



ELSEVIER

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt



An alternative approach to Kida and Ferrero's computations of Iwasawa λ -invariants

Jordan Schettler

ARTICLE INFO

Article history:

Received 11 November 2012

Accepted 20 November 2013

Available online 30 January 2014

Communicated by D. Burns

Keywords:

Iwasawa

Lambda invariant

Hurwitz formula

Fermat prime

Ferrero

Kida

Imaginary quadratic

ABSTRACT

We prove a slight generalization of Iwasawa's 'Riemann–Hurwitz' formula for number fields and use it to generalize Kida and Ferrero's well-known computations of Iwasawa λ -invariants for the cyclotomic \mathbb{Z}_2 -extensions of imaginary quadratic number fields. In particular, we show that if p is a Fermat prime, then similar explicit computations of Iwasawa λ -invariants hold for certain imaginary quadratic extensions of the unique subfield $k \subset \mathbb{Q}(\zeta_{p^2})$ such that $[k : \mathbb{Q}] = p$. In fact, we actually prove more by explicitly computing cohomology groups of principal ideals. The computation of lambda invariants obtained is a special case of a much more general result concerning relative lambda invariants for cyclotomic \mathbb{Z}_2 -extensions of CM number fields due to Yûji Kida. However, the approach used here significantly differs from that of Kida, and the intermediate computations of cohomology groups found here do not hold in Kida's more general setting.

© 2014 Elsevier Inc. All rights reserved.

1. Introduction

Fix a prime p and number field k . Suppose k_∞ is a \mathbb{Z}_p -extension of k , i.e., k_∞ is a Galois extension of k with Galois group $\text{Gal}(k_\infty/k)$ isomorphic to the group \mathbb{Z}_p of p -adic integers. The subfields of k_∞ which contain k all lie in a tower

$$k = k_0 \subset k_1 \subset k_2 \subset \cdots \subset k_\infty$$

with $\text{Gal}(k_n/k) \cong \mathbb{Z}/(p^n)$ for all integers $n \geq 0$. Kenkichi Iwasawa's well-known growth formula (see [Iwa59] or [Iwa73a]) states that there are integers λ, μ, ν such that if A_n denotes the p -primary part of the class group of k_n , then

$$|A_n| = p^{\lambda \cdot n + \mu \cdot p^n + \nu}$$

for all sufficiently large integers n . In particular, $\lambda, \mu \geq 0$ but we can have $\nu < 0$. We call λ, μ, ν the Iwasawa invariants of the extension k_∞/k . There is a special case in which all the invariants are known to vanish.

Theorem 1. (See Iwasawa [Iwa59].) *Let k be a number field having exactly one prime \mathfrak{p} lying over a rational prime p , and let k_∞ be a \mathbb{Z}_p -extension of k . Suppose p does not divide the class number of k . Then for every number field $k_n \subset k_\infty$ which contains k , the prime \mathfrak{p} ramifies totally in k_n/k and p does not divide the class number of k_n ; in particular, all of the Iwasawa invariants for k_∞/k are zero, i.e., $\lambda = \mu = \nu = 0$.*

For every prime p and number field k , there is at least one \mathbb{Z}_p -extension of k ; namely, there is a unique \mathbb{Z}_p -extension of k contained in $\bigcup_{n \geq 0} k(\zeta_{p^n})$ where the ζ_{p^n} are primitive p^n th roots of unity. We denote this \mathbb{Z}_p -extension by k_∞^{cyc} and call it the cyclotomic \mathbb{Z}_p -extension of k . We write $\lambda_p(k), \mu_p(k), \nu_p(k)$ for the Iwasawa invariants of the extension k_∞^{cyc}/k . Conjecturally, the only \mathbb{Z}_p -extension of a totally real number field is the cyclotomic one, and this is known for \mathbb{Q} and real quadratic number fields, for example.

Iwasawa conjectured that $\mu_p(k) = 0$ for all primes p and number fields k , and no counterexamples are known.¹ This conjecture has been verified for abelian number fields by Bruce Ferrero and Lawrence Washington [FW79] and for p -extensions of number fields k with $\mu_p(k) = 0$ by Iwasawa [Iwa73b]. We make the assumption $\mu_p(k) = 0$ throughout the paper.

Bruce Ferrero and Yûji Kida independently calculated $\lambda_2(k)$ for imaginary quadratic fields k . Their computations are explicit:

Theorem 2. (See Ferrero [Fer80]; Kida [Kid79].) *Let $d > 2$ be a squarefree integer. Then*

$$\lambda_2(\mathbb{Q}(\sqrt{-d})) = -1 + \sum_{\substack{p|d \\ p \neq 2}} 2^{\text{ord}_2(p^2-1)-3} \quad (2.1)$$

where the sum ranges over all odd primes p dividing d .

