PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 112, Number 3, July 1991

ON SMALL IWASAWA INVARIANTS AND IMAGINARY QUADRATIC FIELDS

JONATHAN W. SANDS

(Communicated by William Adams)

ABSTRACT. If p is an odd prime that does not divide the class number of the imaginary quadratic field k, and the cyclotomic $\mathbb{Z}_p$-extension of k has λ-invariant less than or equal to two, we prove that every totally ramified $\mathbb{Z}_p$-extension of k has μ-invariant equal to zero and λ-invariant less than or equal to two. Combined with a result of Bloom and Gerth, this has the consequence that $\mu = 0$ for every $\mathbb{Z}_p$-extension of k, under the same assumptions. In the principal case under consideration, Iwasawa's formula for the power of p in the class number of the nth layer of a $\mathbb{Z}_p$-extension becomes valid for all n, and is completely explicit.

I. OVERVIEW

We aim to refine some of the standard results in classical Iwasawa theory in order to obtain more precise information in situations that commonly occur. The case of an imaginary quadratic base field may be regarded as the first nontrivial example of Iwasawa theory, and we will sharpen the picture in this case when the chosen prime lies outside a set that is expected to be finite. This section will introduce the necessary concepts and trace our line of reasoning leading to the main theorem, while stating some important special cases of our intermediate results.

Begin by fixing a prime number p, and a number field k. We wish to consider various Galois extensions K such that the Galois group $\mathrm{Gal}(K/k)$ is topologically isomorphic to the additive group of the p-adic numbers $\mathbb{Z}_p$. For each positive integer n, there is a unique intermediate field K_n of degree p^n over k, and Iwasawa's remarkable formula [12] gives the order of the p-Sylow subgroup $A(K_n)$ of the ideal class group of K_n as $|A(K_n)| = p^{\mu p^n + \lambda n + \nu}$ for all sufficiently large n. The constants $\mu = \mu(K/k)$, $\lambda = \lambda(K/k)$, and $\nu = \nu(K/k)$ are the Iwasawa invariants for the extension K/k.

Received by the editors April 13, 1990.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11R23.
Key words and phrases. Iwasawa invariant, distinguished polynomial, class field.
Research partially supported by NSF Vermont EPSCoR Grant RII-8610679 and by National Security Agency Grant MDA904-89-H-2012.

0002-9939/91 $1.00 + $.25 per page

A perfect understanding of Iwasawa theory over k for the prime p would include knowing the exact order of $A(K_n)$ for each K and n, and this is the problem we address. There are two aspects of the problem for us to consider: determining the Iwasawa invariants, and investigating the validity of Iwasawa's formula for small values of n.

It is known that the ramified primes of a $\mathbb{Z}_p$-extension K/k must divide p (see [14]). We make the assumption throughout that every ramified prime in K/k is totally ramified. This assumption amounts to replacing k by K_N for some N, and thus simplifies the statement of our results while causing no real loss of generality. Replacing k by K_N does not affect the value of λ, nor does it affect the question of the vanishing of μ. It does restrict the values of n that may be considered in an arbitrary $\mathbb{Z}_p$-extension, but allows one to be specific about the restriction. After making this assumption, we base our investigation on the case of $n = 1$. For example, the following lemma applies when $n = 1$, and gives a lower bound on $|A(K_1)|$, even when Iwasawa's formula is not known to hold at this level.

Lemma. *Assume that every ramified prime of K/k is totally ramified. Then*

$$|A(K_n)| \geq |A(k)|p^{\mu(p^n-1)+\min(p^n-1,\lambda)}$$

for each $n \geq 0$. □

Stronger inequalities hold with some conditions on n, but this lemma is best suited to our purposes. Its virtue lies in the fact that no knowledge of λ is required for its application. Friedman [6] and Gerth [7] used similar lemmas to bound μ, and we have simply taken the contribution from λ into account as well. Thus we can sometimes obtain bounds on λ also.

Corollary. *If every ramified prime of K/k is totally ramified and n is an integer such that $|A(K_n)| < |A(k)|p^{(p^n-1)}$, then $\mu = 0$ and $p^\lambda \leq |A(K_n)|/|A(k)|$.* □

Under certain conditions, we will show that Iwasawa's formula actually holds for small n. As an example, the cyclotomic $\mathbb{Z}_p$-extension of k, which we will denote by K^c, is defined to be the $\mathbb{Z}_p$-extension which is contained in the field obtained by adjoining all p-power roots of unity to k. When k is abelian over $\mathbb{Q}$, the invariant $\mu(K^c/k)$ is 0, by the Ferrero-Washington theorem [5]. Denote the corresponding invariant $\lambda(K^c/K)$ by λ_c. The reader may enjoy finding a proof of the following proposition by means of p-adic L-functions. We will use algebraic methods to prove a more general result.

Proposition. *Suppose k is an imaginary quadratic field. Let $l < p - 1$. The following are equivalent:*

(a) $|A(K_1^c)| = |A(k)|p^l$;
(b) $\lambda_c = l$;
(c) $|A(K_n^c)| = |A(k)|p^{ln}$ *for each $n \geq 0$.* □

The computational results of [4] provide many examples where condition (b) of this proposition holds. In fact, we usually find that $\lambda_c \leq 2$, and conclude from the proposition that $|A(K_1^c)| \leq |A(k)|p^2$.

