Pacific Journal of Mathematics

Γ-EXTENSIONS OF IMAGINARY QUADRATIC FIELDS

ROBERT GOLD

Vol. 40, No. 1 September 1972

PACIFIC JOURNAL OF MATHEMATICS
Vol. 40, No. 1, 1972

Γ-EXTENSIONS OF IMAGINARY QUADRATIC FIELDS

ROBERT GOLD

Let p be an odd rational prime and $E_0 = Q(\sqrt{-m})$ a quadratic imaginary number field. There is a unique Γ-extension E of E_0 for the prime p which is absolutely abelian. For each positive integer n there is a subfield E_n of E which is cyclic of degree p^n over E_0 and by Iwasawa the exponent of p in the class number of E_n is of the form $\mu p^n + \lambda n + c$ for sufficiently large n. We here examine the analytic formula for the class number of E_n and in the case $p = 3$ give a simple condition implying that $\mu = 0$. It follows easily from this condition that there are infinitely many imaginary quadratic fields which have Γ-extensions for the prime 3 with the invariants $\mu = 0$ while $\lambda \geqq 1$.

1. Analytic formula. Let Q be the rationals, p an odd prime, n an integer $\geqq 0$, and $\zeta_{p^{n+1}}$ a primitive p^{n+1} root of unity. Let F_n be the subfield of $Q(\zeta_{p^{n+1}})$ of degree p^n over the rationals so that F_n/Q is cyclic, p is the unique ramified prime for the extension, and p is totally ramified. Let $E_0 = Q(\sqrt{-m})$, a quadratic imaginary field where $(m, p) = 1$ and let $E_n = F_n.E_0$, the composite field.

We attempt to study the order, e_n, to which p divides the class number of E_n,

$$h_{E_n} = p^{e_n} \cdot h' \qquad (p, h') = 1$$

by use of the classical analytic formula for an arbitrary number field k:

$$\lim_{s \to 1} (s - 1)\zeta_k(s) = \frac{2^{s+t}\pi^t R_k}{m_k\sqrt{|D_k|}} h_k \tag{1}$$

where, as usual, R_k is the regulator of k; m_k, the order of the group of roots of unity; D_k, the discriminant of k; and s and t, the number of real and complex infinite primes of k.

We note the following sequence of lemmas:

LEMMA 1. *$m_{E_n} = m_{F_n} = 2$ unless $E_0 = Q(\sqrt{-3})$ or $Q(\sqrt{-1})$.*

Proof. By degrees: $[E_n : Q] = 2p^n$.

Note that in the two excluded cases $(p, m_{E_n}) = 1$ if $(p, m) = 1$.

LEMMA 2. $D_{E_n} = D_{F_n}^2 \cdot D_{E_0}^{p^n}$ *and* $D_{F_n} = p^{t_n}$; $t_n = (n+1)p^n - (p^n - 1)/(p-1) - 1$.

Proof. First statement is trivial, second is proved as follows.

Note that $\zeta_{p^{n+1}}$ is a distinguished element for the extension $\mathcal{Q}(\zeta_{p^{n+1}})/F_n$ in the relation its different bears to the different of the extension [3]. The computation of the different of $\mathcal{Q}(\zeta_{p^{n+1}})/F_n$ becomes then an exercise in determinants. The result combined with the well known different of $\mathcal{Q}(\zeta_{p^{n+1}})/\mathcal{Q}$ gives the expression above.

LEMMA 3. $R_{E_n} = R_{F_n} \cdot 2^a$ *some* $a \in Z$.

Proof. F_n is the maximal real subfield of E_n and the result is then well known [1].

