manuscripta math. 33, 339 - 356 (1981)

manuscripta mathematica

AN ARTIN CHARACTER AND REPRESENTATIONS OF PRIMES BY BINARY QUADRATIC FORMS

Pierre KAPLAN and Kenneth S. WILLIAMS*

We show how the decomposition of primes in certain dihedral extensions L of the rationals enables us to obtain results concerning representations of powers of primes by binary quadratic forms and treat here in detail the case of $L = Q(\sqrt{\varepsilon_m}, \sqrt{-\varepsilon_m})$, where m is a square free positive integer such that the norm of the fundamental unit ε_m of $Q(\sqrt{m})$ is -1. Other cases will be treated in subsequent papers.

1. Introduction. Let N,n be squarefree rational integers, whose greatest common divisor is 1 or 2 and such that there exist rational integers a, b and c with

(1.1) $$c^2N = a^2 - nb^2 , \quad (a,b) = (b,c) = (c,a) = 1 .$$

We define

(1.2) $$\eta = a + b\sqrt{n} , \quad \eta' = a - b\sqrt{n}$$

so that

(1.3) $$(\sqrt{\eta} \pm \sqrt{\eta'})^2 = 2a \pm 2c\sqrt{N} .$$

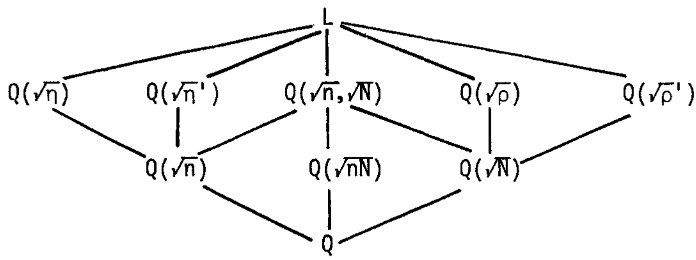
* Research supported by Natural Sciences and Engineering Research Council Canada Grant N° A-7233

0025-2611/81/0033/0339/$03.60

We set

$$(1.4) \qquad \rho = 2a + 2c\sqrt{N}\ ,\quad \rho' = 2a - 2c\sqrt{N}\ ,$$

and consider the subfield structure of the dihedral extension $L = Q(\sqrt{\eta}, \sqrt{\eta'}) = Q(\sqrt{\rho}, \sqrt{\rho'})$.



We define

$$(1.5) \qquad K = Q(\sqrt{n}, \sqrt{N})\ ,\quad k = Q(\sqrt{nN})\ .$$

The extension L/k is cyclic of degree 4. We remark that $K = k(\sqrt{n}) = k(\sqrt{N})$ and that $L = K(\sqrt{\eta}) = K(\sqrt{\rho})$. Noting that n and N (respectively η and ρ) have no common odd prime divisors in k (respectively K) , appealing to Hilbert [4 : Satz 4] , we obtain

LEMMA 1. *The conductor* f *of* L/k *is only divisible by ideals of* k *lying above* 2.

It is known ([3 : Satz 7]) that f is a rational integer. The Artin reciprocity map of the extension L/k defines a character χ of order 4 on a class group C_f of binary quadratic forms.

In §2 we show how knowing the value of χ on ambiguous classes of C_f enables us to determine the representation of certain powers of primes by ambiguous classes of C_f (Propositions 1 and 2).

In §3 we consider a squarefree positive integer m for which the norm of the fundamental unit ε_m of $Q(\sqrt{m})$ is -1 . Then

$$(1.6) \qquad T^2 - mU^2 = -1\ ,$$

where (T, U) denotes the least positive solution of (1.6), so that

$T + U\sqrt{m} = \varepsilon_m$ or ε_m^3. We can thus apply the preceeding with $N = -1$, $n = m$, $a = T$, $b = U$, $c = 1$ and $\eta = T + U\sqrt{m}$. In this case the conductor f of the extension L/k has been determined [1]. We have

$$(1.7) \qquad f = \begin{cases} 1, & \text{if } m \equiv 1 \pmod 8, \\ 2, & \text{if } m \equiv 5 \pmod 8, \\ 4, & \text{if } m \equiv 2 \pmod 8, \end{cases}$$

The main result of this paper gives the value of χ on the ambiguous classes of C_f in this case (see Theorem 1 in §3).

In §4 we give explicit examples of the results of §3.

