The Change in Lambda Invariants for Cyclic p-Extensions of $\mathbb{Z}_p$-Fields

by

Jordan C. Schettler

A Dissertation Submitted to the Faculty of the

DEPARTMENT OF MATHEMATICS

In Partial Fulfillment of the Requirements
For the Degree of

Doctor of Philosophy

In the Graduate College

The University of Arizona

2 0 1 2

THE UNIVERSITY OF ARIZONA
GRADUATE COLLEGE

As members of the Dissertation Committee, we certify that we have read the dissertation prepared by Jordan Schettler

entitled The Change in Lambda Invariants for Cyclic p-Extensions of Z_p-Fields

and recommend that it be accepted as fulfilling the dissertation requirement for the Degree of Doctor of Philosophy

_____ Date: 2/29/2012
William McCallum

_____ Date: 2/29/2012
Romyar Sharifi

_____ Date: 2/29/2012
Dinesh Thakur

_____ Date: 2/29/2012
Kirti Joshi

Final approval and acceptance of this dissertation is contingent upon the candidate's submission of the final copies of the dissertation to the Graduate College.

I hereby certify that I have read this dissertation prepared under my direction and recommend that it be accepted as fulfilling the dissertation requirement.

_____ Date: 2/29/2012
Dissertation Director: William McCallum

Statement by Author

This dissertation has been submitted in partial fulfillment of requirements for an advanced degree at The University of Arizona and is deposited in the University Library to be made available to borrowers under rules of the Library.

Brief quotations from this dissertation are allowable without special permission, provided that accurate acknowledgment of source is made. Requests for permission for extended quotation from or reproduction of this manuscript in whole or in part may be granted by the head of the major department or the Dean of the Graduate College when in his or her judgment the proposed use of the material is in the interests of scholarship. In all other instances, however, permission must be obtained from the author.

Signed: Jordan Schettler

Acknowledgements

Above all other particles in existence are those which have and will comprise my immediate family. My mother Maria, father HC, and brother Ryan, have all given me continuously unconditional love and support for the entire duration of my being. They constitute my foundation, my morals, and my happiness. I could not in any (potentially infinite) measure of time overstate how much they have meant to me. Included now in this inner circle is the love of my life Dana Sellman. She has been an unbelievably joyful and positive addition to my life.

Other members of my extended family and friends also deserve proper acknowledgment. They too have nourished my efforts. My grandfather Dr. James Blankenship has been particularly influential and instrumental to this success. Dr. Blankenship earned his PhD in Physics from the University of Tennessee and has made it very clear to me how proud he was that I chose mathematics as my academic pursuit. He and his wife Jamie have never wavered in their contributions to my education.

I have also reaped the benefits of having some very exceptional K-12 teachers through the years. My fourth grade teacher Pat Krehnke noticed and facilitated my interest in word and logic puzzles. I owe a lot of credit to my fifth grade teacher Ms. Olsen too; I insisted that I be let into her advanced math class and she reluctantly agreed. I had some outstanding educators in high school as well including my Latin teacher Ms. Beasley and my art teacher Andrea Haury, both of whom were highly caring and motivating. Pat Chastain was also very supportive of my efforts at The Center School.

In college too, I had the good fortune of some rather spectacular professors. At the University of Tennessee, Pavlos Tzermias stands out as one of my favorite professors. He was also a great friend and advisor. In particular, he played a major role in my decision to attend the University of Arizona for graduate school. At UA there have been a staggeringly vast number of individuals who have been crucial to navigating the PhD program. Obviously, my advisor William McCallum merits a ton of thanks for his technical and professional advice. Other professors who proved themselves to be indispensable to my development include Klaus Lux, Douglas Ulmer, Dinesh Thakur, Kirti Joshi, Romyar Sharifi, and Robert Indik.

Additionally, I would like to give thanks here to all of my fellow graduate students. Specifically, my office mates Victor Piercey, Ryan Smith, and Geillan Aly, have been extremely supportive friends. It behooves me to also mention that Dave Herzog, who also attended the University of Tennessee, is a truly good-natured friend.

Dedication

To the Trinity: Mom, Pop, and the Schmoe.

Table of Contents

Table of Contents—*Continued*

List of Tables

List of Figures

ABSTRACT

The well-known Riemann-Hurwitz formula for Riemann surfaces (or the corresponding formulas of the same name for curves/function fields) is used in genus computations. In 1979, Yûji Kida proved a strikingly analogous formula in [Kid80] for p-extensions of CM-fields (p an odd prime) which is similarly used to compute Iwasawa λ-invariants. However, the relationship between Kida's formula and the statement for surfaces is not entirely clear since the proofs are of a very different flavor. Also, there were a few hypotheses for Kida's result which were not fully satisfying; for example, Kida's formula requires CM-fields rather than more general number fields and excludes the prime $p = 2$.

Around a year after Kida's result was published, Kenkichi Iwasawa used Galois cohomology in [Iwa81] to establish a more general formula (about representations) that did not exclude the prime $p = 2$ nor need the CM-field assumption. Moreover, Kida's formula follows as a corollary from Iwasawa's formula.

We'll prove a slight generalization of Iwasawa's formula and use this to give a new proof of a result of Kida in [Kid79] and Ferrero in [Fer80] which computes λ-invariants in imaginary quadratic extensions for the prime $p = 2$. We go on to produce special generalizations of Iwasawa's formula in the case of cyclic p-extensions; these formulas can be realized as statements about $\mathbb{Q}_p$-representations, and, in the cases of degree p or p^2, about p-adic integral representations. One upshot of these formulas is a vanishing criterion for λ-invariants which generalizes a result of Takashi Fukuda et al. in [FKOT97]. Other applications include new congruences and inequalities for λ-invariants that cannot be gleaned from Iwasawa's formula. Lastly, we give a scheme theoretic approach to produce a general formula for finite, separable morphisms of Dedekind schemes which simultaneously encompasses the classical Riemann-Hurwitz formula and Iwasawa's formula.

Chapter 1
INTRODUCTION

1.1 Notation

The following notation will be used throughout with a few exceptions:

Symbol	Meaning
$\mathbb{N}_0$, $\mathbb{N}$	the set of nonnegative and positive integers, respectively
$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$	the integer, rational, real, and complex numbers, respectively
p, q	rational primes
$\mathbb{Z}_p$, $\mathbb{Q}_p$	the p-adic integers and rationals, respectively
$\lvert n\rvert_p = p^{-\mathrm{ord}_p(n)}$	normalized p-adic absolute value
F	a field
ℓ, k	number fields
L, K	$\mathbb{Z}_p$-extensions of number fields
$\mathcal{O}_k$, $\mathcal{O}_K$	rings of integers
I_k, I_K	groups of invertible ideals
P_k, P_K	groups of principal invertible ideals
C_k, C_K	class groups
$h(k)$	the class number of k
A_k, A_K	p-primary parts of C_k, C_K, respectively
G	a finite group
$\mathcal{O}^\times$, $\mathcal{O}G$	the units and group ring, respectively, for a ring $\mathcal{O}$
$H^n(G, M)$	nth cohomology group of a $\mathbb{Z}G$-module M
$\mathrm{q}(M) = p^{\chi(G,M)}$	Herbrand quotient $\frac{\lvert H^2(G,M)\rvert}{\lvert H^1(G,M)\rvert}$ when $G \cong \mathbb{Z}/(p^n)$
$H^n(L/K, M)$	$H^n(G, M)$ when $G = \mathrm{Gal}(L/K)$
$\mathcal{C}$	a nonsingular, projective curve over $\overline{F}$
X,Y	schemes
x, y	closed points in X,Y, respectively
$\mathbb{F}(x)$, $\mathbb{F}(y)$	residue fields of x, y
$\mathscr{F}$	a sheaf on X
$H^n(X, \mathscr{F})$	nth sheaf cohomology group

1.2 Motivation

This dissertation is concerned with constructing and analyzing number theoretic analogs of the Riemann-Hurwitz formula for curves:

Theorem 1.1 (Hurwitz)**.** *Let $f\colon X \to Y$ be a finite, separable morphism of complete, nonsingular curves*[1] *over an algebraically closed field F. Then if f has only tame ramification*

$$2g_X - 2 = \deg(f)(2g_Y - 2) + \sum_{x \in X}(e_x - 1) \tag{1.1.1}$$

where g_X, g_Y are the genera of X, Y, respectively, and e_x is the ramification index of f at x.

The number theoretic analogs of Theorem 1.1 that we are interested in come from the Iwasawa theory of $\mathbb{Z}_p$-extensions k_∞ of a number field k. That is, extensions formed from towers

$$k = k_0 \subseteq k_1 \subseteq k_2 \subseteq \ldots \subseteq k_\infty$$

such that

$$\mathrm{Gal}(k_\infty/k) \cong \mathbb{Z}_p \qquad \text{and} \qquad \mathrm{Gal}(k_n/k) \cong \mathbb{Z}/p^n\mathbb{Z} \ \ \forall n \geq 0.$$

The p-part of the class number $h(k_n)$ becomes well-behaved moving up the tower as in the following fundamental theorem of Iwasawa theory.

Theorem 1.2 (Iwasawa's Growth Formula)**.** *Let k_∞/k be as above. There are $\lambda, \mu, \nu \in \mathbb{Z}$ such that if $p^{e(n)}$ is the exact power of p dividing the class number $h(k_n)$, then*

$$e(n) = \lambda n + \mu p^n + \nu$$

for all sufficiently large n.

[1] By a curve over a field F, we mean an integral, separated scheme of finite type over F with dimension 1.

Definition 1.3. The **cyclotomic $\mathbb{Z}_p$-extension** of a number field k is the unique $\mathbb{Z}_p$-extension of k contained in $\cup_{n\geq 0} k(\zeta_{p^n})$. A **$\mathbb{Z}_p$-field** K is the cyclotomic $\mathbb{Z}_p$-extension of some number field k, and the λ-invariant of K/k, denoted by λ_K, does not depend on k. The vanishing of the μ-invariant of K/k (as conjectured by Iwasawa) also does not depend on k, and we denote this by $\mu_K = 0$.

For a $\mathbb{Z}_p$-field K, the ring $\mathcal{O}_K[1/p]$ is a Dedekind domain whose prime spectrum plays the role of the curve Y in Theorem 1.1. We have the following observation about class groups (see [Iwa65]).

If K is the function field of curve Y as in Theorem 1.1 and $p \neq \mathrm{char}(F)$ is prime, the class group $C_K = \mathrm{Pic}^0(Y)$ satisfies $C_K[p^\infty] \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{2g_Y}$.	If K is a $\mathbb{Z}_p$-field with $\mu_K = 0$ and $Y = \mathrm{Spec}(\mathcal{O}_K[1/p])$, the class group $C_K = \mathrm{Pic}(Y)$ satisfies $C_K[p^\infty] \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{\lambda_K}$.

TABLE 1.3.1. Similarities in structures of class groups

For this reason, we might expect there to be a parallel of Equation 1.1.1 for extensions of $\mathbb{Z}_p$-fields with λ_K playing the role of $2g_Y$. Yûji Kida provided the first such parallel in [Kid80]. Kida's formula explicitly computes (relative) λ-invariants in p-extensions of CM $\mathbb{Z}_p$-fields L/K for an odd prime p. Roughly a year later in [Iwa81], Iwasawa proved a formula for cyclic extensions of $\mathbb{Z}_p$-fields L/K of order p with p any prime, and this formula implies Kida's formula. To state Iwasawa's formula and other results, we need the following definition.

Definition 1.4. For a G-module M with G a cyclic p-group we take $\chi(G, M) \in \mathbb{Z}$ to be the exponent of p in the Herbrand quotient

$$\frac{|H^2(G, M)|}{|H^1(G, M)|} = p^{\chi(G,M)}$$

assuming these quantities are finite.

Theorem 1.5 (Iwasawa's Formula)**.** *Let L/K be a p-extension of $\mathbb{Z}_p$-fields with $\mu_K = 0$. Suppose $G = \mathrm{Gal}(L/K) \cong \mathbb{Z}/(p)$ and that L/K is unramified at the infinite places. Then*

$$\lambda_L = p\lambda_K + (p-1)\chi(G, \mathcal{O}_L^\times) + \sum_{w \nmid p} (e(w) - 1)$$

where the sum runs over all places $w \nmid p$ of L and $e(w)$ is ramification index in L/K.

1.3 Preliminary Results

Preliminary to the main results, we prove the following generalization of Iwasawa's formula which is in direct analogy with Theorem 1.1 in light of Table 1.2.

Proposition 1.6. *Let L/K be a p-extension of $\mathbb{Z}_p$-fields with $\mu_K = 0$. Take $X = \mathrm{Spec}(\mathcal{O}_L[1/p])$, $Y = \mathrm{Spec}(\mathcal{O}_K[1/p])$, and $f\colon X \to Y$ to be the induced morphism. Then*

$$\lambda_L = \deg(f)\lambda_K - (p-1)\chi_{L/K} + \sum_{x \in X} (e_x - 1) \tag{1.6.1}$$

where e_x is the ramification index of f at x. Here $\chi_{L/K}$ is an integer defined as follows: for any composition series $1 = H_0 \lhd H_1 \lhd \cdots \lhd H_n = \mathrm{Gal}(L/K)$ we have

$$\chi_{L/K} = \sum_{i=0}^{n-1} p^i \chi(H_{i+1}/H_i, P_L^{H_i})$$

where $P_L \leq I_L$ is the subgroup of principal ideals in the invertible ideals of $\mathcal{O}_L$.

Iwasawa's formula assumes that the extension L/K is unramified at the infinite primes (e.g., this holds when p is odd), and in that case we may replace the $\chi(G, P_L)$ with $-\chi(G, \mathcal{O}_L^\times)$. However, by stating the formula more generally as above, we can recover and extend the explicit computations of Bruce Ferrero (see [Fer80]) and Yûji Kida (see [Kid79]) for λ-invariants of imaginary quadratic number fields.

Corollary 1.7. *Let K be the cyclotomic $\mathbb{Z}_2$-extension of the first layer k in the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ where p is 2 or a Fermat prime and $h(k)$ is odd (e.g., we can take $p \in \{2, 3, 5, 17, 257\}$). Let L be the cyclotomic $\mathbb{Z}_2$-extension of $k(\sqrt{-d})$ with $d \in \mathbb{Z}$ squarefree and $d > 2 \geq (d, p)$. Then*

$$\lambda_L = |S| - 1$$

where S is the set of finite places of L not lying above 2 which are ramified in L/K.

Remark 1.8. Let $d > 1$ be a squarefree integer with $d \equiv 1 \pmod 4$.

Classical 'genus theory'	Ferrero and Kida
If S_0 is the set of finite primes of ℓ which ramify in $\ell/\mathbb{Q} = \mathbb{Q}(\sqrt{-d})/\mathbb{Q}$, $$C_\ell[2^\infty] \cong \bigoplus_{i=1}^{|S_0|-1} \frac{\mathbb{Z}}{(2^{a_i})}$$ for some integers $a_i \geq 1$.	If S is the set of finite primes of L which ramify in $L/\mathbb{Q}_\infty = \mathbb{Q}_\infty(\sqrt{-d})/\mathbb{Q}_\infty$, $$C_L[2^\infty] \cong \bigoplus_{i=1}^{|S|-1} \varinjlim_a \frac{\mathbb{Z}}{(2^a)} \cong (\mathbb{Q}_2/\mathbb{Z}_2)^{|S|-1}. \quad (1.8.1)$$

TABLE 1.8.1. Comparison of genus theory and Iwasawa theory

The corollary above shows that 1.8.1 continues to hold if we replace $\mathbb{Q}$ with $k \subseteq \mathbb{Q}(\zeta_{p^2})$ such that $[k : \mathbb{Q}] = p \nmid d$ is one of the first four Fermat primes.

1.4 Main Results

My main results stem from special formulas for λ-invariants in cyclic p-extensions of $\mathbb{Z}_p$-fields.

Theorem 1.9. *Let L/K be a cyclic p-extension of $\mathbb{Z}_p$-fields with $\mu_K = 0$. Then*

$$\begin{aligned} \frac{\lambda_L - p^n \lambda_K}{p-1} &= p^{n-1}\chi(H_n, C_L) - \sum_{i=1}^{n-1} \varphi(p^{n-i})\chi(H_n/H_i, C_L^{H_i}) \\ &= \frac{p^n}{np - n + 1}\chi(H_n, C_L) + \sum_{i=1}^{n-1} \frac{p^i(p-1)}{(ip - i + p)(ip - i + 1)}\chi(H_i, C_L) \end{aligned}$$

where φ is the totient function and $1 = H_0 \triangleleft \cdots \triangleleft H_n = \mathrm{Gal}(L/K)$ is the composition series.

One upshot of Theorem 1.9 is a vanishing criterion for λ-invariants in special extensions of $\mathbb{Z}_p$-fields. This generalizes a result of Takashi Fukuda et al. in [FKOT97].

Theorem 1.10. *Let L/K be a cyclic p-extension of $\mathbb{Z}_p$-fields which is unramified at every infinite place. Suppose K is the cyclotomic $\mathbb{Z}_p$-extension of a number field k such that $p \nmid h(k)$ and k has only one prime lying above p. Then $\lambda_L = 0$ if and only if, for all prime ideals $\mathfrak{p}$ of K which ramify in L/K and do not lie over p, the order in C_L of the class of the product of prime ideals of L lying over $\mathfrak{p}$ is prime to p.*

Another application of Theorem 1.9 is the derivation of congruences for Iwasawa λ-invariants. Note that Equations 1.1.1 and 1.6.1 imply that $2g_X \equiv 2g_Y \pmod{p-1}$ and $\lambda_L \equiv \lambda_K \pmod{p-1}$, respectively, when $\deg(f) = p$. However, there are stronger congruences in special cases that cannot be deduced from these formulas. For example, the genus of the Fermat curve $X_d : x^{p^d} + y^{p^d} = z^{p^d}$ over $\mathbb{C}$ is $(p^d-1)(p^d-2)/2$, and X_n/X_{n-1} is cyclic of order p, but in fact

$$2g_{X_n} \equiv 2g_{X_{n-1}} \pmod{p^{n-1}(p-1)}.$$

We can prove an Iwasawa theoretic analog of the above congruence.

Theorem 1.11. *Let $K_0 \subset K_1 \subset \ldots \subset K_n$ be a tower of $\mathbb{Z}_p$-fields with $\mu_{K_0} = 0$ such that for all $i = 0, \ldots, n$ the extension K_i/K_0 is cyclic of degree p^i. Then*

$$\lambda_{K_n} \equiv \lambda_{K_i} \pmod{\varphi(p^{i+1})}$$

for all $i = 0, \ldots, n$.

Additionally, underlying Theorem 1.9 is structural information about the dual of the p-primary class group as a Galois module.

Theorem 1.12. *Let $K_0 \subset K_1 \subset \ldots \subset K_n$ be as in Theorem 1.11. Then for $G_i = \mathrm{Gal}(K_i/K_0)$ we have the following decomposition of $\mathbb{Q}_p$-representations of G_n*

$$C_{K_n}[p^\infty]^* \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong \lambda_{K_0}\pi_{G_n} \oplus \bigoplus_{i=1}^{n} \left(\chi(G_i, C_{K_i}) - \chi(G_{i-1}, C_{K_{i-1}})\right) \pi_{\varphi(p^i)}$$

where $*$ denotes the Pontryagin dual, π_{G_n} is the regular representation, and π_d is the unique faithful irreducible representation of degree $d \in \{\varphi(p), \varphi(p^2), \ldots, \varphi(p^n)\}$.

Note: we can recover the first equality in Theorem 1.9 by taking the degrees of the representations in Theorem 1.12 and collecting like terms.

1.5 Organization

Part I is concerned with known formulas. First, we'll briefly review the Riemann-Hurwitz formula for Riemann surfaces in Chapter 2 and then Kida's formula for number fields in Chapter 3. In both cases, we'll give examples and uses. We will not prove the formula for Riemann surfaces, but we will sketch the ideas involved in the proof of Kida's result. Next, a careful look at Iwasawa's work will be given in Chapter 4. An effort has been made to avoid simply rehashing the articles [Kid80] of Kida and [Iwa81] of Iwasawa by instead including background material, organizing the main arguments succinctly (see the proofs of 3.6, 3.12, and 4.12), elucidating technical points which were left either unclear or overly general (see Lemmas 4.8 and 4.9, Proposition 4.11, and Remark 4.15), and providing original concrete examples (see 2.4, 3.10, and 4.16). Throughout, we attempt to give sufficient motivation before introducing key definitions or results.

Part II addresses proofs of these special formulas and their applications that we derive for cyclic p-extensions of $\mathbb{Z}_p$-fields. First, we prove a few facts about the Euler characteristic $\chi(G, -)$ and outline a general plan of attack for computing invariants (see Lemma 5.1 and Remark 5.2). Then we revisit Iwasawa's formula and prove a slight generalization thereof in Chapter 6 (see Theorem 6.2, Corollary 6.4, and

Remark 6.5). Next, we compute a decomposition of the the $\mathbb{Q}_p$-representation $\pi_{L/K}$ of $G = \mathrm{Gal}(L/K)$ corresponding to the p-class group A_L for degree p extensions L/K of $\mathbb{Z}_p$-fields (see Corollary 6.12). At the end of Chapter 6, we use our generalization of Iwasawa's formula to give a new proof of a result of Ferrero found in [Fer80] as mentioned above (see Lemma 6.15, Proposition 6.16, Remark 6.19, and Proposition 6.24).

In Chapter 7, we use Iwasawa's method to produce special formulas for cyclic extensions of degree p^2, disprove a "natural conjecture," discuss the $\mathbb{Q}_p$-representation $\pi_{L/K}$ again, and finally give an alternative proof for the formulas without using classification theorems of $\mathbb{Z}_pG$-modules (see Proposition 7.2, Corollary 7.3, Example 7.6, Corollary 7.8, Theorem 7.11, and Corollary 7.12).

We close out Part II with Chapter 8 in which special formulas for lambda invariants and $\pi_{L/K}$ in arbitrary cyclic p-extensions are given (see Lemma 8.1, Proposition 8.3, Theorem 8.4, Corollary 8.5, Corollary 8.6, Theorem 8.8, Lemma 8.9, Proposition 8.11, Remark 8.12, and Corollary 8.13). As mentioned above, the main applications of these special formulas include congruences and inequalities for λ-invariants that cannot be gleaned from Iwasawa's formula (see Corollary 8.7). At the end of Chapter 8, we prove the generalized vanishing criterion for λ-invariants mentioned above (see Theorem 8.18).

Part III surveys other directions. First, we discuss formulas for the size of the $q \neq p$-part of the class group in q-extensions (see Proposition 9.5 and Theorem 9.7). Next, we delve into a discussion of schemes and the aforementioned geometric interpretation of Iwasawa's formula (see Proposition 10.8 and Corollary 10.24).

Part I

KNOWN FORMULAS

Chapter 2
CLASSICAL FORMULA FOR SURFACES

In this chapter, we recall the definition of a Riemann surface and of ramification in holomorphic maps, state the classical Riemann-Hurwitz formula, and show by example how this formula can be used to compute an unknown genus for a surface R_1 in terms of a known genus for a familiar surface R_2 via a map $R_1 \to R_2$.

2.1 Background

Definition 2.1. Recall that a **Riemann surface** R is a connected 1-dimensional complex manifold, so R is a *surface* in the sense that it has dimension 2 as a real manifold. In other words, R is a connected, second countable, Hausdorff topological space and there are charts $\{(U_i, \varphi_i)\}_{i \in I}$ with the following three properties

- $\{U_i\}_{i \in I}$ forms an open cover of R
- $\varphi_i : U_i \to \mathbb{C}$ is a homeomorphism onto its image for all $i \in I$
- $\varphi_i \circ \varphi_j^{-1}$ is holomorphic on $\varphi_j(U_i \cap U_j)$ for all $i, j \in I$.

The **genus** of R is defined to be the dimension of the $\mathbb{C}$-vector space of holomorphic one-forms on R, which can be thought of as the number of "handles" in the surface.

Remark 2.2. Let $f : R_1 \to R_2$ be a nonconstant holomorphic map between compact Riemann surfaces and fix $x \in R_1$. Then by definition there are charts $\varphi : U \to \mathbb{C}$ around x and $\psi : V \to \mathbb{C}$ around $f(x)$ such that

- $\psi \circ f \circ \varphi^{-1}$ is holomorphic on $\varphi(U \cap f^{-1}(V))$
- without loss of generality $\varphi(x) = 0 = \psi(f(x))$.

Thus there is a disk $|z| < r$ on which

$$(\psi \circ f \circ \varphi^{-1})(z) = \sum_{n=e(x)}^{\infty} a_n z^n$$

where $a_{e(x)} \neq 0$ and $e(x) \geq 1$ is called the **ramification index** of f at x which is independent of the charts φ, ψ. When $e(x) > 1$, we call x a **ramification point** of f and say f is ramified at x.

2.2 Statement and Applications

Theorem 2.3 (Riemann-Hurwitz, late 1800's)**.** *Let $f : R_1 \to R_2$ be a nonconstant holomorphic map between compact Riemann surfaces. Then*

$$2g_1 - 2 = d(2g_2 - 2) + \sum_{x \in R_1} (e(x) - 1) \tag{2.3.1}$$

*where for $i = 1, 2$ the surface R_i has genus g_i. Here d is the **degree** (number of sheets) of f and for all $y \in R_2$*

$$\sum_{x \in f^{-1}(\{y\})} e(x) = d. \tag{2.3.2}$$

We do not give a proof of this theorem, but an analytic proof of the statement as given above can be found in Section 2.5 of [Jos06] and a combinatorial proof using triangulations can be found on page 19 in [FK80]. However, we want to pay attention to the way this formula is applied so we can get an idea of how useful a number field version might be.

Example 2.4. Consider the Fermat curve

$$F_3 = \{[z_1, z_2, z_3] \in \mathbb{CP}^2 : z_1^3 + z_2^3 + z_3^3 = 0\}$$

with the subspace topology; we regard $\mathbb{CP}^2$ as a 2-dimensional complex manifold having charts

$$x = [z_1, z_2, z_3] \mapsto \begin{cases} (z_2/z_1, z_3/z_1) & \text{on } U_1 = \{x : z_1 \neq 0\} \\ (z_1/z_2, z_3/z_2) & \text{on } U_2 = \{x : z_2 \neq 0\} \\ (z_1/z_3, z_2/z_3) & \text{on } U_3 = \{x : z_3 \neq 0\} \end{cases}$$

and with the quotient topology given via

$$\mathbb{CP}^2 = \frac{\mathbb{C}^3 \backslash \{(0,0,0)\}}{\sim}$$

with $x \sim y \Leftrightarrow x = \lambda y$ for some $\lambda \in \mathbb{C}^\times$. Note that F_3 is a compact Riemann surface as an embedded submanifold of $\mathbb{CP}^2$ since it's the level set of a smooth map $\mathbb{CP}^2 \to \mathbb{C} : [z_1, z_2, z_3] \mapsto z_1^3 + z_2^3 + z_3^3$ of constant rank. We have a natural holomorphic map (see Problem J, Section II.4 from [Mir95])

$$f : F_3 \to \mathbb{CP}^1 : [z_1, z_2, z_3] \mapsto [z_1, z_2].$$

Then for fixed $[z_1, z_2] \in \mathbb{CP}^1$ either

$$[z_1, z_2] \in \{[1, -1], [1, -\omega], [1, -\omega^2]\}$$

where $\omega = e^{2\pi i/3}$, in which case

$$f^{-1}(\{[z_1, z_2]\}) = \{[z_1, z_2, 0]\},$$

or

$$f^{-1}(\{[z_1, z_2]\}) = \{[z_1, z_2, -\alpha], [z_1, z_2, -\omega\alpha], [z_1, z_2, -\omega^2\alpha]\}$$

where $\alpha^3 = z_1^3 + z_2^3 \neq 0$. Hence the degree of f is 3 and there are exactly 3 ramification points

$$[1, -1, 0], [1, -\omega, 0], [1, -\omega^2, 0],$$

each having ramification index 3. We know that $R_2 := \mathbb{CP}^1$ is diffeomorphic as a real manifold to the sphere $\mathbb{S}^2$, so $\mathbb{CP}^1$ has genus $g_2 = 0$ since the sphere has no holes (see Figure 2.1).

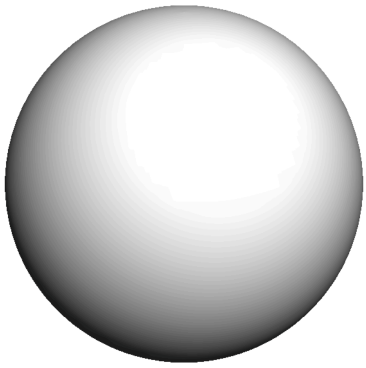


FIGURE 2.1. $R_2 = \mathbb{CP}^1 \approx \mathbb{S}^2$ is a sphere

Hence the Riemann-Hurwitz formula (i.e., equation 2.3.1 in Theorem 2.3 above) with $R_1 := F_3$ gives

$$2g_1 - 2 = 3(2 \cdot 0 - 2) + [(3-1) + (3-1) + (3-1)] = 0,$$

whence F_3 has genus $g_1 = 1$. Thus the classification theorem for closed surfaces implies that F_3 is diffeomorphic as a real manifold to the tours $\mathbb{T}^2$ (see Figure 2.2).

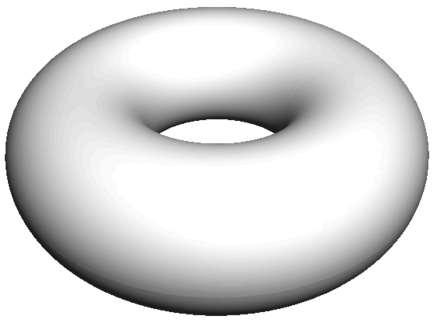


FIGURE 2.2. $R_1 = F_3 \approx \mathbb{T}^2$ is a torus

This means the torus may be "covered" by three sheets, each of which is a copy of the sphere with an incision. The ramification points are then the points where

the sheets overlap. How can we visualize this covering? Let's begin by making a semicircular incision along the equator of the sphere and then flattening/stretching out the resulting sheet into the shape of a rhombus (see Figure 2.3).

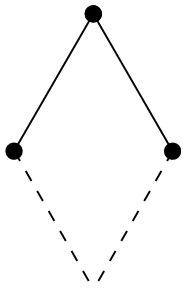


FIGURE 2.3. A sheet in the shape of a rhombus

The solid (respectively dotted) line indicates the presence (respectively absence) of a boundary. Now we bring three of those sheets (rhombi) together in a triangular formation and paste along adjacent sides as suggested in Figure 2.4.

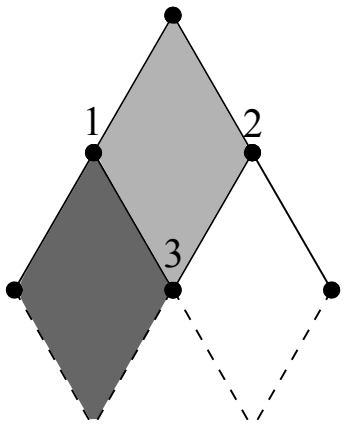


FIGURE 2.4. Three sheets pasted together

Notice that after this pasting the only overlaps are at the points **1**, **2**, and **3** (where two sheets lie on top of one another). Next we form a cylinder by pasting the tab at the top of the previous figure into the slot at the bottom (see Figure 2.5).

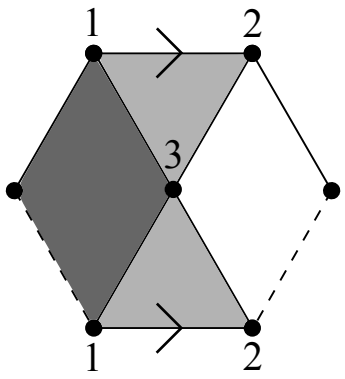


FIGURE 2.5. A cylinder

After this pasting the only overlaps are at the points **1**, **2**, (where two sheets lie on top of one another) and **3** (where now three sheets lie on top of one another). Finally, we form a torus by first twisting the cylinder, then pasting the left and right boundaries together as indicated in Figure 2.6.

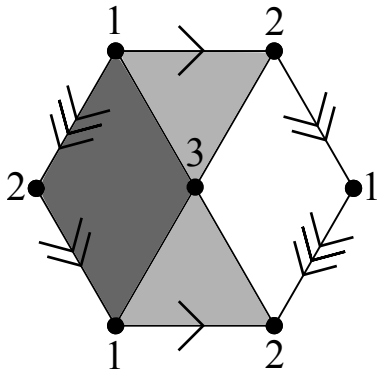


FIGURE 2.6. A torus

Of course, the only overlaps are at the points **1**, **2**, and **3** (where three sheets lie on top of one another); moreover, these points represent the three ramification points of f, each with ramification index 3.

The above example gives an illustration of the usefulness of the Riemann-Hurwitz formula in genus computations. Using similar reasoning, we can show that the genus

g of the Fermat curve

$$F_d := \{[z_1, z_2, z_3] \in \mathbb{CP}^2 : z_1^d + z_2^d + z_3^d = 0\}$$

is given by

$$g = \frac{(d-1)(d-2)}{2}.$$

Remark 2.5. In Example 2.4, both of the Riemann surfaces involved (the sphere and the torus) were *projective algebraic*, meaning that both $\mathbb{CP}^1$ and $F_3 \subseteq \mathbb{CP}^2$ can be regarded as projective varieties with the Zariski topology instead of as complex manifolds with the analytic topology. In fact, any nonsingular projective variety over $\mathbb{C}$ can be regarded as a complex manifold. More generally (as described in Appendix B of [Har97]), there is a functor h from the category of schemes X which are smooth and of finite type over $\mathbb{C}$ to the category of complex manifolds sending X to X_h with the following properties:

- There is a continuous injection $\phi\colon X_h \to X$ such that $\mathrm{im}(\phi)$ is the set of closed points in X.
- X is connected if and only if X_h is connected.
- X is proper over $\mathbb{C}$ if and only if X_h is compact
- If X_h is compact and $X_h \cong Y_h$ as complex manifolds, then $X \cong Y$ as schemes.
- $\dim(X) = \dim(X_h)$

In particular, if X is a connected curve which is smooth and proper over $\mathbb{C}$, then X_h is a compact Riemann surface. There is a converse to this statement. Namely, we have the following theorem.

Theorem 2.6 (Riemann)**.** *For every compact Riemann surface R there exists a connected, normal curve X which is projective over $\mathbb{C}$ such that $X_h \cong R$ as a complex manifold.*

In light of this result, it might not be surprising to learn that there is a general Hurwitz formula for normal, projective curves over fields from which the classical Riemann-Hurwitz formula follows as a corollary. The following theorem, whose development and proof can be found in Chapter 7 of [Liu02], is such a result.

Theorem 2.7. *Let $f\colon X \to Y$ be a finite, separable morphism of normal, projective curves over a field F with* $\deg(f) = d$. *Then*

$$2g_X - 2 = d(2g_Y - 2) + \sum_x (e'_{x/y} - 1)[\mathbb{F}(x) : F]$$

where g_X, g_Y are the arithmetic genera of X, Y, respectively, and the sum extends over the closed points x of X with images y in Y. Here $\mathbb{F}(x)$ is the residue field at x and $e'_{x/y} = e_{x/y}$ is the ramification index when $\mathrm{char}(\mathbb{F}(x)) \nmid e_{x/y}$ *(tame ramification) while $e'_{x/y} > e_{x/y}$ when* $\mathrm{char}(\mathbb{F}(x)) | e_{x/y}$ *(wild ramification).*

Normal projective curves over fields are examples of particularly nice schemes called Dedekind schemes which are curves (schemes of dimension 1) that have the favorable property that their local rings at closed points are discrete valuation rings (DVRs), which are precisely local principal ideal domains that are not fields. An affine Dedekind scheme is the prime spectrum of a Dedekind domain, i.e., an integrally closed Noetherian domain in which every nonzero prime ideal is maximal. One of the main examples of Dedekind domains are the rings of integers in number fields. The remainder of the text will examine the extent to which Riemann-Hurwitz formulas exist for number fields.

Chapter 3
KIDA'S FORMULA FOR CM-FIELDS

At first blush, there may appear to be little or no connection between compact Riemann surfaces and number fields. As mentioned at the end of Chapter 2, however, compact Riemann surfaces arise from normal, projective curves over $\mathbb{C}$ which are schemes of dimension 1 whose local rings are DVRs, and this property is shared by the prime spectra of rings of integers in number fields. We can see some immediate connections with the proceeding observations. Let ℓ/k be an extension of number fields and let $\mathfrak{p}$ be a nonzero prime ideal in the ring of integers $\mathcal{O}_k$ of k. Then $\mathfrak{p}\mathcal{O}_\ell$ factors uniquely into a product of ideals $\mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}$ where each $\mathfrak{P}_i$ is a nonzero prime ideal in $\mathcal{O}_\ell$ with ramification index $e_i = e(\mathfrak{P}_i/\mathfrak{p})$. Moreover, the degree of ℓ/k is

$$\sum_{\mathfrak{P} \in \psi^{-1}(\{\mathfrak{p}\})} e(\mathfrak{P}/\mathfrak{p}) f(\mathfrak{P}/\mathfrak{p}) = [\ell : k]$$

where each $f(\mathfrak{P}_i/\mathfrak{p}) = [\mathcal{O}_\ell/\mathfrak{P}_i : \mathcal{O}_k/\mathfrak{p}]$ is a residue degree and

$$\psi : \mathrm{Spec}(\mathcal{O}_\ell) \to \mathrm{Spec}(\mathcal{O}_k)$$

is given by $\mathfrak{P} \mapsto \mathfrak{P} \cap \mathcal{O}_k$. This gives the analog of equation 2.3.2 in Theorem 2.3. Of course, this is not simply a coincidence, and, in fact, both of these statements are special cases of a more general result from algebraic geometry; specifically, such a result is proved for finite covers of Dedekind schemes in Proposition 1.20 of Chapter 7 from [Sza09].

