RIEMANN-HURWITZ FORMULAS FOR λ-INVARIANTS IN CYCLIC p-EXTENSIONS

JORDAN C. SCHETTLER

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 was not entirely clear since the proofs are of a very different flavor. Around a year after Kida's result was published, Kenkichi Iwasawa used Galois cohomology in [Iwa81] to establish a more general, although apparently less precise, formula (about representations) that did not exclude the prime $p = 2$ nor need the CM-field assumption. Moreover, Kida's follows as a corollary from Iwasawa's formula.

We first define and state properties of an 'Euler characteristic' for group cohomology. Then we'll briefly recall Iwasawa's formula. 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, as 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 of these special formulas include congruences and inequalities for λ-invariants that cannot be gleaned from Iwasawa's formula.

Contents

1. The Euler Characteristic

Suppose L/K is a cyclic p-extension of $\mathbb{Z}_p$-fields (i.e., cyclotomic $\mathbb{Z}_p$-extensions of number fields) with $\mu_K = 0$. 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 (see [HS97])

$$\begin{aligned} \varphi_{M,g} &: M \to M : m \mapsto (g-1)m \\ \psi_{M,g} &: M \to M : m \mapsto (g^{|G|-1} + g^{|G|-2} + \cdots + 1)m. \end{aligned}$$

Using the notation $\mathrm{q}(-)$ for the Herbrand quotient, 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 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. Note that

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

for all $n \in \mathbb{N}$ where $p^m = |G|$, but H^n distributes over direct sums, 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 $H^n(G, B_L) = 0$. Thus using additivity and [Iwa81] 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 [Iwa81] 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 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 $\mu_L = 0$, so if

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

denotes the p-Pontryagin dual functor, then

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

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 duality and the fact that finite abelian p-groups A are self dual 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. Also, 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

$$\begin{aligned}\chi(H/N, A_{L^N}) &= -\chi(H/N, (A_L^N)^*) = -\chi(H/N, (A_L^*)_N) \\ &= -\chi(H/N, (A_L^*)^N) = -\sum_n a_n \chi(H/N, M_n^N).\end{aligned}$$

We can then compare these computations to

$$\lambda_L = \mathrm{rank}_{\mathbb{Z}_p}(A_L^*) = \sum_n a_n \mathrm{rank}_{\mathbb{Z}_p}(M_n) \tag{2.1}$$

and

$$\begin{aligned} \lambda_K &= \mathrm{rank}_{\mathbb{Z}_p}(A_K^*) = \mathrm{rank}_{\mathbb{Z}_p}((A_L^G)^*) \\ &= \mathrm{rank}_{\mathbb{Z}_p}((A_L^*)_G) = \mathrm{rank}_{\mathbb{Z}_p}((A_L^*)^G) \\ &= \sum_n a_n \mathrm{rank}_{\mathbb{Z}_p}(M_n^G). \end{aligned} \tag{2.2}$$

Used in conjunction with Lemma 1, Remark 2 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 $\mathrm{rank}_{\mathbb{Z}_p}(M_n^N)$. 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.

2. Iwasawa's Formula

Suppose that L/K is a cyclic extension of $\mathbb{Z}_p$-fields with degree $[L : K] = p$ and $\mu_K = 0$. We now recall a mild generalization of Iwasawa's Riemann-Hurwitz formula (see [Iwa81]) for the λ-invariants λ_L and λ_K using an 'Euler characteristic' χ and 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 3. *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 $I_pG = (g-1)\mathbb{Z}_pG$.*

In 1980, Iwasawa used Theorem 3 to prove the following generalization of Kida's formula (see [Kid80]) in the case where L/K is unramified at infinite places.

Theorem 4. *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,

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

as $\mathbb{Z}_pG$-modules for some $a \in \mathbb{N}_0$ with $a \leq \lambda_K$.

Sketch. Use Theorem 3 for $\langle g \rangle = G$ to write

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

as $\mathbb{Z}_pG$-modules for some nonnegative integers a, b, c. As in [Iwa81], we can compute the $\mathbb{Z}_p$-ranks, G-invariants, and Euler characteristics, of these indecomposables. The results are summarized in Table 4.1. Thus if S is the set of finite places of K not lying above p which ramify in L/K, then Lemma 1 and the last column in Table 4.1 imply

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

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

TABLE 4.1.

On the other hand, equations 2.1, 2.2 in Remark 2 and the first two columns in Table 4.1 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. □

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

In this section, 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 [Iwa81] using nearly identical techniques to those used to prove Theorem 4. The formula will not be the same as we would get from induction and Iwasawa's formula (Theorem 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 integral representations. 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 5. *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*

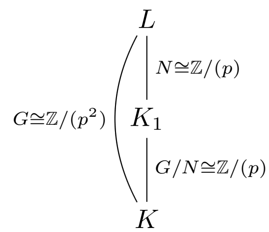
$$\begin{aligned}&I_1,\dots,I_{p-2} \text{ of } C \text{ by } A\oplus E\\ &II_1,\dots,II_p \text{ of } C \text{ by } E\\ &III_1,\dots,III_{p-1} \text{ of } C \text{ by } A\oplus B\\ &IV \text{ of } C \text{ by } A\\ &V_1,\dots,V_{p-1} \text{ of } C \text{ by } B,\end{aligned}$$

so there are exactly

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

isomorphism classes.