2. Representation of powers of primes and Artin character. The ideal class group of conductor f of the ring of integers of k is isomorphic to the class group C_f of primitive binary quadratic forms

$$f = aX^2 + bXY + cY^2 = [a,b,c]$$

of discriminant $b^2 - 4ac = nNf^2$, if $nN \equiv 1 \pmod 4$, $4nNf^2$ if $nN \not\equiv 1 \pmod 4$, which are taken to be positive when $nN < 0$. We refer to [2], [6] for the theory of binary quadratic forms. Thus we can consider the Artin reciprocity map $\sigma : C_f \to G(L/k)$ as a character χ of order 4 on the group C_f. The character χ is defined by

$$\chi : C_f \to C_f/H \simeq G(L/k) \simeq \{1, i, -1, -i\},$$

where $H = \ker \sigma = \ker \chi$. The Artin reciprocity map of K/k induces a homomorphism $C_f \to G(K/k)$, whose kernel H_1 contains H, and as $[H_1 : H] = 2$ we have

$$\chi^{-1}(1, -1) = H_1 .$$

Clearly H_1 contains the principal genus C_f^2, and so can be defined as the kernel of a generic character. Any class B of C_f represents primes q, prime to $2nN$, and these primes satisfy $(\frac{nN}{q}) = +1$. The class B belongs to H_1 if, and only if, such q are completely decomposed in K/k, that is, if

(2.1) $$(\frac{n}{q}) = (\frac{N}{q}) = 1 .$$

Thus H_1 is the subgroup of C_f giving the value $+1$ to the generic character e_n on C_f defined by

(2.2) $$e_n(B) = (\frac{n}{a}) ,$$

where B contains the form $[a, b, c]$, $(a, 2n) = 1$.

We let r_{2^k} denote the 2^k-rank of the group C_f. The 2^{r_2} ambiguous classes are distributed amongst $2^{r_2-r_4}$ of the 2^{r_2} genera, 2^{r_4} in each (see for example [5 : p. 316]). As the group of ambiguous classes is a subgroup of H_1 we have $r_4 > 1$. Moreover $r_4 = 1$ if, and only if, the genera of the ambiguous classes are the genera for which $e_n = 1$.

A prime q such that $(\frac{nN}{q}) = +1$ is represented by two inverse classes Q and Q^{-1} or by one self-inverse (= ambiguous) class Q of forms of C_f. If the class Q is in H_1, that is, if $(\frac{n}{q}) = (\frac{N}{q}) = +1$, then $\sqrt{n}$ can be interpreted as an integer modulo q and the value of $(\frac{\eta}{q})$ is independent of the choice of $\sqrt{n}$ modulo q. Further Q is in H if, and only if, $(\frac{\eta}{q}) = +1$ so that

(2.3) $$(\frac{\eta}{q}) = \chi(Q) .$$

Suppose now that the class Q is in the genus of the ambiguous class A. Then Q is in H_1 and there exists a class B_1 such that $Q = AB_1^2$, so that

$$(2.4) \qquad (\tfrac{n}{q}) = \chi(A)\{\chi(B_1)\}^2 \quad .$$

We note that for any class B, $\{\chi(B)\}^2 = +1$ or -1 according as B is in H_1 or not, so that $\{\chi(B)\}^2 = e_n(B)$, and (2.4) becomes

$$(2.5) \qquad (\tfrac{n}{q}) = \chi(A)e_n(B_1) \quad .$$

Further if the ambiguous class A is in the principal genus, and B_1 is a squareroot of A, then we have

$$(2.6) \qquad \chi(A) = e_n(B_1) \quad .$$

The order of a class B in the group C_f is

$$(2.7) \qquad \text{ord }(B) = 2^\nu \ell \ , \quad \ell \text{ odd} \ .$$

Then the class B^ℓ of order 2^ν can be viewed as an element of the 2-class group of C_f. We note that B and B^ℓ are in the same genus. We begin by proving

LEMMA 2. *If $r_8 = 0$ and if a class B is in a genus of an ambiguous class A, then the class B^ℓ is an ambiguous class of the genus of B.*

PROOF. As the classes B and B^ℓ are in the same genus, there exists a class B_1 such that $B^\ell = AB_1^2$. As $r_8 = 0$, B_1 is of order 1, 2, or 4, so that B_1^2, and therefore B^ℓ, are ambiguous.

We first consider the case $r_8 = 0$.

PROPOSITION 1. *Let n and N be squarefree coprime rational integers satisfying* (1.1). *Let η, η' be defined as in* (1.2) *and let f denote the conductor of $Q(\sqrt{\eta}, \sqrt{\eta'})/Q(\sqrt{nN})$.*

Suppose further that the 8-rank r_8 of the group C_f if zero.

