PACIFIC JOURNAL OF MATHEMATICS
Vol. 80, No. 1, 1979

THE IWASAWA INVARIANT μ FOR QUADRATIC FIELDS

FRANK GERTH III

We let k_0 be a quadratic extension field of the rational numbers, and we let l be a rational prime number. In this paper we show that there exists a constant c (depending on k_0 and l) such that the Iwasawa invariant $\mu(K/k_0) \leqq c$ for all Z_l-extensions K of k_0. In certain cases we give explicit values for c.

1. Introduction. We let Q denote the field of rational numbers, and we let l denote a rational prime number. We let k_0 be a finite extension field of Q, and we let K be a Z_l-extension of k_0 (that is, K/k_0 is a Galois extension whose Galois group is isomorphic to the additive group of the l-adic integers Z^l). We denote the intermediate fields by $k_0 \subset k_1 \subset k_2 \subset \cdots \subset k_n \subset \cdots \subset K$, where Gal (k_n/k_0) is a cyclic group of order l^n. We let A_n denote the l-class group of k_n (that is, the Sylow l-subgroup of the ideal class group of k_n). In [5, §4.2], Iwasawa proves that $|A_n| = l^{e_n}$, where

$$e_n = \mu l^n + \lambda n + \nu \tag{1}$$

for n sufficiently large, and μ, λ, ν are rational integers (called the Iwasawa invariants of K/k_0) which are independent of n. Also $\mu \geqq 0$ and $\lambda \geqq 0$.

Next we let W be the set of all Z_l-extensions of k_0. If $K \in W$, we define

$$W(K, n) = \{K' \in W \mid [K \cap K' : k_0] \geqq l^n\} .$$

Thus $W(K, n)$ consists of all Z_l-extensions of k_0 that contain k_n, where k_n is the unique subfield of K such that $[k_n : k_0] = l^n$. We topologize W by letting $\{W(K, n)$ for $n = 1, 2, \cdots\}$ be a neighborhood basis for each $K \in W$. It can be proved that W is compact with this topology (see [4, §3]). Next we let W' be the set of Z_l-extensions of k_0 with only finitely many primes lying over l. In [4, Proposition 3 and Theorem 4], Greenberg proves that W' is an open dense subset of W and that the Iwasawa invariant μ is locally bounded on W'. So if $K \in W'$, there exists an integer n_0 and a constant c depending only on K such that $\mu(K'/k_0) < c$ for all Z_l-extensions K' of k_0 with $[K \cap K' : k_0] \geqq l^{n_0}$. Greenberg suggests that perhaps μ is bounded on W; that is, perhaps there exists a constant c such that $\mu(K'/k_0) < c$ for every $K' \in W$. If there is only one prime of k_0 above l, then Greenberg does prove in [4, Theorem 6] that μ is bounded on W.

In this paper we shall prove that μ is bounded on W if k_0 is a quadratic extension of $\boldsymbol{Q}$. We state this result as follows.

THEOREM 1. *Let k_0 be a quadratic extension of $\boldsymbol{Q}$, and let $\mathfrak{l}$ be a rational prime number. Then there exists a constant c (depending on k_0 and $\mathfrak{l}$) such that $\mu(K/k_0) \leqq c$ for all $\boldsymbol{Z}_{\mathfrak{l}}$-extensions K of k_0*

2. *Proof of Theorem* 1. We let the notation be the same as in the previous section. We let M be the composite of all $\boldsymbol{Z}_{\mathfrak{l}}$-extensions of k_0, where k_0 is a finite extension field of $\boldsymbol{Q}$. It is known (see [5, Theorem 3]) that $\mathrm{Gal}\,(M/k_0) \approx \boldsymbol{Z}_{\mathfrak{l}}^d$, where $r_2 + 1 \leqq d \leqq [k_0 : \boldsymbol{Q}]$ and r_2 is the number of complex archimedean primes of k_0. We note that when $k_0 = \boldsymbol{Q}$, there is exactly one $\boldsymbol{Z}_{\mathfrak{l}}$-extension F of $\boldsymbol{Q}$, and it is contained in the field obtained by adjoining to $\boldsymbol{Q}$ all $\mathfrak{l}^n$th roots of unity for all n. Then for arbitrary k_0, the composite field Fk_0 is one of the $\boldsymbol{Z}_{\mathfrak{l}}$-extensions of k_0. (It is called the cyclotomic $\boldsymbol{Z}_{\mathfrak{l}}$-extension of k_0.)