Proposition 6. *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

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

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 5 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 ideas laid out in Section 1, 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

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

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,

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

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

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

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 6.1. This table agrees with computations found in [Par66]. Now we do the same calculations with the above modules now regarded as

	$\mathrm{rank}_{\mathbb{Z}_p}(-)$	$(-)^G$	$H^2(G,-)$	$H^1(G,-)$	$\chi(G,-)$
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 6.1.

$\mathbb{Z}_pN$-modules. We already know the $\mathbb{Z}_p$-ranks, so we turn immediately to finding the N-invariants. We get

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

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

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

The results of these computations are summarized in Table 6.2 where $n = 0, \ldots, p$ and $m = 0, \ldots, p-1$. Finally, we go through the calculations for $A^N, B^N, \ldots$ now

	$(-)^N$	$H^2(N,-)$	$H^1(N,-)$	$\chi(N,-)$
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 6.2.

regarded as $\mathbb{Z}_p[G/N]$-modules. We know the $\mathbb{Z}_p$-ranks by inspection of N-invariants column in Table 6.2, 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 have

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

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

$$C^N = \{0\}$$

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

Now the invariants and Euler characteristics follow easily from Table 4.1 in the proof of Theorem 4. The results are summarized in Table 6.3.

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

Table 6.3.

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

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

where $S_{\text{ram}}^{\text{split}}$ consists of those places in S which ramify in K_1/K but split in L/K_1, $S_{\text{split}}^{\text{ram}}$ consists of those places in S which split in K_1/K but ramify in L/K_1, and $S_{\text{ram}}^{\text{ram}}$ 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 extension of $\mathbb{Z}_p$-fields. For convenience, we define

$$\begin{aligned} i &:= i_1 + i_2 + \dots i_{p-2} \\ ii &:= ii_1 + ii_2 + \dots ii_p \\ iii &:= iii_1 + iii_2 + \dots iii_{p-1} \\ v &:= v_1 + v_2 + \dots v_{p-1} \end{aligned}$$

and

$$\begin{aligned} \alpha &:= c + i + ii + iii + iv + v \\ \beta &:= b - c + e - iv \\ \gamma &:= a - b + i + iv - v. \end{aligned}$$

Thus Lemma 1, Remark 2, and the above tables imply

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

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

and

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

Hence

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

which proves Proposition 6. Notice that we did not use α. We will make use of α in the proof of the following corollary. □

Corollary 7. *Let L/K be as in Proposition 6. Suppose $\mu_K = 0$. Then $\mu_{K_1} = \mu_L = 0$ and*

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

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

Although Corollary 7 follows easily from Proposition 6 combined with induction and Theorem 4, we'll give a direct proof here.

Proof. By Remark 2 and the tables in the proof of Proposition 6 we find

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

Therefore

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

and

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

which proves the corollary. □

Now we take note of a few immediate implications of Corollary 7.

Corollary 8. *Let L/K be as in Proposition 6. 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) $\lambda_L \equiv \chi(G/N, P_{K_1}) - |S_{\text{ram}}^{\text{split}}| - |S_{\text{ram}}^{\text{ram}}| = -\chi(G/N, A_{K_1}) \pmod{p}$
(4) $\lambda_L \equiv \chi(N, P_L) - p|S_{\text{split}}^{\text{ram}}| - |S_{\text{ram}}^{\text{ram}}| = -\chi(N, A_L) \pmod{p^2}$
(5) $\text{ord}_p|H^2(G, P_L)| \le 2\lambda_K + \text{ord}_p|H^1(G, P_L)| + |S_{\text{ram}}^{\text{split}}| + |S_{\text{split}}^{\text{ram}}| + 2|S_{\text{ram}}^{\text{ram}}|$

Proof. Corollary 7 immediately implies 1, 2, 3, and 4. To prove 5 we need only note that

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

which completes the proof. □

Remark 9. Let L/K be as in Proposition 6 with $\mu_K = 0$. As we'll see later, we don't need Theorem 5 to prove any of Proposition 6, Corollary 7, 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 6) that

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

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 (by computing the $\mathbb{Z}_p$-rank of A_L^*). 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 $\mathbb{Z}_pG$-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

$$\begin{aligned} B &\cong \frac{\mathbb{Z}_2G}{(g+1)}, \\ C &\cong \frac{\mathbb{Z}_2G}{(g^2+1)}, \\ V_1 &\cong \frac{\mathbb{Z}_2G}{(g+1)(g^2+1)} \end{aligned}$$

as $\mathbb{Z}_2G$-modules.