From the above discussion, it's clear that the ramification of primes in finite extensions of number fields behaves like a branched cover of compact Riemann surfaces, so it seems plausible there should be a formula to determine an invariant of ℓ in terms of the corresponding invariant of k, the degree $[\ell : k]$ of the extension, and a sum

involving the ramification indices of primes. However, it is not all immediate what would be an appropriate invariant or even to which type of extensions such a formula might apply. This chapter is devoted to defining a suitable invariant (= the Iwasawa λ-invariant), deriving a formula (= Kida's formula) of the type found in equation 2.3.1 for certain kinds of extensions (= p-extensions of CM-fields), and then demonstrating how this formula can be used in studying the invariant.

3.1 Background

Remark 3.1. A $\mathbb{Z}_p$**-extension** of a number field k is a field $K \subseteq \mathbb{C}$ such that K/k is Galois and

$$G := \mathrm{Gal}(K/k) \cong \mathbb{Z}_p$$

as topological groups where G has the Krull topology. A subset S of $\mathbb{Z}_p$ is a nontrivial closed subgroup if and only if $S = p^n\mathbb{Z}_p$ for some $n \in \mathbb{N}_0$, so by (infinite) Galois theory the field extensions k_α of k contained in K form a tower

$$k = k_0 \subseteq k_1 \subseteq k_2 \subseteq \ldots \subseteq K$$

such that

$$\mathrm{Gal}(k_n/k) \cong \mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/(p^n)$$

for all $n \in \mathbb{N}_0$. For any such $\mathbb{Z}_p$-extension, the growth of the p-primary parts of the ideal class groups C_{k_n} becomes well-behaved and is described by the following fundamental theorem of Iwasawa theory. The first statement of the theorem appeared in Kenkichi Iwasawa's 1956 invited address *A theorem on Abelian groups and its application to algebraic number theory* at a summer meeting of the American Mathematical Society in Seattle.

Theorem 3.2 (Iwasawa's Growth Formula)**.** *Let K/k be a $\mathbb{Z}_p$-extension. Then there are $\lambda, \mu, \nu \in \mathbb{Z}$ with $\lambda, \mu \geq 0$ such that if p^{e_n} is the exact power of p dividing the class number $h(k_n)$, then*

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

for all sufficiently large n.

Proof. See [Iwa59a] for the first published proof of this result or see Chapter 13, Section 3 in Washington's popular text [Was96]. □

Theorem 3.3. *Let K/k be a $\mathbb{Z}_p$-extension. Then the only primes of k which ramify in K/k lie over p, and one such prime must ramify. Moreover, if*

$$p \nmid h(k)$$

and k has only one prime lying over p, then

$$p \nmid h(k_n)$$

for all $n \in \mathbb{N}_0$, so

$$\lambda = \mu = \nu = 0;$$

in particular, this is always the case for $k = \mathbb{Q}$.

Proof. It's clear that infinite places do not ramify in K/k since infinite places have finite inertia groups (with size 1 or 2) and there are no nontrivial finite subgroups of $\mathbb{Z}_p$. If $\mathfrak{q}$ is a prime ideal of k which ramifies in K/k and p does not divide the absolute norm $N(\mathfrak{q})$, then $\mathfrak{q}$ is tamely ramified in the abelian extension K/k, so the ramification index of $\mathfrak{q}$ in K/k is finite since it divides $N(\mathfrak{q}) - 1$, but this is a contradiction again since there are no nontrivial finite subgroups of $\mathbb{Z}_p$. This shows that only primes lying above p can ramify, but one such prime must ramify since otherwise the infinite extension K would be contained in the Hilbert class field, a finite extension, of k. For a proof of the second statement, see, for example, Proposition (2.1) in [Gre01]. □

Definition 3.4. For given k and p, there may be infinitely many $\mathbb{Z}_p$-extensions K. In fact, it should be noted that if $\widetilde{k}$ is the compositum of all $\mathbb{Z}_p$-extensions of K contained in $\mathbb{C}$, then by Theorem 13.4 in [Was96]

$$\mathrm{Gal}(\widetilde{k}/k) \cong \mathbb{Z}_p^{r_2+1+\delta_k}$$

where r_2 is the number of complex places of k and $\delta_k \geq 0$ is an integer called the **Leopoldt defect** of k. It has been conjectured that $\delta_k = 0$ for all k. The conjecture is true for $k = \mathbb{Q}$ since Theorem 3.3 and the Kronecker Weber theorem together imply that there is a unique $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty$ of $\mathbb{Q}$. We define a $\mathbb{Z}_p$-extension of k

$$k_\infty := k\mathbb{Q}_\infty$$

called the **cyclotomic $\mathbb{Z}_p$-extension** of k (although Iwasawa refers to this k_∞ as a "basic $\mathbb{Z}_p$-extension" in some of his papers). Here k_∞ is the unique $\mathbb{Z}_p$-extension of k contained in $\cup_n k(\zeta_{p^n})$. By taking $K = k_\infty$ in the growth formula we define the **Iwasawa invariants** of k with respect to p as the invariants λ, μ, ν for the extension K/k:

$$\lambda_p(k) = \lambda,\ \mu_p(k) = \mu,\ \nu_p(k) = \nu.$$

From now on we assume all $\mathbb{Z}_p$-extensions are cyclotomic $\mathbb{Z}_p$-extensions. The reason for this will become clear in Chapter 4.

The previous discussion gives no hint why the Iwasawa invariant $\lambda_p(k)$ for a number field k should provide a fitting parallel for twice a genus, but we'll see later that this is indeed the case. We won't be dealing directly with the λ-invariant for the remainder of this chapter, but rather a relative lambda invariant (to be defined below) which is the difference of two such invariants; in that case, the relative lambda invariant is actually a parallel of a genus.

Definition 3.5. A **totally real number field** is a number field whose embeddings are all real, and a **totally complex number field** is a number field with no real

embeddings. A **CM-field** k is a totally complex quadratic extension of a totally real number field k^+. Some examples of CM-fields are $\mathbb{Q}(\zeta_{n+2})$ and $\mathbb{Q}(\sqrt{-n})$ for some $n \in \mathbb{N}$ with $\mathbb{Q}(\zeta_{n+2})^+ = \mathbb{Q}(\zeta_{n+2} + \zeta_{n+2}^{-1})$ and $\mathbb{Q}(\sqrt{-n})^+ = \mathbb{Q}$. Given a CM-field k and prime p, Theorem 3.2 implies that if $p^{e_n^-}$ is the exact power dividing the **relative class number**

$$h^-(k_n) := \frac{h(k_n)}{h(k_n^+)},$$

then

$$e_n^- = \lambda_p^-(k)n + \mu_p^-(k)p^n + \nu_p^-(k)$$

for all sufficiently large n where for $\gamma \in \{\lambda, \mu, \nu\}$ we define the **relative Iwasawa invariant**

$$\gamma_p^-(k) := \gamma_p(k) - \gamma_p(k^+).$$

3.2 Statement and Applications

We're now ready to state Kida's analog of Theorem 2.3. In this result, a subset of the set of primes not lying above p in a cyclotomic $\mathbb{Z}_p$-extension plays the role of a Riemann surface, the relative Iwasawa invariant λ^- plays the role of a genus, and $[\ell_\infty : k_\infty]$ plays the role of the degree of a holomorphic map where ℓ/k is a p-extension of CM-fields. The following is the main theorem in [Kid80].

Theorem 3.6 (Kida, 1979)**.** *Let ℓ/k be a p-extension of CM-fields for some odd prime p. Suppose $\mu_p^-(k) = 0$. Then $\mu_p^-(\ell) = 0$ and we have the formula*

$$2\lambda_p^-(\ell) - 2\delta = [\ell_\infty : k_\infty](2\lambda_p^-(k) - 2\delta) + \sum_{\mathfrak{P} \in S(\ell)} (e(\mathfrak{P}) - 1)$$

where δ is 1 or 0 if $\zeta_p \in k$ or $\zeta_p \notin k$, respectively, $e(\mathfrak{P})$ is the ramification index of $\mathfrak{P}$ in ℓ_∞/k_∞, and

$$S(\ell) := \{\textit{prime ideals } \mathfrak{P} \nmid p \textit{ in } \ell_\infty : \mathfrak{P} \cap \mathcal{O}_{\ell_\infty^+} \textit{ splits in } \ell_\infty/\ell_\infty^+\}.$$

A few remarks are in order about the technical hypotheses needed for Kida's formula above. First, the assumption $\mu_p^-(k) = 0$ holds in many useful contexts as the following famous theorem (proved in [FW79]) implies.

Theorem 3.7 (Ferrero-Washington, 1979)**.** *Let k be an abelian number field and p be a prime. Then*

$$\mu_p(k) = 0.$$

In fact, it is not known if the abelian assumption in Theorem 3.7 is needed.

Conjecture 3.8 (Iwasawa)**.** *Let k be a number field and p be a prime. Then*

$$\mu_p(k) = 0.$$

In addition, we may be able to replace the relative Iwasawa invariants λ^-, μ^- with λ, μ in Kida's formula, as the following conjecture suggests.

Conjecture 3.9 (Greenberg)**.** *Let k^+ be a totally real number field and p be a prime. Then*

$$\lambda_p(k^+) = \mu_p(k^+) = 0.$$

These observations help explain why Kida's formula is more applicable than it appears, as we'll see with the following example.

Example 3.10. Consider the uniquely determined field ℓ^+ in the following tower.

$$\begin{array}{c} \mathbb{Q}(\zeta_{13}) \\ \Big| 2 \\ \mathbb{Q}(\cos(2\pi/13)) \\ \Big| 2 \\ \ell^+ \\ \Big| 3 \\ \mathbb{Q} \end{array}$$

Then $\ell^+/\mathbb{Q}$

- is a totally real Galois extension with $\mathrm{Gal}(\ell^+/\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$,
- is totally ramified at 13,
- and is unramified outside 13.

Therefore $\ell^+(i)/\mathbb{Q}(i)$ is a $\mathbb{Z}/3\mathbb{Z}$-extension of CM-fields and

$$\lambda_3^-(\mathbb{Q}(i)) = \mu_3^-(\mathbb{Q}(i)) = 0$$

by Theorem 3.3 since 3 remains prime in $\mathbb{Q}(i)/\mathbb{Q}$ and $\mathbb{Q}(i)$ has class number 1. Hence we may apply Kida's formula with $p = 3$, $k = \mathbb{Q}(i)$, and $\ell = \ell^+(i)$, to get

$$2\lambda_3^-(\ell) - 2 \cdot 0 = [\ell_\infty : k_\infty](2 \cdot 0 - 2 \cdot 0) + \sum_{\mathfrak{P} \in S(\ell)} (e(\mathfrak{P}) - 1).$$

Of course, $[\ell_\infty : k_\infty] = 3$ since $[\ell_\infty : k_\infty]$ divides $[\ell : k] = 3$ while $\ell_\infty \neq k_\infty$ because 13 ramifies in $\ell_\infty/\mathbb{Q}$ but not in $k_\infty/\mathbb{Q}$. Thus

$$\begin{aligned} \lambda_3^-(\ell) &= \frac{1}{2} \sum_{\mathfrak{P} \in S(\ell)} (e(\mathfrak{P}) - 1) \\ &= \#\{\mathfrak{P} \in S(\ell) : e(\mathfrak{P}) > 1\}. \end{aligned}$$

We can use induction to show that $3^{n+1} || 13^{3^n} - 1$ for all $n \in \mathbb{N}_0$, so 13 remains prime in $\mathbb{Q}_\infty$ since it remains prime in every intermediate field $\mathbb{Q}(\zeta_{3^n})^+$ with $n \in \mathbb{N}$. (In fact, it's enough to note that 13 remains prime in the first level; in general, for any rational prime q there is an $n \in \mathbb{N}_0$ such that q splits completely in $\mathbb{Q}_n/\mathbb{Q}$ and does not split in $\mathbb{Q}_\infty/\mathbb{Q}_n$.) On the other hand, 13 splits in $\mathbb{Q}(i)/\mathbb{Q}$, so there is a unique prime ideal in $\mathcal{O}_{\ell_\infty^+}$ lying over 13, and it splits into two prime ideals $\mathfrak{P}_1, \mathfrak{P}_2$ in $\ell_\infty/\ell_\infty^+$ each of which ramifies in ℓ_∞/k_∞. Therefore the only primes of $S(\ell)$ which ramify in ℓ_∞/k_∞ are $\mathfrak{P}_1, \mathfrak{P}_2$ since any such prime must lie above either 2 or 13 (because these are the only primes in $\mathbb{Q}$ other than 3 which ramify in $\ell_\infty^+(i)/\mathbb{Q}$) but no prime lying above 2 ramifies in ℓ_∞/k_∞ since 2 does not ramify in $\ell^+/\mathbb{Q}$. We conclude $\lambda_3^-(\ell) = 2$.

Moreover, using a more general construction of the same flavor, Kida's formula can be used to prove the following remarkable result found in [FOO06].

Theorem 3.11 (Fujii-Ohgi-Ozaki, 2006)**.** *Let $p \in \{3, 5\}$ and $n \in \mathbb{N}_0$. Then there is a CM-field ℓ such that $\mu_p(\ell) = \mu_p^-(\ell) = 0$ and*

$$\lambda_p(\ell) = \lambda_p^-(\ell) = n.$$

3.3 Outline of Kida's Argument

Now we'll sketch part of the proof that Kida originally gave for Theorem 3.6 in his 1980 paper [Kid80]. A special case of the theorem is presented first. Then the version as stated above is deduced from this. Later, will give a proof of the special case using the techniques found in [Iwa81], so we forego the proof here. An alternate proof of Kida's formula was provided in [Sin84] by Sinnott using p-adic L-functions.

Theorem 3.12 (Special Case of Theorem 3.6)**.** *Let ℓ/k be a p-extension of CM-fields for some odd prime p. Suppose $\mu_p^-(k) = 0$ and $[\ell : k] = [\ell_\infty : k_\infty] = p$. Define s_∞ to be half the number of ramified primes in $S(\ell)$. Then $\mu_p^-(\ell) = 0$ and*

$$\lambda_p^-(\ell) = p\lambda_p^-(k) + (p-1)(s_\infty - \delta),$$

where $\delta = 1$ if $\zeta_p \in k$ while $\delta = 0$ if $\zeta_p \notin k$.

Proof. See Remark 4.15. □

Proof of Theorem 3.6. We have $\mu_p^-(k) = 0 \Rightarrow \mu_p^-(\ell) = 0$ by, for example, [Iwa73a]. Assume first that $[\ell : k] = [\ell_\infty : k_\infty] = p^{m+1}$ for some $m \in \mathbb{N}_0$. We'll show Theorem 3.6 holds for this case by induction on m. The base case $m = 0$ holds by Theorem 3.12. Suppose then that Theorem 3.6 holds for p-extensions ℓ'/k' of CM-fields with $\mu_p^-(k') = 0$ and $[\ell' : k'] = [\ell'_\infty : k'_\infty] = p^m$. We know there is an intermediate field k'' such that k''/k is Galois and $[\ell : k''] = [\ell_\infty : k''_\infty] = p$. (This field corresponds to the

cyclic subgroup generated by an element of order p in the center of $\mathrm{Gal}(\ell/k)$.) In fact, k'' must be a CM-field, so Theorem 3.6 is true for k''/k by our induction hypothesis, giving $\mu_p^-(k'') = 0$ and

$$\lambda_p^-(k'') - \delta = p^m(\lambda_p^-(k) - \delta) + \frac{1}{2}\sum_{\mathfrak{p}\in S(k'')}(e''(\mathfrak{p}) - 1)$$

where $e''(\mathfrak{p})$ is the ramification index of $\mathfrak{p}$ in k''_∞/k_∞. Consequently, Theorem 3.6 must also be true for ℓ/k'', so $\mu_p^-(\ell) = 0$ and

$$\lambda_p^-(\ell) - \delta = p(\lambda_p^-(k'') - \delta) + \frac{1}{2}\sum_{\mathfrak{P}\in S(\ell)}(e'(\mathfrak{P}) - 1)$$

where $e'(\mathfrak{P})$ is the ramification index of $\mathfrak{P}$ in ℓ_∞/k''_∞. Each $\mathfrak{p} \in S(k'')$ must either ramify or split in ℓ_∞/k''_∞. To see this, note that $\mathfrak{p}$ is unramified (see Theorem 3.3) and finitely split in k''_∞/k'' (which we'll prove in Lemma 4.2), so the residue field of $\mathfrak{p}$ in k''_∞ is of the form $\mathbb{F}_{q^{p^\infty}}$ which has no extensions of degree p and thus $\mathfrak{p}$ cannot remain inert in ℓ_∞/k''_∞. If $\mathfrak{p}$ ramifies, then there is a unique $\mathfrak{P} \in S(\ell)$ lying over $\mathfrak{p}$, in which case

$$e(\mathfrak{P}) - 1 = e'(\mathfrak{P})e''(\mathfrak{p}) - 1 = pe''(\mathfrak{p}) - 1 = e'(\mathfrak{P}) - 1 + p(e''(\mathfrak{p}) - 1).$$

If $\mathfrak{p}$ splits, then there are exactly p primes $\mathfrak{P}_1, \ldots, \mathfrak{P}_p \in S(\ell)$ lying over $\mathfrak{p}$, in which case

$$\sum_{i=1}^{p}(e(\mathfrak{P}_i) - 1) = \sum_{i=1}^{p}(e''(\mathfrak{p}) - 1) = \sum_{i=1}^{p}(e'(\mathfrak{P}_i) - 1) + p(e''(\mathfrak{p}) - 1).$$

Therefore

$$\sum_{\mathfrak{P}\in S(\ell)}(e(\mathfrak{P}) - 1) = \sum_{\mathfrak{P}\in S(\ell)}(e'(\mathfrak{P}) - 1) + p\sum_{\mathfrak{p}\in S(k'')}(e''(\mathfrak{p}) - 1),$$

so

$$\begin{aligned}\lambda_p^-(\ell) - \delta &= p\left(p^m(\lambda_p^-(k) - \delta) + \frac{1}{2}\sum_{\mathfrak{p}\in S(k'')}(e''(\mathfrak{p}) - 1)\right) + \frac{1}{2}\sum_{\mathfrak{P}\in S(\ell)}(e'(\mathfrak{P}) - 1)\\ &= p^{m+1}(\lambda_p^-(k) - \delta) + \frac{1}{2}\sum_{\mathfrak{P}\in S(\ell)}(e(\mathfrak{P}) - 1),\end{aligned}$$

whence Theorem 3.6 is true whenever $[\ell : k] = [\ell_\infty : k_\infty]$. If $[\ell : k] \neq [\ell_\infty : k_\infty]$, then there is a CM-field k' such that $k'_\infty = k_\infty$ and ℓ/k' is Galois extension of degree $[\ell_\infty : k_\infty]$. It turns out that $\lambda_p^-(k') = \lambda_p^-(k)$ (see Corollary 4.5 below), so the theorem holds in this case as well. $\square$

Chapter 4
IWASAWA'S FORMULA FOR $\mathbb{Z}_p$-FIELDS

As promised, we now examine a more general number theoretic Riemann-Hurwitz formula proved by Iwasawa in [Iwa81]. In the paper, Iwasawa proves various decomposition formulas for representations of Galois groups and then obtains expressions involving λ-invariants by taking the degrees of the representations. Since we are only interested here in the invariants we will not prove the statements about representations (although one does not have to do much more work than is done below to get them).

4.1 Background and Lemmas

Definition 4.1. A **$\mathbb{Z}_p$-field** $K \subseteq \mathbb{C}$ for some prime p is a finite extension $K/\mathbb{Q}_\infty$. Equivalently, $K = k_\infty$ is the cyclotomic $\mathbb{Z}_p$-extension of a number field k. To see the equivalence of these definitions, note that the primitive element theorem implies a $\mathbb{Z}_p$-field is of the form $\mathbb{Q}_\infty(\alpha) = \mathbb{Q}(\alpha)_\infty$ for some $\alpha \in \mathbb{C}$ algebraic over $\mathbb{Q}_\infty$, and $\mathbb{Q}(\alpha)$ is a number field since α is also algebraic over $\mathbb{Q}$.

Lemma 4.2. *Let K be a $\mathbb{Z}_p$-field. Given a rational prime q, there are only finitely many finite places v of K above q.*

Proof. Note that the decomposition subgroup Z in $\mathrm{Gal}(K/k) \cong \mathbb{Z}_p$ of a finite place v above q is closed, so Z is either trivial or has finite index. However, Z cannot be trivial since $[K_v : k_{v|_k}] = \infty$ because $[\cup_n \mathbb{Q}_q(\zeta_{p^n}) : \mathbb{Q}_q] = \infty$. □

Remark 4.3. Let $K = k_\infty$ be a $\mathbb{Z}_p$-field. Let v be a finite place of K, and for each $n \in \mathbb{N}_0$ let $v(n)$ be the place of k_n below v. For $n \in \mathbb{N}_0 \cup \{\infty\}$, let I_{k_n} denote the group of invertible ideals of $\mathcal{O}_{k_n}$. If $m \in \mathbb{N}_0$, then the cyclic subgroup $I_{v(m)} \leq I_{k_m}$

generated by the maximal ideal in $\mathcal{O}_{k_m}$ associated to $v(m)$ injects into $I_{v(n)}$ whenever $m \leq n \in \mathbb{N}_0$. Thus we may define a subgroup $I_v \leq I_K$ of invertible ideals of K by

$$I_v := \varinjlim_n I_{v(n)}.$$

(Note that I_v is independent of k since if also $K = k'_\infty$, then $k_m = kk' = k'_n$ for some $m, n \in \mathbb{N}_0$.) In fact,

$$\varinjlim_n I_{k_n} \cong I_K = \bigoplus_v I_v$$

where v ranges over all finite places on K with

$$I_v \cong \begin{cases} \mathbb{Z} & \text{if } v \nmid p \\ \bigcup_{n \geq 0} p^{-n}\mathbb{Z} & \text{if } v|p. \end{cases}$$

As usual, we define **class group** of K by $C_K := I_K/P_K$ where

$$P_K := \{x\mathcal{O}_K : x \in K^\times\}$$

is the subgroup of principal inveritble ideals. We write A_K for the p-primary part of C_K.

Now we state a crucial structure theorem for A_K whose proof may be found in [Iwa73b], [Iwa59a], or Proposition 2.5.1 in [Gre10]. Since A_K is a torsion abelian p-group, we may regard it as a torsion $\mathbb{Z}_p$-module.

Theorem 4.4. *Let $K = k_\infty$ be a $\mathbb{Z}_p$-field. Then there is a $\mathbb{Z}_p$-module A' such that*

$$A_K \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{\lambda_p(k)} \oplus A'$$

as $\mathbb{Z}_p$-modules where $p^n A' = 0$ for some $n \in \mathbb{N}_0$. Moreover, $\mu_p(k) = 0$ implies $A' = 0$, and $\mu_p(k) > 0$ implies A' is infinite.

Corollary 4.5. *Let $K = k_\infty$ be a $\mathbb{Z}_p$-field. Suppose $K = k'_\infty$ for another number field k'. Then $\lambda_p(k') = \lambda_p(k)$, and $\mu_p(k') = 0$ if and only if $\mu_p(k) = 0$.*

Proof. We have

$$A_K \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{\lambda_p(k)} \oplus A' \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{\lambda_p(k')} \oplus A''$$

where $p^n A' = p^m A'' = 0$ for some $n, m \in \mathbb{N}_0$. Multiplication by p^{n+m} is a surjective $\mathbb{Z}_p$-endomorphism on $\mathbb{Q}_p/\mathbb{Z}_p$, so if $\phi\colon A_K \to A_K$ is multiplication by p^{n+m}, then

$$(\mathbb{Q}_p/\mathbb{Z}_p)^{\lambda_p(k)} \cong \mathrm{im}(\phi) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{\lambda_p(k')}$$

as $\mathbb{Z}_p$-modules, so applying the functor $\mathrm{Hom}_{\mathbb{Z}_p}(-, \mathbb{Q}_p/\mathbb{Z}_p)$ yields

$$\mathbb{Z}_p^{\lambda_p(k)} \cong \mathbb{Z}_p^{\lambda_p(k')}$$

as $\mathbb{Z}_p$-modules, whence $\lambda_p(k) = \lambda_p(k')$ upon comparing ranks since $\mathbb{Z}_p$ is a PID. The second statement follows by observing that

$$\mu_p(k') = 0 \Rightarrow A'' = 0 \Rightarrow \dim_{\mathbb{F}_p}(A_K/pA_K) = 0$$

while $\mu_p(k') > 0 \Rightarrow A'' \neq pA'' \Rightarrow \dim_{\mathbb{F}_p}(A_K/pA_K) > 0$. □

Definition 4.6. Let $K = k_\infty$ be a $\mathbb{Z}_p$-field. Then by Corollary 4.5 we may define $\lambda_K := \lambda_p(k)$, and we may write $\mu_K = 0$ whenever $\mu_p(k) = 0$.

With Theorem 4.4 in hand, we can now explain (as in [Iwa65]) why λ_K provides an apt counterpart for twice the genus. Let $\mathcal{C}$ be a nonsingular, projective curve[1] over an algebraically closed field $\overline{F}$; e.g., we've noted that a compact Riemann surface arises from such a curve with $\overline{F} = \mathbb{C}$. At the beginning of Chapter 3, we saw that nonzero prime ideals in the ring of integers for a number field k act like points on a surface with respect to ramification. In fact, the natural analog for I_k is the free $\mathbb{Z}$-module $\mathrm{Div}(\mathcal{C})$ (the divisor group) generated by the closed points on $\mathcal{C}$ since they are both groups of discretely valued places. However, if $K = k_\infty$ is the cyclotomic $\mathbb{Z}_p$-extension for some prime p, then $I_K \cong \varinjlim_n I_{k_n}$ as defined above is no longer the free

[1] by a curve I mean a separated, integral scheme of dimension one

$\mathbb{Z}$-module generated by the nonzero primes of $\mathcal{O}_K$. As we'll see, the right match for the class group C_K is the Jacobian $J(\mathcal{C}) := \mathrm{Div}^0(\mathcal{C})/P(\mathcal{C})$ where $\mathrm{Div}^0(\mathcal{C}) \leq \mathrm{Div}(\mathcal{C})$ is the subgroup of divisors degree 0 and $P(\mathcal{C})$ is the set of principal divisors. If $p \neq \mathrm{char}(\overline{F})$, the p-primary part $J_p(\mathcal{C})$ of the Jacobian satisfies

$$J_p(\mathcal{C}) \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{2g}$$

as $\mathbb{Z}_p$-modules where the genus g of $\mathcal{C}$ is defined to be the $\overline{F}$-dimension of the space $\Omega^1_{\mathcal{C}/\overline{F}}$ of all regular differential one-forms on $\mathcal{C}$. Equivalently, g is the dimension of the canonical divisor class (see [Sha94]). When $\mu_K = 0$, this is exactly the same result one obtains for A_K with λ_K filling the part of $2g$.

As found above, p-extensions of CM-fields (as compared to nonconstant holomorphic maps) formed the right framework for Kida's formula, so since we wish to derive a similar formula for general $\mathbb{Z}_p$-fields it's natural to consider (as we do in Remark 4.7 below) Galois extensions of $\mathbb{Z}_p$-fields.

We'll also find the need to study Galois cohomology groups and duality thereof. To motivate why we should do so, we briefly explain here a Riemann-Hurwitz formula similar to Theorem 2.3 for nonsingular, projective curves over an algebraically closed field $\overline{F}$. One method to prove the result for a finite, separable morphism $f\colon \mathcal{C}_1 \to \mathcal{C}_2$ of these curves is by using the induced short exact sequence of relative differential sheaves on $\mathcal{C}_1$

$$0 \to f^*\Omega_{\mathcal{C}_2/\overline{F}} \to \Omega_{\mathcal{C}_1/\overline{F}} \to \Omega_{\mathcal{C}_1/\mathcal{C}_2} \to 0$$

to obtain a long exact sequence of $\overline{F}$-vector spaces in sheaf cohomology. Then we take Euler characteristics χ. Next, we let g_i be the genus of $\mathcal{C}_i$ and use Serre duality to compute

$$\chi(\Omega_{\mathcal{C}_i/\overline{F}}) = -\chi(\mathcal{O}_{\mathcal{C}_i}) = g_i - 1.$$

Then we let K_2 be a canonical divisor of $\mathcal{C}_2$, n be the degree of f, and apply Riemann-Roch to compute

$$\chi(f^*\Omega_{\mathcal{C}_2/\overline{F}}) = \chi(f^*K_2) = \deg(f^*K_2) + 1 - g_1 = n(2g_2 - 2) + 1 - g_1.$$

Putting it all together, we get

$$2g_1 - 2 = n(2g_2 - 2) + \chi(\Omega_{\mathcal{C}_1/\mathcal{C}_2}) = n(2g_2 - 2) + \deg(D)$$

where D is the ramification divisor for f. We cannot mimic this proof exactly, but we can use some of the same type of techniques. In particular, we'll use short exact sequences of G-modules and group cohomology instead of short exact sequences of sheaves and sheaf cohomology, and we'll use Herbrand quotients instead of Euler characteristics.

Remark 4.7. Assume L/K is a finite Galois extension of $\mathbb{Z}_p$-fields with $G := \mathrm{Gal}(L/K)$. Then I_K, I_L are naturally G-modules, and for each finite place v of K we find that

$$I_{L,v} := \bigoplus_{w|v} I_w$$

is a G-submodule of I_L. Thus Remark 4.3 implies

$$I_L = \bigoplus_{v} I_{L,v}$$

as G-modules where v ranges over all finite places of K, so taking group cohomology gives

$$H^n(L/K, I_L) \cong \bigoplus_{v} H^n(L/K, I_{L,v})$$

for all $n \in \mathbb{N}_0$.

We'll need the following two lemmas when computing with long exact sequences on group cohomology.

Lemma 4.8. *Let L/K be a finite p-extension of $\mathbb{Z}_p$-fields for some prime p. Suppose v is a finite place on K. Then for all $n \in \mathbb{N}$ we have*

$$H^n(L/K, I_{L,v}) \cong \begin{cases} \mathbb{Z}/e\mathbb{Z} & \text{if } v \nmid p \text{ and } 2|n \\ 0 & \text{otherwise} \end{cases}$$

as abelian groups where e is the ramification index of v in L/K.

Proof. First, suppose $v \nmid p$. Let w be a place on L which lies over v, and let $Z \leq G := \mathrm{Gal}(L/K)$ denote the decomposition group of w. Then

$$I_{L,v} \cong \mathbb{Z}(G/Z) \cong \mathrm{Hom}_Z(\mathbb{Z}G, \mathbb{Z})$$

as G-modules where $\mathbb{Z}$ has trivial G-action, so for all $n \in \mathbb{N}$ Shapiro's lemma implies

$$H^n(L/K, I_{L,v}) \cong H^n(G, \mathrm{Hom}_Z(\mathbb{Z}G, \mathbb{Z})) \cong H^n(Z, \mathbb{Z})$$

as abelian groups. On the other hand, v is tamely ramified in the p-extension L/K, so $Z \cong \mathbb{Z}/e\mathbb{Z}$ since the decomposition group Z is equal to the inertia group here, giving

$$H^n(L/K, I_{L,v}) \cong \begin{cases} H^2(\mathbb{Z}/e\mathbb{Z}, \mathbb{Z}) \cong (\mathbb{Z}/e\mathbb{Z}) \otimes_{\mathbb{Z}} \mathbb{Z} \cong \mathbb{Z}/e\mathbb{Z} & \text{if } 2|n \\ H^1(\mathbb{Z}/e\mathbb{Z}, \mathbb{Z}) \cong \mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}/e\mathbb{Z}, \mathbb{Z}) \cong 0 & \text{if } 2 \nmid n \end{cases}$$

for all $n \in \mathbb{N}$.

Now suppose $v|p$. Then Remark 4.3 implies $I_{L,v} \cong (\cup_{n \geq 0} p^{-n}\mathbb{Z})^g$ as abelian groups for some $g \in \mathbb{N}$, so for each $a \in I_{L,v}$ there is a unique $a' \in I_{L,v}$ such that $a = pa'$. On the other hand, G is a finite p-group, so by Corollary 16.5 in [HS97] we have

$$p^m H^n(G, I_{L,v}) = 0$$

for all $n \in \mathbb{N}$ where $|G| = p^m$. Thus

$$H^n(L/K, I_{L,v}) \cong 0$$

for all $n \in \mathbb{N}$. □

Lemma 4.9. *Let L/K be a cyclic p-extension of $\mathbb{Z}_p$-fields for some prime p. Suppose L/K is unramified at every infinite place of K. Then for all $n \in \mathbb{N}$ we have*

$$H^n(L/K, L^\times) \cong 0.$$

Proof. We know that $H^1(L/K, L^\times) \cong 0$ by Hilbert's Theorem 90, so since $G := \mathrm{Gal}(L/K)$ is cyclic it suffices to show $H^2(L/K, L^\times) \cong 0$. As argued in Chapter 5 of [Koc97],

$$H^2(L/K, L^\times) \cong \mathrm{Br}(L/K)$$

where $\mathrm{Br}(L/K)$ is the kernel of the natural homomorphism on Brauer groups

$$\phi\colon \mathrm{Br}(K) \to \mathrm{Br}(L).$$

In fact, $\mathrm{Br}(L/K)$ is contained in the p-part of $\mathrm{Br}(K)$ since G is a finite p-group, so if $L = \ell_\infty$ and $K = k_\infty$ for some number fields ℓ and k, then by the proof of Proposition 9 in Chapter II of [Ser97] it's enough to show that for sufficiently large $n \in \mathbb{N}_0$ the natural map

$$\phi_{n,\infty}\colon \bigoplus_{v|\infty} \mathrm{Br}(k_{n,v}) \to \bigoplus_{w|\infty} \mathrm{Br}(\ell_{n,w})$$

is injective where v and w range over all infinite places of k_n and ℓ_n, respectively. Choose n large enough so that ℓ_n/k_n is unramified at every infinite place of k_n. Fix $x = (x_v) \in \ker(\phi_{n,\infty})$. Suppose $x \neq 0$. Then $x_v \neq 0$ for some real place v on k_n, so $x_v \in \mathrm{Br}(k_{n,v}) \cong \mathrm{Br}(\mathbb{R}) = \{[\mathbb{R}], [\mathbb{H}]\}$ corresponds to the quaternion algebra $\mathbb{H}$. Thus for each real place w on ℓ_n lying over v we have that $\phi_{n,\infty}(x)_w \in \mathrm{Br}(\ell_{n,w}) \cong \mathrm{Br}(\mathbb{R})$ also corresponds to the quaternion algebra, but $\phi_{n,\infty}(x) = 0$, so there are no such real places lying over v, which is a contradiction since ℓ_n/k_n is unramified at every infinite place of k_n. □

Next, we define a **p-Pontryagin dual functor** $*$ on (compact or discrete) $\mathbb{Z}_pG$-modules and then prove a congener of Serre duality for group cohomology.

Definition 4.10. Let G be a cyclic p-group. Fix a $\mathbb{Z}_pG$-homomorphism $\varphi\colon A \to B$, and define $\varphi^*\colon B^* \to A^*$ by mapping $f \in B^* := \mathrm{Hom}_{\mathbb{Z}_p}(B, \mathbb{Q}_p/\mathbb{Z}_p)$ to

$$\varphi^*(f) := f \circ \varphi \in A^* := \mathrm{Hom}_{\mathbb{Z}_p}(A, \mathbb{Q}_p/\mathbb{Z}_p).$$

The following proposition is a special of a more general duality (see, for example, [NSW08]), but we give here an ad hoc proof for completeness.

Proposition 4.11. *Let G be a cyclic p-group. Then $*$ defines an exact, additive contravariant functor from the category of $\mathbb{Z}_pG$-modules A to itself such that we have $\mathbb{Z}_pG$-isomorphisms*

(1) $H^n(G, A^*) \cong H_n(G, A)^*$ for all $n \in \mathbb{N}_0$

(2) $\mathbb{Z}_p^* \cong \mathbb{Q}_p/\mathbb{Z}_p$

(3) $(\mathbb{Q}_p/\mathbb{Z}_p)^* \cong \mathbb{Z}_p$

where A^* has the diagonal action of G and $\mathbb{Z}_p, \mathbb{Q}_p/\mathbb{Z}_p$ have the trivial action of G.

Proof. It's clear that $*$ is a well-defined additive contravariant functor, and exactness follows by observing that $\mathbb{Q}_p/\mathbb{Z}_p$ is an injective $\mathbb{Z}_p$-module. Write $G = \langle g \rangle$ with $|G| = p^m$ and define $\mathbb{Z}_pG$-endomorphisms

$$\varphi_{A,g}\colon A \to A\colon a \mapsto (g-1)a$$
$$\psi_{A,g}\colon A \to A\colon (g^{p^m-1} + \cdots + 1)a,$$

so that $\mathrm{im}(\psi_{A,g}) \subseteq A^G$ and by cyclicity of G (see Section 7 of Chapter IV in [HS97])

$$H^1(G, A) \cong \frac{\ker(\psi_{A,g})}{\mathrm{im}(\varphi_{A,g})} \cong H_2(G, A)$$
$$H^2(G, A) \cong \frac{\ker(\varphi_{A,g})}{\mathrm{im}(\psi_{A,g})} \cong H_1(G, A).$$

Note that the map $\psi_{A,g}$ is actually independent of the choice of generator g, as are the sets $\ker(\varphi_{A,g})$ and $\mathrm{im}(\varphi_{A,g})$; the notation is merely for symmetry and consistency.