Now suppose that the base field k is an imaginary quadratic field. Then another $\mathbb{Z}_p$-extension of special interest is the anticylotomic one, denoted K^a, this being the only $\mathbb{Z}_p$-extension of k other than K^c which is Galois over $\mathbb{Q}$. Assume that p is odd and $|A(k)| = 1$; this eliminates only a finite number of primes from consideration. A special case of the theorem of Bloom and Gerth [1] implies that $\mu(K/k) = 0$ for every $\mathbb{Z}_p$-extension K/k, with at most $\lambda_c - 1$ exceptions. Now assume that $\lambda_c \leq 2$; this is expected to again only eliminate a finite number of primes from consideration. Then there is at most one exceptional $\mathbb{Z}_p$-extension of k, which must therefore be stable under complex conjugation, if it exists. Hence it is the anticylotomic $\mathbb{Z}_p$-extension K^a/k. Under these same assumptions, K^a/k is totally ramified at each prime dividing p, and so our results apply.

Now the proposition shows that $|A(K_1^c)| \leq p^2$ under the assumptions that $|A(k)| = 1$ and $\lambda_c \leq 2 < p - 1$. By extending ideas of Gold [8] which relate the class numbers of the first layers of different $\mathbb{Z}_p$-extensions of k to each other, we will deduce that $|A(K_1)| \leq p^2$ if K/k is totally ramified at each prime dividing p. Applying the corollary with $n = 1$ allows us to conclude that $\mu(K/k) = 0$ and $\lambda(K/k) \leq 2$ when K/k is totally ramified at each prime dividing p, p is odd and does not divide the class number h_k of k, and $\lambda_c \leq 2$. (A little extra care is required when $p = 3$; we will attend to this when we give the proof in full detail.) The vanishing of $\mu(K/k)$ holds for $K = K^a$, which was the one possible exception to the special case of the Bloom-Gerth theorem. Thus $\mu(K/k) = 0$ for all $\mathbb{Z}_p$-extensions K/k. Our bound on $\lambda(K/k)$ when $\lambda_c = 2$ is new for all K.

We will refine the arguments presented here and go beyond the determination of λ-invariants. For certain $\mathbb{Z}_p$-extensions K/k (which one might expect to be the most common ones in our setting), we will achieve our goal of determining the exact order of $A(K_n)$ for all n. Our results are summarized in the following main theorem, whose complete proof will be given at the end of the paper.

Theorem. *Suppose that k is an imaginary quadratic field, p is an odd prime that does not divide the class number of k, and $\lambda_c \leq 2$. Then each $\mathbb{Z}_p$-extension K/k has $\mu(K/k) = 0$. The value of $\lambda = \lambda(K/k)$ is less than or equal to 2, and is determined more precisely as follows.*

(a) *If $\lambda_c = 0$, then $\lambda(K/k) = 0$ for each $\mathbb{Z}_p$-extension K/k.*

(b) *If $\lambda_c = 1$, then $\lambda(K/k) = 1$ for each $\mathbb{Z}_p$-extension K/k in which each prime dividing p is totally ramified.*

(c) *If $\lambda_c = 2$, then $1 \leq \lambda(K/k) \leq 2$ for each $\mathbb{Z}_p$-extension K/k in which each prime dividing p is totally ramified.*

Furthermore, the order of $|A(K_n)|$ is given exactly in cases (a), (b), *and* (c)

as $|A(K_n)| = p^{\lambda n}$ *for each* $n \geq 0$ *when* $\lambda = \lambda_c$. *If* $\lambda < \lambda_c$ *in case* (c), *then* $|A(K_n)| \geq p^{\lambda n}$ *for each* $n \geq 0$. □

It should be clear that our proof arises from the combination of three ingredients: inequalities for class numbers in arbitrary $\mathbb{Z}_p$-extensions, equalities which hold in special cases such as cyclotomic extensions over imaginary quadratic fields, and relationships between class numbers at the first layer. We will devote a section to each of these three topics.

II. Iwasawa modules. Lower bounds for $|A(K_n)|$

We review the standard theory [13, 14] with an eye toward refinements that will play a role in our analysis of the initial layer of a fixed $\mathbb{Z}_p$-extension K/k in which every ramified prime is totally ramified.

Let $\Lambda = \varprojlim \mathbb{Z}_p[\mathrm{Gal}(K_n/k)]$, the limit being taken with respect to the natural projection maps. Then $\Lambda \cong \mathbb{Z}_p[[T]]$ under a topological isomorphism which is determined by choosing a topological generator γ of $\mathrm{Gal}(K/k)$ whose image in Λ is mapped to $T+1$ in $\mathbb{Z}_p[[T]]$. We will use this isomorphism to make the identification $\Lambda = \mathbb{Z}_p[[T]]$. The p-Sylow subgroup $A(K_n)$ of the ideal class group of K_n is naturally a $\mathbb{Z}_p[\mathrm{Gal}(K_n/k)]$-module, and thus (taking the inverse limit with respect to the norm maps) $X = \varprojlim A(K_n)$ is a Λ-module. It is known that X is in fact a noetherian torsion Λ-module.

Under our standing assumption that each ramified prime of K/k is totally ramified, if we define distinguished polynomials

$$\nu_n = ((T+1)^{p^n} - 1)/T,$$

then there exists a submodule Y of X such that $X/\nu_n Y \cong A(K_n)$ for all $n \geq 0$. Of course Y is also a torsion Λ-module, and thus by the structure theorem for such modules, there exist positive integers μ_i, distinguished polynomials g_j which are powers of irreducible polynomials, and an injection

$$E = \bigoplus_{i=1}^{d} \Lambda/(p^{\mu_i}) \oplus \bigoplus_{j=1}^{m} \Lambda/(g_j) \hookrightarrow Y$$

with finite cokernel C. (We have used the fact that pseudo-isomorphism is an equivalence relation on *torsion* Λ-modules (see [3, p. 241]), and that E has no nontrivial finite Λ-submodules.) Put λ_j equal to the degree of g_j, $\lambda = \sum_{j=1}^{m} \lambda_j$, and $\mu = \sum_{i=1}^{d} \mu_i$. These are the invariants in Iwasawa's class number formula $|A(K_n)| = p^{\mu p^n + \lambda n + \nu}$, which holds for sufficiently large n. The characteristic polynomial of Y (or X; the same E works for both since $X/Y \cong A(k)$ is finite) is defined to be $g = p^{\mu} \prod_j g_j$, which is in fact uniquely determined. We carefully apply Iwasawa's methods to obtain a formula for $|A(K_n)|$ which holds for *all* n. Let Y^{ν_n} denote the submodule of Y which is annihilated by ν_n.