Here $\text{ord}_2(n)$ denotes the 2-adic order of an integer n , i.e., the largest exponent e such that $2^e | n$. Thus, for example, if p is a prime with $p \equiv \pm 3 \pmod{8}$, then $\text{ord}_2(p^2-1) = 3$, so $\lambda_2(\mathbb{Q}(\sqrt{-p})) = -1 + 2^{3-3} = 0$. In fact, there are infinitely many such primes, so

¹ However, there are non-cyclotomic \mathbb{Z}_p -extensions of number fields which have an Iwasawa invariant $\mu > 0$.

for any integer $m \geq 0$ there are infinitely many choices of $m + 1$ such distinct primes p_1, \dots, p_{m+1} , and we get $\lambda_2(\mathbb{Q}(\sqrt{-p_1 p_2 \cdots p_{m+1}})) = m$.

In [Kid82], Kida further provided a less explicit computation of $\lambda_2^-(k)$ for any CM number field k . In more detail, let k^+ denote the maximal real subfield of k , and let $A^*(k_n^+)$ denote the 2-primary part of the narrow class group of the n th level k_n^+ in the cyclotomic \mathbb{Z}_2 -extension k_∞^+ of k^+ . Kida showed under mild assumptions² that for sufficiently large n we have

$$\lambda_2^-(k) := \lambda_2(k) - \lambda_2(k^+) = \delta - \tau - 1 + \dim_{\mathbb{F}_2} A^*(k_n^+)/A^*(k_n^+)^2 + s_n(k/k^+) \quad (2.2)$$

where δ is 1 or 0 depending on whether or not k_∞^{cyc} contains a primitive 4th root of unity, τ is 1 or 0 depending on whether or not the ramification indices of the primes dividing 2 in $k_\infty^+/ \mathbb{Q}_\infty$ are all even, and $s_n(k/k^+)$ denotes the number finite primes of k_n^{cyc} which ramify in k_n^{cyc}/k_n^+ and do not divide 2.

We will recover Eq. (2.2) for certain CM number fields k having $\delta = \tau = \dim_{\mathbb{F}_2} A^*(k_n^+)/A^*(k_n^+)^2 = 0$ for all n . To do so, we will make use of a general Hurwitz formula for number fields. Such a formula was first proven by Kida in [Kid80] for p -extensions of CM number fields with p an odd prime and then more generally by Iwasawa in [Iwa81] for p -extensions of number fields in which no infinite primes ramify and includes the case $p = 2$. Both formulas need $\mu = 0$ assumptions. We will use a generalization of Iwasawa's formula which does not need this assumption on the ramification of infinite places. In particular, we will be able to apply this general formula directly to an extension $\ell/k = \ell/\ell^+$ of a CM number field ℓ over its maximal real subfield $k = \ell^+$. Kida does not use this method in [Kid82] to derive Eq. (2.2); rather, Kida uses formula (2.2) to establish a Hurwitz formula for CM-fields and the prime $p = 2$.

These Hurwitz formulas for number fields mentioned above have their genesis in an idea coming from Iwasawa in [Iwa65] where he argued that when $\mu_p(k) = 0$, the invariant $\lambda_p(k)$ is a good analog for twice the genus of a curve.

2. Iwasawa's 'Riemann–Hurwitz' formula revisited

Following Iwasawa, we define a \mathbb{Z}_p -field to be the cyclotomic \mathbb{Z}_p -extension field of a number field. In other words, K is a \mathbb{Z}_p -field when $K = k_\infty^{\text{cyc}}$ for the prime p . Note that if $k_\infty^{\text{cyc}} = \ell_\infty^{\text{cyc}}$ for some prime p and number fields k, ℓ , then $\lambda_p(k) = \lambda_p(\ell)$ and we have $\mu_p(k) = 0 \Leftrightarrow \mu_p(\ell) = 0$. Thus for a \mathbb{Z}_p -field K we may define λ_K to be the Iwasawa λ -invariant $\lambda_p(k)$ for any number field k with $K = k_\infty^{\text{cyc}}$. Likewise, we may define the notation $\mu_K = 0$ to indicate that $\mu_p(k) = 0$ for some (and hence every) number field k such that $K = k_\infty^{\text{cyc}}$.

² We need only assume that $\mu_2^*(k^+) = 0$ where $\mu_2^*(k^+)$ is the “narrow” mu-invariant, i.e., the mu-invariant in the Iwasawa's growth formula for the narrow class numbers h_n^* of k_n^+ .

Table 1

Similarities in structures of Picard groups.

If K is the function field of a smooth, projective curve X over \mathbb{C} , then the local rings of X at closed points are DVRs, and the p -primary part of the Picard group satisfies $\text{Pic}(X)[p^\infty] \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{2g_K}$ where g_K is the genus	If K is a \mathbb{Z}_p -field with $\mu_K = 0$ and $X = \text{Spec}(\mathcal{O}_K[1/p])$, then the local rings of X at closed points are DVRs, and the p -primary part of the Picard group satisfies $\text{Pic}(X)[p^\infty] \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{\lambda_K}$ where λ_K is an Iwasawa invariant
---	---

Theorem 3. Suppose K is a \mathbb{Z}_p -field. Let I_K denote the group of invertible fractional ideals in the integer ring \mathcal{O}_K of K , and let $P_K \leq I_K$ denote the subgroup of principal fractional ideals. Then the p -primary part A_K of the class group $C_K = I_K/P_K$ satisfies

$$A_K \cong (\mathbb{Q}_p/\mathbb{Z}_p)^{\lambda_K} \oplus M$$

where $p^n M = 0$ for some $n \geq 0$. Moreover, M is trivial precisely when $\mu_K = 0$.