We now specialize to the case where k_0 is a quadratic extension of $\boldsymbol{Q}$. Then $1 \leqq d \leqq 2$. If k_0 is a real quadratic extension of $\boldsymbol{Q}$, it is known that $d = 1$ (see [5, §2.3]). So there is a unique $\boldsymbol{Z}_{\mathfrak{l}}$-extension K of k_0, and hence the Iwasawa invariant μ is bounded on $W = \{K\}$. Next we suppose k_0 is an imaginary quadratic extension of $\boldsymbol{Q}$. Then $d = 2$, and hence there are infinitely many $\boldsymbol{Z}_{\mathfrak{l}}$-extensions of k_0, since there are infinitely many quotient groups of $\boldsymbol{Z}_{\mathfrak{l}}^2$ isomorphic to $\boldsymbol{Z}_{\mathfrak{l}}$. So W is infinite, and we must show that μ is bounded on W. If there is only one prime of k_0 above $\mathfrak{l}$, then we know from [4, Theorem 6] that μ is bounded on W. Thus it remains to consider the case where k_0 is imaginary quadratic, and $\mathfrak{l}$ decomposes in k_0.

We let $(\mathfrak{l}) = \mathfrak{p}_1\mathfrak{p}_2$, where $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are primes of k_0. We recall from the theory of $\boldsymbol{Z}_{\mathfrak{l}}$-extensions (see [5, Theorem 1]) that no primes other than $\mathfrak{p}_1$ and $\mathfrak{p}_2$ can ramify in a $\boldsymbol{Z}_{\mathfrak{l}}$-extension of k_0. We let $L = Fk_0$, the cyclotomic $\boldsymbol{Z}_{\mathfrak{l}}$-extension of k_0. Since $\mathfrak{l}$ ramifies totally in $F/\boldsymbol{Q}$ and decomposes in $k_0/\boldsymbol{Q}$, then $\mathfrak{p}_1$ and $\mathfrak{p}_2$ ramify totally in L/k_0. We let I_1(resp., I_2) be the inertia group for $\mathfrak{p}_1$(resp., $\mathfrak{p}_2$) for the extension M/k_0. (We note that we get the same inertia group for $\mathfrak{p}_1$ no matter what prime above $\mathfrak{p}_1$ in M that we use because M/k_0 has abelian Galois group. A similar result holds for $\mathfrak{p}_2$.) Next we claim that $I_1 \approx \boldsymbol{Z}_{\mathfrak{l}}$ and $I_2 \approx \boldsymbol{Z}_{\mathfrak{l}}$. Since $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are totally ramified in L/k_0, then I_1 and I_2 have quotient groups which are isomorphic to $\mathrm{Gal}\,(L/k_0) \approx \boldsymbol{Z}_{\mathfrak{l}}$. Also the completions of k_0 at $\mathfrak{p}_1$ and at $\mathfrak{p}_2$ are isomorphic to $\boldsymbol{Q}_{\mathfrak{l}}$, and by local class field theory, the inertia group for the maximal abelian $\mathfrak{l}$-extension of $\boldsymbol{Q}_{\mathfrak{l}}$ is isomorphic to the subgroup $U = \{1 + \alpha\mathfrak{l} \mid \alpha \in \boldsymbol{Z}_{\mathfrak{l}}\}$ of the group of units of $\boldsymbol{Q}_{\mathfrak{l}}$. Since $U \approx \boldsymbol{Z}_{\mathfrak{l}}$ when $\mathfrak{l} \neq 2$, then I_1 and I_2 are isomorphic to quotient groups of $\boldsymbol{Z}_{\mathfrak{l}}$ when $\mathfrak{l} \neq 2$. Combining the above results, we conclude that I_1 and I_2 are isomorphic to $\boldsymbol{Z}_{\mathfrak{l}}$

when $\mathfrak{l} \neq 2$. When $\mathfrak{l} = 2$, $U \approx \boldsymbol{Z}_2 \times (\boldsymbol{Z}_2/2\boldsymbol{Z}_2)$, and we still get $I_1 \approx \boldsymbol{Z}_2$ and $I_2 \approx \boldsymbol{Z}_2$ since I_1 and I_2 are subgroups of Gal $(M/k_0) \approx \boldsymbol{Z}_2^2$.

