# On $T$-Semisimplicity of Iwasawa Modules and Some Computations with $\mathbb{Z}_3$-Extensions

Yannick Van Huele

A dissertation
submitted in partial fulfillment of the
requirements for the degree of

Doctor of Philosophy

University of Washington

2016

Reading Committee:

Ralph Greenberg, Chair

William A. Stein

Max Lieblich

Program Authorized to Offer Degree:
Mathematics

University of Washington

**Abstract**

On $T$-Semisimplicity of Iwasawa Modules and Some Computations with $\mathbb{Z}_3$-Extensions

Yannick Van Huele

Chair of the Supervisory Committee:
Professor Ralph Greenberg
Department of Mathematics

For certain $\mathbb{Z}_p$-extensions of abelian number fields, we study the Iwasawa module associated to the ideal class groups. We show that generic $\mathbb{Z}_p$-extensions of abelian number fields are $T$-semisimple. We also construct the first few layers of the anti-cyclotomic $\mathbb{Z}_3$-extension of certain imaginary quadratic number fields and use these to study the Iwasawa modules corresponding to certain $\mathbb{Z}_3$-extensions of quadratic and biquadratic fields. In particular, we are able to show in some cases that the Iwasawa module is either finite or $T$-semisimple.

# TABLE OF CONTENTS

# LIST OF FIGURES

# LIST OF TABLES

# ACKNOWLEDGMENTS

First and foremost, I would like to thank my adviser, Ralph Greenberg, for introducing me to this beautiful area of mathematics and for much help and guidance throughout my graduate studies.

I would also like to thank William Stein and all of the people who have worked on Sage and the Sage Math Cloud. This thesis would have turned out very differently without the easy access to computing resources and powerful algorithms provided by Sage and the Sage Math Cloud.

Finally, I would like to thank Bharathwaj Palvannan who navigated through the the process of getting a PhD in Iwasawa theory just a little before me, making each step in my journey a little smoother – not least by introducing me to the U-District Zoka, whose tables and teas supported many hours of research.

# DEDICATION

To Alla and all my fellow UW math graduate students.

# Chapter 1

# INTRODUCTION

Let $p$ be an odd prime. In this paper we study the Iwasawa module of class groups associated to a $\mathbb{Z}_p$-extension of a number field and try to answer two questions: For what number fields and $\mathbb{Z}_p$-extensions is the corresponding Iwasawa module $T$-semisimple? And for what number fields and $\mathbb{Z}_p$-extensions is the Iwasawa module finite?

The question of $T$-semisimplicity was first raised by Coates and Lichtenbaum in [6] where they conjectured that the Iwasawa module attached to the cyclotomic $\mathbb{Z}_p$-extension of a number field is always $T$-semisimple. This was proven by Greenberg in [13] when the base field is abelian and then generalized to some other special $\mathbb{Z}_p$-extensions by Carroll and Kisilevsky in [4]. However, in [20] Kisilevsky constructed examples where the Iwasawa module is not $T$-semisimple. We build upon these results to show that the Iwasawa modules associated to generic $\mathbb{Z}_p$-extensions of abelian number fields are $T$-semisimple.

The Iwasawa module for the cyclotomic extension has been extensively studied, but the Iwasawa modules for other $\mathbb{Z}_p$-extensions much less so. There are several difficulties associated with studying the Iwasawa modules associated to noncyclotomic extensions. One such difficulty is the lack of (known) connection to $p$-adic $L$-functions for most of these extensions. Another difficulty is the lack of an explicit construction for the layers of these $\mathbb{Z}_p$-extensions. We give such a construction for the first few layers of particular number fields and use these to compute the class groups. Often, we are then able to show that the Iwasawa module is finite and provide the full structure of the module.

Chapters 2 and 3 set up the background results: Chapter 2 deals with $\mathbb{Z}_p$-extensions of number fields and the Iwasawa modules associated to the ideal class groups. We discuss the structure theorem for finitely generated $\Lambda$-modules and describe the relationship between

the Iwasawa module and the class groups of the layers of the $\mathbb{Z}_p$-extension. In particular, we discuss conditions under which the Iwasawa module is finite. Chapter 3 introduces the concept of $T$-semisimplicity. We present the results of Greenberg and Carroll-Kisilevsky that certain $\mathbb{Z}_p$-extensions of abelian number fields are $T$-semisimple. In particular, we examine the relationship between the decomposition subgroups for primes above $p$ and the known results about $T$-semisimplicity. We also discusss Kisilevsky's examples of nonsemisimple $\mathbb{Z}_p$-extensions.

Chapter 4 deals with new results about $T$-semisimplicity and nonsemisimplicity. More specifically, we explore the following question: If $K$ is a number field admitting one $\mathbb{Z}_p$-extension which is $T$-semisimple, what can we say about the other $\mathbb{Z}_p$-extensions of $K$? Similarly, if $K$ admits a $\mathbb{Z}_p$-extension which is not $T$-semisimple, what can be said about the other $\mathbb{Z}_p$-extensions of $K$? The main result of this chapter (Theorem 4.1.3) is a proof that every $\mathbb{Z}_p$-extension of an abelian number field which is not anti-cyclotomic is $T$-semisimple. As generic $\mathbb{Z}_p$-extensions of a CM number field are not anti-cyclotomic, this shows that generic $\mathbb{Z}_p$-extensions of abelian number fields are $T$-semisimple, a result which was proven independently by Kataoka in [19]. We also show that the existence of one $\mathbb{Z}_p$-extension which is not $T$-semisimple implies the existence of additional $\mathbb{Z}_p$-extensions of $K$ which are not $T$-semisimple (Proposition 4.2.1).

Chapters 5 and 6 are computational. In Chapter 5 we discuss a method for computing the layers of a $\mathbb{Z}_p$-extension: that is, for layer $K_n$ of a $\mathbb{Z}_p$-extension $K_\infty/K$, our method returns a polynomial which determines $K_n/\mathbb{Q}$. We use this method to determine the first few layers of the anticyclotomic $\mathbb{Z}_3$-extension of certain quadratic fields. In Chapter 6 we then describe the 3-part of the class groups of these fields. In particular, for some examples we are able to deduce $T$-semisimplicity or even finiteness of the corresponding Iwasawa modules using information about the class group of the first or second layer of the $\mathbb{Z}_3$-extension. Our computations provide examples of $\mathbb{Z}_p$-extensions which are algebraically $T$-semisimple, but not arithmetically $T$-semisimple, answering a question of Jaulent and Sands (Question 3.6.1). We also highlight some examples where further study may be interesting (Examples 6.2.10 and

6.3.1) along with some new questions which arise from our computations (Question 6.2.3).

Our computations come with a disclaimer: In order to perform the computations in a feasible amount of time, we often made use of algorithms whose validity rests on unproven conjectures (in particular the generalized Riemann hypothesis). In theory, given a sufficiently powerful machine and sufficient time, these computations could be rigorously verified.

All the computations were performed in Sage [9] using the Sage Math Cloud, with many of the algorithms coming from PARI [25].

A glossary of commonly used symbols is proved at the end of this document.

# Chapter 2

# BACKGROUND ON CLASSICAL IWASAWA THEORY

In this chapter we present just the background results from Iwasawa theory that we need to study our particular problem of $T$-semisimplicity. For a more comprehensive treatment, see for example Greenberg's survey article [15], Chapter 13 of Washington's book [26]. I would also recommend the first few chapters from the draft of Greenberg's unfinished book [11].

## *2.1 $\mathbb{Z}_p$-Extensions*

Throughout this chapter (and, indeed, throughout the paper), $p$ will denote an odd prime.

**Definition 2.1.1** ($\mathbb{Z}_p$-Extension)**.** Let $K$ be a number field. A $\mathbb{Z}_p$-extension of $K$ is a Galois extension $K_\infty/K$ whose Galois group is isomorphic to the additive group of $p$-adic integers:

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

We will generally denote $\mathrm{Gal}(K_\infty/K)$ by $\Gamma$.

The closed subgroups of $\mathbb{Z}_p$ are the trivial group along with the subgroups of the form $p^n\mathbb{Z}_p$ for $n \geq 0$. Thus, a $\mathbb{Z}_p$-extension $K_\infty/K$ with Galois group $\Gamma = \mathrm{Gal}(K_\infty/K)$ contains a unique intermediate field $K \subseteq K_n \subseteq K_\infty$ satisfying $\mathrm{Gal}(K_n/K) \simeq \mathbb{Z}/p^n\mathbb{Z}$ for each $n \geq 0$, namely the fixed field of the subgroup $\Gamma^{p^n}$. These fields, along with $K_\infty$ itself, give all subfields of $K_\infty$ containing $K$. We will often identify a $\mathbb{Z}_p$-extension $K_\infty/K$ with this tower of fields. (See Figure 2.1)

The group $\mathbb{Z}_p$ is not itself cyclic, but contains (infinitely many) dense cyclic subgroups. If $K_\infty/K$ is a $\mathbb{Z}_p$-extension and $\gamma_0$ is any element of $\Gamma = \mathrm{Gal}(K_\infty/K)$ whose restriction to

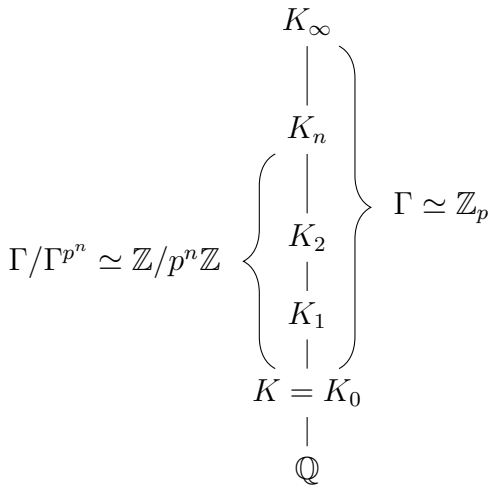


Figure 2.1: A $\mathbb{Z}_p$-extension of $K$ as a tower of fields.

$K_1$ is not the identity element of $\mathrm{Gal}(K_1/K)$, then $\gamma_0$ generates a dense cyclic subgroup of $\Gamma$. We call $\gamma_0$ a *topological generator* for $\Gamma$.

Working with $\mathbb{Z}_p$-extensions allows us to study objects of arithmetic interest in a nice family of number fields. For example, class numbers of number fields are rather mysterious objects. However, Iwasawa showed that a nice pattern emerges when studying the class numbers of fields in a $\mathbb{Z}_p$-extension.

**Theorem 2.1.2** (Iwasawa)**.** *Let $K$ be a number field and $K_\infty/K$ a $\mathbb{Z}_p$-extension. For each $n \geq 0$, let $p^{e_n}$ denote the exact power of $p$ dividing the class number of $K_n$. Then there exist constants $\lambda = \lambda_{K_\infty}$, $\mu = \mu_{K_\infty}$, and $\nu = \nu_{K_\infty}$ such that*

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

*for all $n >> 0$.*

Before discussing this theorem in more detail, let us spend some more time discussing $\mathbb{Z}_p$-extensions. $\mathbb{Z}_p$-extensions of number fields have nice ramification properties.

**Proposition 2.1.3.** *Let $K$ be a number field and suppose $K_\infty/K$ is a $\mathbb{Z}_p$ extension. Then the only primes which may ramify in $K_\infty/K$ are the primes lying above $p$. Furthermore, at least one such prime is ramified and there exists $n_0 \geq 0$ such that every prime which is ramified in $K_\infty/K$ is totally ramified in $K_\infty/K_n$ for all $n \geq n_0$.*

A proof can be found in [26] (see Proposition 13.2 and Lemma 13.3).

**Example 2.1.4** (The Cyclotomic Extension)**.** One example of a $\mathbb{Z}_p$-extension is easy to construct. Consider the field $\mathbb{Q}(\mu_{p^\infty})$ obtained by adjoining all the $p$-th power roots of unity to $\mathbb{Q}$:

$$\mathbb{Q}(\mu_{p^\infty}) = \bigcup_{n \geq 0} \mathbb{Q}(\mu_{p^n}).$$

The extension $\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}$ is Galois with Galois group

$$\begin{aligned} \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) &\simeq \lim_{\leftarrow} \mathrm{Gal}(\mathbb{Q}(\mu_{p^n})/\mathbb{Q}) \\ &\simeq \lim_{\leftarrow} (\mathbb{Z}/p^n\mathbb{Z})^\times \\ &\simeq \mathbb{Z}_p^\times. \end{aligned}$$

Using the $p$-adic logarithm map, one can show that

$$\mathbb{Z}_p^\times \simeq \mu_{p-1} \times (1 + p\mathbb{Z}_p) \simeq \mu_{p-1} \times \mathbb{Z}_p.$$

Thus, $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q})$ admits a unique quotient group isomorphic to $\mathbb{Z}_p$, and hence there exists a unique intermediate field $\mathbb{Q} \subseteq \mathbb{Q}_\infty \subseteq \mathbb{Q}(\mu_{p^\infty})$ satisfying $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q}) \simeq \mathbb{Z}_p$. We call $\mathbb{Q}_\infty$ the *cyclotomic* $\mathbb{Z}_p$-extension of $\mathbb{Q}$.

The cyclotomic extension $\mathbb{Q}_\infty$ is in fact the only $\mathbb{Z}_p$-extension of $\mathbb{Q}$. To see this, suppose that $K_\infty/\mathbb{Q}$ is a $\mathbb{Z}_p$ extension. Then $K_\infty/\mathbb{Q}$ is an abelian extension which, by Proposition 2.1.3, is only ramified at $p$. Thus, the Kronecker-Weber Theorem and class field theory tell us that $K_\infty \subseteq \mathbb{Q}(\mu_{p^\infty})$. But there is exactly one such field satisfying $\mathrm{Gal}(K_\infty/\mathbb{Q}) \simeq \mathbb{Z}_p$, namely $\mathbb{Q}_\infty$.

One can use the field $\mathbb{Q}_\infty$ to construct $\mathbb{Z}_p$-extensions of arbitrary number fields as follows: Let $K$ be a number field and let $K_\infty$ denote the compositum of $K$ and $\mathbb{Q}_\infty$. Then the

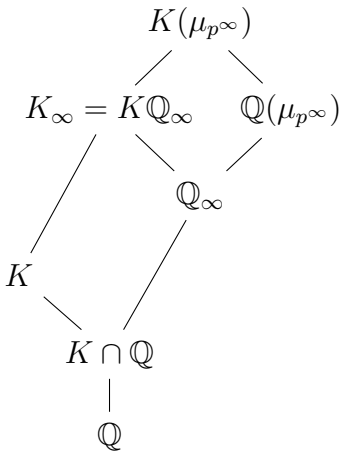


Figure 2.2: The cyclotomic $\mathbb{Z}_p$-extension of a number field.

restriction map gives an isomorphism

$$\mathrm{Gal}(K_\infty/K) \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}_\infty/K \cap \mathbb{Q}) \simeq \mathbb{Z}_p.$$

The field $K\mathbb{Q}_\infty$ is called the cyclotomic $\mathbb{Z}_p$-extension of $K$ and can be characterized as the unique $\mathbb{Z}_p$-extension of $K$ contained in $K(\mu_{p^\infty})$. (See Figure 2.2.)

Unlike $\mathbb{Q}$, an arbitrary number field $K$ may admit many different $\mathbb{Z}_p$-extensions.

**Theorem 2.1.5.** *Let $K$ be a number field and let $\tilde{K}_\infty$ denote the compositum of all $\mathbb{Z}_p$-extensions of $K$. Let $r_1$ denote the number of real embeddings of $K$ and let $r_2$ denote the number of pairs of complex embeddings of $K$. Then*

$$\mathrm{Gal}(\tilde{K}_\infty/K) \cong \mathbb{Z}_p^r$$

*for some $r_2 + 1 \leq r \leq [K : \mathbb{Q}]$.*

A proof is given in Section 2 of [15]. Thus, if $K$ is a number field with any complex embeddings, $\mathrm{Gal}(\tilde{K}/K) \cong \mathbb{Z}_p^s$ for some $s \geq 2$. The group $\mathbb{Z}_p^s$ has uncountably many distinct quotients isomorphic to $\mathbb{Z}_p$. It follows that any number field $K$ which is not totally real

admits uncountably many $\mathbb{Z}_p$-extensions. The $\mathbb{Z}_p$-rank of $\mathrm{Gal}(\tilde{K}_\infty/K)$ can be described using class field theory and is related to the $\mathbb{Z}_p$-rank of the closure of the units $\mathcal{O}_K^\times$ under the inclusion into the product of the local units (completing at primes above $p$). The precise value of $r$ is predicted by Leopoldt's conjecture.

**Conjecture 2.1.6** (Leopoldt's Conjecture)**.** *The lower bound for $r$ in Theorem 2.1.5 is in fact the correct value, i.e., $r = r_2 + 1$.*

(To see a clearer relation to the units group of $\mathcal{O}_K$, note that $r_2 + 1 = (r_1 + 2r_2) - (r_1 + r_2 - 1) = [K : \mathbb{Q}] - \mathrm{rank}_{\mathbb{Z}}(\mathcal{O}_K^\times)$.)

Though the general case of Leopoldt's conjecture is still open, it has been proven in the case of abelian number fields by work of Ax [1] and Brumer [2].

**Theorem 2.1.7.** *Let $K$ be an abelian number field and $\tilde{K}_\infty$ the compositum of all $\mathbb{Z}_p$-extensions of $K$. Then*

$$\mathrm{Gal}(\tilde{K}_\infty/K) \simeq \mathbb{Z}_p^{r_2+1},$$

*where $r_2$ is the number of pairs of complex embeddings $K \hookrightarrow \mathbb{C}$.*

In this case, one can often say more.

**Theorem 2.1.8.** *Let $K/\mathbb{Q}$ be an abelian extension with Galois group $\Delta = \mathrm{Gal}(K/\mathbb{Q})$ of exponent dividing $p-1$. Then, for each character $\chi$ of $\Delta$ which is odd or trivial, there exists a unique $\mathbb{Z}_p$-extension $K_\infty^\chi/K$ such that $K_\infty^\chi/\mathbb{Q}$ is Galois and*

$$\mathrm{Gal}(K_\infty^\chi/\mathbb{Q}) \simeq \Gamma \rtimes_\chi \Delta.$$

Note that $\Delta$ admits precisely $r_2 + 1$ characters which are trivial or odd so this result is consistent with Leopoldt's conjecture. For a proof of Theorem 2.1.8, see either Theorem 1 of [5] or Proposition 3.2.1 of [16] (for a generalization).

**Example 2.1.9.** Let $\chi = \chi_0$, the trivial character of $\Delta$. Note that $K_\infty^{\chi_0}$ is an abelian extension of $\mathbb{Q}$. It follows that $K_\infty^{\chi_0} = K_\infty^{cyc}$,the cyclotomic $\mathbb{Z}_p$-extension of $K$.

**Example 2.1.10** (The Anti-cyclotomic Extension)**.** Let $K$ be an imaginary quadratic field and let $\chi$ denote the nontrivial character of $\Delta = \mathrm{Gal}(K/\mathbb{Q})$. The character $\chi$ is odd and the $\mathbb{Z}_p$-extension $K_\infty^\chi/K$ is called the *anti-cyclotomic* $\mathbb{Z}_p$-extension of $K$, which we will sometimes denote $K_\infty^{anti}$.

**Example 2.1.11.** Let $K = \mathbb{Q}(\mu_p)$ and $\Delta = \mathrm{Gal}(K/\mathbb{Q})$. Let $\omega \in \hat{\Delta}$ be the Teichmüller character – the character by which $\Delta$ acts on $\mu_p$. That is, for each $\delta \in \Delta$,

$$\omega(\delta) = a_\delta,$$

where $a_\delta \in \mu_{p-1} \subseteq \mathbb{Z}_p^\times$ is the unique root of unity satisfying

$$\delta(\zeta) = \zeta^{a_\delta} \qquad \text{for all } \zeta \in \mu_p.$$

The character group of $\Delta$ is cyclic of order $p-1$ and generated by $\omega$. We will see in Example 5.0.3 that the first layer of $K_\infty^\omega$ is given by $\mathbb{Q}(\mu_p, \sqrt[p]{p})$. And, in Section 5.1 we determine the second and third layers in the case where $p = 3$ (in this case $K_\infty^\omega = K_\infty^{anti}$).

## *2.2* $\Lambda$*-Modules*

The idea behind Iwasawa theory is to study objects of arithmetic interest in towers of fields. For us, the towers will be $\mathbb{Z}_p$-extensions and the objects of arithmetic interest are (the $p$-parts of) class groups of the fields the tower. We study these using class field theory: that is, we will study both the class groups and the corresponding Galois groups.

Let $K$ be a number field and let $K_\infty$ be a $\mathbb{Z}_p$-extension of $K$. As usual, let $\Gamma = \mathrm{Gal}(K_\infty/K)$. For each $n \geq 0$, let $L_n$ denote the $p$-Hilbert class field of $K_n$, i.e., the maximal extension of $K_n$ which is pro-$p$, abelian, and unramified. Thus, $L_n$ is the maximal pro-$p$ extension of $K_n$ contained in the Hilbert class field of $K_n$. For $n \geq m \geq 0$, note that $K_nL_m/K_n$ is a pro-$p$, abelian, and unramified extension. Hence,

$$L_m \subseteq K_nL_m \subseteq L_n.$$

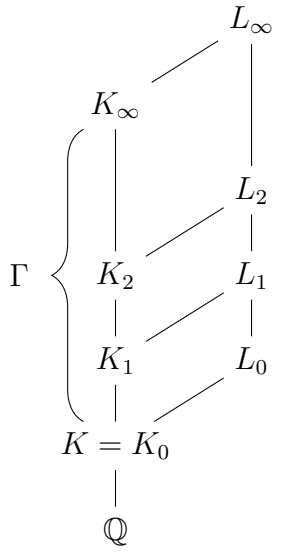


Figure 2.3: The tower of $p$-Hilbert class fields.

Let $L_\infty$ denote the compositum of all the $L_n$:

$$L_\infty = \bigcup_{n \geq 0} L_n.$$

We call $L_\infty$ the pro-$p$ Hilbert class field of $K_\infty$. The pro-$p$ Hilbert class field $L_\infty$ can be characterized as the maximal extension of $K_\infty$ which is pro-$p$, abelian, and unramified. Let us denote by $A_n$ the $p$-primary part of the class group of $K_n$, i.e., $A_n = \mathrm{Cl}(K_n)[p^\infty]$. the Artin map induces an isomorphism $\mathrm{Gal}(L_n/K_n) \cong A_n$. By working with the Artin map and properties of the Frobenius automorphism, one can show that the corresponding map $A_n \to A_m$ is the map induced by the norm map on ideals. That is, for each pair $n \geq m$ we have the following commutative diagram:

$$\begin{array}{ccc} \mathrm{Gal}(L_n/K_n) & \xleftarrow{\sim} & A_n \\ \Big\downarrow{\scriptstyle \mathrm{res}} & & \Big\downarrow{\scriptstyle N_{K_n/K_m}} \\ Gal(L_m/K_m) & \xleftarrow{\sim} & A_m \end{array}$$

Furthermore, these maps form a projective system and so we obtain isomorphisms

$$\mathrm{Gal}(L_\infty/K_\infty) \cong \varprojlim \mathrm{Gal}(L_n/K_n) \cong \varprojlim A_n,$$

where the inverse limits are taken with respect to the restriction maps and norm maps, respectively.

Let $X = \mathrm{Gal}(L_\infty/K_\infty)$. By maximality, we see that $L_\infty$ is Galois over $K$ and we have a short exact sequence:

$$1 \to X \to \mathrm{Gal}(L_\infty/K) \to \Gamma \to 1 \tag{2.2.1}$$

Because $X$ is an abelian normal subgroup of $\mathrm{Gal}(L_\infty/K)$, we can define an action of $\Gamma$ on $X$ as follows. Let $\gamma \in \Gamma$ and let $\tilde{\gamma} \in \mathrm{Gal}(L_\infty/K)$ be any element satisfying $\tilde{\gamma}|_{K_\infty} = \gamma$. Define

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

for all $x \in X$. Note that $\gamma \cdot x$ does not depend on the choice of $\tilde{\gamma}$ since $X$ is abelian and, hence, the action is well defined. The group $X$ is also a pro-$p$ group and, thus, admits a continuous action of $\mathbb{Z}_p$. The actions of $\Gamma$ and $\mathbb{Z}_p$ are compatible, making $X$ into a $\mathbb{Z}_p[\Gamma]$-module. However, it will be more convenient to view $X$ as a module over the completed group ring $\mathbb{Z}_p[[\Gamma]]$.

Serre showed that one can identify $\Lambda$ (noncanonically) with the power series ring $\mathbb{Z}_p[[T]]$ as follows: Let $\gamma_0$ denote a topological generator of $\Gamma$. Then the map

$$\begin{array}{ccc} \mathbb{Z}_p[[\Gamma]] & \longrightarrow & \mathbb{Z}_p[[T]] \\ \gamma_0^z & \mapsto & (1+T)^z \qquad \forall z \in \mathbb{Z}_p \end{array}$$

is an isomorphism. Here, $(1+T)^z$ is defined as follows:

$$(1+T)^z = \sum_{i=0}^{\infty} \binom{z}{i} T^i, \qquad \text{where } \binom{z}{i} = \frac{1}{i!} \prod_{j=1}^{i} (z-j+1) \tag{2.2.2}$$

(Note that this reduces the usual formula when $z$ is an integer.) In particular, note that

$$(1+T)^z = 1 + zT + T^2 f_z$$

for some $f_z \in \Lambda$.

Although the ring $\mathbb{Z}_p[[T]]$ is not a PID, it comes close:

**Fact 2.2.1.**

*(a) The ring $\mathbb{Z}_p[[T]]$ is a local ring with maximal ideal $\mathfrak{m} = (p, T)$.*

*(b) The ring $\mathbb{Z}_p[[T]]$ is noetherian and a unique factorization domain.*

*(c) The ring $\mathbb{Z}_p[[T]]$ has Krull dimension 2 and all height-1 prime ideals are principal and each such height-1 prime is either generated by $p$ or by a monic irreducible polynomial $f(T)$ of the form*

$$f(T) = T^n + pg(T)$$

*for some $n \geq 1$ and $g(T) \in \mathbb{Z}_p[[T]]$. Such an $f$ is called distinguished.*

One way in which the ring $\mathbb{Z}_p[[T]]$ is similar to a PID is that there is a nice description of finitely generated modules over $\mathbb{Z}_p[[T]]$. In order to state it, we first need to introduce the concept of a pseudo-isomorphism.

**Definition 2.2.2.** Let $X$ and $Y$ be finitely generated $\mathbb{Z}_p[[T]]$ modules. A map $F : X \to Y$ is said to be a *pseudo-isomorphism* if $F$ has finite kernel and cokernel.

If we restrict our attention to torsion modules, pseudo-isomorphim determines an equivalence relation: that is, there exists a pseudo-isomorphism $X \to Y$ if and only if there exists a pseudo-isomorphism $Y \to X$. In this case, we write $X \sim Y$.

If $X$ and $Y$ are not torsion modules, pseudo-isomorphism no longer determines an equivalence relation. For example, let $\mathfrak{m} = (p, T)$, the maximal ideal of $\mathbb{Z}_p$. The inclusion $\mathfrak{m} \hookrightarrow \mathbb{Z}_p[[T]]$ is injective with finite cokernel, but there is no pseudo-isomorphism $\mathbb{Z}_p[[T]] \to \mathfrak{m}$.

**Theorem 2.2.3** (Structure Theorem)**.** *Let $X$ be a finitely generated $\mathbb{Z}_p[[T]]$-module. Then there exists a pseudo-isomorphism*

$$X \to \Lambda^r \oplus \bigoplus_{i=1}^{s} \frac{\Lambda}{(f_i(T)^{a_i})}$$

*where each* $(f_i(T))$ *is a height-*1 *prime of* $\mathbb{Z}_p[[T]]$*. Furthermore, the values of* $r$ *and* $s$*, the prime ideals* $(f_i(T))$ *and the corresponding* $a_i$ *are uniquely determined by* $X$*, up to their order.*

If $X$ is a torsion module, then $r = 0$ and, separating $(p)$ from the other height-1 primes, we obtain

$$X \sim \bigoplus_{i=1}^{s} \frac{\Lambda}{(g_i(T)^{a_i})} \oplus \bigoplus_{j=1}^{t} \frac{\Lambda}{(p^{b_j})} \tag{2.2.3}$$

where each $g_i(T)$ is a distinguished irreducible polynomial.

### *2.3* $\mathrm{Gal}(L_\infty/K_\infty)$ *as a* $\Lambda$*-module*

Iwasawa showed that $X = \mathrm{Gal}(L_\infty/K_\infty)$ is a finitely generated torsion $\Lambda$-module. In fact, the invariants in Theorem 2.1.2 can be written as

$$\lambda = \sum_{i=1}^{s} a_i \deg(g_i) \quad \text{and} \quad \mu = \sum_{j=1}^{t} b_j,$$

where $g_i, a_i$, and $b_j$ are as in Equation 2.2.3. This can be deduced from the following results which relate the class groups to the Iwasawa module.

We start with a simple case.

**Proposition 2.3.1.** *Let* $K$ *be a number field with a unique prime lying above* $p$ *and let* $K_\infty/K$ *be a* $\mathbb{Z}_p$*-extension in which this prime is totally ramified. Then* $X = \mathrm{Gal}(L_\infty/K_\infty)$ *is a finitely generated torsion* $\Lambda$*-module and, for all* $n \geq 0$*,*

$$\mathrm{Gal}(L_n/K_n) \simeq X/\omega_n X,$$

*where* $\omega_n = (1+T)^{p^n} - 1$*.*

A proof of Proposition 2.3.1 can be found in Section 1 of [15]. Note that this result is independent of the choice of isomorphism $\Lambda \simeq \mathbb{Z}_p[[T]]$. Indeed, one could describe the module $X/\omega_n X$ intrinsically as $X_{\Gamma^{p^n}}$, the maximal quotient of $X$ fixed by $\Gamma^{p^n}$. More generally, we have the following result:

**Theorem 2.3.2** (Iwasawa)**.** *Let $K_\infty/K$ be a $\mathbb{Z}_p$-extension. Choose $n_0$ so that all the primes of $K_{n_0}$ which are ramified in $K_\infty/K_{n_0}$ are totally ramified. Let $X = \mathrm{Gal}(L_\infty/K_\infty)$ and $Y = \mathrm{Gal}(L_\infty/L_{n_0}K_\infty)$. Then $X$ is a finitely generated torsion $\Lambda$-module and, for all $n \geq n_0$,*

$$\mathrm{Gal}(L_n/K_n) \simeq X/\nu_{n,n_0}Y,$$

*where, for $m \leq n$,*

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

### *2.4 The Genus Field of $K_\infty/K$ and Trivial Zeros*

**Definition 2.4.1.** Let $F'/F$ be a pro-cyclic, pro-$p$ extension of number fields. The *genus field* of $F'/F$ is the maximual unramified pro-$p$ extension of $F'$ which is abelian over $F$.

