INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps. Each original is also photographed in one exposure and is included in reduced form at the back of the book.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

UMI

A Bell & Howell Information Company
300 North Zeeb Road, Ann Arbor MI 48106-1346 USA
313/761-4700 800/521-0600

The Nonexistence of Certain Free pro-p Extensions and Capitulation in a Family of Dihedral Extensions of $\mathbb{Q}$

by

David Hubbard

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

Doctor of Philosophy

University of Washington

1996

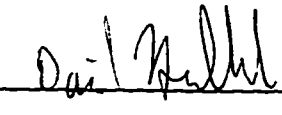
Approved by Ralph Greenberg
Chairperson of Supervisory Committee

Program Authorized
to Offer Degree Mathematics

Date September 23, 1996

Doctoral Dissertation

In presenting this dissertation in partial fulfillment of the requirements for the Doctoral degree at the University of Washington, I agree that the Library shall make its copies freely available for inspection. I further agree that extensive copying of this dissertation is allowable only for scholarly purposes, consistent with "fair use" as prescribed in the U.S. Copyright Law. Requests for copying or reproduction of this dissertation may be referred to University Microfilms, 1490 Eisenhower Place, P.O. Box 975, Ann Arbor, MI 48106, to whom the author has granted "the right to reproduce and sell (a) copies of the manuscript in microform and/or (b) printed copies of the manuscript made from microform."

Signature 

Date Nov 1, 1996

University of Washington

Abstract

The Nonexistence of Certain Free pro-p Extensions and Capitulation in a Family of Dihedral Extensions of $\mathbb{Q}$

by David Hubbard

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

$\mathbb{Z}_p^d$-extensions are a natural way to extend Iwasawa's theory of $\mathbb{Z}_p$-extensions. A further extension would be to look at free pro-p extensions which though nonabelian, can be studied by looking at their maximal abelian subextension, which is a $\mathbb{Z}_p^d$-extension. There is a natural upper bound given by Leopoldt's conjecture for the size of a free pro-p extension of a given number field. We show in the first problem a number field which does not have a free pro-p extension whose size attains this natural upper bound. Although some examples of such number fields are already known, to my knowledge techniques of Iwasawa theory have not been used before to show such a result and should be able to show further insight and examples.

We also make a study of capitulation by computer in a family of S_3-extensions of $\mathbb{Q}$. We compute class groups as well as capitulation and find a variety of behavior. We give proofs for a number of the observations seen. This appears to be the first set of computations done of this type.

Contents

List of Tables

Acknowledgments

I would sincerely like to thank Professor Ralph Greenberg for his time and for all of his efforts and many valuable conversations which introduced me to the beautiful world of number theory and to the ideas and techniques of the field of Iwasawa theory.

Chapter 1

Introduction

After at least ten years of creating the theory of $\mathbb{Z}_p$-extensions, Iwasawa made his great breakthrough around 1970 with what was to be called the "main conjecture" of Iwasawa theory. Connecting the algebraic module we call Y below with the analytic Kubota-Leopoldt p-adic L-functions, the first form of the main conjecture was proved over ten years later in a very long and original paper by Mazur and Wiles building on earlier work of Ribet. See Coates [1] for an overview of Mazur and Wiles' proof of the main conjecture. In this dissertation the main problem we look at will be looked at with techniques started by Iwasawa and furthered by Greenberg and is not among the types of problems which have been traditionally looked at with Iwasawa theory. Specifically, we look at the existence or nonexistence of free pro-p extensions of number fields of certain rank. We will also in a briefer presentation, look at some computer calculations dealing with class groups and the existence of capitulation within a certain family of totally complex extensions of $\mathbb{Q}$ with Galois group S_3, the symmetric group on three generators. These calculations have mostly been done with the KASH program [7] for computational algebraic

number theory and I am very grateful for the support given by the KANT-group in Berlin.

1.1 The Iwasawa Algebra Λ and Galois Groups as Λ-modules

In this section and following sections we will introduce the Iwasawa algebra and a number of standard modules in Iwasawa theory which will be used throughout our presentation. We fix an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ and consider all number fields and field extensions to be contained in $\overline{\mathbb{Q}}$. We also fix a prime number p.

We will frequently in the following have field extensions K of a number field k with $\mathrm{Gal}(K/k)$ topologically isomorphic to $\mathbb{Z}_p^d$, $d \geq 1$, where $\mathbb{Z}_p$ is the additive group of p-adic integers. In these cases we will have various abelian pro-p extensions F of K which will be Galois over k. For instance we could take F to be the maximal abelian unramified pro-p extension of K or even the maximal abelian pro-p extension of K which is unramified outside primes above p. Then $\Gamma = \mathrm{Gal}(K/k)$ will act on $Y = \mathrm{Gal}(F/K)$ and we will be able to make Y into a module over an appropriate ring, the Iwasawa algebra, in a standard way.

The action of Γ on Y is by conjugation. If $\gamma \in \Gamma$ and $y \in Y$, let $\overline{\gamma}$ be any lifting of γ to $\mathrm{Gal}(F/k)$ and define the action of γ on y to be

$$\gamma.g = \overline{\gamma} y \overline{\gamma}^{-1}.$$

This will be independent of the lifting $\overline{\gamma}$ since Y is abelian so this makes Y into a Γ-module. Since Y is also a pro-p group, Y is a $\mathbb{Z}_p$-module in a natural

way. Therefore Y is naturally a module over the completed group ring

$$\mathbb{Z}_p[[\Gamma]] = \varprojlim \mathbb{Z}_p[\Gamma/N]$$

where $[\Gamma : N] < \infty$. Let $\Lambda = \Lambda_{K/k} = \mathbb{Z}_p[[\Gamma]]$. Then Λ is called the Iwasawa algebra and Serre has proved [13] that we have an isomorphism $\Lambda \cong \mathbb{Z}_p[[T_1, \ldots, T_d]]$ so Λ is a noetherian integrally closed local integral domain with Krull dimension $d+1$ and specifically is a UFD. If $\{\gamma_1, \ldots, \gamma_d\}$ is a set of topological generators for Γ, then the above isomorphism is given by the correspondence

$$\gamma_i - 1 \leftrightarrow T_i.$$

We call a Λ-module M pseudo-null, if M has two relatively prime annihilators in Λ and we write $M \sim 0$. Note that over a Dedekind domain, a module is pseudo-null if and only if it is the 0-module. Note also if $\Gamma \cong \mathbb{Z}_p$, then $\Lambda \cong \mathbb{Z}_p[[T]]$ and a module is pseudo-null over Λ if and only if it is finite. However, for $d \geq 2$, a pseudo-null module over Λ can still be quite big and will in general be infinite.

We define modules M and N to be pseudo-isomorphic, written $M \sim N$, if there is a Λ-module map $\phi : M \to N$ with pseudo-null kernel and cokernel.

For $d = 1$, i.e. $\Gamma \cong \mathbb{Z}_p$, we can describe a classification of finitely generated Λ-modules. An elementary Λ-module is defined to be a module of the form

$$E(e_0; \mathfrak{p}_1^{e_1}, \ldots, \mathfrak{p}_s^{e_s}) = \Lambda^{e_0} \oplus \Lambda/\mathfrak{p}_1^{e_1} \oplus \ldots \oplus \Lambda/\mathfrak{p}_s^{e_s}$$

where the $\mathfrak{p}_i$ are height one primes in Λ not necessarily distinct and the e_i are non-negative integers. Then any finitely generated Λ-module M satisfies

$$M \sim E(e_0; \mathfrak{p}_1^{e_1}, \ldots, \mathfrak{p}_s^{e_s})$$

for some unique elementary Λ-module.

Each $\mathfrak{p}_i$ is either the ideal (p) or has the form $(f(T))$ for an irreducible distinguished polynomial $f(T)$. A distinguished polynomial $f(T) \in \Lambda$ has the form

$$f(T) = T^n + a_{n-1}T^{n-1} + \ldots + a_0$$

where $a_i \in \mathbb{Z}_p$ and $p \mid a_i$ for $0 \leq i \leq n-1$. If M is a finitely generated torsion Λ-module and $M \sim E(\mathfrak{p}_1^{e_1}, \ldots, \mathfrak{p}_s^{e_s})$ with $\mathfrak{p}_i = (f_i)$, then $\prod f_i^{e_i}$ is called a characteristic power series of M and it is defined up to a unit in Λ.

An important module associated to the Λ-module X is the Pontrjagin dual $\widehat{X}$ of X. This is defined to be

$$\widehat{X} = \mathrm{Hom}(X, \mathbb{Q}_p/\mathbb{Z}_p)$$

and is a Λ-module through the action of Λ on X. The Pontrjagin dual of a compact totally disconnected module is a discrete torsion module and vice versa. Pontrjagin duality is the statement that for locally compact abelian groups X, there is a canonical isomorphism $\widehat{\widehat{X}} \cong X$.

We should mention here Leopoldt's conjecture which will be important in much of what follows. If k is a number field, then we can consider the composite $\tilde{k}$ of all $\mathbb{Z}_p$-extensions of k. There is always at least one $\mathbb{Z}_p$-extension of a number field since $\mathbb{Q}$ has the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty$ which is contained in $\mathbb{Q}(\mu_{p^\infty})$, μ_{p^∞} the group of p-power roots of unity, and $\mathbb{Q}_\infty$ can always be lifted to any number field. We write this as k_∞ and call it the cyclotomic $\mathbb{Z}_p$-extension of k. Since $\mathbb{Z}_p$-extensions are unramified outside primes above p, class field theory shows that the $\mathbb{Z}_p$-rank of $\mathrm{Gal}(\tilde{k}/k)$ is finite and if $\mathrm{Gal}(\tilde{k}/k) \cong \mathbb{Z}_p^d$ in fact we have $r_2 + 1 \leq d \leq [k : \mathbb{Q}]$. To state Leopoldt's conjecture let $p_1, \ldots, p_g$ be the primes of k above p and let U_{p_i} be the group of local units in the completion K_{p_i} and U_{1,p_i} the principal units. Let

$$U = \prod U_{p_i} \qquad \text{and} \qquad U_1 = \prod U_{1,p_i}.$$

We embed the global units of k diagonally in U and we let E_1 denote the global units whose images lie in U_1. E_1 is a subgroup of finite index in E so E_1 is an abelian group of rank $r_1 + r_2 - 1$.

Leopoldt's Conjecture. *The closure of E_1 within U_1 has maximal rank as $\mathbb{Z}_p$-module, i.e. $r_1 + r_2 - 1$.*

The importance for us is that it follows then that if Leopoldt's conjecture is true then $\mathrm{Gal}(\tilde{k}/k) \cong \mathbb{Z}_p^d$ with $d = r_2 + 1$. We should also mention that Leopoldt's conjecture is also equivalent to the nonvanishing of the p-adic regulator for k.

1.2 The Modules Y_k and A_∞

Let $K \subset \overline{\mathbb{Q}}$ be an algebraic extension of $\mathbb{Q}$, finite or infinite. We denote by L_K the maximal abelian unramified pro-p extension of K and we define $Y_K = \mathrm{Gal}(L_K/K)$. If K is Galois over a subfield k and $\Gamma = \mathrm{Gal}(K/k) \cong \mathbb{Z}_p^d$, then by the maximality of L_K, L_K is also Galois over k so Γ acts on Y_K by conjugation and Y_K becomes a module over the Iwasawa algebra $\Lambda = \Lambda_{K/k} = \mathbb{Z}_p[[\Gamma]]$.

In the case $d = 1$, that is K/k is a $\mathbb{Z}_p$-extension, Iwasawa [5] has shown that Y_K is a finitely generated torsion Λ-module. For general $d \geq 1$, Greenberg [3] has further shown that Y_K is again a finitely generated torsion Λ-module.

If K_i is a finite extension of k contained in K, then we can look at the p-Hilbert class field H_i of K_i. By class field theory H_i will be an unramified abelian p-group extension of K_i and L_K will be the union of all the K_i with $Y_K = \varprojlim \mathrm{Gal}(H_i/K_i)$ under the restriction maps for the $\mathrm{Gal}(H_i/K_i)$. Also by class field theory, $\mathrm{Gal}(H_i/K_i)$ is isomorphic to the p-part A_i of the class group

of K_i. Then $Y_K \cong \varprojlim A_i$ under the norm maps. This gives a connection between Y_K and the p-parts of the ideal class groups in a $\mathbb{Z}_p^d$-extension. In particular, for $d = 1$, if $Y_K \sim E((p^{m_1}), \ldots, (p^{m_t}), (f_1^{\ell_1}), \ldots, (f_s^{\ell_s}))$ with the f_i irreducible distinguished polynomials, then with $\mu = m_1 + \ldots + m_t$ and $\lambda = \ell_1 + \ldots + \ell_s$, Iwasawa has shown the following formula. If K_n is the unique subfield with $\mathrm{Gal}(K_n/k) \cong \mathbb{Z}/p^n\mathbb{Z}$ and p^{e_n} is the power of p dividing the class number of K_n, then there is an integer n_0 and integer ν such that

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

for $n \geq n_0$. If $d > 1$ then Cuoco and Monsky [2] have shown similar formulas for the class numbers of the subfields K_n of K with $\mathrm{Gal}(K_n/k) \cong (\mathbb{Z}/p^n\mathbb{Z})^d$. For instance if p^{e_n} is the power of p dividing the class number of K_n, they have shown there exist nonnegative integers m, ℓ such that

$$e_n = (\ell p + m p^n + O(1)) p^{(d-1)n}$$

as $n \to \infty$.

We can also consider the Λ-module $A_\infty = \varinjlim A_i$ under the lifting maps for ideal classes. A_∞ is a discrete abelian torsion p-group. If a nonprincipal ideal becomes principal when lifted to an extension field then it is said to capitulate. It is not hard to see that $A_\infty = 0$ if and only if every ideal class in each A_i capitulates in some number field in K.

In fact we have the following conjecture of Greenberg,

Conjecture. *If $\tilde{k}$ is the composite of all $\mathbb{Z}_p$-extensions of k then $A_\infty = 0$ for $\tilde{k}$.*

A_∞ being 0 for an extension K should, at least in general, be equivalent to Y_K being pseudo-null. Therefore we expect $Y_{\tilde{k}}$ to be pseudo-null. If k is a

totally real field, then Leopoldt's conjecture implies $\mathrm{Gal}(\tilde{k}/k) \cong \mathbb{Z}_p$ so then a Λ-module is pseudo-null if and only if it is finite and we expect $Y_{\tilde{k}}$ to be finite. In particular no number field k totally real or not has been found for which $Y_{\tilde{k}}$ is not pseudo-null.

If k is not totally real so that there is more than one $\mathbb{Z}_p$-extension of k, then Y_K where K is a $\mathbb{Z}_p$-extension of k, can be infinite. For instance take k to be an imaginary quadratic field and p to be a prime which splits in k into π_1 and π_2. Then within $\tilde{k}/k$, each of the inertia groups for π_1 and π_2 have $\mathbb{Z}_p$-rank one. Therefore since both π_1 and π_2 are ramified in k_∞/k, the extension $\tilde{k}/k_\infty$ is unramified and λ for Y_{k_∞} must be at least one and Y_{k_∞} has $\mathbb{Z}_p$-rank at least one.