This structure theorem, whose proof may be gleaned from [Iwa59] and [Iwa73a], allows us to pin down the analogy between number fields and curves in the spirit of [Iwa65]. The analogy is illustrated in Table 1. A few remarks are in order. The ring \mathcal{O}_K is not Noetherian, but by inverting p , the resulting ring $\mathcal{O}_K[1/p]$ is actually a Dedekind domain, so its prime spectrum is a nice scheme which shares many properties with curves. This also helps to explain why the ramification for the prime p is missing in Iwasawa’s ‘Riemann–Hurwitz’ formula; however, we will not use this interpretation in the proof of Iwasawa’s formula, but the so-called Dedekind different formula implies that a purely geometric proof of Iwasawa’s result should exist. Before stating Iwasawa’s ‘Riemann–Hurwitz’ formula, we need a definition.

Definition 4. Let G be a cyclic p -group. For a G -module M , define the ‘Euler characteristic’ $\chi(G, M) \in \mathbb{Z}$ to be the exponent of p in the Herbrand quotient

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

when both cohomology groups $H^i(G, M)$ are finite for $i = 1, 2$. Note that χ inherits the following properties from the Herbrand quotient:

1. χ is additive on short exact sequences of G -modules³
2. $\chi(G, M) = 0$ when M is a finite G -module
3. $\chi(G, M^*) = -\chi(G, M)$ when $M^* = \text{Hom}_{\mathbb{Z}_p}(M, \mathbb{Q}_p/\mathbb{Z}_p)$ is the p -Pontryagin dual of a $\mathbb{Z}_p G$ -module M .

³ If $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$ is a SES of G -modules and two of the numbers $\chi(G, A)$, $\chi(G, B)$, $\chi(G, C)$ are finite (i.e., well-defined), then so is the other and $\chi(G, A) - \chi(G, B) + \chi(G, C) = 0$.

Table 2Cohomology for $\mathbb{Z}_p G$ -Modules.

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

Theorem 5 (Iwasawa's ‘Riemann–Hurwitz’ formula). Let L/K be a $\mathbb{Z}/(p)$ -extension of \mathbb{Z}_p -fields with $G = \text{Gal}(L/K)$. Suppose $\mu_K = 0$. Then $\mu_L = 0$ and

$$\lambda_L = p\lambda_K - (p-1)\chi(G, P_L) + \sum_{w \nmid p} (e(w) - 1) \quad (5.1)$$

where the sum ranges over all finite places w of L not lying above p , $e(w)$ is the ramification index of w in L/K , and G acts in the obvious way on the principal fractional ideals P_L of the integer ring \mathcal{O}_L in L .

Remark 6. If the extension L/K in Theorem 5 is unramified at the infinite places (always true, e.g., when p is odd), then Iwasawa showed that $H^2(G, L^\times) = 0$, so additivity of the ‘Euler characteristic’ χ shows that $-\chi(G, P_L) = \chi(G, \mathcal{O}_L^\times)$, which recovers the formula as originally stated by Iwasawa in [Iwa81].

Proof of Theorem 5. Using the notation of Theorem 3 above, we let A_L denote the p -primary part of the class group $C_L = I_L/P_L$ where again I_L, P_L are the groups of invertible and principal, respectively, fractional ideals of the integer ring \mathcal{O}_L . The statement that $\mu_L = 0$ follows from $\mu_K = 0$ by a result mentioned above (see [Iwa73b]) since L/K is a p -extension, so the structure theorem implies

$$A_L^* = \text{Hom}_{\mathbb{Z}_p}(A_L, \mathbb{Q}_p/\mathbb{Z}_p) \cong \text{Hom}_{\mathbb{Z}_p}((\mathbb{Q}_p/\mathbb{Z}_p)^{\lambda_L}, \mathbb{Q}_p/\mathbb{Z}_p) \cong \mathbb{Z}_p^{\lambda_L}$$

as \mathbb{Z}_p -modules. On the other hand, we have the following classification theorem.

Theorem 7. (See Diederichsen [Die40].) Let $\langle g \rangle = G \cong \mathbb{Z}/(p)$. The only indecomposable $\mathbb{Z}_p G$ -modules which are free of finite rank over \mathbb{Z}_p are (up to isomorphism) \mathbb{Z}_p , $\mathbb{Z}_p G$, and the augmentation ideal $I_p G = (g-1)\mathbb{Z}_p G$.