To prove (1) for $n = 0$, let $\iota\colon A^G \hookrightarrow A$ denote the inclusion mapping, and note that the induced $\mathbb{Z}_pG$-epimorphism

$$\iota^*\colon A^* \to (A^G)^*$$

has kernel precisely $(g^{-1} - 1)A^*$ since

$$\begin{aligned} f \in \ker(\iota^*) \Leftrightarrow f|_{A^G} = 0 \Leftrightarrow \ker(f) \supseteq A^G = \ker(\varphi_{A,g}) \\ \Leftrightarrow f \text{ descends to map on } A/\ker(\varphi_{A,g}) \cong \operatorname{im}(\varphi_{A,g}). \end{aligned}$$

To prove (1) for $n \geq 1$, first note that the canonical surjections

$$\begin{aligned} \pi_1\colon A &\twoheadrightarrow \operatorname{coker}(\psi_{A,g}), \\ \pi_2\colon A &\twoheadrightarrow \operatorname{coim}(\varphi_{A,g}) \end{aligned}$$

induce $\mathbb{Z}_pG$-isomorphisms

$$\begin{aligned} \alpha_1 &:= \pi_1^*|^{\ker(\psi^*_{A,g})}\colon \operatorname{coker}(\psi_{A,g})^* \to \ker(\psi^*_{A,g}) = \ker(\psi_{A^*,g^{-1}}) \\ \alpha_2 &:= \pi_2^*|^{\operatorname{im}(\varphi^*_{A,g})}\colon \operatorname{coim}(\psi_{A,g})^* \to \operatorname{im}(\varphi^*_{A,g}) = \operatorname{im}(\varphi_{A^*,g^{-1}}). \end{aligned}$$

In fact, for the natural maps

$$\begin{aligned} i\colon \operatorname{im}(\varphi_{A^*,g^{-1}}) &\hookrightarrow \ker(\psi_{A^*,g^{-1}}) \\ j\colon \operatorname{coker}(\psi_{A,g}) &\twoheadrightarrow \operatorname{coim}(\varphi_{A,g}) \end{aligned}$$

we have $i = \alpha_1 \circ j^* \alpha_2^{-1}$, so

$$H^1(G, A^*) \cong \operatorname{coker}(i) \cong \operatorname{coker}(j^*) \cong \ker(j)^* \cong H_1(G, A)^*,$$

and similarly $H^2(G, A^*) \cong H_2(G, A)^*$. Statements (2), (3) are clear. □

4.2 Statement, Proof, and Applications

Theorem 4.12 (Iwasawa, 1980)**.** *Let L/K be a $\mathbb{Z}/(p)$-extension of $\mathbb{Z}_p$-fields for some prime p. Suppose L/K is unramified at every infinite place of K and that $\mu_K = 0$.*

Then $\mu_L = 0$ and we have the formula

$$\lambda_L + H = [L : K](\lambda_K + H) + \sum_{w \nmid p}(e(w) - 1)$$

where $e(w)$ is the ramification index in L/K of a finite place $w \nmid p$ of L, and

$$p^H = \mathrm{q}(\mathcal{O}_L^\times) = \frac{|H^2(L/K, \mathcal{O}_L^\times)|}{|H^1(L/K, \mathcal{O}_L^\times)|}$$

is the Herbrand quotient of the $\mathrm{Gal}(L/K)$*-module $\mathcal{O}_L^\times$.*

Proof. First, we use the ideas found in [Iwa73a] to show $\mu_L = 0$. We know there is a $\mathbb{Z}/p\mathbb{Z}$-extension of number fields ℓ/k with $L = \ell_\infty$ and $K = k_\infty$ (see the above proof of Theorem 3.6), and $K \cap \ell/k$ is an extension of degree at most p, so either $K \cap \ell = k$ or $K \cap \ell = k_1$. If $K \cap \ell = k_1$, then $\ell = k_1$ and consequently $\mu_p(\ell) = p\mu_p(k) = 0$, so we may assume $K \cap \ell = k$. The proof of Theorem 11 in [Iwa59a] (or Proposition 13.23 in [Was96]) shows that for $k' \in \{k, \ell\}$ the sequence $\mathrm{rank}(A(k'_n)) := \dim_{\mathbb{F}_p}(A(k'_n) \otimes_{\mathbb{Z}} \mathbb{F}_p)$ is bounded if and only if $\mu_p(k') = 0$, so $\mathrm{rank}(A(k_n))$ is bounded and we need to prove $\mathrm{rank}(A(\ell_n))$ is bounded. For each $n \in \mathbb{N}_0$ let $v_1, \ldots, v_{s_n}$ denote the places on k_n which are ramified in ℓ_n/k_n with corresponding inertia groups $T_1, \ldots, T_{s_n}$ in $\mathrm{Gal}(M_n/k_n)$ where M_n is the maximal abelian extension of k_n contained in the p-Hilbert class field N_{ℓ_n} of ℓ_n. Then each T_i is a cyclic group of order p and

$$\mathrm{Gal}(M_n/N_{k_n}) = T_1 \cdots T_{s_n}.$$

Therefore

$$\begin{aligned}
\mathrm{rank}(A(\ell_n)) &= \mathrm{rank}(\mathrm{Gal}(N_{\ell_n}/\ell_n)) \\
&\leq p \cdot \mathrm{rank}\left(\frac{\mathrm{Gal}(N_{\ell_n}/\ell_n)}{\mathrm{Gal}(N_{\ell_n}/\ell_n)^{g-1}}\right) \\
&= p \cdot \mathrm{rank}\left(\frac{\mathrm{Gal}(N_{\ell_n}/\ell_n)}{\mathrm{Gal}(N_{\ell_n}/M_n)}\right) \\
&= p \cdot \mathrm{rank}(\mathrm{Gal}(M_n/\ell_n)) \\
&\leq p \cdot \mathrm{rank}(\mathrm{Gal}(M_n/k_n))
\end{aligned}$$

$$\leq p(\text{rank}(\text{Gal}(M_n/N_{k_n})) + \text{rank}(\text{Gal}(N_{k_n}/k_n)))$$
$$\leq p(s_n + \text{rank}(A(k_n))).$$

Thus it's enough to show s_n is bounded. Note that $\ell_n = k_n\ell$ since $K \cap \ell = k$. This implies that any prime ideal $\mathfrak{q}$ in k_n which ramifies in ℓ_n is a factor of a prime ideal $\mathfrak{p}$ in k which ramifies in ℓ, but there are only finitely many non-archimedean places in K lying above every such $\mathfrak{p}$ by Lemma 4.2, so s_n is bounded since for n sufficiently large ℓ_n/k_n is unramified at every infinite place.

Now let S be the set of finite places $v \nmid p$ of K which are ramified in L/K. Define

$$I_S := \bigoplus_{v \in S} I_{L,v}$$
$$I_{L,S} := I_L/I_S \cong \bigoplus_{v \notin S} I_{L,v}$$
$$P_{L,S} := \frac{P_L + I_S}{I_S}.$$

Then for $G := \text{Gal}(L/K) = \langle g \rangle$ we have the following canonical short exact sequences of G-modules

$$P_{L,S} \hookrightarrow I_{L,S} \twoheadrightarrow C_{L,S}$$
$$\mathcal{O}_{L,S}^{\times} \hookrightarrow L^{\times} \twoheadrightarrow P_{L,S}$$

where

$$C_{L,S} := \frac{I_{L,S}}{P_{L,S}} = \frac{I_L/I_S}{(P_L + I_S)/I_S} \cong \frac{I_L}{P_L + I_S} \cong \frac{C_L}{(P_L + I_S)/P_L}.$$

Thus we have long exact sequences

$$\cdots \to H^1(G, I_{L,S}) \to H^1(G, C_{L,S}) \to H^2(G, P_{L,S}) \to H^2(G, I_{L,S}) \to \cdots$$
$$\cdots \to H^1(G, L^{\times}) \to H^1(G, P_{L,S}) \to H^2(G, \mathcal{O}_{L,S}^{\times}) \to H^2(G, L^{\times}) \to \cdots$$

but Lemmas 4.8 and 4.9 imply

$$H^n(G, I_{L,S}) \cong \bigoplus_{v \notin S} H^n(G, I_{L,v}) \cong 0$$
$$H^n(G, L^{\times}) \cong 0$$

for all $n \in \mathbb{N}$, so since $G \cong \mathbb{Z}/p\mathbb{Z}$ we find

$$H^n(G, A_{L,S}) \cong H^n(G, C_{L,S}) \cong H^{n+1}(G, P_{L,S}) \cong H^{n+2}(G, \mathcal{O}_{L,S}^\times) \cong H^n(G, \mathcal{O}_{L,S}^\times)$$

for all $n \in \mathbb{N}$ where $A_{L,S}$ is the p-primary part of $C_{L,S}$. In fact, $A_{L,S} \cong A_L/A_S$ where A_S is the p-primary part of $C_S := (P_L + I_S)/P_L \cong I_S/(P_L \cap I_S)$. Observe that C_S injects into the ideal class group of a number field since S is a set of finitely many non-p-places, so $|A_S| < \infty$. For each $n \in \mathbb{N}_0$ multiplication by p^n is a surjective $\mathbb{Z}_p$-endomorphism on $\mathbb{Q}_p/\mathbb{Z}_p$ and every cyclic subgroup of $\mathbb{Q}_p/\mathbb{Z}_p$ is the kernel of such a map. Moreover, Theorem 4.4 shows that $A_L \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{\lambda_L}$ as $\mathbb{Z}_p$-modules since $\mu_L = 0$, and every cyclic subgroup of $(\mathbb{Q}_p/\mathbb{Z}_p)^{\lambda_L}$ is, after a $\mathbb{Z}_p$-automorphism, the image of a cyclic subgroup C under the natural injection $\iota_1 \colon \mathbb{Q}_p/\mathbb{Z}_p \rightarrowtail (\mathbb{Q}_p/\mathbb{Z}_p)^{\lambda_L}$ onto the first summand, so

$$\frac{(\mathbb{Q}_p/\mathbb{Z}_p)^{\lambda_L}}{\iota_1(C)} \cong \frac{\mathbb{Q}_p/\mathbb{Z}_p}{C} \oplus (\mathbb{Q}_p/\mathbb{Z}_p)^{\lambda_L - 1} \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{\lambda_L}$$

as $\mathbb{Z}_p$-modules. Therefore induction on the size of A_S proves that

$$A_{L,S} \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{\lambda_L}$$

as $\mathbb{Z}_p$-modules. Thus the map

$$A_{L,S} \to (A_{L,S}^*)^* \colon a \mapsto (f \mapsto f(a))$$

defines a $\mathbb{Z}_pG$-isomorphism, so Proposition 4.11 implies

$$H^n(G, A_{L,S}) \cong H_n(G, A_{L,S}^*)^*.$$

On the other hand, $A_{L,S}^* \cong \mathbb{Z}_p^{\lambda_L}$ as $\mathbb{Z}_p$-modules, so the Krull-Schmidt theorem holds for the $\mathbb{Z}_pG$-module $A_{L,S}^*$ by [Rei61], but (as found in [BG64] or seen by modifying the methods in Section 74 of [CR66]) the only finitely-generated indecomposable $\mathbb{Z}_pG$-modules up to isomorphism are $\mathbb{Z}_pG$, $I_pG = (g-1)\mathbb{Z}_pG$ (the augmentation ideal), and $\mathbb{Z}_p$ with trivial G-action, giving

$$A_{L,S}^* \cong \mathbb{Z}_pG^r \oplus I_pG^s \oplus \mathbb{Z}_p^t$$

as $\mathbb{Z}_pG$-modules for some uniquely determined $r, s, t \in \mathbb{N}_0$. Hence

$$\lambda_L = \text{rank}_{\mathbb{Z}_p}(A^*_{L,S}) = pr + (p-1)s + t = p(r+t) + (p-1)(s-t),$$

and

$$\begin{aligned} H^1(G, A_{L,S}) \cong & (H_1(G, \mathbb{Z}_pG)^*)^r \oplus (H_1(G, I_pG)^*)^s \oplus (H_1(G, \mathbb{Z}_p)^*)^t \\ & \cong (0^*)^r \oplus (0^*)^s \oplus ((\mathbb{Z}_p/p\mathbb{Z}_p)^*)^t \\ & \cong (\mathbb{Z}_p/p\mathbb{Z}_p)^t \end{aligned}$$

$$\begin{aligned} H^2(G, A_{L,S}) \cong & (H_2(G, \mathbb{Z}_pG)^*)^r \oplus (H_2(G, I_pG)^*)^s \oplus (H_2(G, \mathbb{Z}_p)^*)^t \\ & \cong (0^*)^r \oplus ((I_pG/I_pG^2)^*)^s \oplus (0^*)^t \\ & \cong (\mathbb{Z}_p/p\mathbb{Z}_p)^s \end{aligned}$$

as $\mathbb{Z}_pG$-modules. In particular, since the Herbrand quotient is multiplicative on short exact sequences of G-modules (see, for example, Proposition 10 in [AW67]) we get

$$p^{s-t} = \text{q}(A_{L,S}) = \text{q}(\mathcal{O}^\times_{L,S}) = \text{q}(\mathcal{O}^\times_{L,S}/\mathcal{O}^\times_L)\text{q}(\mathcal{O}^\times_L) = p^{d+H}$$

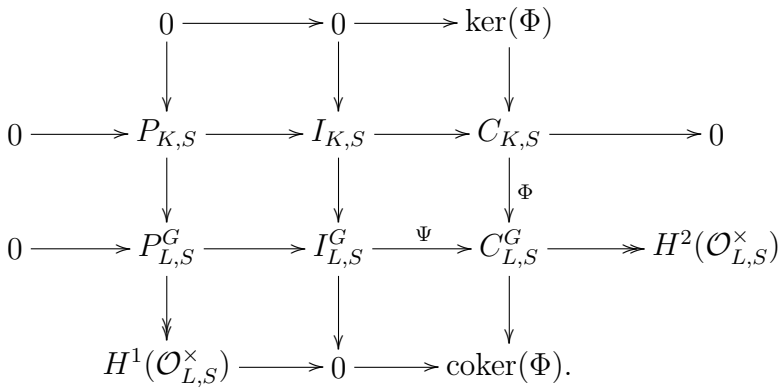
where

$$p^d = \text{q}(\mathcal{O}^\times_{L,S}/\mathcal{O}^\times_L) = \text{q}(P_S) = \text{q}(I_S)/\text{q}(C_S) = \text{q}(I_S) \overset{\text{by lem. } 4.8}{=} p^{|S|}$$

since C_S finite implies $\text{q}(C_S) = 1$ (again, see [AW67]).

Consider the natural map $\phi\colon A_{K,S} \to A^G_{L,S}$. We claim $\ker(\phi), \text{coker}(\phi)$ are finite. To prove this, we'll show that the natural map $\Phi\colon C_{K,S} \to C^G_{L,S}$ has finite kernel and cokernel. From the above long exact sequences in cohomology of G we get the

following commutative diagram with exact rows and columns



Thus $\ker(\Phi) \cong H^1(\mathcal{O}_{L,S}^\times)$ and $\operatorname{coker}(\Phi) = \operatorname{coker}(\Psi) \cong H^2(\mathcal{O}_{L,S}^\times)$ are finite. This proves the claim, so the induced map on $\mathbb{Z}_p$-modules

$$\mathbb{Z}_p^{r+t} \oplus (\mathbb{Z}_p/p\mathbb{Z}_p)^s \cong (A_{L,S}^*)_G \overset{\text{by 4.11}}{\cong} (A_{L,S}^G)^* \xrightarrow{\phi^*} A_{K,S}^* \cong \mathbb{Z}_p^{\lambda_K}$$

has kernel and cokernel which are torsion $\mathbb{Z}_p$-modules, giving $r + t = \lambda_K$. Therefore

$$\lambda_L + H = p\lambda_K + (p-1)(d+H) + H = p(\lambda_K + H) + (p-1)d,$$

as needed. □

Remark 4.13. We can use Theorem 4.12 and induction to express λ_L in terms of λ_K whenever L/K is a finite p-extension of $\mathbb{Z}_p$-fields which is unramified at the infinite places and with $\mu_K = 0$. Note that since finite p-groups are solvable, there is a tower

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n = L$$

of $\mathbb{Z}/(p)$-extensions K_i/K_{i-1}. Define $H_{L/K}$ by

$$p^{H_{L/K}} = \prod_{i=1}^{n} p^{p^{n-i}} \mathrm{q}_i(\mathcal{O}_{K_i}^\times).$$

where

$$\mathrm{q}_i(-) = \frac{|H^2(K_i/K_{i-1}, -)|}{|H^1(K_i/K_{i-1}, -)|}$$

is the Herbrand quotient for the cyclic group $\mathrm{Gal}(K_i/K_{i-1})$. Later, we'll see by Corollary 6.4 that $H_{L/K}$ is independent of the choice of tower when we prove a generalization of the following corollary.

Corollary 4.14. *Let L/K be a finite p-extension of $\mathbb{Z}_p$-fields which is unramified at every infinite place. Suppose $\mu_K = 0$. Then $\mu_L = 0$ and*

$$\lambda_L = [L:K]\lambda_K + (p-1)H_{L/K} + \sum_{w \nmid p}(e(w)-1)$$

where $e(w)$ is the ramification index in L/K of a finite place $w \nmid p$ of L, and $H_{L/K}$ is as in the previous remark.

Remark 4.15. As Iwasawa mentions in [Iwa81], we can use the methods of Theorem 4.12 above to give an alternate proof of Kida's formula, and we'll do so here. Specifically, let ℓ/k be a finite p-extension of CM-fields for some odd prime p, and suppose $\mu_p^-(k) = 0$. We've seen above that the general form of Kida's formula follows from Theorem 3.12, so we may assume $[L:K] = p$ where $K = k_\infty, L = \ell_\infty$. Then also $\mu_p^-(\ell) = 0$, and $A_{L,S} \cong A_{L,S}^- \oplus A_{L^+,S}$ as $\mathbb{Z}_pG$-modules with $A_{L,S}^- \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{\lambda_p^-(\ell)}$ as $\mathbb{Z}_p$-modules. (Note that this direct sum may fail to hold if $p = 2$.) By using similar arguments to those used in proving Iwasawa's formula, we find that

$$\lambda_p^-(\ell) + H^- = p(\lambda_p^-(k) + H^-) + \frac{1}{2}\sum_{\mathfrak{P} \in S(\ell)}(e(\mathfrak{P})-1)$$

with $p^{H^-} = \mathrm{q}(\mathcal{O}_L^\times/\mathcal{O}_{L^+}^\times) = \mathrm{q}(W_L/\{\pm 1\}) = \mathrm{q}(V_L)$ where V_L is the p-part of the set W_L of roots of unity in L. If $\zeta_p \notin k$, then $V_L = \{1\}$, so $\mathrm{q}(V_L) = 1$, giving $H^- = 0$. If $\zeta_p \in k$, then

$$V_L \cong \mathbb{Q}_p/\mathbb{Z}_p$$

as G-modules with trivial action, so

$$p^{H^-} = \frac{\left|\dfrac{\mathbb{Z}}{p\mathbb{Z}} \otimes_{\mathbb{Z}} \dfrac{\mathbb{Q}_p}{\mathbb{Z}_p}\right|}{\left|\mathrm{Hom}_{\mathbb{Z}}\left(\dfrac{\mathbb{Z}}{p\mathbb{Z}}, \dfrac{\mathbb{Q}_p}{\mathbb{Z}_p}\right)\right|} = \frac{1}{p},$$

giving $H^- = -1$.

We conclude with an example demonstrating how Theorem 4.12 can be used in situations where Kida's formula does not apply (i.e., for the prime $p = 2$ and non-CM fields).

Example 4.16. Take $p = 2$, $K = k_\infty$, and $L = \ell_\infty$ with $k = \mathbb{Q}(i)$ and $\ell = \mathbb{Q}(i, \sqrt{6})$. Of course, the number fields $k^+ = \mathbb{Q}$, $k = \mathbb{Q}(i)$, and $\ell^+ = \mathbb{Q}(\sqrt{6})$ each have class number 1, so all of their Iwasawa invariants vanish by Theorem 3.3 since 2 ramifies in k and ℓ^+. Also, both L/K and L^+/K^+ are $\mathbb{Z}/2\mathbb{Z}$-extensions of $\mathbb{Z}_2$-fields, so we may apply Theorem 4.12 to both cases since K is totally complex and L^+ is totally real. We get

$$\lambda_L = 2\lambda_K + H + d = H + d$$
$$0 = \lambda_{L^+} = 2\lambda_{K^+} + H^+ + d^+ = H^+ + d^+$$

where $2^H = \mathrm{q}(\mathcal{O}_L^\times), 2^{H^+} = \mathrm{q}(\mathcal{O}_{L^+}^\times)$ are Herbrand quotients and d (resp. d^+) is the number of non-2-places on K (resp. K^+) which are ramified in L/K (resp. L^+/K^+). On the other hand, we've seen that $H - H^+ = H^- = -1$ by the same argument used in Remark 4.15. (In fact, Kida's formula holds in the case $p = 2$ as shown by Sinnott in [Sin84], but we can't make the same conclusions about the p-primary part of the class group again since we may no longer have the decomposition $A_L \cong A_L^- \oplus A_{L^+}$.) Hence

$$\lambda_L = -1 - d^+ + d.$$

Clearly, $d^+ \geq 1$ since 3 ramifies in $\mathbb{Q}(\sqrt{6})/\mathbb{Q}$ while 3-places do not ramify in $\mathbb{Z}_2$-extensions of number fields, namely, $\mathbb{Q}_\infty/\mathbb{Q}$. In fact, $d^+ = 1$ since $8||3^2 - 1$ implies that there is exactly one prime $\mathbf{3}$ lying above 3 in $\mathbb{Q}_\infty$. In addition, we claim that $d = 2$. To see this, note that $\mathbf{3}$ must either split or ramify in $\mathbb{Q}_\infty(i)/\mathbb{Q}_\infty$, but it does

not ramify since 3 does not ramify in $\mathbb{Q}(i)/\mathbb{Q}$. Hence there are exactly 2 primes lying above 3 in $K = \mathbb{Q}_\infty(i)$, giving $d \leq 2$ as claimed. Therefore

$$\lambda_L = -1 - d^+ + d = -1 - 1 + 2 = 0,$$

but this result cannot be immediately deduced from Theorem 3.3 since $\ell = \mathbb{Q}(i, \sqrt{6})$ has class number 2. On the other hand, $\mathbb{Q}(i, \sqrt{6})$ has the same cyclotomic $\mathbb{Z}_2$-extension as $\mathbb{Q}(i, \sqrt{3})$ which *does* has class number 1, so we can also deduce $\lambda_L = 0$ from this plus Theorem 3.3.

Part II

FORMULAS FOR CYCLIC p-EXTENSIONS

Chapter 5
THE EULER CHARACTERISTIC

Suppose L/K is a cyclic p-extension of $\mathbb{Z}_p$-fields with $\mu_K = 0$. We can express λ_L in terms of λ_K by Corollary 4.14 assuming no infinite places ramify, but we'd like to know if we can get any additional information using cyclicity. Indeed, this will be the case, and a key gadget which we'll need is an **Euler characteristic** χ; take $\langle g \rangle = G = \mathrm{Gal}(L/K)$ and for any $\mathbb{Z}G$-module M with finite cohomology groups H^1, H^2 define

$$\chi(G, M) := \mathrm{ord}_p \left(\frac{|H^2(G, M)|}{|H^1(G, M)|} \right) = \mathrm{ord}_p \left(\frac{|\ker(\varphi_{M,g})/\mathrm{im}(\psi_{M,g})|}{|\ker(\psi_{M,g})/\mathrm{im}(\varphi_{M,g})|} \right)$$

where (as in the proof of Proposition 4.11)

$$\varphi_{M,g} \colon M \to M \colon m \mapsto (g-1)m$$
$$\psi_{M,g} \colon M \to M \colon m \mapsto (g^{|G|-1} + g^{|G|-2} + \cdots + 1)m.$$

Using the notation $\mathrm{q}(-)$ for the Herbrand quotient as in Chapter 4, we have the relation

$$p^{\chi(G,M)} = \mathrm{q}(M).$$

Thus χ is additive on short exact sequences of G-modules with finite H^2, H^1 since Herbrand quotients are multiplicative. In fact, we have the following computation of χ for the p-primary part of the class group.

Lemma 5.1. *Suppose L/K is a cyclic p-extension of $\mathbb{Z}_p$-fields with $G = \mathrm{Gal}(L/K)$. Then*

$$\chi(G, A_L) = -\chi(G, P_L) + \sum_{u \nmid p} \mathrm{ord}_p(e(w/u))$$

where $e(w/u)$ is the ramification index in L/K for a finite place w of L lying over $u \nmid p$. If, in addition, L/K is unramified at every infinite place, then

$$-\chi(G, P_L) = \chi(G, \mathcal{O}_L^\times).$$

Proof. As noted in Lemma 4.8,

$$p^m H^n(G, C_L) = 0$$

for all $n \in \mathbb{N}$ where $p^m = |G|$, but H^n distributes over direct sums (a fact which we've also used in Remark 4.7), so we can (1) split up C_L into a direct sum of its primary components (since it's a torsion abelian group), (2) pull out the direct sum, and (3) take the p-primary part of each summand. This will show that

$$H^n(G, A_L) \cong H^n(G, C_L)$$

for all $n \in \mathbb{N}$ since a q-primary component B_L of C_L with $q \neq p$ is uniquely divisible by p. Alternatively, $H^n(G, B_L)$ is a $\mathbb{Z}_q$-module since B_L is a $\mathbb{Z}_q$-module, but p is invertible in $\mathbb{Z}_q$, so $H^n(G, B_L) = 0$. We could also note, as Romyar Sharifi pointed out, that $H^i(G, C_L/A_L) = 0$ for $i \geq 1$ since C_L/A_L consists of prime-to-p torsion. Thus using additivity, Remark 4.7, and Lemma 4.8, we get

$$\begin{aligned}
\chi(G, A_L) = \chi(G, C_L) &= \chi(G, I_L/P_L) \\
&= -\chi(G, P_L) + \chi(G, I_L) \\
&= -\chi(G, P_L) + \sum_u \chi(G, I_{L,u}) \\
&= -\chi(G, P_L) + \sum_{u \nmid p} \mathrm{ord}_p(e(w/u)).
\end{aligned}$$

If, in addition, L/K is unramified at every infinite place, then Lemma 4.9 implies

$$\chi(G, L^\times) = 0,$$

so using additivity again gives

$$\begin{aligned} -\chi(G, P_L) &= -\chi(G, L^\times/\mathcal{O}_L^\times) \\ &= \chi(G, \mathcal{O}_L^\times) - \chi(G, L^\times) \\ &= \chi(G, \mathcal{O}_L^\times), \end{aligned}$$

as claimed. □

Remark 5.2. Assume further that $\mu_K = 0$ (as is conjectured) in addition to assuming that L/K is a cyclic p-extension of $\mathbb{Z}_p$-fields with $G = \mathrm{Gal}(L/K)$. Then also $\mu_L = 0$ (see the proof of Theorem 4.12), so if

$$(-)^* := \mathrm{Hom}_{\mathbb{Z}_p}(-, \mathbb{Q}_p/\mathbb{Z}_p)$$

denotes the p-Pontryagin dual functor as in Chapter 4, then Theorem 4.4 and Proposition 4.11 together imply that

$$A_L^* \cong_{\mathbb{Z}_p} ((\mathbb{Q}_p/\mathbb{Z}_p)^{\lambda_L})^* \cong_{\mathbb{Z}_p} ((\mathbb{Q}_p/\mathbb{Z}_p)^*)^{\lambda_L} \cong_{\mathbb{Z}_p} \mathbb{Z}_p^{\lambda_L}$$

is a $\mathbb{Z}_pG$-module which is free of finite rank λ_L over $\mathbb{Z}_p$. Thus

$$A_L^* \cong \bigoplus_n M_n^{a_n}$$

is a direct sum of finitely many pairwise non-isomorphic indecomposable $\mathbb{Z}_pG$-modules M_n each with finite rank over $\mathbb{Z}_p$. By the work of Reiner in [Rei61], we know that the Krull-Schmidt theorem holds for $\mathbb{Z}_pG$-modules, so this decomposition is unique up to ordering and choices M_n of representatives of isomorphism classes. Note that Proposition 4.11 and the fact that finite abelian p-groups A are self dual (i.e., $A \cong A^*$) together imply

$$\begin{aligned} \chi(G, M^*) &= \mathrm{ord}_p\left(\frac{|H^2(G, M^*)|}{|H^1(G, M^*)|}\right) = \mathrm{ord}_p\left(\frac{|H^1(G, M)^*|}{|H^2(G, M)^*|}\right) \\ &= \mathrm{ord}_p\left(\frac{|H^1(G, M)|}{|H^2(G, M)|}\right) = -\mathrm{ord}_p\left(\frac{|H^2(G, M)|}{|H^1(G, M)|}\right) \\ &= -\chi(G, M) \end{aligned}$$

when these quantities are finite, and additivity along with the first isomorphism theorem imply

$$\begin{aligned}\chi(G, M_G) &= \chi(G, M/(g-1)M) = \chi(G, M) - \chi(G, (g-1)M) \\ &= \chi(G, M) - \chi(G, M/M^G) = \chi(G, M) - (\chi(G, M) - \chi(G, M^G)) \\ &= \chi(G, M^G).\end{aligned}$$

Hence for any subgroups $N \leq H \leq G$ we find

$$\begin{aligned}\chi(H/N, A_{L^N}) &= -\chi(H/N, (A_L^N)^*) \overset{\text{by prop } 4.11}{=} -\chi(H/N, (A_L^*)_N) \\ &= -\chi(H/N, (A_L^*)^N) = -\sum_n a_n \chi(H/N, M_n^N). \qquad (5.2.1)\end{aligned}$$

We can then compare these computations to

$$\lambda_L = \text{rank}_{\mathbb{Z}_p}(A_L^*) = \sum_n a_n \text{rank}_{\mathbb{Z}_p}(M_n) \qquad (5.2.2)$$

and

$$\begin{aligned}\lambda_K &= \text{rank}_{\mathbb{Z}_p}(A_K^*) \overset{\text{proof of } 4.12}{=} \text{rank}_{\mathbb{Z}_p}((A_L^G)^*) \\ &= \text{rank}_{\mathbb{Z}_p}((A_L^*)_G) = \text{rank}_{\mathbb{Z}_p}((A_L^*)^G) \\ &= \sum_n a_n \text{rank}_{\mathbb{Z}_p}(M_n^G). \qquad (5.2.3)\end{aligned}$$

Used in conjunction with Lemma 5.1, the above Equations 5.2.1, 5.2.2, and 5.2.3, should allow one to express λ_L in terms of (1) λ_K, (2) Euler characteristics of principal ideals or units, and (3) ramification indices of finite places not lying above p, just so long as we can classify the M_n sufficiently well. Now when $|G| \leq p^2$, the work of Heller and Reiner in [HR62] shows that there are finitely many isomorphism classes of indecomposable $\mathbb{Z}_pG$-modules with finite $\mathbb{Z}_p$-rank; moreover, we can classify these indecomposables M_n well enough to determine all possible $\chi(H/N, M_n^N)$ and $\text{rank}_{\mathbb{Z}_p}(M_n^N)$. We'll see later, however, that we can play a similar game for $|G| > p^2$ even though there are infinitely many isomorphism classes of indecomposables in this case.

Chapter 6
DEGREE p

In this chapter, we focus on the case that L/K is a cyclic p-extension of $\mathbb{Z}_p$-fields with $\langle g \rangle = G = \mathrm{Gal}(L/K) \cong \mathbb{Z}/(p)$ and $\mu_K = 0$. First, we'll prove a mild generalization of Iwasawa's formula (see Theorem 4.12) using the Euler characteristic χ. Specifically, we won't need the assumption that infinite places are unramified and we won't "remove" the finite places not lying above p which ramify. We will, however, take for granted the fact that $\mu_K = 0$ implies $\mu_L = 0$ since we already proved this when we went through Iwasawa's proof. In the last section, $p = 2$ will be treated in the case of an imaginary quadratic extension of $\mathbb{Q}_\infty$. In the process, we'll give a slick proof of Ferrero's and Kida's well-known lambda computations. Then we'll extend these computations to a larger class of fields.

As mentioned in the proof of Theorem 4.12, we have the following description of the indecomposable $\mathbb{Z}_pG$-modules which are free of finite rank over $\mathbb{Z}_p$ (attributed to Diederichsen, or see [CR66]).

Theorem 6.1. *Let $\langle g \rangle = G \cong \mathbb{Z}/(p)$. The only indecomposable $\mathbb{Z}_pG$-modules which are free of finite rank over $\mathbb{Z}_p$ are (up to isomorphism) $\mathbb{Z}_p$, $\mathbb{Z}_pG$, and $I_pG = (g-1)\mathbb{Z}_pG$.*

6.1 Iwasawa's Formula Revisited

In 1980, Iwasawa (see [Iwa81]) used Theorem 6.1 to prove the following generalization of Kida's formula (see [Kid80]) in the case where L/K is unramified at infinite places. We give an alternative proof (of a slight generalization) here which still retains the basic flavor.

Theorem 6.2. *Let L/K be a $\mathbb{Z}/(p)$-extension of $\mathbb{Z}_p$-fields for some prime p with $G = \mathrm{Gal}(L/K)$. Suppose $\mu_K = 0$. Then $\mu_L = 0$ and*

$$\lambda_L = p\lambda_K - (p-1)\chi(G, P_L) + \sum_{w \nmid p}(e(w) - 1)$$

where $e(w)$ is the ramification index in L/K of a finite place $w \nmid p$. In fact,

$$A_L^* \cong \mathbb{Z}_p^a \oplus (\mathbb{Z}_p G)^{\lambda_K - a} \oplus (I_p G)^{|S| - \chi(G,P_L) + a}$$

as $\mathbb{Z}_p G$-modules.

Proof. Use Theorem 6.1 for $\langle g \rangle = G$ to write

$$A_L^* \cong \mathbb{Z}_p^a \oplus (\mathbb{Z}_p G)^b \oplus (I_p G)^c$$

as $\mathbb{Z}_p G$-modules for some nonnegative integers a, b, c. We have already computed the $\mathbb{Z}_p$-ranks, G-invariants, and Euler characteristics, of these indecomposables in the proof of Theorem 4.12. The results are summarized in Table 6.2.1. Thus if S is the

	$\mathrm{rank}_{\mathbb{Z}_p}(-)$	$(-)^G$	$H^2(G,-)$	$H^1(G,-)$	$\chi(G,-)$
$\mathbb{Z}_p$	1	$\mathbb{Z}_p$	$\mathbb{Z}_p/p\mathbb{Z}_p$	0	1
$\mathbb{Z}_p G$	p	$\mathbb{Z}_p$	0	0	0
$I_p G$	$p-1$	0	0	$\mathbb{Z}_p/p\mathbb{Z}_p$	-1

TABLE 6.2.1. Cohomology for extensions of degree p

set of finite places of K not lying above p which ramify in L/K, then Lemma 5.1 and the last column in Table 6.2.1 imply

$$-\chi(G, P_L) + |S| = \chi(G, A_L) = -\chi(G, A_L^*) = -a \cdot 1 - b \cdot 0 - c \cdot (-1) = -a + c.$$

On the other hand, equations 5.2.2, 5.2.3 in Remark 5.2 and the first two columns in Table 6.2.1 show that

$$\lambda_K = a \cdot 1 + b \cdot 1 + c \cdot 0 = a + b,$$

and

$$\begin{aligned}\lambda_L &= a \cdot 1 + b \cdot p + c(p-1) = p(a+b) + (p-1)(-a+c) \\ &= p\lambda_K - (p-1)\chi(G, P_L) + (p-1)|S|,\end{aligned}$$

as needed. □

Remark 6.3. We can use Theorem 6.2 and induction to express λ_L in terms of λ_K whenever L/K is a finite p-extension of $\mathbb{Z}_p$-fields with $\mu_K = 0$. Note that since finite p-groups are solvable, there is a tower

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n = L$$

of $\mathbb{Z}/(p)$-extensions. Define $H_{L/K}$ by

$$H_{L/K} = -\sum_{i=1}^{n} p^{n-i}\chi(\mathrm{Gal}(K_i/K_{i-1}), P_{K_i}).$$

We'll see in the corollary below that $H_{L/K}$ is independent of the choice of tower.

Corollary 6.4. *Let L/K be a p-extension of $\mathbb{Z}_p$-fields. Suppose $\mu_K = 0$. Then $\mu_L = 0$ and*

$$\lambda_L = [L:K]\lambda_K + (p-1)H_{L/K} + \sum_{w \nmid p}(e(w) - 1)$$

where $e(w)$ is the ramification index in L/K of a finite place $w \nmid p$ and $H_{L/K}$ is as in Remark 6.3.