Note that our definition of genus field is unorthodox in that we take the genus field to be a pro-$p$ extension of the base field. Thus, our genus field is a subfield of the field one normally calls the genus field. (See for example Section 6 of [8].)

Of particular interest to us is the genus field of $K_\infty/K$, where $K_\infty/K$ is a $\mathbb{Z}_p$-extension. We will denote this genus field by $L_\infty^*$ and often refer to it simply as the genus field of $K_\infty$. In this case $L_\infty^*$ is the maximal field $K_\infty \subseteq L_\infty^* \subseteq L_\infty$ such that $L_\infty^*/K$ is abelian.

Let $\mathcal{G} = \mathrm{Gal}(L_\infty/K)$. Then

$$\mathrm{Gal}(L_\infty^*/K) \simeq \mathcal{G}/\mathcal{G}',$$

where $\mathcal{G}'$ denotes the commutator subgroup of $\mathcal{G}'$. The quotient $\mathcal{G}/X \simeq \Gamma$ is abelian so we see that $\mathcal{G}' \subseteq X$. Note that the subgroup $TX$ consists of commutators so $TX \subseteq \mathcal{G}'$. We have an exact sequence:

$$1 \to X/TX \to \mathcal{G}/TX \to \Gamma \to 1.$$

And, just like the sequence from Equation (2.2.1), this sequence also splits. But $\Gamma$ acts trivially on $X/TX$ so we see that $\mathcal{G}/TX$ is abelian. It follows that $\mathcal{G}' \subseteq TX$ and thus that $\mathcal{G}' = TX$. This implies the following lemma.

**Lemma 2.4.2.** *Let $L_\infty^*$ denote the genus field of $K_\infty/K$ and let $X = \mathrm{Gal}(L_\infty/K_\infty)$. Then $\mathrm{Gal}(L_\infty^*/K_\infty) \simeq X/TX$.*

Given a $\mathbb{Z}_p$-extension $K_\infty/K$, determining the structure of $X$ can be quite difficult. Determining $L_\infty^*$, and thus $X/TX$, is simpler. We illustrate this in the special case when $p$ splits completely in $K/\mathbb{Q}$.

**Proposition 2.4.3.** *Let $K/\mathbb{Q}$ be a number field for which Leopoldt's conjecture holds and suppose $p$ splits completely in $K$. Let $r_2$ denote the number of pairs of complex embeddings of $K$. Let $K_\infty/K$ be a $\mathbb{Z}_p$-extension in which all primes above $p$ are ramified. Then*

$$X/TX \sim \mathbb{Z}_p^{r_2}.$$

*Proof.* Let $L_\infty^*$ denote the genus field of $K_\infty/K$. Let $\tilde{K}_\infty$ denote the compositum of all $\mathbb{Z}_p$-extensions of $K$ and let $\tilde{K}_\infty^*$ denote the largest intermediate field $K_\infty \subseteq \tilde{K}_\infty^* \subseteq \tilde{K}_\infty$ such that $\tilde{K}_\infty^*/K_\infty$ is unramified. Note that $X/TX$ is a finitely generated $\mathbb{Z}_p$-module and, thus, that $L_\infty^*$ is a finite extension of $\tilde{K}_\infty^*$. We will show that $\tilde{K}_\infty^* = \tilde{K}_\infty$.

Completing $K$, $K_\infty$, and $\tilde{K}_\infty$ at compatible primes for each prime of $K$ lying above $p$, we see that $\tilde{K}_\infty/K_\infty$ is unramified: Let $F$, $F_\infty$, and $\tilde{F}_\infty$ denote the completions of $K$, $K_\infty$, and $\tilde{K}_\infty$, respectively. Because $p$ splits completely in $K/Q$, the $F \simeq \mathbb{Q}_p$. By class field theory, the compositum of all $\mathbb{Z}_p$-extensions of $F \simeq \mathbb{Q}_p$ has Galois group isomorphic to $\mathbb{Z}_p^2$ and this compositum contains the unramified $\mathbb{Z}_p$-extension of $F$, which we will denote by $F_\infty^{nr}$. Because $K_\infty/K$ is ramified at all primes above $p$, $F_\infty/F$ is ramified and so the compositum of all $\mathbb{Z}_p$-extensions of $F$ is given by $F_\infty F_\infty^{nr}$. Therefore,

$$F \subseteq F_\infty \subseteq \tilde{F}_\infty \subseteq F_\infty F_\infty^{nr}.$$

Since $F_\infty F_\infty^{nr}/F_\infty$ is unramified, $\tilde{F}_\infty/F_\infty$ is also unramified.

It follows that $\tilde{K}_\infty/K_\infty$ is unramified. Combining Lemma 2.4.2 with Leopoldt's conjecture (Conjecture 2.1.6), we have

$$X/TX \simeq \mathrm{Gal}(L_\infty^*/K_\infty) \sim \mathrm{Gal}(\tilde{K}_\infty/K_\infty) \simeq \mathbb{Z}_p^{r_2}.$$

□

Proposition 2.4.3 tells us the characteristic ideal of $X$ is divisible by $T^{r_2}$. We call these factors of $T$ *trivial zeros*. In the case of the cyclotomic extension, trivial zeros can be interpreted via a $p$-adic $L$-function. This $p$-adic $L$ function satisfies a functional equation which forces a certain order of vanishing at 0. This order is precisely the number of trivial zeros of $X$. More details can be found in [10].

The number of trivial zeros also be determined in the case where $p$ is not totally split in $K/\mathbb{Q}$ using similar local arguments. See Theorem 3.4.1 for another example.

### *2.5 Finiteness Condition*

Rather than just describe the Iwsasawa module $X = \mathrm{Gal}(L_\infty/K_\infty)$ up to pseudo-isomorphism, we could be more ambitious and ask for the exact structure of $X$ as a $\Lambda$-module. In particular, Greenberg studied the Iwasawa modules attached to the cyclotomic extension of totally real number fields in [14] and was often able to provide more information when $X \sim 0$.

**Proposition 2.5.1.** *Let $K$ be a number field with class number prime to $p$. Suppose $K_\infty/K$ is a $\mathbb{Z}_p$-extension in which only one prime is ramified. Then $p$ does not divide the class number of any $K_n$.*

Thus far we have studied the $A_n$ as an inverse system using the norm maps $N_{K_n/K_m} : A_n \to A_m$ for $n \geq m$. There are also maps going the other way $J_{K_n/K_m} : A_m \to A_n$ induced by the inclusion maps

$$\begin{array}{ccc} \mathcal{F}_{K_m} & \hookrightarrow & \mathcal{F}_{K_n} \\ \mathfrak{a} & \mapsto & \mathfrak{a}\mathcal{O}_{K_n} \end{array}$$

The map $J_{K_n/K_m}$ need not be injective. Classes in the kernel of this map are said to *capitulate*.

We may view $A_n$ as a $\Lambda$-module, noting that the action of $\Gamma$ factors through $\Gamma/\Gamma^{p^n}$. Let $\gamma$ denote a topological generator for $\Gamma$. Then, the norm operator for the group $\mathrm{Gal}(K_n/K_m)$

on $A_n$ is given by

$$\sum_{i=0}^{p^{n-m}} \gamma^{ip^m} = \frac{\gamma^{p^n}-1}{\gamma^{p^m}-1} = \frac{(1+T)^{p^n}-1}{(1+T)^{p^m}-1} = \frac{\omega_n}{\omega_m} = \nu_{n,m}$$

where $\omega_n$ and $\nu_{n,m}$ are as in Proposition 2.3.1 and Theorem 2.3.2. Note also that the composition$J_{K_n/K_m} \circ N_{K_n/K_m} : A_n \to A_n$ is the same as the norm operator $\nu_{n,m}$.

**Proposition 2.5.2** (Greenberg)**.** *Let $K$ be a number field with exactly one prime lying above $p$ and let $K_\infty/K$ be a $\mathbb{Z}_p$-extension in which this prime is totally ramified. Suppose that* $\ker(J_{K_n/K}) = A_0$ *for some $n$. Then $X$ is finite. In fact, $X \simeq A_n$.*

*Proof.* Because $K_n/K$ is totally ramified, the norm map $N_{K_n/K} : A_n \to A_0$ is surjective. Therefore,

$$\begin{aligned} J_{K_n/K}(A_0) &= J_{K_n/K}\left(N_{K_n/K}(A_n)\right) \\ &= \nu_{n,0}A_n \end{aligned}$$

Recall from Proposition 2.3.1 that $A_n \simeq X/\omega_n X$. By assumption $J_{K_n/K}(A_0) = 0$ so we see that

$$A_n \simeq \frac{A_n}{\nu_{n,0}A_n} \simeq \frac{X/\omega_n X}{\nu_{n,0}\left(X/\omega_n X\right)} \simeq \frac{X}{\nu_{n,0}X} \tag{2.5.1}$$

Therefore $\omega_n X = \nu_{n,0}X$. But $\omega_n = T\nu_{n,0}X$ so $\nu_{n,0}X/Tof\nu_{n,0}X$. Applying Nakayama's lemma, we find that $\nu_{n,0}X = 0$. Equation (2.5.1) can therefore be rewritten as $X \simeq A_n$. □

**Example 2.5.3.** Let $K$ be a number field with only one prime lying above $p$ and let $K_\infty/K$ be a $\mathbb{Z}_p$-extension. Suppose the $p$-Hilbert Class field of $K$ is contained in $K_\infty$, i.e., $L_0 = K_n$ for some $n$. Then the corresponding Iwasawa module $X = \mathrm{Gal}(L_\infty/K_\infty)$ is trivial.

To see this, let $L_\infty^*$ denote the genus field of $K_\infty/K$. Let $\mathfrak{p}$ denote the prime of $K$ lying above $p$. Though there may be several primes above $p$ in $L_\infty^*$, the Galois group $\mathrm{Gal}(L_\infty^*/K)$ is abelian so there is only one nontrivial inertia subgroup which we'll denote $I_\mathfrak{p}$. Note that $(L_\infty^*)^{I_\mathfrak{p}}$ is an unramified pro-$p$ extension of $K_n = L_0$. We will show that $(L_\infty^*)^{I_\mathfrak{p}} = K_n$ by showing that $K_n$ admits no nontrivial abelian unramified pro-$p$ extension, i.e., that $L_n = K_n$. Because $L_\infty^*/K_\infty$ is unramified, it will then follow that $L_\infty^* = K_\infty$.

Suppose for contradiction that $K_n$ admits a nontrivial pro-$p$ abelian unramified extension. That is, suppose that $A_n$ is not trivial. Then, identifying $A_n$ with $\mathrm{Gal}(L_n/K_n)$ we have the exact sequence

$$1 \to A_n \to \mathrm{Gal}(L_n/K) \to \mathrm{Gal}(K_n/K) \to 1.$$

Let $\bar{\gamma}$ denote a generator for $\mathrm{Gal}(K_n/K)$. Then, by a similar argument to the one used to prove Lemma 2.4.2, one can show that the commutator subgroup of $\mathrm{Gal}(L_n/K)$ is given by

$$(\bar{\gamma} - 1)A_n = \{\bar{\gamma} c \bar{\gamma}^{-1} c^{-1} : c \in A_n\}.$$

However, because $\mathrm{Gal}(K_n/K)$ and $A_n$ are both $p$-groups, $A_n$ admits a nontrivial subgroup which is fixed by the action of $\mathrm{Gal}(K_n/K)$. In particular, $(\bar{\gamma} - 1)A_n$ is a proper subgroup of $A_n$:

$$(\bar{\gamma} - 1)A_n \subsetneq A_n.$$

Consequently, by class field theory, there exists an intermediate field $K_n \subsetneq M \subseteq L_n$ such that $M/K$ is abelian. However, $L_n/K_n$ and $K_n/K$ are both pro-$p$ unramified extensions. It follows that $M/K$ is a pro-$p$ abelian unramified extension. By assumption, $K_n = L_0$, the $p$-Hilbert class field of $K$ so $M \subseteq K_n$, giving the desired contradiction. We may therefore conclude that $K_n = L_n$.

It follows that $L_\infty^* = K_\infty$ and, consequently, that $X/TX = 0$. Hence, by Nakayama's lemma, $X = 0$.

**Example 2.5.4** (The Cyclotomic $\mathbb{Z}_3$-extension of $\mathbb{Q}(\sqrt{254})$)**.** It should be noted that, when capitulation occurs, it need not occur at the first layer. A notorious example is the Iwasawa module attached to the cyclotomic $\mathbb{Z}_3$-extension of $\mathbb{Q}(\sqrt{254})$. In this case, $A_0 \simeq \mathbb{Z}/3\mathbb{Z}$ and capitulation does not occur until the fifth layer of the tower. See the discussion following Corollary 3.4 of [15].

# Chapter 3

# BACKGROUND RESULTS ON $T$-SEMISIMPLICITY

## *3.1 Definition of $T$-semisimplicity*

**Definition 3.1.1.** Let $X$ be a finitely generated torsion $\Lambda$-module. By Theorem 2.2.3, there is a pseudo-isomorphism

$$X \sim \bigoplus_i \frac{\Lambda}{(T^{a_i})} \oplus \bigoplus_j \frac{\Lambda}{(f_j(T)^{b_j})}.$$

We say that $X$ is *$T$-semisimple* if $a_i = 1$ for all $i$. We say that a $\mathbb{Z}_p$-extension is $T$-semisimple if the corresponding Iwasawa module $X = \mathrm{Gal}(L_\infty/K_\infty)$ is $T$-semisimple.

**Proposition 3.1.2.** *Let $X$ be a finitely generated torsion $\Lambda$-module. The following are equivalent:*

*(a) $X$ is $T$-semisimple.*

*(b) The generalized 0-eigenspace of $T$ (or, equivalently, the generalized 1-eigenspace of $\gamma$) acting on $X \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is semisimple, i.e., is actually an eigenspace.*

*(c) The map $X[T] \to X/TX$ obtained by composing the inclusion $X[T] \hookrightarrow X$ with the quotient map $X \to X/TX$ is a pseudo-isomorphism.*

*Proof.* The equivalence between (a) and (b) follows from the fact that tensoring with $\mathbb{Q}_p$ yields an isomorphism

$$X \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \simeq \bigoplus_i \frac{\mathbb{Q}_p[[T]]}{(T^{a_i})} \oplus \bigoplus_j \frac{\mathbb{Q}_p[[T]]}{(f_j(T)^{b_j})}.$$

Thus, we see that the generalized 0-eigenspace of $T$ acting on $X \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ is semisimple precisely when $a_i = 1$ for all $i$.

Note that $X[T]$ and $X/TX$ are always pseudo-isomorphic. Specifically, under the pseudo-isomorphism above, we have

$$\begin{array}{ccc} X[T] & \xrightarrow{\sim} & \displaystyle\bigoplus_i \frac{T^{a_i-1}\Lambda}{(T^{a_i})} \\ & & \downarrow \\ X/TX & \xrightarrow{\sim} & \displaystyle\bigoplus_i \frac{\Lambda}{(T)} \oplus \bigoplus_j \frac{\Lambda}{(f_j(T)^{b_j}, T)} \end{array}$$

where the downward map is given by

$$(T^{a_1-1}x_1 + T^{a_1}\Lambda, \ldots, T^{a_n-1}x_n + T^{a_n}\Lambda) \mapsto (x_1 + T\Lambda, \ldots, x_n + T\Lambda, 0, \ldots, 0).$$

On the other hand, the map $X[T] \to X/TX$ induced by the quotient $X \to X/TX$ is given by

$$(T^{a_1-1}x_1 + T^{a_1}\Lambda, \ldots, T^{a_n-1}x_n + T^{a_n}\Lambda) \mapsto (T^{a_1-1}x_1 + T\Lambda, \ldots, T^{a_n-1}x_n + T\Lambda, 0, \ldots, 0).$$

This is a pseudo-isomorphism precisely when $a_i = 1$ for all $i$. □

Conditions (a) and (b) are the most intuitive ways of thinking about $T$-semisimplicity, but condition (c) turns out to be the most useful for our work.

### *3.2 A Brief History of $T$-Semisimplicity*

In [6], Coates and Lichtenbaum conjectured that if $K/\mathbb{Q}$ is Galois, then $K_\infty^{cyc}/K$ is $T$-semisimple. This was proven in [13] by Greenberg in the case where $K/\mathbb{Q}$ is abelian.

**Theorem 3.2.1** (Greenberg)**.** *Let $K/\mathbb{Q}$ be an abelian number field. Then the cyclotomic $\mathbb{Z}_p$-extension of $K$ is $T$-semisimple.*

The proof uses the $p$-adic analogue of Baker's theorem on linear forms in the logarithms of algebraic numbers, established by Brumer in [2]. Carroll and Kisilevsky then adapted Greenberg's proof in [4] to apply to certain $\chi$-$\mathbb{Z}_p$-extensions.

**Theorem 3.2.2** (Carroll-Kisilevsky)**.** *Let $K/\mathbb{Q}$ be an abelian number field and suppose that the exponent of $\Delta = \mathrm{Gal}(K/\mathbb{Q})$ divides $p-1$. If $\chi$ is a character of $\Delta$ which is odd or trivial and the restriction of $\chi$ to the decomposition subgroup of $p$ in $\Delta$ is trivial, then the $\mathbb{Z}_p$-extension $K_\infty^\chi/K$ is $T$-semisimple.*

Shortly thereafter, it was shown independently by Kisilevsky in [20] and by Jaulent in [17] that there exist $\mathbb{Z}_p$-extensions which are not $T$-semisimple, even if the ground field is abelian over $\mathbb{Q}$. We will discuss Kisilevsky's work on nonsemisimple $\mathbb{Z}_p$-extensions in Section 3.4. But first we will discuss an important feature of the proofs of Theorems 3.2.1 and 3.2.2.

### *3.3 Decomposition Subgroups and $T$-Semisimplicity*

In proving Theorem 3.2.1, Greenberg in fact proved a stronger statement: he proved that the decomposition subgroups for primes above $p$ generate a finite index subgroup of $X/TX$. Carroll and Kisilevsky proved a similar result for the Iwasawa modules corresponding to the extensions $K_\infty^\chi/K$ when $\chi|_{\Delta_p}$ is trivial.

**Proposition 3.3.1.** *Let $K_\infty/K$ be a $\mathbb{Z}_p$-extension and $X = \mathrm{Gal}(L_\infty/K_\infty)$ be the associated Iwasawa module. Suppose the decomposition subgroups for the primes of $K_\infty$ which are ramified in $K_\infty/K$ generate a subgroup of $X/TX$ of $\mathbb{Z}_p$-rank $r$. Then the image of $X[T]$ under $X[T] \to X/TX$ has $\mathbb{Z}_p$-rank at least $r$. In particular, if these decomposition subgroups generate a finite index subgroup of $X/TX$, then $X$ is $T$-semisimple.*

If all such decomposition subgroups of $X$ were contained in $X[T]$, the proof would be almost immediate as the decomposition subgroups of $X$ surject onto those of $X/TX$. However, the decomposition subgroups for the primes ramified in $K_\infty/K$ need not be contained in $X[T]$. We will show instead that they are contained in a larger submodule of $X$, whose image under any quotient map $X \to X/TX$ is essentially the same as that of $X[T]$.

**Lemma 3.3.2.** *Let $n_0 \geq 0$ such that all primes which are ramified in $K_\infty/K$ are totally ramified in $K_\infty/K_{n_0}$. Then for any such prime $\mathfrak{p}$, the decomposition subgroup for $\mathfrak{p}$ in*

$X = \mathrm{Gal}(L_\infty/K_\infty)$ *is contained in* $X[T \cdot \nu_{n_0,0}]$, *where*

$$\nu_{n_0,0} = \frac{\omega_{n_0}}{\omega_0} = \frac{(T+1)^{p^{n_0}} - 1}{T}.$$

(Note that $\nu_{n_0,0}$ is prime to $T$.)

*Proof.* Let $\mathfrak{p}$ be a prime of $K_\infty$ which is ramified in $K_\infty/K$ and let $\mathfrak{P}$ be a prime of $L_\infty$ lying above $\mathfrak{p}$. Let $\mathcal{G}_{n_0} = \mathrm{Gal}(L_\infty/K_{n_0})$ and let $\mathcal{G}_{n_0,\mathfrak{P}}$ and $I_\mathfrak{P}$ denote the decomposition subgroup for $\mathfrak{P}$ and inertia subgroup for $\mathfrak{P}$, respectively. Let $X_\mathfrak{P} = X \cap \mathcal{G}_{n_0,\mathfrak{P}}$ denote the decomposition subgroup for $\mathfrak{P}$ in $X$. Note that $X_\mathfrak{P}$ is a normal subgroup of $\mathcal{G}_{n_0}$, and thus of $\mathcal{G}_{n_0,\mathfrak{P}}$. Because $\mathfrak{P}$ is totally ramified in $K_\infty/K_{n_0}$, we have the following exact sequence, which splits:

$$\begin{array}{ccccccccc} & & & & I_\mathfrak{P} & \dashleftarrow & & & \\ & & & & \downarrow & \ddots & & & \\ 1 & \longrightarrow & X_\mathfrak{P} & \longrightarrow & G_{n_0,\mathfrak{P}} & \longrightarrow & \Gamma^{p^{n_0}} & \longrightarrow & 1 \end{array}$$

Thus, we see that $X_\mathfrak{P}$ and $I_\mathfrak{P}$ are two normal subgroups of $\mathcal{G}_{n_0,\mathfrak{P}}$ which intersect trivially but together generate all of $\mathcal{G}_{n_0,\mathfrak{P}}$: i.e., $\mathcal{G}_{n_0,\mathfrak{P}} = X_\mathfrak{P} \times I_\mathfrak{P}$. In particular, $I_\mathfrak{P}$ acts trivially on $X_\mathfrak{P}$. Since $\Gamma^{p^{n_0}}$ acts on $X$ through $I_\mathfrak{P}$, we see that $\Gamma^{p^{n_0}}$ acts trivially on $X_\mathfrak{P}$. Because $X$ is abelian, $X_\mathfrak{P} = X_\mathfrak{p}$. Thus,

$$X_\mathfrak{p} \subseteq X[(1+T)^{p^{n_0}} - 1] = X[T \cdot \nu_{p^{n_0},0}].$$

□

**Lemma 3.3.3.** *The image of* $X[T]$ *under the composition* $X[T \cdot \nu_{n_0,0}] \to X \to X/TX$ *has finite index in the image of* $X[T \cdot \nu_{n_0,0}]$.

*Proof.* Note that the ideal $(T, \nu_{n_0,0})$ in $\Lambda$ can be written as $(T, p^{n_0})$. In particular, there exist $f, g \in \Lambda$ such that $fT + g\nu_{n_0,0} = p^{n_0}$. Suppose that $x \in X[T \cdot \nu_{n_0,0}]$. Then

$$p^{n_0}x = fTx + g\nu_{n_0,0}x.$$

Note that $g\nu_{n_0,0}x$ is in $X[T]$ and that $p^{n_0}x$ and $g\nu_{n_0,0}x$ have the same image under the quotient map $X \to X/TX$. It follows that

$$p^{n_0}\,\mathrm{im}(X[T\cdot\nu_{n_0,0}]) \subseteq \mathrm{im}(X[T]) \subseteq \mathrm{im}(X[T\cdot\nu_{n_0,0}]).$$

Observing that $\mathrm{im}(X[T\cdot\nu_{n_0,0}])$ is finitely generated as a $\mathbb{Z}_p$-module completes the proof. □

*Proof of Proposition 3.3.1.* Combining Lemmas 3.3.2 and 3.3.3, we can now prove Proposition 3.3.1: Suppose that the decomposition subgroups for primes which are ramified in $K_\infty/K$ generate a rank $r$ subgroup of $X/TX$. Because the decomposition subgroups of $X$ surject onto those of $X/TX$, Lemma 3.3.2 tells us that, for sufficiently large $n_0$ the image of $X[T\cdot\nu_{p^{n_0},0}]$ under the map $X \to X/TX$ has $\mathbb{Z}_p$-rank at least $r$. Therefore, by Lemma 3.3.3, the image of $X[T]$ in $X/TX$ has $\mathbb{Z}_p$-rank at least $r$.

Suppose now that $r = \mathrm{rank}_{\mathbb{Z}_p}(X/TX)$. Because $X[T]$ and $X/TX$ are pseudo-isomorphic, we see that the map $X[T] \to X/TX$ is a pseudo-isomorphism and, consequently, that $X$ is $T$-semisimple. □

**Corollary 3.3.4.** *Let $K/\mathbb{Q}$ be an imaginary quadratic field. Then every $\mathbb{Z}_p$-extension of $K$ is $T$-semisimple*

*Proof.* As usual, let $\tilde{K}_\infty$ denote the compositum of all $\mathbb{Z}_p$-extensions of $K$, so that $\tilde{K}_\infty = K_\infty^{cyc}K_\infty^{anti}$. Note that $\Delta = \mathrm{Gal}(K/\mathbb{Q})$ acts differently on the Galois group of each.

Suppose first that $p$ is inert or ramified in $K/\mathbb{Q}$ and let $\mathfrak{p}$ denote the prime of $K$ lying above $p$. Then $\Delta = \Delta_p$ and we see that $K_\infty^{cyc}$ and $K_\infty^{anti}$ give rise to two different $\mathbb{Z}_p$-extensions of $K_\mathfrak{p}$, the completion of $K$ at $\mathfrak{p}$, both of which are ramified. Furthermore, the compositum of these two local $\mathbb{Z}_p$-extensions does not contain the unramified $\mathbb{Z}_p$-extension of $K_\mathfrak{p}$ (see the proof of Proposition 3.4.3 below). It follows that the inertia subgroup for $\mathfrak{p}$ generates a finite index subgroup of $\tilde{K}_\infty/K$ and, hence, that for each $\mathbb{Z}_p$-extension $K_\infty/K$, the corresponding Iwasawa module has no trivial zeros: $X/TX \sim 0$.

Suppose next that $p$ splits in $K/\mathbb{Q}$. The proof of Theorem 3.2.1 shows that the decomposition subgroups for primes above $p$ generate a finite index subgroup of $\mathrm{Gal}(\tilde{K}_\infty/K_\infty^{cyc})$.

Note that $\tilde{K}_\infty/\mathbb{Q}$ is Galois and $K_\infty^{cyc}/K$ is (totally) ramified at both primes above $p$. Thus, we see that for each of the two primes $\mathfrak{p}$ lying above $p$ in $K$, the decomposition subgroup for $\mathfrak{p}$ in $\tilde{K}_\infty/K$ has $\mathbb{Z}_p$-rank 2. Let $K_\infty/K$ be a $\mathbb{Z}_p$-extension of $K$. Then the decomposition subgroup for $\mathfrak{p}$ in $\mathrm{Gal}(\tilde{K}_\infty/K_\infty)$ has $\mathbb{Z}_p$-rank 1. If only one prime lying above $p$ in $K$ ramifies in $K_\infty/K$, then $\tilde{K}_\infty/K_\infty$ is ramified at the other prime and we see that $X/TX \sim 0$. Otherwise, if both primes ramify in $K_\infty/K$, then $X/TX \sim \mathrm{Gal}(\tilde{K}_\infty/K_\infty)$. We just saw that that the decomposition subgroups for the primes above $p$ generate a finite index subgroup of $\mathrm{Gal}(\tilde{K}_\infty/K_\infty)$ so by Proposition 3.3.1, $K_\infty/K$ is $T$-semisimple. □

In Chapter 4 we study the decomposition subgroups for primes above $p$ in $\mathrm{Gal}(\tilde{K}_\infty/K)$ for a larger class of abelian number fields and show that generic $\mathbb{Z}_p$-extensions of such fields are $T$-semisimple.

### *3.4 Nonsemisimple Iwasawa Modules*

In [20], Kisilevsky proved the following theorem.

**Theorem 3.4.1** (Kisilevsky)**.** *Let $p$ be an odd prime and let $K/\mathbb{Q}$ be a complex abelian number field with Galois group $\Delta = \mathrm{Gal}(K/\mathbb{Q})$ of exponent dividing $p-1$. Suppose there exists a character $\chi \in \hat{\Delta}$ with the following properties:*

*(a) $\chi$ is odd,*

*(b) $\chi$ does not have order 2, but*

*(c) the restriction of $\chi$ to the decomposition subgroup $\Delta_p$ of $\Delta$ has order exactly 2.*

*Then the $\chi$-$\mathbb{Z}_p$-extension of $K$ is not $T$-semisimple.*

The idea behind the proof is to study the composition factors of $X[T]$ and $X/TX$ (described in Theorems 3.4.6 and 3.4.2, respectively). The hypotheses of Theorem 3.4.1 guarantee that

$$(X/TX)^{(\chi^{-1})} \sim \mathbb{Z}_p \quad \text{but} \quad (X[T])^{(\chi^{-1})} \sim 0.$$

The map $X[T] \to X/TX$ is $\Delta$-equivariant, so we see that the cokernel has positive $\mathbb{Z}_p$-rank in this case and thus, that $X$ is not $T$-semisimple.

*Determining the Infinite Components of $X/TX$*

**Theorem 3.4.2** (Kisilevsky)**.** *Let $K/\mathbb{Q}$ be a complex abelian number field with Galois group $\Delta = \mathrm{Gal}(K/\mathbb{Q})$ of exponent dividing $p-1$. Let $\chi$ be a character of $\Delta$ and let $X$ denote the Iwasawa module associated to the $\mathbb{Z}_p$-extension $K_\infty^\chi/K$. Then, for each character $\psi \in \hat{\Delta}$*

$$(X/TX)^{(\psi)} \sim \begin{cases} \mathbb{Z}_p & \psi|_{\Delta_p} = \chi|_{\Delta_p}, \psi \neq \chi, \psi \text{ odd or trivial,} \\ 0 & \text{otherwise.} \end{cases}$$

Let $L_\infty^*$ denote the genus field of $K_\infty^\chi/K$ and let $K_\infty^*$ denote the maximal intermediate field $K_\infty \subseteq K_\infty^* \subseteq L_\infty^*$ such that $\mathrm{Gal}(K_\infty^*/K_\infty)$ is a free $\mathbb{Z}_p$-module. Note that

$$X/TX \simeq \mathrm{Gal}(L_\infty^*/K_\infty^\chi) \sim \mathrm{Gal}(K_\infty^*/K_\infty^\chi).$$

Furthermore, by maximality, we see that $K_\infty^*$ is Galois over $\mathbb{Q}$. It follows that $K_\infty^*$ is a compositum of $\mathbb{Z}_p$-extensions $K_\infty^\psi$. Theorem 3.4.2 then follows from Theorem 2.1.8 along with the following proposition.