3.1. **A Counterexample.** Let L/K be as in Proposition 6 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 (see [Kid80]) and Theorem 4, it is natural to ask whether or not there is a constant c_p depending on p but not on L/K such that

$$\lambda_L \stackrel{?}{=} p^2\lambda_K - c_p\chi(G,P_L) + \sum_{w\nmid p}(e(w)-1). \tag{9.1}$$

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 Remark 7 implies that equation 9.1 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

$$-\chi(G,P_L) \stackrel{?}{=} -2\chi(G/N,P_{K_1}) + 2|S_{\text{ram}}^{\text{split}}|. \tag{9.2}$$

It's easy to show that equation 9.2 holds whenever $-\beta = |S_{\text{ram}}^{\text{split}}| + |S_{\text{split}}^{\text{ram}}|$ since then

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

and so

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

also, if $\beta = 0$, then

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

so

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

which means equation 9.2 holds in this case if and only if L/K is totally ramified, whence $|S_{\text{ram}}^{\text{split}}| + |S_{\text{split}}^{\text{ram}}| = 0 = -\beta$ is just a special case of the above. However, equation 9.2 appears to be false in general assuming Greenberg's conjecture that the lambda invariants for cyclotomic $\mathbb{Z}_p$-extensions of 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 $\chi(G/N,\mathcal{O}_{K_1}^\times) = -\chi(G/N,P_{K_1})$ and $\chi(N,\mathcal{O}_L^\times) = -\chi(N,P_L)$ when L/K is an extension of CM-fields and p is an odd prime. Namely,

$$\begin{aligned}\chi(G/N,\mathcal{O}_{K_1}^\times) &= \frac{\lambda_{K_1}-\lambda_K}{p-1} - |S_{\text{ram}}^{\text{split}}| - |S_{\text{ram}}^{\text{ram}}|\\ &= \frac{\lambda_{K_1}^- - \lambda_K^-}{p-1} - |S_{\text{ram}}^{\text{split}}| - |S_{\text{ram}}^{\text{ram}}|\\ &= -\delta - |S_{\text{ram}+}^{\text{split}+}| - |S_{\text{ram}+}^{\text{ram}+}|\end{aligned} \tag{9.3}$$

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

$$\chi(N,\mathcal{O}_L^\times) = -\delta - p|S_{\text{split}+}^{\text{ram}+}| - |S_{\text{ram}+}^{\text{ram}+}| \tag{9.4}$$

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 6. On the other hand, equation 9.2 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 9.3 and 9.4 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 10. Let $p = 3$ and consider the number field $\mathbb{Q}(\zeta_{133})$. We have

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

and under the isomorphism $a \mapsto (\zeta_{133} \mapsto \zeta_{133}^a)$ we have that $\ell := \mathbb{Q}(\zeta_{133})^{\langle -1\rangle} = \mathbb{Q}(\zeta_{133} + \zeta_{133}^{-1})$ is the maximal real subfield. Define

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

Then

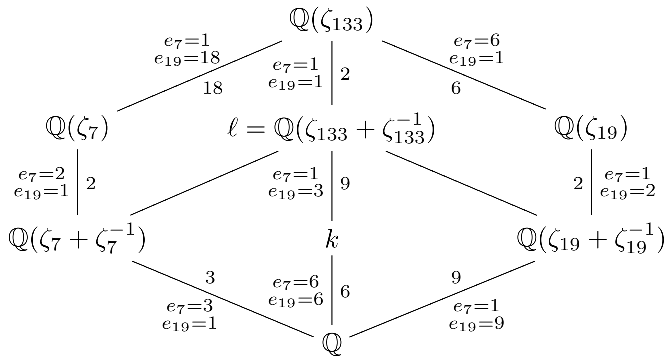
$$\text{Gal}(\ell/k) \cong \langle 4,-1\rangle/\langle -1\rangle = \langle 4\langle -1\rangle\rangle \cong \mathbb{Z}/(9),$$

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

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

There are four subfields of ℓ which have degree 3 over $\mathbb{Q}$. One of them is $\mathbb{Q}(\zeta_7+\zeta_7^{-1})$ in which 19 does not ramify, while one can use SAGE, for example, to check that the other three are ramified at 19. Specifically, $\mathbb{Q}(\zeta_{133})^{\langle 2,-1\rangle} \subseteq k$ has degree 3 over $\mathbb{Q}$ but does not contain $\zeta_7 + \zeta_7^{-1}$, so 19 ramifies in $\mathbb{Q}(\zeta_{133})^{\langle 2,-1\rangle}/\mathbb{Q}$. Also, $\mathbb{Q}(\zeta_{133})/\ell$ is unramified, 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 9.2 assuming that, at least in this case, $\lambda_{L^+} = \lambda_{K_1^+} = \lambda_{K^+} = 0$.

Remark 11. 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 6 without using the classification of indecomposable $\mathbb{Z}_p$-free $\mathbb{Z}_pG$-modules are given later in the chapter.