Let q be a prime represented by a class Q in a genus of ambiguous classes of C_f. Then the class Q^{ℓ}, where ℓ is defined in (2.7), *is an ambiguous class such that*

$$\chi(Q^{\ell}) = \left(\frac{\eta}{q}\right) .$$

PROOF. We apply (2.5) to the prime q and the ambiguous class Q^{ℓ} obtaining

$$\left(\frac{\eta}{q}\right) = \chi(Q^{\ell})e_n(Q^{\frac{-(\ell-1)}{2}}) = \chi(Q^{\ell}) ,$$

as $\quad e_n(Q^{\frac{-\ell-1}{2}}) = \{e_n(Q)\}^{\frac{-\ell-1}{2}} = \{+1\}^{\frac{-\ell-1}{2}} = 1 \quad .$

We remark that $Q^{\ell} = Q^{h'}$, where h' is the largest odd divisor of the order h of C_f.

Now we consider the case $r_4 = 1$. In this case there are two ambiguous classes in the principal genus, the principal class I and another one J ; and in each genus included in H_1 there are two ambiguous classes A and AJ. Using (2.6) one finds that

$$r_8 = 1 \iff \chi(J) = +1 .$$

The 2-class group of C_f is of the type $C(2^{\tau}) \times C(2)^{r_2-1}$, so that the order of C_f, denoted by h, is given by

$$h = 2^{\tau+r_2-1} h' ,$$

where h' is odd. We now set

$$s = h/2^{r_2+1} .$$

The integer s is odd if and only if $r_8 = 0$. If a class B is a fourth power its order divides s. If a class B is a square but not a fourth power its order divides $2s$ but not s, so that B^s is ambiguous and in the principal genus, and therefore $B^s = J$. For any class B the odd number ℓ defined in (2.7) is a divisor of s. If $r_8 = 0$ the ambiguous class B^ℓ is equal to B^s. This proves

LEMMA 3. *If $r_4 = 1$, and if B is in the principal genus, then $B^s = I$ or J according as B is a fourth power or not.*

We will also need the following lemma.

LEMMA 4. *If $r_4 = r_8 = 1$ and A, B are two classes in the same genus, the class A being ambiguous, then $B^s = I$ or J according as AB is a fourth power or not.*

PROOF. By Lemma 2, $(AB)^s = I$ or J according as AB is a fourth power or not. As s is even, $A^s = I$ and the result follows.

We now prove with the notation of Proposition 1

PROPOSITION 2. *Suppose $r_4 = 1$ and let J denote the non-unit ambiguous class in the principal genus of C_f. Then*

(a) $$r_8 = 1 \Leftrightarrow \chi(J) = 1 .$$

Let q be a prime represented by a class in the genus of the ambiguous classes A and AJ. Then

(b) *the class QA is a fourth power if, and only if,* $(\frac{n}{q}) = \chi(A)$,

(c) *if $r_8 = 0$ then $Q^s = A$ or AJ according as*
$$(\tfrac{n}{q}) = \chi(A) \text{ or } -\chi(A) ,$$

(d) *if $r_8 = 1$ then $Q^s = I$ or J according as $(\frac{n}{q}) = \chi(A)$ or $-\chi(A)$.*

PROOF. (a) (b). We apply (2.6) to J and (2.5) to q and A, noting that, as $r_4 = 1$, the genera of the ambiguous classes consist of all genera satisfying $e_n = 1$.

(c) As $r_8 = 0$, by (a) $\chi(J) = -1$ so that $\chi(AJ) = -\chi(A)$. But in this case, $Q^s = Q^\ell$ is ambiguous, by Lemma 1, and so equal to A or AJ. By Theorem 1, $(\frac{n}{q}) = \chi(Q^s)$, so that $Q^s = A$ or AJ according as $(\frac{n}{q}) = \chi(A)$ or $-\chi(A)$ respectively.

(d) As $r_8 = 1$, by Lemma 3, $Q^s = I$ or J according as QA is a fourth power or not. The result now follows from (b).

If Q is in the principal genus we can take $A = I$ and we have

COROLLARY. *Suppose* $r_4 = 1$. *If* Q *is in the principal genus, then* Q *is a fourth power, if and only if* $(\frac{n}{q}) = 1$; *and* q^s *is represented by* I *or* J *according as* $(\frac{n}{q}) = +1$ *or* -1.