**Proposition 3.4.3.** *Let $\chi$ and $\psi$ be two characters of $\Delta$ which are odd or trivial. Then $K_\infty^\chi K_\infty^\psi/K_\infty^\chi$ is unramified if and only if $\chi|_{\Delta_p} = \psi|_{\Delta_p}$.*

*Proof.* Let $\chi$ and $\psi$ be two characters of $\Delta$ which are odd or trivial. As in the proof of Proposition 2.4.3, we will work locally. Let $F$, $F_\infty^\chi$, and $F_\infty^\psi$ denote the completions of $K$, $K_\infty^\chi$, and $K_\infty^\psi$ with respect to compatible primes lying above $p$. Let $\tilde{F}$ denote the compositum of all $\mathbb{Z}_p$-extensions of $F$. The decomposition subgroup $\Delta_p$ acts on $\mathrm{Gal}(\tilde{F}_\infty/F)$. Local class field theory along with a careful study of the unit group $\mathcal{O}_F^\times$ (see for example Proposition 5.7 of Chapter II of [24]) shows that, for each character $\varphi$ of $\Delta_p$

$$\mathrm{Gal}(\tilde{F}_\infty/F)^{(\varphi)} \simeq \begin{cases} \mathbb{Z}_p^2 & \text{if } \varphi \text{ is trivial,} \\ \mathbb{Z}_p & \text{otherwise.} \end{cases} \tag{3.4.1}$$

Let $\bar{\chi}$ and $\bar{\psi}$ denote the restrictions of $\chi$ and $\psi$ to $\Delta_p$. Note that $\Delta_p$ acts on $\mathrm{Gal}(F_\infty^\chi/F)$ by $\bar{\chi}$ and on $\mathrm{Gal}(F_\infty^\psi/F)$ by $\bar{\psi}$. The local field $F$ admits a unique unramified $\mathbb{Z}_p$-extension, which we will denote by $F_\infty^{nr}$, on which $\Delta_p$ acts trivially. Because $K_\infty^\chi$ is Galois over $\mathbb{Q}$, by Proposition 2.1.3, every prime above $p$ must ramify in $K_\infty^\chi/K$ and so $F_\infty^\chi/F$ is a ramified extension. Similarly, $F_\infty^\psi/F$ is also ramified.

If $F_\infty^\chi = F_\infty^\psi$, then, trivially, $F_\infty^\chi F_\infty^\psi/F_\infty^\chi$ is an unramified extension and also $\bar{\chi} = \bar{\psi}$. Let us therefore suppose that $F_\infty^\chi \neq F_\infty^\psi$.

If $\bar{\chi} = \bar{\psi}$, then we see from Equation (3.4.1) that $\bar{\chi}$ and $\bar{\psi}$ are both trivial. Furthemore, because $\Delta_p$ acts trivially on $F_\infty^{nr}$, we must have $F_\infty^{nr} \subseteq F_\infty^\chi F_\infty^\psi$. Because $F_\infty^\chi/F$ and $F_\infty^\psi/F$ are both ramified, it follows that $F_\infty^\chi F_\infty^\psi/F_\infty^\chi$ is unramified.

Conversely, suppose that $F_\infty^\chi F_\infty^\psi/F_\infty^\chi$ is unramified. Then, $F_\infty^{nr} \subseteq F_\infty^\chi F_\infty^\psi$ and, because the extensions $F_\infty^\chi/F$ and $F_\infty^\psi/F$ are both ramified, we see that

$$F_\infty^\chi F_\infty^\psi = F_\infty^\chi F_\infty^{nr} = F_\infty^\psi F_\infty^{nr}.$$

Comparing the action of $\Delta_p$ on the Galois groups of these three fields over $F$, we see that $\bar{\chi} = \bar{\psi}$, the trivial character.

Thus we see that $F_\infty^\chi F_\infty^\psi/F_\infty^\chi$ is unramified if and only if $\chi|_{\Delta_p} = \psi|_{\Delta_p}$. Consequently $K_\infty^\chi K_\infty^\psi/K_\infty^\chi$ is unramified if and only if $\chi|_{\Delta_p} = \psi|_{\Delta_p}$, as desired. □

In the proof above, note that if $\chi|_{\Delta_p}$ is not trivial and $F_\infty^\chi F_\infty^\psi/F_\infty^\chi$ is unramified, then it must be the case that $F_\infty^\chi = F_\infty^\psi$. Combining this observation with Proposition 3.4.3 and the discussion immediatly preceding it yields the following corollary.

**Corollary 3.4.4.** *Let $K/\mathbb{Q}$ be an abelian extension and suppose $\Delta = \mathrm{Gal}(K/\mathbb{Q})$ has exponent dividing $p-1$. Let $\chi$ be an odd character of $\Delta$ whose restriction to the decomposition subgroup $\Delta_p$ is not trivial. Let $X$ denote the Iwasawa module corresponding to $K_\infty^\chi/K$. Then the subgroup of $X/TX$ generated by the decomposition subgroups for primes above $p$ is finite.*

*Determining the Infinite Components of $X[T]$*

**Proposition 3.4.5.** *Let $K/F$ be a cyclic extension of number fields and $G = \mathrm{Gal}(K/F)$. Then, the sequence*

$$1 \to \ker(J_{K/F}) \to \frac{\mathcal{P}_K^G}{\mathcal{P}_F} \to \frac{\mathcal{F}_K^G}{\mathcal{F}_F} \to \frac{\mathrm{Cl}(K)^G}{J_{K/F}(\mathrm{Cl}(F))} \to \frac{\mathcal{O}_F^\times \cap N_{K/F}(K^\times)}{N_{K/F}(\mathcal{O}_K^\times)} \to 1$$

*is exact. Furthermore,*

*(a) Let $\mathfrak{p}_1, \dots \mathfrak{p}_t$ denote the ramified primes in $K/F$ and, for each $i$, let $e_i$ denote the ramification index of $\mathfrak{p}_i$. Then*

$$\frac{\mathcal{F}_K^G}{\mathcal{F}_F} \cong \prod_{i=1}^{t} \mathbb{Z}/e_i\mathbb{Z}.$$

*(b) $\dfrac{\mathcal{P}_K^G}{\mathcal{P}_F} \simeq H^1(G, \mathcal{O}_K^\times)$.*

*(c) Let $n = [K : F]$. If $n$ is odd or all the real primes of $F$ are ramified in $F/K$, then*

$$\left| \frac{\mathcal{O}_F^\times \cap N_{K/F}(K^\times)}{N_{K/F}(\mathcal{O}_K^\times)} \right| \leq \left| \frac{\mathcal{O}_F^\times}{N_{K/F}(\mathcal{O}_K^\times)} \right| = n \left| \frac{\mathcal{P}_K^G}{\mathcal{P}_F} \right|.$$

*Proof.* Let $K/F$ be a cyclic extension of number fields of odd degree $n$ and let $G = \mathrm{Gal}(K/F)$. Let $\mathcal{F}_K$ denote the group of nonzero fractional ideals of $K$ and let $\mathcal{P}_K$ denote the subgroup generated by principal fractional ideals. Consider the short exact sequence defining the class group:

$$1 \to \mathcal{P}_K \to \mathcal{F}_K \to \mathrm{Cl}(K) \to 1$$

This gives rise to a long exact sequence in cohomology

$$1 \to \mathcal{P}_K^G \to \mathcal{F}_K^G \to \mathrm{Cl}(K)^G \to H^1(G, \mathcal{P}_K) \to H^1(G, \mathcal{F}_K)$$

Let $\sigma$ be a generator of $G$. Then, sending a cocycle $f \in H^1(G, \mathcal{F}_K)$ to $f(\sigma)$ yields a (non-canonical) isomorphism

$$H^1(G, \mathcal{F}_K) \simeq \frac{\ker(N : \mathcal{F}_K \to \mathcal{F}_K)}{(\mathcal{F}_K)^{(\sigma-1)}}$$

where $N$ denotes the group-theoretic norm map $N : f \mapsto \prod_{\tau \in G} \tau(f)$. Using this description, one can show that $H^1(G, \mathcal{F}_K)$ is trivial: Let $\mathfrak{a} \in \mathcal{F}_K$ such that $N(\mathfrak{a}) = \mathcal{O}_K$. We wish to show that $\mathfrak{a} = \sigma(\mathfrak{b})/\mathfrak{b}$ for some $\mathfrak{b} \in \mathcal{F}_K$. Note that, because $G$ permutes the primes of $K$ lying above a fixed prime of $F$, it is enough to check the case when

$$\mathfrak{a} = \prod_{i=0}^{n-1} \sigma^i(\mathfrak{P})^{a_i}$$

for some prime $\mathfrak{P}$ of $K$. Note that

$$N(\mathfrak{a}) = N\left(\prod_{i=0}^{n-1} \sigma^i(\mathfrak{P})^{a_i}\right) = \prod_{i=0}^{n-1} N(\sigma^i(\mathfrak{P}))^{a_i} = \prod_{i=0}^{n-1} N(\mathfrak{P})^{a_i} = N(\mathfrak{P})^{\sum_{i=0}^{n-1} a_i}.$$

Thus, because $N(\mathfrak{a}) = \mathcal{O}_K$, we must have

$$\sum_{i=0}^{n-1} a_i = 0.$$

Note that

$$\begin{aligned}
\mathfrak{a} &= \mathfrak{P}^{a_0}\sigma(\mathfrak{P})^{a_1}\sigma^2(\mathfrak{P})^{a_2}\cdots\sigma^{n-1}(\mathfrak{P})^{a_{n-1}} \\
&= \mathfrak{P}^{a_0}\sigma(\mathfrak{P})^{-a_0}\sigma(\mathfrak{P})^{a_0+a_1}\sigma^2(\mathfrak{P})^{a_2}\cdots\sigma^{n-1}(\mathfrak{P})^{a_{n-1}} \\
&\vdots \\
&= \mathfrak{P}^{a_0}\sigma(\mathfrak{P})^{-a_0}\sigma(\mathfrak{P})^{(a_0+a_1)}\sigma^2(\mathfrak{P})^{-(a_0+a_1)}\sigma^2(\mathfrak{P})^{a_0+a_1+a_2}\cdots\sigma^{n-1}(\mathfrak{P})^{a_0+\cdots+a_{n-1}} \\
&= \left(\mathfrak{P}^{a_0}\sigma(\mathfrak{P})^{(a_0+a_1)}\sigma^2(\mathfrak{P})^{(a_0+a_1+a_2)}\cdots\sigma^{n-2}(\mathfrak{P})^{(a_0+\cdots+a_{n-2})}\right)^{1-\sigma}.
\end{aligned}$$

giving the desired result. Thus, our long exact sequence becomes

$$1 \to \mathcal{P}_K^G \to \mathcal{F}_K^G \to \mathrm{Cl}(K)^G \to H^1(G, \mathcal{P}_K) \to 0,$$

yielding the isomorphism

$$0 \to \frac{\mathrm{Cl}(K)^G}{\mathcal{F}_K^G} \xrightarrow{\simeq} H^1(G, \mathcal{P}_K) \to 0. \tag{3.4.2}$$

(where, by abuse of notaion, we also use $\mathcal{F}_K^G$ to denote the subgroup it generates in $\mathrm{Cl}(K)^G$, namely $\{\mathrm{cl}(\mathfrak{a}) : \mathfrak{a} \in \mathcal{F}_K^G\}$). One can also consider the short exact sequence defining the class

group of $F$ along with inclusions of the various terms into the terms of the exact sequence above:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathcal{P}_F & \longrightarrow & \mathcal{F}_F & \longrightarrow & \mathrm{Cl}(F) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow{\scriptstyle J_{K/F}} & & \\ 1 & \longrightarrow & \mathcal{P}_K^G & \longrightarrow & \mathcal{F}_K^G & \longrightarrow & \mathrm{Cl}(K)^G & & \end{array}$$

Applying the snake lemma we obtain another long exact sequence:

$$1 \to \ker(J_{K/F}) \to \frac{\mathcal{P}_K^G}{\mathcal{P}_F} \to \frac{\mathcal{F}_K^G}{\mathcal{F}_F} \to \frac{\mathrm{Cl}(K)^G}{J_{K/F}(\mathrm{Cl}(F))} \to \frac{\mathrm{Cl}(K)^G}{\mathcal{F}_K^G} \to 1 \tag{3.4.3}$$

(The last nontrivial term is simply the cokernel of the map between the previous two terms.) One can combine the two sequences 3.4.2 and 3.4.3 along $\mathrm{Cl}(K)^G/\mathcal{F}_K^G$ to obtain:

$$1 \to \ker(J_{K/F}) \to \frac{\mathcal{P}_K^G}{\mathcal{P}_F} \to \frac{\mathcal{F}_K^G}{\mathcal{F}_F} \to \frac{\mathrm{Cl}(K)^G}{J_{K/F}(\mathrm{Cl}(F))} \to H^1(G, \mathcal{P}_K) \to 0$$

Similarly to the case of $H^1(G, \mathcal{F}_K)$ studied above, we have an isomorphism

$$H^1(G, \mathcal{P}_K) \simeq \frac{\ker(N : \mathcal{P}_K \to \mathcal{P}_K)}{\mathcal{P}_K^{\sigma-1}}.$$

Define a map $\ker(N : \mathcal{P}_K \to \mathcal{P}_K) \to (\mathcal{O}_F^\times \cap N_{K/F}(K^\times))/N_{K/F}(\mathcal{O}_K^\times)$ by sending a principal ideal $(\alpha)$ to the coset with representative $N_{K/F}(\alpha)$. Note that this map is well-defined: if $\alpha$ and $\beta$ generate the same ideal, their norms differ by the norm of a unit, namely the norm of their quotient. This map is surjective. Let us now examine the kernel: Let $\alpha \in K^\times$ such that $N_{K/F}(\alpha) = N_{K/F}(\eta)$ for some unit $\eta \in \mathcal{O}_K^\times$. Then $N_{K/F}(\alpha/\eta) = 1$ and so, by Hilbert's theorem 90, there exists $\beta \in K^\times$ such $\alpha/\eta = \beta^{\sigma-1}$. As ideals we have

$$(\alpha) = (\alpha/\eta) = (\beta^{\sigma-1}) = (\beta)^{\sigma-1}.$$

The kernel of our map is therefore precisely $\mathcal{P}_K^{\sigma-1}$, yielding an isomorphism

$$\frac{\ker(N : \mathcal{P}_K \to \mathcal{P}_K)}{\mathcal{P}_K^{\sigma-1}} \simeq \frac{\mathcal{O}_F^\times \cap N_{K/F}(K^\times)}{N_{K/F}(\mathcal{O}_K^\times)}.$$

Combining this with the results above we obtain the desired long exact sequence.

Let us now prove (a). Let $\mathfrak{a} \in \mathcal{F}_K^G$ and let $\mathfrak{P}$ be a prime of $K$. Then, if $\mathfrak{a}$ is divisible by $\mathfrak{P}$, the fractional ideal $\mathfrak{a}$ must also be divisible by all of the Galois conjugates of $\mathfrak{P}$ as well. Thus, we see that $\mathcal{F}_K^G$ is generated by ideals of the form

$$Q_{\mathfrak{p}} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}, \qquad \mathfrak{p} \subseteq \mathcal{O}_F^{\times}, \text{ prime.}$$

On the other hand,

$$\mathfrak{p}\mathcal{O}_K = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_{\mathfrak{p}}} = Q_{\mathfrak{p}}^{e_{\mathfrak{p}}},$$

where $e_{\mathfrak{p}}$ is the ramification index of $\mathfrak{p}$ in $K/F$. Hence,

$$\frac{\mathcal{F}_K^G}{\mathcal{F}_F} \cong \prod_{i=1}^{t} \mathbb{Z}/e_i\mathbb{Z},$$

giving part (a).

For part (b), consider the exact sequence defining $\mathcal{P}_K$:

$$1 \to \mathcal{O}_K^{\times} \to K^{\times} \to \mathcal{P}_K \to 1.$$

This gives rise to a long exact sequence in cohomology:

$$1 \to \mathcal{O}_F^{\times} \to F^{\times} \to \mathcal{P}_K^G \to H^1(G, \mathcal{O}_K^{\times}) \to H^1(G, K^{\times}) \tag{3.4.4}$$

Noting that the image of $F^{\times}$ in $\mathcal{P}_K^G$ is precisely $\mathcal{P}_F$ and using Hilbert's theorem 90, we obtain the desired isomorphism:

$$\frac{\mathcal{P}_K^G}{\mathcal{P}_F} \xrightarrow{\simeq} H^1(G, \mathcal{O}_K^{\times}).$$

For part (c), the inequality

$$\left| \frac{\mathcal{O}_F^{\times} \cap N_{K/F}(K^{\times})}{N_{K/F}(\mathcal{O}_K^{\times})} \right| \leq \left| \frac{\mathcal{O}_F^{\times}}{N_{K/F}(\mathcal{O}_K^{\times})} \right|$$

is immediate as the group on the left is a subgroup of the one on the right. Note that

$$\frac{\mathcal{O}_F^{\times}}{N_{K/F}(\mathcal{O}_K^{\times})} \simeq H^2(G, \mathcal{O}_K^{\times}).$$

Using part (b), we see that we may complete the proof by computing the Herbrand quotient

$$h(G, \mathcal{O}_K^\times) = \frac{|H^2(G, \mathcal{O}_K^\times)|}{|H^1(G, \mathcal{O}_K^\times)|}.$$

Corollary 2 in Section IX.4 of [21] tells us that $h(G, \mathcal{O}_K^\times) = 1/n$, which completes the proof. □

**Theorem 3.4.6** (Carroll-Kisilevsky)**.** *Let $K/\mathbb{Q}$ be a complex abelian number field with Galois group $\Delta = \mathrm{Gal}(K/\mathbb{Q})$ of exponent dividing $p-1$. Let $\chi$ be a character of $\Delta$ and let $X$ denote the Iwasawa module associated to the $\mathbb{Z}_p$-extension $K_\infty^\chi/K$. Then*

$$\left\{\psi \in \hat{\Delta} : (X[T])^{(\psi)} \sim \mathbb{Z}_p\right\} \subseteq \underbrace{\left\{\psi : \psi|_{\Delta_p} = \chi_0|_{\Delta_p}\right\}}_{\textit{type-D}} \cup \underbrace{\left\{\psi : \chi\psi \text{ is even}, \chi\psi \neq \chi_0, \chi\psi|_{\Delta_p} \neq \chi|_{\Delta_p}\right\}}_{\textit{type-S}}.$$

The characters labeled type-D are related to the decomposition subgroups for primes above $p$ in $X[T]$ in the following sense: Let $D \subseteq X[T]$ denote the subgroup generated by the decomposition subgroups for primes above $p$. Then

$$\left\{\psi \in \hat{\Delta} : D^{(\psi)} \sim \mathbb{Z}_p\right\} \subseteq \left\{\psi : \psi|_{\Delta_p} = \chi_0|_{\Delta_p}\right\} \tag{3.4.5}$$

The idea behind the proof of Theorem 3.4.6 is to apply Proposition 3.4.5 to the extension $K_n/K$ and study how $\Delta$ acts on $\mathrm{Cl}(K_n)^\Gamma/J_{K_n/K}(\mathrm{Cl}(K))$, which is closely related to $A_n$. We do this by studying the action of $\Delta$ on the two neighboring groups in the sequence:

$$\frac{\mathcal{F}_{K_n}^\Gamma}{\mathcal{F}_K} \qquad \text{and} \qquad \frac{\mathcal{O}_K^\times \cap N_{K_n/K}(K_n^\times)}{N_{K_n/K}(\mathcal{O}_{K_n}^\times)}.$$

(Note that the action of $\Gamma$ factors through $\Gamma/\Gamma^{p^n}$, so these groups really are the same as those appearing in Proposition 3.4.5.) Recall from the proof of Proposition 3.4.5 that $\mathcal{F}_{K_n}^\Gamma/\mathcal{F}_K$ is generated by the images of the $Q_\mathfrak{p} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}$, for $\mathfrak{p}$ ramified in $K_n/K$. Because $K_n/\mathbb{Q}$ is Galois, every prime above $p$ is ramified for sufficiently large $n$ and the ramification indices are the same. Thus, we see that $\Delta$ permutes the $Q_\mathfrak{p}$ with the decomposition subgroup $\Delta_p$ acting trivially. It follows that

$$\frac{\mathcal{F}_{K_n}^\Gamma}{\mathcal{F}_K} \simeq \frac{\mathbb{Z}}{p^{(n-n_0)}\mathbb{Z}}\,[\Delta/\Delta_p]$$

for some fixed $n_0$, independent of $n$. The map $\mathcal{F}_{K_n}^{\Gamma}/\mathcal{F}_K \to \mathrm{Cl}(K_n)^{\Gamma}/J_{K_n/K}(\mathrm{Cl}(K))$ is $\Delta$-equivariant and, taking inverse limits with respect to the norm maps $N_{K_n/K}$, we find the $\psi$-component $(X[T])^{(\psi)}$ for every type-D character could potentially have $\mathbb{Z}_p$-rank 1. Furthermore, note that for each prime $\mathfrak{p}$ of $K$ lying above $p$, the image of $Q_{\mathfrak{p}}$ is the class of $\prod_{i=0}^{p^{n_0}-1}\gamma^i(\mathfrak{P}_n)$, where $\mathfrak{P}_n$ is a prime of $K_n$ lying above $\mathfrak{p}$. By class field theory, for sufficiently large $n$, this class generates a finite index (independent of $n$) subgroup of the decomposition subgroup for $\mathfrak{p}$ in $\mathrm{Gal}(L_n/K_n)$. Taking inverse limits, we obtain Equation (3.4.5).

The type-S characters in Theorem 3.4.6 come from studying the action of $\Delta$ on $(\mathcal{O}_K^{\times} \cap N_{K_n/K}(K_n^{\times}))/N_{K_n/K}(\mathcal{O}_{K_n}^{\times})$. This is done in detail in [4].

*Some Examples*

It is not difficult to construct examples satisfying the conditions of Theorem 3.4.1.

**Example 3.4.7.** Let $K = \mathbb{Q}(\mu_5)$ and let $p \equiv 9 \pmod{20}$. Because $p \equiv 1 \pmod 4$, the characters of $\Delta = \mathrm{Gal}(\mathbb{Q}(\mu_5)/\mathbb{Q})$ take values in $\mathbb{Z}_p$. Because, $p \equiv 4 \pmod 5$, we know that $p$ spits in $\mathbb{Q}(\sqrt{5})$, but does not split completely in $K$ so the decomposition subgroup of $\Delta$ is $\mathrm{Gal}(K/\mathbb{Q}(\sqrt{5})$. Let $\chi \in \hat{\Delta}$ be a character of order 4. Then $p$, $K$, and $\chi$ satisfy the hypotheses of Theorem 3.4.1.

In fact, for all primes $p > 3$, one can construct fields $K$ which admit nonsemisimple $\mathbb{Z}_p$-extensions. For example, if $p \notin \{5, 7, 13, 17\}$, then there exists a totally real cyclic extension $F/\mathbb{Q}$ of degree $n > 2$ with $F \subseteq \mathbb{Q}(\mu_{p-1})$ (one needs to check this for primes up to $3 * 16 + 1 = 49$). Note that $p$ splits completely $\mathbb{Q}(\mu_{p-1})$ and thus in $F$. Now, let $F'$ be a quadratic imaginary field in which $p$ is inert and let $K$ denote the compositum $K = FF'$. Let $\psi$ denote a character of $\mathrm{Gal}(F/\mathbb{Q})$ of order $n$ and let $\phi$ denote the nontrivial character of $\mathrm{Gal}(F'/\mathbb{Q})$. Then, extending these to characters of $\mathrm{Gal}(K/\mathbb{Q})$, let $\chi$ denote the character $\chi = \psi\phi$. One then finds that $p$, $K$, and $\chi$ satisfy the hypotheses of Theorem 3.4.1. For the primes $5, 7, 13, 17$ we can use the same construction if we can find a totally real cyclic extension $F/\mathbb{Q}$ in which $p$ splits. For $p = 5$ and $p = 17$, one can take $F$ to be the degree 4

field sitting inside $\mathbb{Q}(\mu_{401})$ and $\mathbb{Q}(\mu_{257})$, respectively. For $p = 7$ and $p = 13$, one can take $F$ to be the degree 3 field sitting inside $\mathbb{Q}(\mu_{19})$ and $\mathbb{Q}(\mu_7)$, respectively.

Note that if $\chi$ is a character satisfying the conditions of Theorem 3.4.1, then $\chi^{-1}$ $(\neq \chi)$ also satisfies these conditions. Thus, we see that in Kisilevsky's examples, $\mathbb{Z}_p$-extensions which are not $T$-semisimple come in pairs. In fact, if a number field $K$ admits one $\mathbb{Z}_p$-extension which is not $T$-semisimple, then $K$ admits many other $\mathbb{Z}_p$-extensions which are not $T$-semisimple. We will discuss this in more detail in Section 4.2.

### *3.5 Further Nonsemisimplicity*

We can take Kisilevsky's idea further and try to study higher degrees of nonsemisimplicity. Using the notation from Definition 3.1.1, we see from Theorem 3.4.1 that showed that $a_i$ can be at least 2 for some $i$. Can any of the $a_i$ be larger than 2? How large can the $a_i$ be? Expanding on Kisilevsky's idea of comparing the composition factors of $X[T]$ and $X/TX$, let us study the composition factors of $TX/T^2X$.

**Lemma 3.5.1.** *Let $K$ be an abelian number field with Galois group $\Delta = \mathrm{Gal}(K/\mathbb{Q})$ of exponent dividing $p-1$. Let $\chi$ be an odd or trivial character of $\Delta$ and let $X$ denote the Iwasawa module corresponding to the $\mathbb{Z}_p$-extension $K_\infty^\chi/K$. Then the map*

$$\begin{aligned} X/TX &\longrightarrow TX/T^2X \\ x+TX &\mapsto Tx+T^2X \end{aligned}$$

*is not $\Delta$-equivariant. Instead, for each $\phi \in \hat{\Delta}$ this map sends the $\phi$-component of $X/TX$ into the $\chi\phi$-component of $TX/T^2X$ and, more generally, of $T^kX/T^{k+1}X$.*

Consequently, the $\phi$ component of $X/TX$ is sent to the $\chi^k\phi$-component of $T^kX/T^{k+1}X$.

*Proof.* Let $\psi \in \hat{\Delta}$ and suppose that $\delta(x+TX) = \psi(\delta)x + TX$ for all $\delta \in \Delta$. Then, there exist $y_\delta \in X$ such that $\delta(x) = \psi(\delta)x + Ty_\delta$. From Equation 2.2.2, we see that

$$\begin{aligned} \delta(Tx) &= \delta T\delta^{-1}\delta x \\ &= \delta((1+T)-1)\delta^{-1}\delta x \\ &= ((1+T)^{\chi(\delta)}-1)\delta(x) \end{aligned}$$

$$\begin{aligned}\delta(Tx) &= (\chi(\delta)T + T^2 f_\delta)(\psi(\delta)x + Ty_\delta) \\ &= \chi(\delta)\psi(\delta)Tx + T^2 z_\delta\end{aligned}$$

for some $f_\delta \in \Lambda$ and $z_\delta \in X$. □

**Example 3.5.2.** Let $K = \mathbb{Q}(\mu_p, \sqrt{d})$ where $d > 1$ is squarefree and $p$ splits in $\mathbb{Q}(\sqrt{d})$. Let $\Delta = \mathrm{Gal}(K/\mathbb{Q})$. We may identify $\Delta$ with $\mathrm{Gal}(\mathbb{Q}(\mu_p/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$. Let $\chi$ denote a character of $\mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$ of order $p-1$ and let $\phi$ denote the nontrivial character of $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$. Later, in our computations, we will take $\chi$ to be $\omega$, the Teichmüller character defined in Example 2.1.11. Applying Theorem 3.4.2 to the $\chi$-extension of $K$, we see that $X/TX \simeq \mathbb{Z}_p$ with

$$\Big\{\psi \in \hat{\Delta} : (X/TX)^{(\psi)} \sim \mathbb{Z}_p\Big\} = \Big\{\chi\phi\Big\}.$$

But, even though $X[T] \sim \mathbb{Z}_p$, we cannot pinpoint the unique character for which $(X[T])^{(\psi)}$ is infinite. Combining Theorem 3.4.6 with Lemma 3.5.1, we are still left with $(p-1)/2$ possibilities for this character:

$$\Big\{\psi \in \hat{\Delta} : (X[T])^{(\psi)} \sim \mathbb{Z}_p\Big\} \subseteq \Big\{\phi\Big\} \cup \Big\{\chi\phi, \chi^3\phi, \ldots, \chi^{p-2}\phi\Big\}.$$

It is certainly possible that $X$ is $T$-semisimple. On the other hand, if the decomposition subgroups for primes above $p$ generate an infinite subgroup of $X$, then the character for $X[T]$ is $\phi$. In this case, by Lemma 3.5.1, none of the quotients $T^k X/T^{k+1}X$ match the character of $X[T]$ until $T^{p-1}X/T^pX$, which would imply that one of the elementary factors for $X$ is $\Lambda/(T^{p^m})$ for some $m \geq 1$.

Similarly, for the $\chi\phi$-extension of $K$, we have

$$\Big\{\psi \in \hat{\Delta} : (X/TX)^{(\psi)} \sim \mathbb{Z}_p\Big\} = \Big\{\chi_0\Big\}$$

and

$$\Big\{\psi \in \hat{\Delta} : (X[T])^{(\psi)} \sim \mathbb{Z}_p\Big\} \subseteq \Big\{\chi_0\Big\} \cup \Big\{\chi, \chi^3, \ldots, \chi^{p-2}\Big\}$$

and so, if the decomposition subgroups for primes above $p$ in $X$ are infinite, we would have a large degree of nonsemisimplicity.

Our claim that Example 3.5.2 is interesting is based on the possibility that it can happen that the decomposition subgroups for primes above $p$ generate an infinite subgroup of $X[T]$, but not of $X/TX$. Can this situation ever occur? We will explore this question by revisiting Example 3.4.7.