Proof. We use induction on n where $p^n = [L:K]$. If $n = 1$, this is just Theorem 6.2. Suppose the formula holds for $n-1$ and let's use the notation in Remark 6.3, so

$$\lambda_{K_{n-1}} = [K_{n-1}:K]\lambda_K + (p-1)H_{K_{n-1}/K} + \sum_{v_{n-1} \nmid p}(e(v_{n-1}) - 1)$$

where $e(v_{n-1})$ is the ramification index in K_{n-1}/K of a finite place $v_{n-1} \nmid p$, and

$$H_{K_{n-1}/K} = -\sum_{i=1}^{n-1} p^{n-1-i}\chi(\mathrm{Gal}(K_i/K_{i-1}), P_{K_i}).$$

Of course, the formula also holds for the $\mathbb{Z}/(p)$-extension L/K_{n-1}, so

$$\lambda_L = [L : K_{n-1}]\lambda_{K_{n-1}} + (p-1)H_{L/K_{n-1}} + \sum_{w\nmid p}(e(w/w_{n-1}) - 1)$$

$e(w/w_{n-1})$ is the ramification index in L/K_{n-1} of a finite place w lying over w_{n-1}, and

$$H_{L/K_{n-1}} = -\chi(\mathrm{Gal}(L/K_{n-1}), P_L).$$

Thus we find

$$\lambda_L = p\lambda_{K_{n-1}} + (p-1)H_{L/K_{n-1}} + \sum_{w\nmid p}(e(w/w_{n-1}) - 1) =$$
$$p^n\lambda_K + (p-1)(pH_{K_{n-1}/K} + H_{L/K_{n-1}}) + p\sum_{v_{n-1}\nmid p}(e(v_{n-1}) - 1) + \sum_{w\nmid p}(e(w/w_{n-1}) - 1).$$

Hence the corollary follows from the following two computations:

$$\begin{aligned} pH_{K_{n-1}/K} + H_{L/K_{n-1}} &= -p\sum_{i=1}^{n-1} p^{n-1-i}\chi(\mathrm{Gal}(K_i/K_{i-1}), P_{K_i}) - \chi(\mathrm{Gal}(L/K_{n-1}), P_L) \\ &= -\sum_{i=1}^{n} p^{n-i}\chi(\mathrm{Gal}(K_i/K_{i-1}), P_{K_i}) \\ &= H_{L/K}, \end{aligned}$$

and

$$\begin{aligned} \sum_{w\nmid p}(e(w) - 1) &= \sum_{v_{n-1}\nmid p}\sum_{w|v_{n-1}}(e(w) - 1) \\ &= \sum_{v_{n-1}\nmid p}\sum_{w|v_{n-1}}(e(w/v_{n-1})e(v_{n-1}) - 1) \\ &= \sum_{v_{n-1}\nmid p}\sum_{w|v_{n-1}}(e(w/v_{n-1})(e(v_{n-1}) - 1) + e(w/v_{n-1}) - 1) \end{aligned}$$

$$= \sum_{v_{n-1}\nmid p} \sum_{w|v_{n-1}} e(w/v_{n-1})(e(v_{n-1})-1) + \sum_{w\nmid p}(e(w/w_{n-1})-1)$$
$$= \sum_{v_{n-1}\nmid p} p(e(v_{n-1})-1) + \sum_{w\nmid p}(e(w/w_{n-1})-1)$$

where the last equality follows from the fact that finite places not lying above p either split or ramify in a cyclic degree p extension of $\mathbb{Z}_p$-fields (see the proof of Theorem 3.6). □

Remark 6.5. Let L/K be as in Corollary 6.4 with $\mu_K = 0$. Again using the notation of Remark 6.3, Lemma 5.1 can be used to show

$$\sum_{i=1}^{n} \varphi(p^{n+1-i})\chi(\mathrm{Gal}(K_i/K_{i-1}), A_{K_i})$$
$$= -(p-1)\sum_{i=1}^{n} p^{n-i}\chi(\mathrm{Gal}(K_i/K_{i-1}), P_{K_i}) + \sum_{i=1}^{n}\varphi(p^{n+1-i})\sum_{v_{i-1}\nmid p}\mathrm{ord}_p(e(v_i/v_{i-1}))$$
$$= (p-1)H_{L/K} + \sum_{w\nmid p}(e(w)-1),$$

so we can restate the formula of Corollary 6.4 in the following form, which we'll find useful in Chapter 8:

$$\lambda_L = [L:K]\lambda_K + \sum_{i=1}^{n}\varphi(p^{n+1-i})\chi(\mathrm{Gal}(K_i/K_{i-1}), A_{K_i}).$$

Now we take note of a few immediate implications of Theorem 6.2.

Corollary 6.6. *Let L/K be a $\mathbb{Z}/(p)$-extension of $\mathbb{Z}_p$-fields for some prime p with $G = \mathrm{Gal}(L/K)$. Suppose $\mu_K = 0$. Then*

1. $\lambda_L \equiv \lambda_K \pmod{p-1}$
2. $\lambda_L \equiv \chi(G, P_L) - |S| = -\chi(G, A_L) \pmod{p}$
3. $\mathrm{ord}_p|H^2(G, P_L)| \leq \lambda_K + \mathrm{ord}_p|H^1(G, P_L)| + |S|$

where S is the set of finite places of K not lying above p which ramify in L/K.

Proof. Theorem 6.2 immediately implies 1 and 2. To prove 3 we need only note that

$$0 \leq \frac{\lambda_L - \lambda_K}{p-1} = \lambda_K - \mathrm{ord}_p|H^2(G, P_L)| + \mathrm{ord}_p|H^1(G, P_L)| + |S|$$

which completes the proof. □

As shown in the discussion preceding Proposition 3.1 of [FKOT97], we can improve upon the inequality in part 3 of Corollary 6.6 in the case where $\lambda_K = 0$.

Lemma 6.7. *Let L/K be a $\mathbb{Z}/(p)$-extension of $\mathbb{Z}_p$-fields which is unramified at every infinite place. Suppose $\mu_K = \lambda_K = 0$. Then*

$$\mathrm{ord}_p|H^2(G, P_L)| = \mathrm{ord}_p|H^1(G, \mathcal{O}_L^\times)| \leq |S|$$

where $G = \mathrm{Gal}(L/K)$.

This result combined with Theorem 6.2 immediately implies the following corollary, which is Proposition 3.1 in [FKOT97].

Corollary 6.8. *Let L/K be a $\mathbb{Z}/(p)$-extension of $\mathbb{Z}_p$-fields which is unramified at every infinite place. Suppose $\mu_K = \lambda_K = 0$. Then $\lambda_L = 0$ if and only if*

$$|S| - \mathrm{ord}_p|H^1(G, \mathcal{O}_L^\times)| = 0 = \mathrm{ord}_p|H^2(G, \mathcal{O}_L^\times)|$$

where $G = \mathrm{Gal}(L/K)$.

The following lemma of Iwasawa is mentioned in [Iwa89] and gives Theorem 3.5 (the main result) of [FKOT97], which we have stated below as Theorem 6.10 in a slightly more general form. We'll prove a generalization of this lemma and theorem in Chapter 8.

Lemma 6.9 (Iwasawa)**.** *Let L/K be a $\mathbb{Z}/(p)$-extension of $\mathbb{Z}_p$-fields which is unramified at every infinite place. Suppose $K = k_\infty$ is the cyclotomic $\mathbb{Z}_p$-extension of a number field k such that $p \nmid h(k)$ and k has only one prime lying above p. Then*

$$\mathrm{ord}_p|H^2(G, \mathcal{O}_L^\times)| = 0.$$

where $G = \mathrm{Gal}(L/K)$.

Theorem 6.10 (T. Fukuda et al., 1997)**.** *Let L/K be a $\mathbb{Z}/(p)$-extension of $\mathbb{Z}_p$-fields which is unramified at every infinite place. Suppose $K = k_\infty$ is the cyclotomic $\mathbb{Z}_p$-extension of a number field k such that $p \nmid h(k)$ and k has only one prime lying above p. Then $\lambda_L = 0$ if and only if the ideal class of every finite place of L not lying above p which is ramified in L/K has order prime to p in the class group C_L.*

Example 6.11. In [FKOT97], the authors use Theorem 6.10 to examine the $p = 3$ case when $L/K = \ell_\infty/\mathbb{Q}_\infty$ where $\ell/\mathbb{Q}$ is a cyclic cubic extension of prime conductor $\mathfrak{f} \equiv 1 \pmod 3$. Since one can verify that $3 \nmid h(\ell)$, if 3 does not split in $\ell/\mathbb{Q}$, then $\lambda_L = 0$ by Theorem 3.3. If 3 does split in $\ell/\mathbb{Q}$ and $\mathfrak{f} \not\equiv 1 \pmod 9$, then $|S| = 1$ and $\lambda_L = 0$ by the theorem since again $3 \nmid h_\ell$. Let's give a small explicit example. Let α be a root of

$$x^3 + x^2 - 20x - 9,$$

and take $\ell = \mathbb{Q}(\alpha)$. Then $\ell \subseteq \mathbb{Q}(\zeta_{61})_+$, so 3 splits and only 61 ramifies in $\ell/\mathbb{Q}$. Also, 61 remains prime in $\mathbb{Q}_\infty/\mathbb{Q}$, so $|S| = 1$ and the class of the unique prime above 61 in L has order prime to 3 in C_L since we can check that $h(\ell) = 1$.

6.2 $\mathbb{Q}_p$-Representations

The proof of Theorem 6.2 actually shows more than just a formula for lambda invariants. It shows a statement about representations (a mild generalization of Theorem 6 in [Iwa81]). Let L/K and $G = \mathrm{Gal}(L/K)$ be as in Theorem 6.2 with $\mu_K = 0$. Define

$$V_L := A_L^* \otimes_{\mathbb{Z}_p} \mathbb{Q}_p,$$

and consider the corresponding representation

$$\pi_{L/K} \colon G \to \mathrm{GL}(V_L).$$

Then there is the following result about the decomposition of $\pi_{L/K}$.

Corollary 6.12. *Let L/K and $G = \mathrm{Gal}(L/K)$ be as in Theorem 6.2 with $\mu_K = 0$. Then we have an isomorphism of $\mathbb{Q}_p$-representations*

$$\pi_{L/K} \cong \lambda_K \pi_G \oplus (|S| - \chi(G, P_L))\pi_{p-1}.$$

where $|S|$ is number of finite places of L not lying above p which ramify in L/K, π_G is the regular representation of G over $\mathbb{Q}_p$, and π_{p-1} is the unique faithful irreducible representation of G over $\mathbb{Q}_p$.

Proof. In the notation of the theorem with $\langle g \rangle = G$ we have

$$V_L \cong (\mathbb{Z}_p^a \oplus (\mathbb{Z}_p G)^b \oplus (I_p G)^c) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong \mathbb{Q}_p^a \oplus (\mathbb{Q}_p G)^b \oplus ((g-1)\mathbb{Q}_p G)^c$$

as $\mathbb{Q}_p G$-modules. Now

$$\mathbb{Q}_p G \cong \frac{\mathbb{Q}_p[x]}{(x^p - 1)} \cong \frac{\mathbb{Q}_p[x]}{(x-1)} \oplus \frac{\mathbb{Q}_p[x]}{(\Phi_p(x))} \cong \mathbb{Q}_p \oplus (g-1)\mathbb{Q}_p G,$$

as $\mathbb{Q}_p G$-modules, so in fact

$$\begin{aligned} V_L &\cong \mathbb{Q}_p^a \oplus \mathbb{Q}_p^b \oplus ((g-1)\mathbb{Q}_p G)^b \oplus ((g-1)\mathbb{Q}_p G)^c \\ &\cong \mathbb{Q}_p^{a+b} \oplus ((g-1)\mathbb{Q}_p G)^{a+b} \oplus ((g-1)\mathbb{Q}_p G)^{-a+c} \\ &\cong (\mathbb{Q}_p G)^{a+b} \oplus ((g-1)\mathbb{Q}_p G)^{-a+c} \\ &\cong (\mathbb{Q}_p G)^{\lambda_K} \oplus ((g-1)\mathbb{Q}_p G)^{|S| - \chi(G, P_L)}. \end{aligned}$$

Note that if $|S| - \chi(G, P_L)$ happens to be negative we interpret the above isomorphism as a difference of representations. Hence it suffices to show that $(g-1)\mathbb{Q}_p G$ corresponds to the unique faithful irreducible representation of G over $\mathbb{Q}_p$. Suppose $\pi_{p-1} \colon G \to \mathrm{GL}(V)$ is a faithful irreducible representation of G over $\mathbb{Q}_p$. It's enough to prove $V \cong (g-1)\mathbb{Q}_p G$ as $\mathbb{Q}_p G$-modules. Since V is a simple $\mathbb{Q}_p G$-module we know that $V \cong \mathbb{Q}_p G / M$ for some maximal ideal M of $\mathbb{Q}_p G$. Now

$$\mathbb{Q}_p G \cong \mathbb{Q}_p[x]/(x^p - 1),$$

so M corresponds to either $(x-1)/(x^p-1)$ or $(\Phi_p(x))/(x^p-1)$ under this isomorphism, but $(x-1)/(x^p-1)$ corresponds to the trivial representation (not faithful), whence

$$V \cong \frac{\mathbb{Q}_p[x]/(x^p-1)}{(\Phi_p(x))/(x^p-1)} \cong \frac{\mathbb{Q}_p[x]}{(\Phi_p(x))} \cong \frac{\mathbb{Q}_p[x]}{((x^p-1)/(x-1))} \cong \frac{(x-1)}{(x^p-1)} \cong (g-1)\mathbb{Q}_p G,$$

which finishes the proof. □

6.3 $p = 2$

In this section, we'll investigate the change in lambda invariants for quadratic extensions of $\mathbb{Z}_2$-fields. We reprove an independently known result of Ferrero ([Fer80]) and Kida ([Kid79]) from a different viewpoint that lends itself to natural generalizations that can be used in constructing prescribed lambda invariants for quadratic extensions of bases other than $\mathbb{Q}_\infty$. We have a formula which describes the change in lambda invariants. Namely, we have Iwasawa's formula, but in general we have to replace $\chi(G, \mathcal{O}_L^\times)$ with $-\chi(G, P_L)$ since $H^2(G, L^\times)$ is nonzero whenever there are infinite places which ramify (see Theorem 6.2). We'll need the following two results of Greenberg and Weber.

Theorem 6.13 (Greenberg)**.** *Suppose F'/F is a quadratic extension of number fields and let $t_\infty = \#$ infinite places of F which ramify in F'. Then*

$$\chi(F'/F, \mathcal{O}_{F'}^\times) = t_\infty - 1.$$

Proof. See Remark 1.2.6 in [Gre10]. □

Theorem 6.14 (Weber)**.** *Let k_n denote the nth layer of the cyclotomic $\mathbb{Z}_2$-extension of $k = \mathbb{Q}$. Then every totally positive element of $\mathcal{O}_{k_n}^\times$ is a square in $\mathcal{O}_{k_n}^\times$.*

Proof. See Sätze 6 and 25 in [Has52]. □

We'll also need the following lemma, which will be used again along with Theorem 6.13 and a generalization of Theorem 6.14 later.

Lemma 6.15. *Let $d > 1$ be a squarefree integer. Suppose F is a number field with discriminant Δ_F such that $(d, \Delta_F)|2$. Then $4\mathcal{O}_{F(\sqrt{-d})} \subseteq \mathcal{O}_F + \sqrt{-d}\mathcal{O}_F$.*

Proof. Without loss of generality, we have $\sqrt{-d} \notin F$. Pick an arbitrary element ε in $\mathcal{O}_{F(\sqrt{-d})}$. Then ε is of the form

$$\varepsilon = x + y\sqrt{-d}$$

where $x, y \in F$, and the norm and trace of ε over F are in $\mathcal{O}_F$. In other words,

$$2x \in \mathcal{O}_F \text{ and } x^2 + dy^2 \in \mathcal{O}_F.$$

Hence it suffices to show that $4y \in \mathcal{O}_F$. We immediately see that

$$d(2y)^2 \in \mathcal{O}_F.$$

Let $\mathfrak{P}$ be a prime ideal of $\mathcal{O}_F$. Suppose $v_{\mathfrak{P}}(4y) < 0$. We will obtain a contradiction. Take $e := v_{\mathfrak{P}}(2) \geq 0$, $-m := v_{\mathfrak{P}}(y) = v_{\mathfrak{P}}(4y) - 2e < 0$, and $n := v_{\mathfrak{P}}(d) \geq 0$. Then

$$2e - m = v_{\mathfrak{P}}(4y) < 0$$

and

$$n + 2(e - m) = v_{\mathfrak{P}}(d(2y)^2) \geq 0.$$

If $e = 0$ (i.e., $\mathfrak{P}$ does not lie above 2), then $n \geq 2m \geq 2$, so $\mathfrak{P} \cap \mathbb{Z} = (q) \neq (2)$ ramifies in $F/\mathbb{Q}$ because $\mathfrak{P}^2 | d\mathcal{O}_F$ and d is squarefree, but this is a contradiction since $(d, \Delta_F)|2$. Thus $e > 0$ and either $n = 0$ (i.e., $2 \nmid d$) or $n = e$ (i.e., $2|d$). It cannot be the case that $n = 0$ since then $2(e - m) \geq 0$ implies

$$2e - m \geq e - m \geq 0,$$

which contradicts $2e - m < 0$. Hence $n = e$, so

$$2(2e - m) \geq 3e - 2m = n + 2(e - m) \geq 0,$$

but again this contradicts $2e - m < 0$. □

Proposition 6.16. *Let $K = k_\infty$ be the cyclotomic $\mathbb{Z}_2$-extension of $k = \mathbb{Q}$ and $L = \ell_\infty$ be the cyclotomic $\mathbb{Z}_2$-extension of an imaginary quadratic number field $\ell = \mathbb{Q}(\sqrt{-d})$ with $d \in \mathbb{Z}$ squarefree and $d > 2$. Then*

$$\chi(G, P_L) = 1$$

where again $G = \mathrm{Gal}(L/K)$.

Proof. We'll show that $|H^1(G, P_L)| = 1$ and $|H^2(G, P_L)| = 2$. For each $n \in \mathbb{N} \cup \{\infty\}$ there is an exact sequence

$$0 \to H^1(G_n, P_{\ell_n}) \to H^2(G_n, \mathcal{O}_{\ell_n}^\times) \to H^2(G_n, \ell_n^\times) \to H^2(G_n, P_{\ell_n}) \to H^1(G_n, \mathcal{O}_{\ell_n}^\times) \to 0$$

where $G_n = \mathrm{Gal}(\ell_n/k_n)$. Let $N_n \colon \ell_n \to k_n$ denote the norm map for all $n \in \mathbb{N} \cup \{\infty\}$. Then Theorem 6.14 implies that for all $n \in \mathbb{N}$ we have

$$\mathcal{O}_{k_n}^\times \cap N_\infty(L^\times) = (\mathcal{O}_{k_n}^\times)^2 = N_n(\mathcal{O}_{\ell_n}^\times)$$

where $(\mathcal{O}_{k_n}^\times)^2$ denotes the set of squares of units. Hence

$$\mathcal{O}_K^\times \cap N_\infty(L^\times) = (\mathcal{O}_K^\times)^2 = N_\infty(\mathcal{O}_L^\times),$$

so we have a commutative diagram

$$\begin{array}{ccc} H^2(G, \mathcal{O}_L^\times) & \longrightarrow & H^2(G, L^\times) \\ \downarrow \wr & & \downarrow \wr \\ \mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2 & \longrightarrow & K^\times/N_\infty(L^\times) \end{array}$$

where the horizontal maps are the natural maps and the vertical maps are isomorphisms. Thus

$$H^1(G, P_L) \cong \ker(\mathcal{O}_K^\times/(\mathcal{O}_K^\times)^2 \to K^\times/N_\infty(L^\times)) = (\mathcal{O}_K^\times \cap N_\infty(L^\times))/(\mathcal{O}_K^\times)^2 = 0,$$

and likewise $H^1(G_n, P_{\ell_n}) = 0$ for all $n \in \mathbb{N}$. For all $n \in \mathbb{N}$ let $t_\infty(n) = \#$ infinite places of k_n which ramify in ℓ_n/k_n. Then using Theorem 6.14 and Dirichlet's unit

theorem shows

$$|H^2(G_n, \mathcal{O}_{\ell_n}^\times)| = \left| \frac{\mathcal{O}_{k_n}^\times}{(\mathcal{O}_{k_n}^\times)^2} \right| = 2^{t_\infty(n)+0-1+1} = 2^{t_\infty(n)}.$$

Also,

$$|H^2(G, \ell_n^\times)| = 2^{t_\infty(n)},$$

so the natural map

$$H^2(G_n, \mathcal{O}_{\ell_n}^\times) \xrightarrow{\sim} H^2(G_n, \ell_n^\times)$$

is an isomorphism by the pigeonhole principle (an injection of finite sets of the same size is a bijection) and, in particular, the natural map

$$\mathcal{O}_{k_n}^\times/(\mathcal{O}_{k_n}^\times)^2 \xrightarrow{\sim} k_n^\times/N_n(\ell_n^\times)$$

is onto, i.e.,

$$k_n^\times = \mathcal{O}_{k_n}^\times N_n(\ell_n^\times).$$

This implies that

$$K^\times = \mathcal{O}_K^\times N_\infty(L^\times),$$

so we also have that the natural map

$$H^2(G, \mathcal{O}_L^\times) \xrightarrow{\sim} H^2(G, L^\times)$$

is an isomorphism, so for all $n \in \mathbb{N} \cup \{\infty\}$ we have

$$H^2(G_n, P_{\ell_n}) \cong H^1(G_n, \mathcal{O}_{\ell_n}^\times)$$

by the long exact sequence in cohomology. Now for $n \in \mathbb{N}$ we have

$$|U_n/V_n| = |H^1(G_n, \mathcal{O}_{\ell_n}^\times)| = \frac{|H^2(G_n, \mathcal{O}_{\ell_n}^\times)|}{2^{\chi(G_n, \mathcal{O}_{\ell_n}^\times)}} = \frac{2^{t_\infty(n)}}{2^{t_\infty(n)-1}} = 2$$

by Theorem 6.13 where U_n is the norm 1 units in $\mathcal{O}_{\ell_n}$ and $V_n = \{\bar{u}/u : u \in \mathcal{O}_{\ell_n}^\times\}$. We claim U_n/V_n is generated by the coset of -1. To prove this, it's enough to show that $-1 \notin V_n$. If not, then $-1 = \bar{u}/u$ for some $u \in \mathcal{O}_{\ell_n}^\times$, so lemma 6.15 implies

$$u = i\frac{a\sqrt{d}}{4}$$

where $a \in \mathcal{O}_{k_n}$. Of course, $u \in \mathcal{O}_{\ell_n}^\times$ is a unit, so $u^{-1} \in \mathcal{O}_{\ell_n}$ is an integer, giving

$$u^{-1} = -i\frac{4}{a\sqrt{d}} = i\frac{b\sqrt{d}}{4}$$

for some $b \in \mathcal{O}_{k_n}$. Hence $abd = -4^2$, so d divides $4^2 = 2^4$ in $\mathcal{O}_{k_n}$, but that means d divides 2^4 in $\mathbb{Z}$. Therefore $d = 1$ or $d = 2$ since d is a squarefree positive integer, which contradicts our assumption that $d > 2$, so indeed U_n/V_n (has order 2 and) is generated by the coset of -1. It follows that U_∞/V_∞ has order 2 and is generated by the coset of -1 since by the claim

$$U_\infty = \bigcup_{n=0}^{\infty} U_n = \bigcup_{n=0}^{\infty} \langle -1 \rangle V_n = \langle -1 \rangle V_\infty$$

while $-1 \notin V_n$ for every n implies

$$-1 \notin V_\infty,$$

which finishes the proof. □

Corollary 6.17. *Let L/K be as in Proposition 6.16. Then*

$$\lambda_L = -1 + |S|$$

where S is the set of finite non-2-places of L which are ramified in L/K.

Proof. We simply apply Iwasawa's formula with $\chi(G, \mathcal{O}_L^\times)$ replaced by $-\chi(G, P_L)$ (i.e., by Theorem 6.2) to get

$$\begin{aligned}
\lambda_L &= 2\lambda_K - (2-1)\chi(G, P_L) + \sum_{w \nmid p} (e_w - 1) \\
&= 2 \cdot 0 - 1 + \sum_{w \in S} (2-1) \\
&= -1 + |S|
\end{aligned}$$

as claimed. □

A couple of remarks are in order. First, we'll discuss the cases which the proposition did not cover. Second, we'll give an alternative argument for one step in the proof of Proposition 6.16 which simplifies the one given above (and does not exclude $d \in \{1, 2\}$), but which has the disadvantage of not having an obvious generalization.

Remark 6.18. In the cases where $\ell = \mathbb{Q}(\sqrt{-d})$ with $d = 1$ or $d = 2$, we know that $\mathbb{Q}(\sqrt{-d})$ is a UFD and 2 ramifies in $\ell/\mathbb{Q}$, so $\lambda_L = 0$ since there's only one prime which ramifies in L/ℓ and $2 \nmid h_\ell = 1$ (see Theorem 3.3). Thus applying the same formula we used in the above corollary gives us

$$0 = \lambda_L = 2\lambda_K - (2-1)\chi(G, P_L) + \sum_{w \nmid 2}(e_w - 1) = 2 \cdot 0 - \chi(G, P_L) + 0 = -\chi(G, P_L).$$

Remark 6.19. As we mentioned above, we can simplify the proof of Proposition 6.16 while including the case $d \in \{1, 2\}$ at the same time. We won't require Theorem 6.13 of Greenberg, but we will use a result of Hasse's which Ferrero used in [Fer80]. It states that if k_n is the nth level of the cyclotomic $\mathbb{Z}_2$-extension of $\mathbb{Q}$ and $\ell_n = k_n(\sqrt{-d})$ where $d \in \mathbb{N}$ is squarefree, then

$$\mathcal{O}_{\ell_n}^\times = \mathcal{O}_{k_n}^\times \mu_{\ell_n}$$

where μ_{ℓ_n} is the set of roots of unity in ℓ_n, so we also have

$$\mathcal{O}_L^\times = \mathcal{O}_K^\times \mu_L$$

where $K = k_\infty$ and $L = \ell_\infty$. Hence for $n \in \mathbb{N} \cup \{\infty\}$

$$U_n := \{u \in \mathcal{O}_{\ell_n}^\times : |u|^2 = 1\} = \mu_{\ell_n}$$

(since the only norm one units in $\mathcal{O}_{k_n}$ are ± 1) and

$$V_n := \{\bar{u}/u : u \in \mathcal{O}_{\ell_n}^\times\} = \{\bar{u}/u : u \in \mu_{\ell_n}\} = \mu_{\ell_n}^2,$$

so we get

$$H^1(G_n, \mathcal{O}_{\ell_n}^\times) \cong U_n/V_n = \mu_{\ell_n}/\mu_{\ell_n}^2 \cong (\mu_{\ell_n}[2^\infty])/(\mu_{\ell_n}[2^\infty])^2.$$

If $d \notin \{1, 2\}$, then $\mu_L[2^\infty] = \{1, -1\}$, so

$$H^1(G, \mathcal{O}_L^\times) \cong \{1, -1\}/\{1\} \cong \mathbb{Z}/(2).$$

If $d \in \{1, 2\}$, then $\mu_L = \mu_{2^\infty} = \mu_L^2$ is the 2-primary part of the set of all roots of unity, so

$$H^1(G, \mathcal{O}_L^\times) \cong \mu_{2^\infty}/\mu_{2^\infty} = 0.$$

Note also that on the finite levels we have

$$U_n/V_n = \begin{cases} \mu_{2^{n+2}}/\mu_{2^{n+1}} & \text{if } d = 1 \\ \mu_{2^{n+1}}/\mu_{2^n} & \text{if } d = 2, \end{cases}$$

which paints a nice picture of why H^1 is still of order two on the finite levels but collapses on the infinite level when $d \in \{1, 2\}$. Coincidentally, this gives a proof of Greenberg's Theorem 6.13 in the special case where F'/F is an imaginary quadratic extension of $\mathbb{Q}$.

Now consider taking the cyclotomic $\mathbb{Z}_2$-extension K of a number field $k \neq \mathbb{Q}$ with a version of Weber's theorem holding for K and perhaps $\lambda_K = 0$. We'd like to be able to explicitly compute the lambda invariant of $L = K(\sqrt{-d})$ for squarefree $d \in \mathbb{N}$ by computing $\chi(G, P_L)$ with $G = \mathrm{Gal}(L/K)$. We'll use the following two theorems, the first of which generalizes Weber's theorem.

Theorem 6.20 (Hughes and Mollin, 1983)**.** *Let ℓ/k be a cyclic 2-extension of real abelian number fields. Suppose $\mathrm{Gal}(k/\mathbb{Q})$ has exponent n such that -1 is congruent to a power of 2 modulo n, and, if $k \neq \ell$, suppose that exactly one prime ramifies in ℓ/k. If $h(k)$ is odd, then every totally positive element of $\mathcal{O}_\ell^\times$ is a square in $\mathcal{O}_\ell^\times$.*

Proof. See the Theorem in Section 3 of [HM83]. □

Corollary 6.21. *Let $\ell = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ where p is a Fermat prime. Then every totally positive element of $\mathcal{O}_\ell^\times$ is a square in $\mathcal{O}_\ell^\times$.*

Corollary 6.22. *Let k_n be the nth layer in the cyclotomic $\mathbb{Z}_2$-extension of the first layer k in the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ where p is a Fermat prime. Suppose $h(k)$ is odd. Then every totally positive element of $\mathcal{O}_{k_n}^\times$ is a square in $\mathcal{O}_{k_n}^\times$.*

Theorem 6.23 (Ichimura and Nakajima, 2009)**.** *Let $\mathbb{Q}_\infty$ be the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ for some prime $p < 500$. Then $C_{\mathbb{Q}_\infty}[2]$ is trivial. In fact, the class number of every number field contained in $\mathbb{Q}_\infty$ is odd.*

Proof. See Proposition 1 and its proof in Section 3 of [IN10]. □

Proposition 6.24. *Let $K = k_\infty$ be the cyclotomic $\mathbb{Z}_2$-extension of the first layer k in the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$ where p is 2 or a Fermat prime and $h(k)$ is odd (e.g., we can take $p \in \{2, 3, 5, 17, 257\}$), and let $L = \ell_\infty$ be the cyclotomic $\mathbb{Z}_2$-extension of $\ell = k(\sqrt{-d})$ with $d \in \mathbb{Z}$ squarefree and $d > 2 \geq (d, p)$. Then*

$$\chi(G, P_L) = 1$$

where again $G = \mathrm{Gal}(L/K)$.

Proof. The proof runs as the proof of Proposition 6.16 mutatis mutandis. □

Corollary 6.25. *Let L/K be as in Proposition 6.24. Then*

$$\lambda_L = -1 + |S|$$

where S is the set of finite non-2-places of L which are ramified in L/K.

Proof. We only need to prove that $\lambda_K = 0$ which will follow from Theorem 3.3 once we show that 2 remains inert in k. When $p = 2$, this is clear, so we may assume $p = 2^{2^n} + 1$ for some $n \in \mathbb{N}_0$. For every $m \in \mathbb{N}$, we have that $F_m - 2 = 2^{2^m} - 1 =$

$F_0F_1\cdots F_{m-1}$ is a product of consecutive Fermat numbers $F_i = 2^{2^i}+1$, but this identity also shows that Fermat numbers are pairwise relatively prime, so $p^2 \nmid 2^{2^m}-1$ since $p = F_n$. This means that the multiplicative order of 2 modulo p^2 is not a power of 2 which forces the residue degree of 2 in $\mathbb{Q}(\zeta_{p^2})$ to be divisible by p. Consequently, the residue degree of 2 in k is p which is equivalent to 2 being inert in k. $\square$

Chapter 7

DEGREE p^2

In this chapter, we suppose that L/K is a cyclic p-extension of $\mathbb{Z}_p$-fields with $\langle g \rangle = G = \mathrm{Gal}(L/K) \cong \mathbb{Z}/(p^2)$ and $\mu_K = 0$. First, we'll prove a formula relating λ_L to λ_K in the flavor of 6.2 using nearly identical techniques. Again, we won't use the assumption that infinite places are unramified and we won't "remove" the finite places not lying above p which ramify. The formula will not be the same as we would get from Remark 6.4. Next, we will disprove (by explicit counter-example) a conjecture which is tempting to make though nonetheless false. We'll also give a decomposition of representations of the same type as Remark 6.12. In the last section, we'll give an alternative proof of the special formula for cyclic extensions of degree p^2. This alternative proof will suggest that it is unnecessary to have a complete description of indecomposable $\mathbb{Z}_pG$-modules which are free of finite $\mathbb{Z}_p$-rank.

We have the following description of the indecomposable $\mathbb{Z}_pG$-modules which are free of finite rank over $\mathbb{Z}_p$ due to Heller and Reiner in 1962 (see [HR62]).

Theorem 7.1. *Let $\langle g \rangle = G \cong \mathbb{Z}/(p^2)$. The only indecomposable $\mathbb{Z}_pG$-modules which are free of finite rank over $\mathbb{Z}_p$ are (up to isomorphism) $A = \mathbb{Z}_p$, $B = \mathbb{Z}_pG/(\Phi_p(g))$, $C = \mathbb{Z}_pG/(\Phi_{p^2}(g))$, $E = \mathbb{Z}_pG/(g^p - 1)$, and extensions*

$$I_1, \ldots, I_{p-2} \text{ of } C \text{ by } A \oplus E$$

$$II_1, \ldots, II_p \text{ of } C \text{ by } E$$

$$III_1, \ldots, III_{p-1} \text{ of } C \text{ by } A \oplus B$$

$$IV \text{ of } C \text{ by } A$$

$$V_1, \ldots, V_{p-1} \text{ of } C \text{ by } B,$$

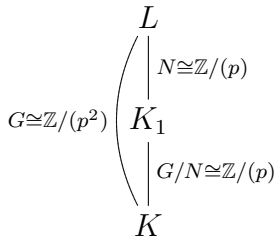
so there are exactly

$$4 + (p-2) + p + (p-1) + 1 + (p-1) = 4p + 1$$

isomorphism classes.

7.1 Special Formulas for $\mathbb{Z}/(p^2)$-Extensions

Proposition 7.2. *Let L/K be a $\mathbb{Z}/(p^2)$-extension of $\mathbb{Z}_p$-fields for some prime p with $G = \mathrm{Gal}(L/K)$, and let L/K_1 be the unique proper subextension with $N = \mathrm{Gal}(L/K_1)$ as seen in the following tower*



Suppose $\mu_K = 0$. Then $\mu_{K_1} = \mu_L = 0$ and

$$-p\chi(G, P_L) = -(2p-1)\chi(G/N, P_{K_1}) - \chi(N, P_L) + (p-1)|S_{\mathrm{ram}}^{\mathrm{split}}|$$

where $S_{\mathrm{ram}}^{\mathrm{split}}$ is the set of finite places of K not lying above p which ramify in K_1/K but split in L/K_1.