Now since Gal $(M/k_0) \approx \boldsymbol{Z}_\mathfrak{l}^2$, $I_1 \approx \boldsymbol{Z}_\mathfrak{l}$, $I_2 \approx \boldsymbol{Z}_\mathfrak{l}$, and $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are totally ramified in L/k_0, then Gal $(M/k_0)/I_1 \approx \boldsymbol{Z}_\mathfrak{l}$ and Gal $(M/k_0)/I_2 \approx \boldsymbol{Z}_\mathfrak{l}$. Thus there exists exactly one $\boldsymbol{Z}_\mathfrak{l}$-extension K_1/k_0(resp., K_2/k_0) in which $\mathfrak{p}_1$(resp., $\mathfrak{p}_2$) is unramified. So if K is any $\boldsymbol{Z}_\mathfrak{l}$-extension of k_0 other than K_1 and K_2, then both $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are ramified in K/k_0 (although not necessarily totally ramified). Then there are only finitely many primes of K above $\mathfrak{l}$, and hence by the results of Greenberg in [3], there is a neighborhood of K in W on which μ is bounded. Suppose we could show that K_1 and K_2 have neighborhoods on which μ is bounded. Then all $K \in W$ would have neighborhoods on which μ is bounded. Since W is compact, W is covered by a finite number of these neighborhoods, and hence μ would be bounded on W. So to complete the proof of Theorem 1, it suffices to show that μ is bounded on some neighborhood of K_1 and on some neighborhood of K_2.

We consider K_1/k_0 with intermediate fields $k_0 \subset k_1 \subset k_2 \subset \cdots \subset k_n \subset \cdots \subset K_1$. Since $\mathfrak{p}_1$ is unramified in K_1/K_0, then $\mathfrak{p}_2$ must ramify in K_1 since by class field theory the maximal unramified abelian extension of k_0 is of finite degree over k_0. So there are only finitely many primes of K_1 above $\mathfrak{p}_2$. Let t denote that finite number. Next we recall that $W(K_1, n) = \{K' \in W \mid [K_1 \cap K' : k_0] \geqq \mathfrak{l}^n\}$, and these sets $W(K_1, n)$ for $n = 1, 2, \cdots$, form a neighborhood basis for K_1 in W. Since Gal $(M/k_0) \approx \boldsymbol{Z}_\mathfrak{l}^2$ and F and K_1 are disjoint $\boldsymbol{Z}_\mathfrak{l}$-extensions of k_0, then it is clear that $M = FK_1$. If f_1 is the subfield of F such that $[f_1 : k_0] = \mathfrak{l}$, then every $K' \in W(K_1, n)$ has a subfield k'_{n+1} such that $[k'_{n+1} : k_n] = \mathfrak{l}$ and $k'_{n+1} \subset f_1 k_{n+1}$. We take n large enough so that $\mathfrak{l}^n > t$. Unless $k'_{n+1} = k_{n+1}$, there are at most $\mathfrak{l}^n$(resp., t) primes of k'_{n+1} above $\mathfrak{p}_1$(resp., $\mathfrak{p}_2$). Then if $k'_{n+1} \neq k_{n+1}$, there are at most $\mathfrak{l}^n$(resp., t) primes of K' above $\mathfrak{p}_1$(resp., $\mathfrak{p}_2$). If we let s denote the number of primes of K' that are ramified over k_0, then $s \leqq \mathfrak{l}^n + t$. From [3, Theorem 1], we see that

$$\mu(K'/k_0) \leqq e'_{n+1}/(\mathfrak{l}^{n+1} - s + 1) \leqq e'_{n+1}/(\mathfrak{l}^{n+1} - \mathfrak{l}^n - t + 1) ,$$

where $\mathfrak{l}^{e'_{n+1}}$ is the order of the $\mathfrak{l}$-class group of k'_{n+1}. Since $[f_1 k_{n+1} : k'_{n+1}] = \mathfrak{l}$, then by class field theory $e'_{n+1} \leqq \varepsilon_{n+1} + 1$, where $\mathfrak{l}^{\varepsilon_{n+1}}$ is the order of the $\mathfrak{l}$-class group of $f_1 k_{n+1}$. So if $K' \in W(K_1, n)$ and $k'_{n+1} \neq k_{n+1}$, then

$$\mu(K'/k_0) \leqq (\varepsilon_{n+1} + 1)/(\mathfrak{l}^{n+1} - \mathfrak{l}^n - t + 1) .$$