In general if k is any totally complex field and p splits completely in k, then for any $\mathbb{Z}_p$-extension K/k in which all primes over p are ramified, we have $\lambda \geq \frac{1}{2}[k : \mathbb{Q}] = r_2$ for the module Y_K so Y_K contains a submodule isomorphic to $\mathbb{Z}_p^{r_2}$.

1.3 The Module X_K

If $K \subset \overline{Q}$ is again an algebraic extension of $\mathbb{Q}$, finite or infinite, let M_K be the maximal abelian pro-p extension of K unramified outside primes of K above p. We often say M_K/K is p-ramified. Clearly $L_K \subset M_K$. Let $X_K = \mathrm{Gal}(M_K/K)$. Again if K contains a subfield k such that $\mathrm{Gal}(K/k) \cong \mathbb{Z}_p^d$ then M_K is Galois over k and X_K is a $\Lambda = \Lambda_{K/k}$ module. Iwasawa [5] proved the following about X_K.

Theorem. (Iwasawa) *If k_∞ is the cyclotomic $\mathbb{Z}_p$-extension of a number field*

k, then X_{k_∞} is a finitely generated Λ-module, $\mathrm{rnk}_\Lambda X_{k_\infty} = r_2$ where r_2 is the number of complex places of k and X_{k_∞} contains no nonzero finite submodules.

Greenberg [4] using an induction argument proved the following extension.

Theorem. (Greenberg) *If k is a number field with $\mathrm{Gal}(K/k) \cong \mathbb{Z}_p^d$ for $d \geq 1$ and Leopoldt's conjecture is true for k and p, then X_K is a finitely generated Λ-module, $\mathrm{rnk}_\Lambda X_K = r_2$ and X_K contains no nonzero pseudo-null submodule.*

The last conclusion in the theorem is somewhat surprising. Note it is analogous to the statement in the first theorem since if $d = 1$, then a Λ-module is pseudo-null if and only if it is finite.

One question that arises is, is X_K torsion free. In the case of k being totally real, we have $r_2 = 0$ so if Leopoldt's conjecture holds for k and p, then X_K is a Λ-torsion module and when Y_K is nonzero X_K will be nonzero and thus is not torsion free. Now consider $\tilde{k}$ the composite of all $\mathbb{Z}_p$-extensions of k. If k contains the p-th roots of unity and Leopoldt's conjecture holds for k and p, then we will see later that $Y_{\tilde{k}}$ being pseudo-null in conjunction with a mild hypothesis on the decomposition groups for primes above p in $\tilde{k}$ will imply $X_{\tilde{k}}$ is torsion free. Therefore while $X_{\tilde{k}}$ can be non-torsion free at times when k is totally real, we expect to have $X_{\tilde{k}}$ torsion free a large part of the time otherwise.

1.4 The Extensions N and N'

Lastly we define two extensions which will appear later in our presentation. If k is a number field which contains the p-th roots of unity and $\mathrm{Gal}(K/k) \cong \mathbb{Z}_p^d$

with $k_\infty \subset K$, then we define N_K to be the extension of K gotten by adjoining all p-power roots of units of K and N'_K to be the extension of K gotten by adjoining all p-power roots of p-units of K. Under the conditions on K, K contains all p-power roots of units so N_K and N'_K are Kummer extensions of K and clearly $N_K \subset N'_K \subset M_K$.

Iwasawa [5] has shown the following theorem.

Theorem. *Let k contain the p-th roots of unity. Then if s is the number of primes above p in k_∞, then the torsion submodule of N'_{k_∞} is a free $\mathbb{Z}_p$-module and is isomorphic to $\mathbb{Z}_p^{s-1}$.*

We will see that $\widehat{A}_\infty$ can often be identified with $\mathrm{Gal}(M/N)$ so in the case K/k is a $\mathbb{Z}_p$-extension, $\mathrm{Gal}(M/N)$ is Λ-torsion. Thus $\mathrm{rnk}_\Lambda \mathrm{Gal}(N/K)$ must equal $\mathrm{rnk}_\Lambda \mathrm{Gal}(M/K)$. However it is still possible for $\mathrm{Gal}(N/K)$ not to be torsion free. In fact it is possible to have $N' = N$ and since Iwasawa's result says $\mathrm{Gal}(N'/K)$ has nontrivial torsion when $s > 1$, $\mathrm{Gal}(N/K)$ will in this case not be torsion free.

Chapter 2

Free pro-p Extensions

2.1 Introduction

The question of the existence of free pro-p extensions of number fields is a largely unexplored one. The purpose of this chapter is to show that a rank 3 free pro-3 extension does not exist for the number field $\mathbb{Q}(\sqrt{-31}, \sqrt{-3})$. Many of our results are much more general than we need for this specific case and will be proved in a quite general context. These techniques can thus be a basis for proving the nonexistence of free pro-p extensions in many cases. In these introductory comments we remark on some basic notions and results concerning free pro-p extensions of number fields.

One of the first things to note is that the rank of a free pro-p extension of a given number field k is bounded, that is if F is an extension of k which is Galois and $G = \mathrm{Gal}(F/k)$ is a free pro-p group, then there is a bound on how large the rank of G can be. Here we are considering G as a topological group where the rank of G is the cardinality of the smallest set of elements of G which generate a dense subgroup of G.

The rank of a free pro-p extension of k is in fact bounded, though usually probably rather weakly, by the degree of k over $\mathbb{Q}$. One can easily see this by noting that if F_d is a free pro-p group of rank d then the maximal abelian pro-p quotient of F_d is isomorphic to $\mathbb{Z}_p^d$ and by class field theory, k cannot have a $\mathbb{Z}_p^d$-extension if d is greater than the degree of k over $\mathbb{Q}$.

This in fact shows that if Leopoldt's conjecture holds for k and p, then the rank d is bounded by the much tighter bound r_2+1 where r_2 is the number of conjugate pairs of complex embeddings of k. One might wonder in this case if in fact there would always be a free pro-p extension of rank r_2+1. Yamagishi [16] has shown examples of number fields k which do not have a free pro-p extension of rank r_2+1 and has in fact given a formula for computing the maximal rank of a free pro-p extension for number fields satisfying certain conditions. If this rank is ρ then the exact statement is as follows,

Theorem. (Yamagishi) *Assume p is odd and k contains the p-th roots of unity. If there exists a prime v_0 of k which is undecomposed in the maximal pro-p extension of k unramified outside p, then the maximal rank of a free pro-p extension of k is*

$$\rho = r_2 + 1 - \frac{1}{2} \sum_{v|p, v \neq v_0} [k_v : \mathbb{Q}_p].$$

Yamagishi's examples are

1) $k = \mathbb{Q}(\sqrt{-\ell})$ where $\ell > 0$ is a prime number with $\ell \equiv 7 \bmod 8$ for the prime $p = 2$. Here $r_2 + 1 = 2$ but $\rho = 1$.

2) $k = \mathbb{Q}(\sqrt{-3}, \sqrt{-5})$ or $k = \mathbb{Q}(\sqrt{-3}, \sqrt{-26})$ with $p = 3$. Here $r_2 + 1 = 3$ but $\rho = 2$.

Yamagishi admits that the condition on v_0 is quite strong and that it in fact implies Leopoldt's conjecture for k and p. We are thus still far from

computing ρ in general and ρ appears to be a quite interesting and mysterious invariant. Since Shafarevich appears to be the first person to have made a general investigation leading to the computation of ρ for a number field [12], I will call ρ Shafarevich's invariant. For another work that has been used to determine this invariant we can also mention Wingberg's free product decomposition for Galois groups [14, 15] used by Yamagishi in his proof of the above formula.

It is a well known result due to Iwasawa [5] that a $\mathbb{Z}_p$-extension of a number field is unramified outside primes above p. Yamagishi [16] has extended this to free pro-p extensions of number fields,

Theorem. (Yamagishi) *If k is a number field then a free pro-p extension of k is unramified outside of p.*

Thus a free pro-p extension of a number field k is contained in the maximal pro-p extension of k unramified outside p.

While ρ need not equal $r_2 + 1$ even when Leopoldt's conjecture holds, Shafarevich has shown the following theorem [12]. This also appears in Movahhedi [9].

Theorem. (Shafarevich) *If p is a regular prime then the maximal pro-p extension unramified outside primes above p of $\mathbb{Q}(\zeta_{p^n})$ where ζ_{p^n} is a primitive p^n-th root of unity is a free pro-p group of rank $r_2 + 1$.*

Thus $\rho = r_2 + 1$ for $\mathbb{Q}(\zeta_{p^n})$ when p is regular. Movahhedi and Nguyen-Quang-Do call such a number field k for which the maximal pro-p extension unramified outside primes above p is a free pro-p group of rank r_2+1, p-rational [10]. Movahhedi [9] gives the following examples of p-rational fields. However Jannsen [6] gave the examples for $p \geq 5$ and $p = 3$ much earlier.

1) $k = \mathbb{Q}(\sqrt{-d})$ for $d > 0$ squarefree and $p \geq 5$. If $p \nmid h_k$ then k is p-rational and $\rho = r_2 + 1 = 2$.

2) For k as above and $p = 3$. If the completions of k at primes above 3 do not contain the third roots of unity, i.e. $d \not\equiv 3 \bmod 9$, then $3 \nmid h_k$ implies k is 3-rational and again $\rho = r_2 + 1 = 2$.

3) For k as above and $p = 2$. If 2 does not split in k, i.e. $d \not\equiv 7 \bmod 8$, then $2 \nmid h_k$ implies k is 2-rational and $\rho = r_2 + 1 = 2$.

Both authors further point out that Leopoldt's conjecture holds for any p-extension unramified outside p of these fields k. This thus gives infinite families of nonabelian extensions of $\mathbb{Q}$ for which Leopolt's conjecture holds.

We can also define a refinement of Shafarevich's invariant. Given a free pro-p extension K of k, we can ask what is the maximal rank of a free pro-p extension of k containing K. In one situation there is a simple answer to this.

Theorem. (Yamagishi [16]) *If k is a number field and Leopoldt's conjecture is true for a prime p and any finite p-extension of k unramified outside p and if also $\rho = r_2 + 1$ for k, then there is a unique F_ρ-extension F/k and any free pro-p extension of k is contained in F.*

Thus for such k and p, the maximal rank of a free pro-p extension containing any given free pro-p extension K of k is always simply $r_2 + 1$.

2.2 A Computation of Shafarevich's Invariant

We now want to show an example of a number field which satisfies Leopoldt's conjecture and where the a priori maximum value $r_2 + 1$ of Shafarevich's invariant is not attained. Yamagishi's formula will turn out not to apply to this

field and we will see how techniques of Iwasawa theory will show the value of Shafarevich's invariant for this field. The field is $k = \mathbb{Q}(\sqrt{-31}, \sqrt{-3})$ with the prime $p = 3$. We have k has degree $[k : \mathbb{Q}] = 4$ and since $\mathrm{Gal}(k/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is abelian, Leopoldt's conjecture holds for k, so with $r_1 = 0$, $r_2 = 2$ the maximal value for Shafarevich's invariant would be $r_2 + 1 = 3$. We will see however that this does not occur for the prime $p = 3$ and that Shafarevich's invariant for k and the prime 3 is actually 2. One can also see that Yamagishi's formula would predict Shafarevich's invariant for k and the prime 3 to be 1. However k contains $\mathbb{Q}(\sqrt{-3})$ and by Shafarevich's result Shafarevich's invariant for $\mathbb{Q}(\sqrt{-3})$ and the prime 3 is 2 so we see Shafarevich's invariant for k and 3 must be greater or equal to 2. This shows that in fact no prime of k remains undecomposed in the maximal pro-3 extension of k unramified outside of primes above 3.

Our proof will start out in a general setting. We will show that if k is a number field how $Y_{\tilde{k}}$ being pseudo-null, where $\tilde{k}$ is the composite of all $\mathbb{Z}_p$-extensions of k, can be used under certain circumstances to show Shafarevich's invariant for k is smaller than would be given by Leopoldt's conjecture. We will then show $Y_{\tilde{k}}$ being pseudo-null will follow from the pseudo-nullity of Y_f where $f = \mathbb{Q}(\sqrt{-31})$. The exact theorem is as follows,

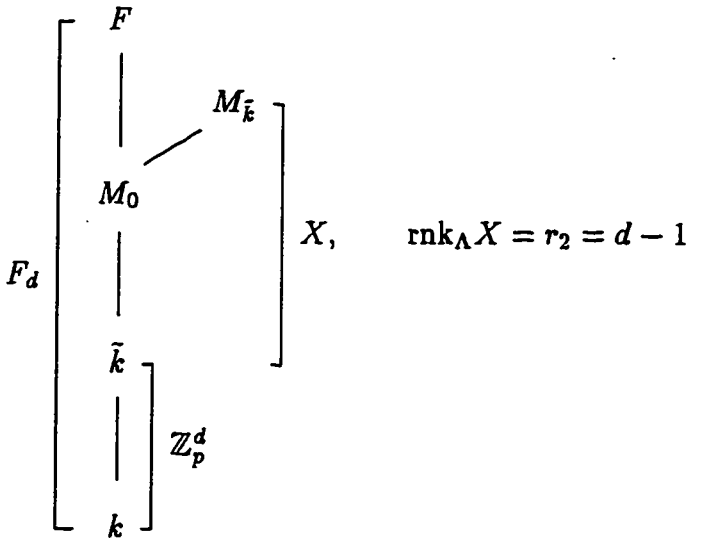
Theorem. *Let k be a number field which contains the p-th roots of unity for some prime p and for which Leopoldt's conjecture holds for the prime p. Let $\tilde{k}$ be the composite of all $\mathbb{Z}_p$-extensions of k and assume the decomposition group for each prime over p in k in $\mathrm{Gal}(\tilde{k}/k)$ has $\mathbb{Z}_p$-rank at least 2. If $Y_{\tilde{k}} \sim 0$ as a $\Lambda_{\tilde{k}/k}$-module and k has a cyclic degree p extension unramified outside primes above p which is not contained in $\tilde{k}$, then k does not have a free pro-p extension of rank $r_2 + 1$ where r_2 is the number of conjugate pairs of complex*

embeddings of k into the complex numbers.

In particular we will see that the field $K = \mathbb{Q}(\sqrt{-31}, \sqrt{-3})$ satisfies all the above conditions with the prime $p = 3$ showing that Shafarevich's invariant for K and $p = 3$ is less than 3. Since K has a rank 2 free pro-p extension coming from $\mathbb{Q}(\sqrt{-3})$, we see $\rho = 2$ for K.

We first show K has a cyclic degree 3 extension unramified outside 3 not contained in the composite of all $\mathbb{Z}_3$-extensions of K. Counting Kummer generators for such extensions of K, we find them coming from the class group of $\mathbb{Q}(\sqrt{-31})$ since the class number is 3, from the prime over 3, from the fundamental unit in the real quadratic subfield $\mathbb{Q}(\sqrt{93})$ of K and from the third root of unity in $\mathbb{Q}(\sqrt{-3})$. Thus there are four such Kummer generators but $\tilde{K}$ is only a $\mathbb{Z}_3^3$-extension of K showing what we want.

The proof of the above theorem will require a number of results. We start with an observation concerning free pro-p extensions.