3. *Determination of Artin chararacter*. From now on we denote by m a squarefree positive integer for which the norm of the fundamental unit ε_m of $Q(\sqrt{m})$ is -1 and we suppose that we are in the case $N = -1$, $n = m$, $a = T$, $b = U$, $c = 1$, where m, T, U satisfy (1.6). We remark that $m = p_1 \ldots p_r$, where $r > 1$ and the p_i are distinct primes with $p_1 = 2$ or $p_1 \equiv 1 \pmod 4$ and $p_2 \equiv \ldots \equiv p_r \equiv 1 \pmod 4$. Moreover all prime factors of U are congruent to 1 modulo 4 and

$$(3.1)\qquad \begin{cases} T \equiv 0 \pmod 4, & \text{if } m \equiv 1 \pmod 8, \\ T \equiv 1 \pmod 2, & \text{if } m \equiv 2 \pmod 8, \\ T \equiv 2 \pmod 4, & \text{if } m \equiv 5 \pmod 8. \end{cases}$$

Before stating Theorem 1, we recall the form of the ambiguous classes of C_f .

If $m \equiv 1 \pmod 8$, we have $f = 1$, and an ambiguous class A contains either a couple $[d, 0, e]$ and $[e, 0, d]$ of ambiguous forms, or a couple $[2d, 2d, \frac{1}{2}(d+e)]$ and $[2e, 2e, \frac{1}{2}(d+e)]$ of ambiguous forms, with $de = m$, $d > 0$, $e > 0$.

If $m \equiv 5 \pmod 8$, we have $f = 2$, and an ambiguous class A contains exactly one ambiguous form $[d, 0, 4e]$, where $de = m$, $d > 0$, $e > 0$.

If $m \equiv 2 \pmod 8$, we have $f = 4$, and an ambiguous class A contains exactly one ambiguous form, either $[d, 0, 32e]$ or $[4d, 4d, d+8e]$ where $2de = m$, $d > 0$, $e > 0$.

We prove

THEOREM 1. *If* m *is a squarefree integer such that* $N(\varepsilon_m) = -1$, *the value of the Artin character* χ *of* L/k *on the ambiguous class* A *is given as follows* :

If $m \equiv 1 \pmod 8$

$$\chi(A) = \begin{cases} \left(\frac{2}{d}\right), & \text{if } A \text{ contains the form } [d,0,e]. \\ \left(\frac{2}{d}\right)(-1)^{T/4}, & \text{if } A \text{ contains the form } [2d,2d,\frac{d+e}{2}] \end{cases}$$

If $m \equiv 5 \pmod 8$

$$\chi(A) = \left(\frac{2}{d}\right), \text{ if } A \text{ contains the form } [d, 0, 4e].$$

If $m \equiv 2 \pmod 8$

$$\chi(A) = \begin{cases} (\frac{2}{d}) & , \underline{\text{if}} \ A \ \underline{\text{contains the form}} \ [d, 0, 32e] , \\ -(\frac{2}{d}) & , \underline{\text{if}} \ A \ \underline{\text{contains the form}} \ [4d, 4d, d+8e] . \end{cases}$$

PROOF. If the ambiguous class A contains a form of the type $[d, 0, e']$, we say that the class A is odd ; otherwise we say that it is even.

Let A be an ambiguous class which is odd so that it contains the form $[d, 0, e']$. Clearly it suffices to show that $\chi(A_p) = (\frac{2}{p})$ for a class A_p containing a form $[p, 0, \frac{mf^2}{p}]$, where p is an odd prime divisor of m. The class A_p corresponds to the ideal class of conductor f in k of the ideal P of k such that $P^2 = p$. Therefore $\chi(A_p) = +1$ or -1 according as P is completely decomposed or not in the extension L/k. Now in K, $P = P_1P_2$, and from the relation $T^2+1 = mU^2$ we see that we can choose P_1 to divide $T-i$, and then P_1 is prime to $2(T+i)$. As $L = K(\sqrt{p})$ we have, denoting by $[-]_K$ the quadratic residue symbol in K :

$$(3.2) \quad \chi(A_p) = [\frac{p}{P_1}]_K = [\frac{2(T+i)}{P_1}]_K = [\frac{4i}{P_1}]_K = [\frac{i}{P_1}]_K = (-1)^{\frac{p-1}{4}} = (\frac{2}{p}) ,$$

as $N(P_1) = p$.

