ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 16, Number 1, Winter 1986

ON THE QUARTIC CHARACTER OF CERTAIN QUADRATIC UNITS AND THE REPRESENTATION OF PRIMES BY BINARY QUADRATIC FORMS

FRANZ HALTER-KOCH

1. For a squarefree rational integer $m > 1$ let ε_m be the fundamental unit of $\mathbf{Q}(\sqrt{m})$ normalized by $\varepsilon_m > 1$. For a rational prime $p \equiv 1 \bmod 4$ let $(\cdot/p)$ be the quadratic and $(\cdot/p)_4$ the quartic residue symbol modulo p. It is the aim of this paper to prove the following conjecture of P. A. Leonard and K. S. Williams ([**8**, Conjecture 3.6]):

THEOREM. *Let q, q' be primes, $q \equiv 3 \bmod 8$, $q' \equiv 7 \bmod 8$, $(q'/q) = 1$, and let s be the odd part of the class number of $\mathbf{Q}(\sqrt{qq'}, \sqrt{-2})$. Let p be a prime such that $(-1/p) = (2/p) = (q/p) = (q'/p) = 1$; then*

$$p^s = x^2 + 8qq'y^2 = c^2 + 8d^2$$

with $x, y, c, d \in \mathbf{Z}$ and

$$\left(\frac{\varepsilon_{qq'}}{p}\right)_4 = \left(\frac{\varepsilon_{2q'}}{p}\right)_4 \cdot (-1)^{y+d}.$$

REMARK 1. When proving the Theorem it will be shown that for the primes p in question $(\varepsilon_{qq'}/p) = (\varepsilon_{2q'}/p) = 1$ and that the quartic symbols are well defined.

REMARK 2. Perhaps the Theorem itself does not deserve an extra publication but the proof is an interesting journey through various branches of algebraic number theory and is intimately connected with the so-called explicit decomposition laws in algebraic number fields which are not yet fully understood.

2. The fields involved. I keep all notations of the Theorem and begin with the unit theory of the biquadratic field

$$K = \mathbf{Q}(\sqrt{qq'}, \sqrt{2q'}),$$

using methods and results of [7].

On account of $(q', qq'/p) = 1$ for all primes p, there is an integral $\delta_{qq'} \in \mathbf{Q}(\sqrt{qq'})$ with

Received by the editor on June 20, 1984

$$N_{\mathbf{Q}(\sqrt{qq'})/\mathbf{Q}}(\delta_{qq'}) = q', \qquad \varepsilon_{qq'} = \frac{\delta_{qq'}^2}{q'};$$

similarly, there are integral elements $\delta_{2q} \in \mathbf{Q}(\sqrt{2q})$ and $\delta_{2q'} \in \mathbf{Q}(\sqrt{2q'})$ such that

$$N_{\mathbf{Q}(\sqrt{2q})/\mathbf{Q}}(\delta_{2q}) = q, \qquad \varepsilon_{2q} = \frac{\delta_{2q}^2}{q},$$

$$N_{\mathbf{Q}(\sqrt{2q'})/\mathbf{Q}}(\delta_{2q'}) = 2, \qquad \varepsilon_{2q'} = \frac{\delta_{2q'}^2}{2}.$$

From [7], Satz 1, it follows that

$$\sqrt{\varepsilon_{qq'}\varepsilon_{2q}},\ \sqrt{\varepsilon_{qq'}\varepsilon_{2q'}},\ \sqrt{\varepsilon_{2q}\varepsilon_{2q'}}$$

is a system of fundamental units of K. For primes p with $(q/p) = (q'/p) = (2/p) = 1$ it follows from the above formulae that

$$\left(\frac{\varepsilon_{qq'}}{p}\right) = \left(\frac{\varepsilon_{2q}}{p}\right) = \left(\frac{\varepsilon_{2q'}}{p}\right) = 1,$$

and if in addition $(-1/p) = 1$, i.e., $p \equiv 1 \bmod 8$, then the quartic symbols

$$\left(\frac{\varepsilon_{qq'}}{p}\right)_4, \quad \left(\frac{\varepsilon_{2q}}{p}\right)_4, \quad \left(\frac{\varepsilon_{2q'}}{p}\right)_4$$

are well defined.
In the following we consider the unit

$$\varepsilon = \sqrt{\varepsilon_{qq'} \cdot \varepsilon_{2q'}} = \frac{\delta_{qq'} \cdot \delta_{2q'}}{\sqrt{2q'}} \in K.$$