Let k now be any number field which satisfies Leopoldt's conjecture for a prime p and let $\tilde{k}$ be the composite of all $\mathbb{Z}_p$-extensions of k so that $\mathrm{Gal}(\tilde{k}/k) \cong \mathbb{Z}_p^d$ where $d = r_2 + 1$ and assume that an extension F of k exists with $\mathrm{Gal}(F/k) \cong F_d$, the free pro-$p$ group on d generators. Then $\tilde{k}$ is the maximal abelian subextension of F/k and is the fixed field of F_d', the closure of the algebraic commutator subgroup of F_d. Now the maximal abelian subextension of $F/\tilde{k}$ will be the fixed field of F_d'', the second commutator subgroup of F_d. Call this M_0. If $M_{\tilde{k}}$ is the maximal abelian pro-p extension of $\tilde{k}$ unramified outside p, then it is easy to see that $M_{\tilde{k}} \cap F = M_0$ since a free pro-p extension is unramified outside p.

If $\Lambda = \mathbb{Z}_p[[\mathrm{Gal}(\tilde{k}/k)]]$, then $X = \mathrm{Gal}(M_{\tilde{k}}/\tilde{k})$ is a Λ-module in the usual way. By Greenberg [4], $\mathrm{rnk}_\Lambda X = r_2 = d - 1$. However we will show that $\mathrm{rnk}_\Lambda \mathrm{Gal}(M_0/\tilde{k}) = d - 1$ so $\mathrm{Gal}(M_{\tilde{k}}/M_0)$ must be Λ-torsion. We will also

show that $Y_{\tilde{k}}$ being pseudo-null will imply X is Λ-torsion free. This will show that $M_{\tilde{k}} \subset F$. Finally, if k has a cyclic p-power order extension unramified outside p not contained in $\tilde{k}$, then $M_{\tilde{k}}$ clearly cannot be contained in F. This contradiction will prove F cannot exist.

We now compute the rank of $\mathrm{Gal}(M_0/\tilde{k})$.

Proposition. *Let F_d be a free pro-p group of rank d and let $\Gamma = F_d/F_d'$. Then $X = F_d'/F_d''$ is a $\Lambda = \mathbb{Z}_p[[\Gamma]]$-module. We have X is Λ-torsion free and* $\mathrm{rnk}_\Lambda X = d - 1$.

Proof. According to Lyndon's resolution for the group Γ (see for instance Nguyen-Quang-Do [11] or Jannsen [6]) there's an exact sequence of Λ-modules,

$$0 \to X \to \Lambda^d \to \Lambda \to \mathbb{Z}_p \to 0.$$

Since X embeds in Λ^d, X is torsion free and since the image of Λ^d in Λ has Λ-rank 1, X must have Λ-rank $d - 1$. □

We now need to show that $Y_{\tilde{k}}$ being pseudo-null will under the above hypothesis on decomposition groups imply X is Λ-torsion free. We first show this for a general type of $\mathbb{Z}_p^d$-extension. Later we will apply this result to $\tilde{k}$. We start with a lemma.

Lemma. *Let k be any number field and K/k a $\mathbb{Z}_p^d$-extension for $d \geq 1$. Then $\widehat{A}_\infty$ is a torsion $\Lambda_{K/k}$-module and in particular $Y_K \sim 0$ implies $\widehat{A}_\infty \sim 0$ where $\widehat{A}_\infty$ is the Pontryagin dual of A_∞.*

Proof. We first note that Y_K is a torsion $\Lambda_{K/k}$-module by Greenberg [3] so the following argument will show $\widehat{A}_\infty$ is always torsion. Let $Y_K \sim 0$ and let $f, g \in \Lambda_{K/k}$ be two relatively prime annihilators of Y_K and let $\Gamma = \mathrm{Gal}(K/k)$. Let k_0 be the maximal unramified extension of k in K and let K_n be the

subfield of K with $\mathrm{Gal}(K_n/k_0) \cong (\mathbb{Z}/p^n\mathbb{Z})^d$. Clearly $A_\infty \cong \varinjlim_{n \geq n_0} A_n$ with A_n being the p-part of the class group of K_n. We wish to show the natural map $Y_K \to Y_{K_n}$ is surjective. To do this we show $Y_{K_n} \cap K_{n+1} = K_n$. We first note since k_0 is the maximal unramified extension of k contained in K, k_0 has no unramified extension contained in K. Now let K' be any cyclic degree p extension of K_n contained in K. Then $\mathrm{Gal}(K'/k_0) \cong (\mathbb{Z}/p^n\mathbb{Z})^{d-1} \times \mathbb{Z}/p^{n+1}\mathbb{Z}$ so K' is the composite of two extensions k' and F with $\mathrm{Gal}(k'/k_0) \cong \mathbb{Z}/p^{n+1}\mathbb{Z}$ and $\mathrm{Gal}(F/k_0) \cong (\mathbb{Z}/p^n\mathbb{Z})^{d-1}$. Now k'/k_0 must be fully ramified at some prime $\mathfrak{p}$ of k_0 over p. If P is a prime of K' over $\mathfrak{p}$ then when we lift k' to F, the inertia group of P in K'/F must have order at least p since the amount of ramification in k'/k_0 that can be lost is limited as $\mathrm{Gal}(F/k_0) \cong (\mathbb{Z}/p^n\mathbb{Z})^{d-1}$. Therefore K'/K_n is ramified at P so any cyclic degree p extension of K_n contained in K is ramified at some prime over p. Therefore $Y_{K_n} \cap K_{n+1} = K_n$ so we see f and g annihilate Y_{K_n} and $A_\infty \sim 0$.

If $\varphi \in \widehat{A}_\infty$ and $c \in A_\infty$ then Γ acts on φ by

$$(\gamma\varphi)(c) = \gamma\varphi(c\gamma^{-1})$$

for $\gamma \in \Gamma$. If we write $\Lambda \cong \mathbb{Z}_p[[T_1, \ldots, T_d]]$ and let the topological generator γ_i correspond to $T_i + 1$, then

$$\gamma_i^{-1} \leftrightarrow \frac{-T_i}{T_i + 1}$$

so $f(\frac{-T_1}{T_1+1}, \ldots, \frac{-T_d}{T_d+1})$ and $g(\frac{-T_1}{T_1+1}, \ldots, \frac{-T_d}{T_d+1})$ annihilate $\widehat{A}_\infty$ and can be seen to be relatively prime. □

Proposition. *Assume k contains the p-th roots of unity and let K/k be a $\mathbb{Z}_p^d$-extension for $d \geq 1$ which contains the cyclotomic $\mathbb{Z}_p$-extension of k. Let M be the maximal abelian pro-p extension of K unramified outside of p*

with $X = \mathrm{Gal}(M/K)$ *and let* $N = K(\{\sqrt[p^n]{\varepsilon} : \varepsilon \in R_K^{\times} \text{ and } n \geq 1\})$. *Then* $\widehat{A}_\infty \cong \mathrm{Gal}(M/N)$ *as* $\Lambda_{K/k}$*-modules.*

Proof. We define a map $\phi : \widehat{A}_\infty \to X$. Let $f : A_\infty \to W$ be an element of $\widehat{A}_\infty$ where W is the group of p power roots of unity. For each $n \geq 0$ let $P_n = \{\alpha \in K^{\times} : \sqrt[p^n]{\alpha} \in M\}$. If $\alpha \in P_n$ then since M/K is unramified outside of primes above p, $(\alpha) = \mathcal{A}^{p^n}\mathcal{B}$ for $\mathcal{A}$ an ideal in K_m for some m and $\mathcal{B}$ a product of ideals in K_m above p. Since all primes above p are ramified to arbitrarily high degree in K/k, in some $K_{m'}$, $\mathcal{B} = I^{p^n}$. Thus in $K_{m'}$, $(\alpha) = \mathcal{A}^{p^n}$ for some $\mathcal{A}$ in $K_{m'}$. If $c \in A_\infty$ is the class represented by $\mathcal{A}$, define $\phi(f) \in X$ by

$$\phi(f)(\sqrt[p^n]{\alpha}) = f(c)\sqrt[p^n]{\alpha}.$$

It is not hard to see this gives a well-defined element of X and that ϕ is a group homomorphism. It is also not hard to see $\phi(f)$ fixes N and that ϕ is a map of $\mathrm{Gal}(K/k)$-modules.

We now construct an inverse ψ for ϕ. If $g \in \mathrm{Gal}(M/N)$ and $c \in A_\infty$, let $\mathcal{A}$ be an ideal in c. For some n, $\mathcal{A}^{p^n} = (\alpha)$ will be principal. Define

$$\psi(g)(c) = g(\sqrt[p^n]{\alpha})/\sqrt[p^n]{\alpha}.$$

Since g fixes N it is not hard to see this is well defined and is an inverse to ϕ. □

Corollary. *If* $Y_K \sim 0$ *then* $M = N$.

Proof. We have $\widehat{A}_\infty \cong \mathrm{Gal}(M/N)$ but since $Y_K \sim 0$, we know $\widehat{A}_\infty \sim 0$ and under the hypothesis on K, $\mathrm{Gal}(M/K)$ has no nonzero pseudo-null submodules by Greenberg [4]. □

We now need to assume that for each prime P in k lying over p, the decomposition group for P in $\mathrm{Gal}(K/k)$ has $\mathbb{Z}_p$-rank at least 2. This would seem likely always to be the case if $\mathrm{Gal}(K/k)$ itself has $\mathbb{Z}_p$-rank at least 2 and K contains the cyclotomic $\mathbb{Z}_p$-extension. We can now prove the following theorem.

Let W be the group of all p-power roots of unity. If K is an algebraic extension of $\mathbb{Q}$ containing W, let E_K be the group of p-units of K. Let $N_K = K(\{\sqrt[p^n]{\alpha} : \alpha \in E_K \text{ and } n \geq 1\})$. We now want to prove the torsion submodule of $\mathrm{Gal}(N_K/K)$ is pseudo-null in a fairly general situation where K is a $\mathbb{Z}_p^d$-extension of k. We start with the following theorem.

Theorem. *Let k contain the p-th roots of unity and let $\mathrm{Gal}(K/k) \cong \mathbb{Z}_p^d$ where $d \geq 2$ and K contains the cyclotomic $\mathbb{Z}_p$-extension k_∞ of k. Let K_m be the unique subfield of K with $\mathrm{Gal}(K_m/K) \cong (\mathbb{Z}/p^m\mathbb{Z})^d$ and let $N_m = N_{K_m k_\infty}$ and $X_m = \mathrm{Gal}(N_m/K_m k_\infty)$. Let $N = N_K$ and $X = \mathrm{Gal}(N/K)$. Then $\mathrm{rnk}_{\Lambda_{K/k}} X = r_2$ and $t(X) \subset \varprojlim t(X_m)$ where $t(X)$ is the torsion submodule of X.*

Proof. Let M be the maximal abelian p-ramified p-extension of K and let $N_0 = K(\{\sqrt[p^n]{\varepsilon} : \varepsilon \in R_K^\times \text{ and } n \geq 1\})$. We know $\hat{A}_\infty \cong \mathrm{Gal}(M/N_0)$ as $\Lambda_{K/k}$-modules and $\hat{A}_\infty$ is torsion so we must have $\mathrm{rnk}\, X = \mathrm{rnk}\, \mathrm{Gal}(M/K)$ and by Greenberg [4], $\mathrm{rnk}\, \mathrm{Gal}(M/K) = r_2$.

To show that $t(X) \subset \varprojlim t(X_m)$, let $\overline{N}$ be the fixed field of $t(X)$ and $\overline{N}_m$ be the fixed field of $t(X_m)$. We will show $K\overline{N}_m \subset \overline{N}$ by a rank argument. First let $k_\infty = K_1' \subset K_2' \subset \ldots \subset K_d' = K$ be a sequence of fields such that $\mathrm{Gal}(K_i'/k) \cong \mathbb{Z}_p^i$ for $1 \leq i \leq d$ and write $\Lambda_i = \Lambda_{K_i'/k} = \mathbb{Z}_p[[T_1, T_2, \ldots, T_i]]$. Let $X_0 = X/t(X)$. We know X_0 is contained in $\Lambda_d^{r_2}$ with finite index so

$$\Lambda_d^{r_2}/X_0 \twoheadrightarrow \Lambda_d^{r_2}/(X_0 + T_d\Lambda_d^{r_2}) \cong \frac{\Lambda_d^{r_2}/T_d\Lambda_d^{r_2}}{(X_0 + T_d\Lambda_d^{r_2})/T_d\Lambda_d^{r_2}} \cong \frac{\Lambda_d^{r_2}/T_d\Lambda_d^{r_2}}{X_0/(X_0 \cap T_d\Lambda_d^{r_2})} \cong$$

$$\frac{\Lambda_{d-1}^{r_2}}{X_0/(X_0 \cap T_d \Lambda_d^{r_2})}$$

and thus the last term is finite. But $X_0/T_dX_0 \twoheadrightarrow X_0/(X_0 \cap T_d\Lambda_d^{r_2})$ is onto so X_0/T_dX_0 has a quotient which is a rank r_2 torsion-free Λ_{d-1}-module. It follows then that $\overline{N}$ contains $K\overline{N}_{d-1}$. Similarly we find $\overline{N}_{d-1}$ contains $K'_{d-1}\overline{N}_{d-2}$ and so on. Therefore $\overline{N}$ contains $K\overline{N}_1$. Now considering K as a $\mathbb{Z}_p^d$-extension of K_m, it is clear that $\overline{N}$ contains $K\overline{N}_m$ for all m so we're done. □

Theorem. *Let $Y = t(X_m)$. Then $(Y(-1) \otimes \mathbb{Q}_p) \oplus \mathbb{Q}_p \cong \oplus_{i=1}^{g} \mathrm{Ind}_{D_i}^{G_m} \mathbb{Q}_p$ where $\mathbb{Q}_p$ is the trivial module.*

Proof. By the theorem of Iwasawa [5, section 8.3], X_m is a free $\mathbb{Z}_p$-module and

$$X_m \subset \Lambda^{r_2 p^{md}} \oplus \mathbb{Z}_p^{s_m - 1}$$

where the containment is of finite index and s_m is the number of primes above p in $K_m k_\infty$. If we let n_0 be large enough so that the number of primes above p in K_{m,n_0} is s_m, then $\mathrm{Gal}(K_m k_\infty / K_{m,n_0})$ will act trivially on $Y(-1) \cong \mathbb{Z}_p^{s_m-1}(-1)$ so if γ is a topological generator of $\mathrm{Gal}(K_m k_\infty / K_m)$ and if

$$\overline{X} = X_m(-1)/(\gamma^{p^{n_0}} - 1)X_m(-1)$$

then

$$\overline{X} \sim \mathbb{Z}_p^{r_2 p^{md} p^{n_0}} \oplus \mathbb{Z}_p^{s_m - 1}.$$

As $\Lambda \cong \Lambda(-1)$, we have

$$\Lambda(-1)/(\gamma^{p^{n_0}} - 1)\Lambda(-1) \cong \mathbb{Z}_p[\overline{\Gamma}]$$

as $\overline{\Gamma}$-modules where $\overline{\Gamma} = \Gamma/\Gamma^{p^{n_0}}$. Therefore

$$\overline{X} \sim \mathbb{Z}_p[\overline{\Gamma}]^{r_2 p^{md}} \oplus \mathbb{Z}_p^{s_m - 1}$$

and

$$(*) \qquad (\overline{X} \otimes \mathbb{Q}_p) \oplus \mathbb{Q}_p \cong \mathbb{Q}_p[\overline{\Gamma}]^{r_2 p^{md}} \oplus \mathbb{Q}_p^{s_m}.$$

We now look at X_m with Kummer theory. Let $E \subset (K_m k_\infty)^\times$ be the group of p-units and let $\mathcal{E} = E \otimes \mathbb{Q}_p/\mathbb{Z}_p$. Then there is a perfect pairing of G_m-modules

$$X_m \times \mathcal{E} \to W$$

where W is the group of p-power roots of unity and we can write a perfect pairing

$$X_m(-1) \times \mathcal{E} \to \mathbb{Q}_p/\mathbb{Z}_p$$

where G_m acts trivially on $\mathbb{Q}_p/\mathbb{Z}_p$. Taking Γ_0-invariants of $\mathcal{E}$ we get a perfect pairing

$$\overline{X} \times \mathcal{E}^{\Gamma_0} \to \mathbb{Q}_p/\mathbb{Z}_p.$$

But $\mathcal{E}^{\Gamma_0}$ is just $E' \otimes \mathbb{Q}_p/\mathbb{Z}_p$ where E' is the free part of the group of p-units of K_{m,n_0}. We then have $E' \cong E_0 \otimes E_p$ where E_0 is the free part of the units of K_{m,n_0} of rank $r_2 p^{md} p^{n_0} - 1$ and E_p is a free $\mathbb{Z}$-module of rank s_m consisting of p-units. It is not hard to see this is a direct sum of G_m-modules. We also have $(E_0 \otimes \mathbb{Q}_p) \oplus \mathbb{Q}_p \cong \mathbb{Q}_p[\overline{\Gamma}]^{r_2 p^{md}}$ as $\overline{\Gamma}$-modules and, looking at the G_m-action on the primes of K_{m,n_0} above p, that $E_p \otimes \mathbb{Q}_p \cong \oplus_{i=1}^{g} \mathrm{Ind}_{D_i}^{G_m} \mathbb{Q}_p$ as G_m-modules.