Proof. Use Theorem 7.1 for $\langle g \rangle = G$ to write

$$A_L^* \cong A^a \oplus B^b \oplus C^c \oplus E^e \oplus I_1^{i_1} \oplus \cdots II_1^{ii_1} \oplus \cdots III_1^{iii_1} \oplus \cdots IV^{iv} \oplus V_1^{v_1} \oplus \cdots$$

as $\mathbb{Z}_pG$-modules for some nonnegative integers a, b, c, e, i_1, …, i_{p-2}, ii_1, …, ii_p, iii_1, …, iii_{p-1}, iv, v_1, …, v_{p-1}. We want to apply the same ideas laid out in Chapter 5 and used in the proof of Theorem 6.2, so we need to know $\mathbb{Z}_p$-ranks, invariants,

and Euler characteristics, for each indecomposable M and each submodule M^N. We begin by computing the $\mathbb{Z}_p$-ranks for the $\mathbb{Z}_pG$-modules A, B, C, and E; we find

$$\begin{aligned}
&\operatorname{rank}_{\mathbb{Z}_p}(A) = \operatorname{rank}_{\mathbb{Z}_p}(\mathbb{Z}_p) = 1\\
&\operatorname{rank}_{\mathbb{Z}_p}(B) = \dim_{\mathbb{Q}_p}(B \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) = \dim_{\mathbb{Q}_p}(\mathbb{Q}_p[x]/(\Phi_p(x))) = \deg(\Phi_p(x)) = p-1\\
&\operatorname{rank}_{\mathbb{Z}_p}(C) = \dim_{\mathbb{Q}_p}(C \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) = \dim_{\mathbb{Q}_p}(\mathbb{Q}_p[x]/(\Phi_{p^2}(x))) = \deg(\Phi_{p^2}(x)) = p^2-p\\
&\operatorname{rank}_{\mathbb{Z}_p}(E) = \dim_{\mathbb{Q}_p}(E \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) = \dim_{\mathbb{Q}_p}(\mathbb{Q}_p[x]/(x^p-1)) = \deg(x^p-1) = p.
\end{aligned}$$

We know that $\mathbb{Z}_p$-ranks are additive on short exact sequences, so the above ranks are enough to determine all the $\mathbb{Z}_p$-ranks for $\mathbb{Z}_pG$-modules. For example,

$$\begin{aligned}
\operatorname{rank}_{\mathbb{Z}_p}(I_1) &= \operatorname{rank}_{\mathbb{Z}_p}(A \oplus E) + \operatorname{rank}_{\mathbb{Z}_p}(C)\\
&= \operatorname{rank}_{\mathbb{Z}_p}(A) + \operatorname{rank}_{\mathbb{Z}_p}(E) + p^2 - p\\
&= 1 + p + p^2 - p\\
&= p^2 + 1.
\end{aligned}$$

Now we compute G-invariants for the $\mathbb{Z}_pG$-modules A, B, C, and E; we find

$$\begin{aligned}
&A^G = \mathbb{Z}_p^G = \mathbb{Z}_p\\
&B^G = \{0\} \text{ since } (x-1, \Phi_p(x)) = 1 \text{ in } \mathbb{Z}_p[x]\\
&C^G = \{0\} \text{ since } (x-1, \Phi_{p^2}(x)) = 1 \text{ in } \mathbb{Z}_p[x]\\
&E^G = \Phi_p(g)E \cong \mathbb{Z}_pG/(g-1) \cong \mathbb{Z}_p \text{ since } (x-1, x^p-1) = x-1 \text{ in } \mathbb{Z}_p[x].
\end{aligned}$$

Note that since $C^G \cong 0$, any extension Y of C by X has G-invariants $Y^G \cong X^G$; this follows because the short exact sequence

$$0 \to X \to Y \to C \to 0$$

gives rise to the long exact sequence in cohomology

$$0 \to X^G \to Y^G \to C^G \to H^1(G, X) \to \cdots.$$

In addition, G-invariants distribute over direct sums, so knowing the above invariants allows us to easily find all other G-invariants for $\mathbb{Z}_pG$-modules. For example, it's now obvious that

$$I_1^G \cong (A \oplus E)^G = A^G \oplus E^G \cong \mathbb{Z}_p^2.$$

Likewise, Euler characteristics are additive on short exact sequences, so it suffices to only do these computations for A, B, C, and E. We get

$$\chi(G, A) = \text{ord}_p\left(\frac{|A/p^2A|}{|\{0\}/\{0\}|}\right) = \text{ord}_p(|\mathbb{Z}/(p^2)|) = 2$$
$$\chi(G, B) = \text{ord}_p\left(\frac{|\{0\}/\{0\}|}{|B/(g-1)B|}\right) = -\text{ord}_p(\mathbb{Z}_p[1]/(\Phi_p(1))) = -\text{ord}_p(\mathbb{Z}/(p)) = -1$$
$$\chi(G, C) = \text{ord}_p\left(\frac{|\{0\}/\{0\}|}{|C/(g-1)C|}\right) = -\text{ord}_p(\mathbb{Z}_p[1]/(\Phi_{p^2}(1))) = -\text{ord}_p(\mathbb{Z}/(p)) = -1$$
$$\chi(G, E) = \text{ord}_p\left(\frac{|\Phi_p(g)E/\Phi_{p^2}(g)\Phi_p(g)E|}{|\{0\}/\{0\}|}\right) = \text{ord}_p(|\mathbb{Z}_p/\Phi_{p^2}(1)\mathbb{Z}_p|) = 1$$

Now, for example, it's clear that

$$\chi(G, I_1) = \chi(G, A \oplus E) + \chi(G, C) = \chi(G, A) + \chi(G, E) - 1 = 2 + 1 - 1 = 2.$$

The results of these computations (as well as possible H^2, H^1 which we won't need) are summarized in Table 7.2.1. This table agrees with computations found in [Par66]. Now we do the same calculations with the above modules now regarded as $\mathbb{Z}_pN$-modules. We already know the $\mathbb{Z}_p$-ranks, so we turn immediately to finding the N-invariants. We get

$$A^N = \mathbb{Z}_p^N = \mathbb{Z}_p$$
$$B^N = B \cong \mathbb{Z}_p^{p-1} \text{ since } (x^p - 1, \Phi_p(x)) = \Phi_p(x) \text{ in } \mathbb{Z}_p[x]$$
$$C^N = \{0\} \text{ since } (x^p - 1, \Phi_{p^2}(x)) = 1 \text{ in } \mathbb{Z}_p[x]$$
$$E^N = E \cong \mathbb{Z}_p^p \text{ since } (x^p - 1, x^p - 1) = x^p - 1 \text{ in } \mathbb{Z}_p[x].$$

Again we have $C^N \cong 0$, so knowing the above invariants is enough to determine all the other N-invariants for $\mathbb{Z}_pN$-modules. Next, we take Euler characteristics (noting

	$\text{rank}_{\mathbb{Z}_p}(-)$	$(-)^G$	$H^2(G,-)$	$H^1(G,-)$	$\chi(G,-)$
A	1	$\mathbb{Z}_p$	$\mathbb{Z}_p/p^2\mathbb{Z}_p$	0	2
B	$p-1$	0	0	$\mathbb{Z}_p/p\mathbb{Z}_p$	-1
C	p^2-p	0	0	$\mathbb{Z}_p/p\mathbb{Z}_p$	-1
E	p	$\mathbb{Z}_p$	$\mathbb{Z}_p/p\mathbb{Z}_p$	0	1
$I_1,\ldots,I_{p-2}$	p^2+1	$\mathbb{Z}_p^2$	$\mathbb{Z}_p/p^2\mathbb{Z}_p$ $(\mathbb{Z}_p/p\mathbb{Z}_p)^2$ $\mathbb{Z}_p/p^2\mathbb{Z}_p \oplus \mathbb{Z}_p/p\mathbb{Z}_p$	0 0 $\mathbb{Z}_p/p\mathbb{Z}_p$	2
$II_1,\ldots,II_p$	p^2	$\mathbb{Z}_p$	0 $\mathbb{Z}_p/p\mathbb{Z}_p$	0 $\mathbb{Z}_p/p\mathbb{Z}_p$	0
$III_1,\ldots,III_{p-1}$	p^2	$\mathbb{Z}_p$	$\mathbb{Z}_p/p^2\mathbb{Z}_p$ $\mathbb{Z}_p/p^2\mathbb{Z}_p$ $\mathbb{Z}_p/p\mathbb{Z}_p$	$\mathbb{Z}_p/p^2\mathbb{Z}_p$ $(\mathbb{Z}_p/p\mathbb{Z}_p)^2$ $\mathbb{Z}_p/p\mathbb{Z}_p$	0
IV	p^2-p+1	$\mathbb{Z}_p$	$\mathbb{Z}_p/p\mathbb{Z}_p$	0	1
$V_1,\ldots,V_{p-1}$	p^2-1	0	0 0	$\mathbb{Z}/p^2\mathbb{Z}_p$ $(\mathbb{Z}_p/p\mathbb{Z}_p)^2$	-2

TABLE 7.2.1. Cohomology for extensions of degree p^2

that B and E have trivial N-action) and find

$$\begin{aligned}
\chi(N,A) &= \text{ord}_p\left(\frac{|A/pA|}{|\{0\}/\{0\}|}\right) = \text{ord}_p(|\mathbb{Z}/(p)|) = 1\\
\chi(N,B) &= (p-1)\chi(N,\mathbb{Z}_p) = p-1\\
\chi(N,C) &= -\text{ord}_p\left(\left|\frac{C}{(g-1)C}\right|\right) - \text{ord}_p\left(\left|\frac{(g-1)C}{(g-1)^2C}\right|\right) - \cdots = -p\\
\chi(N,E) &= p\chi(N,\mathbb{Z}_p) = p
\end{aligned}$$

The results of these computations are summarized in Table 7.2.2 where $n = 0,\ldots,p$ and $m = 0,\ldots,p-1$. Finally, we go through the calculations for $A^N, B^N,\ldots$ now regarded as $\mathbb{Z}_p[G/N]$-modules. We know the $\mathbb{Z}_p$-ranks by inspection of N-invariants column in Table 7.2.2, so we again jump to the G/N-invariants. To compute the G/N-invariants, we must first understand the G/N-action on the N-invariants. We

	$(-)^N$	$H^2(N,-)$	$H^1(N,-)$	$\chi(N,-)$
A	$\mathbb{Z}_p$	$\mathbb{Z}_p/p\mathbb{Z}_p$	0	1
B	$\mathbb{Z}_p^{p-1}$	$(\mathbb{Z}_p/p\mathbb{Z}_p)^{p-1}$	0	$p-1$
C	0	0	$(\mathbb{Z}_p/p\mathbb{Z}_p)^p$	$-p$
E	$\mathbb{Z}_p^p$	$(\mathbb{Z}_p/p\mathbb{Z}_p)^p$	0	p
$I_1,\ldots,I_{p-2}$	$\mathbb{Z}_p^{p+1}$	$(\mathbb{Z}_p/p\mathbb{Z}_p)^{n+1}$	$(\mathbb{Z}_p/p\mathbb{Z}_p)^n$	1
$II_1,\ldots,II_p$	$\mathbb{Z}_p^p$	$(\mathbb{Z}_p/p\mathbb{Z}_p)^n$	$(\mathbb{Z}_p/p\mathbb{Z}_p)^n$	0
$III_1,\ldots,III_{p-1}$	$\mathbb{Z}_p^p$	$(\mathbb{Z}_p/p\mathbb{Z}_p)^n$	$(\mathbb{Z}_p/p\mathbb{Z}_p)^n$	0
IV	$\mathbb{Z}_p$	$\mathbb{Z}_p/p\mathbb{Z}_p$	$(\mathbb{Z}_p/p\mathbb{Z}_p)^p$	$-p+1$
$V_1,\ldots,V_{p-1}$	$\mathbb{Z}_p^{p-1}$	$(\mathbb{Z}_p/p\mathbb{Z}_p)^m$	$(\mathbb{Z}_p/p\mathbb{Z}_p)^{m+1}$	-1

TABLE 7.2.2. Cohomology for the subgroup N

have

$A^N = A \cong \mathbb{Z}_p$

$B^N = B \cong (g-1)\mathbb{Z}_p[G/N]$ since $\mathrm{rank}_{\mathbb{Z}_p}(B) = p-1$ and B has non-trivial G-action

$C^N = \{0\}$

$E^N = E = \mathbb{Z}_p\langle g\rangle/(g^p-1) \cong \mathbb{Z}_p[\langle g\rangle/\langle g^p\rangle] = \mathbb{Z}_p[G/N]$.

Now the invariants and Euler characteristics follow easily from Table 6.2.1 in the proof of Theorem 6.2. The results are summarized in Table 7.2.3.

As in Chapter 6, we let S denote the set of finite places of K not lying above p which ramify in L/K. Then S is the disjoint union

$$S_{\mathrm{ram}}^{\mathrm{split}} \cup S_{\mathrm{split}}^{\mathrm{ram}} \cup S_{\mathrm{ram}}^{\mathrm{ram}}$$

where $S_{\mathrm{ram}}^{\mathrm{split}}$ consists of those places in S which ramify in K_1/K but split in L/K_1, $S_{\mathrm{split}}^{\mathrm{ram}}$ consists of those places in S which split in K_1/K but ramify in L/K_1, and $S_{\mathrm{ram}}^{\mathrm{ram}}$ consists of those places in S which are totally ramified in L/K. Note that we're using again here the fact that finite primes must either split or ramify in a degree p

	$(-)^{G/N}$	$H^2(G/N,-)$	$H^1(G/N,-)$	$\chi(G/N,-)$
A^N	$\mathbb{Z}_p$	$\mathbb{Z}_p/p\mathbb{Z}_p$	0	1
B^N	0	0	$\mathbb{Z}_p/p\mathbb{Z}_p$	-1
C^N	0	0	0	0
E^N	$\mathbb{Z}_p$	0	0	0
$I_1^N,\ldots,I_{p-2}^N$	$\mathbb{Z}_p^2$	$\mathbb{Z}_p/p\mathbb{Z}_p$	0	1
$II_1^N,\ldots,II_p^N$	$\mathbb{Z}_p$	0	0	0
$III_1^N,\ldots,III_{p-1}^N$	$\mathbb{Z}_p$	$\mathbb{Z}_p/p\mathbb{Z}_p$	$\mathbb{Z}_p/p\mathbb{Z}_p$	0
IV^N	$\mathbb{Z}_p$	$\mathbb{Z}_p/p\mathbb{Z}_p$	0	1
$V_1^N,\ldots,V_{p-1}^N$	0	0	$\mathbb{Z}_p/p\mathbb{Z}_p$	-1

TABLE 7.2.3. Cohomology for the quotient G/N

extension of $\mathbb{Z}_p$-fields (see the proof of Theorem 3.6). For convenience, we define

$$i := i_1 + i_2 + \ldots i_{p-2}$$

$$ii := ii_1 + ii_2 + \ldots ii_p$$

$$iii := iii_1 + iii_2 + \ldots iii_{p-1}$$

$$v := v_1 + v_2 + \ldots v_{p-1}$$

and

$$\alpha := c + i + ii + iii + iv + v$$

$$\beta := b - c + e - iv$$

$$\gamma := a - b + i + iv - v.$$

Thus Lemma 5.1, Remark 5.2, and the above tables imply

$$\begin{aligned}
&-\chi(G,P_L) + |S_{\text{ram}}^{\text{split}}| + |S_{\text{split}}^{\text{ram}}| + 2|S_{\text{ram}}^{\text{ram}}| = \chi(G,A_L) = -\chi(G,A_L^*)\\
&= -(2a - b - c + e + 2i + iv - 2v)\\
&= -(b - c + e - iv + 2a - 2b + 2i + 2iv - 2v)\\
&= -(\beta + 2\gamma),
\end{aligned}$$

$$
\begin{aligned}
&- \chi(N, P_L) + p|S^{\text{ram}}_{\text{split}}| + |S^{\text{ram}}_{\text{ram}}| = \chi(N, A_L) = -\chi(N, A^*_L) \\
&= -(a + (p-1)b - pc + pe + i - (p-1)iv - v) \\
&= -(pb - pc + pe - piv + a - b + i + iv - v) \\
&= -(p\beta + \gamma),
\end{aligned}
$$

and

$$
\begin{aligned}
&- \chi(G/N, P_{K_1}) + |S^{\text{split}}_{\text{ram}}| + |S^{\text{ram}}_{\text{ram}}| = \chi(G/N, A_{K_1}) = \chi(G/N, A^N_L) \\
&= -\chi(G/N, (A^N_L)^*) = -\chi(G/N, (A^*_L)_N) = -\chi(G/N, (A^*_L)^N) \\
&= -(a - b + i + iv - v) \\
&= -\gamma.
\end{aligned}
$$

Hence

$$
\begin{aligned}
&- p\chi(G, P_L) + p|S^{\text{split}}_{\text{ram}}| + p|S^{\text{ram}}_{\text{split}}| + 2p|S^{\text{ram}}_{\text{ram}}| \\
&= p\chi(G, A_L) \\
&= -p\beta - 2p\gamma \\
&= (2p-1)(-\gamma) - (p\beta + \gamma) \\
&= (2p-1)\chi(G/N, A_{K_1}) + \chi(N, A_L) \\
&= (2p-1)(-\chi(G/N, P_{K_1}) + |S^{\text{split}}_{\text{ram}}| + |S^{\text{ram}}_{\text{ram}}|) - \chi(N, P_L) + p|S^{\text{ram}}_{\text{split}}| + |S^{\text{ram}}_{\text{ram}}| \\
&= -(2p-1)\chi(G/N, P_{K_1}) - \chi(N, P_L) + (2p-1)|S^{\text{split}}_{\text{ram}}| + p|S^{\text{ram}}_{\text{split}}| + 2p|S^{\text{ram}}_{\text{ram}}|
\end{aligned}
$$

which proves Proposition 7.2. Notice that we did not use α. We will make use of α in the proof of the following corollary. □

Corollary 7.3. *Let L/K be as in Proposition 7.2. Suppose $\mu_K = 0$. Then $\mu_{K_1} = \mu_L = 0$ and*

$$
\begin{aligned}
\lambda_L &= p^2\lambda_K - (p-1)(p\chi(G, P_L) + (p-1)(-\chi(G/N, P_{K_1}) + |S^{\text{split}}_{\text{ram}}|)) + \sum_{w \nmid p}(e(w) - 1) \\
&= (1-p)\lambda_{K_1} + p(2p-1)\lambda_K + p(p-1)(|S^{\text{split}}_{\text{ram}}| + |S^{\text{ram}}_{\text{split}}| + 2|S^{\text{ram}}_{\text{ram}}| - \chi(G, P_L))
\end{aligned}
$$

where $e(w)$ is the ramification index in L/K of a finite place w of L.

Although Corollary 7.3 follows easily from Proposition 7.2 combined with Remark 6.4, we'll give a direct proof here.

Proof. By Remark 5.2 and the tables in the proof of Proposition 7.2 we find

$$\begin{aligned}
\lambda_L &= \mathrm{rank}_{\mathbb{Z}_p}(A_L^*) \\
&= a + (p-1)(b+pc) + pe + (p^2+1)i + p^2(ii+iii) + (p^2-p+1)iv + (p^2-1)v \\
&= p^2(c+i+ii+iii+iv+v) + p(b-c+e-iv) + a - b + i + iv - v \\
&= p^2\alpha + p\beta + \gamma \\
\lambda_{K_1} &= \mathrm{rank}_{\mathbb{Z}_p}(A_{K_1}^*) = \mathrm{rank}_{\mathbb{Z}_p}((A_L^*)^N) \\
&= a + (p-1)b + pe + (p+1)i + p(ii+iii) + iv + (p-1)v \\
&= p(b+e+i+ii+iii+v) + a - b + i + iv - v \\
&= p(\alpha+\beta) + \gamma \\
\lambda_K &= \mathrm{rank}_{\mathbb{Z}_p}(A_K^*) = \mathrm{rank}_{\mathbb{Z}_p}((A_{K_1}^*)^{G/N}) = \mathrm{rank}_{\mathbb{Z}_p}(((A_L^*)^N)^{G/N}) = \mathrm{rank}_{\mathbb{Z}_p}((A_L^*)^G) \\
&= a + e + 2i + ii + iii + iv \\
&= \alpha + \beta + \gamma.
\end{aligned}$$

Therefore

$$\begin{aligned}
\frac{\lambda_L - p^2\lambda_K}{p-1} &= \frac{p^2\alpha + p\beta + \gamma - p^2\alpha - p^2\beta - p^2\gamma}{p-1} = \frac{-(p^2-p)\beta - (p^2-1)\gamma}{p-1} \\
&= -p\beta - (p+1)\gamma = -p(\beta+2\gamma) - (p-1)(-\gamma) \\
&= -p\chi(G,P_L) + p|S_{\mathrm{ram}}^{\mathrm{split}}| + p|S_{\mathrm{split}}^{\mathrm{ram}}| + 2p|S_{\mathrm{ram}}^{\mathrm{ram}}| \\
&\quad - (p-1)(-\chi(G/N,P_{K_1}) + |S_{\mathrm{ram}}^{\mathrm{split}}| + |S_{\mathrm{ram}}^{\mathrm{ram}}|) \\
&= -(p\chi(G,P_L) + (p-1)(-\chi(G/N,P_{K_1}) + |S_{\mathrm{ram}}^{\mathrm{split}}|)) \\
&\quad + p|S_{\mathrm{ram}}^{\mathrm{split}}| + p|S_{\mathrm{split}}^{\mathrm{ram}}| + (p+1)|S_{\mathrm{ram}}^{\mathrm{ram}}| \\
&= -(p\chi(G,P_L) + (p-1)(-\chi(G/N,P_{K_1}) + |S_{\mathrm{ram}}^{\mathrm{split}}|))
\end{aligned}$$

$$+\frac{1}{p-1}\sum_{w\nmid p}(e(w)-1)$$

and

$$\begin{aligned}\frac{\lambda_L - p(2p-1)\lambda_K}{p-1} =& \frac{p^2\alpha + p\beta + \gamma - p(2p-1)\alpha - p(2p-1)\beta - p(2p-1)\gamma}{p-1}\\ =& \frac{(p-p^2)\alpha + (-2p^2+2p)\beta + (-2p^2+p+1)\gamma}{p-1}\\ =& -p\alpha - 2p\beta - (2p+1)\gamma\\ =& -(p(\alpha+\beta)+\gamma) - p(\beta+2\gamma)\\ =& -\lambda_{K_1} + p(-\chi(G,P_L) + |S^{\text{split}}_{\text{ram}}| + |S^{\text{ram}}_{\text{split}}| + 2|S^{\text{ram}}_{\text{ram}}|)\end{aligned}$$

which proves the corollary. □

Now we take note of a few immediate implications of Corollary 7.3.

Corollary 7.4. *Let L/K be as in Proposition 7.2. Suppose $\mu_K = 0$. Then*

1. $\lambda_L \equiv \lambda_K \pmod{p-1}$
2. $\lambda_L \equiv \lambda_{K_1} \pmod{p(p-1)}$
3. $\lambda_L \equiv \chi(G/N, P_{K_1}) - |S^{\text{split}}_{\text{ram}}| - |S^{\text{ram}}_{\text{ram}}| = -\chi(G/N, A_{K_1}) \pmod{p}$
4. $\lambda_L \equiv \chi(N, P_L) - p|S^{\text{ram}}_{\text{split}}| - |S^{\text{ram}}_{\text{ram}}| = -\chi(N, A_L) \pmod{p^2}$
5. $\text{ord}_p|H^2(G,P_L)| \le 2\lambda_K + \text{ord}_p|H^1(G,P_L)| + |S^{\text{split}}_{\text{ram}}| + |S^{\text{ram}}_{\text{split}}| + 2|S^{\text{ram}}_{\text{ram}}|$

Proof. Corollary 7.3 immediately implies 1, 2, 3, and 4. To prove 5 we need only note that

$$\begin{aligned}0 \le \frac{\lambda_L - \lambda_{K_1}}{p(p-1)} + \frac{\lambda_{K_1} - \lambda_K}{p-1} &= \frac{\lambda_L - (1-p)\lambda_{K_1} - p\lambda_K}{p(p-1)}\\ &= 2\lambda_K - \text{ord}_p|H^2(G,P_L)| + \text{ord}_p|H^1(G,P_L)| + |S^{\text{split}}_{\text{ram}}| + |S^{\text{ram}}_{\text{split}}| + 2|S^{\text{ram}}_{\text{ram}}|\end{aligned}$$

which completes the proof. □

Remark 7.5. Let L/K be as in Proposition 7.2 with $\mu_K = 0$. As we'll see later, we don't need Theorem 7.1 to prove any of Proposition 7.2, Corollary 7.3, or Corollary 7.8 below, but by using it we get more information in the form of a decomposition of A_L^* into non-isomorphic indecomposable $\mathbb{Z}_pG$-modules. There does not seem to be a simple way of determining each of the exponents a, b, c, e, i_1, …, i_{p-2}, ii_1, …, ii_p, iii_1, …, iii_{p-1}, iv, v_1, … v_{p-1} which appear, but we can determine b, c, e in terms of the others and Euler characteristics. To do this we note (by the computations in the proof of Proposition 7.2) that

$$\begin{aligned}
b &= a + i + iv - v - \gamma = a + i + iv - v - \chi(G/N, P_{K_1}) + |S_{\text{ram}}^{\text{split}}| + |S_{\text{ram}}^{\text{ram}}| \\
&= a + i + iv - v + \chi(G/N, A_{K_1}), \\
\beta &= -2\gamma + \chi(G, P_L) - |S_{\text{ram}}^{\text{split}}| - |S_{\text{split}}^{\text{ram}}| - 2|S_{\text{ram}}^{\text{ram}}| \\
&= -2\chi(G/N, P_{K_1}) + \chi(G, P_L) + |S_{\text{ram}}^{\text{split}}| - |S_{\text{split}}^{\text{ram}}|, \\
\alpha &= \lambda_K - \beta - \gamma = \lambda_K + \chi(G/N, P_{K_1}) - \chi(G, P_L) + |S_{\text{split}}^{\text{ram}}| + |S_{\text{ram}}^{\text{ram}}|, \\
c &= -(i + ii + iii + iv + v) + \lambda_K + \chi(G/N, P_{K_1}) - \chi(G, P_L) + |S_{\text{split}}^{\text{ram}}| + |S_{\text{ram}}^{\text{ram}}| \\
&= -(i + ii + iii + iv + v) + \lambda_K + \chi(G, A_L) - \chi(G/N, A_{K_1}), \\
e &= \beta - b + c + iv = -(a + 2i + ii + iii + iv) + \lambda_K.
\end{aligned}$$

Moreover, knowing these values for b, c, e in terms of a, i_1, …, i_{p-2}, ii_1, …, ii_p, iii_1, …, iii_{p-1}, iv, v_1, … v_{p-1} and Euler characteristics is sufficient to prove Corollary 7.3 (by computing the $\mathbb{Z}_p$-rank of A_L^*) and Corollary 7.8 (by tensoring A_L^* with $\mathbb{Q}_p$). In the case where $\lambda_K = 1$, we find that $i = 0$ and exactly one of a, e, ii, iii, iv is 1 while the rest are 0. For example, if $\lambda_K = 1 = a$ we get

$$A_L^* \cong A \oplus B^{1-v+\chi(G/N,A_{K_1})} \oplus C^{-v+\chi(G,A_L)-\chi(G/N,A_{K_1})} \oplus V_1^{v_1} \oplus \cdots \oplus V_{p-1}^{v_{p-1}}$$

as $\mathbb{Z}_pG$-modules. In the case where $\lambda_K = 0$, things simplify significantly since then $0 = a = e = i = ii = iii = iv$, so

$$A_L^* \cong B^{-v+\chi(G/N,A_{K_1})} \oplus C^{-v+\chi(G,A_L)-\chi(G/N,A_{K_1})} \oplus V_1^{v_1} \oplus \cdots \oplus V_{p-1}^{v_{p-1}}$$

as $\mathbb{Z}_p G$-modules where $V_1, \ldots, V_{p-1}$ are extensions of C by B. Further simplifying to $p = 2$ yields

$$A_L^* \cong B^{-v+\chi(G/N, A_{K_1})} \oplus C^{-v+\chi(G,A_L)-\chi(G/N,A_{K_1})} \oplus V_1^v$$

with

$$\begin{aligned} B &\cong \frac{\mathbb{Z}_2 G}{(g+1)}, \\ C &\cong \frac{\mathbb{Z}_2 G}{(g^2+1)}, \\ V_1 &\cong \frac{\mathbb{Z}_2 G}{(g+1)(g^2+1)} \end{aligned}$$

as $\mathbb{Z}_2 G$-modules.

Let L/K be as in Proposition 7.2 with $\mu_K = 0$. It would be nice to have a formula for λ_L in which only one Euler characteristic appears. After all, the extension L/K is cyclic, so maybe we can get away with only using $\chi(G, P_L)$. In light of Kida's formula (Theorem 3.6) and Theorem 6.2, it is natural to ask whether or not there is a constant c_p depending on p but not on L/K such that

$$\lambda_L \stackrel{?}{=} p^2 \lambda_K - c_p \chi(G, P_L) + \sum_{w \nmid p} (e(w) - 1). \tag{7.5.1}$$

If there was such a constant c_p, then using Kida's formula in the case where p is odd and L/K is an extension of CM-fields with maximal real subfields L^+/K^+ shows that

$$\begin{aligned} -(p^2-1)\delta &= \lambda_L^- - p^2 \lambda_K^- - \sum_{p \nmid w} (e(w) - 1) + \sum_{p \nmid w^+} (e(w^+) - 1) \\ &= -c_p(\chi(G, P_L) - \chi(G^+, P_{L^+})) = c_p \chi(G, \mathcal{O}_L^\times / \mathcal{O}_{L^+}^\times) \\ &= c_p \chi(G, \mu_L[p^\infty]) = c_p(-2\delta) \end{aligned}$$

where $\delta = 0$ if $\zeta_p \notin K$ and $\delta = 1$ if $\zeta_p \in K$. Thus if there is such a c_p, it must be $(p^2-1)/2$. Hence Corollary 7.3 implies that Equation 7.5.1 is equivalent to

$$-\frac{p^2-1}{2} \chi(G, P_L) \stackrel{?}{=} -(p-1)(p\chi(G, P_L) + (p-1)(-\chi(G/H, P_{K_1}) + |S_{\text{ram}}^{\text{split}}|)),$$

and simplifying gives

$$-\chi(G, P_L) \stackrel{?}{=} -2\chi(G/N, P_{K_1}) + 2|S^{\text{split}}_{\text{ram}}|. \tag{7.5.2}$$

It's easy to show that Equation 7.5.2 holds whenever $-\beta = |S^{\text{split}}_{\text{ram}}| + |S^{\text{ram}}_{\text{split}}|$ since then

$$-(\beta + 2\gamma) = -\chi(G, P_L) + |S^{\text{split}}_{\text{ram}}| + |S^{\text{ram}}_{\text{split}}| + 2|S^{\text{ram}}_{\text{ram}}| = -\chi(G, P_L) - \beta + 2|S^{\text{ram}}_{\text{ram}}|$$

and so

$$-\chi(G, P_L) = -2\gamma - 2|S^{\text{ram}}_{\text{ram}}| = -2\chi(G/N, P_{K_1}) + 2|S^{\text{split}}_{\text{ram}}|;$$

also, if $\beta = 0$, then

$$\begin{aligned} &-\chi(G, P_L) + |S^{\text{split}}_{\text{ram}}| + |S^{\text{ram}}_{\text{split}}| + 2|S^{\text{ram}}_{\text{ram}}| = -2\gamma \\ &= -2\chi(G/N, P_{K_1}) + 2|S^{\text{split}}_{\text{ram}}| + 2|S^{\text{ram}}_{\text{ram}}|, \end{aligned}$$

so

$$-\chi(G, P_L) = -2\chi(G/N, P_{K_1}) + |S^{\text{split}}_{\text{ram}}| - |S^{\text{ram}}_{\text{split}}|,$$

which means Equation 7.5.2 holds in this case if and only if L/K is totally ramified, whence $|S^{\text{split}}_{\text{ram}}| + |S^{\text{ram}}_{\text{split}}| = 0 = -\beta$ is just a special case of the above. However, Equation 7.5.2 appears to be false in general assuming Greenberg's conjecture 3.9 that the lambda invariants for totally real fields are all zero. In fact, it may be possible to construct an explicit counterexample as follows. Using Iwasawa's formula and Kida's formula in tandem, we get formulas for $\chi(G/N, \mathcal{O}^{\times}_{K_1}) = -\chi(G/N, P_{K_1})$ and $\chi(N, \mathcal{O}^{\times}_{L}) = -\chi(N, P_L)$ when L/K is an extension of CM-fields and p is an odd prime. Namely,

$$\begin{aligned} \chi(G/N, \mathcal{O}^{\times}_{K_1}) &= \frac{\lambda_{K_1} - \lambda_K}{p-1} - |S^{\text{split}}_{\text{ram}}| - |S^{\text{ram}}_{\text{ram}}| \\ &= \frac{\lambda^-_{K_1} - \lambda^-_K}{p-1} - |S^{\text{split}}_{\text{ram}}| - |S^{\text{ram}}_{\text{ram}}| \\ &= -\delta - |S^{\text{split}+}_{\text{ram}+}| - |S^{\text{ram}+}_{\text{ram}+}| \end{aligned} \tag{7.5.3}$$

where $S_{\text{ram}+}^{\text{split}+}$ is the set of finite places of K not lying above p which ramify in K_1^+/K^+ and split in L^+/K_1^+, etc; likewise

$$\chi(N, \mathcal{O}_L^\times) = -\delta - p|S_{\text{split}+}^{\text{ram}+}| - |S_{\text{ram}+}^{\text{ram}+}| \tag{7.5.4}$$

where again $\delta = 0$ if $\zeta_p \notin K$ and $\delta = 1$ if $\zeta_p \in K$. On the one hand, we know that

$$p\chi(G, \mathcal{O}_L^\times) = (2p-1)\chi(G/N, \mathcal{O}_{K_1}^\times) + \chi(N, \mathcal{O}_L^\times) + (p-1)|S_{\text{ram}}^{\text{split}}|$$

by Proposition 7.2. On the other hand, Equation 7.5.2 says

$$p\chi(G, \mathcal{O}_L^\times) \stackrel{?}{=} 2p\chi(G/N, \mathcal{O}_{K_1}^\times) + 2p|S_{\text{ram}}^{\text{split}}|,$$

so this amounts to the statement that

$$(2p-1)\chi(G/N, \mathcal{O}_{K_1}^\times) + \chi(N, \mathcal{O}_L^\times) + (p-1)|S_{\text{ram}}^{\text{split}}| \stackrel{?}{=} 2p\chi(G/N, \mathcal{O}_{K_1}^\times) + 2p|S_{\text{ram}}^{\text{split}}|,$$

or, equivalently, using Equations 7.5.3 and 7.5.4 yields

$$\begin{aligned} -\delta - p|S_{\text{split}+}^{\text{ram}+}| - |S_{\text{ram}+}^{\text{ram}+}| = \chi(N, \mathcal{O}_L^\times) &\stackrel{?}{=} \chi(G/N, \mathcal{O}_{K_1}^\times) + (p+1)|S_{\text{ram}}^{\text{split}}| \\ &= -\delta - |S_{\text{ram}+}^{\text{split}+}| - |S_{\text{ram}+}^{\text{ram}+}| + (p+1)|S_{\text{ram}}^{\text{split}}|. \end{aligned}$$

Simplifying gives

$$0 \stackrel{?}{=} p|S_{\text{split}+}^{\text{ram}+}| + (p+1)|S_{\text{ram}}^{\text{split}}| - |S_{\text{ram}+}^{\text{split}+}| \geq p|S_{\text{split}+}^{\text{ram}+}| + p|S_{\text{ram}+}^{\text{split}+}|$$

which is false unless $|S_{\text{split}+}^{\text{ram}+}| = |S_{\text{ram}+}^{\text{split}+}| = 0$, i.e., the only primes which ramify in L^+/K^+ are totally ramified. We now provide a concrete example showing that it is possible to have an extension L^+/K^+ which has a ramified prime that is not totally ramified.

Example 7.6. Let $p = 3$ and consider the number field $\mathbb{Q}(\zeta_{133})$. We have an isomorphism

$$(\mathbb{Z}/(133))^\times \cong \text{Gal}(\mathbb{Q}(\zeta_{133})/\mathbb{Q})$$

induced by $a \mapsto (\zeta_{133} \mapsto \zeta_{133}^a)$. Take $\ell^+ := \mathbb{Q}(\zeta_{133})^{\langle -1 \rangle} = \mathbb{Q}(\zeta_{133} + \zeta_{133}^{-1})$ to be the maximal real subfield and define

$$k^+ := \mathbb{Q}(\zeta_{133})^{\langle 4,-1 \rangle} \subseteq \ell^+.$$

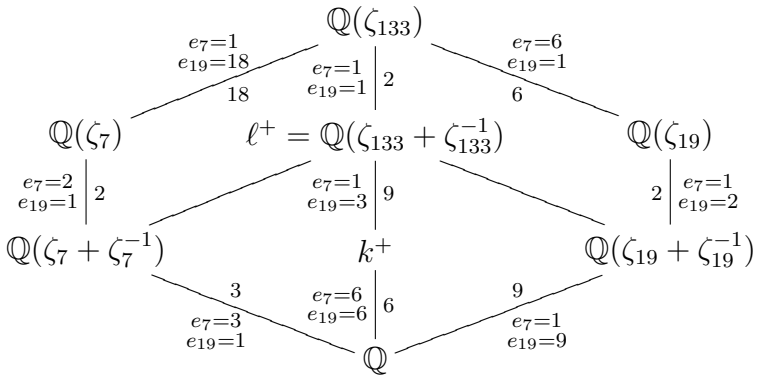
Then

$$\mathrm{Gal}(\ell^+/k^+) \cong \langle 4, -1 \rangle / \langle -1 \rangle = \langle 4 \langle -1 \rangle \rangle \cong \mathbb{Z}/(9),$$

so $L := \ell(i)_\infty, K := k(i)_\infty$ are CM-$\mathbb{Z}_3$-fields with

$$\mathrm{Gal}(L/K) \cong \mathrm{Gal}(L^+/K^+) \cong \mathrm{Gal}(\ell^+/k^+) \cong \mathbb{Z}/(9).$$

There are four subfields of $\mathbb{Q}(\zeta_{133})$ which have degree 3 over $\mathbb{Q}$. One of them is $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$ in which 19 does not ramify, but one can check that 19 ramifies in the other three. In particular, 19 ramifies in $\mathbb{Q}(\zeta_{133})^{\langle 2,-1 \rangle}/\mathbb{Q}$. Also, $\mathbb{Q}(\zeta_{133})/\ell^+$ is unramified at 19, and the ramification index of 19 in $\mathbb{Q}(\zeta_{133})/\mathbb{Q}$ is 18 since 19 is totally ramified in $\mathbb{Q}(\zeta_{19})/\mathbb{Q}$ and is unramified in $\mathbb{Q}(\zeta_7)/\mathbb{Q}$. Thus 19 is totally ramified in $k^+/\mathbb{Q}$, and the unique prime $\mathfrak{P}$ in k^+ lying above 19 has ramification index 3 in ℓ^+/k^+. The information is summarized in the following diagram.



This means there's a prime which is ramified but not totally ramified in L^+/K^+. As noted above, this would produce a counterexample to Equation 7.5.2 assuming that, at least in this case, $\lambda_{L^+} = \lambda_{K_1^+} = \lambda_{K^+} = 0$.

Remark 7.7. A formula which uses only Euler characteristics involving G is given by

$$\lambda_L = (2\varphi(p^2)+1)\lambda_K + \varphi(p^2)\chi(G, A_L) - \varphi(p)^2\chi(G, A_{K_1}).$$

Proofs of this formula as well as of Proposition 7.2 without using the classification of indecomposable $\mathbb{Z}_p$-free $\mathbb{Z}_pG$-modules are given later in the chapter.

7.2 $\mathbb{Q}_p$-Representations

Evoking the ideas of Section 6.2 in the last chapter, the proofs of Proposition 7.2 and Remark 7.3 actually show more than just formulas for Euler characteristics and lambda invariants. They show a statement about representations. Let $L/K_1/K$, $G = \mathrm{Gal}(L/K)$, and $N = \mathrm{Gal}(L/K_1)$, be as in Proposition 7.2 with $\mu_K = 0$. Define

$$V_L := A_L^* \otimes_{\mathbb{Z}_p} \mathbb{Q}_p,$$

and consider the corresponding representation

$$\pi_{L/K} \colon G \to \mathrm{GL}(V_L).$$

Then there is the following result about the decomposition of $\pi_{L/K}$.