Now let $k = E_n$, respectively F_n, in equation (1) and divide the former by the latter. Taking into account the preceding lemmas this simplifies to:

$$\lim_{s\to 1} (\zeta_{E_n}(s)/\zeta_{F_n}(s)) = \frac{2^a \pi^{p^n}}{\sqrt{|D_{E_0}|^{p^n}}} \frac{h_{E_n}}{p^{s_n} h_{F_n}} \tag{2}$$

$$s_n = \frac{1}{2} t_n = \frac{1}{2}((n+1)p^n - (p^n - 1)/(p-1) - 1) .$$

On the other hand $\zeta_{E_n}(s) = \prod L(s, \chi)$ where the product is taken over all Dirichlet characters belonging to the extension $E_n/\mathcal{Q}$. Since $g(E_n/\mathcal{Q}) \cong \mathcal{Z}/2 + \mathcal{Z}/p^n$ we can write $\zeta_{E_n}(s) = \prod L(s, \chi_0^i \chi_1^j)$, $i = 0, 1$; $j = 0, \cdots, p^n - 1$ where χ_0, χ_0^2 are the characters belonging to $E_0/\mathcal{Q}$ while $\chi_1^0, \cdots, \chi_1^{p^n - 1}$ are the characters belonging to $F_n/\mathcal{Q}$. Hence $\zeta_{F_n}(s) = \prod L(s, \chi_1^j)$, $j = 0, \cdots, p^n - 1$ and therefore $\zeta_{E_n}(s)/\zeta_{F_n}(s) = \prod L(s, \chi_0 \chi_1^j)$, $j = 0, \cdots, p^n - 1$. Furthermore the χ_1^{pk}, $k = 0, \cdots, p^{n-1} - 1$ are the characters belonging to $F_{n-1}/\mathcal{Q}$ and therefore

$$\frac{\zeta_{E_n}(s)/\zeta_{F_n}(s)}{\zeta_{E_{n-1}}(s)/\zeta_{F_{n-1}}(s)} = \prod_{\substack{0<j<p^n \\ (j,p)=1}} L(s, \chi_0 \chi_1^j) . \tag{3}$$

Note in passing that χ_1 is an even character and takes on the p^nth roots of unity as values. Comparing (2) and (3) we may write

$$\prod_{\substack{0<j<p^n \\ (j,p)=1}} L(1, \chi_0 \chi_1^j) = \frac{h_{E_n} \cdot h_{F_{n-1}} \pi^{\varphi(p^n)}}{h_{F_n} h_{E_{n-1}} p^{(s_n - s_{n-1})} \sqrt{|D_{E_0}|^{\varphi(p^n)}}} . \tag{4}$$

Note that χ_0 is primitive modulo $d = D_{E_0}$ = the conductor of $E_0/\mathcal{Q}$, while χ_1^j, $(j, p) = 1$ is primitive modulo p^{n+1} = the conductor of $F_n/\mathcal{Q}$. It follows that $\chi_0 \chi_1^j$, $(j, p) = 1$ is primitive with modulus $w = dp^{n+1}$ and is an odd character. It is well known then that

$$L(1, \chi_0\chi_1^j) = \frac{\pi i \tau(\chi_0\chi_1^j)}{w^2} \sum_{\substack{0<k<w \\ (k,w)=1}} \chi_0\bar{\chi}_1^j(k)k \tag{5}$$

where $\tau(\chi_0\chi_1^j)$ is the classical Gauss sum and $|\tau(\chi_0\chi_1^j)| = \sqrt{w}$. Comparing now (4) and (5) and taking absolute values we see

$$\frac{\left|\prod_{\substack{(j,p)=1 \\ 0<j<p^n}} \sum_{\substack{(k,w)=1 \\ 0<k<w}} \chi_0\bar{\chi}_1^j(k)k\right|}{d^{\varphi(p^n)} p^{(n+1)\varphi(p^n)}} = \frac{h_{E_n} h_{F_{n-1}}}{h_{F_n} h_{E_{n-1}}} . \tag{6}$$

Next we examine the sum appearing in (6).