Since

$$\overline{X} \cong \mathrm{Hom}(E' \otimes \mathbb{Q}_p/\mathbb{Z}_p, \mathbb{Q}_p/\mathbb{Z}_p) \cong E' \otimes \mathbb{Z}_p,$$

we have

$$(\overline{X} \otimes \mathbb{Q}_p) \oplus \mathbb{Q}_p \cong (E' \otimes \mathbb{Q}_p) \oplus \mathbb{Q}_p \cong \mathbb{Q}_p[\overline{\Gamma}]^{r_2 p^{md}} \oplus \oplus_{i=1}^{g} \mathrm{Ind}_{D_i}^{G_m} \mathbb{Q}_p.$$

Comparing this with $(*)$, we see

$$\mathbb{Q}_p^{s_m} \cong \oplus_{i=1}^{g} \mathrm{Ind}_{D_i}^{G_m} \mathbb{Q}_p$$

so the theorem follows. □

Theorem. *Let k contain the p-th roots of unity, $\mathrm{Gal}(K/k) \cong \mathbb{Z}_p^d$ for $d \geq 2$ where K contains k_∞ and assume for each prime of k above p, its decomposition group in $\mathrm{Gal}(K/k)$ has $\mathbb{Z}_p$-rank at least two. Let N and X be as in the last two theorems and let $\Lambda = \Lambda_{K/k}$. Then $t(X)$ is pseudo-null as a Λ-module.*

Proof. Let $P_1, \ldots, P_g$ be the primes of k lying over p and let $\mathcal{D}_i$ be the decomposition group for P_i in $G = \mathrm{Gal}(K/k)$. Let $\sigma, \tau \in \mathcal{D}_i$ be such that the subgroup of $\mathcal{D}_i$ generated by σ and τ is $\mathbb{Z}_p^2$ and let K_m, G_m, D_i and X_m be as before. Then it is clear that $\sigma - 1$ and $\tau - 1$ annihilate $\mathrm{Ind}_{\mathcal{D}_i}^G \mathbb{Z}_p$ and are relatively prime so $\mathrm{Ind}_{\mathcal{D}_i}^G \mathbb{Z}_p$ is a pseudo-null Λ-module. Therefore $\oplus_{i=1}^g \mathrm{Ind}_{\mathcal{D}_i}^G \mathbb{Z}_p$ is pseudo-null. Now let $S, T \in \Lambda$ be two relatively prime annihilators of $\oplus_{i=1}^g \mathrm{Ind}_{\mathcal{D}_i}^G \mathbb{Z}_p$. Since under the restriction map from G to G_m, $\mathcal{D}_i$ maps onto D_i, it is not hard to see there is a surjection

$$\Lambda_G \otimes_{\Lambda_{\mathcal{D}_i}} \mathbb{Z}_p \twoheadrightarrow \Lambda_{G_m} \otimes_{\Lambda_{D_i}} \mathbb{Z}_p.$$

and thus S and T also annihilate $\oplus_{i=1}^g \mathrm{Ind}_{D_i}^{G_m} \mathbb{Z}_p$ and therefore annihilate $t(X_m)$. But $t(X) \subset \varprojlim t(X_m)$ so S and T annihilate $t(X)$ as desired. □

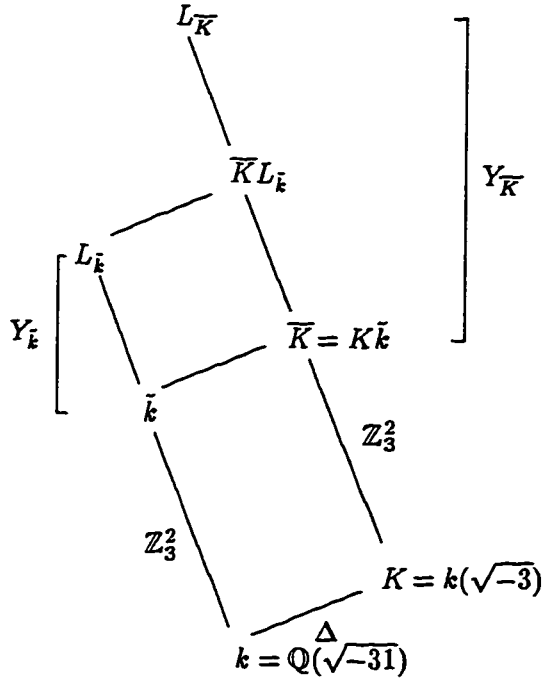
2.3 The Pseudo-nullity of $Y_{\tilde{K}}$

If k is now any algebraic extension of $\mathbb{Q}$, let L_k be the maximal unramified abelian 3-extension of k with $Y_k = \mathrm{Gal}(L_k/k)$. If there is an order two group which acts on Y_k, we let $Y_k^{\pm}$ be the trivial and nontrivial parts of Y_k with $L_k^{\pm}$ the maximal subfields of L_k which are acted on trivially and nontrivially. The same notation will be used on other Galois groups.

Let $k = \mathbb{Q}(\sqrt{-31})$ and $K = k(\sqrt{-3})$. In this section we show that $Y_{\tilde{K}}$ is pseudo-null given that $Y_{\tilde{k}}$ is pseudo-null. The fact that $Y_{\tilde{k}}$ is pseudo-null was

proved in the thesis of J. Minardi [8]. For completeness, we will give his proof in an appendix. Let $\overline{K} = K\tilde{k}$. Our proof will consist of showing that $Y_{\tilde{k}} \sim 0$ implies $Y_{\overline{K}} \sim 0$ and then showing this implies $Y_{\tilde{K}} \sim 0$.

To show that $Y_{\overline{K}} \sim 0$ we note that $\Delta = \mathrm{Gal}(K/k)$ acts on $Y_{\overline{K}}$, splitting it into a direct sum, $Y_{\overline{K}} = Y_{\overline{K}}^{+} \oplus Y_{\overline{K}}^{-}$. We will show $Y_{\overline{K}}^{+} \cong Y_{\tilde{k}}$ and $Y_{\overline{K}}^{-} = 0$ so $Y_{\overline{K}} \sim 0$ follows.



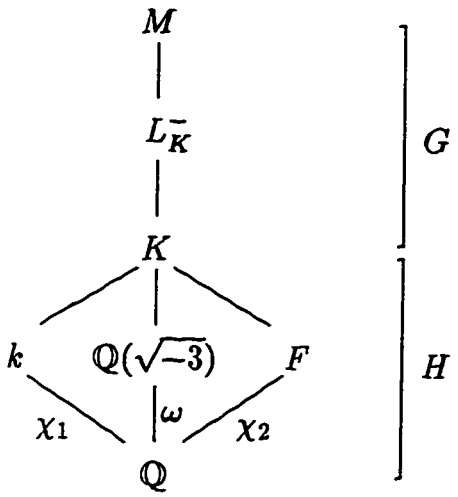
If we lift $L_{\tilde{k}}$ to $\overline{K}$ then it is clear $\mathrm{Gal}(\overline{K}L_{\tilde{k}}/\tilde{k}) \cong Y_{\tilde{k}}$ so we can consider $Y_{\tilde{k}}$ as a module over $\Lambda_{\overline{K}/K}$.

Lemma. *We have $Y_{\overline{K}}^{+} \cong Y_{\tilde{k}}$ and $Y_{\overline{K}}^{+} \sim 0$ as modules over $\Lambda_{\overline{K}/K}$.*

Proof. It is clear that $\overline{K}L_{\tilde{k}} = L_{\overline{K}}^{+}$ so we have $Y_{\overline{K}}^{+} \cong Y_{\tilde{k}}$ and $Y_{\overline{K}}^{+} \sim 0$ follows immediately. □

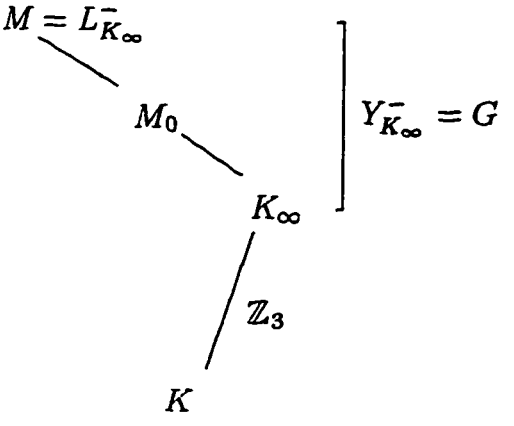
Lemma. $Y_{\overline{K}}^{-} = 0$.

Proof. We will do this in three steps. In order, we will show L_K^-, $L_{K_\infty}^-$ and then $L_{\overline{K}}^-$ all are trivial extensions. Here K_∞ is the cyclotomic $\mathbb{Z}_3$-extension of K.

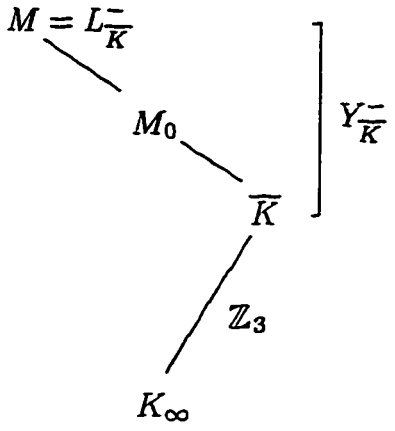


Step 1. We first show L_K^- is trivial using characters. Let $M = L_K$, the 3-Hilbert class field of K, and let $G = \mathrm{Gal}(M/K)$ and $H = \mathrm{Gal}(K/\mathbb{Q})$. Let $G' = G/G^3$ and let $L = M^{G^3}$ so that $\mathrm{Gal}(L/K) \cong G'$. Let χ_0, ω, χ_1 and χ_2 be the characters of H whose kernels have fixed fields $\mathbb{Q}$, $\mathbb{Q}(\sqrt{-3})$, k and the real quadratic subfield F of K respectively. If ε is any of the above characters let G^ε be the maximal subgroup of G for which $\ker \varepsilon$ is the exact subgroup of H fixing it. Then $G = G^{\chi_0} \oplus G^{\omega} \oplus G^{\chi_1} \oplus G^{\chi_2}$ as a direct sum of H-modules. If G^+ is the subgroup of G on which $\mathrm{Gal}(K/k)$ acts trivially then $G^+ = G^{\chi_0} \oplus G^{\chi_1}$. Therefore $L^- = L^{G^+}$ is the maximal subextension of L on which $\mathrm{Gal}(K/k)$ acts nontrivially. But L^- is the composite of L_ω and L_{χ_2}, the maximal subextensions of L for which $\ker \omega$ and $\ker \chi_2$ are precisely the subgroups of H acting trivially on their Galois groups so L_ω and L_{χ_2} are lifts of unramified abelian extensions of $\mathbb{Q}(\sqrt{-3})$ and F. However $\mathbb{Q}(\sqrt{-3})$ and $F = \mathbb{Q}(\sqrt{69})$ both have class number one so they both have no unramified

abelian extensions. L_K^- then must be trivial.



Step 2. For ease of notation let $M = L_{K_\infty}^-$ and $G = Y_{K_\infty}^-$. Then M is Galois over K. Let $\gamma_0 \in \mathrm{Gal}(K_\infty/K)$ be a topological generator of $\mathrm{Gal}(K_\infty/K)$ and let M_0 be the fixed field of $(\gamma_0 - 1)G$. Then M_0 is the maximal abelian extension of K contained in M. By the theory of p-groups, $(\gamma_0 - 1)G$ is not all of G so M_0/K_∞ is a nontrivial extension. Since 3 remains inert in $k/\mathbb{Q}$ and is ramified in K/k there is only one prime over 3 in K. Call this prime P and let I_P be the inertia group for P in $\mathrm{Gal}(M_0/K)$. The fixed field M' of I_P will now be an unramified abelian 3-extension of K on which Δ acts nontrivially. However there are no such extensions of K so $M = K_\infty$ and $L_{K_\infty}^-$ is trivial.