Now $f_1 K_1$ is a $\boldsymbol{Z}_\mathfrak{l}$-extension of f_1. From Equation 1, $\varepsilon_n = \mu_1 \mathfrak{l}^n + \lambda_1 n + \nu_1$ for n sufficiently large, where $\mu_1 = \mu(f_1 K_1/f_1)$, $\lambda_1 = \lambda(f_1 K_1/f_1)$, $\nu_1 = \nu(f_1 K_1/f_1)$. So for n sufficiently large,

$$\varepsilon_{n+1} + 1 = \mu_1 \mathfrak{l}^{n+1} + \lambda_1(n + 1) + \nu_1 + 1$$

and

$$\mu(K'/k_0) \leqq (\varepsilon_{n+1} + 1)/(\ell^{n+1} - \ell^n - t + 1) = \frac{\mu_1 \ell^{n+1} + \lambda_1(n+1) + \nu_1 + 1}{\ell^{n+1} - \ell^n - t + 1} .$$

Since

$$\lim_{n\to\infty} \frac{\mu_1 \ell^{n+1} + \lambda_1(n+1) + \nu_1 + 1}{\ell^{n+1} - \ell^n - t + 1} = \frac{\mu_1}{1 - \ell^{-1}} < 3\mu_1 ,$$

we see that for n sufficiently large, $\mu(K'/k_0) < 3\mu_1$ for all $K' \in W(K_1, n)$. So μ is bounded on some neighborhood of K_1. Similarly μ is bounded on some neighborhood of K_2. Hence our proof of Theorem 1 is complete.

3. Explicit upper bounds for μ in certain cases. We first consider a real quadratic extension $k_0/\boldsymbol{Q}$. Then there is only one $\boldsymbol{Z}_\ell$-extension K of k_0, namely the cyclotomic $\boldsymbol{Z}_\ell$-extension of k_0. It is known that $\mu(K/k_0) = 0$ in this case (see [2]).

Now we consider an imaginary quadratic extension $k_0/\boldsymbol{Q}$. We first suppose that ℓ ramifies or remains prime in k_0. We let H denote the maximal unramified abelian ℓ-extension of k_0, and we let ℓ^α be the exponent of $\mathrm{Gal}\,(H/k_0)$. If K is any $\boldsymbol{Z}_\ell$-extension of k_0 with intermediate fields $k_0 \subset k_1 \subset k_2 \subset \cdots \subset k_n \subset \cdots \subset K$, then the primes above ℓ in k_α ramify totally in K/k_α, and there are at most ℓ^α such primes. Then from [3, Theorem 1], we see that $\mu(K/k_0) \leqq e_\alpha$, where $\ell^{e_\alpha} = |A_\alpha|$. So in Theorem 1, we may take c to be the maximum of the e_α obtained from the extensions k_α of k_0 such that k_α is contained in a $\boldsymbol{Z}_\ell$-extension of k_0 and $[k_\alpha : k_0] = \ell^\alpha$. Frequently we can obtain a better upper bound for μ. For example, if M is the composite of all $\boldsymbol{Z}_\ell$-extensions of k_0 and if $M \cap H = k_0$, then the prime of k_0 above ℓ is totally ramified in each $\boldsymbol{Z}_\ell$-extension of k_0, and hence from [3, Corollary 1], $\mu(K/k_0) \leqq e_0$ for each $\boldsymbol{Z}_\ell$-extension K of k_0.