$$\begin{aligned} S_j = \sum_{0<k<w} \chi_0\bar{\chi}_1^j(k)k &= \sum_{\alpha=0}^{d-1} \sum_{i=0}^{p^{n+1}-1} \chi_0\bar{\chi}_1^j(i + \alpha p^{n+1})(i + \alpha p^{n+1}) \\ &= \sum_{\alpha=0}^{d-1} \sum_{i=0}^{p^{n+1}-1} \chi_0(i + \alpha p^{n+1})\bar{\chi}_1^j(i)i + \alpha p^{n+1} \sum_{i=0}^{p^{n+1}} \bar{\chi}_1^j(i)\chi_0(i + \alpha p^{n+1}) . \end{aligned}$$

But since

$$\sum_{\alpha=0}^{d-1} \sum_{i=0}^{p^{n+1}-1} \bar{\chi}_1^j(i)\chi_0(i + \alpha p^{n+1})i = \sum_{i=0}^{p^{n+1}-1} \bar{\chi}_1^j(i)i \sum_{\alpha=0}^{d-1} \chi_0(i + \alpha p^{n+1}) = 0$$

we have

$$S_j = p^{n+1} \sum_{i=0}^{p^{n+1}-1} \bar{\chi}_1^j(i) \sum_{\alpha=0}^{d-1} \alpha\chi_0(i + \alpha p^{n+1}) .$$

We now make the following assumption for the sake of simplifying notation and proofs: (A) $p^{n+1} \equiv 1(d)$. It then follows that

$$S_j = p^{n+1} \sum_i \bar{\chi}_1^j(i) \sum_\alpha \chi_0(i\alpha + \alpha) .$$

Letting $w_k = \sum_{\alpha=0}^{d-1} \alpha\chi_0(\alpha + k)$ one can easily deduce that $w_0 = w_1$, $w_{k+d} = w_k$, and $w_k = w_0 + d \sum_{\alpha=0}^{k-1} \chi_0(\alpha)$. Then

$$\begin{aligned} S_j &= p^{n+1} \sum_{i=0}^{p^{n+1}-1} \bar{\chi}_1^j(i) w_0 + d \sum_{\alpha=0}^{i-1} \chi_0(\alpha) \\ &= p^{n+1} w_0 \sum_{i=0}^{p^{n+1}-1} \bar{\chi}_1^j(i) + d \sum_{i=0}^{p^{n+1}-1} \bar{\chi}_1^j(i) \sum_{\alpha=0}^{i-1} \chi_0(\alpha) \\ &= dp^{n+1} \sum_{i=0}^{p^{n+1}-1} \bar{\chi}_1^j(i) \cdot \alpha_i ; \quad \text{where} \quad \alpha_i = \sum_{\alpha=0}^{i-1} \chi_0(\alpha) . \end{aligned}$$

Comparing this last result with (6) we see that

$$\prod_{\substack{(j,p)=1 \\ 0<j<p^{n+1}}} \sum_{i=0}^{p^{n+1}-1} \alpha_i \bar{\chi}_1^j(i) = \frac{h_{E_n} h_{F_{n-1}}}{h_{F_n} h_{E_{n-1}}} , \tag{7}$$

and again $\alpha_i = \sum_{\alpha=0}^{i-1} \chi_0(\alpha)$.

We reduce our concern now to the power of p occurring in each member of (7). By results of Iwasawa $(p, h_{F_n}) = (p, h_{F_{n-1}}) = 1$ while for sufficiently large n: $\mathrm{ord}_p(h_{E_n}) = \mu p^n + \lambda n + c$, $\mathrm{ord}_p(h_{E_{n-1}}) = \mu p^{n-1} + \lambda(n-1) + c$ ([2]). Therefore

$$(8) \qquad \mathrm{ord}_p \prod_{0<j<p^{n+1}} \sum_{i=0}^{p^{n+1}-1} \alpha_i \bar{\chi}_1^j(i) = \mu\varphi(p^n) + \lambda .$$

It is clear that $\alpha_i \in \mathscr{Z}$ and hence $\sum_{i=0}^{p^{n+1}-1} \alpha_i \bar{\chi}_1^j(i)$ is an integer in $\mathscr{Q}(\zeta_{p^n})$. In fact, $\prod \sum \alpha_i \bar{\chi}_1^j(i)$ is simply the absolute norm of this integer. Hence

$$(9) \qquad \begin{aligned} \mu\varphi(p^n) + \lambda &= \mathrm{ord}_p \mathscr{N}_Q\left(\sum_{i=0}^{p^{n+1}-1} \alpha_i \chi_1(i)\right) \\ &= \mathrm{ord}_{\mathfrak{p}} \sum_{i=0}^{p^{n+1}-1} \alpha_i \chi_1(i) . \end{aligned}$$

Here $\mathfrak{p}$ is the unique prime of $\mathscr{Q}(\zeta_{p^n})$ dividing p.

