ACTA ARITHMETICA
XCIX.1 (2001)

On power residue characters of units and the representation of numbers by quadratic forms

by

Giorgos Siligardos (Heraklion)

Construction of class fields using radicals involving units is very common (see for example [4], [1], [2]) and since the splitting character of primes into class fields is related to the representation of their powers by quadratic forms, we may obtain representation conditions defined by the power residue characters of units. In this paper we try to find sufficient or necessary conditions depending upon the Legendre symbols of fundamental units for the representation of prime powers for two cases of discriminants specified at the beginning of the introduction.

1. Notation. Throughout the present paper i will be the imaginary number such that $i^2 = -1$, ζ_n will stand for $e^{2\pi i/n}$, $n \in \mathbb{N}$, and ζ_3 will often be denoted as ω. For a real number field $\mathbb{Q}(\sqrt{m})$, $m \in \mathbb{N}$, ε_m will denote its fundamental unit. For a ring R, $R^\times$ will be the multiplicative group of its units. For a number field F we shall denote by R_F its ring of integers and $N_F(\cdot)$ will denote the absolute norm function. If F'/F is a Galois extension of number fields, $G(F'/F)$ will be the associated Galois group and if furthermore F'/F is abelian and $\mathfrak{p}$ is a prime ideal of F, we shall denote by $\left[\frac{F'|F}{\mathfrak{p}}\right]$ the Artin symbol for $\mathfrak{p}$. For a Galois number field extension F'/F and a prime $\mathfrak{p}$ of F, $\mathrm{spl}_{\mathfrak{p}}(F'/F)$ will be the splitting field of $\mathfrak{p}$ in F'/F. Moreover, we shall denote by $f_{\mathfrak{p}}(F'/F)$ the common inertia degree of all primes of F' over $\mathfrak{p}$ in F'/F and for simplicity, when $F = \mathbb{Q}$, we set $f_p(F') = f_{p\mathbb{Z}}(F'/\mathbb{Q})$, $\mathrm{spl}_p(F') = \mathrm{spl}_{p\mathbb{Z}}(F'/\mathbb{Q})$. If F is a number field, $\mathfrak{p}$ a prime ideal of R_F, $\alpha \in R_F$ and $n \in \mathbb{N}$ such that $\mathfrak{p} \nmid \alpha n$, $\zeta_n \in F$ then $\left(\frac{\alpha}{\mathfrak{p}}\right)_n$ will stand for the nth power Legendre symbol. That is, $\left(\frac{\alpha}{\mathfrak{p}}\right)_n$ is the unique nth root of unity such that $\alpha^{(N_F(\mathfrak{p})-1)/n} \equiv \left(\frac{\alpha}{\mathfrak{p}}\right)_n \pmod{\mathfrak{p}}$. It is known (see [3], Exercise 13) that

2000 *Mathematics Subject Classification*: Primary 11R99.

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_n = 1 \quad \text{if and only if} \quad \alpha \equiv x^n \pmod{\mathfrak{p}} \text{ is soluble in } R_F.$$

For the case $n = 2$ we shall omit the subscript n.

Let D be a square-free negative integer with $D \equiv 0, 1 \pmod 4$. We write $D = f^2 D_0$, where D_0 is the fundamental discriminant and $f \in \mathbb{N}$. We denote by $H(D)$ the class group of all primitive positive definite quadratic forms of discriminant D and by $\hbar(D)$ (or simply $\hbar$) its order. Let $k = \mathbb{Q}(\sqrt{D_0})$. Then $k(D)$ will denote the ring class field of k modulo f. By class field theory, the Artin symbol gives isomorphisms

$$H(D) \xleftarrow{\simeq} I_k(f)/P_{k,\mathbb{Z}}(f) \xleftarrow{\simeq} G(k(D)/k)$$

where $I_k(f)$ is the group of all ideals of k which are prime to f and $P_{k,\mathbb{Z}}(f)$ is its subgroup of principal ideals aR_k with $a \in (\mathbb{Z} + fR_k)$, so we may use the notation $\left[\frac{k(D)|k}{C}\right]$ for the image of $C \in H(D)$ in $G(k(D)/k)$.

Now, let e be a positive integer. We shall denote by $H_e(D)$ the product of the q-Sylow subgroups of $H(D)$ for all prime divisors q of e and by $\hbar_e(D)$ (or simply $\hbar_e$) its order. Let $H(D) \cong H_e(D) \times H'_e(D)$. Then $\hbar'_e(D)$ (or simply $\hbar'_e$) will denote the order of $H'_e(D)$ and so $(\hbar'_e, e) = 1$. We set $k_e(D)$ to be the fixed field of $H'_e(D)$ and so $k_e(D)$ is an extension of degree $\hbar_e$ over k containing all intermediate fields of $k(D)/k$ whose order over k divides $\hbar_e$. It is obvious that $H_e(D)$, $k_e(D)$ etc. depend only on the set of prime divisors of e and not on their exponents in the rational prime decomposition of e. If H is a subgroup of $H_e(D)$, we shall denote by $L_H^{(e)}$ the fixed field of H in $k_e(D)$ and if $H = \langle C_1, \ldots, C_r \rangle$, then we set $L^{(e)}_{C_1,\ldots,C_r} = L_H^{(e)}$. Finally for an element C of $H(D)$ and an integer m, the notation $C \to m$ will indicate that m is represented by C.

