61**: 151-153, 1993.
- [3] J.W.S. Cassels, A. Frohlich, editors. *Algebraic Number Theory*. Academic Press, New York, 1967.
- [4] B. Ferrero and L. Washington. The Iwasawa invariant μ_p vanishes for abelian number fields. *Ann. of Math.*, **109**: 377-395, 1979.
- [5] R. Fox. Free differential calculus I. Derivation in the free group ring. *Annals of Math.*, **57**: 547-560, 1953.
- [6] R. Greenberg. On the structure of certain Galois groups. *Invent. Math.*, **47**: 85-99, 1978.
- [7] R. Greenberg. Iwasawa theory - past and present, preprint.
- [8] H. Ichimura and H. Sumida. On the Iwasawa invariants of certain real abelian fields II. *Internat. J. Math.*, **7**, no.6: 721-744, 1996.
- [9] K. Iwasawa. On solvable extensions of algebraic number fields. *Ann. of Math.*, **58**: 548-572, 1953.
- [10] K. Iwasawa. On Γ -extensions of algebraic number fields. *Bull. Amer. Math. Soc.*, **65**: 183-226, 1959.
- [11] K. Iwasawa. On \mathbb{Z}_l -extensions of algebraic number fields. *Ann. of Math.*, **98**: 246-326, 1973.
- [12] K. Iwasawa. Riemann-Hurwitz formula for p -adic Galois representations for number fields. *Tohoku Math. J.*, **33**: 263-288, 1981.
- [13] K. Iwasawa and C. Sims. Computation of invariants in the theory of cyclotomic fields. *J. Math. Soc. Japan*, **18**: 86-96, 1965.
- [14] U. Jannsen. Iwasawa modules up to isomorphism. *Advanced Studies in Pure Math*, **17**: 171-207, 1989.
- [15] H. Koch. *Algebraic Number Theory*. English translation. Springer-Verlag, Berlin, 1997.

- [16] J. Kraft and R. Schoof. Computing Iwasawa modules of real quadratic number fields. Special issue in honor of Frans Oort. *Compositio Math.*, **97**, no.1-2: 135-155, 1995.
- [17] J. Labute. Classification of Demushkin groups. *Canad. J. Math.*, **19**: 106-132, 1967.
- [18] S. Lang. *Cyclotomic Fields I and II*. Graduate Texts in Mathematics, Springer-Verlag, New York, 1990.
- [19] W. McCallum. On the Iwasawa theory of multiple \mathbb{Z}_p -extensions of number fields, preprint.
- [20] J. Neukirch, A. Schmidt, and K. Wingberg. *Cohomology of Number Fields*. Grundlehren der mathematischen Wissenschaften, **323**, Springer-Verlag, 2000.
- [21] T. Nguyen-Quang-Do. Formations de classes et modules d'Iwasawa. *Number Theory*, Noordwijkerhout. Springer Lecture Notes, **1068**: 167-185, 1984.
- [22] K. Ribet. Galois representations and modular forms. *Bulletin of the AMS*, **32**: 375-402, 1995.
- [23] J.P. Serre. Classes des corps cyclotomiques (d'après K. Iwasawa). Sem. Bourbaki, Exp. no. 174, 1958.
- [24] J.P. Serre. *Local Fields*. Graduate Texts in Mathematics, Springer-Verlag, 1975.
- [25] J.P. Serre. *Topics in Galois Theory*. Jones and Bartlett, Boston, MA, 1992.
- [26] J.P. Serre. *Galois Cohomology*, english translation. Springer-Verlag: Berlin Heidelberg, 1997.
- [27] I. Shafarevich. On p -extensions. *Collected Mathematical Papers*, Springer-Verlag, Berlin Heidelberg New York: 6-19, 1989.
- [28] L. Washington. *Introduction to Cyclotomic Fields*, Second Edition, Graduate Texts in Mathematics, Springer-Verlag, New York, 1997.
- [29] K. Wingberg. On Galois groups of p -closed algebraic number fields with restricted ramification. *J. Reine Angew. Math.*, **400**: 185-202, 1989.
- [30] M. Yamagishi. A note on free pro- p extensions of algebraic number fields. *J. Theor. Nombres Bordx.*, **5**: 165-178, 1993.
- [31] M. Yamagishi. On free pro- p extensions of algebraic number fields. Moduli Spaces, Galois Representations, and L -functions (Japanese), (Kyoto, 1993, 1994), **884**: 172-177, 1994.