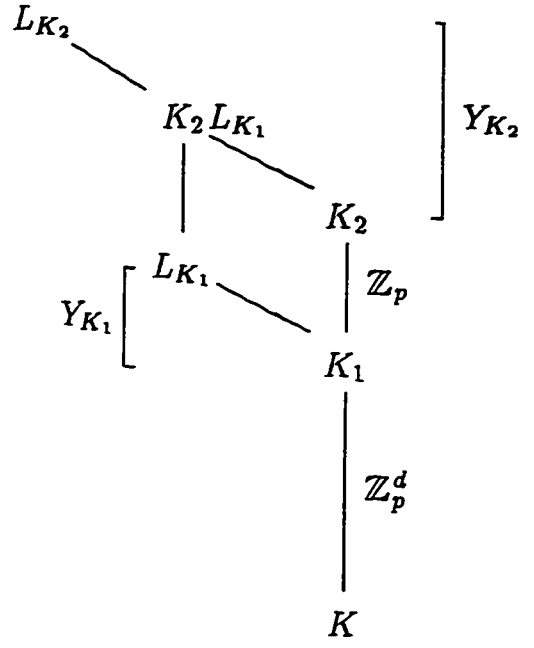


Step 3. Now let $M = L_{\overline{K}}^-$. As before M/K_∞ is Galois and if M_0 is the maximal abelian extension of K_∞ contained in M, then M_0/K_∞ is nontrivial. But there is only one prime above 3 in K_∞ so again $L_{K_\infty}^-$ would be nontrivial. Since $L_{K_\infty}^- = K_\infty$, we must have $L_{\overline{K}}^-$ is trivial so $Y_{\overline{K}}^- = 0$. □

Putting the last two lemmas together, we get

Theorem. *$Y_{\overline{K}} \sim 0$ over $\Lambda_{\overline{K}/K}$.*

Proof. We know $Y_{\overline{K}} \cong Y_{\overline{K}}^+ \oplus Y_{\overline{K}}^- \cong Y_k^-$. But $Y_k^- \sim 0$ so $Y_{\overline{K}} \sim 0$ follows immediately. □



The last step is to show $Y_{\overline{K}} \sim 0$ implies $Y_{\tilde{K}} \sim 0$. We do this with an inductive type argument. We show if K_2/K is a $\mathbb{Z}_p^{d+1}$-extension which contains a $\mathbb{Z}_p^d$-extension K_1/K, then under a suitable condition on decomposition groups $Y_{K_1} \sim 0$ implies $Y_{K_2} \sim 0$. We then apply this to the extension $\tilde{K}/K$ which contains $\overline{K}/K$. For any integer $r \geq 1$, let $\Lambda_r = \mathbb{Z}_p[[T_1, T_2, \ldots, T_r]]$.

Proposition. *Let K_1 be a $\mathbb{Z}_p^d$-extension of a number field K for $d \geq 2$ which is contained in a $\mathbb{Z}_p^{d+1}$-extension K_2 of K. Assume Y_{K_1} is pseudo-null and for every prime over p in K, assume its decomposition group in $\mathrm{Gal}(K_1/K)$ has $\mathbb{Z}_p$-rank at least 2. Then Y_{K_2} is also pseudo-null.*

Proof. We can assume in $\Lambda_{d+1} = \mathbb{Z}_p[[T_1, \ldots, T_{d+1}]]$ that $T_{d+1} = \gamma - 1$ where γ is a topological generator of $\mathrm{Gal}(K_2/K_1)$. Then $Y_{K_2}/T_{d+1}Y_{K_2} \cong \mathrm{Gal}(F/K_1)$ where F is the maximal abelian extension of K_1 contained in L_{K_2}. Let $\mathcal{I}$ be

the sum of the inertia groups in $\mathrm{Gal}(F/K_1)$ of the primes of K_1 lying over p. Note that $\mathcal{I}$ is a finitely generated module over Λ_d and the fixed field of $\mathcal{I}$ is L_{K_1}.

We now show $\mathcal{I} \sim 0$. Let P be a prime of k lying over p and let $\mathcal{D}$ be the decomposition group of P in $\mathrm{Gal}(K_1/k)$. Let $\sigma, \tau \in \mathcal{D}$ be two elements for which the closures of the subgroups they generate have trivial intersection. Choose a prime P_1 of K_1 lying above P and let $\mathcal{I}_1$ be its inertia group in $\mathrm{Gal}(F/K_1)$. Note that $\mathcal{I}_1$ has at most rank one as $\mathbb{Z}_p$-module. As $\mathcal{D}$ acts on $\mathcal{I}_1$, and in fact acts trivially since $\mathcal{I}_1$ injects into $\mathrm{Gal}(K_2/K_1)$ and $\mathrm{Gal}(K_2/k)$ is abelian, $f = \sigma - 1$ and $g = \tau - 1$ annihilate $\mathcal{I}_1$.

If P_2 is another prime of K_1 lying above P, let $\mathcal{I}_2$ be its inertia group in $\mathrm{Gal}(F/K_1)$. It can be seen that f and g also annihilate $\mathcal{I}_2$. Since f and g will be relatively prime, the sum of all inertia groups of primes over P in $\mathrm{Gal}(F/K_1)$ is pseudo-null. Then $\mathcal{I}$ is the sum of a finite number of pseudo-null modules so the following lemma will show $\mathcal{I} \sim 0$ and applying the lemma one more time will show $\mathrm{Gal}(F/K_1) \sim 0$.

Lemma. *Let $\Lambda = \Lambda_d$ for $d \geq 1$ and let the following*

$$0 \to M_1 \to M_2 \to M_3 \to 0$$

be a short exact sequence of Λ-modules. If $M_1 \sim 0$ and $M_3 \sim 0$ then $M_2 \sim 0$.

Proof. M_2 is finitely generated since M_1 and M_3 are. Let $P \subset \Lambda$ be a prime ideal of height ≤ 1. Since localizing is exact,

$$0 \to M_{1,P} \to M_{2,P} \to M_{3,P} \to 0$$

is also exact. Since, by definition, if $M \sim 0$ then $M_P = 0$ for every prime ideal of height ≤ 1, $M_{1,P} = M_{3,P} = 0$, so we have $M_{2,P} = 0$. Thus $M_2 \sim 0$. □

Finally by the following lemma, we see that $\mathrm{Gal}(F/K_1)$ being pseudo-null implies Y_{K_2} is pseudo-null proving the proposition. □

Lemma. *Let $\Lambda = \Lambda_{d+1}$ for an integer $d \geq 0$ and let $T = T_{d+1}$. If M is a finitely generated Λ-module, then $M/TM \sim 0$ as a Λ_d-module implies $M \sim 0$.*

Proof. Let $f, g \in \Lambda_d$ be relatively prime annihilators of M/TM. If $x_1, \ldots, x_n$ generate M, then $fx_i, gx_i \in TM$ so let

$$fx_i = \sum_{k=1}^{n} a_{ik}x_k$$

and

$$gx_i = \sum_{k=1}^{n} b_{ik}x_k$$

with $T \mid a_{ik}$ and $T \mid b_{ik}$.

If

$$\mathcal{A} = (a_{ik})_{ik} - fI_n$$

and

$$\mathcal{B} = (b_{ik})_{ik} - gI_n$$

where I_n is the $n \times n$ identity matrix then

$$\mathcal{A}x_i = 0$$

$$\mathcal{B}x_i = 0, \quad \text{for } 1 \leq i \leq n,$$

where we now represent x_i as an n-tuple.

Thus $\det \mathcal{A}$ and $\det \mathcal{B}$ annihilate M so we just need to show $\det \mathcal{A}$ and $\det \mathcal{B}$ are relatively prime. Let $f_1 = \det \mathcal{A}$ and $g_1 = \det \mathcal{B}$. Then

$$\tilde{f}_1 = f^n$$

and

$$\tilde{g}_1 = g^n$$

where $\tilde{\alpha}$ denotes the reduction of an element $\alpha \in \Lambda$ in $\Lambda/T\Lambda$. Since f and g are relatively prime, $\tilde{f}_1$ and $\tilde{g}_1$ are too. Any common factor h of f_1 and g_1 would then have its reduction $\tilde{h}$ be a unit. Therefore the constant term of $\tilde{h}$ is in $\mathbb{Z}_p^\times$ so the constant term of h is also in $\mathbb{Z}_p^\times$ and h is a unit. Thus f_1 and g_1 are relatively prime. □

Finally we have

Theorem. *If* $K = \mathbb{Q}(\sqrt{-31}, \sqrt{-3})$ *then* $Y_{\tilde{K}} \sim 0$.

Proof. Apply the above proposition to $K_2 = \tilde{K}$ and $K_1 = \overline{K}$. □

2.4 Consequences

We now know that $K = \mathbb{Q}(\sqrt{-31}, \sqrt{-3})$ has no rank 3 free pro-3 extension. There are though a number of questions which are still unanswered. Although we know K has a rank 2 free pro-3 extension coming from $\mathbb{Q}(\sqrt{-3})$ by either the result of Shafarevich or the result of Jannsen and one coming from $\mathbb{Q}(\sqrt{-31})$ by Jannsen, does K have other rank 2 free pro-3 extensions? Does every rank 2 free pro-3 extension of K contain K_∞? Is every $\mathbb{Z}_3$-extension of K contained in a rank 2 free pro-3 extension or what is the set of such $\mathbb{Z}_3$-extensions?

Chapter 3

Some Computations with Dihedral Extensions of $\mathbb{Q}$

We present in this chapter computer calculations done to investigate the occurrence of capitulation in a certain family of number fields. It appears these types of calculations have never been done before and it is hoped this investigation will lead to an understanding of capitulation and its relation to class groups in this setting and other settings. The calculations were mostly done with the KANT program running the KASH shell [7] and I wish to thank greatly the support of the people in the KANT group.

3.1 Introduction

We start with the field $k = \mathbb{Q}(\sqrt{-23})$ which has class number 3 and is the first imaginary quadratic field with a class group with nontrivial 3-part. We first point out that it can be shown that the Hilbert class field of k is the first layer

of the anticyclotomic $\mathbb{Z}_3$-extension of k. This chapter is concerned with the family of cyclic degree three extensions L of k which are Galois over $\mathbb{Q}$ and for which $\mathrm{Gal}(L/\mathbb{Q}) \cong S_3$, the symmetric group on three letters. Since there are two possible Galois groups for a degree six extension of $\mathbb{Q}$, either $\mathbb{Z}/6\mathbb{Z}$ which is abelian or S_3 which is a dihedral group, we will refer to such extensions L as being dihedral over $\mathbb{Q}$. Our main question is, does the order three ideal class of k capitulate in L. This means that if we take any ideal of order three in the ideal class group $\mathcal{C}_k$ of k, then it will become principal when lifted to L. Actually k has two ideal classes of order three, but as the lifting map on ideals gives a homomorphism on ideal class groups, $\mathcal{C}_k \to \mathcal{C}_L$, both ideal classes will capitulate together if either does.

There is an argument using the fact that L is dihedral over $\mathbb{Q}$ that indicates that if capitulation does not take place from k to L, then the 3-part of $\mathcal{C}_L$ would have to have order at least 27. Since it seems that this would make the 3-part of $\mathcal{C}_L$ larger than might be expected commonly to occur, this might indicate capitulation in such extensions is fairly common. We have found that in no case where capitulation does not occur, is the order of the 3-part of $\mathcal{C}_L$ less than 27, verifying the expectation above. We have however found out that for a large class of these extensions, certain ones in which two or more rational primes are ramified, capitulation does not occur. This will be described below.

To find such extensions L, we did a search that yielded a total of 137 extensions. We list data for a certain set of these extensions in a table at the end of the chapter. These fields were found by doing a search of cubic integral polynomials, $f = x^3 + ax^2 + bx + c$, whose discriminant was equal to -23 up to a square. Then, if α is a root of f, the field $L = k(\alpha)$ will be dihedral of order 6 over $\mathbb{Q}$. To reduce the search we can take a to be nonnegative because $-\alpha$ is a root of $x^3 - ax^2 + bx - c$. The above search was done by taking $0 \leq a \leq 200$

and $-200 \leq b, c \leq 200$ for a search of just over 32 million cubic polynomials. The fields we list are listed in order of increasingly negative discriminant and we will often refer to these fields L by the rational primes which ramify in L/k. This is sufficient to identify which primes are ramified from k to L since, as L is Galois over $\mathbb{Q}$, all primes of L over a given rational prime are ramified from k to L if any of them are ramified.

It will be noticed that the fields come in groups of up to three with the same discriminant. It is easy to see there will always be at least three fields with the same discriminant since if L is one such field and H is the Hilbert class field of k, then LH/k is a type $(3,3)$ extension so there are two additional extensions of k, L_1 and L_2, that are contained in LH and it is easy to see both L_1 and L_2 will be dihedral of order 6 over $\mathbb{Q}$ and have the same discriminant as L. One can also see by class field theory or by the use of ray class fields as we do below, that if only a single rational prime is ramified in the extension L/k, then there are always only three such fields. However with two or more rational primes ramified in the extension L/k, there are cases where there are arbitrarily many such extensions with exactly those primes ramified.

3.2 Primes of the First and Second Type

The first thing to notice about the rational primes p that are ramified in these extensions L/k, is that whenever $p \equiv 1 \bmod 3$, then p is split in $k/\mathbb{Q}$ and whenever $p \equiv 2 \bmod 3$, then p remains inert in $k/\mathbb{Q}$. This can be explained fairly simply be class field theory or by looking locally. If $p \equiv 1 \bmod 3$ and p remains inert in $k/\mathbb{Q}$, then it can be seen that all ramified cyclic degree three extensions of the completion of k at the prime above p are abelian over $\mathbb{Q}_p$.

Also if $p \equiv 2 \bmod 3$ and p splits in $k/\mathbb{Q}$, then it is easy to see $\mathbb{Q}_p$ has no ramified cyclic degree 3 extensions. Thus in both cases k has no cyclic degree three extensions ramified only at p which are dihedral over $\mathbb{Q}$. Primes p for which $p \equiv 1 \bmod 3$ and which are split in k or for which $p \equiv 2 \bmod 3$ and which remain inert in k and the prime 3 will all be called admissible primes. It will be noted below that the converse to the above statement holds, if p is an admissible prime then such extensions L of k exist in which p is ramified.

The next thing we note about the primes that ramify in these fields is that there is no example of any field L in which the prime 23 is ramified from k to L. This can again be explained by looking locally and we shall in fact show there is no S_3-extension of $\mathbb{Q}_{23}$ which is fully ramified. If F is a degree two extension of $\mathbb{Q}_{23}$ which is ramified, then since the residue class field of O_F is $\mathbb{F}_{23}$, the field with 23 elements, 3 does not divide the group of roots of unity in O_F and F has no ramified degree three extensions at all.

We now come to the question, when does an extension L of k exist in which only one given rational prime is ramified in L/k. Since we have already seen the prime cannot be 23, there are two possibilities, the rational prime p may remain inert or may be split in $k/\mathbb{Q}$. We will develop a criterion for when such an extension L/k can exist which is ramified only at the given prime p.

We start with the following proposition which calculates ray class groups and a corollary which computes their order in the case we are interested in.

Proposition. *Let K be a number field, m a nonzero ideal in O_K and F the ray class field of K with conductor m. Let $G = (O_K/m)^\times$ and let $\overline{E}$ be the image of the totally positive units of O_K, i.e. $\{\varepsilon \in O_K^\times : \sigma(\varepsilon) > 0$ for all real embeddings σ of K into $\mathbb{C}\}$, in G. Then there is a short exact sequence*

$$0 \to G/\overline{E} \to \mathrm{Gal}(F/K) \to C_K \to 0$$

where C_K is the class group of K.

Proof. Let H be the Hilbert class field of K. Then class field theory gives us that the short exact sequence of Galois groups,

$$0 \to \mathrm{Gal}(F/H) \to \mathrm{Gal}(F/K) \to \mathrm{Gal}(H/K) \to 0$$

corresponds to the short exact sequence involving ray class groups

$$0 \to \mathcal{P} \cap I_m/P_m \to I_m/P_m \to I_m/\mathcal{P} \cap I_m \to 0$$

where $\mathcal{P}$ is the group of principal fractional ideals, I_m is the group of fractional ideals prime to m and $P_m = \{(\alpha) : \alpha \in k^\times$ is totally positive and $\nu_P(\alpha - 1) = \nu_P(m)$ for every prime factor P of $m\}$.