Next we treat the two cases when A is even, that is,

$m \equiv 1 \pmod 8$, A contains $[2d, 2d, \frac{d+e}{2}]$,

$m \equiv 2 \pmod 8$, A contains $[4d, 4d, d+8e]$.

Let $m \equiv 1 \pmod 8$ and suppose that the ambiguous class A is even, so that A contains the form $[2d, 2d, \frac{d+e}{2}]$, where $de = m$. Since A is the product of the classes of $[2, 2, \frac{1+m}{2}]$ and $[d, 0, e]$ in C_1, it suffices to prove

$$\chi((2,1+\sqrt{-m})) = (-1)^{T/4} ,$$

as the ideal class of $(2,1+\sqrt{-m})$ corresponds to the class of the form $[2,2,\frac{1+m}{2}]$.

We begin by showing that if $\chi((2,1+\sqrt{-m})) = +1$ then $T \equiv 0 \pmod 8$. In k we have $2 = (2,1+\sqrt{-m})^2$ and in $Q(i)$ we have $2 = (1+i)^2$ (as ideals). If $\chi((2,1+\sqrt{-m})) = 1$ the ideal $(2,1+\sqrt{-m})$ is completely decomposed in L/k so that the ideal $(1+i)$ is completely decomposed in $L/Q(i)$, and thus in the subextension $Q(\sqrt{\varepsilon_m}+\sqrt{\varepsilon_m'})/Q(i)$. Since $Q(\sqrt{\varepsilon_m}+\sqrt{\varepsilon_m'}) = Q(\sqrt{2(T+i)}) = Q(\sqrt{1-Ti})$, by a result of Hilbert [3: Satz 8], the congruence

$$1 - Ti \equiv Z^2 \pmod{(1+i)^5}$$

is solvable in $\mathbb{Z}[i]$. Thus, there are rational integers a, b, x, y such that

$$1 = Ti = (a+bi)^2 + 4(1+i)(x+yi),$$

that is, with $X = x-y$,

$$(3.3) \quad \begin{cases} 1 = a^2 - b^2 + 4X, \\ -T = 2ab + 4X + 8y. \end{cases}$$

Clearly a is odd and b is even. Thus, taking (3.3) modulo 8, we obtain, with $b = 2c$,

$$X \equiv c \pmod 2, \quad -T \equiv 4(c+X) \pmod 8,$$

so that

$$T \equiv 0 \pmod 8,$$

as required.

We next show that if $T \equiv 0 \pmod 8$ then $\chi((2,1+\sqrt{-m})) = +1$. Interpreting $\sqrt{m}$ as U modulo 8, we see that, if $T \equiv 0 \pmod 8$, then $T+U\sqrt{m} \equiv 1 \pmod 8$, so that, as 2 decomposes as $2_1^2 2_2^2$ in K, both congruences $T+U\sqrt{m} \equiv x_j^2 \pmod{2_j^5}$ $(j = 1,2)$ have solutions in the ring of integers of K as indeed they are solvable in $\mathbb{Z}$. This completes the case when $m \equiv 1 \pmod 8$.

Finally let $m \equiv 2 \pmod 8$ and suppose that the ambiguous class A is even. As above it suffices to prove that χ takes the value -1 on the class A_0 of the form $[4,4,1+4m]$.

Now inclusion induces a natural homomorphism of the ideal class group of conductor 4 of R onto the ideal class group of conductor 2 of R, whose kernel consists of the two ideal classes corresponding to I and A_0.

If $\chi(A_0)$ had the value 1, then χ would take the value 1 on the whole principal ideal class of conductor 2 of R, contradicting the fact that the conductor of the extension L/k is 4.

4. <u>Examples of applications of the results</u>. In this section we keep the hypotheses made at the beginning of § 3. Here the subgroup H_1 is the subgroup of C_f whose classes B satisfy $e_{-1}(B) = +1$.

We denote by q a prime represented by a class Q of determinant $-mf^2$, where f is given by (1.7), and q is such that the genus of Q contains ambiguous classes. Then (2.1) holds, that is, in the present case :

$$(4.1) \qquad \left(\frac{-1}{q}\right) = \left(\frac{m}{q}\right) = 1.$$

If, for C_f, $r_4 = 1$, then (4.1) ensures that the genus of Q contains ambiguous classes, and Proposition 2 (a) together with Theorem 1 gives the value of r_8. In some cases we are able to prove that $N(\varepsilon_m) = -1$.