Corollary 7.8. *Let $L/K_1/K$, $G = \mathrm{Gal}(L/K)$, and $N = \mathrm{Gal}(L/K_1)$, be as in Proposition 7.2 with $\mu_K = 0$. Then we have an isomorphism of $\mathbb{Q}_p$-representations*

$$\pi_{L/K} \cong \lambda_K\pi_G \oplus \chi(G/N, A_{K_1})\pi_{p-1} \oplus (\chi(G, A_L) - \chi(G/N, A_{K_1}))\pi_{p(p-1)}$$

where π_G is the regular representation and π_d is the unique faithful irreducible representation of degree $d \in \{p-1, p(p-1)\}$.

Proof. We'll use all the notation in the proof of Proposition 7.2. Upon tensoring with $\mathbb{Q}_p$, all extensions become split extensions, so we have

$$\begin{aligned} V_L &\cong \left(\frac{\mathbb{Q}_p[x]}{(x-1)}\right)^{a+e+i+ii+iii+iv} \oplus \left(\frac{\mathbb{Q}_p[x]}{\Phi_p(x)}\right)^{b+e+i+ii+iii+v} \oplus \left(\frac{\mathbb{Q}_p[x]}{\Phi_{p^2}(x)}\right)^{c+i+ii+iii+iv+v} \\ &= \left(\frac{\mathbb{Q}_p[x]}{(x-1)}\right)^{\alpha+\beta+\gamma} \oplus \left(\frac{\mathbb{Q}_p[x]}{\Phi_p(x)}\right)^{\alpha+\beta} \oplus \left(\frac{\mathbb{Q}_p[x]}{\Phi_{p^2}(x)}\right)^{\alpha} \end{aligned}$$

as $\mathbb{Q}_pG$-modules where our generator g of G acts as x on $\mathbb{Q}_p[x]$. Now

$$\mathbb{Q}_pG \cong \frac{\mathbb{Q}_p[x]}{(x^{p^2}-1)} \cong \frac{\mathbb{Q}_p[x]}{(x-1)} \oplus \frac{\mathbb{Q}_p[x]}{(\Phi_p(x))} \oplus \frac{\mathbb{Q}_p[x]}{(\Phi_{p^2}(x))}$$

as $\mathbb{Q}_pG$-modules, so in fact

$$\begin{aligned} V_L &\cong \left(\frac{\mathbb{Q}_p[x]}{(x^{p^2}-1)}\right)^{\alpha+\beta+\gamma} \oplus \left(\frac{\mathbb{Q}_p[x]}{\Phi_p(x)}\right)^{-\gamma} \oplus \left(\frac{\mathbb{Q}_p[x]}{\Phi_{p^2}(x)}\right)^{-(\beta+\gamma)} \\ &\cong \left(\frac{\mathbb{Q}_p[x]}{(x^{p^2}-1)}\right)^{\lambda_K} \oplus \left(\frac{\mathbb{Q}_p[x]}{\Phi_p(x)}\right)^{\chi(G/N,A_{K_1})} \oplus \left(\frac{\mathbb{Q}_p[x]}{\Phi_{p^2}(x)}\right)^{\chi(G,A_L)-\chi(G/N,A_{K_1})} \end{aligned}$$

Note that if either $\chi(G/N, A_{K_1})$ or $\chi(G, A_L) - \chi(G/N, A_{K_1})$ happen to be negative, we interpret the above isomorphism as differences of representations. Now suppose $\pi_d \colon G \to \mathrm{GL}(V_d)$ is a faithful irreducible representation of G over $\mathbb{Q}_p$ of some degree d. Since V_d is a simple $\mathbb{Q}_pG$-module we know that $V_d \cong \mathbb{Q}_pG/M_d$ for some maximal ideal M_d

$$\mathbb{Q}_pG \cong \mathbb{Q}_p[x]/(x^{p^2}-1),$$

so M_d corresponds to either $(x-1)/(x^{p^2}-1)$, $(\Phi_p(x))/(x^{p^2}-1)$, or $(\Phi_{p^2}(x))/(x^{p^2}-1)$, under this isomorphism, but $(x-1)/(x^p-1)$ corresponds to the trivial representation (not faithful), whence either

$$V_d \cong \frac{\mathbb{Q}_p[x]/(x^{p^2}-1)}{(\Phi_p(x))/(x^{p^2}-1)} \cong \frac{\mathbb{Q}_p[x]}{(\Phi_p(x))}$$

or

$$V_d \cong \frac{\mathbb{Q}_p[x]/(x^{p^2}-1)}{(\Phi_{p^2}(x))/(x^{p^2}-1)} \cong \frac{\mathbb{Q}_p[x]}{(\Phi_{p^2}(x))}$$

which finishes the proof. □

7.3 Alternative Proof of Proposition 7.2

As mentioned earlier in this chapter, if we only care about formulas for lambda invariants (and not about representations), then we actually don't need the structure Theorem 7.1. In this section, we'll show how to rederive Proposition 7.2 using some simple results about Herbrand quotients inspired by a section in Artin and Tate's *Class Field Theory* ([AT09]).

Let A be an abelian group and suppose there are endomorphisms α, β of A such that $\alpha \circ \beta = 0 = \beta \circ \alpha$. Following [AT09], we define

$$\mathrm{q}_{\alpha,\beta}(A) = \frac{|\ker(\alpha)/\mathrm{im}(\beta)|}{|\ker(\beta)/\mathrm{im}(\alpha)|}$$

when these quantities are finite. When $G = \langle g \rangle$ is a finite cyclic group and A is $\mathbb{Z}G$-module, denote by $h(G, A)$ the Herbrand quotient of A with respect to G, i.e.,

$$h(G, A) = \mathrm{q}_{\varphi,\psi}(A)$$

where (as in Chapter 5 and as in the proof of Proposition 4.11)

$$\varphi = \varphi_{A,g} \colon A \to A \colon a \mapsto (g-1)a$$
$$\psi = \psi_{A,g} \colon A \to A \colon a \mapsto (g^{|G|-1} + g^{|G|-2} + \cdots + 1)a.$$

Lemma 7.9. *Let A be an abelian group and suppose there are endomorphisms α, β of A such that $\alpha \circ \beta = \beta \circ \alpha$. Then*

$$\mathrm{q}_{0,\alpha\circ\beta}(A) = \mathrm{q}_{0,\alpha}(A)\mathrm{q}_{0,\beta}(A)$$

when these quantities are defined.

Proof. We have exact sequences

$$0 \to \ker(\beta) \hookrightarrow \beta^{-1}(\ker(\alpha)) \xrightarrow{\beta} \beta(A) \cap \ker(\alpha) \to 0,$$
$$0 \to \ker(\alpha) \cap \ker(\beta) \hookrightarrow \ker(\beta) \xrightarrow{\alpha} \alpha(\ker(\beta)) \to 0$$

so

$$|\beta^{-1}(\ker(\alpha))| = |A/\beta(A)||\beta(A)/\alpha(\beta(A))|,$$
$$|\ker(\beta)| = |\ker(\alpha) \cap \ker(\beta)||\alpha(\ker(\beta))|.$$

Also, α maps $\ker(\beta)$ to itself and maps $\beta(A)$ to itself since α commutes with β, so

$$\mathrm{q}_{0,\alpha}(A) = \mathrm{q}_{0,\alpha}(\ker(\beta))\mathrm{q}_{0,\alpha}(\beta(A)).$$

Therefore

$$\begin{aligned}
\mathrm{q}_{0,\alpha\circ\beta}(A) &= \frac{|A/\alpha(\beta(A))|}{|\ker(\alpha\circ\beta)|} = \frac{|A/\beta(A)||\beta(A)/\alpha(\beta(A))|}{|\beta^{-1}(\ker(\alpha))|} \\
&= \frac{|A/\beta(A)||\beta(A)/\alpha(\beta(A))|}{|\ker(\beta)||\beta(A)\cap\ker(\alpha)|} = \mathrm{q}_{0,\beta}(A)\mathrm{q}_{0,\alpha}(\beta(A)) \\
&= \mathrm{q}_{0,\beta}(A)\mathrm{q}_{0,\alpha}(A)\mathrm{q}_{0,\alpha}(\ker(\beta))^{-1} \\
&= \mathrm{q}_{0,\beta}(A)\mathrm{q}_{0,\alpha}(A)\frac{|\ker(\alpha)\cap\ker(\beta)|}{|\ker(\beta)/\alpha(\ker(\beta))|} \\
&= \mathrm{q}_{0,\beta}(A)\mathrm{q}_{0,\alpha}(A)
\end{aligned}$$

as needed. □

We can use this lemma to get the following theorem which computes Herbrand quotients of $\mathbb{Z}/(p)$-modules A in terms of the multiplication maps $0\colon A \to A\colon a \mapsto 0$ and $p\colon A \to A\colon a \mapsto pa$.

Theorem 7.10. *Let $G = \langle g\rangle \cong \mathbb{Z}/(p^2)$ for some prime p, $N = \langle g^p\rangle$, and A be a $\mathbb{Z}G$-module. Suppose $\mathrm{q}_{0,p}(A)$ is defined. Then*

$$h(N,A)^{p-1} = \frac{\mathrm{q}_{0,p}(A^N)^p}{\mathrm{q}_{0,p}(A)}$$

and likewise

$$h(G/N, A^N)^{p-1} = \frac{\mathrm{q}_{0,p}(A^G)^p}{\mathrm{q}_{0,p}(A^N)}.$$

Proof. See the proof of Theorem q.4 in [AT09]. □

We can analogously compute Herbrand quotients of $\mathbb{Z}/(p^2)$-modules in terms of the multiplication maps by p and 0 on submodules.

Theorem 7.11. *Let G, N, and A be as in Theorem 7.10. Suppose $\mathrm{q}_{0,p^2}(A)$ is defined. Then*

$$h(G,A)^{p(p-1)} = \frac{\mathrm{q}_{0,p}(A^G)^{2p^2-p}}{\mathrm{q}_{0,p}(A)\mathrm{q}_{0,p}(A^N)^{p-1}}.$$

Proof. We want to analyze

$$\begin{aligned} h(G,A) &= h(G,A^G)h(G,A^{g-1}) = \mathrm{q}_{0,p^2}(A^G)h(G,A^{g-1}) \\ &= \mathrm{q}_{0,p^2}(A^G)h(G,(A^N)^{g-1})h(G,A^{g^p-1}) \end{aligned} \tag{7.11.1}$$

where, for example, $A^{g-1} = \mathrm{im}(\varphi)$. Note that

$$h(G,A^{g^p-1}) = \mathrm{q}_{g-1,0}(A^{g^p-1}) = \mathrm{q}_{0,g-1}(A^{g^p-1})^{-1} \tag{7.11.2}$$

and that Lemma 7.9 gives

$$\mathrm{q}_{0,p(g-1)}(A^{g^p-1}) = \mathrm{q}_{0,p}(A^{g^p-1})\mathrm{q}_{0,g-1}(A^{g^p-1}). \tag{7.11.3}$$

Of course, we also know that $\Phi_{p^2}(g)$ annihilates A^{g^p-1}, so g acts as a primitive p^2th root of unity on A^{g^p-1}, which implies that p acts as $(g-1)^{p^2-p}$ times a unit in the group ring. Consequently,

$$\mathrm{q}_{0,p(g-1)}(A^{g^p-1}) = \mathrm{q}_{0,(g-1)^{p^2-p+1}}(A^{g^p-1}) = \mathrm{q}_{0,g-1}(A^{g^p-1})^{p^2-p+1} \tag{7.11.4}$$

by repeated application of Lemma 7.9. Thus combining Equations 7.11.2, 7.11.3, and 7.11.4, gives

$$\begin{aligned} h(G,A^{g^p-1})^{p^2-p} &\overset{7.11.2}{=} \mathrm{q}_{0,g-1}(A^{g^p-1})^{-(p^2-p)} = \frac{\mathrm{q}_{0,g-1}(A^{g^p-1})}{\mathrm{q}_{0,g-1}(A^{g^p-1})^{p^2-p+1}} \\ &\overset{7.11.4}{=} \frac{\mathrm{q}_{0,g-1}(A^{g^p-1})}{\mathrm{q}_{0,p(g-1)}(A^{g^p-1})} \overset{7.11.3}{=} \frac{1}{\mathrm{q}_{0,p}(A^{g^p-1})} \\ &= \frac{\mathrm{q}_{0,p}(A^N)}{\mathrm{q}_{0,p}(A)}. \end{aligned} \tag{7.11.5}$$

Therefore Equations 7.11.1 and 7.11.5 together give

$$\begin{aligned}
h(G,A)^{p(p-1)} &\overset{7.11.1}{=} \mathrm{q}_{0,p^2}(A^G)^{p(p-1)} h(G,(A^N)^{g-1})^{p(p-1)} h(G,A^{g^p-1})^{p(p-1)} \\
&\overset{7.11.5}{=} \mathrm{q}_{0,p^2}(A^G)^{p(p-1)} h(G,(A^N)^{g-1})^{p(p-1)} \frac{\mathrm{q}_{0,p}(A^N)}{\mathrm{q}_{0,p}(A)} \\
&= \mathrm{q}_{0,p^2}(A^G)^{p(p-1)} \left(\frac{h(G/N,A^N)}{h(G/N,A^G)}\right)^{p(p-1)} \frac{\mathrm{q}_{0,p}(A^N)}{\mathrm{q}_{0,p}(A)} \\
&= \mathrm{q}_{0,p^2}(A^G)^{p(p-1)} \frac{h(G/N,A^N)^{p(p-1)}}{\mathrm{q}_{0,p}(A^G)^{p(p-1)}} \cdot \frac{\mathrm{q}_{0,p}(A^N)}{\mathrm{q}_{0,p}(A)} \\
&\overset{\text{thm } 7.10}{=} \mathrm{q}_{0,p^2}(A^G)^{p(p-1)} \frac{\mathrm{q}_{0,p}(A^G)^{p^2}/\mathrm{q}_{0,p}(A^N)^p}{\mathrm{q}_{0,p}(A^G)^{p(p-1)}} \cdot \frac{\mathrm{q}_{0,p}(A^N)}{\mathrm{q}_{0,p}(A)} \\
&= \mathrm{q}_{0,p}(A^G)^{2p(p-1)} \frac{\mathrm{q}_{0,p}(A^G)^p}{\mathrm{q}_{0,p}(A^N)^p} \cdot \frac{\mathrm{q}_{0,p}(A^N)}{\mathrm{q}_{0,p}(A)} \\
&= \frac{\mathrm{q}_{0,p}(A^G)^{2p^2-p}}{\mathrm{q}_{0,p}(A)\mathrm{q}_{0,p}(A^N)^{p-1}}
\end{aligned}$$

as claimed. □

Now we can put Theorems 7.10 and 7.11 together to relate various Herbrand quotients of subgroups and quotient groups.

Corollary 7.12. *Let G, N, and A be as in Theorem 7.10. Suppose $\mathrm{q}_{0,p^2}(A)$ is defined. Then*

$$h(G,A)^p = h(N,A)h(G/N,A^N)^{2p-1}.$$

Also,

$$h(G,A^N)^2 = \frac{h(G/N,A^N)^2}{h(G,A^G)}.$$

Proof. On the one hand, Theorem 7.10 implies

$$\begin{aligned}
h(N,A)^{p-1} h(G/N,A^N)^{(2p-1)(p-1)} &= \frac{\mathrm{q}_{0,p}(A^N)^p}{\mathrm{q}_{0,p}(A)} \left(\frac{\mathrm{q}_{0,p}(A^G)^p}{\mathrm{q}_{0,p}(A^N)}\right)^{2p-1} \\
&= \frac{\mathrm{q}_{0,p}(A^G)^{2p^2-p}}{\mathrm{q}_{0,p}(A)\mathrm{q}_{0,p}(A^N)^{p-1}}.
\end{aligned}$$

On the other hand, Theorem 7.11 says

$$h(G,A)^{p(p-1)} = \frac{\mathrm{q}_{0,p}(A^G)^{2p^2-p}}{\mathrm{q}_{0,p}(A)\mathrm{q}_{0,p}(A^N)^{p-1}}.$$

These quantities are equal, and thus the first statement follows by taking $(p-1)$th roots. Now plug in $A = A^N$. Then we get

$$\begin{aligned} h(G,A^N)^{p(p-1)} &= \frac{\mathrm{q}_{0,p}(A^G)^{2p^2-p}}{\mathrm{q}_{0,p}(A^N)^p} = \left(\frac{\mathrm{q}_{0,p}(A^G)^p}{\mathrm{q}_{0,p}(A^N)}\right)^p \mathrm{q}_{0,p}(A^G)^{p(p-1)} \\ &= h(G/N,A^N)^{p(p-1)}\mathrm{q}_{0,p}(A^G)^{p(p-1)}, \end{aligned}$$

so

$$h(G,A^N)^2 = \frac{h(G/N,A^N)^2}{\mathrm{q}_{0,p}(A^G)^2} = \frac{h(G/N,A^N)^2}{h(G,A^G)}$$

which proves the second statement. □

Remark 7.13. Once again, let G, N, and A be as in Theorem 7.10. Suppose $\mathrm{q}_{0,p^2}(A)$ is defined. Then Remark 7.12 holds. In particular, we can let $A = A_L$ where L/K, G, N are as Proposition 7.2 since

$$\mathrm{q}_{0,p^2}(A_L) = \mathrm{q}_{0,p^2}((\mathbb{Q}_p/\mathbb{Z}_p)^{\lambda_L}) = \left(\frac{1}{|(\mathbb{Q}_p/\mathbb{Z}_p)[p^2]|}\right)^{\lambda_L} = p^{-2\lambda_L}.$$

Taking p-orders in the first statement of Corollary 7.12 yields

$$p\chi(G,A_L) = \chi(N,A_L) + (2p-1)\chi(G/N,A_L^N),$$

so this along with Lemma 5.1 gives another proof of Proposition 7.2. We are also in position to give a proof of the formula in Remark 7.7. We use Corollaries 6.4 and 7.12 to find

$$\begin{aligned} \lambda_L &\overset{6.4}{=} p^2\lambda_K + (p-1)(p\chi(G/N,A_{K_1}) + \chi(N,A_L)) \\ &\overset{7.12}{=} p^2\lambda_K + (p-1)(-(p-1)\chi(G/N,A_{K_1}) + p\chi(G,A_L)), \end{aligned}$$

but taking p-orders in the second statement of Corollary 7.12 yields

$$2\chi(G, A_{K_1}) = 2\chi(G/N, A_{K_1}) - \chi(G, A_K) = 2\chi(G/N, A_{K_1}) + 2\lambda_K,$$

so in fact

$$\begin{aligned}\lambda_L &= p^2\lambda_K + (p-1)(-(p-1)(-\lambda_K + \chi(G, A_{K_1})) + p\chi(G, A_L)) \\ &= (2p(p-1)+1)\lambda_K - (p-1)^2\chi(G, A_{K_1}) + p(p-1)\chi(G, A_L)\end{aligned}$$

which is precisely the formula in Remark 7.7.

Chapter 8

DEGREE $\geq p^3$

In this chapter, we suppose that $G \cong \mathbb{Z}/(p^n)$ for some arbitrary n. In [HR63], it was shown that for $n \geq 3$ there are infinitely many isomorphism classes of indecomposable $\mathbb{Z}_pG$-modules which are free of finite rank over $\mathbb{Z}_p$. It should still be possible, however, to produce formulas similar to those found in the previous chapter, so long as we can classify the indecomposables up to $\mathbb{Z}_p$-rank, invariants, and Herbrand quotients. After all, we discovered in the last section of the previous chapter that the structure theorem for $\mathbb{Z}_pG$-modules for $G \cong \mathbb{Z}/(p^2)$ (Theorem 7.1) was unnecessary to prove Proposition 7.2. We begin with the following lemma. If M is an R-module (R a commutative ring with 1), we say a submodule $N \leq M$ is R**-pure** when $rM \cap N \subseteq rN$ for every $r \in R$.

Lemma 8.1. *Let $G = \langle g \rangle \cong \mathbb{Z}/(p^n)$ for some prime p and some $n \in \mathbb{N}$. Suppose M is a $\mathbb{Z}_pG$-module which is free of finite rank over $\mathbb{Z}_p$. Then there is a short exact sequence of $\mathbb{Z}_pG$-modules*

$$0 \to M' \to M \to \mathbb{Z}_p[\zeta_{p^n}]^{\oplus r} \to 0$$

where M' is a $\mathbb{Z}_p$-pure $\mathbb{Z}_pG$-submodule of M which is annihilated by $g^{p^{n-1}} - 1$ and $\mathbb{Z}_p[\zeta_{p^n}]$ has $\mathbb{Z}_pG$-module structure given by

$$\mathbb{Z}_p[\zeta_{p^n}] \cong \frac{\mathbb{Z}_pG}{\Phi_{p^n}(g)\mathbb{Z}_pG}$$

with $\Phi_{p^n}(x) = p^n$th cyclotomic polynomial.

Proof. Define

$$M' := \{m \in M : (g^{p^{n-1}} - 1)m = 0\}.$$

Then M' is a $\mathbb{Z}_pG$-submodule of M since it's the kernel of a $\mathbb{Z}_pG$-homomorphism, namely, the multiplication by $g^{p^{n-1}} - 1$ map on M. We know M' is $\mathbb{Z}_p$-pure since if $rm = m'$ for some $r \in \mathbb{Z}_p$, some $m \in M$, and some $m' \in M'$, then

$$r((g^{p^{n-1}} - 1)m) = (g^{p^{n-1}} - 1)(rm) = (g^{p^{n-1}} - 1)m' = 0,$$

so $(g^{p^{n-1}} - 1)m = 0$ (i.e., $m \in M'$) because M is $\mathbb{Z}_p$-torsion free. Also, M/M' is annihilated by $\Phi_{p^n}(g)$ since

$$(g^{p^{n-1}} - 1)(\Phi_{p^n}(g)m) = ((g^{p^{n-1}} - 1)(\Phi_{p^n}(g))m = (g^{p^n} - 1)m = 0$$

for all $m \in M$. Thus M/M' is a $\mathbb{Z}_p[\zeta_{p^n}]$-module which (since $M' \leq M$ is $\mathbb{Z}_p$-pure and $\mathbb{Z}_p$ is a PID) is free of finite rank over $\mathbb{Z}_p$. Note that $\mathbb{Z}_p \cap \mathbb{Z}_p[\zeta_{p^n}]\alpha$ is a non-zero ideal of $\mathbb{Z}_p$ when $0 \neq \alpha \in \mathbb{Z}_p[\zeta_{p^n}]$, so if $\alpha\overline{m} = 0$ for some $\overline{m} \in M/M'$, then $r\overline{m} = \beta(\alpha\overline{m}) = 0$ where $0 \neq r = \beta\alpha \in \mathbb{Z}_p$ for some $\beta \in \mathbb{Z}_p[\zeta_{p^n}]$, so $\overline{m} = 0$ because M/M' is $\mathbb{Z}_p$-free. Hence M/M' is torsion free as a $\mathbb{Z}_p[\zeta_{p^n}]$-module; moreover, M/M' is finitely generated over $\mathbb{Z}_p[\zeta_{p^n}]$ since it's finitely generated over $\mathbb{Z}_p$. Thus M/M' is free of finite rank over $\mathbb{Z}_p[\zeta_{p^n}]$ since $\mathbb{Z}_p[\zeta_{p^n}]$ is a PID. □

This lemma suggests that it may suffice to compute $\mathbb{Z}_p$-ranks and Euler characteristics for $\mathbb{Z}_pG$ modules of the form $\mathbb{Z}_p[\zeta_{p^i}]$. This is indeed the case, and Proposition 8.3 below makes this idea precise. In the proof of the proposition, we'll need the five-term, inflation-restriction exact sequence, so we recall the statement here.

Theorem 8.2 (Inflation-Restriction Sequence)**.** *Let G be a profinite group and N be a closed normal subgroup. Then for every $\mathbb{Z}G$-module M there is an exact sequence*

$$\begin{aligned} 0 \to H^1(G/N, M^N) &\xrightarrow{\text{inf}} H^1(G, M) \xrightarrow{\text{res}} H^1(N, M)^{G/N} \\ &\to H^2(G/N, M^N) \xrightarrow{\text{inf}} H^2(G, M) \end{aligned}$$

where inf *denotes inflation and* res *denotes restriction.*

8.1 General Formulas for $\mathbb{Z}/(p^n)$-Extensions

Proposition 8.3. *Let $G = \langle g \rangle \cong \mathbb{Z}/(p^n)$ for some prime p and some $n \in \mathbb{N}_0$. Suppose M is a $\mathbb{Z}_pG$-module which is free of finite rank over $\mathbb{Z}_p$. Then there is a sequence $r_0, \ldots, r_n \in \mathbb{N}_0$ such that for every subgroup $N_i = \langle g^{p^i} \rangle$ with $0 \leq i \leq n$ we have*

$$\operatorname{rank}_{\mathbb{Z}_p}(M^{N_i}) = \sum_{t=0}^{i} r_t \varphi(p^t)$$

and

$$\chi(N_i, M) = (n-i) \sum_{t=0}^{i} r_t \varphi(p^t) - p^i \sum_{t=i+1}^{n} r_t.$$

Proof. We use induction on n and Lemma 8.1. If $n = 0$, then $\mathbb{Z}_pG \cong \mathbb{Z}_p = \mathbb{Z}_p[\zeta_{p^0}]$ and $M \cong \mathbb{Z}_p[\zeta_{p^0}]^{r_0}$ is a free $\mathbb{Z}_p$-module for some $r_0 \in \mathbb{N}_0$, so the proposition is clear in this case since $0 \leq i \leq n = 0$ implies

$$\operatorname{rank}_{\mathbb{Z}_p}(M^{N_0}) = \operatorname{rank}_{\mathbb{Z}_p}(M) = r_0 = \sum_{t=0}^{0} r_t \varphi(p^t)$$

and

$$\chi(N_0, M) = 0 = (0-0) \sum_{t=0}^{0} r_t \varphi(p^t) - p^0 \sum_{t=1}^{0} r_t,$$

where

$$\sum_{t=1}^{0} r_t = 0$$

is an empty sum. Now suppose $n \geq 1$ and the proposition is true for $n-1$. By Lemma 8.1, we have a short exact sequence of $\mathbb{Z}_pG$-modules

$$0 \to M' \to M \to \mathbb{Z}_p[\zeta_{p^n}]^{\oplus r_n} \to 0$$

where M' can be regarded as a $\mathbb{Z}_pG'$-module where $G' = G/N_{n-1} \cong \mathbb{Z}/(p^{n-1})$. By induction, there is a sequence $r_0, \ldots, r_{n-1} \in \mathbb{N}_0$ such that for every subgroup $N_i' =$

N_i/N_{n-1} with $0 \leq i \leq n-1$ we have

$$\mathrm{rank}_{\mathbb{Z}_p}(M^{N_i}) = \mathrm{rank}_{\mathbb{Z}_p}(M'^{N_i}) = \mathrm{rank}_{\mathbb{Z}_p}(M'^{N_i'}) = \sum_{t=0}^{i} r_t\varphi(p^t)$$

and

$$\chi(N_i', M') = (n-1-i)\sum_{t=0}^{i} r_t\varphi(p^t) - p^i \sum_{t=i+1}^{n-1} r_t$$

since $\mathbb{Z}_p[\zeta_{p^n}]^{N_i} = 0$. We need to compute the difference $\chi(N_i, M') - \chi(N_i', M')$, which we do using the inflation-restriction sequence (Theorem 8.2). We get an exact sequence

$$0 \to H^1(N_i', M') \to H^1(N_i, M') \to H^1(N_{n-1}, M')^{N_i'} \to H^2(N_i', M') \to H^2(N_i, M').$$

Moreover, we can determine the cokernel of the last map. In fact, as in the proof of Proposition 4.11, we have

$$H^2(N_i', M') \cong \frac{M'^{N_i'}}{(1 + g^{p^i} + \cdots + g^{p^i(p^{n-1-i}-1)})M'}$$

and

$$H^2(N_i, M') \cong \frac{M'^{N_i}}{(1 + g^{p^i} + \cdots + g^{p^i(p^{n-i}-1)})M'},$$

but

$$\begin{aligned}&(1 + g^{p^{n-1}} + \cdots + g^{p^{n-1}(p-1)})(1 + g^{p^i} + \cdots + g^{p^i(p^{n-1-i}-1)})\\ &= 1 + g^{p^i} + \cdots + g^{p^i(p^{n-i}-1)},\end{aligned}$$

so the last map in the sequence is multiplication by $1 + g^{p^{n-1}} + \cdots + g^{p^{n-1}(p-1)}$; thus its cokernel is

$$\frac{M'^{N_i}}{(1 + g^{p^{n-1}} + \cdots + g^{p^{n-1}(p-1)})M'^{N_i'}} = \frac{M'^{N_i}}{pM'^{N_i}}.$$

Therefore applying $\mathrm{ord}_p|-|$ to the exact sequence gives

$$\chi(N_i, M') - \chi(N_i', M') = \mathrm{ord}_p|M'^{N_i}/pM'^{N_i}| = \mathrm{rank}_{\mathbb{Z}_p}(M'^{N_i}) = \sum_{t=0}^{i} r_t\varphi(p^t)$$

since $H^1(N_{n-1}, M') = 0$. Hence

$$\begin{aligned}\chi(N_i, M) &= \chi(N_i, M') + r_n\chi(N_i, \mathbb{Z}_p[\zeta_{p^n}]) \\ &= \chi(N_i', M') + \sum_{t=0}^{i} r_t\varphi(p^t) + r_n\chi(N_i, \mathbb{Z}_p[\zeta_{p^n}]) \\ &= (n-i)\sum_{t=0}^{i} r_t\varphi(p^t) - p^i \sum_{t=i+1}^{n-1} r_t + r_n\chi(N_i, \mathbb{Z}_p[\zeta_{p^n}]),\end{aligned}$$

but $H^2(N_i, \mathbb{Z}_p[\zeta_{p^n}]) = 0$ and

$$H^1(N_i, \mathbb{Z}_p[\zeta_{p^n}]) = \frac{\mathbb{Z}_p[\zeta_{p^n}]}{(\zeta_{p^n}^{p^i} - 1)} \cong \frac{\mathbb{Z}_p[x]}{(x^{p^i} - 1) + (\Phi_{p^n}(x))} \cong \frac{\mathbb{Z}_p[\mathbb{Z}/(p^i)]}{(\Phi_{p^n}(1))} = \frac{\mathbb{Z}_p[\mathbb{Z}/(p^i)]}{(p)},$$

so $\chi(N_i, \mathbb{Z}_p[\zeta_{p^n}]) = -p^i$ as needed. Also, it's clear that $\chi(N_n, M) = 0$ and

$$\begin{aligned}\mathrm{rank}_{\mathbb{Z}_p}(M^{N_n}) &= \mathrm{rank}_{\mathbb{Z}_p}(M) \\ &= \mathrm{rank}_{\mathbb{Z}_p}(M') + r_n\mathrm{rank}_{\mathbb{Z}_p}(\mathbb{Z}[\zeta_{p^n}]) \\ &= \sum_{t=0}^{n-1} r_t\varphi(p^t) + r_n\varphi(p^n),\end{aligned}$$

which finishes the proof of the proposition. □

Now we use Proposition 8.3 to prove generalizations of Propositions 7.2 and Corollary 7.3. The idea is to regard the r_i's as $n+1$ place-holders and to find rational dependence among $n+2$ vectors. In other words, we'll use some linear algebra. First, we relate $n+1$ lambda invariants (corresponding to $\mathbb{Z}_p$-ranks of $(A_{K_n}^*)^{N_i}$) to $\chi(G_n, A_{K_n})$. The formula we'll get is a generalization of the formula from the second equality in Corollary 7.3.

Theorem 8.4. *Let p be prime and $K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n$ be a tower of $\mathbb{Z}_p$-fields such that for all i the extension K_i/K_0 is cyclic of degree p^i. Suppose $\mu_{K_0} = 0$. Then $\mu_{K_1} = \cdots = \mu_{K_n} = 0$ and*

$$\sum_{i=0}^{n-1} \varphi(p^i)\lambda_{K_{n-i}} = p^{n-1}(1 + n(p-1))\lambda_{K_0} + \varphi(p^n)\chi(G_n, A_{K_n})$$

where $G_n = \mathrm{Gal}(K_n/K_0)$.

Proof. We apply Proposition 8.3 to the $\mathbb{Z}_pG_n$-module $A^*_{K_n}$, which is free of finite rank λ_{K_n} over $\mathbb{Z}_p$. Thus there is a sequence $r_0, r_1, \ldots, r_n \in \mathbb{N}_0$ such that for all $i = 0, 1, \ldots, n$ we have

$$\lambda_{K_i} = \mathrm{rank}_{\mathbb{Z}_p}(A^*_{K_i}) = \mathrm{rank}_{\mathbb{Z}_p}((A^*_{K_n})^{N_i}) = \sum_{t=0}^{i} r_t\varphi(p^t)$$

$$\chi(G_n, A_{K_n}) = -\chi(N_0, A^*_{K_n}) = -nr_0 + \sum_{t=1}^{n} r_t$$

where $N_i = \mathrm{Gal}(K_n/K_i)$. Hence

$$\begin{aligned}
\sum_{i=0}^{n-1} \varphi(p^i)\lambda_{K_{n-i}} &= \sum_{i=0}^{n-1}\sum_{t=0}^{n-i} r_t\varphi(p^i)\varphi(p^t) \\
&= \sum_{i=0}^{n-1} \varphi(p^i)r_0 + \sum_{t=1}^{n}\sum_{i=0}^{n-t} \varphi(p^i)\varphi(p^t)r_t \\
&= \left(1 + (p-1)\sum_{j=0}^{n-2} p^j\right) r_0 + \sum_{t=1}^{n} r_t\varphi(p^t)\left(1 + (p-1)\sum_{j=0}^{n-t-1} p^j\right) \\
&= p^{n-1}r_0 + \varphi(p^n)(r_1 + \cdots + r_n) \\
&= p^{n-1}(1 + n(p-1))r_0 + \varphi(p^n)(-nr_0 + r_1 + \cdots r_n) \\
&= p^{n-1}(1 + n(p-1))\lambda_{K_0} + \varphi(p^n)\chi(G_n, A_{K_n})
\end{aligned}$$

which finishes the proof. □

Corollary 8.5. *Under the same assumptions as Theorem 8.4, we have*

$$\lambda_{K_n} = p^n\lambda_{K_0} + \varphi(p^n)\chi(G_n, A_{K_n}) - (p-1)\sum_{i=1}^{n-1} \varphi(p^i)\chi(G_i, A_{K_i})$$

where $G_i = \mathrm{Gal}(K_i/K_0)$.

Proof. We'll use strong induction on n. First, it's clear that the statement holds when $n = 0$. (It's also clear in the case $n = 1$ since then the statement is just Theorem 6.2.) Now take $n \geq 1$. Suppose the statement holds for all cyclic p-extensions of degree $\leq p^{n-1}$. Then by Theorem 8.4 we get

$$\begin{aligned}
\lambda_{K_n} &= p^{n-1}(1+n(p-1))\lambda_{K_0} + \varphi(p^n)\chi(G_n, A_{K_n}) - \sum_{i=1}^{n-1} \varphi(p^i)\lambda_{K_{n-i}} \\
&\overset{\text{induc.}}{=} p^{n-1}(1+n(p-1))\lambda_{K_0} + \varphi(p^n)\chi(G_n, A_{K_n}) \\
&- \sum_{i=1}^{n-1} \varphi(p^i) \left(p^{n-i}\lambda_{K_0} + \varphi(p^{n-i})\chi(G_{n-i}, A_{K_{n-i}}) - (p-1) \sum_{j=1}^{n-i-1} \varphi(p^j)\chi(G_j, A_{K_j}) \right) \\
&= p^{n-1}(1+n(p-1))\lambda_{K_0} + \varphi(p^n)\chi(G_n, A_{K_n}) - p^{n-1}(p-1)(n-1)\lambda_{K_0} \\
&- (p-1) \sum_{i=1}^{n-1} \varphi(p^{n-1})\chi(G_{n-i}, A_{K_{n-i}}) + (p-1) \sum_{i=1}^{n-1} \sum_{j=1}^{n-i-1} \varphi(p^i)\varphi(p^j)\chi(G_j, A_{K_j}) \\
&= p^n\lambda_{K_0} + \varphi(p^n)\chi(G_n, A_{K_n}) - (p-1)\varphi(p^{n-1})\chi(G_{n-1}, A_{K_{n-1}}) \\
&- (p-1) \sum_{j=1}^{n-2} \varphi(p^{n-1})\chi(G_j, A_{K_j}) + (p-1) \sum_{j=1}^{n-2} \varphi(p^j) \left(\sum_{i=1}^{n-j-1} \varphi(p^i) \right) \chi(G_j, A_{K_j}) \\
&= p^n\lambda_{K_0} + \varphi(p^n)\chi(G_n, A_{K_n}) - (p-1)\varphi(p^{n-1})\chi(G_{n-1}, A_{K_{n-1}}) \\
&- (p-1) \sum_{j=1}^{n-2} \varphi(p^j)p^{n-j-1}\chi(G_j, A_{K_j}) + (p-1) \sum_{j=1}^{n-2} \varphi(p^j)(p^{n-j-1}-1)\chi(G_j, A_{K_j}) \\
&= p^n\lambda_{K_0} + \varphi(p^n)\chi(G_n, A_{K_n}) - (p-1)\varphi(p^{n-1})\chi(G_{n-1}, A_{K_{n-1}}) \\
&- (p-1) \sum_{j=1}^{n-2} \varphi(p^j)\chi(G_j, A_{K_j}) \\
&= p^n\lambda_{K_0} + \varphi(p^n)\chi(G_n, A_{K_n}) - (p-1) \sum_{j=1}^{n-1} \varphi(p^j)\chi(G_j, A_{K_j})
\end{aligned}$$

as needed. □

Now we combine this corollary with Remark 6.5 to get the following generalization of Proposition 7.2.