2. Introduction. In this paper we shall study two cases of discriminants:

Case I: $D = -256qr$, q, r primes with $q \equiv 5 \pmod 8$, $r \equiv 3 \pmod 8$, $\hbar_2(D_0) \mid 4$.

Case II: $D = -4m$, $m > 1$ square-free integer with $m \equiv 1 \pmod{12}$, $\hbar_3(D_0) \mid 9$.

We have

$$D_0 = \begin{cases} -qr & \text{in Case I,} \\ -4m & \text{in Case II.} \end{cases}$$

In [5] it is proved that for Case I, $k_2(D)$ contains exactly four subfields of degree 4 over k. In this case $H_2(D)$ is of type $\langle A, B, C \rangle$ with $B^2 = C^2 = I$ and $A^8 = I$ or $A^4 = I$, where I is the principal class of $H(D)$. These four fields are $L^{(2)}_{A^4,B,C}$, $L^{(2)}_{A^2B,C}$, $L^{(2)}_{A^2C,B}$, $L^{(2)}_{A^2B,BC}$. One of these fields (namely

$L^{(2)}_{A^4,B,C}$) is responsible for the determination of specific prime powers represented by ambiguous classes in each genus. Here we shall prove that these fields, composed pairwise, give two fields generated with the aid of the 4th root of ε_{qr} over $\mathbb{Q}(i,\sqrt{qr})$ and we shall see how the 4th and the 2nd degree power residue symbols of ε_{qr} are connected with the representation of prime powers by classes of $H_2(-256qr)$ of order dividing 4.

In Case II we shall find sufficient conditions using the 3rd power residue symbol of ε_{3q} for the representation of some prime powers of exponent $\hbar'_e$ by a class C of $H_e(D)$, with $C^e = I$ for $e \in \{3,6\}$. This paper is somehow a continuation of [5] and is influenced by [4].

3. Preliminaries

PROPOSITION 1. *Let D be a negative square-free integer with $D \equiv 0,1 \pmod 4$. Let $e \in \{2,3,4,6\}$, p an odd prime integer with $\left(\frac{D}{p}\right) = 1$. If $C \in H(D)$ with $C^e = 1$ and $\mathrm{spl}_p(k_e(D)) = L_C^{(e)}$ then $C \to p^{\hbar'_e}$. If $e = 4$ then moreover the relations $\mathrm{spl}_p(k_2(D)) = L_C^{(2)}$ and $C \to p^{\hbar'_2}$ are equivalent.*

Proof. If $p = \mathfrak{p}_0\mathfrak{p}_1$ is the prime decomposition of p in k then since $\mathrm{spl}_p(k_e(D)) = L_C^{(e)}$ we have

$$\left\langle \left[\frac{k_e(D) \mid k}{\mathfrak{p}_0} \right] \right\rangle = \left\langle \left[\frac{k_e(D) \mid k}{C} \right] \right\rangle.$$

But $(\hbar'_e, e) = 1$ and so we have

$$\left[\frac{k_e(D) \mid k}{C} \right] = \left[\frac{k_e(D) \mid k}{\mathfrak{p}_0^{\pm\hbar'_e}} \right],$$

implying

$$\left[\frac{k(D) \mid k}{C} \right] = \left[\frac{k(D) \mid k}{\mathfrak{p}_0^{\pm\hbar'_e}} \right],$$

which means that $C \to p^{\hbar'_e}$. For the assertion about $e = 4$ the reader is referred to Lemma 1 of [4]. ∎

COMMENTS. The essence of Proposition 1 is Lemma 1 of [4] where the stronger part concerning $e = 4$ is proved. Proposition 1 is a partial trivial extension of Halter-Koch's result to classes of order not only dividing 4. The proof of Lemma 1 of [4] is valid only in one direction for $e = 3,6$; the reader may see in [4] that the failure of the equivalence is due the fact that the only integer n having the property: "$\forall x, y \in \mathbb{Z}$, if $(x+y, n) = 1$ then $(x-y, n) = 1$" is $n = 2$. Also, Proposition 1 deals only with $e = 2,3,4,6$ because these e's are the only such that $e \geq 2$ and $\left(\frac{\mathbb{Z}}{e\mathbb{Z}}\right)^\times$ has at most two generators.

By [5] and by our assumptions for Case II we have the following lemma:

LEMMA 1. *For $s \in \mathbb{Z}$, $s \geq 2$, the following hold*:

In Case I, $H_2(-2^{2s}qr) = (2^{s-2+c_{qr}}, 2, 2)$, *where* $H_2(-qr) = (2^{c_{qr}+1})$.

In Case II, $H_3(D) \in \{(3), (3,3), (3^2)\}$.