Example 1. $m = p_1p_2 \dots p_r$, $r = 2$ *or an odd number, all* $p_i \equiv 1 \pmod 8$, *all* $(\frac{p_i}{p_j}) = -1$, $i \neq j$; $f = 1$. Here $r_4 = 1$ and $N(\varepsilon_m) = -1$, as the only ambiguous classes of discriminant $-4m$ and $+m$ in the principal genera are the principal classes and, respectively, the class J of $[2,2,\frac{m+1}{2}]$ and the class of $[-1,0,m]$.

One has $r_8 = 1$ if and only if $(-1)^{T/4} = 1$, that is, $T \equiv 0 \pmod 8$.

Here one has $\chi(A) = 1$ for all odd classes, and $\chi(A) = (-1)^{T/4}$ for all even classes so that :

(a) *If* $r_8 = 0$, *the class* Q^{ℓ} *is the odd or the even ambiguous class of the genus of* Q *according as* $(\frac{\varepsilon_m}{q}) = 1$ *or* -1.

(b) *If* $r_8 = 1$, $Q^s = I$ *or* J *according as* $(\frac{\varepsilon_m}{q}) = 1$ or -1.

Example 2. $m = p_1p_2$, *where* $p_1 \equiv p_2 \equiv 5 \pmod 8$ *and* $(\frac{p_1}{p_2}) = -1$; $f = 1$.

Here $N(\varepsilon_m) = -1$, $r_4 = 1$ and J is the class of $[2p_1, 2p_2, \frac{p_1p_2}{2}]$. Also $s = \frac{h}{8}$.

We find first, as $\chi(J) = -(-1)^{T/4}$, *that* $r_8 = 1$ *if, and only if,* $T \equiv 4 \pmod 8$.

(a) If $r_8 = 0$, $\chi(I) = 1$, $\chi(J) = -1$, and $\chi([p_1, 0, p_2]) = -1$, so that $\chi(\bar{I}) = 1$, where $\bar{I}$ is the class of $[2,2,(p_1p_2+1)/2]$, and :

<u>If</u> $(\frac{-1}{q}) = (\frac{q}{p_1}) = (\frac{q}{p_2}) = -1$, <u>then</u> $Q^\ell = \bar{I}$ <u>or</u> J <u>according</u> <u>as</u> $(\frac{\varepsilon_m}{q}) = 1$ <u>or</u> -1.

<u>If</u> $(\frac{-1}{q}) = 1$, $(\frac{q}{p_1}) = (\frac{q}{p_2}) = -1$, <u>then</u> $Q^\ell = \bar{I}$ <u>or</u> $\{[p_1,0,p_2]\}$ <u>according as</u> $(\frac{\varepsilon_m}{q}) = 1$ <u>or</u> -1.

(b) If $r_8 = 1$, $\chi(I) = \chi(J) = 1$, and $\chi([p_1,0,p_2]) = \chi(\bar{I}) = -1$, so that :

<u>If</u> $(\frac{-1}{q}) = (\frac{q}{p_1}) = (\frac{q}{p_2}) = 1$, <u>then</u> $Q^s = I$ <u>or</u> J <u>according as</u> $(\frac{\varepsilon_m}{q}) = 1$ <u>or</u> -1.

<u>If</u> $(\frac{-1}{q}) = 1$, $(\frac{q}{p_1}) = (\frac{q}{p_2}) = -1$, <u>then</u> $Q^s = J$ <u>or</u> I <u>accor-ding as</u> $(\frac{\varepsilon_m}{q}) = 1$ <u>or</u> -1.

We remark that this example is Case VI of Theorem 2 of [7], but with the case $r_8 = 1$ treated as well.

<u>Example 3</u>. <u>All</u> $p_i \equiv 1 \pmod 8$ <u>and</u> $r_8 = 0$ $(r_2 \geqslant r_4 > r_8 = 0)$; $f = 1$.

For all ambiguous classes one has $e_{-1} = 1$. Also for the odd ambiguous classes one has $\chi(A) = +1$, and for the even ambiguous classes $\bar{A} = A\bar{I}$ one has $\chi(\bar{A}) = (-1)^{T/4}$. This means that for the classes K of order 4 whose square is odd, one has $e_2(K) = 1$, and for the classes $\bar{K}$ of order 4 whose square is even, then $e_2(\bar{K}) = (-1)^{T/4}$. If $(-1)^{T/4}$ were 1, then all classes of order 1, 2 or 4 would give value 1 to e_{-1} ; but, as $r_8 = 0$, a class L has an odd power L^n of order 1, 2 or 4, and for any class L the character

$e_{-1}(L) = e_{-1}(L^n)$ would be 1. This contradicts the fact that there always exists a class giving to the generic characters any set of values compatible with the product formula, so that $(-1)^{T/4} = -1$, and $\chi(A) = +1$ for odd classes, $\chi(\bar{A}) = -1$ for even classes. Hence in this case we must have $T \equiv 4 \pmod 8$. Applying Proposition 1 one sees that _the class_ Q^{ℓ} _is odd or even according as_ $(\frac{\varepsilon_m}{q}) = +1$ _or_ -1.