Hence

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

as $\mathbb{Z}_p G$ -modules for some nonnegative integers a, b, c . It is easy to compute the \mathbb{Z}_p -ranks, G -invariants, and Euler characteristics, of these indecomposables. The results are summarized in Table 2. Moreover, if S is the set of finite places of K which do not lie above p and ramify in L/K , then Iwasawa showed in [Iwa81] that

$$\chi(G, I_L) = |S|.$$

Also, the last column in Table 2 implies

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

Hence duality gives

$$\chi(G, A_L) = -\chi(G, A_L^*) = -a + c,$$

but

$$\chi(G, C_L) = \chi(G, A_L)$$

since G is a p -group and C_L is torsion, so $\chi(G, P_L)$ is also finite and additivity gives

$$-\chi(G, P_L) + |S| = -\chi(G, P_L) + \chi(G, I_L) = \chi(G, C_L) = -a + c.$$

Also, the natural map

$$A_K \rightarrow A_L^G$$

has finite kernel and finite cokernel since the same is true of $C_K \rightarrow C_L^G$ as may be seen from the snake lemma. Thus the first two columns in Table 2 show that

$$\lambda_K = \text{rank}_{\mathbb{Z}_p}(A_K^*) = \text{rank}_{\mathbb{Z}_p}((A_L^G)^*) = \text{rank}_{\mathbb{Z}_p}((A_L^*)^G) = a \cdot 1 + b \cdot 1 + c \cdot 0 = a + b.$$

Putting all of this together, we get

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

as needed. We have shown more than just a formula for the λ -invariants; 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 for some nonnegative integer a with $\chi(G, P_L) - |S| \leq a \leq \lambda_K$. \square

3. Main result

Theorem 8. Suppose p is a prime of the form $2^t + 1$ for some integer $t \geq 0$ and let $d > 2$ be a squarefree integer such that $(d, p) \leq 2$. Take k to be the unique real subfield of $\mathbb{Q}(\zeta_{2p^2})$ such that $[k : \mathbb{Q}] = p$, and take $K = k_\infty^{\text{cyc}}$ to be the cyclotomic \mathbb{Z}_2 -extension of k . If the class number h_k of k is odd (e.g., we can take $p \in \{2, 3, 5, 17, 257\}$), then

$$|H^1(G, P_L)| = 1 \quad \text{and} \quad |H^2(G, P_L)| = 2$$

where $L = K(\sqrt{-d})$, $G = \text{Gal}(L/K)$, and P_L denotes the principal fractional ideals of L . In particular, we have $\chi(G, P_L) = 1$, and [Theorem 5](#) implies the following special case of [\[Kid82\]](#):

$$\lambda_2(k(\sqrt{-d})) = -1 + |S|$$

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

Remark 9. Note that the field k in [Theorem 8](#) is the first layer in the cyclotomic \mathbb{Z}_p -extension of \mathbb{Q} . Thus when $p = 2$, [Theorem 8](#) precisely recovers [Theorem 2](#) since, in that case, $K = k_\infty^{\text{cyc}} = \mathbb{Q}_\infty$ is the cyclotomic \mathbb{Z}_2 -extension of \mathbb{Q} and for each odd prime q there are exactly $2^{\text{ord}_2(q^2-1)-3}$ primes of $\mathbb{Q}_\infty^{\text{cyc}}$ which lie above q .

Proof of Theorem 8. We first apply the general form of Iwasawa's ‘Riemann–Hurwitz’ formula (Eq. (5.1)) to the extension L/K of \mathbb{Z}_2 -fields where we take $L = K(\sqrt{-d}) = \ell_\infty^{\text{cyc}}$ to be the cyclotomic \mathbb{Z}_2 -extension of $\ell = k(\sqrt{-d})$ and as above $G = \text{Gal}(L/K)$. We get

$$\lambda_2(k(\sqrt{-d})) = \lambda_L = 2\lambda_K - \chi(G, P_L) + |S|.$$

Thus it suffices to show that $\lambda_K = 0$, $|H^1(G, P_L)| = 1$, and $|H^2(G, P_L)| = 2$.

First, we prove that $\lambda_K = 0$ using [Theorem 1](#). We have assumed that h_k is odd, and, in fact, this assumption is valid⁴ for $p \in \{2, 3, 5, 17, 257\}$. Hence it is enough to show that k has exactly one prime lying above 2. When $p = 2$, this is clear since $k = \mathbb{Q}(\sqrt{2})$, so we may assume $p = 2^t + 1$ for some integer $t \geq 1$. Of course, we must have $t = 2^r$ (i.e., $p = F_r = 2^{2^r} + 1$ is a prime Fermat number) for some integer $r \geq 0$. For every $j \geq 1$, we can factor

$$F_j - 2 = 2^{2^j} - 1 = F_0 F_1 \cdots F_{j-1}$$

as a product of consecutive Fermat numbers $F_i = 2^{2^i} + 1$. This identity shows that Fermat numbers are pairwise relatively prime, so $p^2 \nmid 2^{2^j} - 1$ for any $j \geq 0$ since $p = F_r$ is a prime Fermat number. This means that the multiplicative order of 2 modulo p^2 is

⁴ This follows, e.g., from results of Humio Ichimura and Shoichi Nakajima; see Proposition 1 and its proof in Section 3 of [\[IN10\]](#).

not a power of 2 which forces the residue degree of 2 in $\mathbb{Q}(\zeta_{p^2}) = \mathbb{Q}(\zeta_{2p^2})$ to be divisible by p . Consequently, the residue degree of 2 in k is p , which is equivalent to 2 being inert in k . Hence $\lambda_K = 0$.

