MATHEMATICS OF COMPUTATION
VOLUME 61, NUMBER 204
OCTOBER 1993, PAGES 881-887

THE RELATIVE CLASS NUMBERS OF IMAGINARY CYCLIC FIELDS OF DEGREES 4, 6, 8, AND 10

KURT GIRSTMAIR

ABSTRACT. We express the relative class number of an imaginary abelian number field K of prime power conductor as a sort of Maillet determinant. Thereby we obtain explicit relative class number formulas for fields K of conductor p, $p \geq 3$ prime, and degree $2d = [K: \mathbb{Q}] \leq 10$, in terms of sums of $2d$-power residues. In particular, tables are given for $p \leq 10000$.

INTRODUCTION

Let p, m be in $\mathbb{N}$, p prime. In a number of papers the relative class number of the p^mth cyclotomic field has been expressed as a rational determinant (Maillet's determinant; cf. [1, 8, 10, 11], see also [12, 3]). Moreover, an explicit relative class number formula in terms of quartic power residues modulo p has been given for imaginary cyclic quartic fields of conductor p [9, 7]. The aim of the present article is to study a generalization of Maillet's determinant that yields relative class number formulas for *arbitrary* imaginary abelian fields K of conductor p^m (Theorem 1). By specializing these formulas to fields K of degree $[K: \mathbb{Q}] = 2d$ and conductor p, we obtain *explicit* relative class number formulas in the cases $d = 1, 2, 3, 4, 5$ (the formula for $d = 1$ is well known, of course). Our formulas are used to compute relative class number tables for $d = 3, 4, 5$ and $p \leq 10000$ (Tables 1–3 in the Supplement section; the respective table for $d = 2$ can be found in [6]).

1. GENERALIZED MAILLET DETERMINANTS

Let K be an imaginary abelian number field of conductor n. In particular, K is contained in the nth cyclotomic field $\mathbb{Q}(\zeta_n)$, $\zeta_n = e^{2\pi i/n}$. By G_n we denote the Galois group

$$G_n = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}).$$

Let $(\mathbb{Z}/n\mathbb{Z})^\times$ be the prime residue group $\bmod n$. There is a canonical isomorphism

$$(\mathbb{Z}/n\mathbb{Z})^\times \to G_n$$

which maps the residue class $\overline{k}$, $k \in \mathbb{Z}$, onto σ_k, σ_k being defined by $\sigma_k(\zeta_n) = \zeta_n^k$. For this reason we shall frequently identify $\overline{k}$ with σ_k, and thus the group $(\mathbb{Z}/n\mathbb{Z})^\times$ with G_n.

Received by the editor August 30, 1991 and, in revised form, November 17, 1992.
1991 *Mathematics Subject Classification*. Primary 11R29, 11R20, 11-04.

Let $H \subseteq G_n$ be the Galois group

$$H = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/K) = \{\sigma \in G_n\,;\ \sigma|_K = \mathrm{id}\}.$$

Since K is imaginary, H does not contain complex conjugation $\sigma_{-1} = \overline{-1}$. Therefore, $K^+ = K \cap \mathbb{R}$ is a proper subfield of K, and $H^+ = \langle\{\overline{-1}\} \cup H\rangle$ is the Galois group $H^+ = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/K^+)$. The group index $[H^+ : H]$ equals 2. We write $d = [K^+ : \mathbb{Q}]$, which means $[K : \mathbb{Q}] = 2d$. Now let X_n be the character group of G_n, $X \subseteq X_n$ the character group of K (i.e., the character group of G_n/H), X^+ the character group of K^+, and $X^- = X \backslash X^+$. We fix an arbitrary character ψ in X^-. This is the same as saying $\psi(\overline{k}) = 1$ for each $\overline{k} \in H$, and $\psi(\overline{-1}) = -1$.

For a given number $k \in \mathbb{Z}$, let $[k] = [\overline{k}]$ be defined by

$$k \equiv [k] \mod n \quad \text{and} \quad [k] \in \{0, 1, \dots, n-1\}.$$

If $(k, n) = 1$, we put

$$E_k = \psi(\overline{k}) \sum_{\substack{j=1 \\ \overline{j} \in H}}^{n} (2[kj] - n).$$

Proposition 1. *With the above notations,*

$$E_k = \sum_{\substack{j=1 \\ \overline{j} \in \overline{k}H^+}}^{n} \psi(\overline{j})[j].$$

In particular, E_k depends on the residue class of $\overline{k}$ modulo H^+ only.