LEMMA 2. *In Case* I, *every cyclic extension L of k of order 4 unramified outside 2 and dihedral over $\mathbb{Q}$ is contained in $k_2(-256qr)$.*

In Case II, *every abelian unramified extension L of k of order 3 (or 2) is contained in $k_3(-4m)$ (or $k_2(-4m)$).*

Proof. For Case I see [5]. For Case II we note that L is contained in the Hilbert class field of k which is $k(-4m)$. ∎

4. Extensions of k generated with the aid of radicals of units

PROPOSITION 2. *Let q, r be prime numbers with $q \equiv 5 \pmod 8$, $r \equiv 3 \pmod 8$. Let also $\mathsf{w} \in \{1, 2\}$, and*

$$t = \begin{cases} 1 & \text{if } \left(\frac{q}{r}\right) = 1, \\ 2 & \text{if } \left(\frac{q}{r}\right) = -1. \end{cases}$$

Set $k = \mathbb{Q}(\sqrt{-qr})$, $k_0 = \mathbb{Q}(\sqrt{qr})$, $K = kk_0$, $\alpha = \sqrt[4]{\mathsf{w}^2\varepsilon_{qr}}$, $M = K(\alpha)$. The following hold: *There exists some $\mathsf{v} \in K$ such that $\mathsf{w}^2\varepsilon_{qr} = tq\mathsf{v}^2$. Moreover M/K is a cyclic Kummerian extension of order 4, $M/\mathbb{Q}$ is dihedral with $G(M/\mathbb{Q}) = \langle\sigma, \tau\rangle \rtimes \langle\varrho\rangle$ and $\sigma(\sqrt{qr}) = \sqrt{qr}$, $\tau(\sqrt{qr}) = -\sqrt{qr}$, $\varrho(\sqrt{qr}) = \sqrt{qr}$, $\sigma(i) = i$, $\tau(i) = -i$, $\varrho(i) = -i$, $\sigma(\alpha) = i\alpha$, $\tau(\alpha) = \mathsf{w}/\alpha$, $\varrho(\alpha) = \alpha$. Also M/K is unramified outside 2 and the fixed fields of $\langle\tau\rangle$, $\langle\sigma\tau\rangle$ are cyclic extensions of k of order 4 unramified outside 2 and dihedral over $\mathbb{Q}$. Finally $K(\sqrt{\varepsilon_{qr}}) = k(i, \sqrt{tq})$.*

Proof. The equation $x^2 - qry^2 = tq$ is solvable in rational integers (see Lemma 2 of [5]), so setting $b = x + y\sqrt{qr}$, $\overline{b} = x - y\sqrt{qr}$ we have $b\overline{b} = tq$. Since $2, q$ are ramified in k_0 we may write $tq = \mathfrak{a}^2$, where $\mathfrak{a}$ is an ideal of k_0 and it is easy to see (b has norm tq) that $(b) = \mathfrak{a}$ and so there is a unit ε of k_0 such that $b^2 = tq\varepsilon$. If $\varepsilon = \varepsilon_{qr}^{\lambda}$, then λ is necessarily odd, so setting

$$\mathsf{v} = \frac{\mathsf{w}(b\varepsilon_{qr}^{(-\lambda+1)/2})}{tq}$$

we have $\alpha^4 = \mathsf{w}^2\varepsilon_{qr} = tq\mathsf{v}^2$. Let $G(K/\mathbb{Q}) = \langle\tau, \varrho\rangle$ with $\tau(\sqrt{qr}) = -\sqrt{qr}$, $\varrho(\sqrt{qr}) = \sqrt{qr}$, $\tau(i) = -i$, $\varrho(i) = -i$. We see that $\tau(\mathsf{v}) = \mathsf{w}^2/(tq\mathsf{v})$, $\varrho(\mathsf{v}) = \mathsf{v}$ and $\tau(\alpha^4) = \left(\frac{\mathsf{w}}{\alpha}\right)^4$, $\varrho(\alpha^4) = \alpha^4$ and so we may extend τ, ϱ in M so that $\tau(\alpha) = \left(\frac{\mathsf{w}}{\alpha}\right)$, $\varrho(\alpha) = \alpha$. Setting $G(M/K) = \langle\sigma\rangle$ with $\sigma(\alpha) = i\alpha$, the assertion follows. ∎

Similarly to the above we may prove the following:

PROPOSITION 3. *Let m be a square-free positive integer such that $m \equiv 1 \pmod 4$. Set $k = \mathbb{Q}(\sqrt{-m})$, $k_0 = \mathbb{Q}(\sqrt{3m})$, $K = kk_0 = k(\omega)$, $\alpha = \sqrt[3]{\varepsilon_{3m}}$, $M = K(\alpha)$. Then M/K is a Kummerian extension of order 3 and $M/\mathbb{Q}$ is dihedral of order 12. Moreover, $G(M/\mathbb{Q}) = \langle \sigma, \tau \rangle \rtimes \langle \varrho \rangle$ with $\sigma(\sqrt{-m}) = \sqrt{-m}$, $\tau(\sqrt{-m}) = \sqrt{-m}$, $\varrho(\sqrt{-m}) = -\sqrt{-m}$, $\sigma(\sqrt{-3}) = \sqrt{-3}$, $\tau(\sqrt{-3}) = -\sqrt{-3}$, $\varrho(\sqrt{-3}) = -\sqrt{-3}$, $\sigma(\alpha) = \omega\alpha$, $\tau(\alpha) = 1/\alpha$, $\varrho(\alpha) = \alpha$. M/k is an abelian extension of order 6 unramified outside 3 and the fixed field of $\langle \tau \rangle$ is an intermediate extension of M/k of order 3 over k and dihedral over $\mathbb{Q}$.*