**Example 3.5.3.** As in Example 3.4.7, let $K = \mathbb{Q}(\mu_5)$, let $p \equiv 9 \pmod{20}$, and let $\chi$ be a character of order 4 of $\Delta = \mathrm{Gal}(K/\mathbb{Q})$. We have seen that the Iwasawa module $X$ corresponding to $K_\infty^\chi$ is not $T$-semisimple. In this case, we have

$$\left\{\psi \in \hat{\Delta} : (X/TX)^{(\psi)} \sim \mathbb{Z}_p\right\} = \left\{\chi^{-1}\right\}$$

and

$$\left\{\psi \in \hat{\Delta} : (X[T])^{(\psi)} \sim \mathbb{Z}_p\right\} \subseteq \left\{\chi_0\right\} \cup \left\{\chi\right\}.$$

Here $\chi_0$ is of type-D and $\chi$ is of type-S. Working with Lemma 3.5.1 leads us to the following observation.

**Observation 3.5.4.** *Either there exist examples of $\mathbb{Z}_p$-extensions for which the decomposition subgroups for primes above $p$ generate an infinite subgroup of $X[T]$ but not of $X/TX$ or there exist examples of $\mathbb{Z}_p$-extensions for which $T^2X/T^3X$ is infinite.*

### *3.6 Some More Questions*

Proposition 3.3.1 gives a sufficient condition for $T$-semisimplicity. In light of this, Jaulent and Sands call extensions satisfying the hypothesis of Proposition 3.3.1 *arithmetically semisimple* as opposed to our definition of $T$-semisimple modules which they refer to as *algebraically semisimple*. In the appendix of [18], Jaulent and Sands asked if these two conditions are equivalent (i.e., if the sufficient condition for $T$-semisimplicity is also a necessary condition).

**Question 3.6.1.** *(Jaulent-Sands) Is every $\mathbb{Z}_p$-extension which is algebraically $T$-semisimple also arithmetically $T$-semisimple? That is, if $K_\infty/K$ is a $T$-semisimple $\mathbb{Z}_p$-extension and $X$ the corresponding Iwasawa module, must $X/TX$ be generated (up to finite index) by the decomposition subgroups for primes above $p$?*

We answer answer this question in the negative by providing explicit counterexamples: See Example 6.2.6 and Example 6.2.9.

The examples in Section 3.5 aim to study what one might call vertical nonsemisimplicity. That is, can one find examples where $T^kX/T^{k+1}X$ is nontrivial for large $k$. One could also study horizontal nonsemisimplicity and ask if one can find examples where $TX/T^2X$ has large $\mathbb{Z}_p$-rank. In Proposition 4.1.6 we will see that if $K/\mathbb{Q}$ is an abelian extension in which $p$ splits completely and if all primes above $p$ ramify in $K_\infty/K$, then $\mathrm{rank}_{\mathbb{Z}_p}(TX/T^2X) \leq \max\{\mathrm{rank}_{\mathbb{Z}_p}(X/TX) - 3, 0\}$. And in Corollary 4.2.2 we will see that $\mathrm{rank}_{\mathbb{Z}_p}(TX/T^2X) < \mathrm{rank}_{\mathbb{Z}_p}(X/TX)$ if the genus field of $K_\infty$ contains any $T$-semisimple $\mathbb{Z}_p$-extension.

# Chapter 4

# NEW RESULTS ON $T$-SEMISIMPLICITY

## *4.1 $T$-Semisimple $\mathbb{Z}_p$-Extensions*

**Definition 4.1.1.** Let $K$ be a CM field and denote the totally real subfield of $K$ by $K^+$. Let $K_\infty/K$ be a $\mathbb{Z}_p$-extension of $K$ with $\Gamma = \mathrm{Gal}(K_\infty/K)$. We say that $K_\infty$ is *anti-cyclotomic* if $K_\infty/K^+$ is Galois and complex conjugation acts nontrivially on $\Gamma$.

Throughout this chapter we will use $\tau$ to denote the complex conjugation automorphism for a CM field: if $K$ is a CM field with totally real subfield $K^+$, then $\mathrm{Gal}(K/K^+) = \langle\tau\rangle$.

Let $K$ be a number field. Let $\mathcal{E}(K)$ denote the set of all $\mathbb{Z}_p$-extensions of $K$ and, for each $\mathbb{Z}_p$-extension $K_\infty/K$ let $\mathcal{E}(K_\infty, n)$ denote the subset consisting of extensions $K'_\infty/K$ sharing the same $n$-th layer:

$$\mathcal{E}(K_\infty, n) = \{K'_\infty \in \mathcal{E}(K) : K_n \subseteq K_\infty \cap K'_\infty\}.$$

In Section 3 of [12], Greenberg showed that one can topologize $\mathcal{E}(K)$ by taking the collection $\{\mathcal{E}(K_\infty, n) : K_\infty \in \mathcal{E}(K), n \geq 0\}$ as a basis of open sets. Under this topology, $\mathcal{E}(K)$ is a compact Hausdorff space.

**Proposition 4.1.2.** *Let $K$ be a CM number field. Then the subset of $\mathcal{E}(K)$ consisting of $\mathbb{Z}_p$-extensions which are not anti-cyclotomic is dense. That is, generic $\mathbb{Z}_p$-extensions of $K$ are not anti-cyclotomic.*

*Proof.* Let us first show that the set of non-anti-cyclotomic extensions is open. Suppose that $K_\infty/K$ is not anti-cyclotomic. Then, for sufficiently large $n$, either $K_n/K^+$ is not Galois or $K_n/K^+$ is abelian. In either case, complex conjugation does not act nontrivially on $\mathrm{Gal}(K_n/K)$. It follows that every $\mathbb{Z}_p$-extension in $\mathcal{E}(K_\infty, n)$ is not anti-cyclotomic.

To show that the set of non-anti-cyclotomic extensions is dense, it suffices to show that $\mathcal{E}(K_\infty, n)$ contains a $\mathbb{Z}_p$-extension which is not anti-cyclotomic for all $K_\infty/K$ and $n \geq 0$. If $K_\infty/K$ is not anti-cyclotomic, this is immediate so let us consider the case where $K_\infty/K$ is anti-cyclotomic.

Note that $K_\infty$ is the only anti-cyclotomic $\mathbb{Z}_p$-extension of $K$ contained in the compositum $K_\infty K_\infty^{cyc}$. Let $\Xi = \mathrm{Gal}(K_\infty K_\infty^{cyc}/K) \simeq \mathbb{Z}_p^2$. Let $\xi_+$ and $\xi_-$ be topological generators for $\Xi^+$ and $\Xi^-$, respectively. Note that $K_n$ is the fixed field of the closure of the subgroup generated by $\xi_+$ and $(\xi_-)^{p^n}$. Let $K'_\infty$ denote the field fixed by the subgroup $\overline{\langle \xi_+ (\xi_-)^{p^n} \rangle} \subseteq \Xi$. Then $K_n \subseteq K'_\infty$ but $K'_\infty/K$ is not anti-cyclotomic. That is, $\mathcal{E}(K_\infty, n)$ contains a $\mathbb{Z}_p$-extension which is not anti-cyclotomic. □

**Theorem 4.1.3.** *Let $K$ be an abelian number field and $K_\infty/K$ a $\mathbb{Z}_p$-extension which is not anti-cyclotomic. Then $K_\infty/K$ is $T$-semisimple.*

Let $K_\infty/K$ be a $\mathbb{Z}_p$-extension which is not anti-cyclotomic and let $X$ denote the Iwasawa module associated to $K_\infty/K$. By Proposition 3.3.1, it suffices to show that the decomposition subgroups for primes above $p$ generate a finite index subgroup of $X/TX$ or, equivalently, that the decomposition subgroups for primes above $p$ generate a finite index subgroup of $\mathrm{Gal}(\tilde{K}_\infty/K_\infty)$.

Note that this is sufficient even in the case where not all primes above $p$ are ramified in $K_\infty/K$. In this case, the genus field $L^*_\infty$ of $K_\infty/K$ is not a finite extension of $\tilde{K}_\infty$. Instead, $L^*_\infty$ is a finite extension of some intermediate field $K_\infty \subseteq K^*_\infty \subseteq \tilde{K}_\infty$. Note that $\mathrm{Gal}(K^*_\infty/K_\infty)$ is a quotient of $\mathrm{Gal}(\tilde{K}_\infty/K)$ and the decompositions subgroups of the latter group surject onto those of the former. In particular, if the decomposition subgroups for primes above $p$ generate a finite index subgroup for $\mathrm{Gal}(\tilde{K}_\infty/K_\infty)$, then the same is true for $\mathrm{Gal}(K^*_\infty/K_\infty)$.

In order to study the dcomposition subgroups for primes above $p$ in $\mathrm{Gal}(\tilde{K}_\infty/K_\infty)$, let us begin by studying the decomposition in the larger group $\tilde{\Gamma} = \mathrm{Gal}(\tilde{K}_\infty/K)$.

**Lemma 4.1.4.** *Let $s$ denote the number of distinct primes lying above $p$ in $K^+$, the totally*

*real subfield of $K$, then for each prime $\mathfrak{p}$ of $K$ lying above $p$, we have*

$$\mathrm{rank}_{\mathbb{Z}_p}(\tilde{\Gamma}_{\mathfrak{p}}) = \frac{n}{2s} + 1$$

*Proof.* Case 1: $\tau \in \Delta_p$.

Suppose that complex conjugation is contained in the decomposition subgroup $\Delta_p$ of $\Delta$. Note that there are exactly $s$ primes lying above $p$ in $K$. We know from Proposition 3.4.3 that $K_\infty^{cyc}$ admits no unramified $\mathbb{Z}_p$-extension which is abelian over $K$. It follows that the $s$ decomposition subgroups $\tilde{\Gamma}_{\mathfrak{p}}$ for primes above $p$ in $\tilde{\Gamma}$ are actually inertia subgroups. It also follows that that the decomposition subgroups of $\tilde{\Gamma}^- = \mathrm{Gal}(\tilde{K}_\infty/K_\infty^{cyc})$ generate a finite index subgroup of $\tilde{\Gamma}^-$.

Because $\tau \in \Delta_p$, complex conjugation acts on each $\tilde{\Gamma}_{\mathfrak{p}}$, yielding a decomposition into plus and minus parts:

$$\tilde{\Gamma}_{\mathfrak{p}} = \left(\tilde{\Gamma}_{\mathfrak{p}}\right)^+ \oplus \left(\tilde{\Gamma}_{\mathfrak{p}}\right)^- .$$

The plus part is nontrivial because $K_\infty^{cyc}/K$ is ramified at $\mathfrak{p}$. It follows that $(\tilde{\Gamma}_{\mathfrak{p}})^+$ is a finite index subgroup of $\tilde{\Gamma}^+$ for each $\mathfrak{p}$ and, therefore that the intersection of all the $\tilde{\Gamma}_{\mathfrak{p}}$ contains a free $\mathbb{Z}_p$-module of rank 1. Now, for each $\mathfrak{p}$, $(\tilde{\Gamma}_{\mathfrak{p}})^-$ is a free $\mathbb{Z}_p$-module of rank $r$ for some $r > 0$. Recall that $K_{\mathfrak{p}}$, the completion of $K$ at $\mathfrak{p}$, admits $[K_{\mathfrak{p}} : \mathbb{Q}_p] + 1 = \frac{n}{s} + 1$ independent $\mathbb{Z}_p$-extensions. One of these is unramified and complex conjugation acts trivially on half of the remaining extensions. It follows that $0 \leq r \leq \frac{n}{2s}$.

Recall that the $s$ decomposition subgroups $(\tilde{\Gamma}_{\mathfrak{p}})^-$ generate a finite index subgroup of $\tilde{\Gamma}^-$, a free $\mathbb{Z}_p$-module of rank $\frac{n}{2}$. The only way this can happen is if $r$ attains the upper bound $r = \frac{n}{2s}$.

Case 2: $\tau \notin \Delta_p$

Suppose now that complex conjugation is not contained in $\Delta_p$. The proof is very similar to the previous case, except that we will focus on conjugate pairs of decomposition subgroups instead of the decomposition subgroups themselves.

As before, let $s$ denote the number of distinct primes lying above $p$ in $K^+$. Then there are exactly $2s$ primes lying above $p$ in $K$. For each prime $\mathfrak{p}$, let $\bar{\mathfrak{p}}$ denote its conjugate:

$\bar{\mathfrak{p}} = \tau(\mathfrak{p})$. It is no longer true that complex conjugation acts on each decomposition subgroup $\tilde{\Gamma}_{\mathfrak{p}}$. However, $\tilde{\Gamma}_{\mathfrak{p}}$ does contain a subgroup on which complex conjugation acts, namely the decomposition subgroup of $\tilde{\Gamma}^- : \tilde{\Gamma}_{\mathfrak{p}} \cap \tilde{\Gamma}^-$.

Note also that, in $\tilde{\Gamma}^-$, the decomposition subgroups for the conjugate primes $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ are the same. Let $r$ denote the $\mathbb{Z}_p$-rank of $\tilde{\Gamma}_{\mathfrak{p}} \cap \tilde{\Gamma}^-$. Then, because $K_\infty^{cyc}/K$ is ramified at $\mathfrak{p}$, we see that $\text{rank}_{\mathbb{Z}_p}(\tilde{\Gamma}_{\mathfrak{p}}) = r + 1$. To determine $r$, we will once again work locally. This time, the completion $K_{\mathfrak{p}}$ admits $[K_{\mathfrak{p}} : \mathbb{Q}_p] + 1 = \frac{n}{2s} + 1$ independent $\mathbb{Z}_p$-extensions. It follows that $r + 1 \leq \frac{n}{2s} + 1$.

Theorem 3.2.1 tells us that the decomposition subgroups for primes above $p$ generate a finite index subgroup of $\tilde{\Gamma}^-$, a free $\mathbb{Z}_p$-module of rank $\frac{n}{2}$. We have seen that there are at most $s$ distinct decomposition subgroups (since the decomposition subgroups for $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ are the same) and that each such group has $\mathbb{Z}_p$-rank $r \leq \frac{n}{2s}$. It follows that $r$ attains the upper bound of $\frac{n}{2s}$. □

*Proof Theorem 4.1.3.* Let $K_\infty/K$ be a $\mathbb{Z}_p$-extension which is not anti-cyclotomic. Let $\tilde{\Gamma} = \text{Gal}(\tilde{K}_\infty/K)$ as above and also and set $\Theta = \text{Gal}(\tilde{K}_\infty/K)$.

We first reduce to a linear algebra problem. Let $G = \tilde{\Gamma} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$ and $H = \Theta \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Let $\mathfrak{p}$ be a prime of $K$ lying above $p$ and let $\tilde{\Gamma}_{\mathfrak{p}}$ denote the decomposition subgroup of $\mathfrak{p}$ in $\tilde{\Gamma}$ and let $G_{\mathfrak{p}} \subseteq G$ denote the subspace generated by $\tilde{\Gamma}_{\mathfrak{p}}$ in $G$:

$$G_{\mathfrak{p}} = \tilde{\Gamma}_{\mathfrak{p}} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$

We will refer to $G_{\mathfrak{p}}$ as the decomposition subspace of $\mathfrak{p}$ in $G$. In a similar manner, one can define the decomposition subspaces for subspaces and quotients of $G$. In particular

$$H_{\mathfrak{p}} = \Theta_{\mathfrak{p}} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = \left(\Theta \cap \tilde{\Gamma}_{\mathfrak{p}}\right) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p = \left(\Theta \otimes_{\mathbb{Z}_p} \mathbb{Q}_p\right) \cap \left(\tilde{\Gamma}_{\mathfrak{p}} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p\right) = H \cap G_{\mathfrak{p}},$$

as one would hope.

Our goal is to show that $H = \text{Span}(\{H_{\mathfrak{p}} : \mathfrak{p}|p\})$.

Let $\pi$ denote the quotient map $\pi : G \to G/G^+$. Recall that the $\mathbb{Z}_p$-extension $K_\infty$ is not anti-cyclotomic. This means that $G^+$ is not contained in $H$. It follows that $\pi$ induces an

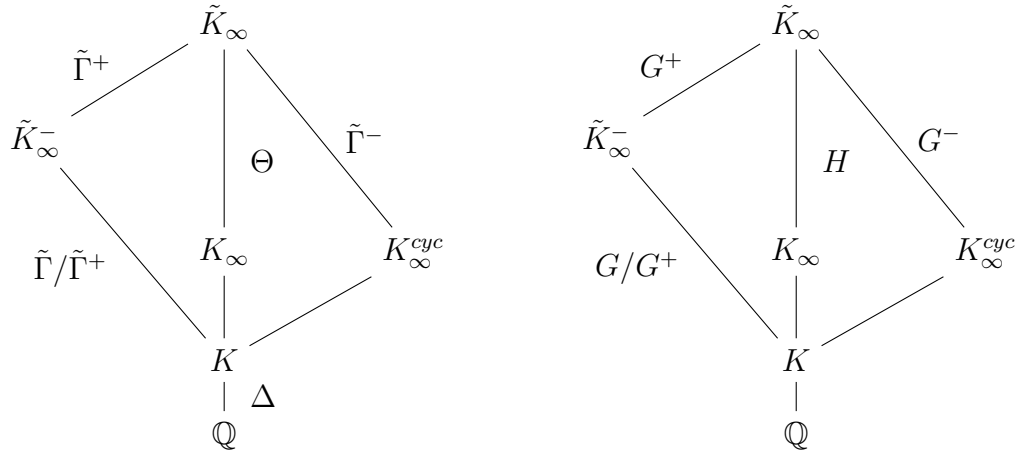


Figure 4.1: The various Galois groups (left) and the corresponding vector spaces (right) studied in the proof of Theorem 4.1.3.

isomorphism $\pi : H \xrightarrow{\simeq} G/G^+$. We will show that the images of the $H_\mathfrak{p}$ under the map $\pi$ span $G/G^+$. As with the proof of Lemma 4.1.4, there are two cases to consider.

Case 1: $\tau \in \Delta_p$

In the proof of Lemma 4.1.4, we saw that $G^-$ is generated by the decomposition subspaces $(G^-)_\mathfrak{p}$ for $\mathfrak{p}|p$ (since $K_\infty^{cyc}$ admits no unramified $\mathbb{Z}_p$-extensions). Combining this with the fact that $G/G^+ = \pi(G^-)$, we see that

$$G/G^+ = \mathrm{Span}\left(\{\pi\left((G^-)_\mathfrak{p}\right) : \mathfrak{p}|p\}\right).$$

Note that $(G^-)_\mathfrak{p}$ and $H_\mathfrak{p}$ are both $\frac{n}{2s}$-dimensional subspaces of the $(\frac{n}{2s}+1)$-dimensional space $G_\mathfrak{p}$. The maps $G^- \to G/G^+$ and $H \to G/G^+$ are both isomorphisms, so $\pi((G^-)_\mathfrak{p})$ and $\pi(H_\mathfrak{p})$ are on $\frac{n}{2s}$-dimensional subspaces of $\pi(G_\mathfrak{p})$. On the other hand, $G_\mathfrak{p} \cap G^+ = G^+$ so $\pi(G_\mathfrak{p})$ is itself $\frac{n}{2s}$-dimensional. It follows that

$$\pi\left(H_\mathfrak{p}\right) = \pi(G_\mathfrak{p}) = \pi\left((G^-)_\mathfrak{p}\right)$$

and, therefore, that

$$G/G^+ = \mathrm{Span}\left(\{\pi\left(H_\mathfrak{p}\right) : \mathfrak{p}|p\}\right).$$

Because $H \xrightarrow{\pi} G/G^+$ is an isomorphism, it follows that

$$H = \text{Span}\{H_{\mathfrak{p}} : \mathfrak{p}|p\}.$$

Case 2: $\tau \notin \Delta_p$

In this case, we will consider conjugate pairs of decomposition subspaces $H_{\mathfrak{p}}$ and $H_{\bar{\mathfrak{p}}}$ and show that

$$G/G^+ = \text{Span}\left(\{\pi\left(H_{\mathfrak{p}}H_{\bar{\mathfrak{p}}}\right) : \mathfrak{p}|p\}\right).$$

The proof of Theorem 3.2.1 shows that $G^-$ is generated by the decomposition subspaces $(G^-)_{\mathfrak{p}}$ for $\mathfrak{p}|p$. Therefore, because $G^-$ surjects onto $G/G^+$, it suffices to show that

$$\pi\left((G^-)_{\mathfrak{p}}\right) \subseteq \text{Span}\left(\{\pi\left(H_{\mathfrak{p}}H_{\bar{\mathfrak{p}}}\right) : \mathfrak{p}|p\}\right)$$

for all $\mathfrak{p}|p$.

If $H_{\mathfrak{p}} = H_{\bar{\mathfrak{p}}}$, then complex conjugation acts on $H_{\mathfrak{p}}$, which can be decomposed as

$$H_{\mathfrak{p}} = H_{\mathfrak{p}}^+ H_{\mathfrak{p}}^-$$

Since $G^+ \nsubseteq H$, we have $H_{\mathfrak{p}}^+ = 0$. Consequently, $H_{\mathfrak{p}} = (G^-)_{\mathfrak{p}}$.

Suppose instead that $H_{\mathfrak{p}} \neq H_{\bar{\mathfrak{p}}}$. Then, because each $H_{\mathfrak{p}}$ is $\frac{n}{2s}$-dimensional, $H_{\mathfrak{p}}H_{\bar{\mathfrak{p}}}$ is a subspace of dimension at least $\frac{n}{2s}+1$. Note that $G_{\mathfrak{p}}G_{\bar{\mathfrak{p}}}$ has dimension $\frac{n}{2s}+2$ since $G_{\mathfrak{p}} \cap G_{\bar{\mathfrak{p}}} = (G^-)_{\mathfrak{p}}$. Therefore, since $G^+ \subseteq G_{\mathfrak{p}}G_{\bar{\mathfrak{p}}}$, we see that

$$\dim\left(\pi\left(G_{\mathfrak{p}}G_{\bar{\mathfrak{p}}}\right)\right) = \frac{n}{2s} + 1.$$

We have $\pi(H_{\mathfrak{p}}H_{\bar{\mathfrak{p}}}) \subseteq \pi\left(G_{\mathfrak{p}}G_{\bar{\mathfrak{p}}}\right)$. Furthemore, $\pi : H \to G/G^+$ is injective so, comparing dimensions we see that $\pi(H_{\mathfrak{p}}H_{\bar{\mathfrak{p}}}) = \pi\left(G_{\mathfrak{p}}G_{\bar{\mathfrak{p}}}\right)$ and thus

$$\pi((G^-)_{\mathfrak{p}}) \subseteq \pi(H_{\mathfrak{p}}H_{\bar{\mathfrak{p}}}),$$

as desired. It follows that

$$\text{Span}\left(\{\pi\left(H_{\mathfrak{p}}H_{\bar{\mathfrak{p}}}\right) : \mathfrak{p}|p\}\right) \supseteq \text{Span}\left(\{\pi\left((G^-)_{\mathfrak{p}}\right) : \mathfrak{p}|p\}\right) = G/G^+$$

Finally, because $\pi : H \to G/G^+$ is an isomorphism, we see that

$$H = \mathrm{Span}\left(\{H_{\mathfrak{p}} : \mathfrak{p}|p\}\right).$$

This completes the proof of Theorem 4.1.3. □

**Corollary 4.1.5.** *Generic $\mathbb{Z}_p$-extensions of abelian number fields are $T$-semisimple.*

This result was proven independently by Kataoka (See Corollary 4.8 of [19]). He actually proves a more general result than we do: If $K$ is any number field which admits an arithmetically $T$-semisimple $\mathbb{Z}_p$-extension (i.e. one which satisfies the hypotheses of Proposition 3.3.1), then generic $\mathbb{Z}_p$-extensions of $K$ are arithmetically $T$-semisimple. In contrast, our proof requires the cyclotomic $\mathbb{Z}_p$-extension to be arithmetically $T$-semisimple and relies heavily on the action of complex conjugation so, while our proof could carry over to CM fields, it will not apply to arbitrary number fields. However, our more restricted focus allows us to explicitly identify a dense open subset consisting of $T$-semisimple extensions.

We relied only on Theorem 3.2.1. In certain cases, we can obtain a little more information if we also make use of Theorem 3.2.2?

**Proposition 4.1.6.** *Let $K/\mathbb{Q}$ be an abelian extension. Let $p$ be an odd prime such that the exponent of* $\mathrm{Gal}(K/\mathbb{Q})$ *divides $p-1$ and such that $p$ splits completely in $K/\mathbb{Q}$. Let $K_\infty/K$ be a $\mathbb{Z}_p$-extension in which all the primes above $p$ ramify and let $X$ denote the associated Iwasawa module. Then the image of the map*

$$X[T] \to X/TX$$

*has $\mathbb{Z}_p$-rank at least* $\min(3, \mathrm{rank}_{\mathbb{Z}_p}(X/TX))$.

*Proof.* We will prove this by showing that the decomposition subgroups of primes above $p$ generate a submodule of $X/TX$ of $\mathbb{Z}_p$-rank at least $\min(3, \mathrm{rank}_{\mathbb{Z}_p}(X/TX))$. We will make use of the fact that the $\chi$-$\mathbb{Z}_p$-extensions of $K$ are all $T$-semisimple.

If $\mathrm{rank}_{\mathbb{Z}_p}(X/TX) = 1$, then $K$ is quadratic and $X$ is $T$-semisimple by Corollary 3.3.4 so let us suppose that $\mathrm{rank}_{\mathbb{Z}_p}(X/TX) \geq 2$. If $K_\infty/K$ is not anti-cyclotomic, then the result is

a consequence of Theorem 4.1.3, so let us suppose that $K_\infty \subseteq \tilde{K}_\infty^-$. Using the same notation as above, we have $G^+ \subseteq H_\mathfrak{p} H_{\bar{\mathfrak{p}}}$ for all $\mathfrak{p}|p$.

We will start by showing that $H_\mathfrak{p} \neq H_{\bar{\mathfrak{p}}}$ and thus that $\dim(H_\mathfrak{p} H_{\bar{\mathfrak{p}}}) = 2$. Suppose otherwise. Then, because $K_\infty$ is anti-cyclotomic and all primes $\mathfrak{p}$ are ramified in $K_\infty/K$, we have $H_\mathfrak{p} = H_{\bar{\mathfrak{p}}} = G^+$ for all $\mathfrak{p}|p$. Consequently, the decomposition subgroup for every prime above $p$ has $\mathbb{Z}_p$-rank 1 in $\mathrm{Gal}(\tilde{K}_\infty/\tilde{K}_\infty^-)$. Let $\psi$ be any odd character of $\Delta$. Then the decomposition subgroups for primes above $p$ in $\mathrm{Gal}(\tilde{K}_\infty/K_\infty^\psi)$ each have $\mathbb{Z}_p$-rank 1. But $\mathrm{Gal}(\tilde{K}_\infty/K_\infty^\psi)$ contains $\mathrm{Gal}(\tilde{K}_\infty/\tilde{K}_\infty^-)$ so the decomposition subgroups must all be contained in $\mathrm{Gal}(\tilde{K}_\infty/\tilde{K}_\infty^-) \simeq \mathbb{Z}_p$. However, we know from the proof of Theorem 3.2.2 that these decomposition subgroups generate a finite index subgroup of $\mathrm{Gal}(\tilde{K}_\infty/K_\infty^\psi)$. But

$$\mathrm{rank}_{\mathbb{Z}_p}\left(\mathrm{Gal}(\tilde{K}_\infty/K_\infty^\psi)\right) = \mathrm{rank}_{\mathbb{Z}_p}\left(X/TX\right) \geq 2,$$

yielding the desired contradiction. It follows that $\dim(H_\mathfrak{p} H_{\bar{\mathfrak{p}}}) = 2$ and thus that $\dim\left(\mathrm{Span}\{H_\mathfrak{p} : \mathfrak{p}|p\}\right) \geq 2$.

Finally, suppose that $\mathrm{rank}_{\mathbb{Z}_p}(X/TX) > 2$ but $\dim\left(\mathrm{Span}\{H_\mathfrak{p} : \mathfrak{p}|p\}\right) = 2$. Then we have

$$\mathrm{Span}\{H_\mathfrak{p} : \mathfrak{p}|p\} = H_\mathfrak{p} H_{\bar{\mathfrak{p}}} = H_{\delta(\mathfrak{p})} H_{\delta(\bar{\mathfrak{p}})} = \delta(H_\mathfrak{p} H_{\bar{\mathfrak{p}}})$$

for all $\delta \in \Delta$. Consequently, $\Delta$ acts on $\mathrm{Span}\{H_\mathfrak{p} : \mathfrak{p}|p\}$ which can be decomposed into 1-dimension eigenspaces corresponding to the trivial character $\chi_0$ and another character $\varphi$. Let $K_\infty^*$ denote the compositum of the $\chi$-extensions for $\chi \neq \chi_0, \varphi$:

$$K_\infty^* = \prod_{\chi \neq \chi_0, \varphi} K_\infty^\chi.$$

It follows that the decomposition subgroups for primes above $p$ in $\mathrm{Gal}(\tilde{K}_\infty/K_\infty)$ are contained in the subgroup $\mathrm{Gal}(\tilde{K}_\infty/K_\infty^*)$ Now, let $\psi$ be another odd character of $\Delta$ with $\psi \neq \varphi$. Note that for each $\mathfrak{p}$, the decomposition subgroup for $\mathfrak{p}$ in $\mathrm{Gal}(\tilde{K}_\infty/K_\infty^\psi)$ has $\mathbb{Z}_p$-rank 1. Since $\mathrm{Gal}(\tilde{K}_\infty/K_\infty^\psi)$ contains $\mathrm{Gal}(\tilde{K}_\infty/K_\infty^*)$ and $\tilde{\Gamma}_\mathfrak{p} \cap \mathrm{Gal}(\tilde{K}_\infty/K_\infty^*) \simeq \mathbb{Z}_p$, it follows that all the decomposition subgroups of $\mathrm{Gal}(\tilde{K}_\infty/K_\infty^\psi)$ for primes above $p$ are contained in $\mathrm{Gal}(\tilde{K}_\infty/K_\infty^*)$. Therefore, these decomposition subgroups generate a subgroup of $\mathbb{Z}_p$-rank 2.