Proof. Since $\psi(\overline{j}) = 1$ for all elements $\overline{j} \in H$, one obtains

$$E_k = \sum_{\overline{j} \in H} \psi(\overline{kj})(2[kj] - n).$$

Now E_k can be rewritten as

$$\begin{aligned} E_k &= \frac{1}{2} \sum_{\overline{j} \in H} (\psi(\overline{kj})(2[kj] - n) + \psi(\overline{-kj})(2[-kj] - n)) \\ &= \frac{1}{2} \sum_{\overline{j} \in \overline{k}H^+} \psi(\overline{j})(2[j] - n) \\ &= \sum_{\overline{j} \in \overline{k}H^+} \psi(\overline{j})[j] - \frac{n}{2}\psi(\overline{k}) \sum_{\overline{j} \in H^+} \psi(\overline{j}). \end{aligned}$$

However, the last sum is 0, since $\psi(\overline{j}) = 1$ for $\overline{j} \in H$, $\psi(\overline{j}) = -1$ for $\overline{j} \in H^+ \backslash H$, and $|H| = |H^+ \backslash H| = d$. $\square$

In view of Proposition 1 we may write $E_k = E_r$, where r is the residue class of $\overline{k}$ modulo H^+.

Let $\mathscr{R} \subseteq \mathbb{Z}$ be a system of representatives of G_n/H^+. In particular, $|\mathscr{R}| = d$. Suppose, moreover, that $\mathscr{R}$ is ordered in some way. We put

$$D = \det(E_{kj})_{k, j \in \mathscr{R}} = \det(E_{rs})_{r, s \in G_n/H^+},$$

and

$$D^* = \det(E_{rs-1})_{r,s \in G_n/H^+}.$$

Finally, let $\delta = |\{k \in \mathscr{R}\,;\, \overline{k}^2 \in H^+\}|$. We get

Proposition 2. *In the above situation,*

$$D = (-1)^{(d-\delta)/2} \cdot D^*.$$

Proof. Consider the permutation

$$\rho\colon G_n/H^+ \to G_n/H^+$$

of G_n/H^+, defined by $\rho(r) = r^{-1}$. Clearly, $D = \operatorname{sign}(\rho) \cdot D^*$. But $\operatorname{sign}(\rho) = (-1)^\varepsilon$, with $\varepsilon = |\{r \in G_n/H^+\,;\, r \neq r^{-1}\}|/2 = (d - |\{r \in G_n/H^+\,;\, r^2 = 1\}|)/2 = (d-\delta)/2$. □

For a prime divisor p of n, let e_p (resp. e_p^+) be the ramification index of p in K (resp. K^+). Similarly, g_p (resp. g_p^+) denotes the number of prime divisors of p in K (resp. K^+).

Theorem 1. *Let the above notations hold. Then $D^* = 0$ if there is a p, $p|n$, with $g_p = 2g_p^+$. Otherwise,*

$$D^* = (-2n)^d 2^\kappa h^-/(Q \cdot w),$$

with

$\kappa = \sum\{g_p^+\,;\, p|n,\, g_p = g_p^+,\, e_p = e_p^+\}$,
h^- = *relative class number of* K,
Q = *unit index of* K,
w = *number of roots of unity in* K (*for notation, cf.* [5]).

Proof. By its definition, D^* is a group determinant belonging to the abelian group G_n/H^+, which means (cf. [5, p. 23])

$$D^* = \prod_{\chi \in X^+} \left(\sum_{r \in G_n/H^+} \chi(r) \cdot E_r \right).$$

It is easy to see that

$$\sum_{r \in G_n/H^+} \chi(r) \cdot E_r = \sum_{\substack{k=1 \\ (k,n)=1}}^{n} \chi\psi(\overline{k}) \cdot k,$$

whence

$$D^* = \prod_{\chi \in X^-} \left(\sum_{\substack{k=1 \\ (k,n)=1}}^{n} \chi(\overline{k}) \cdot k \right).$$