Finally we suppose that k_0 is an imaginary quadratic extension of $\boldsymbol{Q}$ and that ℓ decomposes in k_0. In this case we shall give an explicit upper bound for μ only under certain conditions. We let M be the composite of all $\boldsymbol{Z}_\ell$-extensions of k_0, and we let M_1 be the maximal extension of k_0 contained in M such that $\mathrm{Gal}\,(M_1/k_0)$ has exponent ℓ. We note that $\mathrm{Gal}\,(M_1/k_0) \approx (\boldsymbol{Z}_\ell/\ell\boldsymbol{Z}_\ell)^2$ since $\mathrm{Gal}\,(M/k_0) \approx \boldsymbol{Z}_\ell^2$, and hence M_1 contains $\ell + 1$ subfields of degree ℓ over k_0. We let $(\ell) = \mathfrak{p}_1$ and $\mathfrak{p}_2$ are primes in k_0. We shall assume that there is exactly one prime of M_1 above $\mathfrak{p}_1$ and exactly one prime of M_1 above $\mathfrak{p}_2$. (Note: From our discussion in §2 and our definition of M_1, we see that there is exactly one prime of M_1 above $\mathfrak{p}_1$ precisely when $\mathfrak{p}_1$ remains prime in one of the extensions of k_0 of degree ℓ and ramifies in the other l extensions of degree l over k_0. A similar result applies to $\mathfrak{p}_2$.) Then there is exactly one prime of M above $\mathfrak{p}_1$ and exactly one prime of M above $\mathfrak{p}_2$. It then follows from [3, Corollary 2] that we may take c in Theorem 1 to be the maximum of the numbers $e_1/(l-1)$ obtained from the fields k_1 contained in M_1 with $[k_1: k_0] = l$. As usual, l^{e_1} is the order of the l-class group of k_1.

In some of these situations where l decomposes in k_0, we can actually find μ, λ, ν exactly for every $\boldsymbol{Z}_l$-extension of k_0. We assume that l does not divide the class number of k_0. We let M_i be the maximal extension of k_0 contained in M such that $\mathrm{Gal}(M_i/k_0)$ has exponent l^i. (We note that $\mathrm{Gal}(M_i/k_0) \approx (\boldsymbol{Z}_l/l^i\boldsymbol{Z}_l)^2$.) We also assume that there is exactly one prime of M_1 above $\mathfrak{p}_1$ and exactly one prime of M_1 above $\mathfrak{p}_2$. Then there is only one prime of M_i above $\mathfrak{p}_1$ for each i, and only one prime of M_i above $\mathfrak{p}_2$ for each i. We recall from §2 that there is a unique $\boldsymbol{Z}_l$-extension K_1(resp., K_2) of k_0 in which $\mathfrak{p}_1$(resp., $\mathfrak{p}_2$) is unramified. Since l does not divide the class number of k_0, then $\mathfrak{p}_2$(resp., $\mathfrak{p}_1$) is totally ramified in K_1(resp., K_2). So K_1(resp., K_2) is a $\boldsymbol{Z}_l$-extension of k_0 in which exactly one prime is ramified, and that prime is totally ramified. Since l does not divide the class number of k_0, then l does not divide the class number of every subfield of K_1(resp., K_2). (See [6].) So $\mu(K_1/k_0) = \lambda(K_1/k_0) = \nu(K_1/k_0) = 0$ and $\mu(K_2/k_0) = \lambda(K_2/k_0) = \nu(K_2/k_0) = 0$. If K_1 has subfields $k_0 \subset k_1' \subset k_2' \subset \cdots \subset k_n' \subset \cdots \subset K_1$, we note that $\mathrm{Gal}(M_i/k_i')$ is a cyclic group of order l^i for each i. Since l does not divide the class number of k_i', and since there is only one prime of M_i (namely the prime of M_i above $\mathfrak{p}_1$) that is ramified over k_i', we see that l does not divide the class number of M_i for each i. Now we let K be any $\boldsymbol{Z}_l$-extension of k_0 with intermediate fields $k_0 \subset k_1 \subset k_2 \subset \cdots \subset k_n \subset \cdots \subset K$, and we suppose K_2 has intermediate fields $k_0 \subset k_1'' \subset k_2'' \subset \cdots \subset k_n'' \subset \cdots \subset K_2$. If $K \cap K_1 = k_0$ and $K \cap K_2 = k_0$, then $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are totally ramified in k_n/k_0, and then M_n/k_n is an unramified cyclic extension of degree l^n. Since l does not divide the class number of M_n, then M_n must be the Hilbert l-class field of k_n, and hence by class field theory the l-class group of k_n is a cyclic group of order l^n for all n. So $\mu(K/k_0) = 0$, $\lambda(K/k_0) = 1$, $\nu(K/k_0) = 0$. Now suppose $K \cap K_1 = k_j'$. By arguments similar to those above, it can be proved that the l-class group of k_n is trivial if $n \leqq j$ and a cyclic group of order l^{n-j} if $n > j$. So $\mu(K/k_0) = 0$, $\lambda(K/k_0) = 1$, $\nu(K/k_0) = -j$. Similarly if $K \cap K_2 = k_j''$, then $\mu(K/k_0) = 0$, $\lambda(K/k_0) = 1$, $\nu(K/k_0) = -j$.