Consider the map

$$\begin{aligned} \mathcal{P} \cap I_m &\to G/\overline{E}. \\ (r/s) &\mapsto rs^{-1} \end{aligned}$$

where for any ideal in $\mathcal{P} \cap I_m$, we always pick a totally positive generator. It is not hard to see this is well-defined and the kernel is P_m. Therefore

$$\mathcal{P} \cap I_m/P_m \cong G/\overline{E}$$

and the proposition follows. □

Corollary. *Let $k = \mathbb{Q}(\sqrt{-23})$ and let p be a prime number. If F_n is the ray class field for (p^n) considered as an ideal of O_k and H is the Hilbert class field of k, then*

$$|\mathrm{Gal}(F_n/H)| = \begin{cases} (p^2-1)p^{2n-2}/2 & \text{if } p \text{ remains inert in } k \\ (p-1)^2p^{2n-2}/2 & \text{if } p \text{ is odd and splits in } k \\ p^{2n-2} & \text{if } p = 2 \\ (p-1)p^{n-1}/2 & \text{if } p = 23 \end{cases}$$

We can now determine the criterion for the existence of the extension L of k in which only p is ramified. Let p and F_n be as in the corollary. Then if there were an extension L of k in which only p was ramified, LH would be contained in F_n for some n so it is necessary that 3 divide the order of $\mathrm{Gal}(F_n/H)$ for some n in order for the extension L to exist.

First, when p is inert in $k/\mathbb{Q}$, we have seen that we must have $p \equiv 2 \bmod 3$ in order for the above extension L to exist. Let P be the prime above p in k. The prime p is odd because we are assuming p remains inert in k so $\overline{E}$ has order 2. Thus if we take $n = 1$, then $(O_k/m)^\times$ has order $p^2 - 1$ so $G/\overline{E}$ has order $(p^2 - 1)/2$. Therefore the condition $p \equiv 2 \bmod 3$ is sufficient for H to have a degree three extension F contained in F_1 and F will be Galois over $\mathbb{Q}$ by uniqueness since it is the only degree three extension of H abelian over k ramified only at primes above p.

The question now arises is $\mathrm{Gal}(F/k) \cong \mathbb{Z}/9\mathbb{Z}$ or is $\mathrm{Gal}(F/k) \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. The extension L/k will exist if and only if $\mathrm{Gal}(F/k)$ is of type $(3,3)$, i.e. in the latter case. To determine this we consider the prime 2. The prime 2 splits into two primes $\mathcal{Q}_1$ and $\mathcal{Q}_2$ in k each of which is nonprincipal. Thus each of $\mathcal{Q}_1$ and $\mathcal{Q}_2$ remain inert in H/k. Now if the primes $\mathcal{Q}_1'$ and $\mathcal{Q}_2'$ of H lying over $\mathcal{Q}_1$ and $\mathcal{Q}_2$ are split in F/H, then we can let L be the splitting field of $\mathcal{Q}_1$ in F. This will show $\mathrm{Gal}(F/k)$ is of type $(3,3)$ as we wanted. Then since H is dihedral over $\mathbb{Q}$, and there is no cyclic degree three extension of k ramified only at P abelian over $\mathbb{Q}$, the only possibility is that L too is dihedral over $\mathbb{Q}$. Therefore F/k is cyclic of degree 9 if the prime in k over 2 remains inert in F/k and of type $(3,3)$ otherwise.

It is now not hard to find a criterion for the splitting of primes above 2 in F/H. Let α be a generator of $\mathcal{Q}_1^3$ in k. Then by class field theory, the image of (α) in $\mathcal{P} \cap I_m/P_m$ corresponds to the Frobenius element for $\mathcal{Q}_1$ in $\mathrm{Gal}(F_1/H)$.

Thus F/k will be of type $(3,3)$ if and only if (α) is a cube in $\mathcal{P} \cap I_m/P_m$. Since $\mathcal{P} \cap I_m/P_m \cong G/\overline{E}$ and $G/\overline{E}$ is cyclic of order $(p^2-1)/2$, we see (α) is a cube if and only if $\alpha^{\frac{p^2-1}{3}} \in P_m$, i.e. if and only if $\alpha^{\frac{p^2-1}{3}} \equiv 1 \bmod P$, a criterion which can be checked numerically.

When p splits in $k/\mathbb{Q}$ we can proceed similarly. First, let P_1 and P_2 be the two primes of k above p. We consider the ray class fields $F_{n,1}$ and $F_{n,2}$ for k which have conductor P_1^n and P_2^n respectively. Again both $F_{n,1}$ and $F_{n,2}$ contain H. If $G_1 = (O_k/P_1^n)^\times$ and $G_2 = (O_k/P_2^n)^\times$ with $\overline{E}_1$ and $\overline{E}_2$ being the images of $O_k^\times$ in G_1 and G_2, then we know $\mathrm{Gal}(F_{n,1}/H) \cong G_1/\overline{E}_1$ and $\mathrm{Gal}(F_{n,2}/H) \cong G_2/\overline{E}_2$. Since p splits in k, $(O_k/P_1^n)^\times \cong (O_k/P_2^n)^\times \cong (\mathbb{Z}/p^n\mathbb{Z})^\times$ has order $(p-1)p^{n-1}$ and there will be a nontrivial 3-part only when $p \equiv 1 \bmod 3$ or $p = 3$ so we assume from now on that p satisfies this.

Since we are looking for extensions of k in which only P_1 and P_2 are ramified, we should also look at the ray class fields F_n with conductor $P_1^n P_2^n$. We see here that if $G = (O_k/P_1^n P_2^n)^\times$ and $\overline{E}$ is the image of $O_k^\times$ in G then $G/\overline{E} \cong \mathrm{Gal}(F_n/H)$. Now $|G_1/\overline{E}_1| = |G_2/\overline{E}_2| = \frac{(p-1)p^{n-1}}{2}$ so looking at the composite $F_{n,1}F_{n,2}$ we see $[F_{n,1}F_{n,2} : H] = \frac{((p-1)p^{n-1})^2}{4}$. However $[F_n : H] = |G/\overline{E}| = \frac{((p-1)p^{n-1})^2}{2}$ so F_n is a degree two extension of $F_{n,1}F_{n,2}$. As we are only looking at 3-extensions of H, we can restrict ourselves to $F_{n,1}F_{n,2}$.

Now take $n = 1$ if $p \equiv 1 \bmod 3$ and $n = 2$ if $p = 3$. Then both $F_{n,1}$ and $F_{n,2}$ will contain nontrivial 3-extensions of H which are cyclic. Let $\overline{F}_{n,1}$ and $\overline{F}_{n,2}$ be the first layers of these cyclic 3-extensions. $\overline{F}_{n,1}$ and $\overline{F}_{n,2}$ are distinct and are conjugate fields over k so there is a unique cyclic degree three extension F of H contained in $\overline{F}_{n,1}\overline{F}_{n,2}$ which is Galois over $\mathbb{Q}$ and on which $\mathrm{Gal}(k/\mathbb{Q})$ acts nontrivially. We now have the same question as before, do the primes $\mathcal{Q}_1$ and $\mathcal{Q}_2$ of k above 2 remain inert in F/k or are they split to some degree. The extension $\overline{F}_{n,1}\overline{F}_{n,2}/H$ also contains a cyclic degree three extension F' of

H such that $\mathrm{Gal}(k/\mathbb{Q})$ acts trivially on $\mathrm{Gal}(F'/H)$. This is the lift of a cyclic degree three extension of $\mathbb{Q}$ so F'/k is an extension of type $(3,3)$. Since $\mathcal{Q}_1$ and $\mathcal{Q}_2$ remain inert in H/k, the primes of H above them must split in F'/H. Therefore these primes are split in F/H if and only if they split completely in $\overline{F}_{n,1}\overline{F}_{n,2}/H$ which will be true if and only if the image of α is a cube in $\mathrm{Gal}(F_{n,1}F_{n,2}/H)$. Lastly, this will be true if and only if the image of α is a cube in either $\mathrm{Gal}(F_{n,1}/H)$ or $\mathrm{Gal}(F_{n,2}/H)$, each of which implies the other.

We can now state the above results in the following

Proposition. *Let p be a prime which either remains inert in k and for which $p \equiv 2 \bmod 3$ or which splits in k and for which $p \equiv 1 \bmod 3$. Then an extension L/k cyclic of order 3 and dihedral over $\mathbb{Q}$ with only primes above p ramified exists if and only if*

$$\alpha^{\frac{p^2-1}{3}} \equiv 1 \bmod P$$

in the first case with P the unique prime of k above p, or

$$\alpha^{\frac{p-1}{3}} \equiv 1 \bmod P$$

in the second case where P can be either of the the two primes of k over p. Here α is any generator of the cube of either of the two ideals of k over 2.

We have checked the above criterion by computer for all primes up to 1000 and have found complete agreement with all of the fields found in our search. In addition, this check indicates there exist an additional nine primes between 600 and 1000 which have extensions that are only ramified at that prime in addition to seventeen such primes less than 1000 found by the search.

We will now show that for every prime p which is admissible, there are extensions L/k in which p is ramified and in fact there are infinitely many such extensions. To start with, we have the following theorem.

Theorem. *Let p and q be distinct admissible primes. Then, if the first layers of the 3-part of the ray class fields of k with conductors $m = (p)$ and $m = (q)$ both are of type $\mathbb{Z}/9\mathbb{Z}$, then there is a cyclic degree three extension of k dihedral over $\mathbb{Q}$ with only p and q ramified from k to L. In other words, if p and q are such that there do not exist extensions L/k of the above type with just p and just q ramified, then there exists such an extension L/k where both p and q are ramified and only they are ramified.*

Proof. Let F_1 be the unique extension with $\mathrm{Gal}(F_1/k) \cong \mathbb{Z}/9\mathbb{Z}$ and only p ramified which is Galois over $\mathbb{Q}$ and let F_2 be the unique extension with $\mathrm{Gal}(F_2/k) \cong \mathbb{Z}/9\mathbb{Z}$ and only q ramified which is Galois over $\mathbb{Q}$. Then F_1F_2 is a type $(3,3)$ extension of H, the Hilbert class field of k. Thus the primes above 2, which are all inert in F_1/k and F_2/k, cannot be fully inert in F_1F_2/H since $\mathrm{Gal}(F_1F_2/H)$ is not cyclic. Thus let L be the splitting field of the primes above 2 in F_1F_2/k. Then L is a cyclic degree three extension of k and since $\mathrm{Gal}(k/\mathbb{Q})$ acts nontrivially on $\mathrm{Gal}(F_1/k)$ and $\mathrm{Gal}(F_2/k)$ it is not hard to see L is dihedral over $\mathbb{Q}$ too. □

We can now remark that for any admissible prime we can see there are infinitely many extensions L/k in which that prime is ramified for in the case of a prime p where there is an extension L/k in which only the prime p is ramified we just need to take the composite with any other extension L/k with different primes ramified. In the light of the two possibilities for the ray class field, we will call an admissible prime for which the first layer of the ray class field is of type $(3,3)$ a prime of the first type. If the corresponding part of the ray class field is of type (9) then we will call the prime a prime of the second type.

3.3 Capitulation

Now we wish to find a criterion for when capitulation is possible in these extensions L/k. If the primes of k above 2 capitulate in L, then α will be a norm from L to k so α needs to be a norm locally at every prime of k for capitulation to be possible. Since the local norm map is onto for unramified extensions, this gives us a criterion at the ramified primes in L/k.

If α is not a norm locally at a prime p, we will say there is an obstruction to capitulation and when α is a norm at p, we will say the obstruction to capitulation is satisfied. If the obstruction to capitulation is satisfied at all ramified primes in an extension L/k, then capitulation may happen but if is still not guaranteed that capitulation will happen. While the Hasse Norm Theorem says that α will be a norm globally if and only if it is a norm everywhere locally, it can happen that α is the norm of a noninteger in $L^\times$ and thus capitulation does not have to happen even when the obstruction to capitulation is satisfied everywhere. We have in fact computed a number of cases where α is a norm according to the Hasse Norm Theorem but capitulation does not happen.

The following theorem treats the possibility of capitulation in all cases.

Theorem. *Let L/k be a cyclic degree three extension such that L is dihedral over $\mathbb{Q}$. If all of the ramified primes are of the first type then there is no obstruction to capitulation in L/k. If on the other hand, any of the ramified primes are of the second type, then capitulation cannot happen in L/k.*

Proof. First assume p is a prime ramified in L/k of the first type. Then α must be a cube locally at p so α is automatically a norm locally. Therefore if all

primes which ramify in L/k are of the first type, then there is no obstruction to capitulation in L/k.

Now suppose some prime ramified in L/k is inert and of the second type. Then we know α is not a cube in $O_{k_P}^\times$ where P is the prime of k above p. However, since the norm subgroup of $O_{k_P}^\times$ is stable under $\mathrm{Gal}(k/\mathbb{Q})$, the norm subgroup must be $(O_{k_P}^\times)^3$ which means α cannot be a norm. Therefore capitulation cannot happen in L/k.

On the other hand if some prime ramified in L/k is split and of the second type, then α is not a cube locally at either of the two primes P_1 and P_2 of k above p. Thus if ζ_3 is a primitive third root of unity in k_P, then either $\alpha \equiv \zeta_3$ mod cubes or $\alpha \equiv \zeta_3^2$ mod cubes in $O_{k_{P_1}}^\times$. If $\overline{\alpha}$ is the complex conjugate of α, then $\alpha\overline{\alpha} = 8$ is a cube so if $\alpha \equiv \zeta_3$ then $\overline{\alpha} \equiv \zeta_3^2$ mod cubes and vice versa. Therefore it is not possible for both α and $\overline{\alpha}$ to be norms locally at P_1 in L/k and capitulation again cannot happen in L/k. □

3.4 Dirichlet Density

Now that we have seen that there is no obstruction to capitulation in an extension L if and only if all primes ramified are of the first type, we next determine how many primes there are of the first type.

Theorem. *The Dirichlet density of the set of admissible primes is* $1/2$ *and the Dirichlet density of the set of primes of the first type is* $1/6$. *In particular, the Dirichlet density of the set of primes of the first type which split in* k *is* $1/12$ *and those which remain inert in* k *is also* $1/12$.

Proof. We can check the frequency of admissible primes by taking the biquadratic field $F = k(\sqrt{-3})$. Then, if p is a prime and $p \equiv 1 \bmod 3$, p will

be split in $\mathbb{Q}(\sqrt{-3})$ so if p splits in k, p will split completely in F and the Frobenius of p will be the identity in $\mathrm{Gal}(F/\mathbb{Q})$. So by the Tchebotarev Density Theorem, these primes will have a Dirichlet density of 1/4. Similarly if $p \equiv 2 \bmod 3$, then p remains inert in $\mathbb{Q}(\sqrt{-3})$ so if p also remains inert in k, then the Frobenius of p is the element of order 2 in $\mathrm{Gal}(F/\mathbb{Q})$ which fixes the totally real subfield $L = \mathbb{Q}(\sqrt{69})$. Again by the Tchebotarev Density Theorem, the Dirichlet density of these primes will be 1/4. Therefore the admissible primes have Dirichlet density 1/2.