Now let f_χ denote the conductor of χ, and χ_f the primitive character of $(\mathbb{Z}/f_\chi\mathbb{Z})^\times$ that belongs to χ. A reduction formula of Hasse (cf. [5, p. 18]) says

$$\sum_{\substack{k=1 \\ (k,n)=1}}^{n} \chi(\overline{k}) \cdot k = n \cdot \prod_{p|n} (1 - \chi_f(p)) \cdot B_\chi,$$

where B_χ is the generalized Bernoulli number

$$B_\chi = \sum_{k=1}^{f_\chi} \chi_f(\overline{k}) \cdot k/f_\chi.$$

The product $\prod_{\chi\in X^-}(1-\chi_f(p))$ can be evaluated in a well-known way (cf., e.g., [2]). We obtain

$$\prod_{\chi\in X^-}(1-\chi_f(p)) = \begin{cases} 0 & \text{if } g_p = 2g_p^+, \\ 1 & \text{if } e_p = 2e_p^+, \\ 2 & \text{if } g_p = g_p^+, \ e_p = e_p^+. \end{cases}$$

Finally,

$$\prod_{\chi\in X^-} B_\chi = (-2)^d \cdot h^-/(Q\cdot w)$$

(cf. [5, p. 12]). On putting these results together, one gets the theorem. □

Let us now consider the *special case* $n = p^m$, p an odd prime. Then K is a cyclic extension of $\mathbb{Q}$ with $[K:\mathbb{Q}] = 2d$. Since $e_p = 2e_p^+$, the number κ is 0. According to [5, p. 68], the unit index Q equals 1. The number w is given by the following

Proposition 3. *With the above conventions,*

$$w = \begin{cases} 2\cdot p^m & \textit{if } K = \mathbb{Q}(\zeta_n), \\ 2 & \textit{otherwise.} \end{cases}$$

Proof. Assume that K contains a root of unity different from ± 1. Then K contains a root of unity of p-power order. Therefore, $\zeta_p \in K$. But then $[\mathbb{Q}(\zeta_n): K] = p^k$ for some k, $0 \le k \le m-1$. Since $\mathbb{Q}(\zeta_n)$ is cyclic over $\mathbb{Q}$, there is only one subfield K of $\mathbb{Q}(\zeta_n)$ with this property, viz., $K = \mathbb{Q}(\zeta_{p^{m-k}})$. However, $n = p^m$ is the conductor of K; hence $k = 0$. □

On collecting the above observations, we obtain the

Corollary to Theorem 1. *Let $p \ge 3$ be prime, $n = p^m$, $m \ge 1$, and K be an imaginary abelian field of conductor n and degree $2d = [K:\mathbb{Q}]$. Then*

$$D^* = \begin{cases} (-1)^d(2n)^{d-1}\cdot h^- & \textit{if } K = \mathbb{Q}(\zeta_n), \\ (-n)^d \cdot 2^{d-1}\cdot h^- & \textit{otherwise.} \end{cases}$$

2. The case of a prime conductor

Let, in particular, $n = p \ge 3$ be prime, which implies that $2d|(p-1)$. Then

$$H = G_p^{2d} = \{\overline{k}^{2d}; \overline{k} \in G_p\}.$$

Since $\overline{-1}$ is not in H, we get $(-1)^{(p-1)/(2d)} \equiv -1 \bmod p$, and $p \equiv 1 + 2d \bmod 4d$. If, conversely, $p \equiv 1 + 2d \bmod 4d$, there is a uniquely determined subfield K of $\mathbb{Q}(\zeta_p)$ with $[K:\mathbb{Q}] = 2d$, and K is imaginary. We now choose a number $g \in \mathbb{Z}\backslash p\mathbb{Z}$ such that $\mathscr{R} = \{1, g, g^2, \dots, g^{d-1}\}$ is a system of representatives for G_p/H^+. This is the same as saying that

$$(*) \qquad g^{k(p-1)/d} \not\equiv 1 \bmod p$$

for each $k \in \{1, \dots, d-1\}$. We define

$$(**) \qquad F_k = \sum_{j=1}^{p-1} (2[g^k j^{2d}] - p), \qquad k \in \mathbb{Z}.$$