But, by assumption, $\text{rank}_{\mathbb{Z}_p}(\text{Gal}(\tilde{K}_\infty/K_\infty^\psi)) \geq 3$. We know from the proof of Theorem 3.2.2 that the decomposition subgroups for primes above $p$ generate a finite index subgroup of $\text{Gal}(\tilde{K}_\infty/K_\infty^\psi)$, yielding the desired contradiction. It must therefore be the case that $\dim \text{Span}\{H_\mathfrak{p} : \mathfrak{p}|p\} > 2$. The desired result then follows from Proposition 3.3.1. □

**Corollary 4.1.7.** *Let $K/\mathbb{Q}$ be a complex abelian extension of degree 4. Let $p$ be an odd prime such that the exponent of $\text{Gal}(K/\mathbb{Q})$ divides $p-1$ and such that $p$ splits completely in $K/\mathbb{Q}$. Then every $\mathbb{Z}_p$-extension of $K$ is $T$-semisimple.*

*Proof.* If $K_\infty/K$ is not anti-cyclotomic, the result follows by Theorem 4.1.3. If all four primes above $p$ are ramified in $K_\infty/K$, the result follows from Proposition 4.1.6. Suppose then that $K_\infty/K$ is anti-cyclotomic and that there exists a prime $\mathfrak{p}$ of $K$ lying above $p$ which is not ramified in $K_\infty/K$. We will show that $K_\infty/K$ admits no trivial zeros and is therefore (vacuously) $T$-semisimple

Let $I_\mathfrak{p}$ denote the inertia subgroup of $\mathfrak{p}$ in $\text{Gal}(\tilde{K}_\infty/K_\infty)$. Because $K_\infty/K$ is anti-cyclotomic, $K_\infty$ is Galois over $K^+$. Consequently $\bar{\mathfrak{p}}$ must also be unramified in $K_\infty/K$. Note that $I_\mathfrak{p} I_{\bar{\mathfrak{p}}}$ is a finite index subgroup of $\text{Gal}(\tilde{K}_\infty/K)$. It follows that the genus field of $K_\infty/K$ is simply a finite extension of $K_\infty$. Therefore $X/TX \sim 0$ as claimed. □

## *4.2 Nonsemisimple $\mathbb{Z}_p$-Extensions*

We saw that Kisilevsky's examples of nonsemisimple extensions came in pairs. In fact, the existence of a single extension which is not $T$-semisimple forces the existence of uncountably many more.

**Proposition 4.2.1.** *Let $K_\infty^1/K$ be a $\mathbb{Z}_p$-extension which is not $T_1$-semisimple and let $X_1$ denote the associated Iwasawa module. Let $K_\infty^2$ be another $\mathbb{Z}_p$-extension of $K$ satisfying the following conditions:*

*(a) $K_\infty^2$ is contained in the genus field of $K_\infty^1$*

*(b) Every prime which is ramified in $K_\infty^1/K$ is also ramified in $K_\infty^2/K$*

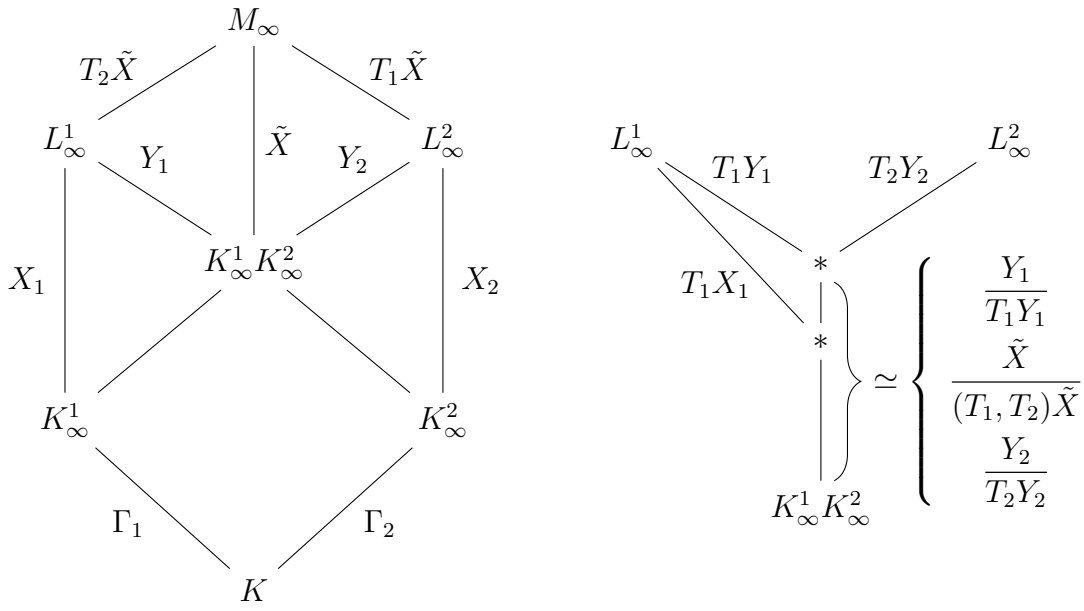


Figure 4.2: Some of the fields and Galois groups used in the proof of Proposition 4.2.1

*(c) $K^2_\infty$ is contained in the fixed field of $X_1[T_1]$*

*Then the extension $K^2_\infty/K$ is not $T_2$-semisimple.*

*Proof.* For $i = 1, 2$, let $\Gamma_i = \mathrm{Gal}(K^i_\infty/K)$ and let $\Lambda_i = \mathbb{Z}_p[[\Gamma_i]]$ denote the corresponding Iwasawa algebra which, as usual, we will identify with a power series ring $\mathbb{Z}_p[[T_i]]$. Let $L^i_\infty$ denote the pro-$p$ Hilbert class field of $K^i_\infty$ and let $X_i = \mathrm{Gal}(L^i_\infty/K^i_\infty)$.

Let $M_\infty$ denote the pro-$p$ Hilbert class field of $K^1_\infty K^2_\infty$ and let $\tilde{X} = \mathrm{Gal}(M_\infty/K^1_\infty K^2_\infty)$. Then $\tilde{X}$ is a module over the ring $\tilde{\Lambda} = \mathbb{Z}_p[[\Gamma_1\Gamma_2]] \simeq \mathbb{Z}_p[[T_1, T_2]]$ and is related to $X_1$ and $X_2$. To identify $\mathrm{Gal}(L^1_\infty/K^1_\infty K^2_\infty) = X_1 \cap \tilde{X}$ as a quotient of $\tilde{X}$, one needs to quotient out by the commutator subgroup of $\mathrm{Gal}(M_\infty/K^1_\infty)$. The commutator subgroup contains $T_2\tilde{X}$ and, because, $\mathrm{Gal}(M_\infty/K^1_\infty)/\tilde{X} \simeq \mathbb{Z}_p$, the submodule $T_2\tilde{X}$ is in fact the whole commutator subgroup. Set $Y_1 = \tilde{X}/T_2\tilde{X}$ and $Y_2 = \tilde{X}/T_1\tilde{X}$. Then we have $Y_i = \mathrm{Gal}(L^i_\infty/K^1_\infty K^2_\infty)$. The various fields and Galois groups are pictured in Figure 4.2.

By assumption, $X_1[T_1] \subseteq Y_1$ and thus $X_1[T_1] \subseteq Y_1[T_1]$, but $Y_1$ is a submodule of $X_1$ so we see that in fact $X_1[T_1] = Y_1[T_1]$. Therefore

$$\mathrm{rank}_{\mathbb{Z}_p}\left(\frac{Y_1}{T_1Y_1}\right) = \mathrm{rank}_{\mathbb{Z}_p}\left(Y_1[T_1]\right) = \mathrm{rank}_{\mathbb{Z}_p}\left(X_1[T_1]\right) = \mathrm{rank}_{\mathbb{Z}_p}\left(\frac{X_1}{T_1X_1}\right).$$

Note that, as Galois groups, we have

$$\frac{Y_1}{T_1Y_1} = \frac{\tilde{X}/T_2\tilde{X}}{T_1\left(\tilde{X}/T_2\tilde{X}\right)} \simeq \frac{\tilde{X}}{(T_1,T_2)\tilde{X}} \simeq \frac{\tilde{X}/T_1\tilde{X}}{T_2\left(\tilde{X}/T_1\tilde{X}\right)} = \frac{Y_2}{T_2Y_2}.$$

Conditions (a) and (b) together imply that $K_\infty^1$ and $K_\infty^2$ have the same genus field: Because $K_\infty^2$ is contained in the genus field of $K_\infty^1$, the field $K_\infty^1K_\infty^2$ is an unramified extension of $K_\infty^1$. Therefore, the primes ramified in $K_\infty^1K_\infty^2/K$ are precisely the primes ramified in $K_\infty^1/K$, and each inertia subgroup is isomorphic to $\mathbb{Z}_p$. But all such primes are ramified in $K_\infty^2/K$ (with inertia subgroups isomorphic to $\mathbb{Z}_p$). It follows that $K_\infty^1K_\infty^2/K_\infty^2$ is also unramified. Now, let $N_\infty^1$ denote the genus field of $K_\infty^1$, i.e., the maximal unramified pro-$p$ extension of $K_\infty^1$ which is abelian over $K$. Then $N_\infty^1$ contains $K_\infty^2$ and is unramified over $K_\infty^1K_\infty^2$. Because $K_\infty^1K_\infty^2/K_\infty^2$ is unramified, it follows that $N_\infty^1$ is an unramified pro-$p$ extension of $K_\infty^2$ which is abelian over $K$ so $N_\infty^1$ is contained in the genus field of $K_\infty^2$. Applying the same argument with the roles of $K_\infty^1$ and $K_\infty^2$ reversed, we conclude that $K_\infty^1$ and $K_\infty^2$ have the same genus field. In particular, this means that

$$\mathrm{rank}_{\mathbb{Z}_p}\left(\frac{X_1}{T_1X_1}\right) = \mathrm{rank}_{\mathbb{Z}_p}\left(\frac{X_2}{T_2X_2}\right).$$

Now, consider the following commutative diagram:

$$\begin{array}{ccc} Y_2[T_2] & \longrightarrow & \dfrac{Y_2}{T_2Y_2} \\ \big\downarrow & & \big\downarrow \\ X_2[T_2] & \longrightarrow & \dfrac{X_2}{T_2X_2} \end{array}$$

All four modules have the same $\mathbb{Z}_p$-rank. However, the cokernel (and thus the kernel) of the map

$$Y_2/T_2Y_2 \to Y_2/(T_2X_2 \cap Y_2) \to X_2/T_2X_2$$

has $\mathbb{Z}_p$-rank 1. It follows that the kernel of the map $X_2[T_2] \to X_2/T_2X_2$ has positive $\mathbb{Z}_p$-rank and, thus, that $X_2$ is not $T_2$-semisimple. □

When $\mathrm{rank}_{\mathbb{Z}_p}(X_1/T_1X_1) = 1$, one can give a different proof, which we sketch below: Let $Z_1$ denote the module

$$Z_1 = \frac{(X_1/T_1^2X_1)}{(X_1/T_1^2X_1)\,[p^\infty]}$$

and let $E_\infty$ denote the corresponding extension of $K_\infty^1$: $\mathrm{Gal}(E_\infty/K_\infty^1) \simeq Z_1$. Note that $Z_1$ is annihilated by $T_1^2$ and does not have any finite submodules. In fact, there is an inclusion

$$Z_1 \hookrightarrow \frac{\Lambda_1}{(T_1^2)}.$$

From the exact sequence

$$0 \to Z_1[T_1] \longrightarrow Z_1 \xrightarrow{T_1} T_1Z_1 \to 0$$

we obtain an isomorphism $T_1Z_1 \simeq Z_1/Z_1[T_1]$. By construction, $Z_1$ has no finite submodules so the same holds for $T_1Z_1$ and thus also $Z_1/Z_1[T_1]$. It follows that $Z_1/Z_1[T_1] \simeq \mathbb{Z}_p$. It must therefore be the case that the fixed field of $Z_1[T_1]$ in $E_\infty$ is $K_\infty^1K_\infty^2$.

The extension $E_\infty/K_\infty^2$ is certainly pro-$p$ and unramified. We need to show that it is also abelian. Note that $Z_1[T_1] \simeq \mathrm{Gal}(E_\infty/K_\infty^1K_\infty^2)$ is in the center of $\mathrm{Gal}(E_\infty/K)$, and thus in the center of $\mathrm{Gal}(E_\infty/K_\infty^2)$. But the quotient $Z_1/Z_1[T_1]$is pro-cyclic. It follows that $\mathrm{Gal}(E_\infty/K_\infty^2)$ is abelian.

**Corollary 4.2.2.** *Let $K_\infty^1/K$ and $K_\infty^2/K$ be two $\mathbb{Z}_p$-extensions with the same genus field. Then, if $K_\infty^2$ is $T$-semisimple, the image of the map $X_1[T] \to X_1/T_1X_1$ has positive $\mathbb{Z}_p$-rank.*

*Proof.* By Proposition 4.2.1, since $K_\infty^1$ and $K_\infty^2$ share the same genus field, but $K_\infty^2$ is $T$-semisimple, it must be the case that $K_\infty^2$ is not fixed by $X_1[T_1]$. We have the exact sequence

$$0 \to \mathrm{Gal}(L_\infty^1/K_\infty^1K_\infty^2) \to X \to \mathrm{Gal}(K_\infty^1K_\infty^2/K_\infty^1) \to 0$$

Since $K_\infty^2$ is not fixed by $X_1[T_1]$, the submodule $X_1[T_1]$ is not contained in the kernel of the map $X \to \mathrm{Gal}(K_\infty^1 K_\infty^2/K_\infty^1)$ and, therefore the image of $X_1[T_1]$ generates a nontrivial subgroup of $\mathrm{Gal}(K_\infty^1 K_\infty^2/K_\infty^1) \simeq \mathbb{Z}_p$. Consequently, the image of $X_1[T_1]$ has $\mathbb{Z}_p$-rank 1. We obtain the desired result by observing that $\mathrm{Gal}(K_\infty^1 K_\infty^2/K_\infty^1)$ is a quotient of $X_1/T_1X_1$. $\square$

Corollary 4.2.2 is not a very strong result, but it does have one interesting feature. This corollary gives some information about $T$-semisimplicity that is not tied to information about the decomposition subgroups for primes above $p$. We will make use of this in Example 6.2.6 to show that every $\mathbb{Z}_3$-extension of $\mathbb{Q}(\mu_3, \sqrt{7})$ is $T$-semisimple.

# Chapter 5

# THE FIRST LAYERS OF ANTI-CYCLOTOMIC EXTENSIONS

The goal of this chapter is to give a method for computing the first few layers of $\mathbb{Z}_3$-extensions of quadratic and biquadratic fields. We begin with a few useful lemmas.

**Lemma 5.0.1.** *Let $p$ be an odd prime and $K$ an imaginary quadratic field and let $q \neq p$ be a prime which is inert in $K/\mathbb{Q}$. Then $q$ splits completely in $K_\infty^{anti}/K$, the anti-cyclotomic $\mathbb{Z}_p$-extension of $K$.*

*Proof.* Let $K_n$ denote the $n$-th layer of $K_\infty^{anti}$. Then $\mathrm{Gal}(K_n/\mathbb{Q})$ is a dihedral group of order $2p^n$. Furthermore, $q$ is unramified in $K_n/\mathbb{Q}$ and inert in $K/\mathbb{Q}$ so the decomposition subgroup of a prime lying over $q$ is cyclic of even order. However, the only such subgroups of a dihedral group of order $2p^n$ have order exactly 2. It follows that $q$ splits completely in $K_n/K$ for each $n$ and thus in $K_\infty^{anti}/K$. □

**Lemma 5.0.2.** *Let $K$ be a number field containing $\mu_p$ and let $M/K$ be a cyclic extension of $K$ of degree $p$ which is unramified outside of $p$. Let $\mathcal{O}'_K = \mathcal{O}_K[\frac{1}{p}]$ and let $\mathcal{F}'_K$ denote the group of nonzero fractional ideals of $\mathcal{O}'_K$. Then $M = K(\sqrt[p]{\alpha})$ for some Kummer generator $\alpha$ satisfying $\alpha\mathcal{O}'_K = I^p$ for some fractional ideal $I \in \mathcal{F}'_K$ whose class in $\mathrm{Cl}(\mathcal{O}'_K)$ is either of order $p$ or trivial. In particular, if the class of $I$ is trivial, then $\alpha$ can be chosen to be a unit of $\mathcal{O}'_K$. Furthermore, every extension $K(\sqrt[p]{\alpha})$ with $\alpha$ of this form is unramified outside of $p$.*

*Proof.* First, suppose that $M/K$ is cycic degree $p$ extension which is unramified outside of $p$. By Kummer theory, we know that $M = K(\sqrt[p]{\alpha})$ for some $\alpha \in K^\times$. Note that $\sqrt[p]{\alpha}$ generates the same fractional ideal of $\mathcal{O}_M$ as each of its Galois conjugates, so is invariant under the action of $\mathrm{Gal}(M/K)$. Note also that if $\mathfrak{a}$ is an ideal which is invariant under the action of $\mathrm{Gal}(M/K)$ and divisible only by primes which are unramified in $M/K$, then $N_{M/K}(\mathfrak{a})$ is a

$p$-th power in $\mathcal{F}_K$. Thus, taking the norm down to $K$, we find that the fractional ideal of $\mathcal{O}'_K$ generated by $\alpha$ is a $p$-th power in $\mathcal{F}'_K$. That is, that

$$(\alpha) = I^p \qquad \text{some } I \in \mathcal{F}'_K.$$

Furthermore, because $I^p$ is principal, it must be the case that the class of $I$ in $\mathrm{Cl}(\mathcal{O}'_K)$ has order 1 or $p$. If $I = \beta^p(\mathcal{O}_K[\frac{1}{p}])$, then $\alpha/\beta^p$ is a $p$-unit whose $p$-th root generates the same Kummer extension.

Now, to see that every extension $K(\sqrt[p]{\alpha})$ with $\alpha$ as above is unramified outside of $p$, let us work locally. Let $\mathfrak{q}$ be a prime of $K$ which does not divide $p$ and let $K_\mathfrak{q}$ denote the completion of $K$ at $\mathfrak{q}$. Note that $\mathrm{ord}_\mathfrak{q}(\alpha) \equiv 0 \pmod{p}$. Thus, there exists $\eta \in \mathcal{O}_{K_\mathfrak{q}}^\times$ such that $K_\mathfrak{q}(\sqrt[p]{\alpha}) = K_\mathfrak{q}(\sqrt[p]{\eta})$. Note that the polynomial $x^p - \eta$ has no repeated roots over the residue field $\mathcal{O}_{K_\mathfrak{q}}/\mathfrak{q}$. It follows that $K_\mathfrak{q}(\sqrt[p]{\eta})/K_\mathfrak{q}$ is unramified and, hence, that $K(\sqrt[p]{\alpha})$ is unramified at $\mathfrak{q}$. □

**Example 5.0.3.** Let $K = \mathbb{Q}(\mu_p)$ and let $\omega$ denote the Teichmüller character. Let $K_1$ denote the first layer of the $\omega$-$\mathbb{Z}_p$-extension $K_\infty^\omega/K$. By Lemma 5.0.2, we have

$$K_1 = K(\sqrt[p]{\alpha})$$

where, in the notation of Lemma 5.0.2, $\alpha\mathcal{O}'_K = I^p$ for some fractional ideal $I \in \mathcal{F}'_K$. By Kummer theory, we have

$$\langle\alpha\rangle(K^\times)^p/(K^\times)^p \simeq \mathrm{Hom}(\mathrm{Gal}(K_1/K), \mu_p)$$

and the isomorphism is $\mathrm{Gal}(K/\mathbb{Q})$-equivariant. Because $\mathrm{Gal}(K/\mathbb{Q})$ acts on $\mathrm{Gal}(K_1/K)$ and $\mu_p$ by the same character, it follows that $\mathrm{Gal}(K/\mathbb{Q})$ acts trivially on $\langle\alpha\rangle(K^\times)^p/(K^\times)^p$. In particular, we see that we can take $\alpha \in \mathbb{Q}$. Because $K$ is a degree $p-1$ extension of $\mathbb{Q}$ and $K_1/K$ is not a trivial extension, we see that the class of $I$ must be trivial and, thus, that $\alpha$ is a $p$-unit of $\mathbb{Q}$. Since $K$ contains $\mu_p$, we may take $\alpha = p$:

$$K_1 = K(\sqrt[p]{p}).$$

## 5.1 The Anti-cyclotomic $\mathbb{Z}_3$-extension of $\mathbb{Q}(\mu_3)$

We construct the first three layers in the anticyclotomic tower as a tower of Kummer extensions by looking at the behavior of primes in this extension.

Let $K = \mathbb{Q}(\mu_3)$ and let $K_\infty/K$ denote the anticyclotomic $\mathbb{Z}_3$-extension of $K$. Let $q$ be a prime satisfying $q \equiv 2 \pmod 3$. Thus, by Lemma 5.0.1, $q$ splits completely in $K_\infty/K$. We have already seen that the first layer of $K_\infty/K$ is given by $K_1 = K(\sqrt[3]{3}) = \mathbb{Q}(\mu_3, \sqrt[3]{3})$. Note that $K = \mathbb{Q}(\mu_3)$ has class number 1 and has only one prime above 3. It follows that this prime must be totally ramified in $K_\infty/K$. Hence, by Proposition 2.5.1, the prime 3 does not divide the class number of any layer $K_n$. Consequently, $\mathrm{Cl}(\mathcal{O}'_{K_n})$ has no classes of order 3. Combining this with Lemma 5.0.2, we see that each successive layer in the $\mathbb{Z}_3$-extension is a Kummer extension of the form

$$K_{n+1} = K_n(\sqrt[3]{\alpha_n})$$

for some 3-unit $\alpha_n \in K_n^\times$.

The roots of unity of $K_1$ are precisely $\mu_6$. Let $\zeta_3$ denote a primitive third root of unity. The group of units of $K_1$ has rank 2 and the unique prime above 3 is principal. Thus, the subgroup of $K_1^\times/(K_1^\times)^3$ corresponding to degree 3 cyclic extensions of $K_1$ unramified outside of 3 has 3-rank 4. Using Sage, I found this subgroup to be generated by the cosets of the following four elements:

$$\begin{aligned} u_0 &= -\zeta_3 \\ u_1 &= \left(\frac{-2-\zeta_3}{3}\right)\alpha_1^2 - \alpha_1 - 1 \\ u_2 &= \left(\frac{1-\zeta_3}{3}\right)\alpha_1^2 + (-1-\zeta_3)\,\alpha_1 + \zeta_3 \\ \pi_1 &= \left(\frac{-2-\zeta_3}{3}\right)\alpha_1^2 \end{aligned}$$

(Here, $u_1$ and $u_2$ generate the free part of $\mathcal{O}_{K_1}^\times$ and $\pi_1$ generates the ideal above 3.) Note that there are $3^4 - 1 = 80$ nontrivial elements in $\langle u_0, u_1, u_2, \pi_1\rangle K_1^\times/(K_1^\times)^3$, but only $(3^4 - 1)/(3 - 1) = 40$ distinct subgroups of order 3. I looked at Kummer extensions for Kummer

generators of the form $\alpha_e = u_0^{e_0} u_1^{e_1} u_2^{e_2} \pi_1^{e_4}$ with $e = (e_0, e_1, e_2, e_3) \in \mathbb{P}^3(\mathbb{F}_3)$ and $e_i = 1$ for $i = \min\{j : e_j \neq 0\}$.

Rather than directly compute the splitting of primes in each of the possible Kummer extensions $K_1(\sqrt[3]{\alpha_e})$, I factored the reduction of the polynomial $x^3 - \alpha_e$ over each of the residue fields $K_1/\mathfrak{p}$ for primes $\mathfrak{p} \subseteq \mathcal{O}_{K_1}$ lying above 2. Of the 40 candidate Kummer generators $\alpha_e$, only one had the property that $x^3 - \alpha_e$ split into 3 primes over all three residue fields: $e = (1, 1, 1, 2)$. The minimal polynomial for this $\alpha_e$ is $x^3 + 9x^2 + 27x + 3$. Therefore, $K_2 = K(\beta_2)$, where $\beta_2$ is a root of $f_2(x) = x^9 + 9x^6 + 27x^3 + 3$. I confirmed this by checking that $f_2(x)$ factors into 9 linear terms over all residue fields $\mathcal{O}_K/(q)$ for all primes $q \equiv 2 \pmod 3$ up to 1000.

To compute $K_3$, we must consider 10 independent Kummer generators. These are listed in Figure 5.1. We thus need to check $(3^{10} - 1)/(3 - 1) = 29524$ different Kummer extensions. I found that $K_3 = K_2(\beta_3)$ where

$$\beta_3 = \sqrt[3]{u_0^1 \cdot u_1^1 \cdot u_2^1 \cdot u_3^2 \cdot u_4^1 \cdot u_5^2 \cdot u_6^0 \cdot u_7^1 \cdot u_8^1 \cdot \pi_2^1}$$

and that a polynomial for $K_3$ is given by

$$\begin{aligned} f_3(x) = x^{54} &- 459x^{48} + 1180413x^{42} + 32196753x^{36} + 473384979x^{30} + 4700376783x^{24} \\ &+ 33508681263x^{18} + 126530496171x^{12} + 181247124096x^6 + 192000000 \end{aligned}$$

Asking Sage for an index 2 subfield, one findes that $K_3$ is also the splitting field of

$$\begin{aligned} \tilde{f}_3(x) = x^{27} &- 27x^{24} + 324x^{21} - 1980x^{18} + 5022x^{15} \\ &+ 8262x^{12} - 30348x^9 - 304236x^6 + 1365417x^3 - 3 \end{aligned}$$

Note that the group of 3-units of $K_3$ has rank 27 and contains $\mu_3$ so, to compute compute $K_4$ using this methond, one would need to check $(3^{28} - 1)/(3 - 1) = 11438396227480$ Kummer generators.

### *5.2 The Anti-cyclotomic $\mathbb{Z}_3$-extension of $\mathbb{Q}(\sqrt{-3d})$ for $d \equiv 2 \pmod 3$*

Now let $F = \mathbb{Q}(\sqrt{-3d})$ where $d > 0$, $d \equiv 2 \pmod 3$, and $d$ is squarefree.

$$
\begin{aligned}
u_0 &= 1+\zeta \\
u_1 &= \left(\frac{1-\zeta}{12}\right)\beta^6 + \left(\frac{1}{2}\right)\beta^3 + \left(\frac{-1-\zeta}{4}\right) \\
u_2 &= \left(\frac{-1+\zeta}{12}\right)\beta^6 + \left(\frac{\zeta}{2}\right)\beta^3 + \left(\frac{-1-\zeta}{4}\right) \\
u_3 &= \left(\frac{2+\zeta}{6}\right)\beta^8 + \left(\frac{1-4\zeta}{12}\right)\beta^7 + \left(\frac{-1-2\zeta}{4}\right)\beta^6 + \left(\frac{13+5\zeta}{6}\right)\beta^5 + \left(\frac{-1-6\zeta}{2}\right)\beta^4 \\
&\quad + \left(\frac{-5-5\zeta}{2}\right)\beta^3 + \left(\frac{9+6\zeta}{2}\right)\beta^2 + \left(\frac{-5-20\zeta}{4}\right)\beta + \left(\frac{-5}{4}\right) \\
u_4 &= \left(\frac{2+\zeta}{6}\right)\beta^8 + \left(\frac{-5-4\zeta}{12}\right)\beta^7 + \left(\frac{2+\zeta}{4}\right)\beta^6 + \left(\frac{13+8\zeta}{6}\right)\beta^5 + \left(\frac{-5-6\zeta}{2}\right)\beta^4 \\
&\quad + \left(\frac{5+5\zeta}{2}\right)\beta^3 + \left(\frac{9+3\zeta}{2}\right)\beta^2 + \left(\frac{-15-20\zeta}{4}\right)\beta + \left(\frac{5\zeta}{4}\right) \\
u_5 &= \left(\frac{1-\zeta}{6}\right)\beta^8 + \left(\frac{-1-5\zeta}{12}\right)\beta^7 + \left(\frac{-2-\zeta}{4}\right)\beta^6 + \left(\frac{8-5\zeta}{6}\right)\beta^5 + \left(\frac{1-5\zeta}{2}\right)\beta^4 \\
&\quad + \left(\frac{-5-5\zeta}{2}\right)\beta^3 + \left(\frac{3-6\zeta}{2}\right)\beta^2 + \left(\frac{5-15\zeta}{4}\right)\beta + \left(\frac{-5\zeta}{4}\right) \\
u_6 &= \left(\frac{-8-13\zeta}{6}\right)\beta^8 + \left(\frac{-13-5\zeta}{12}\right)\beta^7 + \left(\frac{-1+\zeta}{4}\right)\beta^6 \\
&\quad + \left(\frac{-71-115\zeta}{6}\right)\beta^5 + \left(\frac{-19-7\zeta}{2}\right)\beta^4 + \left(\frac{-4+5\zeta}{2}\right)\beta^3 \\
&\quad + \left(\frac{-69-112\zeta}{2}\right)\beta^2 + \left(\frac{-107-39\zeta}{4}\right)\beta + \left(\frac{-19+33\zeta}{4}\right) \\
u_7 &= \left(\frac{-1}{2}\right)\beta^8 + \left(\frac{1+\zeta}{4}\right)\beta^7 + \left(\frac{-2-\zeta}{3}\right)\beta^6 + \left(\frac{-10+\zeta}{3}\right)\beta^5 + \left(\frac{1+4\zeta}{2}\right)\beta^4 \\
&\quad + (-3-3\zeta)\beta^3 + \left(\frac{-15+8\zeta}{2}\right)\beta^2 + \left(\frac{-11+3\zeta}{4}\right)\beta + (\zeta) \\
u_8 &= \left(\frac{1+2\zeta}{12}\right)\beta^8 + \left(\frac{1}{4}\right)\beta^7 + \left(\frac{1-\zeta}{4}\right)\beta^6 + \left(\frac{1+2\zeta}{3}\right)\beta^5 + (1-\zeta)\beta^4 \\
&\quad + (-2\zeta)\beta^3 + \left(\frac{-7+2\zeta}{4}\right)\beta^2 + \left(\frac{3-4\zeta}{4}\right)\beta + \left(\frac{3+\zeta}{4}\right) \\
\pi_2 &= \left(\frac{1+2\zeta}{12}\right)\beta^8 + \left(\frac{2+4\zeta}{3}\right)\beta^5 + \left(\frac{9+14\zeta}{4}\right)\beta^2
\end{aligned}
$$

Figure 5.1: The 10 independent Kummer generators used to compute the third layer of the anti-cyclotomic $\mathbb{Z}_3$-extension of $\mathbb{Q}(\mu_3)$. In each expression, $\zeta = \zeta_3$ and $\beta = \beta_2$.