(2.1) **Proposition.** *Assume that every ramified prime of K/k is totally ramified. Then*

$$|A(K_n)| = |A(k)|\,|Y^{\nu_n}|\,|E/\nu_n E|$$

for each $n \geq 0$, and there exist positive integer constants c and N such that $|Y^{\nu_n}| = p^c$ for all $n \geq N$.

Proof. To each term in the exact sequence

$$0 \to E \to Y \to C \to 0$$

we apply the endomorphism defined by multiplication by ν_n. The snake lemma yields the long exact sequence

$$0 \to E^{\nu_n} \to Y^{\nu_n} \to C^{\nu_n} \to E/\nu_n E \to Y/\nu_n Y \to C/\nu_n C \to 0.$$

The terms of finite order flanking $E/\nu_n E$ show that it is finite, and consequently that ν_n is relatively prime to each g_j in the unique factorization domain Λ. This implies that $E^{\nu_n} = 0$. Since C is finite, C^{ν_n} and $C/\nu_n C$ have the same order. We conclude that

$$|A(K_n)| = |X/\nu_n Y| = |X/Y|\,|Y/\nu_n Y| = |A(k)|\,|Y^{\nu_n}|\,|E/\nu_n E|,$$

which is the first assertion of the proposition.

The second assertion follows from the fact that $\nu_n | \nu_{n+1}$. Thus $Y^{\nu_n} \subset Y^{\nu_{n+1}}$, and the long exact sequence also shows that these submodules of Y have order dividing $|C|$ for all n. Hence Y^{ν_n} must eventually be independent of n. □

Now a computation of the order $|E/\nu_n E|$ is clearly called for. We again use standard methods, but take extra care in the consideration of small values of n.

(2.2) **Proposition.** *Let $n \geq 0$.*

(a) *If $E = \Lambda/(p^\mu)$, then $|E/\nu_n E| = p^{\mu(p^n - 1)}$.*

(b) *If $E = \Lambda/(g)$ with g a distinguished polynomial of degree λ, then $|E/\nu_n E| \geq p^{\min(\lambda, p^n - 1)}$.*

(c) *If $\lambda < p-1$ in* (b), *or if $\lambda = p-1$ and p^2 divides $g(0)$, then $|E/\nu_n E| = p^{\lambda n}$.*

(2.3) *Remarks.* (1) For our main result on the values of Iwasawa invariants as stated in the theorem of the overview we will only need the case of $n = 1$. However, the fact that the proposition applies for all n has important implications for the validity of Iwasawa's formula, as seen in the proposition of the overview and Theorem (3.1) in the next section.

(2) Part (a) of (2.2) appears in [14, Chapter 13]; we will streamline the proof slightly.

(3) We have chosen a proof of (c) which may be viewed as extending the method of [14, Chapter 13]. A shorter proof is available if one invokes the

formula

$$|\Lambda/(g, \nu_n)| = \prod_{\nu_n(\zeta-1)=0} p^{\operatorname{ord}_p(g(\zeta-1))},$$

derived from [2, p. 530].

Proof of (2.2). If $f \in \Lambda$ is a fixed distinguished polynomial of degree d and $h \in \Lambda$, then the proof of the Weierstrauss preparation theorem for Λ (see [14, Proposition 7.2]) shows that one may uniquely write $h = qf + r$ with $q \in \Lambda$ and $r = a_0 + a_1 T + \cdots + a_{d-1} T^{d-1}$. Thus the assignment $h \mapsto (a_0, a_1, \ldots, a_{d-1})$ induces a $\mathbb{Z}_p$-module isomorphism $\Lambda/(f) \tilde{\to} \mathbb{Z}_p^d$.

We may assume that $n \geq 1$ throughout, as the case of $n = 0$ is trivially true in each part.

(a) Taking $f = \nu_n$, we have $\Lambda/(\nu_n) \cong \mathbb{Z}_p^{p^n-1}$, and

$$E/\nu_n E \cong \mathbb{Z}_p^{p^n-1}/(p^\mu \mathbb{Z}_p)^{p^n-1} \cong (\mathbb{Z}/p^\mu \mathbb{Z})^{p^{n-1}}.$$

Therefore the order is $p^{\mu(p^n-1)}$.

(b) Let $m = \min(\lambda, p^n - 1)$. Then we have the inclusion of ideals $(g, \nu_n) \subset (T^m, p)$. Hence $|E/\nu_n E| = |\Lambda/(g, \nu_n)| \geq |\Lambda/(T^m, p)| = |(\mathbb{Z}/p\mathbb{Z})^m| = p^m$.