5. Main results

5.1. *Case I.* Set $M = K(\sqrt[4]{\varepsilon_{qr}})$, $M' = K(\sqrt[4]{4\varepsilon_{qr}})$, $k_0 = \mathbb{Q}(\sqrt{qr})$, $K = kk_0$. By Proposition 2, M has two subfields L_1, L_2 which are cyclic extensions of k of order 4 unramified outside 2. Also, M' has two subfields L_1', L_2' which are cyclic extensions of k of order 4 unramified outside 2. By Lemma 2, L_1, L_2, L_1', L_2' are contained in $k(-256qr)$ and so since $H_2(-256qr)$ has exactly four subgroups giving quotient groups cyclic of order 4 (namely $L^{(2)}_{A^4,B,C}$, $L^{(2)}_{A^2B,C}$, $L^{(2)}_{A^2C,B}$, $L^{(2)}_{A^2B,BC}$) (see [5], Proposition 4):

$$\begin{aligned}\{L_1, L_2, L_1', L_2'\} &= \{L^{(2)}_{A^4,B,C}, L^{(2)}_{A^2B,C}, L^{(2)}_{A^2C,B}, L^{(2)}_{A^2B,BC}\}\\ &= \{k(\sqrt{\omega\mu}) \mid \omega = \pm 1, \pm 2\},\end{aligned}$$

where x, y are arbitrary integral solutions of $qx^2 - ry^2 = t$, $\mu = t - y\sqrt{-tr}$ and

$$t = \begin{cases} 1 & \text{if } \left(\frac{q}{r}\right) = 1,\\ 2 & \text{if } \left(\frac{q}{r}\right) = -1.\end{cases}$$

Now, $\sqrt{2} \notin M, M'$ and $i \in M, M'$, giving $\{k(i, \sqrt{\mu}),\ k(i, \sqrt{2\mu})\} = \{M, M'\}$. We will determine whether $M = k(i, \sqrt{\mu})$ or $M = k(i, \sqrt{2\mu})$. For this, we need the following lemma:

LEMMA 3. *If q, r are prime numbers with $q \equiv 5 \pmod 8$, $r \equiv 3 \pmod 8$ and $\varepsilon_{qr} = u + v\sqrt{qr}$ is the fundamental unit of $\mathbb{Q}(\sqrt{qr})$, then $u \equiv -1 \pmod q$.*

Proof. By $u^2 - qrv^2 = 1$ we have $u \equiv \pm 1 \pmod q$. If $u = 1 + \kappa q$ for a $\kappa \in \mathbb{Z}$, then squaring we get $\kappa(q\kappa + 2) = rv^2$. Suppose first that κ is odd. Then $(\kappa, q\kappa + 2) = 1$. The case $r \mid \kappa$ gives $qrv_1^2 + 2 = v_2^2$ where $v = v_1v_2$ and leads to a contradiction since $\left(\frac{2}{q}\right) = -1$. The case $r \nmid \kappa$ implies $v_1^2q + 2 = rv_2^2$ with $v = v_1v_2$, which also leads to a contradiction upon taking Legendre quadratic symbols modulo q and modulo r. Now, let κ be even. Write $\kappa = 2\kappa'$ and so $\kappa'(q\kappa' + 1) = rv'^2$ where $v = 2v'$. The case $r \mid \kappa'$ gives $v_1^2 - qrv_2^2 = 1$ where $v = 2v_1v_2$ and $u + 1 = 2v_1^2$. So $v_1 < u$ and $v_2 < v$, which is a contradiction since $u + v\sqrt{qr}$ is the fundamental unit. The case $r \nmid \kappa'$ gives $v_1^2q + 1 = rv_2^2$ with $v = v_1v_2$ and thus taking quadratic Legendre symbols

modulo q and modulo r we have $\left(\frac{q}{r}\right)=1$, and $\left(\frac{q}{r}\right)=-1$, which also leads to a contradiction. ∎