Corollary 8.6. *Under the same assumptions as Theorem 8.4, we have*

$$p^{n-1}\chi(G_n, A_{K_n}) = \sum_{i=1}^{n-1} \varphi(p^i)\chi(G_i, A_{K_i}) + \sum_{i=1}^{n} p^{n-i}\chi(N_{i-1}/N_i, A_{K_i}).$$

where $N_i = \mathrm{Gal}(K_n/K_i)$ *and again* $G_i = \mathrm{Gal}(K_i/K_0)$.

Proof. We have

$$\begin{aligned} p^{n-1}\chi(G_n, A_{K_n}) &= \sum_{i=1}^{n-1} \varphi(p^i)\chi(G_i, A_{K_i}) + \frac{\lambda_{K_n} - p^n\lambda_{K_0}}{p-1} \\ &= \sum_{i=1}^{n-1} \varphi(p^i)\chi(G_i, A_{K_i}) + \sum_{i=1}^{n} p^{n-i}\chi(N_{i-1}/N_i, A_{K_i}) \end{aligned}$$

where the first equality follows from Corollary 8.5 and the second equality follows from Remark 6.5. □

Corollary 8.7. *Let* $L/K = K_n/K_0$ *be as in Theorem 8.4. Suppose* $\mu_K = 0$. *Then*

1. $\lambda_L \equiv \lambda_{K_i} \pmod{\varphi(p^{i+1})}$ *for every* $i = 0, \ldots, n$
2. *(a)* $\lambda_L \equiv -p^{n-1}\chi(G, A_L) - (p-1)\sum_{i=1}^{n-1} \varphi(p^i)\chi(G_i, A_{K_i}) \pmod{p^n}$

   (b) $p \nmid n-1 \Rightarrow \lambda_L \equiv \sum_{i=1}^{n-1} \frac{p^i(p-1)^2}{[(i+1)p-i][ip-i+1]}\chi(N_{n-i}, A_L) \pmod{p^n}$
3. $\mathrm{ord}_p|H^2(G, P_L)| \leq n\lambda_K + \mathrm{ord}_p|H^1(G, P_L)| + \chi(G, I_L)$

where $G_i = \mathrm{Gal}(K_i/K)$, $N_i = \mathrm{Gal}(L/K_i)$, *and* $G = G_n = N_0$.

Proof. For part 1, we only need to prove that for all $i = 1, \ldots, n$

$$\lambda_{K_i} \equiv \lambda_{K_{i-1}} \pmod{\varphi(p^i)}, \tag{8.7.1}$$

which we'll do by strong induction on n. We've already proven the base case $n = 1$ in Corollary 6.6 (and the case $n = 2$ in Corollary 7.4). Suppose then that Equation 8.7.1 holds for all $i < n$. Then for all $i = 1, \ldots, n-1$

$$p^{n-i}(\lambda_{K_i} - \lambda_{K_{i-1}}) \equiv 0 \pmod{\varphi(p^n)},$$

so

$$\begin{aligned}\lambda_{K_n} - \lambda_{K_{n-1}} &\equiv \lambda_{K_n} - \lambda_{K_{n-1}} + \sum_{i=1}^{n-1} p^{n-i}(\lambda_{K_i} - \lambda_{K_{i-1}}) \\ &= \sum_{i=0}^{n-1} \varphi(p^i)\lambda_{K_{n-i}} - p^{n-1}\lambda_{K_0} \\ &= p^{n-1}(1 + n(p-1))\lambda_{K_0} + \varphi(p^n)\chi(G_n, A_{K_n}) - p^{n-1}\lambda_{K_0} \\ &= \varphi(p^n)\lambda_{K_0} + \varphi(p^n)\chi(G_n, A_{K_n}) \equiv 0 \pmod{\varphi(p^n)}.\end{aligned}$$

For part 2, the first statement (a) follows immediately from Theorem 8.4 while the second statement (b) follows immediately from Theorem 8.8 below. To prove part 3, we note that

$$\begin{aligned}0 \leq \sum_{i=0}^{n-1} \frac{\lambda_{K_{n-i}} - \lambda_{K_{n-i-1}}}{\varphi(p^{n-i})} &= \frac{1}{\varphi(p^n)} \sum_{i=0}^{n-1} p^i(\lambda_{K_{n-i}} - \lambda_{K_{n-i-1}}) \\ &= \frac{1}{\varphi(p^n)} \left(\sum_{i=0}^{n-1} p^i \lambda_{K_{n-i}} - \sum_{i=1}^{n} p^{i-1} \lambda_{K_{n-i}} \right) \\ &= \frac{1}{\varphi(p^n)} \left(\lambda_{K_n} + \sum_{i=1}^{n-1} (p^i - p^{i-1})\lambda_{K_{n-i}} - p^{n-1}\lambda_{K_0} \right) \\ &= \frac{1}{\varphi(p^n)} \left(\sum_{i=0}^{n-1} \varphi(p^i)\lambda_{K_{n-i}} - p^{n-1}\lambda_{K_0} \right) \\ &= \frac{1}{\varphi(p^n)} \left(p^{n-1}(1 + n(p-1))\lambda_{K_0} + \varphi(p^n)\chi(G_n, A_{K_n}) - p^{n-1}\lambda_{K_0} \right) \\ &= n\lambda_{K_0} - \chi(G_n, P_{K_n}) + \chi(G_n, I_{K_n}) \\ &= n\lambda_K - \mathrm{ord}_p|H^2(G, P_L)| + \mathrm{ord}_p|H^1(G, P_L)| + \chi(G, I_L),\end{aligned}$$

which finishes the proof. □

Now we relate the n Euler characteristics associated to subgroups (instead of quotients or subquotients)

$$\chi(N_0, A_{K_n}), \chi(N_1, A_{K_n}), \ldots, \text{ and } \chi(N_{n-1}, A_{K_n})$$

to the 2 lambda invariants λ_{K_n} and λ_{K_0}. The result is of different nature since it involves non-integer coefficients.

Theorem 8.8. *Let p be prime and $K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n$ be a tower of $\mathbb{Z}_p$-fields such that for all i the extension K_i/K_0 is cyclic of degree p^i. Suppose $\mu_{K_0} = 0$ and K_n/K_0. Then $\mu_{K_1} = \cdots = \mu_{K_n} = 0$ and*

$$\frac{\lambda_{K_n} - p^n\lambda_{K_0}}{p-1} = \frac{p^n}{np-n+1}\chi(N_0, A_{K_n}) + \sum_{i=1}^{n-1} \frac{p^i(p-1)}{[(i+1)p-i][ip-i+1]}\chi(N_{n-i}, A_{K_n})$$

where $N_i = \mathrm{Gal}(K_n/K_i)$.

The following lemma will make the proof of the above theorem much easier.

Lemma 8.9. *For all $n \in \mathbb{N}$ we have*

$$\sum_{i=1}^{n-1} \frac{p^i(p-1)i}{[(i+1)p-i][ip-i+1]} = \frac{p^{n-1}+p^{n-2}+\cdots+1-n}{np-n+1}$$

and

$$\sum_{i=1}^{n-1} \frac{1}{[(i+1)p-i][ip-i+1]} = \frac{n-1}{p(np-n+1)}.$$

Proof. We use induction on n. If $n = 1$, then both right hand sides are zero and both left hand sides are empty sums, so the lemma is clear in this case. Now suppose $n \geq 2$ and the statement is true for $n-1$. Then

$$\begin{aligned}
&\sum_{i=1}^{n-1} \frac{p^i(p-1)i}{[(i+1)p-i][ip-i+1]} \\
&= \frac{p^{n-1}(p-1)(n-1)}{(np-n+1)((n-1)p-n+2)} + \sum_{i=1}^{n-2} \frac{p^i(p-1)i}{[(i+1)p-i][ip-i+1]} \\
&= \frac{p^{n-1}(p-1)(n-1)}{(np-n+1)((n-1)p-n+2)} + \frac{p^{n-2}+p^{n-3}+\cdots+1-(n-1)}{(n-1)p-n+2} \\
&= \frac{p^{n-1}(p-1)(n-1) + \left(\frac{p^{n-1}-1}{p-1} - (n-1)\right)(np-n+1)}{(np-n+1)((n-1)p-n+2)} \\
&= \frac{p^{n-1}(p-1)(n-1) + \left(\frac{p^{n-1}-1}{p-1} - (n-1)\right)(p-1)}{(np-n+1)((n-1)p-n+2)} + \frac{\frac{p^{n-1}-1}{p-1} - (n-1)}{np-n+1} \\
&= \frac{(p^{n-1}-1)(p-1)(n-1) + p^{n-1} - 1}{(np-n+1)((n-1)p-n+2)} + \frac{\frac{p^{n-1}-1}{p-1} - (n-1)}{np-n+1}
\end{aligned}$$

$$= \frac{p^{n-1}-1}{np-n+1} + \frac{p^{n-2}+p^{n-3}+\cdots+1-(n-1)}{np-n+1}$$
$$= \frac{p^{n-1}+p^{n-2}+\cdots+1-n}{np-n+1}$$

and

$$\sum_{i=1}^{n-1} \frac{1}{[(i+1)p-i][ip-i+1]}$$
$$= \frac{1}{(np-n+1)((n-1)p-n+2)} + \sum_{i=1}^{n-2} \frac{1}{[(i+1)p-i][ip-i+1]}$$
$$= \frac{1}{(np-n+1)((n-1)p-n+2)} + \frac{n-2}{p((n-1)p-n+2)}$$
$$= \frac{p+(n-2)(np-n+1)}{p(np-n+1)((n-1)p-n+2)}$$
$$= \frac{p+(n-2)(p-1)+(n-2)((n-1)p-n+2)}{p(np-n+1)((n-1)p-n+2)}$$
$$= \frac{(n-1)p-n+2+(n-2)((n-1)p-n+2)}{p(np-n+1)((n-1)p-n+2)} = \frac{n-1}{p(np-n+1)}$$

as claimed. □

Proof of Theorem 8.8. We may assume $n \geq 1$ since the statement is obvious in the case where $n = 0$ since then both sides of the equation are zero. Proposition 8.3 implies that there are $r_0, \ldots, r_n \in \mathbb{N}_0$ such that

$$\lambda_{K_0} = \operatorname{rank}_{\mathbb{Z}_p}((A^*_{K_n})^{N_0}) = r_0,$$
$$\lambda_{K_n} = \operatorname{rank}_{\mathbb{Z}_p}(A^*_{K_n}) = \sum_{t=0}^{n} r_t \varphi(p^t)$$

and

$$\chi(N_i, A_{K_n}) = -\chi(N_i, A^*_{K_n}) = -(n-i)\sum_{t=0}^{i} r_t\varphi(p^t) + p^i \sum_{t=i+1}^{n} r_t$$

for all $i \in \{0, \ldots, n\}$. On the one hand,

$$\frac{\lambda_{K_n} - p^n\lambda_{K_0}}{p-1} = \frac{\sum_{t=0}^{n} r_t\varphi(p^t) - p^n r_0}{p-1} = -(p^{n-1}+p^{n-2}+\cdots+1)r_0 + \sum_{t=1} r_t p^{t-1}.$$

On the other hand, the coefficient of r_0 occurring on the right hand side of the statement is

$$\begin{aligned}
&\frac{p^n}{np-n+1}(-n)+\sum_{i=1}^{n-1}\frac{p^i(p-1)(-i)}{[(i+1)p-i][ip-i+1]}\\
&=\frac{-np^n}{np-n+1}-\frac{p^{n-1}+p^{n-2}+\cdots+1-n}{np-n+1}\\
&=\frac{-np^n+n-\frac{p^n-1}{p-1}}{np-n+1}\\
&=\frac{-n(p-1)\frac{p^n-1}{p-1}-\frac{p^n-1}{p-1}}{np-n+1}\\
&=-\frac{p^n-1}{p-1}\\
&=-(p^{n-1}+p^{n-2}+\cdots+1)
\end{aligned}$$

and the coefficient of r_t for $t\geq 1$ is

$$\begin{aligned}
&\frac{p^n}{np-n+1}+\varphi(p^t)\sum_{i=1}^{n-t}\frac{p^i(p-1)(i)}{[(i+1)p-i][ip-i+1]}+\\
&p^n(p-1)\sum_{i=n-t+1}^{n-1}\frac{1}{[(i+1)p-i][ip-i+1]}\\
&=\frac{p^n}{np-n+1}-p^{t-1}(p-1)\frac{\frac{p^{n-t+1}-1}{p-1}-(n-t+1)}{(n-t+1)p-(n-t+1)+1}+\\
&p^n(p-1)\left(\frac{n-1}{p(np-n+1)}-\frac{n-t}{p((n-t+1)p-(n-t+1)+1)}\right)\\
&=\frac{p^n+p^{n-1}(p-1)(n-1)}{np-n+1}-\\
&\frac{p^t(p^{n-t+1}-1-(p-1)(n-t+1))+p^n(p-1)(n-t)}{p((n-t+1)p-n+t)}\\
&=p^{n-1}-\frac{p^{n+1}-p^t((n-t+1)p-n+t)+(n-t)p^n(p-1)}{p((n-t+1)p-n+t)}\\
&=p^{n-1}+p^{t-1}-\frac{p^{n+1}+(n-t)p^n(p-1)}{p((n-t+1)p-n+t)}\\
&=p^{n-1}+p^{t-1}-p^n\frac{p+(n-t)(p-1)}{p((n-t+1)p-n+t)}\\
&=p^{n-1}+p^{t-1}-p^{n-1}=p^{t-1},
\end{aligned}$$

which completes the proof. □

8.2 Λ-Modules

In the late summer of 2009, I sent an email to Ralph Greenberg, Professor of mathematics at the University of Washington, asking if anyone had used the structure theorem (Theorem 7.1) of $\mathbb{Z}_pG$-modules which are free of finite rank over $\mathbb{Z}_p$ with $G \cong \mathbb{Z}/(p^2)$ to derive a formula in the spirit of Iwasawa's as found in Theorem 6.2. He responded by saying that he wasn't aware of anyone doing this, but he further suggested that I consider all $\mathbb{Z}_pG$-modules with $G \cong \mathbb{Z}/(p^n)$ as $\Lambda = \mathbb{Z}_p[[T]]$-modules. In this way, I can use the following structure theorem for finitely generated Λ-modules, which is the very result one can use to prove Iwasawa's growth formula (Theorem 3.2.

Theorem 8.10. *Let M be a finitely generated Λ-module. Then there is a Λ-module homomorphism*

$$\theta\colon M \to \Lambda^r \oplus \bigoplus_{i=1}^{s} \frac{\Lambda}{(f_i(T)^{m_i})} \oplus \bigoplus_{j=1}^{t} \frac{\Lambda}{(p^{n_j})}$$

such that $\ker(\theta), \operatorname{coker}(\theta)$ *are finite and where each $f_i(T) \in \mathbb{Z}_p[T]$ is irreducible with $f_i(T) \equiv$ power of $T \pmod{p}$.*

We'll now use this theorem to prove the following proposition from which Proposition 8.3 follows as an easy corollary.

Proposition 8.11. *Let $G = \langle g \rangle \cong \mathbb{Z}/(p^n)$ for some prime p and some $n \in \mathbb{N}_0$. Suppose M is a $\mathbb{Z}_pG$-module which is free of finite rank over $\mathbb{Z}_p$. There is an injective $\mathbb{Z}_pG$-module homomorphism with finite cokernel*

$$M \rightarrowtail \bigoplus_{i=0}^{n} \mathbb{Z}_p[\zeta_{p^i}]^{\oplus r_i}$$

for some $r_0, \ldots, r_n \in \mathbb{N}_0$ where each $\mathbb{Z}_p[\zeta_{p^i}]$ has $\mathbb{Z}_pG$-module structure given by

$$\mathbb{Z}_p[\zeta_{p^i}] \cong \frac{\mathbb{Z}_pG}{\Phi_{p^i}(g)\mathbb{Z}_pG}.$$

Proof. We know

$$\Lambda \cong \varprojlim_{m\in\mathbb{N}} \mathbb{Z}_p[\mathbb{Z}/(p^m)]\colon T \mapsto (g_m - 1)_{m\in\mathbb{N}}$$

with $\mathbb{Z}/(p^m) = \langle g_m\rangle$ written multiplicatively, so $\mathbb{Z}_pG$ is a quotient ring of Λ. In this way, every $\mathbb{Z}_pG$-module is a Λ-module with T acting as $g-1$, so Theorem 8.10 implies there is a Λ-module homomorphism

$$\theta\colon M \to \mathbb{Z}_p[[T]]^r \oplus \bigoplus_{i=1}^{s} \frac{\mathbb{Z}_p[[T]]}{(f_i(T)^{m_i})} \oplus \bigoplus_{j=1}^{t} \frac{\mathbb{Z}_p[[T]]}{(p^{n_j})}$$

such that $\ker(\theta), \operatorname{coker}(\theta)$ are finite and where each $f_i(T) \in \mathbb{Z}_p[T]$ is irreducible with $f_i(T) \equiv$ power of $T \pmod p$. Immediately, we see that $\ker(\theta) = 0$ since M is a free over $\mathbb{Z}_p$. If we tensor with $\mathbb{Q}_p$, we get an isomorphism

$$M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong \mathbb{Q}_p[[T]]^{\oplus r} \oplus \bigoplus_{i=1}^{s} \frac{\mathbb{Q}_p[T]}{(f_i(T)^{m_i})}$$

of $\mathbb{Q}_p[T]$-modules, but $\dim_{\mathbb{Q}_p}(M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p) = \operatorname{rank}_{\mathbb{Z}_p}(M) < \infty$ while $\dim_{\mathbb{Q}_p}(\mathbb{Q}_p[[T]]) = \infty$, so $r = 0$. Now $x^{p^n} - 1$ kills the left hand side where $x := T + 1$, so $x^{p^n} - 1$ kills each

$$\frac{\mathbb{Q}_p[x]}{(h_i(x)_i^m)}$$

where $h_i(x) = f_i(x-1)$ is monic and irreducible. Hence each $h_i(x)^{m_i}$ divides $x^{p^n} - 1$ in $\mathbb{Q}_p[x]$, but $x^{p^n} - 1$ is the squarefree product of the (monic, irreducible) p^j-cyclotomic polynomials $\Phi_{p^j}(x)$ for $0 \le j \le n$, so every m_i is 1 and every $h_i(x)$ is $\Phi_{p^j}(x)$ for some $0 \le j \le n$. Hence our isomorphism becomes

$$M \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong \bigoplus_{i=1}^{s} \frac{\mathbb{Q}_p[x]}{(h_i(x))} = \bigoplus_{j=0}^{n} \left(\frac{\mathbb{Q}_p[x]}{(\Phi_{p^j}(x))}\right)^{\oplus r_j} \cong \bigoplus_{j=0}^{n} \left(\frac{\mathbb{Q}_pG}{\Phi_{p^j}(g)\mathbb{Q}_pG}\right)^{\oplus r_j}$$

as $\mathbb{Q}_pG$-modules for some $r_0, \ldots, r_n \in \mathbb{N}_0$. We'll use this isomorphism in the next section to analyze $\mathbb{Q}_p$-representations. In the meantime, we have

$$\theta\colon M \rightarrowtail \bigoplus_{j=0}^{n} \left(\frac{\mathbb{Z}_p[[x]]}{(\Phi_{p^j}(x))}\right)^{\oplus r_j} \oplus \bigoplus_{j=1}^{t} \frac{\mathbb{Z}_p[[x]]}{(p^{n_j})},$$

but we know $\mathrm{im}(\theta)$ has trivial intersection with each $\mathbb{Z}_p[[x]]/(p^{n_j})$ factor since $p^{n_j} \nmid x^{p^n} - 1$, so there can be no such factors since $\mathrm{coker}(\theta)$ is finite while $\mathbb{Z}_p[[x]]/(p^m)$ is infinite when $m \in \mathbb{N}$. Also, since each $f_i(T) \equiv$ power of $T \pmod p$, we may apply a division algorithm (see Proposition 7.2 in [Was96]) to conclude

$$\frac{\mathbb{Z}_p[[x]]}{(h_i(x))} = \frac{\mathbb{Z}_p[[T]]}{(f_i(T))} \cong \frac{\mathbb{Z}_p[T]}{(f_i(T))} = \frac{\mathbb{Z}_p[x]}{(h_i(x))}$$

as $\mathbb{Z}_p[x]$-modules where again $x = T + 1$. Therefore

$$\theta \colon M \rightarrowtail \bigoplus_{j=0}^{n} \left(\frac{\mathbb{Z}_p[x]}{(\Phi_{p^j}(x))} \right)^{\oplus r_j} \cong \bigoplus_{j=0}^{n} \left(\frac{\mathbb{Z}_p G}{\Phi_{p^j}(g)\mathbb{Z}_p G} \right)^{\oplus r_j}$$

is a $\mathbb{Z}_p G$-module homomorphism with finite cokernel. □

Remark 8.12. Let $M, G = \langle g \rangle \cong \mathbb{Z}/(p^n)$ be as in Proposition 8.11. As mentioned above, the proposition can be used to give another proof of Proposition 8.3. To see this, we observe that if C is a finite $\mathbb{Z}_p G$-module, then $\chi(N_i, C) = 0$ and $\mathrm{rank}_{\mathbb{Z}_p}(C^{N_i}) = 0$ for all $i \in \{0, \ldots, n\}$ where (as in 8.3) $N_i = \langle g^{p^i} \rangle$. Thus since χ and $\mathrm{rank}_{\mathbb{Z}_p}$ are additive on short exact sequences, we see that it suffices to do the following computations:

$$\begin{aligned}
\mathbb{Z}_p[\zeta_{p^j}]^{N_i} &= \begin{cases} \mathbb{Z}_p[\zeta_{p^j}] & \text{if } j \leq i \\ 0 & \text{if } j > i \end{cases} \\
\chi(N_i, \mathbb{Z}_p[\zeta_{p^j}]) &= \mathrm{ord}_p \left(\frac{|H^2(N_i, \mathbb{Z}_p[\zeta_{p^j}])|}{|H^1(N_i, \mathbb{Z}_p[\zeta_{p^j}])|} \right) \\
&= \begin{cases} \mathrm{ord}_p \left| \frac{\mathbb{Z}_p[\zeta_{p^j}]}{p^{n-i}\mathbb{Z}_p[\zeta_{p^j}]} \right| = (n-i)\varphi(p^j) & \text{if } j \leq i \\ \mathrm{ord}_p \left| \frac{|\mathbb{Z}_p[\zeta_{p^j}]}{(1-\zeta_{p^j}^{p^i})\mathbb{Z}_p[\zeta_{p^j}]} \right|^{-1} = -p^i & \text{if } j > i. \end{cases}
\end{aligned}$$

8.3 $\mathbb{Q}_p$-Representations

Again evoking the ideas of Section 6.2, the proofs of Proposition 8.11 and Theorem 8.4 actually show more than just formulas for Euler characteristics and lambda invariants. They show a statement about representations. Let $K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n = L$

be a tower of $\mathbb{Z}_p$ fields with $G_i = \mathrm{Gal}(K_i/K)$ and $N_i = \mathrm{Gal}(L/K_i) = \langle g^{p^i} \rangle \cong \mathbb{Z}/(p^i)$ for all $i \in \{0, \ldots, n\}$. Assume $\mu_K = 0$ and define

$$V_L := A_L^* \otimes_{\mathbb{Z}_p} \mathbb{Q}_p.$$

Consider the corresponding representation

$$\pi_{L/K} \colon G \to \mathrm{GL}(V_L).$$

There is the following result about the decomposition of $\pi_{L/K}$.

Corollary 8.13. *Let $K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n = L$ be as above with $\mu_K = 0$. Then we have an isomorphism of $\mathbb{Q}_p$-representations*

$$\pi_{L/K} \cong \lambda_K \pi_G \oplus \bigoplus_{i=1}^{n} \left(\chi(G_i, A_{K_i}) - \chi(G_{i-1}, A_{K_{i-1}}) \right) \pi_{\varphi(p^i)}$$

where π_G is the regular representation and π_d is the unique faithful irreducible representation of degree $d \in \{\varphi(p), \varphi(p^2), \ldots, \varphi(p^n)\}$.

Proof. We'll use all the notation in the proof of Proposition 8.11. In the proof of 8.11 with $A_L^* = M$, we had $r_0, r_1, \ldots, r_n \in \mathbb{N}_0$ such that

$$V_L \cong \bigoplus_{j=0}^{n} \left(\frac{\mathbb{Q}_p[x]}{(\Phi_{p^j}(x))} \right)^{\oplus r_j}$$

as $\mathbb{Q}_p G$-modules where our generator g of G acts as x on $\mathbb{Q}_p[x]$. Remark 8.12 shows that these $r_0, \ldots, r_n$ are the same as those found in the proof of Theorem 8.4. In particular, this means $r_0 = \lambda_K$, so

$$V_L \cong (\mathbb{Q}_p G)^{\oplus \lambda_K} \oplus \bigoplus_{j=1}^{n} \left(\frac{\mathbb{Q}_p[x]}{(\Phi_{p^j}(x))} \right)^{\oplus r_j - r_0}$$

where (as always) we interpret negative exponents as a difference of representations.

It remains only to determine $r_1 - r_0, r_2 - r_0, \ldots, r_n - r_0$. To do this, we first compute

$$\begin{aligned}\chi(G_i, A_{K_i}) &= -\chi(G_i, A_{K_i}^*) = -\chi(G/N_i, (A_K^*)^{N_i}) = -\sum_{j=0}^{n} r_j \chi(G/N_i, \mathbb{Z}_p[\zeta_{p^j}]^{N_i}) \\ &= -\sum_{j=0}^{i} r_j \chi(G/N_i, \mathbb{Z}_p[\zeta_{p^j}]) = -r_0\chi(G/N_i, \mathbb{Z}_p) - \sum_{j=1}^{i} r_j \chi(G/N_i, \mathbb{Z}_p[\zeta_{p^j}]) \\ &= -ir_0 + r_1 + \cdots r_i.\end{aligned}$$

This shows

$$r_1 - r_0 = \chi(G_1, A_{K_1}) = \chi(G_1, A_{K_1}) - \chi(G_0, A_{K_0}),$$

$$r_2 - r_0 = r_1 + r_2 - 2r_0 - (r_1 - r_0) = \chi(G_2, A_{K_2}) - \chi(G_1, A_{K_1}),$$

and, in general,

$$\begin{aligned}r_i - r_0 &= r_1 + \cdots + r_i - ir_0 - (r_1 + \cdots + r_{i-1} - (i-1)r_0) \\ &= \chi(G_i, A_{K_i}) - \chi(G_{i-1}, A_{K_{i-1}})\end{aligned}$$

by induction. □

8.4 Vanishing Criteria for λ_L

In this section we'd like to give a couple of generalized vanishing criteria for λ_L of the kind found in Theorem 6.10 of Fukuda et al. in the case where L/K is a cyclic p-extension of $\mathbb{Z}_p$-fields. We'll need a couple of lemmas. The first lemma will lead to the first vanishing criterion.

Lemma 8.14. *Let L/K be a cyclic p-extension of $\mathbb{Z}_p$-fields with $G = \mathrm{Gal}(L/K)$. Suppose $\mu_K = \lambda_K = 0$. Then*

$$\mathrm{ord}_p|H^1(G, \mathcal{O}_L^\times)| + \mathrm{ord}_p|(I_L^G P_L)/(I_K P_L)| = \chi(G, I_L)$$

Proof. There's a short exact sequence of $\mathbb{Z}_pG$-modules

$$(I_K P_L^G)/I_K \rightarrowtail I_L^G/I_K \twoheadrightarrow I_L^G/(I_K P_L^G).$$

Also, $I_K \cap P_L^G = P_K$ since $P_L^G/P_K \cong H^1(G, \mathcal{O}_L^\times)$ being a p-group implies

$$(I_K \cap P_L^G)/P_K \subseteq P_L^G/P_K \subseteq A_K \cong 0$$

by our $\mu_K = \lambda_K = 0$ assumption. Thus using the third isomorphism theorem twice gives

$$\frac{I_K P_L^G}{I_K} \cong \frac{P_L^G}{I_K \cap P_L^G} = \frac{P_L^G}{P_K} \cong H^1(G, \mathcal{O}_L^\times)$$

and

$$\frac{I_L^G}{I_K P_L^G} = \frac{I_L^G}{I_L^G \cap (I_K P_L)} \cong \frac{I_L^G P_L}{I_K P_L}.$$

This completes the proof since

$$\mathrm{ord}_p |I_L^G/I_K| = \chi(G, I_L)$$

by the proof of Lemma 5.1. □

Theorem 8.15. *Let L/K be a cyclic p-extension of $\mathbb{Z}_p$-fields which is unramified at every infinite place with $G = \mathrm{Gal}(L/K)$. Suppose $\mu_K = 0$. Then $\lambda_L = 0$ if and only if the following three conditions hold:*

(i) $\lambda_K = 0$

(ii) $\mathrm{ord}_p |H^2(G, \mathcal{O}_L^\times)| = 0$

(iii) $\mathrm{ord}_p |(I_L^G P_L)/(I_K P_L)| = 0$

Proof. Condition (i) is obviously necessary for $\lambda_L = 0$, so we may assume that $\lambda_K = 0$. Consider the tower

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n = L$$

of $\mathbb{Z}_p$-fields where $G_i = \mathrm{Gal}(K_i/K) \cong \mathbb{Z}/(p^i)$ for all $i = 0, \ldots, n$. Then Lemma 8.14 and Lemma 5.1 imply

$$\begin{aligned}\chi(G_i, A_{K_i}) &= \mathrm{ord}_p|H^2(G_i, \mathcal{O}_{K_i}^\times)| - \mathrm{ord}_p|H^1(G_i, \mathcal{O}_{K_i}^\times)| + \chi(G, I_{K_i}) \\ &= \mathrm{ord}_p|H^2(G_i, \mathcal{O}_{K_i}^\times)| + \mathrm{ord}_p|(I_{K_i}^{G_i} P_{K_i})/(I_K P_{K_i})| \geq 0,\end{aligned}$$

for all $i = 1, \ldots, n$. Thus Corollary 8.5 shows that $\lambda_L = 0$ if and only if $\chi(G_i, A_{K_i}) = 0$ for all $i = 1, \ldots, n$, and the above computation proves that $\chi(G_i, A_{K_i}) = 0$ if and only if

$$\mathrm{ord}_p|H^2(G_i, \mathcal{O}_{K_i}^\times)| = \mathrm{ord}_p|(I_{K_i}^{G_i} P_{K_i})/(I_K P_{K_i})| = 0. \tag{8.15.1}$$

To complete the proof, it suffices to show that if Equation 8.15.1 holds for $i = n$, then it holds for all $i = 1, \ldots, n$. To show this it's enough to note that for all $i = 1, \ldots, n$ we have a surjection

$$\frac{\mathcal{O}_K^\times}{N_{L/K}(\mathcal{O}_L^\times)} \twoheadrightarrow \frac{\mathcal{O}_K^\times}{N_{K_i/K}(\mathcal{O}_{K_i}^\times)}$$

and an injection

$$\frac{I_{K_i}^{G_i} P_{K_i}}{I_K P_{K_i}} \rightarrowtail \frac{I_L^G P_L}{I_K P_L}$$

the second of which follows by observing that $(I_{K_i}^{G_i} P_{K_i}) \cap (I_K P_L) \subseteq I_{K_i} \cap (I_K P_L) \subseteq I_K P_{K_i}$. □

We'll need the following theorem to prove our next lemma.

Theorem 8.16. *Let ℓ/k be a Galois extension of number fields with $G = \mathrm{Gal}(\ell/k)$. Then there is an exact sequence of abelian groups*

$$0 \to \ker(J_{\ell/k}) \to H^1(G, \mathcal{O}_\ell^\times) \to \bigoplus_v \frac{\mathbb{Z}}{(e(w/v))} \to C_\ell^{[G]}/J_{\ell/k}(C_k) \to 0$$

where $C_\ell^{[G]}$ is the subgroup of C_ℓ^G generated by classes of G-fixed ideals, the direct sum ranges over all finite places v of k having ramification index $e(w/v)$ with w a place of ℓ lying over v, and

$$J_{\ell/k}\colon C_k \to C_\ell$$

is the natural map sending the class $[I]$ of an ideal I to the class $[\mathcal{O}_\ell I]$. Further, if G is cyclic and ℓ/k is unramified at every infinite place, then

$$\mathrm{q}(\mathcal{O}_\ell^\times) = \frac{|H^2(G,\mathcal{O}_\ell^\times)|}{|H^1(G,\mathcal{O}_\ell^\times)|} = \frac{1}{[\ell:k]}.$$

We will forego the proof of the first statement since we'll prove a very similar statement (with identical method of proof) for $\mathbb{Z}_p$-fields in Proposition 9.5. For a proof of the second statement, the reader is referred to Proposition 1.2.4 in [Gre10].

Lemma 8.17. *Let L/K be a cyclic p-extension of $\mathbb{Z}_p$-fields which is unramified at every infinite place. Suppose $K = k_\infty$ is the cyclotomic $\mathbb{Z}_p$-extension of a number field k such that $p \nmid h(k)$ and k has only one prime lying above p. Then*

$$\mathrm{ord}_p|H^2(G,\mathcal{O}_L^\times)| = 0.$$

where $G = \mathrm{Gal}(L/K)$.

Proof. Here we generalize the method of proof found in [FKOT97], where the result is proved in the case that L is totally real and $[L:K] = p$. First, note that if $\mathfrak{p}$ is the unique prime ideal of k lying over p, then $\mathfrak{p}_n/\mathfrak{p}$ is totally ramified in k_n/k and $p \nmid h(k_n)$ for all $n \in \mathbb{N}_0$. Thus using Theorem 8.16 on the extension k_n/k_m with $G_{n/m} = \mathrm{Gal}(k_n/k_m)$ we find that for all $m, n \in \mathbb{N}_0$ with $m \le n$

$$\begin{aligned}\left|\frac{\mathcal{O}_{k_m}^\times}{N_{k_n/k_m}(\mathcal{O}_{k_n}^\times)}\right| &= |H^2(G_{n/m},\mathcal{O}_{k_n}^\times)| = p^{-(n-m)}|H^1(G_{n/m},\mathcal{O}_{k_n}^\times)| \\ &= p^{-(n-m)}e(\mathfrak{p}_n/\mathfrak{p}_m)\frac{|\ker(J_{k_n/k_m})|}{|C_{k_n}^{[G_{n/m}]}/J_{k_n/k_m}(C_{k_m})|} \\ &= p^{-(n-m)}p^{n-m}\frac{|C_{k_m}|}{\left|C_{k_n}^{[G_{n/m}]}\right|} = 1\end{aligned}$$

where the last equality follows because $H^2(G_{n/m}, \mathcal{O}_{k_n}^\times)$ is a p-group and $\mathrm{ord}_p|C_{k_m}| = \mathrm{ord}_p|C_{k_n}^{[G_{n/m}]}| = 0$. Thus $N_{k_n/k_m}(\mathcal{O}_{k_n}^\times) = \mathcal{O}_{k_m}^\times$ for all $m, n \in \mathbb{N}_0$ with $m \leq n$, so if $L = \ell_\infty$ for some number field ℓ with $\mathrm{Gal}(\ell/k) \cong \mathrm{Gal}(L/K) \cong \mathbb{Z}/(p^d)$, then the induced maps

$$\widetilde{N}_{k_n/k_m} \colon \frac{\mathcal{O}_{k_n}^\times}{N_{\ell_n/k_n}(\mathcal{O}_{\ell_n}^\times)} \longrightarrow \frac{\mathcal{O}_{k_m}^\times}{N_{\ell_m/k_m}(\mathcal{O}_{\ell_m}^\times)}$$

are surjective for all $m, n \in \mathbb{N}_0$ with $m \leq n$. On the other hand, using Theorem 8.16 on the extension ℓ_n/k_n with $G_n = \mathrm{Gal}(\ell_n/k_n) \cong \mathrm{Gal}(L/K) \cong \mathbb{Z}/(p^d)$ we find

$$\begin{aligned}
\left|\frac{\mathcal{O}_{k_n}^\times}{N_{\ell_n/k_n}(\mathcal{O}_{\ell_n}^\times)}\right| &= |H^2(G_n, \mathcal{O}_{\ell_n}^\times)| = p^{-d}|H^1(G_n, \mathcal{O}_{\ell_n}^\times)| \\
&= p^{-d}\left(\prod_{i=1}^{s_n} e(w_i/v_i)\right)\frac{|C_{k_n}|}{\left|C_{\ell_n}^{[G_n]}\right|} \\
&= p^{-d}\left(\prod_{i=1}^{s_n} e(w_i/v_i)\right)\left|C_{\ell_n}^{[G_n]}\right|_p \\
&\leq p^{-d}p^{ds_\infty} = p^{d(s_\infty - 1)}
\end{aligned}$$

where s_n is the number of ramified primes of k_n in ℓ_n/k_n and $s_\infty < \infty$ is the number of ramified primes of K in L/K. Therefore the maps $\widetilde{N}_{k_n/k_m}$ are isomorphisms of finite abelian groups for sufficiently large m, n. Now consider the canonical maps

$$\widetilde{\rho}_{k_n/k_m} \colon \frac{\mathcal{O}_{k_m}^\times}{N_{\ell_m/k_m}(\mathcal{O}_{\ell_m}^\times)} \longrightarrow \frac{\mathcal{O}_{k_n}^\times}{N_{\ell_n/k_n}(\mathcal{O}_{\ell_n}^\times)}$$

for $m \leq n$. These maps have the property that $\widetilde{N}_{k_n/k_m} \circ \widetilde{\rho}_{k_n/k_m}$ is the exponentiation by p^{n-m} map when the groups are written multiplicatively. Thus when $n - m \geq d(s_\infty - 1)$ the composition $\widetilde{N}_{k_n/k_m} \circ \widetilde{\rho}_{k_n/k_m}$ is the trivial map, but $\widetilde{N}_{k_n/k_m}$ is an isomorphism for sufficiently large m, so $\widetilde{\rho}_{k_n/k_m}$ is the trivial map when m is sufficiently large and $n \geq m + d(s_\infty - 1)$. Therefore

$$H^2(G, \mathcal{O}_L^\times) \cong \varinjlim_n H^2(G_n, \mathcal{O}_{\ell_n}^\times) \cong 0$$

which finishes the proof. □

Now we're ready to give the more specialized and easily applicable vanishing criterion.