3.2. **An Alternative Proof for $\mathbb{Z}/(p^2)$-Extensions.** 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 5. In this section, we'll show how to rederive Proposition 6 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

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

Lemma 12. *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 $0 : A \to A : a \mapsto 0$ and $p : A \to A : a \mapsto pa$.

Theorem 13. *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 14. *Let G, N, and A be as in Theorem 13. 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

$$\begin{aligned}
h(G, A) &= h(G, A^G)h(G, A^{g-1}) = \mathrm{q}_{0,p^2}(A^G)h(G, A^{g-1}) \\
&= \mathrm{q}_{0,p^2}(A^G)h(G, (A^N)^{g-1})h(G, A^{g^p-1}) \qquad (14.1)
\end{aligned}$$

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

$$h(G, A^{g^p-1}) = \mathrm{q}_{g-1,0}(A^{g^p-1}) = \mathrm{q}_{0,g-1}(A^{g^p-1})^{-1} \tag{14.2}$$

and that Lemma 12 gives

$$\mathrm{q}_{0,p(g-1)}(A^{g^p-1}) = \mathrm{q}_{0,p}(A^{g^p-1})\mathrm{q}_{0,g-1}(A^{g^p-1}). \tag{14.3}$$

Of course, we also know that $\varphi_{p^2}(g)$ 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 $(g-1)^{p^2-p}$ and, consequently,

$$\mathrm{q}_{0,p(g-1)}(A^{g^p-1}) = \mathrm{q}_{0,(g-1)^{p^2-p+1}}(A^{g^p-1}) = \mathrm{q}_{0,g-1}(A^{g^p-1})^{p^2-p+1} \tag{14.4}$$

by repeated application of Lemma 12. Thus combining equations 14.2, 14.3, and 14.4, gives

$$\begin{aligned} h(G, A^{g^p-1})^{p^2-p} &\overset{14.2}{=} \mathrm{q}_{0,g-1}(A^{g^p-1})^{-(p^2-p)} = \frac{\mathrm{q}_{0,g-1}(A^{g^p-1})}{\mathrm{q}_{0,g-1}(A^{g^p-1})^{p^2-p+1}} \\ &\overset{14.4}{=} \frac{\mathrm{q}_{0,g-1}(A^{g^p-1})}{\mathrm{q}_{0,p(g-1)}(A^{g^p-1})} \overset{14.3}{=} \frac{1}{\mathrm{q}_{0,p}(A^{g^p-1})} \\ &= \frac{\mathrm{q}_{0,p}(A^N)}{\mathrm{q}_{0,p}(A)}. \end{aligned} \tag{14.5}$$

Therefore equations 14.1 and 14.5 together give

$$\begin{aligned} h(G,A)^{p(p-1)} &\overset{14.1}{=} \mathrm{q}_{0,p^2}(A^G)^{p(p-1)} h(G,(A^N)^{g-1})^{p(p-1)} h(G, A^{g^p-1})^{p(p-1)} \\ &\overset{14.5}{=} \mathrm{q}_{0,p^2}(A^G)^{p(p-1)} h(G,(A^N)^{g-1})^{p(p-1)} \frac{\mathrm{q}_{0,p}(A^N)}{\mathrm{q}_{0,p}(A)} \\ &= \mathrm{q}_{0,p^2}(A^G)^{p(p-1)} \left(\frac{h(G/N, A^N)}{h(G/N, A^G)}\right)^{p(p-1)} \frac{\mathrm{q}_{0,p}(A^N)}{\mathrm{q}_{0,p}(A)} \\ &= \mathrm{q}_{0,p^2}(A^G)^{p(p-1)} \frac{h(G/N, A^N)^{p(p-1)}}{\mathrm{q}_{0,p}(A^G)^{p(p-1)}} \cdot \frac{\mathrm{q}_{0,p}(A^N)}{\mathrm{q}_{0,p}(A)} \\ &\overset{\text{thm } 13}{=} \mathrm{q}_{0,p^2}(A^G)^{p(p-1)} \frac{\mathrm{q}_{0,p}(A^G)^{p^2}/\mathrm{q}_{0,p}(A^N)^p}{\mathrm{q}_{0,p}(A^G)^{p(p-1)}} \cdot \frac{\mathrm{q}_{0,p}(A^N)}{\mathrm{q}_{0,p}(A)} \\ &= \mathrm{q}_{0,p}(A^G)^{2p(p-1)} \frac{\mathrm{q}_{0,p}(A^G)^p}{\mathrm{q}_{0,p}(A^N)^p} \cdot \frac{\mathrm{q}_{0,p}(A^N)}{\mathrm{q}_{0,p}(A)} \\ &= \frac{\mathrm{q}_{0,p}(A^G)^{2p^2-p}}{\mathrm{q}_{0,p}(A)\mathrm{q}_{0,p}(A^N)^{p-1}} \end{aligned}$$

as claimed. □

Now we can put Theorems 13 and 14 together to relate various Herbrand quotients of subgroups and quotient groups.