As in the case of the anti-cyclotomic extension of $\mathbb{Q}(\mu_3)$, our strategy for computing layers of $F_\infty^{anti}/F$ will be to consider many different Kummer extensions and use knowledge about the splitting of primes in $F_\infty^{anti}/F$ to identify the Kummer extension corresponding to $F_n$. Of course, $F$ does not contain $\mu_3$ so we will instead work with Kummer extensions of the biquadratic field $K = F(\mu_3)$.

We are particularly interested in computing the layers of $F_\infty^{anti}$ when the Iwasawa module has a chance of being nontrivial. There is only one prime above 3 in $F = \mathbb{Q}(\sqrt{-3d})$ so, as we saw in Example 2.5.3, the Iwasawa module is trivial if $F_\infty^{anti}$ contains the 3-Hilbert class field of $F$. It turns out this can be determined by studying the class group of the real quadratic field $\mathbb{Q}(\sqrt{d})$.

It has long been known that the class groups of $\mathbb{Q}(\sqrt{-3d})$ and $\mathbb{Q}(\sqrt{d})$ are related.

**Lemma 5.2.1** (Scholz Reflection Principle)**.** *Let $d > 1$ be squarefree. Let $r_+$ denote the 3-rank of the real quadratic field $\mathbb{Q}(\sqrt{d})$ and let $r_-$ denote the 3-rank of the imaginary quadratic field $\mathbb{Q}(\sqrt{-3})$. Then*

$$r_+ \leq r_- \leq r_+ + 1.$$

See Theorem 10.10 of [26] for a proof.

**Lemma 5.2.2.** *Let $d > 0$ such that $d \equiv 2 \pmod 3$ and 3 does not divide the class number of $\mathbb{Q}(\sqrt{d})$. Let $F$ denote the imaginary quadratic field $F = \mathbb{Q}(\sqrt{-3d})$. Then the 3-Hilbert class field of $F$ is contained in $F_\infty^{anti}$ and the first layer of $F_\infty^{anti}/F$ is the unique index 2 subfield of*

$$\mathbb{Q}(\mu_3, \sqrt{d}, \sqrt[3]{\epsilon})$$

*containing $F$, where $\epsilon$ denotes the fundamental unit of $\mathbb{Q}(\sqrt{d})$.*

*Proof.* Let $\mathfrak{p}$ denote the unique prime lying above 3 in $F$. The idea of the proof is to show that the minus part of the ray class group for modulus $\mathfrak{p}^n$ is cyclic for all $n$.

Let us first introduce some notation. For any modulus $\mathbf{m} = \mathfrak{q}_1^{k_1} \cdots \mathfrak{q}_m^{k_m}$ of $F$, let $F_{\mathbf{m}} \subseteq F^\times$ denote the subgroup consisting of elements supported outside of $\mathbf{m}$:

$$F_{\mathbf{m}} = \left\{ \alpha \in F^\times : \mathrm{ord}_{\mathfrak{q}}(\alpha) = 0 \text{ for all finite } \mathfrak{q}_i | \mathbf{m} \right\},$$

and let $F_{\mathbf{m},1} \subseteq F_{\mathbf{m}}$ denote the subgroup consisting of elements $\alpha$ which are positive at all the real places of $\mathbf{m}$ and satisfy

$$\mathrm{ord}_{\mathfrak{q}_i}(\alpha - 1) \geq k_i$$

for all finite primes $\mathfrak{q}_i$ dividing $\mathbf{m}$. Let $\mathcal{U}_{F,1} = \mathcal{O}_F^\times \cap F_{\mathbf{m},1}$. Then $C_{\mathbf{m}}$, the ray class group of $F$ with modulus $\mathbf{m}$, fits into an exact sequence

$$1 \to \frac{\mathcal{O}_F^\times}{\mathcal{U}_{F,1}} \to \frac{F_{\mathbf{m}}}{F_{\mathbf{m},1}} \to C_{\mathbf{m}} \to \mathrm{Cl}(F) \to 1.$$

See Theorem 1.7 in Chapter 5 of [23] for a proof. Because $F$ is an imaginary quadratic field which does not contain the cube roots of unity, the left-most term in the sequence is of order 1 or 2.

Now, let $M_\infty^-$ denote the maximal abelian pro-3 extension of $F$ which is unramified outside of 3 and such that complex conjugation acts nontrivially on $\mathrm{Gal}(M_\infty^-/F)$. Let $I_{\mathfrak{p}}(M_\infty^-)$ denote the inertia subgroup for $\mathrm{Gal}(M_\infty^-/F)$. Then, working with the exact sequence above, we obtain the following commutative diagram:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \varprojlim \left( \dfrac{F_{\mathfrak{p}^k}}{F_{\mathfrak{p}^k,1}}[3^\infty] \right)^- & \longrightarrow & \varprojlim \left( C_{\mathfrak{p}^k}[3^\infty] \right)^- & \longrightarrow & A_0 & \longrightarrow & 0 \\
 & & & & \downarrow \cong & & \downarrow \cong & & \\
0 & \longrightarrow & I_{\mathfrak{p}}(M_\infty^-) & \longrightarrow & \mathrm{Gal}(M_\infty^-/F) & \longrightarrow & \mathrm{Gal}(L_0/F) & \longrightarrow & 0
\end{array}$$

where the rows are exact the the isomorphisms are given by the Artin map. Now the quotient $\mathrm{Gal}(M_\infty^-/F)/\mathrm{Gal}(M_\infty^-/F)^3$ is isomporphic to the Galois group of the compositum of all cubic extensions of $F$ contained in $M_\infty^-$. These are in one-to-one correspondence with cubic extensions of $K = F(\mu_3)$ contained in $M_\infty^-(\mu_3)$.

Suppose that $K(\sqrt[3]{\alpha})/K$ is one such extension. Note that complex conjugation acts nontrivially on both $\mathrm{Gal}(K(\sqrt[3]{\alpha})/K)$ and $\mu_3$ while $\mathrm{Gal}(K/F)$ acts trivially on $\mathrm{Gal}(K(\sqrt[3]{\alpha})/K)$ but nontrivially on $\mu_3$. It follows that $\mathrm{Gal}(K/\mathbb{Q})$ acts on

$$\mathrm{Hom}(\mathrm{Gal}(K(\sqrt[3]{\alpha})/K), \mu_3)$$

by the nontrivial even character of $\mathrm{Gal}(K/\mathbb{Q})$. It follows from Kummer theory that $\alpha$ can be chosen to be an element of the real quadratic field $\mathbb{Q}(\sqrt{d})$, $\alpha \notin \mathbb{Q}$. But then, by Lemma 5.0.2 and our assumption that 3 does not divide the class number of $\mathbb{Q}(\sqrt{d})$, we see that $\alpha$ must be one of $\epsilon$ or $\epsilon^2$. As these generate the same extension, it follows that

$$\mathrm{Gal}(M_\infty^-(\mu_3)/K)/\mathrm{Gal}(M_\infty^-(\mu_3)/K)^3 \simeq \mathrm{Gal}(K(\sqrt[3]{\epsilon})/K) \simeq \mathbb{Z}/3\mathbb{Z}.$$

In particular, this implies that $\mathrm{Gal}(M_\infty^-/F)$ is pro-cyclic and, thus, that $M_\infty^- = F_\infty^{anti}$ and $L_0 \subseteq F_\infty^{anti}$. □

Let us now consider the case where 3 divides the class number of $\mathbb{Q}(\sqrt{d})$. In this case, there are multiple cubic extensions of $F$ which are unramified outside of 3 and on whose Galois groups $\mathrm{Gal}(F/\mathbb{Q})$ acts nontrivially. Therefore, Lemma 5.0.1 is no longer sufficient to determine the anti-cyclotomic extension by itself. Now we must also consider the splitting behavior of primes which split in $F/\mathbb{Q}$.

**Proposition 5.2.3.** *Let $F = \mathbb{Q}(\sqrt{-3d})$, with $d > 0$, $d \equiv 2 \pmod 3$, and $d$ squarefree. Let $q$ be a prime which splits in $F/\mathbb{Q}$ and let $\mathfrak{q}$ be a prime of $F$ lying above $q$. Let $h_\mathfrak{q}$ denote the order of the class of $\mathfrak{q}$, let $\alpha_q$ be generator for the principal ideal $\mathfrak{q}^{h_\mathfrak{q}}$, and set*

$$\beta_q = \left(\alpha_q/\overline{\alpha_q}\right)^2.$$

*Let $n_0$ be such that $F_{n_0} = L_0 \cap F_\infty^{anti}$ and let $b_q$ be given by*

$$b_q = \frac{\mathrm{ord}_\mathfrak{p}\left(\beta_q - 1\right) - 1}{2}.$$

*Then the decomposition field of $\mathfrak{q}$ in $F_\infty^{anti}/F$ is $F_{n_q}$ where*

$$n_q = b_q + n_0 - \mathrm{ord}_3(h_q).$$

*Proof.* Note that $\mathfrak{q}$ is unramified in $F_\infty^{anti}/F$. Therefore, the decomposition subgroup for $\mathfrak{q}$ in $\Gamma = \mathrm{Gal}(F_\infty^{anti}/F)$ is topologically generated by the Frobenius automorphism $\mathrm{Frob}_\mathfrak{q}$. We will show that $3^{b_q}$ is the index of $\overline{\langle \mathrm{Frob}_\mathfrak{q}^{h_q} \rangle}$ in $I_\mathfrak{p}(F_\infty^{anti})$, the inertia subgroup for $\mathfrak{p}$ in $\Gamma$. It

will then follow that $3^{b_q+n_0}$ is the index of $\overline{\langle \mathrm{Frob}_{\mathfrak{q}}^{h_q} \rangle}$ in $\Gamma$ and, thus, that $3^{b_q+n_0-\mathrm{ord}_3(h_q)}$ is the index the decomposition subgroup for $\mathfrak{q}$ in $\Gamma$

Let $M_\infty^-$ denote the maximal abelian pro-3 extension of $F$ which is unramified outside of 3 and such that complex conjugation acts nontrivially on $\mathrm{Gal}(M_\infty^-/F)$. Note that $M_\infty^-$ is a finite extension of $F_\infty^{anti}$. Let $I_{\mathfrak{p}}(M_\infty^-)$ denote the inertial subgroup for $\mathfrak{p}$ in $\mathrm{Gal}(M_\infty^-/F)$. Just as in the proof of Lemma 5.2.2, we have the following commutative diagram whose rows are exact:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \varprojlim \left( \dfrac{F_{\mathfrak{p}^n}}{F_{\mathfrak{p}^n,1}}[3^\infty] \right)^- & \longrightarrow & \varprojlim \left( C_{\mathfrak{p}^k}[3^\infty] \right)^- & \longrightarrow & A_0 & \longrightarrow & 0 \\ & & & & \downarrow \cong & & \downarrow \cong & & \\ 0 & \longrightarrow & I_{\mathfrak{p}}(M_\infty^-) & \longrightarrow & \mathrm{Gal}(M_\infty^-/F) & \longrightarrow & \mathrm{Gal}(L_0/F) & \longrightarrow & 0 \end{array}$$

where the isomorphisms are given by the Artin map. We thus have an isomorphism

$$\varprojlim \left( \frac{F_{\mathfrak{p}^n}}{F_{\mathfrak{p}^n,1}}[3^\infty] \right)^- \xrightarrow{\simeq} I_{\mathfrak{p}}(M_\infty^-).$$

Let $\mathcal{O}_{F_{\mathfrak{p}}}$ denote the ring of integers of the completion of $F$ at $\mathfrak{p}$. Then

$$\varprojlim \left( \frac{F_{\mathfrak{p}^n}}{F_{\mathfrak{p}^n,1}}[3^\infty] \right)^- \simeq \left( \left( \mathcal{O}_{F_{\mathfrak{p}}}^\times \right)^2 \right)^- \simeq (1+\mathfrak{p})^-,$$

where now $\mathfrak{p}$ denotes the maximal ideal of $\mathcal{O}_{F_{\mathfrak{p}}}$ and $(1+\mathfrak{p})^-$ denotes the subgroup of $1+\mathfrak{p}$ on which $\mathrm{Gal}(F_{\mathfrak{p}}/\mathbb{Q}_3)$ acts nontrivially.

Let us now determine the image of $\beta_q$ in $I_{\mathfrak{p}}(M_\infty^-) \subseteq \mathrm{Gal}(M_\infty^-/F)$. Note that $\beta_q = (\alpha_q/\overline{\alpha_q})^2$ is sent to the class of $\left( \mathfrak{q}^{h_q}/\overline{\mathfrak{q}^{h_q}} \right)^2$ in $\varprojlim \left( C_{\mathfrak{p}^k}[3^\infty] \right)^-$. But $\mathfrak{q}\overline{\mathfrak{q}} = (q)$ is principal so $\beta_q$ is sent to the class of $\mathfrak{q}^{4h_q}$. Therefore, we see that the subgroup of $\varprojlim \left( \frac{F_{\mathfrak{p}^n}}{F_{\mathfrak{p}^n,1}}[3^\infty] \right)^-$ generated by $\beta_q$ maps isomorphically to the subgroup of $I_{\mathfrak{p}}(M_\infty^-)$ generated by $\mathrm{Frob}_{\mathfrak{q}}^{4h_q}$. Since $I_{\mathfrak{p}}(M_\infty^-)$ is a pro-3 group, this is the same as the subgroup generated by $\mathrm{Frob}_{\mathfrak{p}}^{h_q}$.

Let us now compute the index of the closed subgroup generated by $\beta_q$ in $(1+\mathfrak{p})^-$. Note that $(1+\mathfrak{p})^- \simeq \mathbb{Z}_3$. We begin by showing that, for each $a$, the unique index $3^a$ subgroup of $(1+\mathfrak{p})^-$ is given by

$$(1+\mathfrak{p})^- \cap (1+\mathfrak{p}^{1+2a}).$$

Let $\pi = \sqrt{-3d}$, a uniformizer for $\mathcal{O}_{F_\mathfrak{p}}$. Then every element of $1+\mathfrak{p}$ can be written as $1+u\pi^k$ for some $k \geq 1$ and $u \in \mathcal{O}_{F_\mathfrak{p}}^\times$. Futhermore, one can write $u = x + y\pi$ for $x, y \in \mathbb{Z}_3$ where $x \notin \mathfrak{p}$. Suppose $1 + (x+y\pi)\pi^k$ is in $(1+\mathfrak{p})^-$. Then, conjugating $1 + x\pi^k + y\pi^{k+1}$, we must have

$$1 + x(-\pi)^k + y(-\pi)^{k+1} = \frac{1}{1 + x\pi^k + y\pi^{k+1}}.$$

Rearranging, we obtain

$$(1+(-1)^k)x + (1+(-1)^{k+1})y\pi + (-1)^k x^2\pi^k + (-1)^{k+1}y^2\pi^{k+2} = 0.$$

If $k$ is even, we find that $2x = -x^2\pi^k + y^2\pi^{k+2} \in \mathfrak{p}$, a contradiction. We conclude that for each element in $\eta \in (1+\mathfrak{p})^-$, there exists an odd $k \geq 1$ such that $\eta \in 1+\mathfrak{p}^k$ but $\eta \notin 1+\mathfrak{p}^{k+1}$ for some odd $k$. Conversely, suppose $k \geq 1$ is odd. Set

$$\eta = \frac{1+\pi^k}{1-\pi^k} = \frac{(1+\pi^k)^2}{1-\pi^{2k}}.$$

Note that $(1-\pi^{2k})^{-1} \in 1+\mathfrak{p}^{2k}$ and $(1+\pi^k)^2 \in 1+\mathfrak{p}^k$ but $(1+\pi^k)^2 \notin 1+\mathfrak{p}^{k+1}$. Therefore, $\eta \in 1+\mathfrak{p}^k$ but $\eta \notin 1+\mathfrak{p}^{k+1}$. Thus, for each odd $k \geq 1$, there exists $\eta \in (1+\mathfrak{p})^-$ such that $\eta \in 1+\mathfrak{p}^k$ but $\eta \notin 1+\mathfrak{p}^{k+1}$. Note further that, for each $a \geq 1$, $(1+\mathfrak{p})^{3a} \subseteq (1+\mathfrak{p}^{1+2a})$.

Thus, for each $a$, the unique index $3^a$ subgroup of $(1+\mathfrak{p})^-$ is given by

$$(1+\mathfrak{p})^- \cap (1+\mathfrak{p}^{1+2a}).$$

In particular, it follows that the closed subgroup generated by $\beta_q$ has index $3^{b_q}$ where

$$b_q = \frac{\mathrm{ord}_\mathfrak{p}(\beta_q - 1) - 1}{2}.$$

Consequently, $\overline{\langle \mathrm{Frob}_\mathfrak{q}^{h_q} \rangle}$ generates an index $3^{b_q}$ subgroup of $I_\mathfrak{p}(M_\infty^-)$.

Finally, note that the quotient map $\mathrm{Gal}(M_\infty^-/F) \to \Gamma$ gives rise to an isomorphism $I_\mathfrak{p}(M_\infty^-) \to I_\mathfrak{p}(F_\infty^{anti})$, both of which are isomorphic to $\mathbb{Z}_p$. It follows that $\overline{\langle \mathrm{Frob}_\mathfrak{q}^{h_q} \rangle}$ has index $3^{b_q}$ in $I_\mathfrak{p}(F_\infty^{anti})$, as desired. $\square$

Of course, in order to use Proposition 5.2.3, one must be able to determine $n_0$. This can be done experimentally: by the Chebotarev density theorem, two thirds of the primes $\mathfrak{q}$ are inert in $F_1/F$ and thus in $F_\infty^{anti}/F$. Thus, one has

$$n_0 = \min\Big\{ \operatorname{ord}_3(h_q) - b_q : q \text{ split in } F/\mathbb{Q} \Big\}.$$

This minimum value can be attained by looking at a large enough set of primes and checking the result against the candidate fields $F_1$. For example, in my calculations, I looked at all $q \leq 200$ to determine $n_0$.

It is sometimes possible to determine $n_0$ without any additional calculations. For example, we will show in Proposition 6.3.2 that if $A_0 \simeq \mathbb{Z}/3\mathbb{Z}$, then $n_0 = 0$.

**Example 5.2.4.** Let $F = \mathbb{Q}(\sqrt{-3 \cdot 254})$. In [3], Candiotti showed that the first layer of $F_\infty^{anti}/F$ is a subfield of $F(\mu_3, \sqrt[3]{\epsilon})$, where $\epsilon = 255 + 16\sqrt{254}$ is the fundamental unit of $F$. In this example, we will illustrate how to Proposition 5.2.3 by verifying Candiotti's calculation and then we will go on to calculate the second layer of $F_\infty^{anti}/F$. The 3-part of the ideal class group of $\mathbb{Q}(\sqrt{254})$ is cyclic of order 3 and is generated by the class of the ideal $(5, 3+\sqrt{254})$, whose cube is the principal ideal $(-111 - 7\sqrt{254})$.

The prime $q = 7$ splits in $F$. One of its factors is the prime ideal $\mathfrak{q} = (7, 1+\alpha)$, which generates a class of order 6 in $\mathrm{Cl}(F)$. Raising $P_7$ to the 6-th power, we obtain the principal ideal $\mathfrak{q}^6 = (89 + 12\alpha)$. We project onto the minus part by dividing the generator by its conjugate. And, squaring gives an element which is congruent to 1 modulo $\mathfrak{p}$:

$$\left(\frac{89+12\alpha}{89-12\alpha}\right)^2 = \frac{6888043297 - 434919504\alpha}{13841287201} \overset{call}{=} \beta_7$$

One finds that

$$\beta_7 \equiv 1 \pmod{\mathfrak{p}^3} \quad \text{but} \quad \beta_7 \not\equiv 1 \pmod{\mathfrak{p}^4}.$$

One way to see this is to note that the norm of $\beta_7 - 1$ is

$$N_{F/\mathbb{Q}}(\beta_7 - 1) = \frac{13906487808}{13841287201} = 2^9 \cdot 3^3 \cdot 7^{-12} \cdot 89^2 \cdot 127.$$

(though, in practice, I simply had Sage compute the valuation of $\beta_7 - 1$ with respect to $\mathfrak{p}$). Note that

$$(1+\mathfrak{p})^3 \subseteq 1+\mathfrak{p}^3.$$

Because the map $F_{\mathfrak{m}}/F_{\mathfrak{m},1} \to C_{\mathfrak{m}}$ is injective on the 3-part, we conclude that the prime above 7 is inert in $F_1/F$, and thus in $F_\infty/F$.

The prime $q = 47$ also splits in $F$. One of its factors is the prime ideal $\mathfrak{q} = (47, 15+\alpha)$, which generates a class of order 6 in $\mathrm{Cl}(F)$. Raising $\mathfrak{q}$ to the 6-th power, we obtain the principal ideal $\mathfrak{q}^6 = (42101 - 3438\alpha)$. Similarly to what we did above, let us consider the element

$$\beta_{47} = \left(\frac{42101 - 3438\alpha}{42101 + 3438\alpha}\right)^2 = \frac{-11523404646284851583 + 4188421719363078504\alpha}{116191483108948578241}.$$

In this case, one finds that

$$\beta_{47} \equiv 1 \pmod{\mathfrak{p}^5} \quad \text{but} \quad \beta_{47} \not\equiv 1 \pmod{\mathfrak{p}^6}.$$

We conclude that the primes above 47 split in $F_1/F$, but the primes above these then remain inert in $F_\infty/F_1$.

The same process can be performed for any prime which splits in $F/\mathbb{Q}$. Table 5.1 shows the results for all primes $2 < q \leq 200$ which split in $F/\mathbb{Q}$.

Working with the field $K = F(\mu_3)$, we can make use of Lemma 5.0.2. Let $\kappa$ denote the element $\kappa = -111 - 7\sqrt{254}$ so that $(\kappa)$ is the cube of a nonprincipal ideal. Then $F_1(\mu_3) = K(\sqrt[3]{\alpha_{(i,j)}})$ for some $\alpha_{(i,j)} = \epsilon^i\kappa^j$, which can be determined from the splitting behavior of primes in $F_1/F$. To do this, we factor the polynomial $t^3 - \alpha_{(i,j)}$ over the residue fields for a choice of prime $\mathfrak{q}$ lying over $q$. The results are gathered in Table 5.2, where we see that $F_1$ is the unique index-2 subfield of $K(\sqrt[3]{\epsilon})$ containing $F$.

Factoring $x^2 - (-3 \cdot 254)$ over all the index-2 subfields of $K(\sqrt[3]{\epsilon})$ in Sage, we find that $F_1$ is the splitting field of the polynomial

$$x^6 + 6x^5 + 327x^4 - 7052x^3 + 110991x^2 - 1492410x + 16133737.$$

| $q$ | $\lvert\mathrm{cl}(\mathfrak{q})\rvert$ | $\mathrm{ord}_{\mathfrak{p}}(\beta_q)$ | decomposition field | $q$ | $\lvert\mathrm{cl}(\mathfrak{q})\rvert$ | $\mathrm{ord}_{\mathfrak{p}}(\beta_q)$ | decomposition field |
|---|---|---|---|---|---|---|---|
| 7 | 6 | 3 | $F_0$ | 109 | 6 | 3 | $F_0$ |
| 19 | 3 | 3 | $F_0$ | 137 | 6 | 7 | $F_2$ |
| 47 | 6 | 5 | $F_1$ | 149 | 6 | 3 | $F_0$ |
| 59 | 6 | 5 | $F_1$ | 151 | 2 | 1 | $F_0$ |
| 71 | 6 | 3 | $F_0$ | 163 | 3 | 7 | $F_2$ |
| 73 | 3 | 5 | $F_1$ | 181 | 2 | 3 | $F_1$ |
| 83 | 6 | 3 | $F_0$ | 191 | 6 | 3 | $F_0$ |
| 89 | 6 | 3 | $F_0$ | 197 | 6 | 9 | $F_3$ |

Table 5.1: Predicted splitting behavior in the anticyclotomic extension of the imaginary quadratic field $F = \mathbb{Q}(\sqrt{-3 \cdot 254})$ of the primes $2 < q \leq 200$ which split in $F$.

Using the Sage optimized_representation command, we find that $F_1$ is also the splitting field of the polynomial

$$x^6 - 36x^4 + 324x^2 + 109728.$$

To find a polynomial for $F_2$, we work with Kummer extensions of $K_1 = F_1(\mu_3)$. There are of course many more Kummer extensions to consider now: The units group of $K_1$ has rank 5 and contains $\mu_3$. This gives us six Kummer generators. Computing the class group of $K_1$, we find that

$$\mathrm{Cl}(K_1) \simeq \mathbb{Z}/18\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}.$$

In particular, the 3-rank is 4, giving four additional Kummer generators. The prime lying $\mathfrak{P}$ lying above 3 in $K_1$ is not principal. In fact, its class has order 3 in $\mathrm{Cl}(K_1)$ and is the cube of an ideal $\mathfrak{a}$. Thus, we obtain two new Kummer generators from $\mathfrak{P}^3$ and $\mathfrak{P}/\mathfrak{a}$ for a total of $6 + 4 + 2 = 12$ Kummer generators. These Kummer generators are not all independent, but Lemma 5.0.2 tells us that we can choose a Kummer generator for $K_2 = F_2(\mu_3)$ that is a product of them.

| $q$ | factors of $f_{(1,0)}$ | factors of $f_{(1,1)}$ | factors of $f_{(1,2)}$ | factors of $f_{(0,1)}$ | Prediction |
|---|---|---|---|---|---|
| 7 | 1 | 1 | 1 | 3 | 1 (inert) |
| 19 | 1 | 3 | 1 | 1 | 1 (inert) |
| 47 | 3 | 1 | 1 | 1 | 3 (split) |
| 59 | 3 | 1 | 1 | 1 | 3 (split) |
| 71 | 1 | 1 | 1 | 3 | 1 (inert) |
| 73 | 3 | 1 | 1 | 1 | 3 (split) |
| 83 | 1 | 3 | 1 | 1 | 1 (inert) |
| 89 | 1 | 3 | 1 | 1 | 1 (inert) |
| 109 | 1 | 3 | 1 | 1 | 1 (inert) |
| 137 | 3 | 1 | 1 | 1 | 3 (split) |
| 149 | 1 | 1 | 1 | 3 | 1 (inert) |
| 151 | 1 | 1 | 3 | 1 | 1 (inert) |
| 163 | 3 | 1 | 1 | 1 | 3 (split) |
| 181 | 3 | 3 | 3 | 3 | 3 (split) |
| 191 | 1 | 3 | 1 | 1 | 1 (inert) |
| 197 | 3 | 1 | 1 | 1 | 3 (split) |

Table 5.2: Comparison of the splitting behavior of primes in the four candidates for the first layer of the anti-cyclotomic $\mathbb{Z}_3$-extension of $F = \mathbb{Q}(\sqrt{-3 \cdot 254})$. Compare with Table 5.1.

Using Lemma 5.0.1, I was able to narrow down the set of $(3^{12}-1)/(3-1) = 265720$ candidate Kummer generators to just 13 having the property that the primes which are inert in $F/\mathbb{Q}$ split completely in $K_2/K_1$. Using Proposition 5.2.3, I was able to restrict this further to 3 Kummer generators such that the splitting of such that the corresponding Kummer extension was compatible with Table 5.1.

Finally, aware that our 12 starting Kummer generators were not independent, I had Sage check that the final three candidate Kummer generators generated the same extension.

A similar process was used to determine a polynomial for $F_1$ for all values $1 < d \leq 1250$ such that $d \equiv 2 \pmod 3$, $d$ is squarefree, and 3 divides the class number of the real quadratic field $\mathbb{Q}(\sqrt{d})$. The resulting polynomials are listed in Table 5.3. In each case, the splitting behavior was determined for all primes up to 200. For convenience, a single prime whose splitting behavior should allow one to distinguish the first layer of the anti-cyclotomic $\mathbb{Z}_3$-extension of $\mathbb{Q}(\sqrt{-3d})$ is listed.