It remains to show that $|H^1(G, P_L)| = 1$ and $|H^2(G, P_L)| = 2$. First, we fix some notation. Write out the towers for the \mathbb{Z}_2 -extensions K/k and $L/\ell = K(\sqrt{-d})/k(\sqrt{-d})$ as

$$k \subset k_1 \subset k_2 \subset \cdots \subset k_\infty := K, \quad \ell \subset \ell_1 \subset \ell_2 \subset \cdots \subset \ell_\infty := L.$$

Note that we have dropped the superscripted cyclotomic “cyc” notation for convenience. In this way,

$$\text{Gal}(k_n/k) \cong \text{Gal}(\ell_n/\ell) \cong \mathbb{Z}/(2^n) \quad \text{for all positive integers } n \in \mathbb{N}$$

and

$$G_n := \text{Gal}(\ell_n/k_n) \cong \mathbb{Z}/(2) \quad \text{for all indices } n \in \mathbb{N} \cup \{\infty\}.$$

Thus we have exact sequences

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

and we have norm maps $N_n: \ell_n \rightarrow k_n$ for all indices $n \in \mathbb{N} \cup \{\infty\}$. In this case, $N_n(\alpha) = \alpha\bar{\alpha} = |\alpha|^2$ is just the square modulus since the restriction of complex conjugation generates G_n for all indices $n \in \mathbb{N} \cup \{\infty\}$. Thus the images of these norms maps consist entirely of totally positive⁵ elements.

Now we need a theorem. It generalizes a result of Weber’s (see Sätze 6 and 25 in [Has52]) which Ferrero used in [Fer80].

Theorem 10. (See Hughes and Mollin [HM83].) *Let F'/F be a cyclic 2-extension of real abelian number fields. Suppose $\text{Gal}(F/\mathbb{Q})$ has exponent n such that -1 is congruent to a power of 2 modulo n , and, if $F \neq F'$, suppose that exactly one prime ramifies in F'/F . If the class number h_F of F is odd, then every totally positive element of $\mathcal{O}_{F'}^\times$ is a square in $\mathcal{O}_{F'}^\times$.*

For all $n \in \mathbb{N}$ we apply Theorem 10 to the extension $F'/F = k_n/k$ to get

$$\mathcal{O}_{k_n}^\times \cap N_\infty(L^\times) = (\mathcal{O}_{k_n}^\times)^2 = N_n(\mathcal{O}_{\ell_n}^\times) \quad (10.1)$$

where $(\mathcal{O}_{k_n}^\times)^2$ denotes the subgroup of squares of units. In fact, taking unions shows that Eq. (10.1) also holds for $n = \infty$, so

⁵ Recall that an algebraic number α is called totally positive if the images of α under every embedding $\mathbb{Q}(\alpha) \hookrightarrow \mathbb{C}$ are real and positive.

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

and likewise $H^1(G_n, P_{\ell_n}) = 0$ for all $n \in \mathbb{N}$.

Hence it remains only to show that $|H^2(G, P_L)| = 2$. To do this, we first prove $|H^1(G, \mathcal{O}_L^\times)| = 2$ and then show that the surjection $H^2(G, P_L) \rightarrow H^1(G, \mathcal{O}_L^\times)$ is also an injection.

For each $n \in \mathbb{N}$, let $t_\infty(n)$ denote the number of infinite places of k_n which ramify in ℓ_n/k_n . Since k_n is totally real and ℓ_n is totally complex, $t_\infty(n) = [k_n : \mathbb{Q}]$ is just the number of real places of k_n , so Dirichlet's unit theorem gives

$$\mathcal{O}_{k_n}^\times \cong \mathbb{Z}^{t_\infty(n)+0-1} \oplus \frac{\mathbb{Z}}{(2)}$$

as abelian groups. Then using [Theorem 10](#) again shows

$$\begin{aligned} |H^2(G_n, \mathcal{O}_{\ell_n}^\times)| &= \left| \frac{\mathcal{O}_{k_n}^\times}{(\mathcal{O}_{k_n}^\times)^2} \right| = \left| \frac{\mathbb{Z}^{t_\infty(n)-1} \oplus (\mathbb{Z}/(2))}{2(\mathbb{Z}^{t_\infty(n)-1} \oplus (\mathbb{Z}/(2)))} \right| \\ &= 2^{t_\infty(n)-1+1} = 2^{t_\infty(n)}. \end{aligned} \quad (10.2)$$

Now we state another needed result, whose proof may be found, for example, in [\[Gre10\]](#).