We conclude with an example to which the results of the previous paragraph apply. We let $k_0 = \boldsymbol{Q}(\sqrt{-11})$ and $l = 3$. We note that 3 does not divide the class number of k_0, and 3 decomposes in k_0 (in face, $3 = \alpha_1\alpha_2$ with $\alpha_1 = (1 + \sqrt{-11})/2$ and $\alpha_2 = (1 - \sqrt{-11})/2$). If M_1 is the maximal extension of k_0 of exponent l contained in the composite of all Z_l-extensions of k_0, we must show that there is only one prime ideal of M_1 above (α_1) and only one prime ideal of M_1 above (α_2). Then the results of the previous paragraph will apply to k_0. Now we let $E = \boldsymbol{Q}(\sqrt{-11}, \zeta)$, where $\zeta = (-1 + \sqrt{-3})/2$ (a primitive cube root of unity). Then $[E: \boldsymbol{Q}] = 4$, and the three quadratic subfields are k_0, $\boldsymbol{Q}(\sqrt{33})$, $\boldsymbol{Q}(\sqrt{-3})$. We note that there is exactly one prime of E above (α_1) and exactly one prime of E above (α_2). Since 3 does not divide the class numbers of the quadratic subfields of E, then it is easy to see that 3 does not divide the class number of E. It then follows from Kummer theory that the maximal abelian extension of E of exponent 3 in which only primes above 3 are ramified is $E(\alpha_1^{1/3}, \alpha_2^{1/3}, \zeta^{1/3}, \varepsilon^{1/3})$, where $\varepsilon = 23 + 4\sqrt{33}$ is the fundamental unit of $\boldsymbol{Q}(\sqrt{33})$. It is not difficult to see that $M_1E = E(\zeta^{1/3}, \varepsilon^{1/3})$ (cf. [1, Example 3]). Again using Kummer theory, a calculation shows that the prime of E above (α_1) remains prime in one of the cubic extensions of E contained in M_1E and ramifies in the other three cubic extensions of E contained in M_1E. A similar result is valid for the prime of E above (α_2). It follows that there can be only one prime of M_1 above (α_1) and only one prime of M_1 above (α_2). Hence the results of the previous paragraph apply to $k_0 = \boldsymbol{Q}(\sqrt{-11})$.

Note. We have learned that the Russian mathematician V. A. Babaĭcev has obtained by other methods a proof of Theorem 1 (see Math. USSR Izvestija, 10 (1976), 675-685).

REFERENCES

1. J. Carroll and H. Kisilevsky, *Initial layers of Z_l-extensions of complex quadratic fields*, Compositio Mathematica, **32** (1976). 157-168.

2. B. Ferrero and L. Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields*, to appear.

3. F. Gerth, *Upper bounds for μ in Z_l-extensions*, to appear.

4. R. Greenberg, *The Iwasawa invariants of Γ-extensions of a fixed number field*, Amer. J. Math., **95** (1973), 204-214.

5. K. Iwasawa, *On Z_l-extensions of algebraic number fields*, Ann. Math., **98** (1973), 246-326.

6. ———, *A note on class numbers of algebraic number fields*, Abh. Math. Sem. Univ. Hamburg, **20** (1956), 257-258.

Received April 4, 1978. Partly supported by NSF Grant MCS 78-01459.

THE UNIVERSITY OF TEXAS
AUSTIN, TX 78712