For some of these, a polynomial for $F_2$ was also determined. These polynomials are given in Table 5.4. The values of $d$ in Table 5.4 correspond to those for which one cannot determine the Iwasawa module using just $F_1$. See Section 6.3 (in particular Table 6.5) for more details.

| $d$ | $\alpha = \epsilon$ | polynomial for $F_1$ | prime to check |
|---|---|---|---|
| 254 | yes | $x^6 - 36x^4 + 324x^2 + 109728$ | 47 |
| 257 | no | $x^6 - 3x^5 + 72x^4 - 139x^3 + 1569x^2 - 1500x + 7900$ | 5 |
| 326 | no | $x^6 + 126x^4 + 3969x^2 + 140832$ | 7 |
| 359 | no | $x^6 - 90x^4 + 2025x^2 + 38772$ | 11 |
| 443 | no | $x^6 + 198x^4 + 9801x^2 + 191376$ | 19 |
| 473 | yes | $x^6 - 3x^5 + 168x^4 + 391x^3 + 5931x^2 + 52632x + 103372$ | 31 |
| 506 | no | $x^6 + 126x^4 + 3969x^2 + 218592$ | 13 |
| 659 | no | $x^6 - 20x^4 - 114x^3 + 2077x^2 - 10722x + 21042$ | 73 |
| 761 | no | $x^6 - 3x^5 + 270x^4 - 535x^3 + 9597x^2 - 9330x + 87964$ | 37 |
| 785 | yes | $x^6 + 18x^4 + 81x^2 + 84780$ | 7 |
| 839 | no | $x^6 - 90x^4 + 2025x^2 + 362448$ | 17 |
| 842 | no | $x^6 - 126x^4 + 3969x^2 + 818424$ | 71 |
| 899 | yes | $x^6 - 18x^4 + 81x^2 + 97092$ | 73 |
| 1091 | no | $x^6 - 2x^5 - 85x^4 + 166x^3 + 5042x^2 - 29624x + 53968$ | 73 |
| 1211 | no | $x^6 + 180x^4 + 8100x^2 + 523152$ | 31 |
| 1223 | no | $x^6 + 48x^4 - 1758x^3 + 33597x^2 - 240318x + 1069830$ | 13 |
| 1229 | no | $x^6 + 111x^4 - 768x^3 + 11376x^2 - 42624x + 147456$ | 23 |

Table 5.3: Polynomials defining $F_1$ for the anti-cyclotomic extension of $F = \mathbb{Q}(\sqrt{-3d})$. In each case, the splitting behavior was determined for all primes up to 200. For convenience, a single prime whose splitting behavior should allow one to distinguish the first layer of the anti-cyclotomic $\mathbb{Z}_3$-extension of $\mathbb{Q}(\sqrt{-3d})$ is listed.

| $d$ | polynomial for $F_2$ |
|---|---|
| 254 | $x^{18} - 54x^{16} - 300x^{15} + 2835x^{14} - 6300x^{13} + 45876x^{12} + 552600x^{11}$ $+ 4295115x^{10} + 21941464x^9 + 321839946x^8 + 1224491364x^7$ $+ 10852733325x^6 + 45697528404x^5 + 133798898664x^4 + 271328605296x^3$ $+ 497740810068x^2 + 476120870064x + 309895670416$ |
| 443 | $x^{18} - 144x^{16} + 13554x^{14} - 265536x^{12} - 29052567x^{10} + 3918571344x^8$ $- 163064159964x^6 + 3818111955840x^4 - 4150807649280x^2$ $+ 153834899963904$ |
| 473 | $x^{18} + 54x^{16} - 6x^{15} + 351x^{14} - 6228x^{13} + 31995x^{12} - 101826x^{11} + 1535787x^{10}$ $- 4898516x^9 + 14551803x^8 - 57723390x^7 + 356653506x^6 - 1148793264x^5$ $+ 2376972909x^4 - 3022987224x^3 + 2489628276x^2 - 1065458592x$ $+ 173534416$ |
| 659 | $x^{18} - 12x^{17} - 36x^{16} + 730x^{15} + 2985x^{14} - 52818x^{13} + 53862x^{12} + 1743552x^{11}$ $- 7879152x^{10} - 20922608x^9 + 302236464x^8 - 1234402656x^7$ $+ 2890317520x^6 - 4548925728x^5 + 5523976800x^4 - 7058516736x^3$ $+ 10305667968x^2 - 9390251520x + 3708441600$ |
| 899 | $x^{18} + 234x^{16} - 480x^{15} + 26199x^{14} - 4176x^{13} + 1766388x^{12} + 4096224x^{11}$ $+ 75308499x^{10} + 159107952x^9 + 3211183818x^8 + 9925749936x^7$ $+ 50762482209x^6 - 42511476672x^5 + 714157328664x^4 - 1360154256048x^3$ $+ 3961074336948x^2 - 23051775350880x + 31103030260800$ |
| 1091 | $x^{18} - 294x^{16} - 2230x^{15} + 18606x^{14} + 407022x^{13} + 3176736x^{12} + 15081678x^{11}$ $+ 49590897x^{10} + 108537338x^9 + 59581662x^8 - 711760560x^7 - 3572443496x^6$ $- 9642908544x^5 - 14151100320x^4 + 12232263936x^3 + 123908415360x^2$ $+ 244560563712x + 185981862912$ |
| 1211 | $x^{18} - 36x^{16} - 2808x^{15} - 4266x^{14} + 490392x^{13} + 6529488x^{12} + 82760544x^{11}$ $+ 992742273x^{10} + 8620667224x^9 + 65842602516x^8 + 489438005400x^7$ $+ 3014356889016x^6 + 13785224883120x^5 + 44919744967008x^4$ $+ 95621203710048x^3 + 110176776845136x^2 + 38519579181888x$ $+ 21150525422656$ |

Table 5.4: Polynomials giving the second layer of the anticyclotomic extension of $\mathbb{Q}(\sqrt{-3d})$.

# Chapter 6
# CLASS GROUP COMPUTATIONS

We recall the following disclaimer from the introduction: In order to perform the computations in a feasible amount of time, we often made use of algorithms whose validity rests on unproven conjectures (in particular the generalized Riemann hypothesis). In theory, given a sufficiently powerful machine and sufficient time, these computations could be rigorously verified.

## *6.1 A Brief Digression*

It is well known that the quadratic field $\mathbb{Q}(\mu_3)$ has class number 1 and, we know from Proposition 2.5.1 that every field in the anticyclotomic $\mathbb{Z}_3$-extension (or any other $\mathbb{Z}_3$-extension) of $\mathbb{Q}(\mu_3)$ has class number prime to 3. Therefore, the anti-cyclotomic $\mathbb{Z}_3$-extension of $\mathbb{Q}(\mu_3)$ by itself is not very interesting from an Iwasawa-theoretic point of view (though in the next section we will later use it to build interesting $\mathbb{Z}_3$-extensions of biquadratic fields). However, using Sage, I computed the class numbers of the first three layers of the anticyclotomic extension and found that all three fields have class number 1.

**Question 6.1.1.** *How far up the anticyclotomic $\mathbb{Z}_3$-tower of $\mathbb{Q}(\mu_3)$ must one go to find a field with nontrivial class group?*

## *6.2 The $\omega$-$\mathbb{Z}_3$-Extension of $K = \mathbb{Q}(\mu_3, \sqrt{d})$, $d \equiv 1 \pmod 3$*

Let $K = \mathbb{Q}(\mu_3, \sqrt{d})$ with $d > 1$ squarefree and $d \equiv 1 \pmod 3$. We will study the $\omega$-$\mathbb{Z}_3$-extension of $K$ (that is, the compositum of $K$ and the anti-cyclotomic $\mathbb{Z}_3$-extension of $\mathbb{Q}(\mu_3)$). Our motivation for doing this is the discussion in Example 3.5.2. Specifically, we are interested in this example for two reasons: first, there are no known examples of

nonsemisimple $\mathbb{Z}_3$-extensions and, second, we would like to know if there's any chance of higher nonsemisimplicity for the $\omega$-$\mathbb{Z}_p$-extension of $\mathbb{Q}(\mu_p, \sqrt{d})$, $p > 3$.

Even without the discussion from Example 3.5.2, one might consider $K_\infty^\omega$ to be the simplest example of a $\mathbb{Z}_3$-extension where $T$-semisimplicity is unknown. We have seen that every $\mathbb{Z}_p$-extension of a quadratic field is $T$-semisimple. For biquadratic fields, know the following: If $p$ splits completely in the biquadratic field, we know that all $\mathbb{Z}_p$-extensions are $T$-semisimple (Corollary 4.1.7). On the other hand, if $p$ does not split at all, there are no trivial zeros.

*How the class groups are computed*

The field $K_1$ is a degree 12 number field. Calculating $A_1$ is usually quite manageable. However, since we are only interested in the 3-part of the class group, we can speed up the computations significantly by computing the 3-part fo the class group for two index 2 subfields instead (of degree 6 over $\mathbb{Q}$). Similarly, $K_2$ is a degree 36 number field, and it is often too difficult to compute the class group directly. However, in some cases it is possible to determine $A_2$ by working with index 2 subfields (of degree 18 over $\mathbb{Q}$).

There are many ways to lift $\Delta = \mathrm{Gal}(K/\mathbb{Q})$ to a subgroup of $\mathrm{Gal}(K_1/\mathbb{Q})$. We will identify $\Delta$ with the subgroup $\tilde{\Delta} = \mathrm{Gal}(K_1/\mathbb{Q}(\sqrt[3]{3}))$. Specifically, let $\tilde{\tau}$ denote a generator of $\mathrm{Gal}(K_1/\mathbb{Q}(\sqrt{d}, \sqrt[3]{3}))$ and let $\tilde{\sigma}$ denote a generator of $\mathrm{Gal}(K_1/\mathbb{Q}(\mu_3, \sqrt[3]{3}))$. Then $\tilde{\tau}$ is a complex conjugation of $K_1$ and $\tilde{\tau}|_K = \tau$ and $\tilde{\sigma}|_K = \sigma$.

The group $\langle\tilde{\tau}\rangle$ acts on $A_1$. Because $A_1$ is a $p$-group and $\langle\tilde{\tau}\rangle$ has order 2, we can decompose $A_1$ using the action of $\langle\tilde{\tau}\rangle$. Note that $\tilde{\sigma}(c) = c^{-1}$ for all $c \in A_1$. One way to see this is to note that 3 does not divide the class number of $\mathbb{Q}(\mu_3, \sqrt[3]{3})$ so the norm map $A_1 \to \mathrm{Cl}(\mathbb{Q}(\mu_3, \sqrt[3]{3})[3^\infty]$ is trivial, i.e.,

$$N_{K_1/\mathbb{Q}(\mu_3, \sqrt[3]{3})}(c) = c\tilde{\sigma}(c) = 1$$

for all $c \in A_1$. Now, let us consider the norm maps from $A_1$ to $\mathrm{Cl}(\mathbb{Q}(\sqrt{d}, \sqrt[3]{3}))[3^\infty]$ and

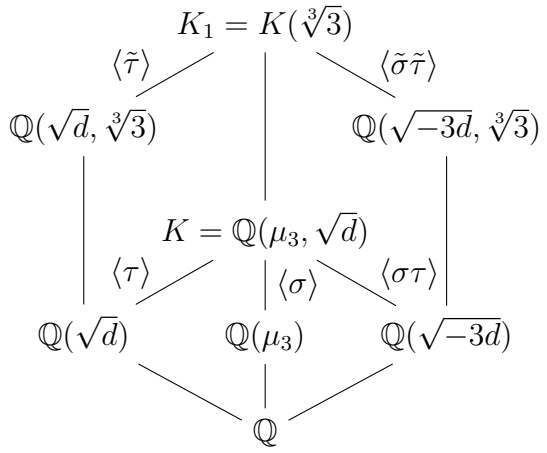


Figure 6.1: The fields used to compute $A_1$ for $K = \mathbb{Q}(\mu_3, \sqrt{d})$ and $K_1 = K(\sqrt[3]{3})$

$\mathrm{Cl}(\mathbb{Q}(\sqrt{-3d}, \sqrt[3]{3}))[3^\infty]$. Note that

$$\begin{aligned} \ker\left(N_{K_1/\mathbb{Q}(\sqrt{d}, \sqrt[3]{3})}\right) &= \{c \in A_1 : c\tilde{\tau}(c) = 1\} \\ &= \{c \in A_1 : \tilde{\tau}(c) = c^{-1}\} \end{aligned}$$

and, because $\tilde{\sigma}(c) = c^{-1}$ for all $c \in A_1$,

$$\begin{aligned} \ker\left(N_{K_1/\mathbb{Q}(\sqrt{-3d}, \sqrt[3]{3})}\right) &= \{c \in A_1 : c\tilde{\sigma}\tilde{\tau}(c) = 1\} \\ &= \{c \in A_1 : \tilde{\tau}(c) = c\} \end{aligned}$$

Therefore

$$\begin{aligned} \mathrm{Cl}(\mathbb{Q}(\sqrt{d}, \sqrt[3]{3}))[3^\infty] &\simeq \{c \in A_1 : \tilde{\tau}(c) = c\} \\ \mathrm{Cl}(\mathbb{Q}(\sqrt{-3d}, \sqrt[3]{3}))[3^\infty] &\simeq \{c \in A_1 : \tilde{\tau}(c) = c^{-1}\} \end{aligned}$$

Consequently, $A_1$ is the direct sum of the 3-part of the class groups of $\mathbb{Q}(\sqrt{d}, \sqrt[3]{3})$ and $\mathbb{Q}(\sqrt{-3d}, \sqrt[3]{3})$. A similar argument shows that one can compute $A_n$ using pairs of index 2 subfields for all $n \geq 0$.

*The $\mathcal{O}$-module Structure of $A_1$*

Let $h_K$ denote the class number of $K = \mathbb{Q}(\mu_3, \sqrt{d})$. We will focus on the special case when 3 does not divide $h_K$. We will see in Lemma 6.2.4 that the corresponding Iwasawa module is particularly nice in this case: specifically, $X$ is cyclic. My initial motivation for studying fields $K$ for which 3 does not divide the class number was a result of computing $A_1$ for many examples: Restricting to the case of class number prime to 3 some interesting patterns emerged. For example, after computing a few examples, one quickly notices that $A_1$ seems to be the product of two cyclic groups. This can be explained by studying $A_1$ as a module over the ring $\mathcal{O} = \mathbb{Z}_3[\zeta_3]$, the ring of integers of $\mathbb{Q}_3(\mu_3)$. Note that $\mathcal{O}$ is a discrete valuation ring and that $\zeta_3 - 1$ is a uniformizer.

**Lemma 6.2.1.** *Let $K = \mathbb{Q}(\mu_3, \sqrt{d})$ with $d > 1$, squarefree, and $d \equiv 1 \pmod 3$. Let $X$ denote the Iwasawa module corresponding to $K_\infty^\omega/K$ and let $A_n$ denote the 3-part of the the $n$-th layer of $K_\infty^\omega/K$. Suppose that $3 \nmid h_K$ (i.e. $A_0 = 0$). Then $A_1$ is a cyclic $\mathcal{O}$-module:*

$$A_1 \simeq \frac{\mathcal{O}}{(\zeta_3 - 1)^r} \simeq \frac{\mathbb{Z}}{3^a\mathbb{Z}} \times \frac{\mathbb{Z}}{3^b\mathbb{Z}},$$

*where $b \leq a \leq b + 1$ and $a + b = r$. Here the first isomorphism is as $\mathcal{O}$-modules and the second as abelian groups*

*Proof.* Let $\sigma$ denote a generator for $\mathrm{Gal}(K_1/K)$. Then $A_1$ is a module over the ring $\mathbb{Z}_3[\sigma]$. Because $3 \nmid h_K$, the norm map $\nu : A_1 \to A_1$ is trivial. Therefore, $A_1$ is a module over the ring

$$\frac{\mathbb{Z}_3[\sigma]}{(\sigma^2 + \sigma + 1)} \simeq \mathbb{Z}_3[\zeta_3] = \mathcal{O}.$$

Comparing the orders of the groups in Proposition 3.4.5, we see that $A_1^{\mathrm{Gal}(K_1/K)}$ is cyclic of order 3. It follows that $(A_1)_{\mathrm{Gal}(K_1/K)} = A_1/(\sigma - 1)A_1$ is also cyclic of order 3. Hence, by Nakayama's lemma, $A_1$ is a cyclic $\mathcal{O}$-module. The group isomorphism follows by considering the filtration $\mathcal{O} \supseteq (\zeta_3 - 1) \supseteq (\zeta_3 - 1)^2 \supseteq \cdots$. □

| $\mathrm{ord}_3(\lvert A_1\rvert)$ | number of $d$ | percentage | number of prime $d$ | percentage |
|---|---|---|---|---|
| any | 11662 | 100% | 2446 | 100% |
| 1 | 7781 | 66.72% | 1636 | 66.88% |
| 2 | 0 | 0% | 0 | 0% |
| 3 | 2589 | 22.20% | 537 | 21.95% |
| 4 | 876 | 7.51% | 192 | 7.85% |
| 5 | 288 | 2.47% | 55 | 2.25% |
| 6 | 92 | 0.79% | 20 | 0.82% |
| 7 | 22 | 0.19% | 1 | 0.04% |
| 8 | 8 | 0.07% | 3 | 0.12% |
| 9 | 5 | 0.04% | 1 | 0.04% |
| $\geq 10$ | 1 | 0.01% | 1 | 0.04% |

Table 6.1: Statistics about the size of $A_1$ for the $\omega$-$\mathbb{Z}_3$-extension of $K = \mathbb{Q}(\mu_3, \sqrt{d})$ for all values of $d \leq 83542$ with $d \equiv 1 \pmod 3$ and $3 \nmid h_K$. By Lemma 6.2.1, $\mathrm{ord}_3(\lvert A_1\rvert)$ completely determines the structure of $A_1$.

In the proof of Lemma 6.2.1 we could view $A_1$ as a $\Lambda$-module. Doing so, we have $A_1^{\mathrm{Gal}(K_1/K)} = A_1[T]$ and $(A_1)_{\mathrm{Gal}(K_1/K)} = A_1/TA_1$. This is the notation we shall adopt for the remainder of the chapter.

*Some Statistics for $A_1$*

I computed $A_1$ for fields in $K = \mathbb{Q}(\mu_3, \sqrt{d})$ satisfying $d \equiv 1 \pmod 3$ and $3 \nmid h_K$ for values of $d$ up to $d = 83542$ of which there are 11662 examples, 2446 of which are prime. Statistics about the size of $A_1$ are given in Table 6.2. (Note that $\mathrm{ord}_3(\lvert A_1\rvert)$ completely determines the structure of $A_1$ by Lemma 6.2.1.) For each value of $\mathrm{ord}_3(\lvert A_1\rvert)$, we give the first five corresponding values of $d$ along with the first five corresponding prime values of $d$ in Table 6.2.

Two features stand out in Table 6.2. First, that $\mathrm{ord}_3(\lvert A_1\rvert) \neq 2$ for any of the examples

| $\mathrm{ord}_3(\lvert A_1\rvert)$ | First five $d$ | First five prime $d$ |
|---|---|---|
| 1 | $7, 10, 13, 19, 22$ | $7, 13, 19, 61, 97$ |
| 3 | $37, 46, 190, 283, 301$ | $37, 283, 367, 541, 631$ |
| 4 | $31, 73, 91, 118, 211$ | $31, 73, 211, 313, 421$ |
| 5 | $154, 334, 619, 1438, 1459$ | $619, 1459, 3313, 3541, 4129$ |
| 6 | $514, 1123, 1402, 1819, 4387$ | $1123, 4423, 10399, 11527, 19963$ |
| 7 | $2290, 2605, 4861, 16114, 19906$ | $4861$ |
| 8 | $4213, 6493, 10177, 21799, 27370$ | $10177, 21799, 42139$ |
| 9 | $25162, 26089, 55417, 78145, 82039$ | $82039$ |
| 10 | $78277$ | $78277$ |

Table 6.2: The first few values of $d$ for which $A_1$ has a given size for the $\omega$-$\mathbb{Z}_3$-extension of $K = \mathbb{Q}(\mu_3, \sqrt{d})$, $d \equiv 1 \pmod 3$, $3 \nmid h_K$.

considered. We will prove that $\mathrm{ord}_3(\lvert A_1\rvert)$ can never be 2 (see Lemma 6.2.2). The second feature of note is that, skipping the row with $\mathrm{ord}_3(\lvert A_1\rvert) = 2$, the percentages decrease by roughly a factor of 3 as we go from one row to the next. Specifically, we have

$$\frac{\lvert\{d : \mathrm{ord}_3(\lvert A_1\rvert) = 1\}\rvert}{\lvert\{d\}\rvert} \approx \frac{2}{3} \quad \text{and, for } r \geq 3, \quad \frac{\lvert\{d : \mathrm{ord}_3(\lvert A_1\rvert) = r\}\rvert}{\lvert\{d\}\rvert} \approx \frac{2}{3^{r-1}} \tag{6.2.1}$$

We will discuss this phenomenon in more detail, but a convincing explanation is still lacking.

*A Special Restriction*

**Lemma 6.2.2.** *Let $d \equiv 1 \pmod 3$ and let $K$ denote the biquadratic field $K = \mathbb{Q}(\mu_3, \sqrt{d})$. Let $K_1 = K(\sqrt[3]{3})$ and let $L_1$ denote the 3-Hilbert class field of $K_1$. Suppose that $3 \nmid h_K$. Then $A_1 = \mathrm{Gal}(L_1/K_1)$ cannot be an $\mathcal{O}$-module of the form $\mathcal{O}/(\zeta_3 - 1)^2$ and thus, cannot be isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.*

*Proof.* We know from Lemma 6.2.1 that $A_1 \simeq \mathcal{O}/(\zeta_3 - 1)^r$ for some $r \geq 1$ and, therefore,

that

$$A_1[T] \simeq \mathbb{Z}/3\mathbb{Z} \simeq A_1/T_1A_1.$$

Note that the decomposition subgroup $\Delta_3$ of $\Delta = \mathrm{Gal}(K/\mathbb{Q})$ acts nontrivially on $T^kA_1/T^{k+1}A_1$ when $k$ is even and trivially when $k$ is odd. In particular, $\Delta_3$ acts nontrivially on $A_1/TA_1$. Suppose for contradiction that $r = 2$. From Proposition 3.4.5, we see that $\Delta_3$ acts trivially on the subgroup of $A_1$ generated by the decomposition subgroups for primes above 3. In particular, $A_1[T]$ is generated by these decomposition subgroups.

Let $F_1'$ denote the first layer of the anticyclotomic $\mathbb{Z}_3$-extension of $\mathbb{Q}(\sqrt{-3d})$ and let $K_1' = F'(\mu_3)$. Then $K_1' = K(\sqrt[3]{\alpha})$ for some $\alpha$. $\Delta$ acts on $\mathrm{Gal}(K_1'/K)$ by $\omega\phi$ and, thus on $\mathrm{Hom}(\mathrm{Gal}(K_1'/K), \mu_3)$ by $\phi$. It follows that $\alpha$ can be chosen to be a 3-unit in $\mathbb{Q}(\sqrt{d})$: Specifically, let $\mathfrak{p}$ be one of the primes above 3 in $\mathbb{Q}(\sqrt{d})$,let $\pi$ be a generator for $\mathfrak{p}^{h_{\mathbb{Q}(\sqrt{d})}}$, and $\epsilon$ the fundamental unit of $F'$. Then $\alpha$ can be taken to be one of

$$\left\{\epsilon, \frac{\pi}{\sigma(\pi)}, \epsilon\frac{\pi}{\sigma(\pi)}, \epsilon^2\frac{\pi}{\sigma(\pi)}\right\}$$

where $\sigma$ denotes the nontrivial element of $\mathrm{Gal}(K/\mathbb{Q}(\mu_3))$. We will show that $\alpha$ must be different from $\epsilon$. To see this, note that the completions of $K_1$ and $K_1'$ at a prime above 3 are the same since both lie within the unique $\mathbb{Z}_3$-extension of $\mathbb{Q}_3(\mu_3)$ which is Galois over $\mathbb{Q}_3$ and on which $\mathrm{Gal}(\mathbb{Q}_3(\mu_3)/\mathbb{Q}_3)$ acts nontrivially. Thus, it suffices to show that $\epsilon$ and 3 generate different subgroups in $\mathbb{Q}_3(\mu_3)^\times/\left(\mathbb{Q}_3(\mu_3)\right)^3$ and this follows by considering valuations: Note that $\mathrm{ord}_{(1-\zeta_3)}(3) = 2$ . However, for all $\beta \in \mathbb{Q}_3(\mu_3)^\times$ and $n \in \mathbb{Z}$, we have

$$\mathrm{ord}_{1-\zeta_3}\left((\epsilon\beta^3)^n\right) \equiv 0 \pmod 3$$

Consequently, we may suppose that

$$\alpha \in \left\{\frac{\pi}{\sigma(\pi)}, \epsilon\frac{\pi}{\sigma(\pi)}, \epsilon^2\frac{\pi}{\sigma(\pi)}\right\}$$

Let $\mathfrak{P}$ denote the prime of $K_1'$ lying above $\mathfrak{p}$ so that $\mathfrak{p} = \mathfrak{P}^6$. By abuse of notation, let $\sigma\tau$ denote the generator of $\mathrm{Gal}(K_1'/F_1')$. Because there is only one prime above 3 in $F'$ and because $3 \nmid h_{F'}$, the class number of $F_1'$ is not divisible by 3. In particular, the class of

$\mathfrak{P}\sigma\tau(\mathfrak{P})$ has order prime to 3. On the other hand, we have the following equality of fractional ideals of $K_1'$:

$$\left(\frac{\mathfrak{P}}{\sigma\tau(\mathfrak{P})}\right)^{6h_{\mathbb{Q}(\sqrt{d})}} = \left(\frac{\pi}{\sigma\tau(\pi)}\right) = \left(\frac{\pi}{\sigma(\pi)}\right) = (\alpha) = \left(\sqrt[3]{\alpha}\right)^3$$

It follows that $(\mathfrak{P}/\sigma\tau(\mathfrak{P}))^{2h_{\mathbb{Q}(\sqrt{d})}}$ is principal and, thus, that the class of $\mathfrak{P}/\sigma\tau(\mathfrak{P})$ has order prime to 3. Because both $\mathfrak{P}\sigma\tau(\mathfrak{P})$ and $\mathfrak{P}/\sigma\tau(\mathfrak{P})$ have order prime to 3 in $\mathrm{Cl}(K_1')$, the same is true of the classes of $\mathfrak{P}$ and $\sigma\tau(\mathfrak{P})$. Therefore, the decomposition subgroups for the primes above $p$ in $A_1' = \mathrm{Gal}(L_1'/K_1')$ are trivial.

Now, because $A_1 \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, we find that $L_1$ is an unramified extension of $K_1K_1'$ and thus an unramified pro-3 extension of $K_1'$. Furthermore, $\mathrm{Gal}(L_1/K_1K_1')$ is a central subgroup of $\mathrm{Gal}(L_1/K_1')$ and the quotient by this subgroup is $\mathrm{Gal}(K_1K_1'/K_1') \simeq \mathbb{Z}/3\mathbb{Z}$, a cyclic group. It follows that $L_1/K_1'$ is actually an abelian extension and, thus, that $L_1 \subseteq L_1'$. In particular, $A_1[T]$ is a subquotient of $A_1'$. But $A_1[T]$ is generated by the decomposition subgroups for primes above 3 and these decomposition subgroups are trivial in $A_1'$. We have arrived at the desired contradiction and may conclude that $r$ cannot be 2. □

*Cohen-Lenstra with a Twist*

We will attempt to explain the distribution of the values of $\mathrm{ord}_3(|A_1|)$ following the philosophy of the Cohen-Lenstra heuristics. Given the constraints on $A_1$ described above, it is perhaps unsurprising that our attempt at an explanation leaves much to be desired.

The Cohen-Lenstra heuristics, first stated in [7], are a tool which has done a very good job of predicting the number of quadratic fields with a given class group. The idea behind the heuristics for imaginary quadratic fields to treat the $p$-part of the class group (for $p > 2$) as a random abelian $p$-group and say that each possible group should occur with probability inversely proportional to the size of its automorphism group.

One could try to apply the same idea, not to all finite abelian $p$-groups, but just to the

subset of those which we believe can occur as $A_1$. As abelian groups, we have

$$\left|\mathrm{Aut}\left(\frac{\mathbb{Z}}{3^a\mathbb{Z}}\times\frac{\mathbb{Z}}{3^b\mathbb{Z}}\right)\right| = \begin{cases} 2 & \text{if } a=1, b=0, \\ 16\cdot 3^{4b-3} & \text{if } b=a\geq 1, \\ 4\cdot 3^{4b-1} & \text{if } b=a-1\geq 1. \end{cases}$$

(See for example Section 1.2.1 of [22].) Thus, for example,

$$\left|\mathrm{Aut}\left(\frac{\mathbb{Z}}{27\mathbb{Z}}\times\frac{\mathbb{Z}}{9\mathbb{Z}}\right)\right| = 4\cdot 3^7 = \frac{9}{4}\left|\mathrm{Aut}\left(\frac{\mathbb{Z}}{9\mathbb{Z}}\times\frac{\mathbb{Z}}{9\mathbb{Z}}\right)\right| = 3^4\left|\mathrm{Aut}\left(\frac{\mathbb{Z}}{9\mathbb{Z}}\times\frac{\mathbb{Z}}{3\mathbb{Z}}\right)\right|.$$

But, in Table 6.2, $\mathrm{ord}_3(|A_1|)=3$ does not seem to occur 81 times as often as $\mathrm{ord}_3(|A_1|)=5$ nor 36 times as often as $\mathrm{ord}_3(|A_1|)=4$.

However, $A_1$ is not merely an abelian group, but also an $\mathcal{O}$-module. Let us instead apply the same idea to cyclic $\mathcal{O}$-modules. As $\mathcal{O}$-modules, we have

$$\left|\mathrm{Aut}\left(\frac{\mathcal{O}}{(\zeta_3-1)^r}\right)\right| = 2\cdot 3^{r-1}.$$

Using this as the basis for our predictions, we would expect to find 3 times as many examples of $A_1$ with $A_1\simeq\mathcal{O}/(\zeta_3-1)^r$ as with $A_1\simeq\mathcal{O}/(\zeta_3-1)^{r+1}$. More precisely, we expect the proportion of examples with $A_1\simeq\mathcal{O}/(\zeta_3-1)^r$ to be $(2)/3^r$.

This is very close to the behavior observed in Table 6.2, but the absence $\mathcal{O}/(\zeta_3-1)^2$ as a possible structure for $A_1$ throws everything off.

**Question 6.2.3.** *Are the densities predicted in Equation 6.2.1 correct? More precisely, let $S$ denote the set of squarefree integers $d>1$ such that $d\equiv 1 \pmod 3$ and 3 does not divide the class number of $K=\mathbb{Q}(\mu_3,\sqrt{d})$ and, for each $k\geq 1$ let $S_k$ denote the set*

$$S_k = \left\{d\in S : \mathrm{ord}_3\left(\left|\mathrm{Cl}\left(\mathbb{Q}(\mu_3,\sqrt{d},\sqrt[3]{3})\right)\right|\right)=k\right\}.$$

*For $n\in\mathbb{Z}_{\geq 1}$, set*

$$\delta_{k,n} = \frac{|\{d\in S_k : d<n\}|}{|\{d\in S : d<n\}|}.$$

*Do the sequences $\{\delta_{k,n}\}_{n\geq 1}$ converge and, if so, are the following limits correct?*

$$\lim_{n\to\infty}\delta_{k,n} = \begin{cases} 2/3 & k=1 \\ 0 & k=2 \\ 2/3^{k-1} & k>2 \end{cases}$$

*Some Examples*

**Lemma 6.2.4.** *Let $K = \mathbb{Q}(\mu_3, \sqrt{d})$ where $d \equiv 1 \pmod 3$ and $3 \nmid h_K$. Let $X$ denote the Iwasawa module corresponding to the $\mathbb{Z}_3$-extension $K_\infty^\omega/K$. Then $X$ is a cyclic $\Lambda$-module: More specifically, because $X$ admits one trivial zero, $X \simeq \Lambda/T\mathfrak{a}$ for some ideal $\mathfrak{a} \subseteq \Lambda$.*

*Proof.* Let $L_\infty^*$ denote the genus field of $K_\infty^\omega/K$. We know that $X/TX \sim \mathbb{Z}_3$. We will show that $X/TX$ is actually isomorphic (not just pseudo-isomorphic) to $\mathbb{Z}_3$ by showing that $\mathrm{Gal}(L_\infty^*/K) \simeq \mathbb{Z}_3^2$.

Note that there are two primes above 3 in $K$ and that both are totally ramified in $K_\infty^\omega/K$. Let us denote these primes by $\mathfrak{p}_1$ and $\mathfrak{p}_2$, respectively, and let $I_{\mathfrak{p}_i}$ denote the inertia subgroup for $\mathfrak{p}_i$ in $\mathrm{Gal}(L_\infty^*/K)$. Then $I_{\mathfrak{p}_1} I_{\mathfrak{p}_2} \simeq \mathbb{Z}_3^2$ and $(L_\infty^*)^{I_{\mathfrak{p}_1} I_{\mathfrak{p}_2}} = L_0$. But, by assumption, $3 \nmid h_K$ so $L_0 = K$.