Theorem 11. *Suppose F'/F is a quadratic extension of number fields and let t_∞ denote the number of infinite places of F which ramify in F' . Then*

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

We now apply [Theorem 11](#) for the extension $F'/F = \ell_n/k_n$ to conclude that

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

for all positive integers $n \in \mathbb{N}$ since we have already shown in Eq. (10.2) above that $|H^2(G_n, \mathcal{O}_{\ell_n}^\times)| = 2^{t_\infty(n)}$. On the other hand, for $n \in \mathbb{N} \cup \{\infty\}$ we have

$$U_n/V_n \cong H^1(G_n, \mathcal{O}_{\ell_n}^\times)$$

where U_n is the norm 1 units in \mathcal{O}_{ℓ_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 for all indices $n \in \mathbb{N} \cup \{\infty\}$. We need the following lemma which we do not prove here but is not hard to establish (see, for example, Lemma 6.15 in [\[Sch12\]](#)).

Lemma 12. *Let $d > 1$ be a squarefree integer. Suppose F is a number field with discriminant Δ_F such that $(d, \Delta_F) \leq 2$. Then $4\mathcal{O}_{F(\sqrt{-d})} \subseteq \mathcal{O}_F + \sqrt{-d}\mathcal{O}_F$.*

Suppose contrary to the claim that $-1 = \bar{u}/u \in V_n$ for some $u \in \mathcal{O}_{\ell_n}^\times$ and some positive integer $n \in \mathbb{N}$. Then both u and u^{-1} are in \mathcal{O}_{ℓ_n} , so since $u = -\bar{u}$ and $u^{-1} = -\overline{u^{-1}}$ the lemma implies

$$u = \frac{a\sqrt{-d}}{4} \quad \text{and} \quad u^{-1} = \frac{b\sqrt{-d}}{4}$$

for some $a, b \in \mathcal{O}_{k_n}$. 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 $d > 2$. Thus for each $n \in \mathbb{N}$ we know that $-1 \notin V_n$ and $|U_n/V_n| = 2$, so U_n/V_n is generated by the coset of -1 . It follows that $H^1(G, \mathcal{O}_L^\times) \cong U_\infty/V_\infty$ is also generated by the coset of -1 and has order 2 since

$$U_\infty = \bigcup_{n \in \mathbb{N}} U_n = \bigcup_{n \in \mathbb{N}} \langle -1 \rangle V_n = \langle -1 \rangle V_\infty \quad \text{and} \quad -1 \notin \bigcup_{n \in \mathbb{N}} V_n = V_\infty.$$

To summarize, we have an exact sequence

$$0 \rightarrow H^2(G, \mathcal{O}_L^\times) \rightarrow H^2(G, L^\times) \rightarrow H^2(G, P_L) \rightarrow H^1(G, \mathcal{O}_L^\times) \rightarrow 0$$

where $|H^1(G, \mathcal{O}_L^\times)| = 2$, so to prove $|H^2(G, P_L)| = 2$ (and thus finish the proof of [Theorem 8](#)) we only need to show that the map $H^2(G, \mathcal{O}_L^\times) \rightarrow H^2(G, L^\times)$ is onto since that would imply the map $H^2(G, L^\times) \rightarrow H^2(G, P_L)$ is trivial and, consequently, that the map $H^2(G, P_L) \rightarrow H^1(G, \mathcal{O}_L^\times)$ is bijective.

We have a commutative square

$$\begin{array}{ccc} H^2(G, \mathcal{O}_L^\times) & \longrightarrow & H^2(G, L^\times) \\ \downarrow \wr & & \downarrow \wr \\ \varinjlim_n \frac{\mathcal{O}_{k_n}^\times}{N_n(\mathcal{O}_{\ell_n}^\times)} & \longrightarrow & \varinjlim_n \frac{k_n^\times}{N_n(\ell_n^\times)} \end{array}$$

where the horizontal maps are the natural maps and the vertical maps are isomorphisms. Pick some $n \in \mathbb{N}$ and $x_n \in k_n^\times$. Then the commutative square above implies that proving the surjectivity of $H^2(G, \mathcal{O}_L^\times) \rightarrow H^2(G, L^\times)$ amounts to showing there is an $m \in \mathbb{N}$ and a $y_m \in \mathcal{O}_{k_m}^\times$ such that we have an equality of cosets $x_n N_j(\ell_j^\times) = y_m N_j(\ell_j^\times)$ for some integer $j \geq \max\{n, m\}$. In fact, we show that we can take $j = m + 1$.

For the moment, let m be an arbitrary positive integer. Define S_m to be the set of places of k_m which do not split in ℓ_m . We have a commutative diagram

$$\begin{array}{ccccc}
 \frac{\mathcal{O}_{k_{m+1}}^\times}{N_{m+1}(\mathcal{O}_{\ell_{m+1}}^\times)} & \xrightarrow{\beta_{m+1}} & \frac{k_{m+1}^\times}{N_{m+1}(\ell_{m+1}^\times)} & \xrightarrow{\sim} & \bigoplus'_{v' \in S_{m+1}} \text{Br}(\ell_{m+1, w'} / k_{m+1, v'}) \\
 \uparrow \alpha_m & & \uparrow \gamma_m & & \uparrow \delta_m \\
 \frac{\mathcal{O}_{k_m}^\times}{N_m(\mathcal{O}_{\ell_m}^\times)} & \xrightarrow{\beta_m} & \frac{k_m^\times}{N_m(\ell_m^\times)} & \xrightarrow{\sim} & \bigoplus'_{v \in S_m} \text{Br}(\ell_{m, w} / k_{m, v})
 \end{array} \quad (12.1)$$

where α, β, δ are the natural maps and the restricted direct sum \bigoplus' on relative local Brauer groups contains only those tuples which lie in the kernel of the natural map to \mathbb{Q}/\mathbb{Z} given by the sum of local invariants.⁶ We have already noted that β_m, β_{m+1} are injective, and α_m is injective for the same reason, i.e., Theorem 10 implies

$$\mathcal{O}_{k_m}^\times \cap N_{m+1}(\mathcal{O}_{\ell_{m+1}}) = (\mathcal{O}_{k_m}^\times)^2 = N_m(\mathcal{O}_{\ell_m}^\times).$$