A consequence of the above lemma is that $\varepsilon_{qr}\equiv -1 \pmod q$ and thus $f_q(M)=2$ and $f_q(M')=1$. We may check easily (see [5], Proposition 4) that

$$f_q(k(\sqrt{\mu},i))=\left.\begin{cases}1 & \text{if } \left(\frac{q}{r}\right)=-1\\ 2 & \text{if } \left(\frac{q}{r}\right)=1\end{cases}\right\}=\frac{2}{t}$$

and thus

$$\begin{aligned}(M,M')&=\begin{cases}(k(i,\sqrt{\mu}),k(i,\sqrt{2\mu})) & \text{if } \left(\frac{q}{r}\right)=1,\\ (k(i,\sqrt{2\mu}),k(i,\sqrt{\mu})) & \text{if } \left(\frac{q}{r}\right)=-1,\end{cases}\\ &=(k(i,\sqrt{t\mu}),k(i,\sqrt{2t\mu})).\end{aligned}$$

Now, it is straightforward to see that, by Proposition 6 of [5], $M'=L^{(2)}_{A^4,B,C}(i)$. Moreover, the symbol u_p defined in Theorem 1 of [5] for primes p with $\left(\frac{-256qr}{p}\right)=\left(\frac{tq}{p}\right)=1$ as

$$u_p=\begin{cases}(-1)^{(p-1)/2} & \text{if } p\,|\,x,\\ \left(\frac{-\mu}{p}\right) & \text{if } p\nmid x \text{ and } \left(\frac{q}{r}\right)=-1,\\ \left(\frac{-2\mu}{p}\right) & \text{if } p\nmid x \text{ and } \left(\frac{q}{r}\right)=1,\end{cases}$$

has the property:

$$u_p=1 \quad \text{if and only if} \quad f_p(L^{(2)}_{A^4,B,C})=1.$$

We may now prove the following lemma:

LEMMA 4. *Let p be an odd prime with $\left(\frac{D}{p}\right)=1$ and let $\mathfrak{p}$ be a prime of k_0 over p.*

1. *If $p\equiv 1 \pmod 4$ then*

$$\left(\frac{tq}{p}\right)=\left(\frac{\varepsilon_{qr}}{\mathfrak{p}}\right), \quad \text{and if} \quad \left(\frac{\varepsilon_{qr}}{\mathfrak{p}}\right)=1 \quad \text{then} \quad u_p=\left(\frac{\varepsilon_{qr}}{\mathfrak{p}}\right)_4\left(\frac{2}{p}\right).$$

2. *If $p\equiv 3 \pmod 4$ then*

$$\left(\frac{tq}{p}\right)=\left(\frac{\varepsilon_{qr}}{\mathfrak{p}}\right)_4.$$

Proof (see Figure 0 below). First of all we note that $f_p(k)=1$. Now, when $p\equiv 1 \pmod 4$ we have $f_p(K)=1$, giving

$$f_p(K(\sqrt{\varepsilon_{qr}}))=2 \;\Leftrightarrow\; f_p(k(\sqrt{tq}))=2, \quad \text{so} \quad \left(\frac{tq}{p}\right)=\left(\frac{\varepsilon_{qr}}{\mathfrak{p}}\right).$$

Moreover, when $\left(\frac{\varepsilon_{qr}}{\mathfrak{p}}\right)=1$ we have $\left(\frac{4\varepsilon_{qr}}{\mathfrak{p}}\right)_4=\pm 1$ and

$$\left(\frac{4\varepsilon_{qr}}{\mathfrak{p}}\right)_4 = 1 \;\Leftrightarrow\; f_p(M') = 1 \;\Leftrightarrow\; f_p(L^{(2)}_{A^4,B,C}) = 1 \;\Leftrightarrow\; u_p = 1.$$

If $p \equiv 3 \pmod 4$ then $f_p(K) = 2$ and since $K(\sqrt{\varepsilon_{qr}})/K$ is of type $(2,2)$ we have $f_p(K(\sqrt{\varepsilon_{qr}})) = 1$. So, if $f_p(k(\sqrt{tq})) = 2$ then $f_p(L^{(2)}_{A^4,B,C}) = 4$, giving $f_p(M') = 4$, which means $\left(\frac{4\varepsilon_{qr}}{\mathfrak{p}}\right)_4 = -1$, and if $f_p(k(\sqrt{tq})) = 1$ we have $f_p(M') = 2$, giving $\left(\frac{4\varepsilon_{qr}}{\mathfrak{p}}\right)_4 = 1$. The desired relations are an immediate consequence of the relation

$$\left(\frac{4}{\mathfrak{p}}\right)_4 = \left(\frac{2}{\mathfrak{p}}\right) = \begin{cases} \left(\frac{2}{p}\right) & \text{if } p \equiv 1 \pmod 4, \\ 1 & \text{if } p \equiv 3 \pmod 4. \end{cases} \blacksquare$$

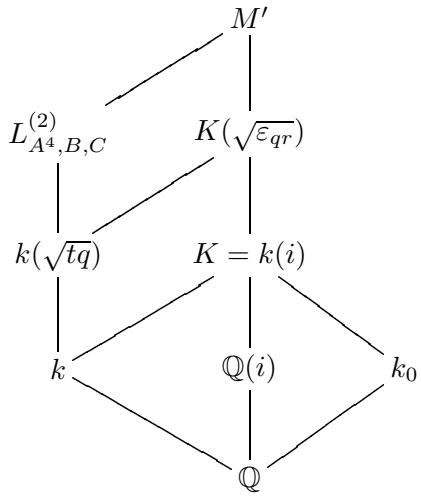

Fig. 0

In what follows we restrict our attention to the case $\left(\frac{q}{r}\right) = -1$ where we may get the following theorem connecting quadratic and quartic power residue symbols of ε_{qr} and representation of prime powers by classes of $H(-256qr)$ of order dividing 4.