(c) Taking $f = g$ this time, we have

$$(\dagger) \qquad E = \Lambda/(g) \cong \mathbb{Z}_p^\lambda$$

as $\mathbb{Z}_p$-modules. Consider the image of $\nu_n = \sum_{k=1}^{p^n} \binom{p^n}{k} T^{k-1} \pmod g$ under this isomorphism. We can factor

$$\binom{p^n}{k} = \left(\frac{p^n}{k}\right)\left(\frac{p^n-1}{1}\right)\left(\frac{p^n-2}{2}\right)\left(\frac{p^n-(k-1)}{k-1}\right)$$

in $\mathbb{Z}_p$, so $\binom{p^n}{k} = w(p^n/k)$, $w \in \mathbb{Z}_p$. Now g is distinguished, so that $g = T^\lambda - pj$ for some $j \in \mathbb{Z}_p[T]$. Thus $T^\lambda \equiv pj$ and $T^{k-1} \equiv (pj)^{[(k-1)/\lambda]} T^{r(k)} \pmod g$ for $k > \lambda$, where the square brackets represent the greatest integer function. If $k = pt$, then t divides p^{t-1} in $\mathbb{Z}_p$ so $k = pt$ divides $p^t = p^{[(pt-t)/(p-1)]}$, which divides $p^{[(pt-1)/(p-1)]} = p^{[(k-1)/(p-1)]}$, which divides $p^{[(k-1)/\lambda]}$. This shows that $p^{[(k-1)/\lambda]} = vk$, $v \in \mathbb{Z}_p$, which clearly also holds for $(k, p) = 1$. We conclude that

$$\binom{p^n}{k} T^{k-1} \equiv w\left(\frac{p^n}{k}\right) vkj^{[(k-1)/\lambda]} T^{r(k)} = wvp^n j^{[(k-1)/\lambda]} T^{r(k)} \pmod g.$$

Therefore $\nu_n \equiv p^n z \pmod g$ for some $z \in \Lambda$, and $\nu_n \pmod g$ has the same image under the $\mathbb{Z}_p$-isomorphism $(\dagger)$ as $p^n z \pmod g$. We now see that this image lies in $p^n(\mathbb{Z}_p^\lambda)$. To summarize, so far we have found that if $\lambda \leq p - 1$, then $\nu_n = gq + r$, where $r \equiv 0 \pmod{p^n}$.

We can now write $r = p^n u$, where u is a polynomial of degree at most $\lambda - 1$, and consider $u(0)$. As $n \geq 1$, we have

$$T^{(p^n-1)} \equiv \nu_n = gq + r \equiv gq \equiv T^\lambda q \pmod p.$$

Thus $g = T^{\lambda} - pj$ and $q = T^{p^n-\lambda-1} + ph$, with $j, h \in \Lambda$. Multiplying out yields

$$(*) \qquad \nu_n = T^{p^n-1} - pjT^{p^n-\lambda-1} + phT^{\lambda} - p^2jh + r,$$

so

$$(**) \qquad \nu_n \equiv T^{p^n-1} - pjT^{p^n-\lambda-1} + phT^{\lambda} + r \pmod{p^2}.$$

For $n = 1$, we consider the constant term in $(**)$. The strict inequality $p - 1 > \lambda$ (or the alternate assumption that p^2 divides $-g(0) = pj(0)$) allows us to obtain $p = \nu_1(0) \equiv r(0) = pu(0) \pmod{p^2}$, or $1 \equiv u(0) \pmod{p}$. Thus $u(0)$ is a unit in $\mathbb{Z}_p$ and hence u is a unit in Λ. For $n = 2$, we consider the coefficient of T^{λ} in $(**)$ when $\lambda < p - 1$. Since $p^2 - \lambda - 1 > \lambda >$ (degree of r), this coefficient is $0 \equiv \binom{p^2}{\lambda+1} \equiv ph(0) \pmod{p^2}$. The first congruence follows from the equation $\binom{p^2}{\lambda+1} = w(p^2/(\lambda+1))$ derived above. We conclude that $p|h(0)$. Return to $(*)$, and evaluate the constant term $\pmod{p^3}$ using this fact (or the assumption that p divides $j(0)$ when $\lambda = p - 1$):

$$p^2 = \nu_2(0) = -p^2j(0)h(0) + r(0) \equiv r(0) = p^2u(0) \pmod{p^3}.$$

Again $1 \equiv u(0) \pmod{p}$, and u is a unit in Λ.

If $n = 1$ or 2, we now have $\nu_n = gq + r = gq + p^n u$, where u is a unit. Thus we obtain the equality of ideals in Λ:

$$(g, \nu_n) = (g, r) = (g, p^n u) = (g, p^n).$$

Finally

$$E/\nu_n E \cong \Lambda/(g, \nu_n) = \Lambda/(g, p^n) \cong E/p^n E \cong \mathbb{Z}_p^{\lambda}/p^n(\mathbb{Z}_p^{\lambda}) \cong (\mathbb{Z}_p/p^n\mathbb{Z}_p)^{\lambda},$$

so $|E/\nu_n E| = p^{\lambda n}$ as claimed.

Now if $n > 2$, we simply note that $|E/\nu_n E| = p^{\lambda(n-2)}|E/\nu_2 E|$, as proved in [14, Lemma 13.18] (with $e = 0$, $n_0 = 1$, and $d = \lambda$). Combined with the fact we have just established that $|E/\nu_2 E| = p^{2\lambda}$, this completes the proof. □

We are now ready to prove the lemma and corollary stated in the overview.

(2.4) **Lemma.** *Assume that every ramified prime of K/k is totally ramified. Then*

$$|A(K_n)| \geq |A(k)|p^{\mu(p^n-1)+\min(p^n-1,\lambda)}$$

for each $n \geq 0$.