Theorem 8.18. *Let L/K be a cyclic p-extension of $\mathbb{Z}_p$-fields which is unramified at every infinite place. Suppose $K = k_\infty$ is the cyclotomic $\mathbb{Z}_p$-extension of a number field k such that $p \nmid h(k)$ and k has only one prime lying above p. Then $\lambda_L = 0$ if and only if, for all prime ideals $\mathfrak{p}$ of K which ramify in L/K and do not lie over p, the order in C_L of the class of the product of prime ideals of L lying over $\mathfrak{p}$ is prime to p.*

Proof. The "$\Rightarrow$" implication is clear. The "$\Leftarrow$" theorem follows from Theorem 8.15 by noting that (1) the assumptions we've made ensure that conditions (i) and (ii) hold by Theorem 3.3 and Lemma 8.17, respectively, and (2) $(I_L^G P_L)/(I_K P_L)$ is a p-group generated by the classes of products of prime ideals of L lying over $\mathfrak{p}$ where $\mathfrak{p}$ runs through all prime ideals of K which ramify in L/K and do not lie above p. $\square$

Part III

OTHER DIRECTIONS

Chapter 9
DEGREE $q \neq p$

There are difficulties in applying the methods of the prior chapters to the case where L/K is a $\mathbb{Z}/(q^n)$-extension of $\mathbb{Z}_p$-fields for a prime $q \neq p$. One issue for cyclic q-extensions is that if we now appropriately define

$$\chi(G,-) := \operatorname{ord}_q\left(\frac{|H^2(G,-)|}{|H^1(G,-)|}\right),$$

then $\chi(G, I_L)$ is no longer finite (i.e., well-defined) since H^2 will be infinite. The following example illustrates this difficulty.

Example 9.1. Let $p = 3$, $q = 2$ with $L/K = \mathbb{Q}_\infty(i)/\mathbb{Q}_\infty$. Any rational non-$p$-prime $r \equiv 3 \pmod 4$ remains inert in $\mathbb{Q}(i)/\mathbb{Q}$, and consequently (since $2 \neq 3$) any prime $\mathfrak{r}$ in $\mathcal{O}_K$ lying above r remains inert in L/K. This $\mathfrak{r}$ contributes a factor of $\mathbb{Z}/q\mathbb{Z}$ to $H^2(G, I_L)$. There are infinitely many such r, so $\chi(G, I_L)$ is not finite.

The point here is that $\chi(G, I_L)$ is a sum of terms of the form $\operatorname{ord}_q(ef)$ where e, f are the ramification index and residue degree, respectively, but when $q = p$ we always have $f = 1$, so there were only finitely many nonzero $\operatorname{ord}_p(ef)$ (corresponding to the ramified places not lying above p) in that case. It will turn out, however, that $|H^1(G, \mathcal{O}_L^\times)|/|H^1(G, P_L)|$ is still finite in special cases, and, moreover, this quantity is related to the q-part (not the p-part) of the class groups of L and K. Before specializing to cyclic q-extensions, we'll mention some results about fairly general extensions of $\mathbb{Z}_p$-fields.

Lemma 9.2. *Let ℓ/k be an extension of number fields. We have homomorphisms*

$$J_{\ell/k}\colon C_k \to C_\ell\colon [\mathfrak{p}] \mapsto [\mathfrak{p}\mathcal{O}_\ell]$$
$$N_{\ell/k}\colon C_\ell \to C_k\colon [\mathfrak{P}] \mapsto [\mathfrak{p}^f]$$

where $\mathfrak{P}$ is a prime ideal of $\mathcal{O}_\ell$, $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_k$, and $f = [\mathcal{O}_\ell/\mathfrak{P} : \mathcal{O}_k/\mathfrak{p}]$. We have

$$(N_{\ell/k} \circ J_{\ell/k})(c) = c^{[\ell:k]}$$

and, if ℓ/k is Galois,

$$(J_{\ell/k} \circ N_{\ell/k})(d) = \prod_{\sigma \in \mathrm{Gal}(\ell/k)} \sigma(d)$$

for all $c \in C_k$ and all $d \in C_\ell$.

Proof. See Greenberg's monograph [Gre10] for example. □

Taking direct limits in the above lemma immediately yields the following.

Corollary 9.3. *Let L/K be an extension of $\mathbb{Z}_p$-fields. We have homomorphisms*

$$J_{L/K} := \varinjlim_n J_{\ell_n/k_n} : C_K \to C_L$$
$$N_{L/K} := \varinjlim_n N_{\ell_n/k_n} : C_L \to C_K$$

where L, K are the cyclotomic $\mathbb{Z}_p$-extensions of number fields ℓ, k, respectively. We have

$$(N_{L/K} \circ J_{L/K})(c) = c^{[L:K]}$$

and, if L/K is Galois,

$$(J_{L/K} \circ N_{L/K})(d) = \prod_{\sigma \in \mathrm{Gal}(L/K)} \sigma(d)$$

for all $c \in C_K$ and all $d \in C_L$.

Corollary 9.4. *Let L/K be an extension of $\mathbb{Z}_p$-fields. We have*

$$[L : K]\ker(J_{L/K}) = 0$$

and, if L/K is Galois,

$$[L : K]C_L^G \subseteq J_{L/K}(C_K).$$

The following proposition is inspired by Proposition 1.2.3 in [Gre10].

Proposition 9.5. *Let L/K be a Galois extension of $\mathbb{Z}_p$-fields with $G = \mathrm{Gal}(L/K)$. Then there is an exact sequence of abelian groups*

$$0 \to \ker(J_{L/K}) \to H^1(G, \mathcal{O}_L^\times) \to \bigoplus_v \frac{\mathbb{Z}}{(e'(w/v))} \to C_L^{[G]}/J_{L/K}(C_K) \to 0$$

where $C_L^{[G]}$ is the subgroup of C_L^G generated by classes of G-fixed ideals, the direct sum ranges over all finite places v of K with w a place of L lying over v and

$$e'(w/v) = \begin{cases} e(w/v) & \text{if } v \nmid p \\ e(w/v)|e(w/v)|_p & \text{if } v|p. \end{cases}$$

Further, the exact sequence extends

$$0 \to \ker(J_{L/K}) \to H^1(G, \mathcal{O}_L^\times) \to \bigoplus_v \frac{\mathbb{Z}}{(e'(w/v))} \to C_L^G/J_{L/K}(C_K) \to H^1(G, P_L) \to 0$$

Proof. We use the snake lemma on the following commutative diagram with exact rows and columns:

$$\begin{array}{ccccccccc}
 & & 0 & \longrightarrow & 0 & \longrightarrow & \ker(J_{L/K}) & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \longrightarrow & P_K & \longrightarrow & I_K & \longrightarrow & C_K & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow{\scriptstyle J_{L/K}} & & \\
0 & \longrightarrow & P_L^G & \longrightarrow & I_L^G & \xrightarrow{\Psi} & C_L^G & \xrightarrow{\rho} & H^1(G, P_L) \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & H^1(G, \mathcal{O}_L^\times) & \longrightarrow & I_L^G/I_K & \longrightarrow & C_L^G/J_{L/K}(C_K) & &
\end{array}$$

This proves the first part of the theorem. Additionally, we know that

$$I_L \cong \bigoplus_v I_{L,v} \cong \bigoplus_v \mathrm{Hom}_{Z_v}(\mathbb{Z}G, R_v)$$

as G-modules where the direct sum ranges over all finite places v of K with decomposition group Z_v of w/v for some place w on L lying over v and R_v has trivial G-action

with $R_v = \mathbb{Z}$ if $v \nmid p$ while $R_v = \cup_{n\geq 0} p^{-n}\mathbb{Z}$ if $v|p$. Thus Shapiro's lemma implies

$$H^1(G, I_L) \cong \bigoplus_v H^1(G, \mathrm{Hom}_{Z_v}(\mathbb{Z}G, R_v)) \cong \bigoplus_v H^1(Z_v, R_v) \cong 0$$

since each R_v is torsion free. In this way, the map occurring in the above diagram

$$\rho\colon C_L^G \to H^1(G, P_L)$$

is surjective. Therefore we need only observe that

$$J_{L/K}(C_L) \subseteq C_L^{[G]} = \mathrm{im}(\Psi) = \ker(\rho)$$

and the proof is complete. See also Equation (A.4) in [HS05] and the proof of Proposition 1.3.4 in [Gre10]. □

9.1 Abelian $\mathbb{Z}_p$-Fields

Lemma 9.6. *Let L be an **abelian $\mathbb{Z}_p$-field**, i.e., L is the cyclotomic $\mathbb{Z}_p$-extension of an abelian number field. Then $\mu_L = 0$ and for every prime $q \neq p$, the q-primary part of the class group, denoted by $C_L[q^\infty]$, is finite.*

Proof. See Washington's text [Was96]. □

Theorem 9.7. *Let L/K be a cyclic extension of abelian $\mathbb{Z}_p$-fields with $G = \mathrm{Gal}(L/K)$ and $(p, |G|) = 1$. Then*

$$\frac{|H^1(G, \mathcal{O}_L^\times)|}{|H^1(G, P_L)|} \cdot \frac{|C_L^G / J_{L/K}(C_K)|}{|\ker(J_{L/K})|} = \prod_v e(w/v)$$

where the product ranges over all finite places v of K with w a place of L lying over v.

Corollary 9.8. *Let L/K be a cyclic q-extension of abelian $\mathbb{Z}_p$-fields with $q \neq p$ and $G = \mathrm{Gal}(L/K)$. Then*

$$\frac{|H^1(G, \mathcal{O}_L^\times)|}{|H^1(G, P_L)|} \cdot \frac{|C_L^G[q^\infty]|}{|C_K[q^\infty]|} = \prod_v e(w/v)$$

where the product ranges over all finite places v of K with w a place of L lying over v.

Chapter 10
DEDEKIND SCHEMES

In this chapter, we find a general context for which Dedekind's different formula is true, and we'll see how this formula simultaneously encapsulates both the Hurwitz formula for curves and Iwasawa's formula. First, we'll need to establish/review some definitions and lemmas.

Definition 10.1. Suppose X, Y are schemes with Y locally Noetherian (i.e., there is an affine open cover $\{\mathrm{Spec}(B_i)\}_{i\in I}$ of Y with each B_i Noetherian). Let $f : X \to Y$ be a morphism of finite type (i.e., for every affine open subset V of Y we have that $f^{-1}(V)$ is quasi-compact and $\mathcal{O}_X(U)$ is a finitely generated $\mathcal{O}_Y(V)$-algebra whenever U is an affine open subset of $f^{-1}(V)$). We say f is a **local complete intersection** (or **LCI**) if for every $x \in X$ there is an open neighborhood U of x such that $f|_U = g \circ i$ where $i : U \to W$ is a regular immersion (i.e., i is an immersion and for every $x \in X$ we have that $\ker(\mathcal{O}_{Y,f(x)} \to \mathcal{O}_{X,x})$ is generated by a sequence $b_1, \ldots b_n \in \mathcal{O}_{Y,f(x)}$ such that b_m is not a zero-divisor in $\mathcal{O}_{Y,f(x)}/(b_1, \ldots, b_{m-1})$ for all m) and $g : W \to Y$ is a smooth morphism.

For schemes $X \xrightarrow{f} Y \longrightarrow Z$, we always have an exact sequence

$$f^*\Omega_{Y/Z} \to \Omega_{X/Z} \to \Omega_{X/Y} \to 0$$

of sheaves of relative differentials. If $f^*\Omega_{Y/Z} \to \Omega_{X/Z}$ happens to be a monomorphism, we can apply an 'Euler characteristic' χ (meaning a functor which is additive on short exact sequences) to compute $\chi(\Omega_{X/Y})$ (which should contain ramification information) via $\chi(\Omega_{X/Z}) = \chi(f^*\Omega_{Y/Z}) + \chi(\Omega_{X/Y})$. Indeed, this is the method Hartshorne uses in [Har97] to prove the Riemann-Hurwitz formula for nonsingular, projective curves over an algebraically closed field. The notion of an LCI (defined above) provides a

general framework in which we might hope to employ the same tactics. The following lemma, found in [Liu02], gives conditions for when this first morphism in the above sequence is a monomorphism.

Lemma 10.2. *Let $f : X \to Y$ be a dominant, separable LCI of Noetherian, integral schemes over a scheme Z. Then there is a short exact sequence of $\mathcal{O}_X$-modules*

$$0 \to f^*\Omega_{Y/Z} \to \Omega_{X/Z} \to \Omega_{X/Y} \to 0.$$

We want to consider morphisms which satisfy the hypotheses of the above result, and we'll be interested in a class of schemes which captures the similarities between normal, projective curves over fields and spectrums of Dedekind domains. To this end, we make the following definitions, as found in [Sza09] or with less restrictions in [Liu02].

Definition 10.3. A **Dedekind scheme** is a normal, integral scheme of dimension 1 which is separated and Noetherian.

Remark 10.4. Let X be a Dedekind scheme. Then $\mathcal{O}_{X,x}$ is a PID for all $x \in X$ and a DVR when x is a closed point. In particular, X is regular.

Example 10.5. If $\mathcal{O}$ is a Dedekind domain which is not a field, then $\mathrm{Spec}(\mathcal{O})$ is a Dedekind scheme. In particular, $\mathrm{Spec}(\mathcal{O}_k)$ is a Dedekind scheme when k is a number field. Likewise, $\mathrm{Spec}(\mathcal{O}_K[1/p])$ is a Dedekind scheme when K is a $\mathbb{Z}_p$-field; to see why $\mathcal{O}_K[1/p]$ is a Dedekind domain, we'll use the following definition and lemma.

Definition 10.6. A **Prüfer domain** is an integral domain in which every finitely generated, nonzero ideal is invertible.

Lemma 10.7. *Let $\mathcal{O}$ be a Prüfer domain, and let F be its field of fractions. Then*

1. *The integral closure of $\mathcal{O}$ in an algebraic extension of F is a Prüfer domain.*

2. If S is a ring such that $\mathcal{O} \subseteq S \subseteq F$, then S is a Prüfer domain.

3. $\mathcal{O}$ is a Dedekind domain $\Leftrightarrow$ $\mathcal{O}$ is Noetherian.

Proposition 10.8. *Let K be a $\mathbb{Z}_p$-field. Then $\mathcal{O}_K[1/p]$ is a Dedekind domain.*

Proof. First, $\mathcal{O}_K$ is a Prüfer domain by part 1 of the above lemma since it's the integral closure of $\mathbb{Z}$ (obviously a Prüfer domain) in K (an algebraic extension of $\mathbb{Q}$). Second, $\mathcal{O}_K[1/p]$ is a Prüfer domain by part 2 of the above lemma since $\mathcal{O}_K \subseteq \mathcal{O}_K[1/p] \subseteq K$. Thus by part 3 of the above lemma it suffices to show $\mathcal{O}_K[1/p]$ is Noetherian. Ket k be a number field such that $K = k_\infty$. Every proper, nonzero ideal in $\mathcal{O}_K[1/p]$ is of the form $I[1/p]$ where I is a nonzero ideal in $\mathcal{O}_K$ such that

$$I \cap \{1, p, p^2, \ldots\} = \varnothing.$$

Take

$$I_n := \mathcal{O}_{k_n} \cap I$$

for all $n \in \mathbb{N}_0$. Finite places are finitely split in cyclotomic $\mathbb{Z}_p$-extensions and non-p-places are unramified in $\mathbb{Z}_p$ extensions, so there is an $m \in \mathbb{N}_0$ such that

$$I_n = \mathcal{O}_{k_n} I_m$$

for all $n \geq m$. Hence

$$I = \bigcup_{n=1}^{\infty} I_n = \mathcal{O}_K I_m$$

is finitely generated as an $\mathcal{O}_K$-module since I_m is finitely generated as an $\mathcal{O}_{k_m}$-module. Therefore $I[1/p]$ is finitely generated as an $\mathcal{O}_K[1/p]$-module. □

Example 10.9. Normal, projective curves over a field F are Dedekind schemes.

The next lemma (proved in [Liu02]) will guarantee that the finite, separable morphisms we consider are, in fact, LCIs.

Lemma 10.10. *Let $f : X \to Y$ be a morphism of finite type of regular, locally Noetherian schemes. Then f is an LCI.*

With lemmas 10.2 and 10.10 in hand, we immediately obtain the following corollary by noting that finite, separable morphisms of Dedekind schemes are surjective on the underlying topological spaces (whence dominant).

Corollary 10.11. *Let $f : X \to Y$ be a finite, separable morphism of Dedekind schemes over a scheme Z. Then there is a short exact sequence of $\mathcal{O}_X$-modules*

$$0 \to f^*\Omega_{Y/Z} \to \Omega_{X/Z} \to \Omega_{X/Y} \to 0.$$

When $X = \mathcal{C}_1, Y = \mathcal{C}_2$ are nonsingular, projective curves over $Z = \mathrm{Spec}(\overline{F})$ where $\overline{F}$ is an algebraically closed field, we can take our Euler characteristic to be

$$\chi_{\overline{F}}(\mathscr{F}) := \sum_{n=0}^{\infty} (-1)^n \dim_{\overline{F}}(H^n(X, \mathscr{F})).$$

Then we follow suit as in the discussion before Remark 4.7. In what follows, we furnish a more general notion of degree and Euler characteristic, and we outline a plan for constructing a general Riemann-Hurwitz formula for finite, separable morphisms of Dedekind schemes. In this context, $\Omega_{X/Y}$ contains the ramification info via Dedekind's different formula as stated below. Now we define canonical sheaves which play a crucial role in the proceeding discussion.

Definition 10.12. Let $f : X \to Y$ be a quasi-projective LCI with Y locally Noetherian. Then f factors as

$$X \xrightarrow{i} W \xrightarrow{g} Y$$

where i is an immersion and g is smooth. The conormal sheaf $\mathrm{C}_{X/W}$ and the sheaf of relative differentials $\Omega_{W/Y}$ are locally free of some finite ranks m and n, respectively. Thus the determinants

$$\det(\mathrm{C}_{X/W}) = \bigwedge^m \mathrm{C}_{X/W} \qquad\qquad \det(\Omega_{W/Y}) = \bigwedge^n \Omega_{W/Y}$$

are invertible sheaves, and we may define the **canonical sheaf** of X/Y as

$$\omega_{X/Y} := \det(\mathrm{C}_{X/W})^\vee \otimes_{\mathcal{O}_X} i^* \det(\Omega_{W/Y})$$

which is an invertible sheaf of $\mathcal{O}_X$-modules that turns out not to depend on the choice of W. Note that if f happens to be smooth, then

$$\omega_{X/Y} = \det(\Omega_{X/Y}).$$

We know that finite, separable morphisms of Dedekind schemes are LCIs, and it's natural to guess more is true.

Proposition 10.13. *Let $f : X \to Y$ be a finite, separable morphism of Dedekind schemes. Then f is quasi-projective.*

It is easy to see this proposition in some special cases. Specifically, finite morphisms of affine schemes are projective, and finite, separable morphisms of normal projective curves over a field F are quasi-projective. In these situations, we have the following formula which Liu uses in [Liu02] to prove a fairly general Riemann-Hurwitz formula for normal projective curves over an arbitrary base field F.

Theorem 10.14 (Adjunction Formula)**.** *Let $X \xrightarrow{f} Y \longrightarrow Z$ be quasi-projective LCIs. Then*

$$\omega_{X/Z} \cong \omega_{X/Y} \otimes_{\mathcal{O}_X} f^*\omega_{Y/Z}.$$

Next, we define a general Euler characteristic and degree, which can then be applied to the short exact sequence of sheaves of relative differentials and the adjunction formula above.

Definition 10.15. Suppose X is a Dedekind scheme which is a quasi-projective LCI over a scheme Z. For a sheaf $\mathscr{F}$ of $\mathcal{O}_X$-modules define

$$\chi_Z(\mathscr{F}) := \sum_{n=0}^{\infty} (-1)^n \dim_Z(H^n(X, \mathscr{F}))$$

with

$$\dim_Z(M) := \sum_x \text{length}_{\mathcal{O}_{Z,z}}(M_x)$$

where the sum ranges over all closed points $x \in X$ with images $z \in Z$. Also, for an effective divisor D of X define

$$\deg_Z(D) := \sum_{x \in D} \text{length}_{\mathcal{O}_{X,x}}(\mathcal{O}_{D,x})[\mathbb{F}(x) : \mathbb{F}(z)]$$

where $(D, \mathcal{O}_D)$ is the closed subscheme of X corresponding to the invertible sheaf of ideals $\mathcal{O}_X(-D)$ and $\mathbb{F}(x), \mathbb{F}(y)$ are residue fields. Extend this definition to all divisors D by

$$\deg_Z(D) = \deg_Z(E) - \deg_Z(F)$$

where $D = E - F$ and E, F are effective divisors.

As one would want, χ_Z is additive on short exact sequences and $\chi_Z = \chi_F$ when $Z = \text{Spec}(F)$ for some field F.

Lemma 10.16. *Let X, Z be as above. For every short exact sequence of $\mathcal{O}_X$-modules*

$$0 \to \mathscr{F}' \to \mathscr{F} \to \mathscr{F}'' \to 0$$

we have

$$\chi_Z(\mathscr{F}) = \chi_Z(\mathscr{F}') + \chi_Z(\mathscr{F}'')$$

whenever two of the three terms are finite.

Also, $\deg_Z$ and χ_Z are related by the following two lemmas.

Lemma 10.17. *Suppose X is a Dedekind scheme and D is an effective divisor. Then*

$$\deg_Z(D) = \chi_Z(\mathcal{O}_D).$$

Proof. We know $(D, \mathcal{O}_D)$ is affine, so

$$\begin{aligned}\chi_Z(\mathcal{O}_D) &= \dim_Z(H^0(D, \mathcal{O}_D)) = \sum_{x \in D} \text{length}_{\mathcal{O}_{Z,z}}(\mathcal{O}_{D,x}) \\ &= \sum_{x \in D} \text{length}_{\mathcal{O}_{X,x}}(\mathcal{O}_{D,x})[\mathbb{F}(x) : \mathbb{F}(z)] = \deg_Z(D).\end{aligned}$$

□

Lemma 10.18. *Suppose X is a Dedekind Z-scheme and D is a divisor on X. Then*

$$\deg_Z(D) = \chi_Z(\mathcal{O}_X(D)) - \chi_Z(\mathcal{O}_X)$$

when these quantities are finite.

Sketch. We proceed as in [Liu02]. Write $D = E - F$ for effective divisors E, F. Note that there is a short exact sequence of $\mathcal{O}_X$-modules

$$0 \to \mathcal{O}_X(-F) \to \mathcal{O}_X \to \mathcal{O}_F \to 0.$$

Then apply the exact functor $- \otimes_{\mathcal{O}_X} \mathcal{O}_X(E)$ to conclude by Lemma 10.17 that

$$\chi_Z(\mathcal{O}_X(D)) = \chi_Z(\mathcal{O}_X(E)) - \deg_Z(F) = \deg_Z(E) + \chi_Z(\mathcal{O}_X) - \deg_Z(F)$$

which leads to the desired result. □

We are prompted by this second statement to make the following definition.

Definition 10.19. Suppose X is a Dedekind scheme over a scheme Z and $\mathscr{F}$ is an invertible sheaf of $\mathcal{O}_X$-modules. Define

$$\deg_Z(\mathscr{F}) := \chi_Z(\mathscr{F}) - \chi_Z(\mathcal{O}_X).$$

Now we state the result (found in [Sza09] e.g.) which motivates why we would expect there to be a general Riemann-Hurwitz formula in the context of finite, separable morphisms of Dedekind schemes.

Theorem 10.20 (Dedekind's Different Formula)**.** *Let $f : X \to Y$ be a finite, separable morphism of Dedekind schemes. Define the* ***different*** *$\mathcal{D}_{X/Y}$ as the annihilator sheaf of $\Omega_{X/Y}$. Then $\mathcal{D}_{X/Y} = \mathcal{O}_X(-D_{X/Y})$ where*

$$D_{X/Y} = \sum_i m_i x_i$$

is an effective divisor supported at the points x_i where f is not étale, and we have

$$m_i = e_i' - 1$$

where $e_i' = e_i$ is the ramification index of x_i/y_i when f is tamely ramified at x_i and $e_i' > e_i$ when f is wildly ramified at x_i.

From the theory of normal, projective curves over a field F, it's natural to conjecture the following relationship between the different and the canonical sheaf.

Conjecture 10.21. *Let $f : X \to Y$ be a finite, separable morphism of Dedekind schemes which are quasi-projective LCIs over a scheme Z. Then f is quasi-projective and*

$$\deg_Z(\omega_{X/Y}) = -\deg_Z(\mathcal{D}_{X/Y}).$$

As soon as this conjecture holds, we get a family of Riemann-Hurwitz formulas parameterized by the base scheme Z.

Corollary 10.22. *Let $X \xrightarrow{f} Y$ be a finite, separable morphism of Dedekind schemes which are quasi-projective LCIs over a scheme Z. Then*

$$\deg_Z(\omega_{X/Z}) = \deg(f)\deg_Z(\omega_{Y/Z}) + \sum_x [\mathbb{F}(x) : \mathbb{F}(z)](e_{x/y}' - 1)$$

where the sum ranges over the closed points x of X with images y in Y, z in Z and $e_{x/y}' = e_{x/y}$ at tame ramification while $e_{x/y}' > e_{x/y}$ at wild ramification.

Even if the above conjecture is not true in the generality stated, it is true at least for normal projective curves over fields and for affine schemes. This captures the classical Hurwitz formula and Iwasawa's formula together.

Proposition 10.23. *Conjecture 10.21 above is true when X, Y are affine. More precisely,*

$$\omega_{X/Y} \otimes_{\mathcal{O}_X} \mathcal{D}_{X/Y} \cong \mathcal{O}_X.$$

Sketch. The idea is to use Theorem 4.32 in [Liu02] which says that if $f : X \to Y$ is a flat, projective LCI of some relative dimension r with Y locally Noetherian, then the "r-dualizing sheaf" ω_f is isomorphic to $\omega_{X/Y}$. On the other hand, if f is, moreover, finite and X is also locally Noetherian, then

$$\omega_f = f^!\mathcal{O}_Y := \mathcal{H}om_{\mathcal{O}_Y}(f_*\mathcal{O}_X, \mathcal{O}_Y).$$

For affine Dedekind schemes $X = \mathrm{Spec}(B)$, $Y = \mathrm{Spec}(A)$ where $A \hookrightarrow B$ is an inclusion of Dedekind domains such that the induced inclusion of function fields L/K is a finite, separable extension, we know that the natural morphism $f : X \to Y$ is indeed a flat, projective, finite LCI, so

$$\omega_{X/Y} \cong \mathrm{Hom}_A(B, A)^{\sim},$$

but there is an isomorphism

$$W_{B/A} \cong \mathrm{Hom}_A(B, A)$$

where

$$W_{B/A} = \{\beta \in L | \mathrm{Tr}_{L/K}(\beta B) \subseteq A\}$$

is the codifferent, which is the inverse fractional ideal of the different. □

We can actually compute $\deg(\omega_{X/Z})$, $\deg(\omega_{Y/Z})$ in a special Iwasawa theoretic context.

Corollary 10.24. *Let $K_0 = \mathbb{Q}_\infty \subseteq \ldots \subseteq K_m = K \subseteq \ldots \subseteq K_n = L$ be a tower of $\mathbb{Z}/(p)$-extensions unramified at the infinite places. Putting $X = \mathrm{Spec}(\mathcal{O}_L[1/p]), Y = \mathrm{Spec}(\mathcal{O}_K[1/p]), Z = \mathrm{Spec}(\mathcal{O}_{\mathbb{Q}_\infty}[1/p])$ we have*

$$\begin{aligned}\deg(\omega_{Y/Z}) &= \lambda_K - q_K \\ \deg(\omega_{X/Y}) &= \sum_{w \nmid p}(e_w - 1) \\ \deg(\omega_{X/Z}) &= \lambda_L - q_L \\ &= [L:K]\deg(\omega_{Y/Z}) + \deg(\omega_{X/Z})\end{aligned}$$

where

$$q_{K_j} = (p-1)\sum_{i=1}^{j} p^{j-i}\chi(\mathrm{Gal}(K_i/K_{i-1}), \mathcal{O}_{K_i}^\times).$$

Remark 10.25. A purely geometric proof of the above corollary or, more generally, Iwasawa's formula seems within the realm of possibility but is lacking. In particular, there is a way of realizing the quantity $\lambda_L - q_L$ as an Euler characteristic coming from sheaf cohomology. Let L/K be a p-extension of $\mathbb{Z}_p$-fields with p an odd prime. Then for a sheaf $\mathscr{F}$ of $G = \mathrm{Gal}(L/K)$-modules on $X = \mathrm{Spec}(\mathcal{O}_L[1/p])$ we may define

$$\chi_G(\mathscr{F}) = \sum_{n=0}^{\infty}(-1)^n \dim_G(H^n(X, \mathscr{F}))$$

where for any fixed tower of $\mathbb{Z}/(p)$-extensions $K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_m = L$ we take

$$\dim_G(M) = \sum_{i=1}^{m}\varphi(p^{m+1-i})\chi(N_{i-1}/N_i, M^{N_i})$$

with $N_i = \mathrm{Gal}(L/K_i)$. In this notation, we have

$$p^m - 1 - \chi_G(\mathcal{O}_X^\times) = \lambda_L - p^m\lambda_K - \sum_{i=1}^{m}\varphi(p^{m+1-i})\chi(N_{i-1}/N_i, \mathcal{O}_{K_i}^\times) = \chi_Y(\mathcal{O}_{D_{X/Y}}).$$

Here we are cheating a bit since we're using Iwasawa's formula, but if one could establish the equality of the left and right hand sides of the above equation independently

(by knowing some general results about how χ_G and χ_Y are related), then this would actually prove Iwasawa's formula in a more geometric fashion.

References

[AT09] E. Artin and J.T. Tate. *Class Field Theory.* AMS Chelsea Pub., 2009.

[AW67] M. Atiyah and C. Wall. Cohomology of groups. In J. Cassels and A. Frölich, editors, *Algebraic Number Theory*, Washington, D.C., 1967. Thompson Book Company Inc.

[BG64] S. D. Berman and P. M. Gudivok. Indecomposable representations of finite groups over the ring of p-adic integers. *Izv. Akad. Nauk SSSR Ser. Mat.*, 28:875–910, 1964. (Russian).

[CR66] Charles W. Curtis and Irving Reiner. *Representation Theory of Finite Groups and Associative Algebras.* Interscience Publishers, 1966.

[CS06] J. Coates and R. Sujatha. *Cyclotomic Fields and Zeta Values.* Springer, 2006.

[Fer80] Bruce Ferrero. The cyclotomic $\mathbb{Z}_2$-extension of imaginary quadratic fields. *Amer. J. Math.*, 102(3):447–459, 1980.

[FK80] Hershel M. Farkas and Irwin Kra. *Riemann surfaces*, volume 71 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1980.

[FKOT97] Takashi Fukuda, Keiichi Komatsu, Manabu Ozaki, and Hisao Taya. On Iwasawa λ_p-invariants of relative real cyclic extensions of degree p. *Tokyo J. Math.*, 20(2):475–480, 1997.

[FOO06] Satoshi Fujii, Yoshihiro Ohgi, and Manabu Ozaki. Construction of $\mathbb{Z}_p$-extensions with prescribed Iwasawa λ-invariants. *J. Number Theory*, 118(2):200–207, 2006.

[FW79] Bruce Ferrero and Lawrence C. Washington. The Iwasawa invariant μ_p vanishes for abelian number fields. *Ann. of Math. (2)*, 109(2):377–395, 1979.

[Gou97] Fernando Q. Gouvêa. *p-adic Numbers: An Introduction.* Springer, second edition, 1997.

[Gre01] Ralph Greenberg. Iwasawa theory - Past and present. *Advanced Studies in Pure Math.*, 30:335–385, 2001.

[Gre10] Ralph Greenberg. Topics in Iwasawa theory. `math.washington.edu/~greenber/book.pdf`, 2010.

[Har97] Robin Hartshorne. *Algebraic Geometry*. Springer, corrected eighth printing edition, 1997.

[Has52] Helmut Hasse. *Über die Klassenzahl abelscher Zahlkörper*. Akademie Verlag, Berlin, 1952.

[HM83] I. Hughes and R. Mollin. Totally positive units and squares. *Proceedings of the American Mathematical Society*, 87(4):613–616, 1983.

[HR62] A. Heller and I. Reiner. Representations of cyclic groups in rings of integers, I. *The Annals of Mathematics*, 76(1):73–92, 1962.

[HR63] A. Heller and I. Reiner. Representations of cyclic groups in rings of integers, II. *The Annals of Mathematics*, 77(2):318–328, 1963.

[HS97] P. J. Hilton and U. Stammbach. *A Couse in Homological Algebra*. Springer, second edition, 1997.

[HS05] Yoshitaka Hachimori and Romyar T. Sharifi. On the failure of pseudonullity of Iwasawa modules. *J. Algebraic Geom.*, 14(3):567–591, 2005.

[IN10] Humio Ichimura and Shoichi Nakajima. On the 2-part of the ideal class group of the cyclotomic $\mathbb{Z}_p$-extension over the rationals. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg*, 80:175–182, 2010.

[IR90] Kenneth Ireland and Michael Rosen. *A Classical Introduction to Modern Number Theory*. Springer, second edition, 1990.

[Iwa59a] Kenkichi Iwasawa. On Γ-extensions of algebraic number fields. *Bull. Amer. Math. Soc.*, 65:183–226, 1959.

[Iwa59b] Kenkichi Iwasawa. Sheaves for algebraic number fields. *Ann. of Math. (2)*, 69(2):408–413, March 1959.

[Iwa65] Kenkichi Iwasawa. Analogies between number fields and function fields. *Annual science conference proceedings - Yeshiva University, Belfer Graduate School of Science*, 2:203–208, 1965.

[Iwa73a] Kenkichi Iwasawa. *On the μ-invariants of $\mathbb{Z}_l$-extensions*. Number theory, algebraic geometry and commutative algebra, in honor of Yasuo Akizuki, Kinokuniya, Tokyo, 1973. pp 1-11.

[Iwa73b] Kenkichi Iwasawa. On $\mathbb{Z}_l$-extensions of algebraic number fields. *Ann. of Math. (2)*, 98:246–326, 1973.

[Iwa81] Kenkichi Iwasawa. Riemann-Hurwitz formula and p-adic Galois representations for number fields. *Tohoku Math. J. (2)*, 33(2):263–288, 1981.

[Iwa89] Kenkichi Iwasawa. A note on capitulation problem for number fields. *Proc. Japan Acad. Ser. A Math. Sci.*, 65(2):59–61, 1989.

[Jos06] Jürgen Jost. *Compact Riemann Surfaces: An Introduction to Contemporary Mathematics*. Springer, third edition, 2006.

[Kid79] Yûji Kida. On cyclotomic $\mathbb{Z}_2$-extensions of imaginary quadratic fields. *Tohoku Math. J.*, 31:91–96, 1979.

[Kid80] Yûji Kida. l-extensions of CM-fields and cyclotomic invariants. *J. Number Theory*, 12(4):519–528, 1980.

[Koc97] Helmut Koch. *Algebraic number theory*. Springer, 1997.

[Lan90] Serge Lang. *Cyclotomic Fields I and II*. Springer, second edition, 1990. Assisted by Karl Rubin.

[Liu02] Qing Liu. *Algebraic Geometry and Arithmetic Curves*. Oxford University Press, 2002. Translated by Reinie Erné.

[Mir95] Rick Miranda. *Algebraic Curves and Riemann Surfaces*. AMS, 1995. Graduate Studies in Mathematics, Vol 5.

[Neu99] Jürgen Neukirch. *Algebraic Number Theory*. Springer, 1999. Translated from German by Norbert Schappacher.

[Nis06] Yoshinori Nishino. On the Iwasawa invariants of the cyclotomic $\mathbb{Z}_2$-extensions of certain real quadratic fields. *Tokyo J. Math.*, 29(1):239–245, 2006.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. *Cohomology of number fields*. Springer-Verlag, Berlin, second edition, 2008.

[Par66] J. T. Parr. Cohomology of cyclic groups of prime square order. *Pacific Journal of Mathematics*, 17(3):467–473, 1966.

[Rei61] Irving Reiner. The Krull-Schmidt theorem for integral group representations. *Bull. Amer. Math. Soc.*, 67(4):365–367, 1961.

[Ser97] Jean-Pierre Serre. *Galois Cohomology*. Springer, 1997. Translated from French by Patrick Ion.

[Sha94] Igor R. Shafarevich. *Basic Algebraic Geometry 1: Varieties in Projective Space*. Springer-Verlag, second edition, 1994.

[Sin84] Warren M. Sinnott. On p-adic L-functions and the Riemann-Hurwitz genus formula. *Compositio Mathematica*, 53(1):3–17, 1984.

[Sza09] Tamás Szamuely. *Fundamental Groups and Galois Groups*. Cambridge University Press, 2009.

[Was96] Lawrence C. Washington. *Introduction to Cyclotomic Fields*. Springer, second edition, 1996.