A prime p of the first type will further have α being a cube locally at p. Therefore if we take $F' = F(\sqrt[3]{\alpha})$ then p will split from F to F'. We now show F' is Galois over $\mathbb{Q}$. Clearly F' is Galois over k. Since $N_{k/\mathbb{Q}}(\alpha) = 8$, $\alpha\overline{\alpha} = 8$ where $\overline{\alpha}$ is the complex conjugate of α so $\overline{\alpha} = \alpha^{-1}$ mod cubes. Thus $\sqrt[3]{\overline{\alpha}} \in F'$ so F' is Galois over $\mathbb{Q}$.

Primes which split in k and are of the first type will split completely in $F'/\mathbb{Q}$ so since $[F' : \mathbb{Q}] = 12$, by the Tchebotarev density theorem their Dirichlet density will be 1/12.

Primes which are inert in k and are of the first type will have a Frobenius of order two in $\mathrm{Gal}(F'/\mathbb{Q})$. We will show the Frobenius is in the center of $\mathrm{Gal}(F'/\mathbb{Q})$. We know the restriction of the Frobenius to $\mathrm{Gal}(F/\mathbb{Q})$ is the element of order two which fixes L. However it is not hard to see by Kummer theory that F' is cyclic of order six over L. Since $\mathrm{Gal}(F'/L)$ is normal and it only has a single element of order two, that element must be in the center of $\mathrm{Gal}(F'/\mathbb{Q})$. Thus the conjugacy class of the Frobenius has only one element so the Dirichlet density of these primes is again 1/12 and the Dirichlet density of all primes of the first type is 1/6. □

3.5 Questions

We now mention some questions which remain open. For each extension L/k we can take the composite with the Hilbert class field H of k and find two other extensions L_1 and L_2 which have the same discriminant as L. In these three extensions, the primes over 2 will remain inert in two of them and will be split in the third. In our examples the existence of capitulation and the nature of the 3-part of the class groups have been fairly independent of the behavior in the corresponding other two extensions with the same discriminant. One question is, is it possible to find any correlation among the behaviors in these sets of extensions or can one show these phenomena are actually random in some well defined way.

A big question is, are there infinitely many primes of the first type for which capitulation happens in the extensions L where only that prime is ramified. Also, are there infinitely many primes of the first type for which capitulation does not happen when that prime is the only ramified prime. One can also take composites of extensions with primes of the first type ramified. One can ask how does capitulation in these extensions with many primes ramified depend on capitulation happening or not happening in the corresponding extensions where only one of the primes is ramified.

3.6 Table of Results

The following is a table of computer calculations done with the field $k = \mathbb{Q}(\sqrt{-23})$. In addition to the fields listed in the table with primes of the first type ramified, the computer search also found fields with the following primes of the first type ramified: 1187, 1229, 3011 and 6047 which remain inert in k and 2707, 2971, 6481 and 8263 which split in k.

The computer search found fields with primes of the first type ramified for all the primes of the first type less than 600. Using the criterion for primes of the first type, the following were found to be all the primes of the first type from 600 to the first one past 1500. Those that remain inert in k: 617, 641, 797, 911, 977, 1019, 1091, 1187, 1217, 1229, 1259, 1307, 1493 and 1532. Those that split in k: 673, 823, 859, 997, 1231, 1237, 1327 and 1567.

The fields are listed according to the prime which ramifies in it. For each prime, the three fields with that prime ramified are listed in a column. The first two fields in each column are the two fields in which the primes over 2 in k remain inert and the third field is the field in which the primes over 2 in k split. A "c" means capitulation occurs in that field and an "nc" means capitulation does not occur.

The class groups are listed according to their cyclic factors. For instance "(21,63)" would mean the class group was $\mathbb{Z}/21\mathbb{Z} \times \mathbb{Z}/63\mathbb{Z}$. An asterisk on a class group means the class group was computed using a bound of 500 instead of the Minkowski bound because the Minkowski bound was too high to use in that case. I have been informed by the people who made the software used that they know of no cases where a bound of 500 has produced an incorrect class group.

Table 3.1: Table of capitulation and class groups.

Primes which remain inert in k.

83	c	(3,3)	113	c	(3,3)	137	nc	$(3,9)^*$
	c	(3,3)		c	(3,3)		nc	$(9,27)^*$
	c	(3,3)		c	$(3,3)^*$		nc	$(21,63)^*$
149	c	(3,3)	467	c	$(3,3)^*$	521	c	$(6,6)^*$
	c	(3,3)		c	$(3,3)^*$		c	$(6,6)^*$
	c	$(6,6)^*$		c	$(3,3)^*$		c	$(3,3)^*$
557	c	$(6,6)^*$	1091	c	$(9,9)^*$			
	c	$(15,15)^*$		nc	$(3,12,12)^*$			
	c	$(6,6)^*$		c	$(9,9)^*$			

Primes which split in k.

151	c	(3,3)	163	nc	(3,9)	307	c	$(3,3,9)^*$
	nc	$(3,9)^*$		c	$(3,3)^*$		nc	$(3,3,9)^*$
	c	$(6,6)^*$		c	$(3,3)^*$		nc	$(3,6,18)^*$
397	nc	$(3,9)^*$	409	c	$(3,3)^*$	541	c	$(3,3)^*$
	c	$(3,3)^*$		c	$(3,3)^*$		c	$(3,3)^*$
	c	$(6,6)^*$		nc	$(3,9)^*$		nc	$(6,18)^*$
547	c	$(3,3)^*$	601	c	$(3,3)^*$	811	c	(3,3)
	c	$(3,3)^*$		c	$(6,6)^*$		c	$(3,6,18)^*$
	c	$(3,3,9)^*$		nc	$(3,9)^*$		c	$(48,48)^*$
967	c	$(3,6,18)^*$	1153	c	$(3,3)^*$			
	c	$(3,3)^*$		nc	$(3,9)^*$			
	c	$(33,33)^*$		c	$(15,15)^*$			

Bibliography

[1] J. Coates, *The Work of Mazur and Wiles on Cyclotomic Fields*, Sém. Bour., exp. 575, (1980/81)

[2] A. Cuoco and P. Monsky, *Class Numbers in $\mathbb{Z}_p^d$-extensions*, Math. Ann. **255** (1981), 235–258.

[3] R. Greenberg, *The Iwasawa Invariants of Γ-extensions of a Fixed Number Field*, Amer. J. Math. **XCV** (1973) 204–214.

[4] R. Greenberg, *On the structure of certain Galois groups*, Inv. Math. **47** (1978), 85–99.

[5] K. Iwasawa, *On $\mathbb{Z}_\ell$-extensions of algebraic number fields*, Ann. of Math. (2) **98** (1973), 246–326.

[6] U. Jannsen, *On the structure of Galois groups as Galois Modules*, Number Theory Noordwijkerhout 1983, Lecture Notes in Math. **1068** (1984), 109–126.

[7] KASH, a computational algebraic number theory shell, the KANT-group, Technische Universität Berlin, Fachbereich 3 Mathematik, Straße des 17. Juni 136, 10623 Berlin, Germany

[8] J. Minardi, *Iwasawa modules for $\mathbb{Z}_p^d$-extensions of algebraic number fields*, Thesis, University of Washington, 1986

[9] A. Movahhedi, *Sur les p-extensions des corps p-rationnels*, Math. Nach. **149** (1990) 163–176.

[10] A. Movahhedi and Nguyen-Quang-Do, *Sur l'arithmétique des corps de nombres p-rationnels*, Séminaire de Théorie des Nombres, Paris 1987–88, Progr. Math., **81**, Birkhäuser Boston, Ma., 1990, 155–200.

[11] T. Nguyen-Quang-Do, *Formations de classes et modules d'Iwasawa*, Number Theory Noordwijkerhout 1983, Lecture Notes in Math. **1068** (1984), 167–185.

[12] I. R. Shafarevich, *Extensions with given points of ramification*, Inst. Hautes Etudes Sci. Publ. Math. **18** (1964), 295–319; English transl. in Amer. Math. Soc. Transl. Ser. 2 **59** (1966), 128–149; see also Collected Mathematical Papers, 295–316.

[13] J.-P. Serre, *Classes des corps cyclotomiques*, Sém. Bour., exp. 174, (1958/59).

[14] K. Wingberg, *On Galois groups of p-closed algebraic number fields with restricted ramification*, J. Reine Angew. Math. **400** (1989), 185–202.

[15] K. Wingberg, *On Galois groups of p-closed algebaic number fields with restricted ramification II*, J. Reine Angew. Math. **416** (1991), 187–194.

[16] M. Yamagishi, *A note on free pro-p-extensions of algebraic number fields*, Journal de Théorie des Nombres de Bordeaux **5** (1993), 165–178.

Appendix A

The Proof of Pseudo-nullity for $Y_{\tilde{k}}$

We now give Minardi's proof that $Y_{\tilde{k}} \sim 0$ for $k = \mathbb{Q}(\sqrt{-31})$ and $p = 3$. We will prove if $Y_{\tilde{k}}$ is not pseudo-null, then $Y_{\tilde{k}}$ cannot have any proper nonzero pseudo-null submodule and we will then show that the sum of the decomposition groups for primes above 3 in $Y_{\tilde{k}}$ is a nonzero pseudo-null submodule. $Y_{\tilde{k}}$ will then have to be pseudo-null.

Let $\Gamma = \mathrm{Gal}(\tilde{k}/k)$ and let $\Lambda = \Lambda_{\tilde{k}/k}$. We first note 3 remains inert in $k/\mathbb{Q}$, $h_k = 3$ and since 3 does not divide the class number of $\mathbb{Q}(\sqrt{93})$, counting Kummer generators for k shows us the Hilbert class field of k is contained in the composite of all $\mathbb{Z}_3$-extensions of k, that is $L_k \subset \tilde{k}$. Also note the prime above 3 in k splits completely in L_k since 3 remains inert in k.

Lemma 1 i) *If K/k is any $\mathbb{Z}_3$-extension containing L_k then $Y_K = 0$.*

ii) *Let $\{\sigma, \tau\} \subset \Gamma$ be a $\mathbb{Z}_3$-basis with K the fixed field of σ. Let $S = \sigma - 1$ and $T = \tau - 1$ in Λ. Then $Y_{\tilde{k}}/SY_{\tilde{k}} \cong \Lambda/(S, 3 + 3T + T^2)$ and in particular $Y_{\tilde{k}}$*

is a cyclic module.

Proof. i) Identify T with its image in $\Lambda_{K/k}$ and consider the fixed field of TY_K. This will be the maximal abelian extension of k contained in L_K. If this is a proper extension of K, then k has a 3-ramified cyclic 3-extension which becomes unramified when lifted to K. However by the Kummer generator argument mentioned in the introduction, $M_k = \tilde{k}$ and since $L_k \subset K$, the extension $\tilde{k}/K$ is fully ramified so no 3-ramified cyclic 3-extension of k becomes unramified over K. Therefore $TY_K = Y_K$ and $Y_K = 0$.

ii) Let L_0 be the fixed field of $SY_{\tilde{k}}$, that is, the maximal abelian extension of K contained in $L_{\tilde{k}}$. We will show L_0 is actually abelian over L_k. If I_1, I_2 and I_3 are the inertia groups in $\mathrm{Gal}(L_0/K)$ for primes over 3, then $\mathrm{Gal}(K/L_k)$ acts on each of these and in fact acts trivially since I_i injects by restriction into $\mathrm{Gal}(\tilde{k}/K)$ and $\tilde{k}/L_k$ is abelian. But $Y_K = 0$ so $\mathrm{Gal}(L_0/K) = \sum I_i$. Therefore $\mathrm{Gal}(K/L_k)$ acts trivially on $\mathrm{Gal}(L_0/K)$ so L_0 is abelian over L_k.

We wish now to show $L_0 = \widetilde{L_k}$. Then, since $\mathrm{Gal}(L_0/K) = \sum I_i$ is a cyclic $\Lambda_{K/k}$-module we would have

$$\sum I_i \cong \frac{\Lambda_{K/k}}{\omega_1 \Lambda_{K/k}} \cong \frac{\Lambda}{(S, (T+1)^3 - 1)},$$

with $\omega_1 = \tau^3 - 1$ where τ is considered as its restriction to $\mathrm{Gal}(K/k)$.

Since the prime over 3 splits completely in L_k/k, the local degree at 3 in L_k is two so the inertia groups for primes over 3 in $\widetilde{L_k}$ have $\mathbb{Z}_3$-rank two. Since primes over 3 are fully ramified in $\tilde{k}/L_k$, $\widetilde{L_k}$ must be unramified over $\tilde{k}$ and therefore $\widetilde{L_k}$ must be contained in L_0. We will actually show $M_{L_k} = \widetilde{L_k}$, from which $L_0 = \widetilde{L_k}$ follows.

The class number of L_k is prime to 3 since $Y_K = 0$ and K/L_k is fully ramified above 3. Thus $X_{L_k} = \mathrm{Gal}(M_{L_k}/L_k)$ is isomorphic to $(\prod U_i)/\overline{E}$ where

U_1, U_2 and U_3 are the local principal units at the completion of L_k at primes above 3 and $\overline{E}$ is the closure of the image of the global units of L_k congruent to 1 at all primes above 3. The U_i do not contain the cube roots of unity so $\prod U_i$ is a free $\mathbb{Z}_3$-module of rank 6. X_{L_k} has torsion if and only if there exists a global unit $\eta \in E$ which is a cube in each U_i but not in E. If such a unit exists consider the field $L_k k^*(\sqrt[3]{\eta})$ where $k^* = k(\sqrt{-3})$. As $\mathrm{Gal}(k^*/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^2$ and $\mathbb{Q}(\sqrt{93})$ has class number one, we have $3 \mid h_{k^*}$ but $9 \nmid h_{k^*}$ so $L_{k^*} = k^* L_k$. Since $L_k k^*(\sqrt[3]{\eta})/L_k k^*$ is nontrivial but is split at all primes above 3 because of the choice of η, it is an unramified extension. This shows the maximal unramified abelian 3-extension of k^* would be larger than $k^* L_k$ contradicting that $9 \nmid h_{k^*}$. Thus there is no such η and $M_{L_k} = \widetilde{L_k}$ proving $L_0 = \widetilde{L_k}$.

Since $M_k = \tilde{k}$, $\tilde{k}$ is the maximal abelian subextension of L_0/k so

$$\mathrm{Gal}(L_0/\tilde{k}) = T\mathrm{Gal}(L_0/K)$$

and

$$\mathrm{Gal}(L_0/\tilde{k}) \cong T\frac{\Lambda}{(S,(T+1)^3-1)} \cong \frac{\Lambda}{(S,3+3T+T^2)}.$$

Since $\mathrm{Gal}(L_0/\tilde{k}) \cong Y_{\tilde{k}}/SY_{\tilde{k}}$ we have $Y_{\tilde{k}}/SY_{\tilde{k}}$ is cyclic over $\Lambda/S\Lambda$ so $Y_{\tilde{k}}$ is cyclic over Λ by Nakayama's lemma. □

Now let K' be any $\mathbb{Z}_3$-extension of k not containing L_k. Then K'/k is fully ramified at the prime above 3 and we can consider K' to be the fixed field of τ. We again identify σ and S with their images in $\mathrm{Gal}(K'/k)$ and $\Lambda_{K'/k}$.