Then $\psi(\overline{g}^k) \cdot F_k = 2d \cdot E_{g^k}$. By Proposition 2 and the corollary of Theorem 1,

$$(***) \qquad \det(\psi(\overline{g}^{j+k}) F_{j+k})_{j,k=0,\dots,d-1} = (2d)^d \cdot D = c \cdot h^-,$$

with

$$c = \begin{cases} (-1)^{(3d-1)/2} \cdot 2^{2d-1} \cdot p^{d-1} \cdot d^d & \text{if } d = (p-1)/2, \\ & p \equiv 3 \bmod 4, \\ (-1)^{(3d-2)/2} \cdot 2^{2d-1} \cdot p^{d-1} \cdot d^d & \text{if } d = (p-1)/2, \\ & p \equiv 1 \bmod 4, \\ (-1)^{(3d-1)/2} \cdot 2^{2d-1} \cdot (pd)^d & \text{if } d < (p-1)/2, \\ & d \text{ odd}, \\ (-1)^{(3d-2)/2} \cdot 2^{2d-1} \cdot (pd)^d & \text{if } d < (p-1)/2, \\ & d \text{ even}. \end{cases}$$

Examples. For small numbers d it is easy to write down the determinant in $(***)$ term by term. We do so for $d = 1, \dots, 5$.

1. Let $d = 1$, i.e., $p \equiv 3 \bmod 4$, and $p > 3$. In this case $(***)$ means

$$F_0 = \sum_{j=1}^{p-1} (2[j^2] - p) = -2p \cdot h^-.$$

This is well known (cf. [4, p. 387]).

2. Let $d = 2$, i.e., $p \equiv 5 \bmod 8$, and $p > 5$. Because of $(\frac{2}{p}) \equiv 2^{(p-1)/2} \equiv -1 \bmod p$, the number $g = 2$ has property $(*)$, and the character ψ can be defined by

$$\psi(\overline{2}) = i, \qquad \psi(\overline{k}) = 1,$$

for all $k \in H = G_p^4$. With F_k defined as in $(**)$, formula $(***)$ reads as

$$\det \begin{pmatrix} F_0 & iF_1 \\ iF_1 & F_0 \end{pmatrix} = F_0^2 + F_1^2 = 32 \cdot p^2 \cdot h^-.$$

3. Let $d = 3$, i.e., $p \equiv 7 \bmod 12$, and $p > 7$. Choose a number $g' \in \mathbb{Z} \backslash p\mathbb{Z}$ such that $g'^{(p-1)/3} \not\equiv 1 \bmod p$. Then put $g = g'^2$. Moreover, since $p \equiv 3 \bmod 4$, the Legendre symbol $\psi = (\frac{\cdot}{p})$ is an odd character with $H = G_p^6$ contained in $\operatorname{Ker}\psi$. However, $\psi(\overline{g}^k) = 1$, $k = 0, 1, 2$, and, with F_k as in $(**)$, formula $(***)$ takes the form

$$3 \cdot F_0 \cdot F_1 \cdot F_2 - (F_0^3 + F_1^3 + F_2^3) = 864 \cdot p^3 \cdot h^-.$$

4. Let $d = 4$, i.e., $p \equiv 9 \bmod 16$, and $p > 9$. Choose $g \in \mathbb{Z} \backslash pZ$ such that $(\frac{g}{p}) \equiv g^{(p-1)/2} \equiv -1 \bmod p$. Then g has property $(*)$, and ψ can be defined by $\psi(\overline{g}) = \zeta_8 = e^{\pi i/4}$, $\psi(\overline{k}) = 1$ for all $\overline{k} \in H = G_p^8$. With F_k as in $(**)$, our

formula $(***)$ reads as

$$-(F_0^4+F_1^4+F_2^4+F_3^4)-2(F_0^2F_2^2+F_1^2F_3^2)$$
$$-4(F_0^2F_1F_3-F_1^2F_0F_2-F_2^2F_1F_3+F_3^2F_0F_2)=-32768\cdot p^4\cdot h^-.$$