We now rewrite $\sum \alpha_i \chi_1(i)$ in terms of an integral basis of $\mathscr{Q}(\zeta_{p^n})$. Let g be a primitive root modulo p^{n+1}, i.e. $\bar{g}$ generates $(\mathscr{Z}/p^{n+1})^*$. Then $\sum_{i=0}^{p^{n+1}-1} \alpha_i \chi_1(i) = \sum_{s=0}^{\varphi(p^{n+1})-1} \alpha_{g_s} \chi_1(g^s)$ where $0 < g_s < p^{n+1}$ and $g_s \equiv g^s(p^{n+1})$. Then $\eta = \chi_1(g)$ is a primitive p^nth root of unity and

$$\sum_{s=0}^{\varphi(p^{n+1})-1} \chi_1(g^s)\alpha_{g_s} = \sum_{s=0}^{\varphi(p^{n+1})-1} \eta^s \alpha_{g_s} .$$

Since $1, \eta, \cdots, \eta^{\varphi(p^n)-1}$ form a $\mathscr{Z}$-basis for the integers of $\mathscr{Q}(\zeta_{p^n})$ we may rewrite this last sum, using identities of the form $1 + \eta^{p^{n-1}} + \cdots + \eta^{(p-1)p^{n-1}} = 0$, as

$$\sum_{s=0}^{\varphi(p^{n+1})-1} \eta^s \alpha_{g_s} = \sum_{s=0}^{\varphi(p^n)-1} \eta^s \sum_{i=0}^{p-2} (\alpha_{g_{s+ip^n}} - \alpha_{g_{\varphi(p^n)+t+ip^n}})$$

where $0<t<p^{n-1}$ and $t \equiv s(p^{n-1})$. It follows from (9) then that

$$(10) \qquad \mu\varphi(p^n) + \lambda = \mathrm{ord}_{\mathfrak{p}} \sum_{s=0}^{\varphi(p^n)-1} \eta^s \sum_{i=0}^{p-2} (\alpha_{g_{s+ip^n}} - \alpha_{g_{\varphi(p^n)+t+ip^n}}) .$$

For sufficiently large n the left member of (10) is $\geqq \varphi(p^n)$ if and only if $\mu > 0$. However the right member is greater than $\varphi(p^n)$ if and only if $\mathfrak{p}^{\varphi(p^n)} = (p)$ divides the algebraic integer in brackets. Since this integer is written in terms of an integral basis it is divisible by (p) if and only if the coefficients of η^s is divisible by p for every s. Hence $\mu > 0$ if and only if p divides

$$(11) \qquad \sum_{i=0}^{p-2} (\alpha_{g_{s+ip^n}} - \alpha_{g_{\varphi(p^n)+t+ip^n}}) \qquad s = 0, 1, \cdots, \varphi(p^n) - 1 .$$

2. **Special case of $p = 3$.** If we specialize to $p = 3$, $s = 0$ we

may proceed in the following manner. For $p=3$, $s=0$ equation (11) reads

$$\alpha_{g_0}+\alpha_{g_{3^n}}-\alpha_{g_{(3^n)}}-\alpha_{g_{3^n+\varphi(3^n)}}\,. \tag{12}$$