THEOREM 1. *In Case* I, *let* $\left(\frac{q}{r}\right) = -1$. *Let also* p *be an odd prime with* $\left(\frac{-256qr}{p}\right) = 1$ *and* $\mathfrak{p}$ *a prime of* R_{k_0} *over* p. *The following assertions hold*:

(1) $p^{\hbar'_2}$ *is always represented by a class* C *of* $H(-256qr)$ *with* $C^4 = I$.

(2) $p^{\hbar'_2}$ *is represented by an ambiguous class of* $H(-256qr)$ *if and only if* $\left(\frac{tq}{p}\right) = 1$.

(3) *If* $p \equiv 1 \pmod 4$, *then* $p^{\hbar'_2}$ *is represented by an ambiguous class of* $H(-256qr)$ *if and only if* $\left(\frac{\varepsilon_{qr}}{\mathfrak{p}}\right) = 1$ *and moreover*, $p^{\hbar'_2}$ *is represented by one of* I, C *if and only if* $\left(\frac{\varepsilon_{qr}}{\mathfrak{p}}\right)_4 = \left(\frac{2}{p}\right)$.

(4) *If* $p \equiv 3 \pmod 4$, *then* $p^{\hbar_2'}$ *is represented by an ambiguous class of* $H(-256qr)$ *if and only if* $\left(\frac{\varepsilon_{qr}}{\mathfrak{p}}\right)_4 = 1$.

Proof. Since $\left(\frac{q}{r}\right) = -1$ we have $H_2(-256qr) = \langle A, B, C\rangle$ with $A^4 = B^2 = C^2 = 1$. Now $H_2(D_s)/H_2(D)^2$ has elements $\{I, A^2\}, \{B, A^2B\}$, $\{C, A^2C\}, \{BC, A^2BC\}$, $\{A, A^3\}$, $\{AB, A^3B\}$, $\{AC, A^3C\}$, $\{ABC, A^3BC\}$. Since the genus field modulo D is $k(\sqrt{q}, \zeta_8)$, the Artin map induces the following isomorphism (see [5], Proposition 1):

$$H_2(D)/H_2(D)^2 \xrightarrow{\simeq} (\mathbb{Z}/8\mathbb{Z})^\times \times \{\pm 1\}$$

with

$$C \bmod (H_2(D_s)^2) \to \left(\left[\frac{\mathbb{Q}(\zeta_8) \mid \mathbb{Q}}{m}\right], \left[\frac{\mathbb{Q}(\sqrt{q}) \mid \mathbb{Q}}{m}\right]\right) \quad \text{for } C \to m.$$

By Proposition 3 of [5], for an odd prime p with $\left(\frac{-256qr}{p}\right) = 1$ we obtain the following criteria:

(A) *If* $p^{\hbar_2'}$ *is represented by an ambiguous class then*

$$\left(\frac{q}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 7 \pmod 8, \\ -1 & \text{if } p \equiv 3, 5 \pmod 8. \end{cases}$$

The other cases of $\left(\frac{q}{p}\right)$ must be distributed in the other genera of $H_2(-256qr)$ and so we have the following result (see also Proposition 1):

(B) *If* $X \to p^{\hbar_2'}$ *with* $X \in \{A, AB, AC, ABC\}$ *then*

$$\left(\frac{q}{p}\right) = \begin{cases} -1 & \text{if } p \equiv 1, 7 \pmod 8, \\ 1 & \text{if } p \equiv 3, 5 \pmod 8. \end{cases}$$