Corollary 15. *Let G, N, and A be as in Theorem 13. 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 13 implies

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

On the other hand, Theorem 14 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

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

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 16. Once again, let G, N, and A be as in Theorem 13. Suppose $\mathrm{q}_{0,p^2}(A)$ is defined. Let $A = A_L$ where L/K, G, N are as Proposition 6. Then Corollary 15 holds 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 15 yields

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

so this along with Lemma 1 gives another proof of Proposition 6. We are also in position to give a proof of the formula in Remark 11. We use induction on Theorem 4 and Corollary 15 to find

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

but taking p-orders in the second statement of Corollary 15 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

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

which is precisely the formula in Remark 11.

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

In this section, 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 5) was unnecessary to prove Proposition 6. 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 17. *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 nonzero 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 19 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 18 (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*

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

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

Proposition 19. *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 $r_0, \dots, r_n \in \mathbb{N}_0$ such that for every subgroup $N_i = \langle g^{p^i} \rangle$ with $0 \le i \le n$ 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 17. 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 $0 \le i \le n = 0$ 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 $n \ge 1$ and the proposition is true for $n - 1$. By Lemma 17, 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 $r_0, \dots, r_{n-1} \in \mathbb{N}_0$ such that for every subgroup $N_i' = N_i/N_{n-1}$ with $0 \le i \le n - 1$ we have

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

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 18). 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, 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

$$\frac{M'^{N_i}}{(1 + g^{p^{n-1}} + \cdots + g^{p^{n-1}(p-1)})M'^{N_i'}} = \left(\frac{M'}{pM'}\right)^{N_i'} \cong H^2(N_{n-1}, M')^{N_i'}.$$

Therefore applying $\mathrm{ord}_p|-|$ to the exact sequence gives

$$\begin{aligned}\chi(N_i, M') - \chi(N_i', M') &= \mathrm{ord}_p\left(\frac{|H^2(N_{n-1}, M')^{N_i'}|}{|H^1(N_{n-1}, M')^{N_i'}|}\right) = \mathrm{ord}_p|M'^{N_i}/pM'^{N_i}| \\ &= \mathrm{rank}_{\mathbb{Z}_p}(M'^{N_i}) = \sum_{t=0}^{i} r_t\varphi(p^t)\end{aligned}$$

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 19 to prove generalizations of Propositions 6 and Corollary 7. 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.

Theorem 20. *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 19 to the $\mathbb{Z}_p G_n$-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

$$\begin{aligned} \lambda_{K_i} &= \mathrm{rank}_{\mathbb{Z}_p}(A^*_{K_i}) = \mathrm{rank}_{\mathbb{Z}_p}((A^*_{K_n})^{N_i}) = \sum_{t=0}^{i} r_t \varphi(p^t) \\ \chi(G_n, A_{K_n}) &= -\chi(N_0, A^*_{K_n}) = -nr_0 + \sum_{t=1}^{n} r_t \end{aligned}$$

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 21. *Under the same assumptions as Theorem 20, 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 4.) Now take $n \geq 1$. Suppose the statement holds for all cyclic p-extensions of degree $\leq p^{n-1}$. Then by Theorem 20 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 induction on Theorem 4 to get the following generalization of Proposition 6.

Corollary 22. *Under the same assumptions as Theorem 20, 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 21 and the second equality follows from induction on Theorem 4. □

Corollary 23. *Let $L/K = K_n/K_0$ be as in Theorem 20. Suppose $\mu_K = 0$. Then*

(1) $\lambda_L \equiv \lambda_{K_i} \pmod{\varphi(p^{i+1})}$ *for every* $i = 0, \dots, n$
(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) $\mathrm{ord}_p|H^2(G, P_L)| \le n\lambda_K + \mathrm{ord}_p|H^1(G, P_L)| + \chi(G, I_L)$

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 $i = 1, \dots, n$

$$\lambda_{K_i} \equiv \lambda_{K_{i-1}} \pmod{\varphi(p^i)}, \tag{23.1}$$

which we'll do by strong induction on n. The base case $n = 1$ follows easily from Theorem 4. Suppose then that Equation 23.1 holds for all $i < n$. Then for all $i = 1, \dots, n-1$

$$p^{n-i}(\lambda_{K_i} - \lambda_{K_{i-1}}) \equiv 0 \pmod{\varphi(p^n)},$$

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 20 while the second statement (b) follows immediately from Theorem 24 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 24. *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 25. *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