Consequently, $X/TX \simeq \mathbb{Z}_3$ and, thus, $X/\mathfrak{m}X \simeq \mathbb{Z}/3\mathbb{Z}$. Applying Nakayama's lemma, we conclude that $X$ is indeed a cyclic $\Lambda$-module. □

Let us consider the special case when $A_1 \simeq \mathbb{Z}/3\mathbb{Z}$. By Theorem 2.3.2, because the primes above 3 are totally ramified in $K_\infty^\omega/K$, we have

$$A_1 \simeq \frac{X}{\nu_{1,0}X} \simeq \frac{\Lambda/T\mathfrak{a}}{\nu_{1,0}\left(\Lambda/T\mathfrak{a}\right)} \simeq \frac{\Lambda}{\nu_{1,0}\Lambda + T\mathfrak{a}}.$$

If $\mathfrak{a} \neq \Lambda$, then $\mathfrak{a} \subseteq \mathfrak{m}$ and we have a surjection $A_1 \to \Lambda/(\nu_{1,0}\Lambda + T\mathfrak{m})$. For $p = 3$, we have $\nu_{1,0} = T^2 + 3T + 3$ so

$$\nu_{1,0}\Lambda + T\mathfrak{m} = (T^2 + 3T + 3, 3T, T^2) = (3, T^2).$$

Furthermore, $\Lambda/(3, T^2) \simeq (\mathbb{Z}/3\mathbb{Z})^2$. Therefore, if $A_1 \simeq \mathbb{Z}/3$, it must be the case that $\mathfrak{a} = \Lambda$.

**Proposition 6.2.5.** *Let $K$ and $X$ be as in Lemma 6.2.4. If, $A_1 \simeq \mathbb{Z}/3\mathbb{Z}$. Then $X \simeq \Lambda/(T)$.*

**Example 6.2.6.** Let $K = \mathbb{Q}(\mu_3, \sqrt{d})$ for $d = 7$. Recall from Table 6.2 that $A_1 \simeq \mathbb{Z}/3\mathbb{Z}$ for the $\mathbb{Z}_p$-extension $K_\infty^\omega/K$. By Proposition 6.2.5, it follows that the corresponding Iwasawa module is isomorphic to $\Lambda/(T)$. Furthermore, by Corollary 3.4.4, the decomposition subgroups for

| $T\mathfrak{a}$ | $A_1$ | $A_2$ | $\mathfrak{a}+\nu_{1,0}\Lambda$ | $\mathfrak{a}+\nu_{2,0}\Lambda$ |
|---|---|---|---|---|
| $T\Lambda$ | $C_3$ | $C_9$ | $(3,T)$ | $(9,T)$ |
| $T^2\Lambda$ | $C_3\times C_3$ | $C_9\times C_9$ | $(3,T^2)$ | $(9,T^2)$ |
| $T^3\Lambda$ | $C_9\times C_3$ | $C_{27}\times C_9\times C_3$ | $(9,3T,T^2+3)$ | $(27,9T,84T^2+9,T^3)$ |
| $T^4\Lambda$ | $C_9\times C_9$ | $C_{27}\times C_{27}\times C_3\times C_3$ | $(9,T^2+3T+3)$ | $(27,84T^2+36T+9,T^4)$ |
| $T\mathfrak{m}$ | $C_3\times C_3$ | $C_9\times C_3$ | $(3,T^2)$ | $(9,3T,T^2)$ |
| $3T\Lambda$ | $C_9\times C_3$ | $C_{27}\times (C_3)^{\oplus 7}$ | $(9,3T,T^2+3)$ | $(27,3T,T^8+9)$ |
| $3T^2\Lambda$ | $C_9\times C_9$ | $C_{27}\times C_{27}\times (C_3)^{\oplus 6}$ | $(9,T^2+3T+3)$ | $(27,3T^2,T^8+36T+9)$ |

Table 6.3: The group structure of $A_1$ and $A_2$ if $X=\Lambda/T\mathfrak{a}$ for a few choices of $\mathfrak{a}$.

primes above $p$ generate a finite subgroup of $X/TX$ (looking carefully at the proof, we see that in fact the decomposition subgroups are all trivial). This example provides a negative answer to the question of Jaulent and Sands (Question 3.6.1). In fact, using Corollary 4.2.2, we see that every $\mathbb{Z}_3$-extension of $K=\mathbb{Q}(\mu_3,\sqrt{7})$ is $T$-semisimple.

The same argument works for $d=10,13,19,22,61,97$ or any other value for which $A_1\simeq\mathbb{Z}/3\mathbb{Z}$.

For different candidate ideals $\mathfrak{a}$ one can use Theorem 2.3.2 to determine the corresponding group structure of $A_1$ and $A_2$ and narrow down the possibilities. When $p=3$, we have

$$\begin{aligned}\nu_{1,0} &= T^2+3T+3\\ \nu_{2,0} &= T^8+9T^7+36T^6+84T^5+126T^4+126T^3+84T^2+36T+9\end{aligned}$$

The groups $A_1$ and $A_2$ which would occur for various $\Lambda$-modules of the form $\Lambda/T\mathfrak{a}$ are listed in Table 6.3.

If $A_1$ is not cyclic of order 3, then it does not completely determine $X$. $A_2$ was computed for the first few fields $K=\mathbb{Q}(\mu_3,\sqrt{d})$ (ordered by $d$) satisfying $|A_1|>3$. The results are presented in Table 6.2. Both $A_1$ and $A_2$ are broken into two components: the component coming from the index 2 subfields of $K_1$ and $K_2$ containing $\mathbb{Q}(\sqrt{d})$ and the component coming

| $d$ | $\mathrm{ord}_3(\lvert A_1\rvert)$ | $\mathrm{ord}_3(\lvert A_2\rvert)$ | $A_1$ | | $A_2$ | |
|---|---|---|---|---|---|---|
| | | | $d$ | $-3d$ | $d$ | $-3d$ |
| 31 | 4 | 5 | $C_9$ | $C_9$ | $C_9$ | $C_9 \times C_3$ |
| 37 | 3 | 5 | $C_3$ | $C_9$ | $C_9$ | $C_9 \times C_3$ |
| 46 | 3 | 5 | $C_3$ | $C_9$ | $C_9$ | $C_9 \times C_3$ |
| 73 | 4 | 5 | $C_9$ | $C_9$ | $C_9$ | $C_9 \times C_3$ |
| 91 | 4 | 12 | $C_9$ | $C_9$ | $C_{27} \times C_3 \times C_3 \times C_3$ | $C_{27} \times C_3 \times C_3 \times C_3$ |
| 118 | 4 | ? | $C_9$ | $C_9$ | $C_9$ | ? |
| 154 | 5 | 7 | $C_9$ | $C_{27}$ | $C_{27}$ | $C_{27} \times C_3$ |
| 190 | 3 | 5 | $C_3$ | $C_9$ | $C_9$ | $C_9 \times C_3$ |
| 211 | 4 | ? | $C_9$ | $C_9$ | ? | ? |
| 214 | 4 | ? | $C_9$ | $C_9$ | $C_9$ | ? |
| 283 | 3 | 5 | $C_3$ | $C_9$ | $C_9$ | $C_9 \times C_3$ |

Table 6.4: The group structure of $A_1$ and $A_2$ for the $\omega$-$\mathbb{Z}_3$-extension of the first few fields $K = \mathbb{Q}(\mu_3, \sqrt{d})$, $d \equiv 1 \pmod 3$. The groups $A_1$ and $A_2$ are broken up into the components coming from the different index 2 subfields (containing either $\mathbb{Q}(\sqrt{d})$ or $\mathbb{Q}(\sqrt{-3d})$). The question marks correspond to calculations I was unable to carry out.

from the index 2 subfields of $K_1$ and $K_2$ containing $\mathbb{Q}(\sqrt{-3d})$. So, for example, when $d = 31$ we have $A_1 \simeq \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ and $A_2 \simeq \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. The entries with question marks correspond to computations I was unable to complete.

**Lemma 6.2.7.** *Suppose $X = \Lambda/T\mathfrak{a}$. Then $\nu_{n,0}X \cap TX = \nu_{n,0}TX$ and we have an isomorphism*

$$T\left(\frac{X}{\nu_{n,0}X}\right) \simeq \frac{TX}{\nu_{n,0}(TX)}.$$

*Proof.* Certainly $\nu_{n,0}TX \subseteq \nu_{n,0}X \cap TX$. To show the reverse containment, suppose that $x \in \nu_{n,0}X \cap TX = \nu_{n,0}\left(\frac{\Lambda}{T\mathfrak{a}}\right) \cap T\left(\frac{\Lambda}{T\mathfrak{a}}\right)$. Then, there exist $y, z \in \Lambda$ such that

$$x = \nu_{n,0}y + T\mathfrak{a} = Tz + T\mathfrak{a}.$$

Therefore, $\nu_{n,0}y \in T\Lambda$ and, because $\Lambda$ is a UFD it follows that $y \in T\Lambda$. Hence, $x \in \nu_{n,0}T\Lambda$ as desired. □

**Proposition 6.2.8.** *Let $K$ and $X$ be as in Lemma 6.2.4. Suppose that $|A_{n+1}| = 3|A_n|$ for some $n \geq 0$. Then*

$$X \sim \Lambda/T \qquad \textit{and} \qquad TX \simeq TA_n.$$

*Proof.* First, note that

$$\frac{A_n}{TA_n} \simeq \frac{X/\nu_{n,0}X}{T\left(X/\nu_{n,0}X\right)} \simeq \frac{X}{(T,\nu_{n,0})X} \simeq \frac{\Lambda/T\mathfrak{a}}{(T,\nu_{n,0})\left(\Lambda/T\mathfrak{a}\right)} \simeq \frac{\Lambda}{(T,\nu_{n,0})\Lambda}.$$

The constant term of $\nu_{n,0} = \left((1+T)^{3^n} - 1\right)/T$ is $3^n$ so $(T,\nu_{n,0}) = (T,3^n)$. Consequently, $|A_n/TA_n| = 3^n$. Similarly, $|A_{n+1}/TA_{n+1}| = 3^{n+1}$. Therefore,

$$|TA_{n+1}| = \frac{|A_{n+1}|}{|A_{n+1}/TA_{n+1}|} = \frac{3|A_n|}{3^{n+1}} = \frac{|A_n|}{|A_n/TA_n|} = |TA_n|.$$

Because $K_\infty^\omega/K$ is totally ramified, the norm map gives a surjection $A_{n+1} \to A_n$ and, thus, $TA_{n+1} \to TA_n$. It follows that the norm map yields an isomorphism $TA_{n+1} \xrightarrow{\simeq} TA_n$. From Lemma 6.2.7, we have isomorphisms

$$TA_{n+1} \simeq \frac{TX}{\nu_{(n+1),0}(TX)} \quad \text{and} \quad TA_n \simeq \frac{TX}{\nu_{n,0}(TX)}.$$

Note that $\nu_{(n+1),0} = \nu_{(n+1),n} \cdot \nu_{n,0}$. Studying the isomorphisms above, we find that isomorphism induced by the norm map is precisely the quotient map

$$\frac{TX}{\nu_{(n+1),0}(TX)} \to TA_n \simeq \frac{TX}{\nu_{n,0}(TX)}.$$

It follows that

$$\frac{\nu_{n,0}TX}{\nu_{(n+1),n}\left(\nu_{n,0}TX\right)} = \frac{\nu_{n,0}TX}{\nu_{(n+1),0}X} = 0.$$

By Nakayama's Lemma, it follows that $\nu_{n,0}TX = 0$ and, hence, by Lemma 6.2.7 that

$$TA_n \simeq T\left(\frac{X}{\nu_{n,0}X}\right) \simeq \frac{TX}{\nu_{n,0}TX} \simeq TX.$$

Therefore, the map $X \to X/TX \simeq \Lambda/(T)$ is a pseudo-isomorphism. □

**Example 6.2.9.** From Table 6.2, we see that the hypotheses of Proposition 6.2.8 are satisfied for $d = 31$ or 73 and $n = 1$. It follows that $K_\infty^\omega$ is $T$-semisimple with $TX \simeq TA_1$ finite of order 27.

For $d = 37, 46, 91, 154, 190$, $A_1$ and $A_2$ are not sufficient to determine the Iwasawa module.

**Example 6.2.10.** The case of $d = 91$ is particularly interesting. Our computations leave open the possibilities that $X$ is not $T$-semisimple and $X$ has positive $\mu$-invariant. Going from $A_1$ to $A_2$ we see both horizontal and vertical growth and these groups are compatible with $X \simeq \Lambda/(3T^2)$. Of course, it could also happen that $\mu = 0$ and $TX$ is finite (for example if $\mathfrak{a} = (3, T^8)$).

**Question 6.2.11.** *What is the Iwasawa module corresponding to the $\omega$-$\mathbb{Z}_3$-extension of $\mathbb{Q}(\mu_3, \sqrt{91})$? Is $TX$ finite? Is $X$ $T$-semisimple? Is the $\mu$-invariant of $X$ zero?*

## 6.3 The Anti-cyclotomic $\mathbb{Z}_3$-Extension of $F = \mathbb{Q}(\sqrt{-3d})$, $d \equiv 2 \pmod 3$

As in Section 5.2, let $F = \mathbb{Q}(\sqrt{-3d})$ for positive squarefree $d \equiv 2 \pmod 3$. For the values of $d$ in Table 5.3, I computed $A_0$ and $A_1$ and checked capitulation. In the cases where $A_0$ does not capitulate at the first layer (i.e. $J_{F_1/F_0}$ is not the zero map) as well as the case $d = 254$, I also computed $A_2$ and checked capitulation from $A_0$ to $A_2$. These results are gathered in Table 6.5. In each of the examples considered, $A_0$ is cyclic. Thus, to check capitulation, we simply need to check the class in $A_n$ of an ideal whose class generates $A_0$.

Capitulation seems to occur quite frequently at the first layer when $A_0 \simeq \mathbb{Z}/3\mathbb{Z}$. In this case, Proposition 2.5.2. tells us that $X \simeq A_1$. For $d = 899$ and $d = 1211$, capitulation does not occur until the second layer and $A_1$ is different in these two cases.

**Example 6.3.1.** A particularly interesting example is that of $F = \mathbb{Q}(\sqrt{-3 \cdot 473})$. We see from Table 6.5 that capitulation does not occur in at the first or second layer of the anti-cyclotomic extension. Does capitulation ever occur and, if so, how far up the tower does it occur?

| d | $A_0$ | $A_1$ | $A_2$ | order of generator for $A_0$ | | |
|---|---|---|---|---|---|---|
| | | | | in $A_0$ | in $A_1$ | in $A_2$ |
| 254 | $C_3$ | $C_9 \times C_9$ | $C_9 \times C_9$ | 3 | 1 | 1 |
| 257 | $C_3$ | $C_3 \times C_3$ | - | 3 | 1 | - |
| 326 | $C_3$ | $C_3 \times C_3$ | - | 3 | 1 | - |
| 443 | $C_9$ | $C_9 \times C_3$ | $C_9 \times C_9$ | 9 | 3 | 1 |
| 473 | $C_3$ | $C_9 \times C_3$ | $C_{27} \times C_9$ | 3 | 3 | 3 |
| 506 | $C_3$ | $C_3 \times C_3$ | - | 3 | 1 | - |
| 659 | $C_9$ | $C_3$ | $C_9 \times C_3$ | 9 | 3 | 3 |
| 761 | $C_3$ | $C_3 \times C_3$ | - | 3 | 1 | - |
| 785 | $C_3$ | $C_9 \times C_9$ | - | 3 | 1 | - |
| 839 | $C_3$ | $C_3 \times C_3$ | - | 3 | 1 | - |
| 842 | $C_3$ | $C_3 \times C_3$ | - | 3 | 1 | - |
| 899 | $C_3$ | $C_3 \times C_3 \times C_3$ | $C_3 \times C_3 \times C_3 \times C_3$ | 3 | 3 | 1 |
| 1091 | $C_9$ | $C_3$ | $C_9 \times C_3$ | 9 | 3 | 3 |
| 1211 | $C_3$ | $C_9 \times C_3$ | $C_9 \times C_9$ | 3 | 3 | 1 |
| 1223 | $C_3$ | $C_3 \times C_3$ | - | 3 | 1 | - |
| 1229 | $C_3$ | $C_3 \times C_3$ | - | 3 | 1 | - |

Table 6.5: The group structure of $A_0$, $A_1$ and $A_2$ for the anti-cyclotomic $\mathbb{Z}_3$ extension of $F = \mathbb{Q}(\sqrt{-3d})$. Capitulation of $A_0$ is tracked in the last columns.

Note that when $A_0$ is cyclic of order 3, $A_1$ is larger than $A_0$ in all of our examples, even when $A_0$ capitulates at the first layer. We can prove that this always happens.

**Proposition 6.3.2.** *Let $d \equiv 2 \pmod 3$ such that 3 divides the class number of $\mathbb{Q}(\sqrt{d})$ and let $F = \mathbb{Q}(\sqrt{-3d})$. Let $F_\infty/F$ denote the anticyclotomic $\mathbb{Z}_3$-extension of $F$ and, for each $n$, let $A_n$ denote the 3-Hilbert class group of $F_n$. Finally, suppose that $A_0 \simeq \mathbb{Z}/3\mathbb{Z}$. Then*

*(a) The extension $F_\infty/F$ is totally ramified at the prime above 3.*

*(b) The 3-part of the class group grows in the first layer: $|A_1| > |A_0|$.*

*(c) If $A_0$ does not capitulate at the first layer, then $\mathrm{ord}_3(|A_1|)$ is odd.*

*(d) If $A_0$ capitulates at the first layer, then*

$$A_1 \simeq \left(\frac{\mathbb{Z}}{3^a\mathbb{Z}}\right)^2 \quad \textit{and} \quad X \simeq \frac{\Lambda}{(3^a, \nu_{1,0})}$$

*for some $a \geq 1$*

*Proof.* Let $M_\infty^-$ and $I_\mathfrak{p}(M_\infty^-)$ be as in Lemma 5.2.2. Recall the exact sequence

$$0 \to I_\mathfrak{p}(M_\infty^-) \to \mathrm{Gal}(M_\infty^-/F) \to \mathrm{Gal}(L_0/F) \to 0.$$

As groups, we then have

$$0 \to \mathbb{Z}_3 \to \mathrm{Gal}(M_\infty^-/F) \to \mathbb{Z}/3\mathbb{Z} \to 0.$$

Now, because 3 divides the class number of $\mathbb{Q}(\sqrt{d})$, $F$ admits two independent cubic extensions on which complex conjugation acts nontrivially. One of these is a subfield of $F(\mu_3, \sqrt[3]{\epsilon})$, where $\epsilon$ is a fundamental unit of $\mathbb{Q}(\sqrt{d})$ and the other is a subfield of $F(\mu_3, \sqrt[3]{\alpha})$, where $(\alpha)$ is the cube of an ideal whose class has order 3 in $\mathrm{Cl}(\mathbb{Q}(\sqrt{d}))$. It follows that $\mathrm{Gal}(M_\infty^-/F)$ has 3-rank 2 and, thus, that $F_\infty^{anti}$ and $L_0$ are disjoint.

Suppose first that $A_0$ does not capitulate in $A_1$. The composition $A_0 \overset{J_{F_1/F}}{\to} A_1 \overset{N_{F_1/F}}{\to} A_0$ simply sends each element to its cube. In particular, this means $N_{F_1/F} \circ J_{F_1/F}$ has a nontrivial

kernel. By assumption, $J_{F_1/F}$ is injective so it follows that the norm map $N_{F_1/F}$ has a nontrivial kernel. Because the prime above 3 is totally ramified in $F_\infty^{anti}/F$, the norm map is surjective (this is simply the statement that $\mathrm{Gal}(L_0K_1/K_1) \simeq \mathrm{Gal}(L_0/K)$). Thus, we have the exact sequence

$$0 \to \ker(N_{K_1/K}) \to A_1 \to A_0 \to 0.$$

Since the kernel of $N_{K_1/K}$ is nontrivial, it follows that $|A_1| > |A_0|$.

Suppose instead that $A_0$ capitulates in $A_1$. Then the exact sequence from Proposition 3.4.5 becomes

$$1 \to \ker(J_{F_1/F}) \to \frac{\mathcal{P}_{F_1}^\Gamma}{\mathcal{P}_F} \to \frac{\mathcal{F}_{F_1}^\Gamma}{\mathcal{F}_F} \to A_1^\Gamma \to \frac{\mathcal{O}_F^\times \cap N_{F_1/F}(F_1^\times)}{N_{F_1/F}(\mathcal{O}_{F_1}^\times)} \to 1.$$

Because $F$ is an imaginary quadratic field not containing $\mu_3$, we have $\mathcal{O}_F^\times = \{\pm 1\}$ and so

$$\mathcal{O}_F^\times \supseteq N_{F_1/F}(\mathcal{O}_{F_1}^\times) \supseteq N_{F_1/F}(\mathcal{O}_F^\times) = \left(\mathcal{O}_F^\times\right)^3 = \mathcal{O}_F^\times.$$

It follows that $\mathcal{O}_F^\times / N_{F_1/F}(\mathcal{O}_{F_1}^\times)$ is trivial. By part (c) of Proposition 3.4.5, we see that $\mathcal{P}_{F_1}^\Gamma/\mathcal{P}_F$ is cyclic of order 3. Since $\ker(J_{F_1/F}) = A_0 \simeq \mathbb{Z}/3\mathbb{Z}$ it follows that the map

$$\frac{\mathcal{F}_{F_1}^\Gamma}{\mathcal{F}_F} \to A_1^\Gamma$$

is an isomorphism and, thus, that the decomposition subgroup for $\mathfrak{p}$ in $\mathrm{Gal}(L_1/F_1)$ is cyclic of order 3. On the other hand, the decomposition subgroup for $\mathfrak{p}$ in $\mathrm{Gal}(L_0/F_0)$ is trivial. To see this, consider the extension $L_0/\mathbb{Q}$. We have $\mathrm{Gal}(L_0/\mathbb{Q}) \simeq S_3$ and the inertia subgroup of $\mathfrak{p}$ is of order 2. Each subgroup of $S_3$ of order 2 is its own normalizer so it follows that the decomposition subgroup of $\mathfrak{p}$ in $\mathrm{Gal}(L_0/\mathbb{Q})$ is also of order 2. Combining this with the fact that $F_1/F$ is ramified at $\mathfrak{p}$, we see that the restriction $\mathrm{Gal}(L_1/F_1) \to \mathrm{Gal}(L_0/F_0)$ is surjective and has a nontrivial kernel. It follows that $|A_1| > |A_0|$. This completes the proof of part (b).

We have a filtration

$$\frac{A_1}{TA_1} \to \frac{TA_1}{T^2A_1} \to \cdots \to \frac{T^kA_1}{T^{k+1}A_1} \to \cdots$$

Similarly to the proof of Lemma 3.5.1, one can show that complex conjugation acts non-trivially on $T^k A_1/T^{k+1}A_1$ when $k$ is even and trivially when $k$ is odd. The last term in the filtration is exactly $A_1[T]$. If there is no capitulation, we have $A_1[T] = J_{F_1/F}(A_0)$ so complex conjugation acts nontrivially on both the first and last term of the filtration. It follows that the filtration has odd length and, thus, that $\mathrm{ord}_3(|A_1|)$ is odd.

If capitulation occurs, the last term in the filtration, $A_1[T]$, is the decomposition subgroup for $\mathfrak{p}$. Because 3 is ramified in $F/\mathbb{Q}$, complex conjugation acts trivially on $\frac{\mathcal{F}_{F_1}^{\Gamma}}{\mathcal{F}_F}$ and thus on $A_1[T]$. It follows that the filtration has even length and thus that $\mathrm{ord}_3(|A_1|)$ is even. In fact, we can say more: Because $A_0$ capitulates in $A_1$, the norm operator $\nu_{1,0} : A_1 \to A_1$ is the zero map. It follows that $A_1$ is a cyclic $\mathcal{O}$-module of order $3^{2a}$ for some $a$. That is, $A_1 \simeq \mathcal{O}/(\zeta_3 - 1)^{2a} = \mathcal{O}/(3^a)$. Therefore,

$$X \simeq A_1 \simeq \frac{\Lambda}{(3^a, \nu_{1,0})}.$$

□

# BIBLIOGRAPHY


[1] James Ax. On the units of an algebraic number field. *Illinois Journal of Mathematics*, 9(4):584–589, 1965.

[2] Armand Brumer. On the units of algebraic number fields. *Mathematika*, 14(2):121–4, 1967.

[3] Alan Candiotti. Computations of Iwasawa invariants and $\mathbf{K}_2$. *Compositio Mathematica*, 29(1):89–111, 1974.

[4] J. Carroll and H. Kisilevsky. On the Iwasawa invariants of certain $\mathbb{Z}_p$-extensions. *Compositio Mathematica*, 49(2):217–229, 1983.

[5] Joseph Carroll and H Kisilevsky. On Iwasawas $\lambda$-invariant for certain $\mathbb{Z}_l$-extensions. *Acta Arithmetica*, 40(1):1–8, 1981.

[6] John Coates and Stephen Lichtenbaum. On l-adic zeta functions. *Annals of Mathematics*, pages 498–550, 1973.

[7] Henri Cohen and Hendrik W Lenstra Jr. Heuristics on class groups of number fields. In *Number Theory Noordwijkerhout 1983*, pages 33–62. Springer, 1984.

[8] David A Cox. *Primes of the form $x^2 + ny^2$: Fermat, class field theory, and complex multiplication*, volume 34. John Wiley & Sons, 2011.

[9] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 6.10)*, 2015. `http://www.sagemath.org`.

[10] Bruce Ferrero and Ralph Greenberg. On the behavior of p-adic L-functions at s = 0. *Inventiones mathematicae*, 50(1):91–102, 1978.

[11] Ralph Greenberg. Topics in Iwasawa theory. `https://www.math.washington.edu/~greenber/book.pdf`. accessed April 19, 2013.

[12] Ralph Greenberg. The Iwasawa invariants of $\Gamma$-extensions of a fixed number field. *American Journal of Mathematics*, 95(1):204–214, 1973.

[13] Ralph Greenberg. On a certain l-adic representation. *Inventiones mathematicae*, 21(1-2):117–124, 1973.

[14] Ralph Greenberg. On the Iwasawa invariants of totally real number fields. *American Journal of Mathematics*, 98(1):263–284, 1976.

[15] Ralph Greenberg. Iwasawa theory–past and present. *Adv. Studies in Pure Math*, 30:335–385, 2001.

[16] Ralph Greenberg. Galois representations with open image. *preprint*, 2011.

[17] Jean-François Jaulent. Sur la théorie des genres dans les tours métabéliennes. *Seminaire de Théorie des Nombres de Bordeaux*, 11:1–18, 1981-1982.

[18] Jean-François Jaulent and Jonathan W Sands. Sur quelques modules d'Iwasawa semi-simples. *Compositio Mathematica*, 99(3):325–341, 1995.

[19] Takenori Kataoka. A consequence of Greenberg's generalized conjecture on Iwasawa invariants of $\mathbb{Z}_p$-extensions. *arXiv preprint arXiv:1602.07916*, 2016.

[20] H. Kisilevsky. Some non-semi-simple Iwasawa modules. *Compositio Mathematica*, 49(3):399–404, 1983.

[21] Serge Lang. *Algebraic number theory*, volume 110. Springer Science & Business Media, 1994.

[22] Johannes Lengler. The Cohen–Lenstra heuristic for finite abelian groups. *Doktorarbeit, Universität des Saarlandes, Saarbrücken, Germany*, 2009.

[23] J.S. Milne. Class field theory (v4.02), 2013. Available at www.jmilne.org/math/.

[24] Jurgen Neukirch, Norbert Schappacher, and G Harder. *Algebraic number theory*. Springer-Verlag, 1999.

[25] The PARI Group, Bordeaux. *PARI/GP*, 2014. `http://pari.math.u-bordeaux.fr/`.

[26] Lawrence C Washington. *Introduction to cyclotomic fields*, volume 83. Springer Science & Business Media, 1997.

# Appendix A

## GLOSSARY OF SYMBOLS

| | |
|---|---|
| $A_n$ | The $p$-part of the class group of $K_n$ |
| $\Delta$ | The Galois group of $K/\mathbb{Q}$ |
| $\Delta_p$ | The decomposition subgroup for $p$ of $\Delta$ |
| $\mathcal{F}_K$ | The group of fractional ideals of $K$ |
| $\Gamma$ | The Galois group of the $\mathbb{Z}_p$-extension $K_\infty/K$ |
| $\tilde{\Gamma}$ | The Galois group of the multiple $\mathbb{Z}_p$-extension $\tilde{K}_\infty/K$ |
| $K$ | A number field |
| $K_n$ | The $n$-th layer of the $\mathbb{Z}_p$-extension $K_\infty/K$ |
| $K_\infty$ | A $\mathbb{Z}_p$-extension of $K$ |
| $\tilde{K}_\infty$ | The compositum of all $\mathbb{Z}_p$-extensions of $K$ |
| $J_{K_n/K_m}$ | The map $A_m \to A_n$ induced by the inclusion $\mathcal{F}_{K_m} \hookrightarrow \mathcal{F}_{K_n}$ |
| $L_n$ | The $p$-Hilbert class field of $K_n$ |
| $L_\infty$ | The pro-$p$ Hilbert class field of $K_\infty$ |
| $L_\infty^*$ | The genus field of $K_\infty/K$ |
| $\Lambda$ | The completed group ring $\mathbb{Z}_p[[\Gamma]]$ |
| $\mathfrak{m}$ | The maximal ideal $\mathfrak{m} = (p, T)$ of $\mathbb{Z}_p[[T]]$ |
| $\nu_{n,m}$ | The element $\omega_n/\omega_m$ of $\mathbb{Z}_p[[T]]$ |
| $\mathcal{O}$ | $\mathcal{O} = \mathbb{Z}_3[\zeta_3]$, the ring of integers of $\mathbb{Q}_3(\mu_3)$ |
| $\omega$ | The Teichmüler character $\omega : \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q}) \to \mathbb{Z}_p$ |
| $\omega_n$ | The element $(1+T)^n - 1$ of $\mathbb{Z}_p[[T]]$ |

| | |
|---|---|
| $\mathcal{P}_K$ | The group of principal fractional ideals of $K$ |
| $\tau$ | The complex conjugation automorphism of a CM field |
| $X$ | The Iwasawa module $X = \mathrm{Gal}(L_\infty/K_\infty)$ |