Then the second assertion of the Theorem is equivalent with

$$\left(\frac{\varepsilon}{p}\right) = (-1)^{y+d},$$

i. e., it remains to show:

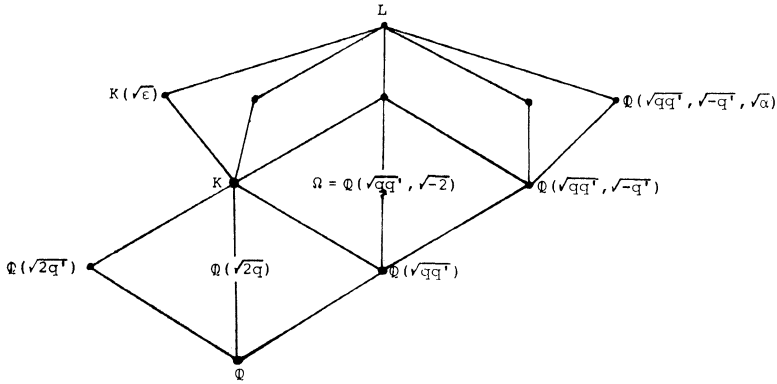
(1) *p splits completely in $K(\sqrt{\varepsilon})$, if and only if $y + d \equiv 0 \bmod 2$.*

Instead of the field $K(\sqrt{\varepsilon})$ I shall consider its normal closure, and for this reason I first consider the extension $K(\sqrt{\varepsilon})/\mathbf{Q}(\sqrt{qq'})$. As

$$N_{K/\mathbf{Q}(\sqrt{qq'})}(\varepsilon) = \frac{\delta_{qq'} \cdot \delta_{2q'}}{\sqrt{2q'}} \cdot \frac{\delta_{qq'} \cdot 2}{-\delta_{2q'}\sqrt{2q'}} = -\varepsilon_{qq'},$$

the extension $K(\sqrt{\varepsilon})/\mathbf{Q}(\sqrt{qq'})$ is not normal and its normal closure L is a dihedral extension of $\mathbf{Q}(\sqrt{qq'})$ with $[L: \mathbf{Q}(\sqrt{qq'})] = 8$. The intermediate fields of $L/\mathbf{Q}(\sqrt{qq'})$, which are quadratic over $\mathbf{Q}(\sqrt{qq'})$, are $K = \mathbf{Q}(\sqrt{qq'}, \sqrt{2q'})$, $\mathbf{Q}(\sqrt{qq'}, \sqrt{-\varepsilon_{qq'}}) = \mathbf{Q}(\sqrt{qq'}, \sqrt{-q'})$, and $\Omega = \mathbf{Q}(\sqrt{qq'},$

$\sqrt{-2}$). L/Ω is cyclic and $L/\mathbf{Q}(\sqrt{qq'})$ is also the normal closure of a quartic extension $\mathbf{Q}(\sqrt{qq'}, \sqrt{-q'}, \sqrt{\alpha})/\mathbf{Q}(\sqrt{qq'})$ for some $\alpha \in \mathbf{Q}(\sqrt{qq'}, \sqrt{-q'})$ (see [2, §1]).



The conjugates of ε (over $\mathbf{Q}$) are the three numbers

$$\frac{\delta_{qq'} \cdot 2}{-\delta_{2q'}\sqrt{2q'}} = \varepsilon \cdot (-2) \cdot \delta_{2q'}^{-2},$$

$$\frac{-2q'}{\delta_{qq'}\delta_{2q'}\sqrt{2q'}} = \varepsilon \cdot (-2q') \cdot (\delta_{qq'}\delta_{2q'})^{-2},$$

and

$$\frac{q'\delta_{2q'}}{\delta_{qq'}\sqrt{2q'}} = \varepsilon\, q' \cdot \delta_{qq'}^{-2}.$$

Therefore the normal closure of $K(\sqrt{\varepsilon})$ (over $\mathbf{Q}$) is the field

$$\bar{L} = K(\sqrt{\varepsilon}, \sqrt{-2}, \sqrt{q'}) = L(\sqrt{-1}),$$

and $\bar{L}/\Omega$ is an abelian extension of type (4, 2). $\bar{L}$ is also the normal closure of L over $\mathbf{Q}$, thus of the form

$$\bar{L} = L \cdot L',$$

where L' is a field conjugate to L.