$$\begin{aligned}
&\sum_{i=1}^{n-1} \frac{p^i(p-1)i}{[(i+1)p-i][ip-i+1]} \\
=&\frac{p^{n-1}(p-1)(n-1)}{(np-n+1)((n-1)p-n+2)} + \sum_{i=1}^{n-2} \frac{p^i(p-1)i}{[(i+1)p-i][ip-i+1]} \\
=&\frac{p^{n-1}(p-1)(n-1)}{(np-n+1)((n-1)p-n+2)} + \frac{p^{n-2}+p^{n-3}+\cdots+1-(n-1)}{(n-1)p-n+2} \\
=&\frac{p^{n-1}(p-1)(n-1) + \left(\frac{p^{n-1}-1}{p-1} - (n-1)\right)(np-n+1)}{(np-n+1)((n-1)p-n+2)} \\
=&\frac{p^{n-1}(p-1)(n-1) + \left(\frac{p^{n-1}-1}{p-1} - (n-1)\right)(p-1)}{(np-n+1)((n-1)p-n+2)} + \frac{\frac{p^{n-1}-1}{p-1} - (n-1)}{np-n+1} \\
=&\frac{(p^{n-1}-1)(p-1)(n-1) + p^{n-1} - 1}{(np-n+1)((n-1)p-n+2)} + \frac{\frac{p^{n-1}-1}{p-1} - (n-1)}{np-n+1} \\
=&\frac{p^{n-1}-1}{np-n+1} + \frac{p^{n-2}+p^{n-3}+\cdots+1-(n-1)}{np-n+1} \\
=&\frac{p^{n-1}+p^{n-2}+\cdots+1-n}{np-n+1}
\end{aligned}$$

and

$$\begin{aligned}
&\sum_{i=1}^{n-1} \frac{1}{[(i+1)p-i][ip-i+1]} \\
=&\frac{1}{(np-n+1)((n-1)p-n+2)} + \sum_{i=1}^{n-2} \frac{1}{[(i+1)p-i][ip-i+1]} \\
=&\frac{1}{(np-n+1)((n-1)p-n+2)} + \frac{n-2}{p((n-1)p-n+2)} \\
=&\frac{p+(n-2)(np-n+1)}{p(np-n+1)((n-1)p-n+2)} \\
=&\frac{p+(n-2)(p-1)+(n-2)((n-1)p-n+2)}{p(np-n+1)((n-1)p-n+2)} \\
=&\frac{(n-1)p-n+2+(n-2)((n-1)p-n+2)}{p(np-n+1)((n-1)p-n+2)} = \frac{n-1}{p(np-n+1)}
\end{aligned}$$

as claimed. □

Proof of Theorem 24. 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 19 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 $i \in \{0, \dots, n\}$. 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

$$\begin{aligned}
& \frac{p^n}{np-n+1} + \varphi(p^t)\sum_{i=1}^{n-t} \frac{p^i(p-1)(i)}{[(i+1)p-i][ip-i+1]} + \\
& p^n(p-1)\sum_{i=n-t+1}^{n-1} \frac{1}{[(i+1)p-i][ip-i+1]} \\
= & \frac{p^n}{np-n+1} - p^{t-1}(p-1)\frac{\frac{p^{n-t+1}-1}{p-1} - (n-t+1)}{(n-t+1)p-(n-t+1)+1} + \\
& p^n(p-1)\left(\frac{n-1}{p(np-n+1)} - \frac{n-t}{p((n-t+1)p-(n-t+1)+1)}\right)
\end{aligned}$$

$$
\begin{aligned}
&= \frac{p^n + p^{n-1}(p-1)(n-1)}{np-n+1} - \\
&\quad \frac{p^t(p^{n-t+1} - 1 - (p-1)(n-t+1)) + p^n(p-1)(n-t)}{p((n-t+1)p-n+t)} \\
&= p^{n-1} - \frac{p^{n+1} - p^t((n-t+1)p-n+t) + (n-t)p^n(p-1)}{p((n-t+1)p-n+t)} \\
&= p^{n-1} + p^{t-1} - \frac{p^{n+1} + (n-t)p^n(p-1)}{p((n-t+1)p-n+t)} \\
&= p^{n-1} + p^{t-1} - p^n \frac{p + (n-t)(p-1)}{p((n-t+1)p-n+t)} \\
&= p^{n-1} + p^{t-1} - p^{n-1} = p^{t-1},
\end{aligned}
$$

which completes the proof. □

5. 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 5) 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 4. 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 26. *Let M be a finitely generated Λ-module. Then there is a Λ-module homomorphism*

$$\theta : M \to \Lambda^r \oplus \bigoplus_{i=1}^{s} \frac{\Lambda}{(f_i(T)^{m_i})} \oplus \bigoplus_{j=1}^{t} \frac{\Lambda}{(p^{n_j})}$$

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 19 follows as an easy corollary.

Proposition 27. *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

$$\Lambda \cong \varprojlim_{m\in\mathbb{N}} \mathbb{Z}_p[\mathbb{Z}/(p^m)] : T \mapsto (g_m - 1)_{m\in\mathbb{N}}$$