Proof. From Proposition (2.1), we have that $|A(K_n)| \geq |A(k)|\,|E/\nu_n E|$. Applying Proposition (2.2)(a) and (b) to each summand of

$$E = \bigoplus_{i=1}^{n} \Lambda/(p^{\mu_i}) \oplus \bigoplus_{j=1}^{m} \Lambda/(g_j)$$

results in $|E/\nu_n E| \geq p^{\mu(p^n-1)+a}$, where $a = \sum_{j=1}^{m} \min(p^n - 1, \lambda_j) \geq \min(p^n - 1, \sum_{j=1}^{m} \lambda_j) = \min(p^n - 1, \lambda)$. □

(2.5) **Corollary.** *If every ramified prime of K/k is totally ramified and n is an integer such that $|A(K_n)| < |A(k)|p^{(p^n-1)}$, then $\mu = 0$ and $p^\lambda \leq |A(K_n)|/|A(k)|$.*

III. Special cases. The exact order of $A(K_n)$

(3.1) **Theorem.** *Suppose that every ramified prime in K/k is totally ramified, and $\mu = \mu(K/k) = 0$. Suppose also that $\lambda = \lambda(K/k) < p - 1$ (or that $\lambda = p - 1$ and p^2 divides $g(0)$). Then $|A(K_n)| = |A(k)|\,|Y^{\nu_n}|p^{\lambda n} \geq |A(k)|p^{\lambda n}$ for each $n \geq 0$. If in addition, $X = \varprojlim A(K_n)$ has no nontrivial finite Λ-submodules, then $|A(K_n)| = |A(k)|p^{\lambda n}$ for each $n \geq 0$.*

Proof. The first assertion follows directly from (2.1) upon applying (2.2)(c) to each summand of $E = \bigoplus_{j=1}^{m} \Lambda/(g_j)$. The proof of Proposition (2.1) shows that Y^{ν_n} is a finite Λ-submodule of X. So it is trivial under the additional hypothesis of the second assertion. □

We immediately obtain a corollary which generalizes part of a theorem of Gold [8].

(3.2) **Corollary.** *Suppose that every ramified prime in K/k is totally ramified and that $X = \varprojlim A(K_n)$ has no nontrivial finite Λ-submodules. Let $l < p - 1$. Then the following are equivalent:*

(a) $|A(K_1)| = |A(k)|p^l$;
(b) $\mu = 0$ *and* $\lambda = l$; *and*
(c) $|A(K_n)| = |A(k)|p^{ln}$ *for each* $n \geq 0$.

Proof. (a) ⇒ (b). Corollary (2.5) with $n = 1$ implies that $\mu = 0$ and $\lambda \leq l < p - 1$. Then Theorem (3.1) shows that $|A(K_n)| = |A(k)|p^{\lambda n}$ for each $n \geq 0$. Taking $n = 1$ again yields $\lambda = l$.

(b) ⇒ (c). This follows directly from (3.1).

(c) ⇒ (a). This is clear. □

If p is odd, k is a CM-field, and $K = K^c$ is the cyclotomic $\mathbb{Z}_p$-extension, then we have the decomposition with respect to complex conjugation: $X = X^+ \oplus X^-$. Here X^- has no finite Λ-submodules [14, Proposition 13.28] and X^+ is conjectured to be finite [10]. It is trivial if the maximal totally real subfield k^+ of k has only one prime dividing p and $|A(k^+)| = 1$ [11]. If k is also abelian over $\mathbb{Q}$, then $\mu = 0$ by the Ferrero-Washington theorem. Thus we can obtain applications of (3.1). In particular, X has no finite submodules and $\mu = 0$ when p is odd and k is an imaginary quadratic field. Also, the extension K_n^c/k must then be totally ramified at each prime above p because the abelian extension $(K_n^c)^+/\mathbb{Q}$ is totally ramified at p and has degree p^n, which is prime to the degree of $k/\mathbb{Q}$. The proposition in the overview now follows.

There are of course versions of (3.1) and (3.2) for X^- when $K = K^c$ is the cyclotomic $\mathbb{Z}_p$-extension. We state these versions without proof, as the necessary modifications are clear and the details straightforward.

(3.3) **Theorem.** *Suppose that k is a CM-field, p is odd, every ramified prime in K^c/k is totally ramified, and $\mu^- = 0$, $\lambda^- < p-1$. Then $|A^-(K_n)| = |A^-(k)|p^{\lambda^- n}$ for each $n \geq 0$.*

(3.4) **Corollary.** *Suppose that k is a CM-field, p is odd, and every ramified prime in K^c/k is totally ramified. Let $l < p-1$. Then the following are equivalent:*

(a) $|A^-(K_1)| = |A^-(k)|p^l$;
(b) $\mu^- = 0$ *and* $\lambda^- = l$; *and*
(c) $|A^-(K_n)| = |A^-(k)|p^{ln}$ *for each* $n \geq 0$.

There is also a useful general criterion for Y to have no nontrivial finite Λ-submodules.

(3.5) **Proposition.** *Suppose that every ramified prime in K/k is totally ramified, and $\mu = \mu(K/k) = 0$. Suppose also that $\lambda = \lambda(K/k) < p-1$ (or that $\lambda = p-1$ and p^2 divides $g(0)$). Then the following are equivalent:*

(a) *Y has no nontrivial finite Λ-submodules;*
(b) $|A(K_n)| = |A(k)|p^{\lambda n}$ *for each* $n \geq 0$; *and*
(c) $|A(K_m)| = |A(k)|p^{\lambda m}$ *for some* $m \geq 1$.

Proof. The implication (a) $\Rightarrow$ (b) follows from the proof of Theorem (3.1), and (b) $\Rightarrow$ (c) is clear.