Example 4. a) $m = p_1p_2$, $p_1 \equiv 1$, $p_2 \equiv 5 \pmod 8$; $(\frac{p_1}{p_2}) = -1$.

b) $m = p_1 \ldots p_r$, all $p_i \equiv 5 \pmod 8$, r odd, all $(\frac{p_i}{p_j}) = -1$, $i \neq j$.

c) $m = p_1p_2p_3$, all $p_i \equiv 5 \pmod 8$, $(\frac{p_1}{p_2}) = 1$, $(\frac{p_2}{p_3}) = (\frac{p_3}{p_1}) = -1$.

d) $m = p_1p_2p_3$, $p_1 \equiv 5$, $p_2 \equiv p_3 \equiv 1 \pmod 8$, 2 or 3 of the $(\frac{p_i}{p_j}) = -1$.

In all these cases $f = 2$ and one sees that $r_4 = 1$, $r_8 = 0$, as the only ambiguous class $\neq I$ of determinant $-4m$ in the principal genus is the class of $[4,0,m]$. One can then apply Proposition 1. For example in case a) we have :

If $(\frac{-1}{q}) = (\frac{q}{p_1}) = (\frac{q}{p_2}) = 1$, then $Q^{\ell} = I$ or $\bar{I}$ according as $(\frac{\varepsilon_m}{q}) = 1$ or -1.

If $(\frac{-1}{q}) = 1$, $(\frac{q}{p_1}) = (\frac{q}{p_2}) = -1$, then $Q^{\ell} = A_1$ or A_2 according as $(\frac{\varepsilon_m}{q}) = 1$ or -1, where A_j denotes the class of $[q_j, 0, 4\frac{m}{q_j}]$. (This is the result of [7], Theorem 2, IV).

Example 5. $m = p_1p_2$, $p_1 \equiv 1$, $p_2 \equiv 5 \pmod 8$, $(\frac{p_1}{p_2}) = 1$, $f = 2$.

Here $r_2 = 2$, $r_4 = 2$. We suppose $N(\varepsilon_m) = -1$ and $r_8 = 0$. A prime $q \equiv 1 \pmod 4$ represented by a genus of ambiguous forms of discriminant $-4m$ is represented by the principal genus ; it is thus represented by the principal genus of discriminant $-16m$, and by Proposition 2

$$Q^\ell = I \text{ or } A_1 \text{ if } (\frac{\varepsilon_m}{q}) = 1,\ Q^\ell = \bar{I} \text{ or } A_2 \text{ if } (\frac{\varepsilon_m}{q}) = -1.$$

(This is the result of [7], Theorem 2, III).

Example 6. $m = p_1p_2p_3$, $p_1 \equiv 5$, $p_2 \equiv p_3 \equiv 1 \pmod 8$, $(\frac{p_1}{p_2}) = (\frac{p_1}{p_3}) = 1$, $(\frac{p_1}{p_2}) = -1$. Here $f = 2$, $r_2 = 2$. We suppose that $N(\varepsilon_m) = -1$ and $r_8 = 0$.

If $(\frac{-1}{q}) = (\frac{q}{p_1}) = (\frac{q}{p_2}) = (\frac{q}{p_3}) = 1$, then $Q^\ell = I$ or $A_1\bar{I}$ if $(\frac{\varepsilon_m}{p}) = 1$, and $Q^\ell = \bar{I}$ or A_1 if $(\frac{\varepsilon_m}{q}) = -1$.

If $(\frac{-1}{q}) = (\frac{q}{p_1}) = 1$ and $(\frac{q}{p_2}) = (\frac{q}{p_3}) = 1$, then $Q^\ell = A_2$ or A_3 if $(\frac{\varepsilon_m}{q}) = 1$ and $Q^\ell = A_2\bar{I}$ or $A_3\bar{I}$ if $(\frac{\varepsilon_m}{q}) = -1$.