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 26 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 $\operatorname{im}(\theta)$ 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 $\operatorname{coker}(\theta)$ 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

$$\theta\colon M \rightarrowtail \bigoplus_{j=0}^{n} \left(\frac{\mathbb{Z}_p[x]}{(\Phi_{p^j}(x))}\right)^{\oplus r_j} \cong \bigoplus_{j=0}^{n} \left(\frac{\mathbb{Z}_pG}{\Phi_{p^j}(g)\mathbb{Z}_pG}\right)^{\oplus r_j}$$

is a $\mathbb{Z}_pG$-module homomorphism with finite cokernel. □

Remark 28. Let $M, G = \langle g\rangle \cong \mathbb{Z}/(p^n)$ be as in Proposition 27. As mentioned above, the proposition can be used to give another proof of Proposition 19. To see this, we observe that if C is a finite $\mathbb{Z}_pG$-module, then $\chi(N_i, C) = 0$ and $\operatorname{rank}_{\mathbb{Z}_p}(C^{N_i}) = 0$ for all $i \in \{0, \dots, n\}$ where (as in 19) $N_i = \langle g^{p^i}\rangle$. Thus since χ and $\operatorname{rank}_{\mathbb{Z}_p}$ are additive on short exact sequences, we see that it suffices to do the following computations:

$$\mathbb{Z}_p[\zeta_{p^j}]^{N_i} = \begin{cases} \mathbb{Z}_p[\zeta_{p^j}] & \text{if } j \le i \\ 0 & \text{if } j > i \end{cases}$$

$$\chi(N_i, \mathbb{Z}_p[\zeta_{p^j}]) = \operatorname{ord}_p\left(\frac{|H^2(N_i, \mathbb{Z}_p[\zeta_{p^j}])|}{|H^1(N_i, \mathbb{Z}_p[\zeta_{p^j}])|}\right)$$

$$= \begin{cases} \operatorname{ord}_p\left|\frac{\mathbb{Z}_p[\zeta_{p^j}]}{p^{n-i}\mathbb{Z}_p[\zeta_{p^j}]}\right| = (n-i)\varphi(p^j) & \text{if } j \le i \\ \operatorname{ord}_p\left|\frac{|\mathbb{Z}_p[\zeta_{p^j}]}{(1-\zeta_{p^j}^{p^i})\mathbb{Z}_p[\zeta_{p^j}]}\right|^{-1} = -p^i & \text{if } j > i. \end{cases}$$

6. $\mathbb{Q}_p$-Representations

Let $K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n = L$ be a tower of $\mathbb{Z}_p$ fields with $G_i = \operatorname{Gal}(K_i/K)$ and $N_i = \operatorname{Gal}(L/K_i) = \langle g^{p^i}\rangle \cong \mathbb{Z}/(p^i)$ for all $i \in \{0, \dots, n\}$. Assume $\mu_K = 0$ and define

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

Consider the corresponding representation

$$\pi_{L/K} : G \to \operatorname{GL}(V_L).$$

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

Corollary 29. *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*

$$\pi_{L/K} \cong \lambda_K \pi_G \oplus \bigoplus_{i=1}^{n} \big(\chi(G_i, A_{K_i}) - \chi(G_{i-1}, A_{K_{i-1}})\big)\, \pi_{\varphi(p^i)}$$

where π_G is the regular representation and π_d is the unique faithful irreducible representation of degree $d \in \{\varphi(p), \varphi(p^2), \dots, \varphi(p^n)\}$.

Proof. We'll use all the notation in the proof of Proposition 27. In the proof of 27 with $A_L^* = M$, we had $r_0, r_1, \dots, r_n \in \mathbb{N}_0$ such that

$$V_L \cong \bigoplus_{j=0}^{n} \left(\frac{\mathbb{Q}_p[x]}{(\Phi_{p^j}(x))}\right)^{\oplus r_j}$$

as $\mathbb{Q}_pG$-modules where our generator g of G acts as x on $\mathbb{Q}_p[x]$. Remark 28 shows that these $r_0, \dots, r_n$ are the same as those found in the proof of Theorem 20. In particular, this means $r_0 = \lambda_K$, so

$$V_L \cong (\mathbb{Q}_pG)^{\oplus \lambda_K} \oplus \bigoplus_{j=1}^{n} \left(\frac{\mathbb{Q}_p[x]}{(\Phi_{p^j}(x))}\right)^{\oplus r_j - r_0}$$

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

$$r_1 - r_0 = \chi(G_1, A_{K_1}),$$

$$r_2 - r_0 = r_1 + r_2 - 2r_0 - (r_1 - r_0) = \chi(G_2, A_{K_2}) - \chi(G_1, A_{K_1}),$$

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. □

7. 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 [FKOT97]. 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 30. *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 Z_pG-modules

$$(I_K P_L^G)/I_K \rightarrowtail I_L^G/I_K \twoheadrightarrow I_L^G/(I_K PL^G).$$

Also, $I_K \cap P_L^G = P_K$ since

$$(I_K \cap P_L^G)/P_K \subseteq A_K \cong 0$$

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 1. □

Theorem 31. *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 30 and Lemma 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 21 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

$$\mathrm{ord}_p|H^2(G_i, \mathcal{O}_{K_i}^\times)| = \mathrm{ord}_p|(I_{K_i}^{G_i} P_{K_i})/(I_K P_{K_i})| = 0. \tag{31.1}$$

To complete the proof, it suffices to show that if Equation 31.1 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 $(I_{K_i}^{G_i} P_{K_i}) \cap I_K P_L = I_K P_{K_i}$. ∎

We'll need the following theorem to prove our next lemma.