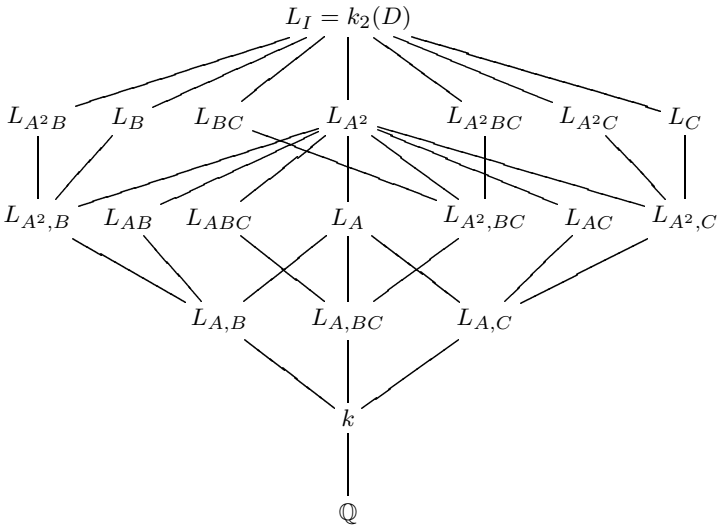

Fig. 1. Field tower for the Case I with $(\frac{q}{r}) = -1$

L_0 was defined as $k(\sqrt{tq})$ in [5] giving $L_0 = k(\sqrt{2q})$ for $\left(\frac{q}{r}\right) = -1$ and so by Figure 1 of [5] the inverse of (A) holds. By Figure 1 of the present paper and simple decomposition arguments, the inverse of (B) also holds and so we have proved (1). (We note that for every $X \in \{A, AB, AC, ABC\}$ we have $L_X = L_{A^2X}$, which means: $X \to p^{\hbar'_2}$ if and only if $A^2X \to p^{\hbar'_2}$.) Now, $f_p(L_0) = 1$ if and only if $\left(\frac{tq}{p}\right) = 1$ if and only if $p^{\hbar'_2}$ is represented by an ambiguous class (see Figure 1 of [5]) and thus (2) comes immediately. Also, (2) and Lemma 4 give the first assertion of (3). Finally, by Theorem 1 of [5] and Lemma 4 we have (4) and the second assertion of (3). ∎

Although things for $\left(\frac{q}{r}\right) = 1$ are not so nice as in the case $\left(\frac{q}{r}\right) = -1$ we may still get the following theorem whose proof is similar to the above and uses the results of Theorem 1 of [5], Figure 3 of [5] and Lemma 4:

THEOREM 2. *In Case* I, *let* $\left(\frac{q}{r}\right) = 1$. *Let also* p *be an odd prime with* $\left(\frac{D}{p}\right) = 1$ *and* $\mathfrak{p}$ *a prime of* R_{k_0} *over* p. *The following assertions hold*:

(1) $p^{\hbar'_2}$ *is represented by a class* C *of* $H(-256qr)$ *with* $C^4 = I$ *if and only if* $\left(\frac{tq}{p}\right) = 1$.

(2) *If* $p \equiv 1 \pmod 4$, *then* $p^{\hbar'_2}$ *is represented by a class* C *of* $H(-256qr)$ *with* $C^4 = I$ *if and only if* $\left(\frac{\varepsilon_{qr}}{\mathfrak{p}}\right) = 1$, *and moreover*, $p^{\hbar'_2}$ *is represented by an ambiguous class of* $H(D)$ *if and only if* $\left(\frac{\varepsilon_{qr}}{\mathfrak{p}}\right)_4 = \left(\frac{2}{p}\right)$.

(3) *If* $p \equiv 3 \pmod 4$, *then* $p^{\hbar'_2}$ *is represented by a class* C *of* $H(-256qr)$ *with* $C^4 = I$ *if and only if* $\left(\frac{\varepsilon_{qr}}{\mathfrak{p}}\right)_4 = 1$.

5.2. *Case II.* For Case II, we set $k = \mathbb{Q}(\sqrt{-m})$, $k_0 = \mathbb{Q}(\sqrt{3m})$, $K = kk_0$, $M = K(\sqrt[3]{\varepsilon_{3m}})$ and we apply Proposition 3. Let L be the fixed field of $\langle\tau\rangle$. Since 3 decomposes as $3 = (1-\omega)^2$ in $\mathbb{Q}(\sqrt{-3})$ and $(1-\omega)$ is a prime of $\mathbb{Q}(\sqrt{-3})$ which is inert in K, it follows that $(3) = (1-\omega)^2$ is the prime decomposition of 3 in K. By the decomposition law in Kummerian extensions, 3 is ramified in M if and only if

$$\varepsilon_{3m} \equiv x^3 \pmod{(1-\omega)^3}$$

is soluble in K. Thus we get the following theorem:

THEOREM 3. *In Case* II, *if* $\varepsilon_{3m} \equiv x^3 \pmod{(1-\omega)^3}$ *is not soluble in* K *and* p *is an odd prime such that* $\left(\frac{D}{p}\right) = 1$ *then*:

(1) *If* $H_3(D)$ *is of type* (3) *or* (3, 3) *then there is some* $C \in H(D)$ *such that* $C^3 = 1$ *with* $C \to p^{\hbar'_3}$.

(2) *If* $H_3(D)$ *is of type* (3^2) *then if "*$p \equiv 2 \pmod 3$*" or "*$p \equiv 1 \pmod 3$, $\left(\frac{\varepsilon_{3m}}{p}\right)_3 = 1$*" then there is some* $C \in H(D)$ *such that* $C^3 = 1$ *with* $C \to p^{\hbar'_3}$.

(3) *If the assumptions of* (1) *or* (2) *hold, and there is some* $C \in H(D)$ *such that* $C^2 = 1$ *with* $C \to p^{\hbar'_2}$, *then there is* $E \in H(D)$ *such that* $E^6 = 1$ *with* $E \to p^{\hbar'_6}$.