To prove that (c) $\Rightarrow$ (a), let Z be the maximal finite Λ-submodule of Y (see [13]). (We could in fact define $Z = Y^{\nu_N}$ with N as in Proposition (2.1)). Then $Y^{\nu_n} \subset Z$ for each n, so that $Y^{\nu_n} = Z^{\nu_n}$. Under our assumption, Theorem (3.1) shows that $1 = |Y^{\nu_m}| = |Z^{\nu_m}|$. Thus Z^{ν_m} is trivial. This implies that multiplication by ν_m is injective on Z, and hence surjective, since Z is finite. From the equality $\nu_m Z = Z$, we conclude by Nakayama's lemma that $Z = 0$. □

IV. Initial layers of $\mathbb{Z}_p$-extensions over a fixed imaginary quadratic field

The key idea of this section comes from a well-known fact concerning the tower of p-Hilbert class fields over a number field F. By the p-Hilbert class field of F, we mean the maximal unramified abelian p-extension H of F. The Artin map of class field theory induces an isomorphism $A(F) \xrightarrow{\sim} \mathrm{Gal}(H/F)$ in which the class of a prime ideal is mapped to the corresponding Frobenius automorphism. In this connection, it is best to regard $A(F)$ as a quotient of the ideal class group of F, rather than as a subgroup. The well-known fact we have

in mind states that $A(H)$ is trivial if $A(F)$ is cyclic. Hence the p-Hilbert class field of H is itself, and the tower of p-Hilbert class fields over F terminates with H. This fact and our modification amount to a direct translation via class field theory of a group-theoretic result [9, p. 173].

(4.1) **Proposition.** *Suppose G is a finite p-group and G' is its commutator subgroup. If G/G' is cyclic then G' is trivial.*

Our modification is to consider instead the p-split p-Hilbert class field H' of F, defined to be the maximal abelian unramified p-extension of F in which each prime over p in k splits completely. So H' is the subfield of H which is fixed by the decomposition groups in $\mathrm{Gal}(H/F)$ of all primes above p in F. Since these decomposition groups are generated by the Frobenius automorphisms of the primes above p in F, we define $A'(F)$ to be the quotient of $A(F)$ by the subgroup generated by the classes of prime ideals dividing p, and obtain an induced isomorphism $A'(F) \xrightarrow{\sim} \mathrm{Gal}(H'/F)$. Now we state and prove the result we will need. The proof of the fact mentioned above is completely analogous.

(4.2) **Lemma.** *If $A'(F)$ is cyclic, then $A'(H')$ is trivial.*

Proof. Let H'' be the p-split p-Hilbert class field of H'. Using the fact that H'/F is Galois and the set of primes above p in H' is stable under $\mathrm{Gal}(H'/F)$, a standard argument shows that H'' is also Galois over F. Let $G = \mathrm{Gal}(H''/F)$. The fixed field of G' is the maximal abelian extension of F in H'', hence is H'. Thus $G' = \mathrm{Gal}(H''/H') \cong A'(H')$ and $G/G' \cong \mathrm{Gal}(H'/F) \cong A'(F)$. Application of (4.1) completes the proof. □

From now on, we will assume that k is a fixed imaginary quadratic field and p is an odd prime which does not divide the class number h_k of k. Iwasawa's group-theoretic result [11] (see also [14, Theorem 10.4]) immediately identifies trivial cases of which we may dispose.

(4.3) **Proposition.** *Let k be an imaginary quadratic field and p be a prime that does not divide $h(k)$ and does not split in k. Then every $\mathbb{Z}_p$-extension K/k has $\mu = 0 = \lambda$, and in fact $|A(K_n)| = 1$ for each $n \geq 0$.*

Proof. There is only one prime dividing p in k, hence only one ramified prime in K_n/k, and this is a cyclic extension of degree p^n. In this situation, Iwasawa's result states that $A(K_n)$ is trivial if $A(k)$ is. □

It remains only to consider the case in which p splits in k as $(p) = \mathfrak{p}\bar{\mathfrak{p}}$. Note that k has no unramified p-extensions when $|A(k)| = 1$, and therefore K_1^a/k is ramified. Being Galois over $\mathbb{Q}$, it must be ramified at both $\mathfrak{p}$ and $\bar{\mathfrak{p}}$. So K^a/k is totally ramified at both primes dividing p. We observed this earlier for K^c/k without the assumption on h_k.

Since k is imaginary quadratic, it is known that the compositum $\mathfrak{k}$ of all $\mathbb{Z}_p$-extensions of k has $\mathrm{Gal}(\mathfrak{k}/k) \cong \mathbb{Z}_p^2$ (see [14, Theorem 13.4], for example). Let L_n be the compositum of K_n^c and K_n^a, which is abelian of degree p^{2n} over

k. Then L_n contains the nth layer of each $\mathbb{Z}_p$-extension of k. In particular, L_n contains an extension E_n of degree p^n over k in which $\mathfrak{p}$ is unramified, so the ramification index of $\mathfrak{p}$ in L_n/k is p^n. (Our fields L_n and E_n are the same as those of Gold in [8], by virtue of the Lemma there.) This implies that L_n/K_n is unramified whenever K/k is totally ramified at both $\mathfrak{p}$ and $\bar{\mathfrak{p}}$. Hence there is a homomorphism from $A(K_n)$ onto $\mathrm{Gal}(L_n/K_n)$ induced by the Artin map of class field theory, and consequently a Λ-module homomorphism φ_n from X onto $\mathrm{Gal}(L_n/K_n)$. Now $\mathrm{Gal}(K_n/k)$, and hence Γ, acts trivially on $\mathrm{Gal}(L_n/K_n)$, since L_n/k is an abelian extension. This shows that $\gamma - 1 = T$ annihilates the image of φ_n, and there is an induced map from X/TX onto $\mathrm{Gal}(L_n/K_n)$. Since this holds for each n, we see that X/TX is infinite. As $X/Y \cong A(k)$ is finite, Y/TY must also be infinite. Also, the standard Λ-module E of Proposition (2.1) injects into Y with finite cokernel, so E/TE is infinite as well. This implies that T divides the characteristic polynomial g of X. We have proved an important fact, which does not require the assumption of p being relatively prime to the class number of k.

(4.4) **Proposition.** *Let k be an imaginary quadratic field and p be an odd prime which splits in k. Suppose that K/k is a $\mathbb{Z}_p$-extension in which both divisors of p are totally ramified. Then T divides the characteristic polynomial g of the corresponding Λ-module X, and consequently $\lambda(K/k) \geq 1$.*

Next we come to the key result of this section.