5. Finally, let $d=5$, i.e., $p\equiv 11 \bmod 20$, and put $p>11$. Choose a number $g'\in\mathbb{Z}\backslash p\mathbb{Z}$ such that $g'^{(p-1)/5}\not\equiv 1 \bmod p$. Then $g=g'^2$ has property $(*)$. Again, the Legendre symbol $\psi=(\frac{\cdot}{p})$ is an odd character of G_p, with $H\subseteq \operatorname{Ker}\psi$ and $\psi(\overline{g})=1$. We obtain

$$\begin{aligned}&F_0^5+F_1^5+F_2^5+F_3^5+F_4^5\\&\quad-5\{F_0^3(F_1F_4+F_2F_3)+F_1^3(F_0F_2+F_3F_4)+F_2^3(F_0F_4+F_1F_3)\\&\qquad\qquad+F_3^3(F_0F_1+F_2F_4)+F_4^3(F_0F_3+F_1F_2)\}\\&\quad+5\{F_0(F_1^2F_4^2+F_2^2F_3^2)+F_1(F_0^2F_2^2+F_3^2F_4^2)\\&\qquad+F_2(F_0^2F_4^2+F_1^2F_3^2)+F_3(F_0^2F_1^2+F_2^2F_4^2)+F_4(F_0^2F_3^2+F_1^2F_2^2)\}\\&\qquad\qquad-5\cdot F_0F_1F_2F_3F_4=-1600000\cdot p^5\cdot h^-.\end{aligned}$$

Remarks. 1. Of course it is possible to give analogous relative class number formulas for $d\geq 6$, too. In the case $d=6$, however, the determinant $\det(\psi(\overline{g})^{j+k}F_{j+k})$ consists of 68 monomials in $F_0,\ldots,F_5$. Therefore, the formula is too complicated to be written in full.

2. Let $d=2^q\cdot d'$, d' odd. Then X contains a character ψ of order 2^{q+1}. Obviously, $\psi(\overline{-1})=\overline{-1}$ and $\psi(\overline{k})=1$ for all $\overline{k}\in H=G_p^{2d}$. Thus, ψ has the required properties, and we may say that there is always an appropriate character ψ of G_p of *2-power order.*

3. Tables

We have used the formulas of Examples $1,\ldots,5$ to compute the relative class numbers h_{2d}^- of imaginary subfields $K\subseteq\mathbb{Q}(\zeta_p)$ with $[K:\mathbb{Q}]=2d$, $d\in\{2,3,4,5\}$ and $2d+1<p<500000$. In the Supplement we display the result for $d=3,4,5$ and $p<10000$ (Tables 1, 2, 3). The respective table for $[K:\mathbb{Q}]=4$ can be found in [6].

Bibliography

1. L. Carlitz and F. R. Olson, *Maillet's determinant*, Proc. Amer. Math. Soc. **6** (1955), 265–269.
2. K. Girstmair, *An index formula for the relative class number of an abelian number field*, J. Number Theory **32** (1989), 100–110.
3. ——, *A recursion formula for the relative class number of the p^n-th cyclotomic field*, Abh. Math. Sem. Univ. Hamburg **61** (1991), 131–138.
4. H. Hasse, *Vorlesungen über Zahlentheorie*, Springer-Verlag, Berlin-Göttingen-Heidelberg, 1950.
5. ——, *Über die Klassenzahl abelscher Zahlkörper*, Akademie-Verlag, Berlin, 1952.
6. R. Hudson, *Class numbers of imaginary cyclic quartic fields and related quaternary systems*, Pacific J. Math. **115** (1984), 129–142.
7. R. Hudson and K. Williams, *A class number formula for certain quartic fields*, Carleton Math. Series 174 (1981).
8. J. Kühnová, *Maillet's determinant $D_{p^{n+1}}$*, Archivum Math. **15** (1979), 209–212.

9. B. Setzer, *The determination of all imaginary, quartic, abelian number fields with class number* 1, Math. Comp. **35** (1980), 1383–1386.

10. L. Skula, *Another proof of Iwasawa's class number formula*, Acta Arith. **39** (1981), 1–6.

11. K. Tateyama, *Maillet's determinant*, Sci. Papers College Gen. Ed. Tokyo **32** (1982), 97–100.

12. K. Wang, *On Maillet determinant*, J. Number Theory **18** (1984), 306–312.

INSTITUT FÜR MATHEMATIK, UNIVERSITÄT INNSBRUCK, TECHNIKERSTRASSE 25/7, A-6020 INNSBRUCK, AUSTRIA

E-mail address: kurt.girstmair@uibk.ac.at