Example 7. $m = p_1p_2p_3$, $p_1 \equiv 5$, $p_2 \equiv p_3 \equiv 1 \pmod 8$, $(\frac{p_1}{p_2}) = (\frac{p_2}{p_3}) =+1$, $(\frac{p_1}{p_3}) = -1$; $f = 2$.

Here $r_2 = 3$, $r_4 = 2$. We suppose $N(\varepsilon_m) = -1$ and $r_8 = 0$.

If $(\frac{-1}{q}) = (\frac{q}{p_1}) = (\frac{q}{p_2}) = (\frac{q}{p_3})$, then $Q^\ell = I$ or A_2 is $(\frac{\varepsilon_m}{q}) = 1$, $Q^\ell = \bar{I}$ or $\bar{A}_2$ if $(\frac{\varepsilon_m}{q}) = -1$.

If $(\frac{-1}{q}) = (\frac{q}{p_2}) = 1$, $(\frac{q}{p_1}) = (\frac{q}{p_3}) = -1$, then $Q^\ell = A_3$ or

$A_1\bar{I}$ if $(\frac{\varepsilon_m}{q}) = 1$, $Q^\ell = A_1$ or $A_3\bar{I}$ if $(\frac{\varepsilon_m}{q}) = -1$.

Example 8. $m = 2p$, $p \equiv 1 \pmod 4$; $f = 4$.

The ambiguous classes of discriminant $-64m$ are $I, A, \bar{I}, \bar{A}$ containing respectively $[1, 0, 32p]$, $[32, 0, p]$, $[4, 4, 8p+1]$, $[4p, 4p, p+8]$.

If $p \equiv 5 \pmod 8$, then I and $\bar{A}$ are in the principal genus, so that $r_4 = 1$ and as $\chi(I) = \chi(\bar{I}) = 1$, $\chi(A) = \chi(\bar{A}) = -1$ one finds by Proposition 2 that $r_8 = 0$ and :

If $(\frac{-1}{q}) = (\frac{2}{q}) = (\frac{p}{q}) = 1$, then $Q^\ell = I$ or $\bar{A}$ according as $(\frac{\varepsilon_m}{q}) = 1$ or -1.

If $(\frac{-1}{q}) = 1$, $(\frac{2}{q}) = (\frac{p}{q}) = -1$, then $Q^\ell = \bar{I}$ or A according as $(\frac{\varepsilon_m}{q}) = 1$ or -1.

If $p \equiv 1 \pmod 8$, $I, A, \bar{I}$ and $\bar{A}$ are in the principal genus, so that $r_4 = 2$, and $\chi(I) = \chi(A) = 1$, $\chi(\bar{I}) = \chi(\bar{A}) = -1$ and using Proposition 1 :

If p is such that $N(\varepsilon_m) = -1$ and $r_8 = 0$, and q such that $(\frac{-1}{q}) = (\frac{2}{q}) = (\frac{p}{q}) = 1$ then $Q^\ell = I$ or A if $(\frac{\varepsilon_m}{q}) = 1$, and $Q^\ell = \bar{I}$ or $\bar{A}$ if $(\frac{\varepsilon_m}{q}) = -1$.

REFERENCES

[1] D.A. BUELL, P.A. LEONARD and K.S. WILLIAMS, Note on the quadratic character of a quadratic unit, submitted for publication

[2] C.F. GAUSS, Disquisitiones Arithmeticae, translated into English by Arthur A. Clarke, Yale University Press, 1966

[3] F. HALTER-KOCH, Arithmetische Theorie der Normalkörper von 2. Potenzgrad mit Dieder gruppe, J. Number Theory, 3 (1971) pp. 412-443

[4] D. HILBERT, Über die Theorie des relativquadratischen Zahlkörpers, Math. Ann. 51 (1899), 1-127

[5] P. KAPLAN, Sur le 2-groupe des classes d'idéaux des corps quadratiques, J. Reine Angew. Math 283/284 (1976), 313-363

[6] P. KAPLAN, Cours d'Arithmétique, UER de Mathématiques, Université de Nancy I, (1973)

[7] K.S. WILLIAMS, On the evaluation of $(\varepsilon_{q_1q_2}/p)$, Rocky Moutain J. Math. (to appear)

10, Allée Jacques Offenbach
54420 - Saulxures les Nancy
FRANCE

Department of Mathematics and Statistics
Carleton University
Ottawa, Ontario, CANADA KIS 5B6

(Received August 5, 1980)