(4.5) **Proposition.** *Let k be an imaginary quadratic field and p be an odd prime which splits in k and does not divide h_k. Suppose that $\mathcal{K}$ and K are $\mathbb{Z}_p$-extensions of k in which both primes dividing p are totally ramified. If $|A(\mathcal{K}_1)| = p^2$, then $|A(K_1)| = p^2$.*

Proof. Let $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ be the primes dividing p in k, and let $\mathfrak{p}_{\mathcal{K}}$ and $\bar{\mathfrak{p}}_{\mathcal{K}}$ be the primes dividing them in $\mathcal{K}_1$. Being the only primes which are ramified over k, $\mathfrak{p}_{\mathcal{K}}$ and $\bar{\mathfrak{p}}_{\mathcal{K}}$ represent (modulo pth powers) generators of the group of (strongly) ambiguous ideal classes (i.e., ideal classes represented by ideals which are invariant under the action of the Galois group of $\mathcal{K}_1/k$). Yokoi [15] gives the order of this group as

$$\frac{h_k \prod_{\mathfrak{q}} e(\mathfrak{q})}{[\mathcal{K}_1 : k](U(k) : N_{\mathcal{K}_1/k} U(\mathcal{K}_1))},$$

where $\mathfrak{q}$ runs through the primes of k which ramify in $\mathcal{K}_1$, $e(\mathfrak{q})$ is the ramification index of the prime $\mathfrak{q}$ in $\mathcal{K}_1$, $N_{\mathcal{K}_1/k}$ is the relative norm, and $U(F)$ denotes the group of units of the number field F. In our situation, p does not divide h_k, $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ are the only ramified primes, $e(\mathfrak{p}) = e(\bar{\mathfrak{p}}) = p$, $[\mathcal{K}_1 : k] = p$, and p does not divide $|U(k)|$ since p is unramified in k. We conclude that the images of the primes dividing p generate a subgroup of $A(\mathcal{K}_1)$ of order p. Thus $|A'(\mathcal{K}_1)| = |A(\mathcal{K}_1)|/p$, and similarly, $|A'(K_1)| = |A(K_1)|/p$. The proof of this proposition reduces to showing that $|A'(K_1)| = p$ when $|A'(\mathcal{K}_1)| = p$.

Let H' be the p-split p-Hilbert class field of $\mathscr{K}_1$. By [8, proof of Theorem 3], $\mathfrak{p}$ splits in E_1/k under our assumptions. (If $\mathfrak{p}$ does not split in E_1/k, then there is at most one ramified prime in L_1/E_1, as well as in E_1/k. Two applications of the result of Iwasawa mentioned in the proof of Proposition (4.3) lead to the conclusion that $A(L_1)$ is trivial. Hence L_1 is the p-Hilbert class field of $\mathscr{K}_1$, and $|A(\mathscr{K}_1)| = p$, which is a contradiction.) Hence $\mathfrak{p}_{\mathscr{K}}$ splits in $L_1/\mathscr{K}_1$. Likewise, $\bar{\mathfrak{p}}_{\mathscr{K}}$ must also split in L_1. The definition of H' then implies that $H' \supset L_1$, and therefore

$$p = |\operatorname{Gal}(L_1/\mathscr{K}_1)| \leq |\operatorname{Gal}(H'/\mathscr{K}_1)| = |A'(\mathscr{K}_1)| = p.$$

We now see that equality must hold, and in fact $L_1 = H'$.

At this point, Lemma (4.2) applies with $F = \mathscr{K}_1$, and yields that $A'(L_1)$ is trivial. Consequently L_1 has no nontrivial unramified abelian p-extensions in which each divisor of p splits completely. In particular, L_1 must contain the p-split p-Hilbert class field of K_1. On the other hand, L_1 is contained in this field, by the same argument used in the case of $\mathscr{K}_1$. As $|\operatorname{Gal}(L_1/K_1)| = p$, we conclude that $|A'(K_1)| = p$. □

Having completed the proof of the key proposition which will apply when $\lambda_c = 2$, we can quickly state and prove the simpler proposition which will apply when $\lambda_c = 1$.

(4.6) **Proposition.** *Let k be an imaginary quadratic field and p be an odd prime which splits in k and does not divide h_k. Suppose that $\mathscr{K}$ and K are $\mathbb{Z}_p$-extensions of k in which both primes dividing p are totally ramified. If $|A(\mathscr{K}_1)| = p$, then $|A(K_1)| = p$.*

Proof. In this case we have $L_1 = H$, the p-Hilbert class field of $\mathscr{K}_1$, and $A(L_1)$ is trivial. Hence L_1 is also the p-Hilbert class field of K_1, and $|A(K_1)| = p$. □

We now turn to the proof of the main theorem, stated in the overview. Assume that p is an odd prime that does not divide the class number of the imaginary quadratic field k. Consider first the case of $\lambda_c = 0$. By the contrapositive of Proposition (4.4), p does not split in k. Then Proposition (4.3) implies that $|A(K_n)| = 1$ for each K and n, establishing the vanishing of $\mu(K/k)$, the vanishing of $\lambda(K/k)$ claimed in part (a), and the class number formula for all n.

Now consider the cases of $\lambda_c = 1$ and $\lambda_c = 2$. By the contrapositive of Proposition (4.3), p splits in k. From Proposition (4.4) we see that T divides the characteristic polynomial of K^c, a fact which we need for the application of Theorem (3.1) in case $\lambda_c = p - 1$, i.e., $p = 3$ and $\lambda_c = 2$. Theorem (3.1) now implies that $|A(K_1^c)| = p^{\lambda_c}$. Let K/k be a $\mathbb{Z}_p$-extension which is totally ramified at both primes dividing p. Proposition (4.4) shows that T divides the characteristic polynomial g of $Y = X = \varprojlim A(K_n)$, and $\lambda = \lambda(K/k) \geq 1$. We apply Propositions (4.5) and (4.6) with $\mathscr{K} = K^c$ to deduce that $|A(K_1)| = p^{\lambda_c}$.