Thus $\beta_{m+1} \circ \alpha_m$ is injective, so commutativity of the left side of diagram (12.1) and Eq. (10.2) imply

$$|\text{im}(\gamma_m \circ \beta_m)| = |\text{im}(\beta_{m+1} \circ \alpha_m)| = |\mathcal{O}_{k_m}^\times / N_m(\mathcal{O}_{\ell_m}^\times)| = 2^{t_\infty(m)}. \quad (12.2)$$

Let H_m be the subgroup consisting of those tuples in $\bigoplus'_{v \in S_m} \text{Br}(\ell_{m, w} / k_{m, v})$ which are trivial on the components corresponding to finite places $v \in S_m$ which split in k_{m+1} . We claim that the image of H_m under δ_m also has size $2^{t_\infty(m)}$. First, note that for each $v \in S_m$ the relative local Brauer group $\text{Br}(\ell_{m, w} / k_{m, v})$ has order two since

$$\text{Br}(\ell_{m, w} / k_{m, v}) \cong \begin{cases} \ker(\text{Br}(\mathbb{R}) \rightarrow \text{Br}(\mathbb{C}) = 0) = \text{Br}(\mathbb{R}) \cong \mathbb{Z}/(2) & \text{if } v \text{ is infinite,} \\ \ker(\mathbb{Q}/\mathbb{Z} \xrightarrow{\times 2} \mathbb{Q}/\mathbb{Z}) = \frac{1}{2}\mathbb{Z}/\mathbb{Z} \cong \mathbb{Z}/(2) & \text{if } v \text{ is finite.} \end{cases}$$

If $v \in S_m$ is a finite place which does not split in k_{m+1} , then the map δ_m kills the component of $\text{Br}(\ell_{m, w} / k_{m, v})$ since the local degree is $[k_{m+1} : k_m] = 2$. Also, the infinite places in k_∞/k are totally split, so if $v \in S_m$ is an infinite place, then there are exactly two (real) places v'_1, v'_2 of k_{m+1} which lie above v ; in this case, the map δ_m on the component $\text{Br}(\ell_{m, w} / k_{m, v})$ is given by

$$\text{Br}(\ell_{m, w} / k_{m, v}) \rightarrow \text{Br}(\ell_{m+1, w'_1} / k_{m+1, v'_1}) \oplus \text{Br}(\ell_{m+1, w'_2} / k_{m+1, v'_2}) : \alpha \mapsto (\alpha, \alpha).$$

Therefore $|\delta_m(H_m)| = 2^{t_\infty(m)}$ as claimed since, in particular, H_m contains all tuples whose only nonzero components correspond to infinite places and, if needed to make the sum of local invariants zero, exactly one finite place that does not split in k_{m+1} .

Now we specify m . Finite places are finitely split in the cyclotomic \mathbb{Z}_p -extension of a number field, so there is a sufficiently large positive integer $m \geq n$ such that every finite

⁶ Note that $v \in S_m$ uniquely specifies a place w of ℓ_m which lies above v . Also, if $v \notin S_m$ is a place of k_m , then $\text{Br}(\ell_{m, w} / k_{m, v})$ is trivial for any place w of ℓ_m lying over v .

place $v \in S_m$ with $\text{ord}_v(x_n) \neq 0$ does not split in k_{m+1} . Increasing m if necessary, we may also assume that the finite places $v \in S_m$ which ramify in ℓ_m/k_m do not split in k_{m+1} . For finite places $v \in S_m$ which are unramified in ℓ_m/k_m with $\text{ord}_v(x_n) = 0$, we have $x_n \in \mathcal{O}_{k_{m,v}}^\times$, but $N_m(\mathcal{O}_{\ell_{m,w}}^\times) = \mathcal{O}_{k_{m,v}}^\times$ (see Theorem 2 in Chapter 31 of [Lor08]), so the image of $x_n N_m(\ell_m^\times)$ in $\bigoplus'_{v \in S_m} \text{Br}(\ell_{m,w}/k_{m,v}) \cong \bigoplus'_{v \in S_m} k_{m,v}^\times / N_m(\ell_{m,w}^\times)$ is contained in H_m . Equivalently,