Clearly $g_0=1$, $g_{3^n}=3^{n+1}-1$; while for appropriate choice of g we have $g_{\varphi(3^n)}=3^n+1$ (resp. 2.3^n+1) and $g_{\varphi(3^n)+3^n}=2\cdot 3^n-1$ (resp. 3^n-1). Hence (12) reads, letting $M(m)=\sum_{\alpha=0}^{m}\chi_0(\alpha)$,

$$\begin{aligned}&M(0)+M(3^{n+1})-M(3^n)-M(2\cdot 3^n-2)\\&(\text{resp. } M(0)+M(3^{n+1}-2)-M(2\cdot 3^n)-M(3^n-2))\,.\end{aligned} \tag{13}$$

Clearly $M(0)=0$ and recalling that (A) $3^{n+1}\equiv 1$ (d) we see that $M(3^{n+1}-2)=M(d-1)=0$ as well. Since $\chi_0(-1)=-1$ we have the trivial but useful identity $M(m)=M(kd-m-1)$, $kd-m-1>0$. By this it follows that $M(2\cdot 3^n-2)=M(kd+1-3^n-2)=M(kd-3^n-1)=M(3^n)$ (resp. $M(3^n-2)=M(2\cdot 3^n)$). Hence (13) reduces to $-2M(3^n)$ (resp. $-2M(2\cdot 3^n)$) and so $\mu>0$ if and only if $M(3^n)\equiv 0$ (3) (resp. $M(2\cdot 3^n)\equiv 0$ (3)).

Again by (A): $M(2\cdot 3^n)=M(kd+1-3^n)=M(3^n-2)=M(3^n)-\chi_0(3^n)-\chi_0(3^n-1)$. Since both congruences above must be satisfied it follows that $\mu>0$ if and only if $\chi_0(3^n)+\chi_0(3^n-1)\equiv 0$ (3). Multiplying by $\chi_0(3)\neq 0$ we have $[\chi_0(3^n)+\chi_0(3^n-1)]=\chi_0(3)=\chi_0(1)-\chi_0(2)$. Hence we may finally state in the language of Iwasawa

THEOREM. *Let $E_\infty=\bigcup E_n$ be the absolutely abelian Γ-extension for the prime* 3 *of $\mathcal{Q}(\sqrt{-m})$; $(m,3)=1$. If* 2 *does not split in $\mathcal{Q}(\sqrt{-m})/\mathcal{Q}$ then the invariant μ equals* 0.

EXAMPLE 1. $E_0=\mathcal{Q}(\sqrt{-5})$. Since $\chi_0(3)=+1$, 3 splits in $\mathcal{Q}(\sqrt{-5})/\mathcal{Q}$ and it is easy to see from the structure of the genus field for E_n/E_0 that $\lambda\geqq 1$. On the other hand, $\chi_0(2)=0$ and therefore $\mu=0$. Obviously all $\mathcal{Q}(\sqrt{-m})$ for $m\equiv 7,10$ (12) behave in this manner.

EXAMPLE 2. $E_0=\mathcal{Q}(\sqrt{-23})$. This field has class number 3 and is therefore of some interest. Unfortunately $\chi_0(2)=1$, but we may use the remark above that $\mu>0$ if and only if $M(3^n)\equiv 0$ (3). By (A): $M(3^n)=M(3^{-1})=M(8)$ in this case. But $M(8)=4\not\equiv 0$ (3) and so again $\mu=0$.

REFERENCES

1. H. Hasse, *Uber die Klassenzahl Abelscher Zahlkörper*, Akademie-Verlag, 1952.
2. K. Iwasawa, *On Γ-extensions of algebraic number fields*, Bull. Amer. Math. Soc., **65** (1959).

3. S. Lang, *Algebraic Numbers*, Addison-Wesley, 1964 (III, 2)

Received March 12, 1970. The contents of this paper are part of the author's Ph. D. thesis, M. I. T., 1968, written under Professor N. Ankeny. The author would like to thank Professors Ankeny and K. Iwasawa for their aid and encouragement.

OHIO STATE UNIVERSITY

Printed in Japan by International Academic Printing Co., Ltd., Tokyo, Japan

Pacific Journal of Mathematics

Vol. 40, No. 1 September, 1972