Except when $\lambda_c = p - 1$, we conclude from Corollary (2.5) with $n = 1$ that $\mu(K/k) = 0$ and $\lambda(K/k) \leq \lambda_c$. So $1 \leq \lambda(K/k) \leq \lambda_c$, and we have established the vanishing of $\mu(K/k)$ when K/k is totally ramified at both primes dividing p, as well as the results on $\lambda(K/k)$ in parts (b) and (c) of the theorem.

The theorem of Bloom and Gerth for our special case already implies that $\mu(K/k) = 0$ for *all* $\mathbb{Z}_p$-extensions K/k when $\lambda_c = 1$, and for all but the anticyclotomic $\mathbb{Z}_p$-extension K^a/k when $\lambda_c = 2$. As we have already observed, K^a/k is totally ramified at both primes dividing p, under our assumption that p does not divide h_k. Thus our result shows that $\mu(K^a/k) = 0$ when $\lambda_c = 2$ as well.

When $\lambda_c = p - 1$, we must refine our arguments. In this case, Lemma (2.4) with $n = 1$ and $|A(K_1)| = p^{\lambda_c}$ yields $p - 1 = \lambda_c \geq \mu(K/k)(p - 1) + \min(p - 1, \lambda(K/k))$. Since $\lambda(K/k) \geq 1$, we see that $\mu(K/k) = 0$ still holds. Suppose that $g = \prod g_j$ and λ_j is the degree of g_j. Then the proof of Lemma (2.4) actually shows that $p - 1 = \lambda_c \geq \sum \min(p - 1, \lambda_j)$. If there is more than one term in the sum, then each term must in fact be λ_j, and so $\lambda_c \geq \sum \lambda_j = \lambda(K/k) = \lambda$, as claimed. If there is only one term in the sum, then g is a power of an irreducible polynomial. As g is divisible by T, we must have $g = T^{\lambda}$. Proposition (2.1) shows that $p^{\lambda_c} = |A(K_1)| \geq |\Lambda/(T^{\lambda}, \nu_1)|$. Now it is easy to see that $\Lambda/(\nu_1)$ is a noetherian local domain whose maximal ideal is principal, generated by the element T. Thus it is a discrete valuation ring ([2, p. 392]) with maximal ideal of index p. Raising the maximal ideal to the power λ yields an ideal of index p^{λ}. Equivalently $|\Lambda/(T^{\lambda}, \nu_1)| = p^{\lambda}$, and we again conclude that $\lambda_c \geq \lambda$.

It remains for us to prove the class number formulas in cases (b) and (c). The inequality $|A(K_n)| \geq p^{\lambda n}$ holds for all n by Theorem (3.1). This theorem with $n = 1$ also shows that $|A(K_1)| = |Y^{\nu_1}|p^{\lambda}$. As $|A(K_1)| = p^{\lambda_c}$, we see that in fact $|A(K_1)| = p^{\lambda}$ (and $|Y^{\nu_1}| = 1$) when $\lambda_c = \lambda$. Proposition (3.5) now implies that $|A(K_n)| = p^{\lambda n}$ for all n when $\lambda_c = \lambda$, and the proof of the main theorem is complete.

Acknowledgments

I thank Eduardo Friedman for his ideas that improved the results presented here. I also thank all the members of the Quebec-Vermont Number Theory Seminar for their support, and especially David Dummit, Richard Foote, and Hershy Kisilevsky for their input that improved the exposition of this paper.

References

1. J. R. Bloom and F. Gerth III, *The Iwasawa invariant μ in the composite of two $\mathbb{Z}_l$-extensions*, J. Number Theory **13** (1981), 262–267.
2. N. Bourbaki, *Commutative algebra*, Addison-Wesley, Reading, MA, 1972.
3. A. Cuoco and P. Monsky, *Class numbers in $\mathbb{Z}_p^d$-extensions*, Math. Ann. **255** (1981), 235–258.

4. D. S. Dummit, D. Ford, H. Kisilevsky, and J. W. Sands, *Computation of Iwasawa lambda invariants for imaginary quadratic fields*, J. Number Theory (to appear).
5. B. Ferrero and L. Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. Math. **109** (1979), 377–395.
6. E. Friedman, *Iwasawa invariants*, Math. Ann. **271** (1985), 13–30.
7. F. Gerth III, *Upper bounds for an Iwasawa invariant*, Compositio Math. **39** (1979), 3–10.
8. R. Gold, *The non-triviality of certain $\mathbb{Z}_l$-extensions*, J. Number Theory **6** (1974), 369–373.
9. D. Gorenstein, *Finite groups*, Harper and Row, New York, 1968.
10. R. Greenberg, *On the Iwasawa invariants of totally real number fields*, Amer. J. Math. **98** (1976), 263–284.
11. K. Iwasawa, *A note on class numbers of algebraic number fields*, Abh. Math. Sem. U. Hamburg **20** (1956), 257–258.
12. ____, *On Γ-extensions of algebraic number fields*, Bull. Amer. Math. Soc. **65** (1959), 183–226.
13. ____, *On $\mathbb{Z}_l$-extensions of algebraic number fields*, Ann. of Math. **98** (1973), 246–326.
14. L. C. Washington, *Introduction to cyclotomic fields*, Springer-Verlag, New York, 1982.
15. H. Yokoi, *On the class number of a relatively cyclic number field*, Nagoya Math. J. **29** (1967), 31–44.

Department of Mathematics and Statistics, University of Vermont, Burlington, Vermont 05405