$$x_n N_m(\ell_m^\times) \in \tilde{H}_m \quad (12.3)$$

where \tilde{H}_m denotes the subgroup of $k_m^\times / N_m(\ell_m^\times)$ which maps isomorphically onto H_m in the above commutative diagram (12.1). We have $|\gamma_m(\tilde{H}_m)| = |\delta_m(H_m)| = 2^{t_\infty(m)}$ and we will show that $\text{im}(\gamma_m \circ \beta_m) \subseteq \gamma_m(\tilde{H}_m)$, so Eq. (12.2) implies via the pigeonhole principle that

$$\gamma_m(\tilde{H}_m) = \text{im}(\gamma_m \circ \beta_m). \quad (12.4)$$

To see $\text{im}(\gamma_m \circ \beta_m) \subseteq \gamma_m(\tilde{H}_m)$, we first note that the study of Brauer groups for local fields shows $\text{im}(\beta_m)$ maps injectively into the subgroup of $\bigoplus'_{v \in S_m} \text{Br}(\ell_{m,w}/k_{m,v})$ consisting of tuples which are trivial on all components other than those corresponding to infinite places and to finite places which ramify in ℓ_m/k_m . Since the finite places $v \in S_m$ which ramify in ℓ_m/k_m are non-split in k_{m+1} we know that $\text{im}(\beta_m) \subseteq \tilde{H}_m$, and hence $\text{im}(\gamma_m \circ \beta_m) \subseteq \gamma_m(\tilde{H}_m)$, as needed. Finally, Eqs. (12.3) and (12.4) give

$$x_n N_{m+1}(\ell_{m+1}^\times) = \gamma_m(x_n N_m(\ell_m^\times)) = \gamma_m(\beta_m(y_m N_m(\mathcal{O}_{\ell_m}^\times))) = y_m N_{m+1}(\ell_{m+1}^\times)$$

for some $y_m \in \mathcal{O}_{k_m}^\times$, which finishes the proof. \square

References

- [Die40] Fritz-Erdmann Diederichsen, Über die Ausreduktion ganzzahliger Gruppendarstellungen bei arithmetischer Äquivalenz, Abh. Math. Sem. Hansischen Univ. 13 (1940) 357–412.
- [Fer80] Bruce Ferrero, The cyclotomic \mathbb{Z}_2 -extension of imaginary quadratic fields, Amer. J. Math. 102 (3) (1980) 447–459.
- [FW79] Bruce Ferrero, Lawrence C. Washington, The Iwasawa invariant μ_p vanishes for abelian number fields, Ann. of Math. (2) 109 (2) (1979) 377–395.
- [Gre10] Ralph Greenberg, Topics in Iwasawa theory, <http://math.washington.edu/>, 2010.
- [Has52] Helmut Hasse, Über die klassenzahl abelscher zahlkörper, Akademie Verlag, Berlin, 1952.
- [HM83] I. Hughes, R. Mollin, Totally positive units and squares, Proc. Amer. Math. Soc. 87 (4) (1983) 613–616, (English).
- [IN10] Humio Ichimura, Shoichi Nakajima, On the 2-part of the ideal class group of the cyclotomic \mathbb{Z}_p -extension over the rationals, Abh. Math. Sem. Univ. Hamburg 80 (2010) 175–182.
- [Iwa59] Kenkichi Iwasawa, On Γ -extensions of algebraic number fields, Bull. Amer. Math. Soc. 65 (1959) 183–226.
- [Iwa65] Kenkichi Iwasawa, Analogies Between Number Fields and Function Fields, Ann. Sci. Conf. Proc., vol. 2, Yeshiva University, Belfer Graduate School of Science, 1965, pp. 203–208.
- [Iwa73a] Kenkichi Iwasawa, On \mathbb{Z}_l -extensions of algebraic number fields, Ann. of Math. (2) 98 (1973) 246–326.
- [Iwa73b] Kenkichi Iwasawa, On the μ -Invariants of \mathbb{Z}_l -Extensions, Number Theory, Algebraic Geometry and Commutative Algebra, Kinokuniya, Tokyo, 1973, pp. 1–11, in honor of Yasuo Akizuki.

- [Iwa81] Kenkichi Iwasawa, Riemann–Hurwitz formula and p -adic Galois representations for number fields, *Tohoku Math. J. (2)* 33 (2) (1981) 263–288.
- [Kid79] Yûji Kida, On cyclotomic \mathbb{Z}_2 -extensions of imaginary quadratic fields, *Tohoku Math. J.* 31 (1979) 91–96.
- [Kid80] Yûji Kida, l -extensions of CM-fields and cyclotomic invariants, *J. Number Theory* 12 (4) (1980) 519–528.
- [Kid82] Yûji Kida, Cyclotomic \mathbb{Z}_2 -extensions of J -fields, *J. Number Theory* 14 (3) (1982) 340–352.
- [Lor08] Falko Lorenz, *Algebra, vol. II: Fields with Structure, Algebras and Advanced Topics*, Universitext, Springer, New York, 2008, Translated from the German by Silvio Levy, With the collaboration of Levy.
- [Sch12] Jordan Schettler, *The Change in Lambda Invariants for Cyclic p -Extensions of \mathbb{Z}_p -Fields*, Ph.D. thesis, The University of Arizona, 2012.