Lemma 2 i) *The fixed field of $SY_{K'}$ is $K'L_k$ so $Y_{K'}/SY_{K'} \cong \mathbb{Z}/3\mathbb{Z}$.*

ii) *$Y_{\tilde{k}}/TY_{\tilde{k}}$ is isomorphic to a submodule of $Y_{K'}$ of index 3. If $Y_{K'}$ is finite then $Y_{\tilde{k}} \sim 0$, otherwise $Y_{\tilde{k}}/TY_{\tilde{k}} \cong \Lambda/(T, F(S,T))$ with $F(0,0) = 3$.*

Proof. i) Let L_1 be the fixed field of $SY_{K'}$. Since L_1/k is abelian and there is only one prime above 3 in k, the fixed field of the inertia subgroup of $\mathrm{Gal}(L_1/k)$ is unramified and so must be L_k. Thus $L_1 = K'L_k$ and $Y_{K'}/SY_{K'} \cong \mathrm{Gal}(K'L_k/K') \cong \mathbb{Z}/3\mathbb{Z}$.

ii) Since $\mathbb{Z}/3\mathbb{Z}$ is a cyclic $\mathbb{Z}_3$-module, $Y_{K'}$ is cyclic over $\Lambda_{K'/k}$ so let $Y_{K'} \cong \Lambda_{K'/k}/\mathfrak{b}$ and note $\Lambda_{K'/k} \cong \mathbb{Z}_3[[S]]$. Now let L_0 be the fixed field of $TY_{\tilde{k}}$. Since there is only one prime over 3 in K', it is clear $\mathrm{Gal}(L_0/\tilde{k}) \cong \mathrm{Gal}(L_{K'}/K'L_k)$ so $Y_{\tilde{k}}/TY_{\tilde{k}}$ is isomorphic to a submodule of $Y_{K'}$ of index 3. If $Y_{K'}$ is finite then $\mathrm{Gal}(L_0/\tilde{k})$ is finite and $Y_{\tilde{k}} \sim 0$. Now suppose $Y_{K'}$ is infinite. Since $SY_{K'}$ has index 3 in $Y_{K'}$, $\mathfrak{b} + S\Lambda_{K'/k}$ has index 3 in $\Lambda_{K'/k}$ so $\mathfrak{b} + S\Lambda_{K'/k} = (3, S)$. This means $\mathfrak{b}$ must have an element f with constant term 3. Therefore f is irreducible and since we're assuming $Y_{K'}$ is infinite, $\mathfrak{b} = (f)$ and $Y_{K'} \cong \Lambda_{K'/k}/f\Lambda_{K'/k}$ with $f(0) = 3$. Thus

$$Y_{\tilde{k}}/TY_{\tilde{k}} \cong (3, S)\frac{\Lambda_{K'/k}}{f\Lambda_{K'/k}} \cong \frac{\Lambda_{K'/k}}{f\Lambda_{K/'k}} \cong \frac{\Lambda}{(T, F(S,T))}$$

where $F(S,T)$ is any element of Λ which reduces to $f(S)$ in $\Lambda/T\Lambda$. Again by Nakayama's lemma we see $Y_{\tilde{k}}$ is a cyclic Λ-module. □

We can now form the following key conclusion.

Lemma 3 *If $Y_{\tilde{k}}$ is not pseudo-null, then $Y_{\tilde{k}} \cong \Lambda/F\Lambda$ where $F(0,0) = 3$ so $Y_{\tilde{k}}$ contains no nonzero pseudo-null submodule.*

Proof. We know $Y_{\tilde{k}}$ is cyclic so $Y_{\tilde{k}} \cong \Lambda/\mathfrak{A}$ for some ideal $\mathfrak{A} \subset \Lambda$. By the previous lemma, $\mathfrak{A} + T\Lambda = (T, f)$ where $f \in \mathbb{Z}_3[[S]]$ satisfies $f(0) = 3$. Then $\mathfrak{A}$ must contain an element $F(S,T)$ with $F(S,0) = f$ so $F(0,0) = f(0) = 3$. Therefore F is irreducible so if $Y_{\tilde{k}} \nsim 0$, we have $\mathfrak{A} = (F)$ and $Y_{\tilde{k}} \cong \Lambda/F\Lambda$. If a nonzero element $\alpha + F\Lambda \in \Lambda/F\Lambda$ had an annihilator G relatively prime to F,

then $G\alpha = FH$ for some $H \in \Lambda$. Then $F \mid G\alpha$ so $F \mid G$ or $F \mid \alpha$ but neither of these can happen so $Y_{\tilde{k}}$ has no nonzero pseudo-null submodules. □

We now introduce a conjecture on the p-units of a number field F. Let U_1, ..., U_g be the local principal units in the completions of F at the primes above p and let E_p denote the p-units of F. One can embed E_p into $U_1 \times \ldots \times U_g$ by

$$e \mapsto (e\pi_1^{-\nu_1(e)}/\omega_1(e\pi_1^{-\nu(e)}), \ldots, e\pi_g^{-\nu_g(e)}/\omega_g(e\pi_g^{-\nu_g(e)}))$$

where $\pi_i \in F$ is a local uniformizer at the i-th prime and ν_i, ω_i are the corresponding valuation and Teichmüller representative. Part of what Jaulent has conjectured is that the closure of the image of E_p has $\mathbb{Z}_p$-rank equal to one less than the $\mathbb{Z}$-rank of E_p. We will call this Jaulent's conjecture for F and p.

Lemma 4 *Any completion of $\widetilde{L_k}$ over 3 contains the unramified $\mathbb{Z}_3$-extension of $\mathbb{Q}_3$.*

Proof. We have seen $\mathrm{Gal}(\widetilde{L_k}/L_k) \cong (\prod U_i)/\overline{E}$. Let $\mathfrak{p}_i$ be the prime corresponding to U_i and let π_i be a generator of $\mathfrak{p}_i^8$ so that $\pi_i \equiv 1 \bmod \mathfrak{p}_j$ for $j \neq i$ (note that $8 = N_{L_k/\mathbb{Q}}(\mathfrak{p}_i) - 1$ for $i = 1, 2, 3$.) The decomposition group for $\mathfrak{p}_i$ in $\mathrm{Gal}(\widetilde{L_k}/L_k)$ is then generated as a $\mathbb{Z}_3$-module by the images of U_i and π_i in $(\prod U_i)/\overline{E}$. Clearly the $\mathbb{Z}_3$-rank of $\overline{E}_p$ is strictly larger than the $\mathbb{Z}_3$-rank of $\overline{E}$ if and only if the completions of $\mathrm{Gal}(\widetilde{L_k}/k)$ above 3 contain the unramified $\mathbb{Z}_3$-extension of $\mathbb{Q}_3$. Thus we only need to verify Jaulent's conjecture for L_k and $p = 3$. This is done after stating our final result in the next proposition. □

Proposition 1 $Y_{\tilde{k}} \sim 0$.

Proof. Let D_1, D_2 and D_3 be the decomposition groups for the primes over 3 in $Y_{\tilde{k}}$. Since the completion of $\widetilde{L_k}$ over each $\mathfrak{p}_i$ contains the unramified

$\mathbb{Z}_3$-extension of $\mathbb{Q}_3$, we have $D_i \cong \mathbb{Z}_3$. Therefore $\mathcal{D} \doteq \sum D_i$ is a finite rank $\mathbb{Z}_3$-module so $\mathcal{D}$ is a nonzero pseudo-null Λ-submodule of $Y_{\tilde{k}}$. Therefore $Y_{\tilde{k}} \sim 0$. □

Lemma 5 *Jaulent's conjecture holds for the field $H = L_k$ and the prime $p = 3$.*

Proof. Since $f(x) = x^3 + x - 1$ has discriminant -31, the splitting field L of f contains $K = \mathbb{Q}(\sqrt{-31})$ and has Galois group S_3 over $\mathbb{Q}$. We wish to show this splitting field is H. Certainly $\mathbb{Q}(\sqrt{-31})/\mathbb{Q}$ is ramified only at 31 and $L/\mathbb{Q}(\sqrt{-31})$ is either unramified or only ramified above 31. We will show there is no S_3-extension of $\mathbb{Q}_{31}$ containing $\mathbb{Q}_{31}(\sqrt{-31})$. Since $\mathbb{Q}_{31}$ contains the cube roots of unity, $L_{\mathcal{P}}/K_P$ is a Kummer extension where $\mathcal{P}$ and P are maximal ideals of L and K over 31. Now $K_P^\times \cong <\pi> \times \mu_{30} \times U$ where π is a uniformizer for K_P and U is the group of principal units in K_P. Since U is divisible by 3,

$$K_P^\times/(K_P^\times)^3 \cong <\pi>/<\pi>^3 \times \mu_3.$$

If we look at the $\Delta = \mathrm{Gal}(K_P/\mathbb{Q}_{31})$ action on $K_P^\times/(K_P^\times)^3$, we see that Δ acts trivially both on $<\pi>/<\pi>^3$ and μ_3 (take $\pi = \sqrt{-31}$.) Thus there are no S_3-extensions of $\mathbb{Q}_{31}$ containing $\mathbb{Q}_{31}(\sqrt{-31})$. Therefore L/K is unramified and $L = H$.

Let u_1, u_2 and u_3 be the roots of $f(x)$. Then $\pi_1 = u_1 + 1$ is a root of $x^3 - 3x^2 + 4x - 3$ so $(u_1 + 1)\mathcal{O}_H = \mathfrak{p}_1$ is a prime over 3 and similarly for $\pi_2 = u_2 + 1$, $\pi_3 = u_3 + 1$ and $\mathfrak{p}_2 = (\pi_2)$, $\mathfrak{p}_3 = (\pi_3)$. For each $\mathfrak{p}_i$ we have a map $\psi_i : H^\times \to H^\times$ given by

$$x \mapsto x/3^{\nu_i(x)}$$

where ν_i is the valuation at $\mathfrak{p}_i$. Since $\mathcal{O}_{\mathfrak{p}_i}^{\times} \cong \mu_8 \times U_i$ where U_i is the group of local principal units, we also have the projections

$$\omega_i : \mathcal{O}_{\mathfrak{p}_i}^{\times} \to U_i.$$

The embeddings $\varphi_i : H \to H_{\mathfrak{p}_i}$ for $i = 1, 2, 3$ now yield a map

$$\varphi : H^{\times} \to U_1 \times U_2 \times U_3$$

given by

$$x \mapsto (\omega_1\varphi_1\psi_1(x), \omega_2\varphi_2\psi_2(x), \omega_3\varphi_3\psi_3(x)).$$

We will denote $U_1 \times U_2 \times U_3$ by U.

Let $\overline{E}$ denote the closure of $\varphi(E_H)$ in U. Since $M_H = \tilde{H}$, it follows that $\overline{E}$ is a direct summand of the $\mathbb{Z}_3$-module U. Now let E_3 be the 3-units of H and let $\overline{E}_3$ be the closure of $\varphi(E_3)$ in U. Because $\mathrm{Gal}(H/\mathbb{Q}) \cong S_3$ acts on $\overline{E}_3$ and the group of units of K is finite, $\overline{E}_3$ is the direct sum of copies of the 2-dimensional representation of S_3. Therefore since $\mathrm{rnk}_{\mathbb{Z}_3}\overline{E} = 2$, $\mathrm{rnk}_{\mathbb{Z}_3}\overline{E}_3$ is 2 or 4. Thus it is only necessary to show $\overline{E}_3$ is strictly larger than $\overline{E}$. Consider the 3-unit $\alpha = (u_3 + 1)^8$. We have $\alpha \equiv 1 \bmod \mathfrak{p}_1\mathfrak{p}_2$ and that if $\varphi(\alpha) \in \overline{E}$ then for each $n \geq 1$, there is an $\eta_n \in E$ with $\eta_n \equiv \alpha \bmod \mathfrak{p}_1^n\mathfrak{p}_2^n$. Assume there are such η_n. If $\tau \in \mathrm{Gal}(H/\mathbb{Q})$ is the order two automorphism which interchanges u_1 and u_2 and fixes u_3, then $\tau\alpha = \alpha$, $\tau\mathfrak{p}_1 = \mathfrak{p}_2$, $\tau\mathfrak{p}_2 = \mathfrak{p}_1$ so $\tau\eta_n \equiv \eta_n \bmod \mathfrak{p}_1^n\mathfrak{p}_2^n$. Let F be the fixed field of τ. If $\varepsilon = \mathrm{N}_{H/F}(\eta_n)$, then $\varepsilon \equiv \alpha^2 \bmod P^n$ where $P = \mathcal{O}_F \cap \mathfrak{p}_1$. We will show below that u_3^8 is not a cube at $\mathfrak{p}_1$. Therefore u_3^8 generates the image of E_F in $(1 + P)/(1 + P^n)$. Now α is a principal unit at P and α^2 is in the image of E_F in $(1 + P)/(1 + P^n)$ so α is in the image too. Therefore we can take $\eta_n = u_3^{a_n}$ for some $a_n \in \mathbb{Z}$.

It will be enough to show $\varphi_1(\alpha)$ and $\varphi_1(u_3)$ generate different nonzero subgroups in U_1/U_1^3. Since 3 is prime in $\mathcal{O}_{\mathfrak{p}_1}$, one has

$$U_1/U_1^3 \cong \hat{\mathfrak{p}}_1/\hat{\mathfrak{p}}_1^2 \cong \mathcal{O}_{\mathfrak{p}_1}/\hat{\mathfrak{p}}_1$$

via the isomorphisms

$$x \mapsto x-1 \mapsto \frac{x-1}{3}.$$

i) Since u_1, u_2, u_3 solve $x^3+x-1=0$, one finds $u_1+u_2+u_3=0$ and $u_1u_2+u_1u_3+u_2u_3=1$ whence

$$u_1^2+u_3^2+u_1u_3+1=0.$$

ii) One can see directly $\frac{u_3^8-1}{3} = u_3-1$ and that $(u_3+1)^8 = 26u_3^2+25u_3+35$.

iii) Modulo $\mathfrak{p}_1^2$ we have, $u_1^2+2u_1+1 \equiv 0$ and $u_1^3+u_1-1 \equiv 0$ so $u_1 \equiv 2$ using that $9 \equiv 0$.

iv) From i) and iii), $u_3^2 \equiv 4-2u_3 \bmod \mathfrak{p}_1^2$ so from ii), $\frac{(u_3+1)^8-1}{3} \equiv 1 \bmod \mathfrak{p}_1$.

Since $u_1 \equiv -1 \bmod \mathfrak{p}_1$, we see from i), $u_3^2-u_3+2 \equiv 0 \bmod \mathfrak{p}_1$ so the image of u_3 in $\mathcal{O}_H/\mathfrak{p}_1$ generates the residue field extension over $\mathbb{Z}/3\mathbb{Z}$ and therefore u_3-1 and 1 generate different nonzero subgroups of $\mathcal{O}_H/\mathfrak{p}_1$ as desired. In particular, $0 \not\equiv u_3-1 \equiv \frac{u_3^8-1}{3} \bmod \mathfrak{p}_1$ so $\varphi_1(u_3)$ is not a cube in U_1. This proves Jaulent's conjecture in this case. □

VITA

David Hubbard was born in San Rafael, California on September 29, 1955. He attended Stanford University for two years and then after working in the computer programming and computer service fields, he finished his last two years of undergraduate study at UC Berkeley and received his B.A. in Mathematics in May 1987. He has been in the graduate program in Mathematics at the University of Washington since then.