Theorem 32. *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

$$J_{\ell/k} : C_k \to C_\ell$$

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 here. The reader is referred to [Gre10].

Lemma 33. *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 having exactly one place lying above p and class number $h(k)$ with $p \nmid h(k)$. Then*

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

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

Proof. Here we adapt and generalize the method of proof for a weaker statement found in [FKOT97]. 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 32 on the extension k_n/k_m with $G_{n/m} = \operatorname{Gal}(k_n/k_m)$ we find that for all $m, n \in \mathbb{N}_0$ with $m \leq n$

$$\begin{aligned}\left|\frac{\mathcal{O}_{k_m}^\times}{N_{k_n/k_m}(\mathcal{O}_{k_n}^\times)}\right| &= |H^2(G_{n/m}, \mathcal{O}_{k_n}^\times)| = p^{-(n-m)}|H^1(G_{n/m}, \mathcal{O}_{k_n}^\times)| \\ &= p^{-(n-m)} e(\mathfrak{p}_n/\mathfrak{p}_m)\frac{|\ker(J_{k_n/k_m})|}{|C_{k_n}^{[G_{n/m}]}/J_{k_n/k_m}(C_{k_m})|} \\ &= p^{-(n-m)}p^{n-m}\frac{|C_{k_m}|}{\left|C_{k_n}^{[G_{n/m}]}\right|} = 1\end{aligned}$$

where the last equality follows because $H^2(G_{n/m}, \mathcal{O}_{k_n}^\times)$ is a p-group and $\operatorname{ord}_p|C_{k_m}| = \operatorname{ord}_p|C_{k_n}^{[G_{n/m}]}| = 0$. 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 $\operatorname{Gal}(\ell/k) \cong \operatorname{Gal}(L/K) \cong \mathbb{Z}/(p^d)$, then the induced maps

$$\widetilde{N}_{k_n/k_m} : \frac{\mathcal{O}_{k_n}^\times}{N_{\ell_n/k_n}(\mathcal{O}_{\ell_n}^\times)} \longrightarrow \frac{\mathcal{O}_{k_m}^\times}{N_{\ell_m/k_m}(\mathcal{O}_{\ell_m}^\times)}$$

are surjective for all $m, n \in \mathbb{N}_0$ with $m \leq n$. On the other hand, using Theorem 32 on the extension ℓ_n/k_n with $G_n = \operatorname{Gal}(\ell_n/k_n) \cong \operatorname{Gal}(L/K) \cong \mathbb{Z}/(p^d)$ 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

$$\widetilde{\rho}_{k_n/k_m} : \frac{\mathcal{O}_{k_m}^\times}{N_{\ell_m/k_m}(\mathcal{O}_{\ell_m}^\times)} \longrightarrow \frac{\mathcal{O}_{k_n}^\times}{N_{\ell_n/k_n}(\mathcal{O}_{\ell_n}^\times)}$$

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 34. *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 having exactly one place lying above p and class number $h(k)$ with $p \nmid h(k)$. Then $\lambda_L = 0$ if and only if $\mathrm{ord}_p|(I_L^G P_L)/(I_K P_L)| = 0$.*

Proof. The theorem follows immediately from Theorem 31 since the assumptions we've made ensure that conditions (i) and (ii) hold. □

References

[AT09] E. Artin and J.T. Tate, *Class field theory*, AMS Chelsea Pub., 2009.

[CR66] Charles W. Curtis and Irving Reiner, *Representation theory of finite groups and associative algebras*, Interscience Publishers, 1966.

[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** (1997), no. 2, 475–480.

[Gre10] Ralph Greenberg, *Topics in Iwasawa theory*, math.washington.edu/, 2010.

[HR62] A. Heller and I. Reiner, *Representations of cyclic groups in rings of integers, I*, The Annals of Mathematics **76** (1962), no. 1, 73–92.

[HR63] ______, *Representations of cyclic groups in rings of integers, II*, The Annals of Mathematics **77** (1963), no. 2, 318–328.

[HS97] P. J. Hilton and U. Stammbach, *A couse in homological algebra*, second ed., Springer, 1997.

[Iwa81] Kenkichi Iwasawa, *Riemann-Hurwitz formula and p-adic Galois representations for number fields*, Tohoku Math. J. (2) **33** (1981), no. 2, 263–288.

[Kid80] Yûji Kida, *l-extensions of CM-fields and cyclotomic invariants*, J. Number Theory **12** (1980), no. 4, 519–528.

[Par66] J. T. Parr, *Cohomology of cyclic groups of prime square order*, Pacific Journal of Mathematics **17** (1966), no. 3, 467–473.

[Rei61] Irving Reiner, *The Krull-Schmidt theorem for integral group representations*, Bull. Amer. Math. Soc. **67** (1961), no. 4, 365–367.

[Was96] Lawrence C. Washington, *Introduction to cyclotomic fields*, second ed., Springer, 1996.