Proof. (1) is obvious by the assumptions about class structure, decomposition laws and Proposition 1. For (2), if $p \equiv 2 \pmod 3$ or $p \equiv 1 \pmod 3$, $\left(\frac{\varepsilon_{3m}}{\mathfrak{p}}\right)_3 = 1$ then by the decomposition laws in the cyclic extension M/k we get $f_p(L/k) = 1$ and so there is some $C_1 \in H(D)$ with $C_1^3 = 1$ such that $L_{C_1}^{(3)} = \mathrm{spl}_p(k_3(D))$. If moreover there exists some $C_2 \in H(D)$ such that $C_2^2 = 1$ with $L_{C_2}^{(2)} = \mathrm{spl}_p(k_2(D))$ then we may set $E = C_1C_2$, giving $E^6 = 1$ and

$$L_E^{(6)} = L_{C_1}^{(3)} L_{C_2}^{(2)} = \mathrm{spl}_p(k_2(D))\mathrm{spl}_p(k_3(D)) = \mathrm{spl}_p(k_6(D)),$$

which (by Proposition 1) gives $E \to p^{\hbar_6'}$. ∎

6. Calculation of power residue symbols. In this section we give an elegant way of computing the power Legendre symbols appearing in this paper in terms of a recurrent sequence. The idea is taken from [4] to which the reader is referred for similar calculations.

PROPOSITION 4. *Let $m \in \mathbb{N}$, $m \equiv 3 \pmod 4$, be square-free and $n \in \mathbb{N}$. Let also p be an odd prime with $p \nmid n$. Set $F = \mathbb{Q}(\sqrt{m}, \zeta_n)$ and let $\mathfrak{p}$ be a prime ideal of F over p. If $\varepsilon = u + v\sqrt{m}$ is a unit of $\mathbb{Q}(\sqrt{m})$ then $u^2 - mv^2 = 1$. Define the sequence $(\mathbf{A}_j)_{j\in\mathbb{N}}$ as: $\mathbf{A}_0 = 2$, $\mathbf{A}_1 = 2u$, $\mathbf{A}_{j+2} = 2u\mathbf{A}_{j+1} - \mathbf{A}_j$. Then $\mathbf{A}_j = \varepsilon^j + \varepsilon^{-j}$ for all $j \in \mathbb{N}$ and*

$$\left(\frac{\varepsilon}{\mathfrak{p}}\right)_n = 1 \quad \textit{if and only if} \quad \mathbf{A}_{(N_F(\mathfrak{p})-1)/n} \equiv 2 \pmod p.$$

Proof. Since $m \equiv 3 \pmod 4$, the equation $x^2 - my^2 = -1$ has no integral solutions, so $u^2 - mv^2 = 1$. Also, since $\mathfrak{p} \nmid n$, we have $N_F(\mathfrak{p}) \equiv 1 \pmod n$ (see [3], Exercise 5.13). The relation $\mathbf{A}_j = \varepsilon^j + \varepsilon^{-j}$ may easily be proved using induction, and since

$$\begin{aligned}\mathbf{A}_j \equiv 2 \pmod{\mathfrak{p}} &\Leftrightarrow \varepsilon^j + \varepsilon^{-j} - 2 \equiv 0 \pmod{\mathfrak{p}} \\ &\Leftrightarrow (\varepsilon^j - 1)^2 \equiv 0 \pmod{\mathfrak{p}} \Leftrightarrow \varepsilon^j \equiv 1 \pmod{\mathfrak{p}},\end{aligned}$$

we have

$$\begin{aligned}\left(\frac{\varepsilon}{\mathfrak{p}}\right)_n = 1 &\Leftrightarrow \varepsilon^{(N_F(\mathfrak{p})-1)/n} \equiv 1 \pmod{\mathfrak{p}} \Leftrightarrow \mathbf{A}_{(N_F(\mathfrak{p})-1)/n} \equiv 2 \pmod{\mathfrak{p}} \\ &\Leftrightarrow \mathbf{A}_{(N_F(\mathfrak{p})-1)/n} \equiv 2 \pmod p. \ ∎\end{aligned}$$

Acknowledgements. This work has been carried out under the supervision of Professor J. Antoniadis. I would like to thank him for his guidance. Many thanks also to my friend David M$^{\mathrm{c}}$Clurkin for dictionary help.

References

[1] H. Cohn, *Introduction to the Construction of Class Fields*, Cambridge Univ. Press, 1985.

[2] H. Cohn and G. Cooke, *Parametric form of an eight class field*, Acta Arith. 30 (1976), 367–377.

[3] A. D. Cox, *Prime Numbers of the Form* $x^2 + ny^2$, Wiley, New York, 1989.

[4] F. Halter-Koch, *Representation of primes by binary quadratic forms of discriminant* $-256q$ *and* $-128q$, Glasgow Math. J. 35 (1993), 261–268.

[5] G. Siligardos, *The embedding problem and representation of prime powers by ambiguous classes of quadratic forms*, J. Number Theory 85 (2000), 305–319.

Department of Mathematics
University of Crete
Heraklion, Greece
E-mail: siligard@math.uoc.gr

Received on 5.5.2000
and in revised form on 6.8.2000 (3820)