The primes p as in the Theorem split completely in $\mathbf{Q}(\sqrt{-1}, \sqrt{-2}, \sqrt{q}, \sqrt{q'}) = \Omega(\sqrt{-q'}, \sqrt{-1})$, and they split completely in $K(\sqrt{\varepsilon})$ if and only if they do so in $\bar{L}$. Therefore it remains to show:

(2) *If a prime p splits completely in $\Omega(\sqrt{-q'}, \sqrt{-1})$, then $p^s = x^2 + 8qq'y^2 = c^2 + 8d^2$ with $x, y, c, d \in \mathbf{Z}$, and $y + d \equiv 0 \bmod 2$ if and only if p splits completely in $\bar{L}$.*

3. Arithmetic characterization of $\bar{L}/\Omega$. In this section I shall prove:

(3) *$\bar{L}$ is the maximal 2-extension which lies in the ray class field modulo 2 of Ω.*

$\mathbf{Q}(\sqrt{qq'}, \sqrt{-q'})/\mathbf{Q}(\sqrt{qq'})$ is obviously unramified outside infinity, and thus $\Omega(\sqrt{-q'})/\Omega$ is also unramified (later on I will show that $\Omega(\sqrt{-q'})$ is the Hilbert 2-classfield of Ω). As $L = \Omega(\sqrt{-q'}, \sqrt{\varepsilon})$, L/Ω is unramified outside 2. Let $\mathfrak{m}$ be the prime divisor of 2 in Ω ($2 \cong \mathfrak{m}^2$ and $\mathfrak{m}$ has degree 2); then the conductor f of L/Ω is a power of $\mathfrak{m}$, and as it is an ideal of $\mathbf{Q}(\sqrt{qq'})$ ([**2**, Satz 7]) it is a power of 2, say

$$f = 2^s, \quad s \geqq 0.$$

As L and L' are conjugate over $\mathbf{Q}$, the conductor of L'/Ω is also 2^s and thus the extension $\bar{L}/\Omega$ has conductor 2^s too.

To calculate f, I use the field $\mathbf{Q}(\sqrt{qq'}, \sqrt{-q'}, \sqrt{\alpha})$ and [**2**, Satz 24] (see also [**3**, (3.4)]), which implies

$$f^2 = N_{\mathbf{Q}(\sqrt{qq'}, \sqrt{-q'})/\mathbf{Q}(\sqrt{qq'})}(\mathfrak{b}) \cdot \frac{\mathfrak{b}_1}{\mathfrak{b}_0},$$

where $\mathfrak{b}, \mathfrak{b}_1, \mathfrak{b}_0$ are the relative discriminants of

$$\mathbf{Q}(\sqrt{qq'}, \sqrt{-q'}, \sqrt{\alpha})/\mathbf{Q}(\sqrt{qq'}, \sqrt{-q'}), \ \mathbf{Q}(\sqrt{qq'}, \sqrt{-q'})/\mathbf{Q}(\sqrt{qq'}),$$
$$\Omega/\mathbf{Q}(\sqrt{qq'}).$$

2 splits in $\mathbf{Q}(\sqrt{qq'}, \sqrt{-q'})$ into two prime factors $\mathfrak{d}_1, \mathfrak{d}_2$ of degree 2 and I suppose that exactly $\mathfrak{d}_1^{s_1}\mathfrak{d}_2^{s_2}$ divides $\mathfrak{b}$. Then, by [**3**, Lemma 2],

$$s_1 \leqq 3, \quad s_2 \leqq 3,$$

and exacty $2^{s_1+s_2}$ divides $N_{*/*}(\mathfrak{b})$. As $\mathbf{Q}(\sqrt{qq'}, \sqrt{-q'})/\mathbf{Q}(\sqrt{qq'})$ is unramified, 2 does not divide $\mathfrak{b}_1$ and, again by [**3**, Lemma 2], 2^3 exactly divides $\mathfrak{b}_0$. Putting everthing together I obtain

$$s = \frac{1}{2}(s_1 + s_2 - 3) \leqq \frac{3}{2},$$

so

$$s = 1 \text{ or } s = 0.$$

And if $\bar{\Omega}$ denotes the maximal 2-extension lying in the ray class field modulo 2 of Ω, then, by the above,

$$\bar{L} \subset \bar{\Omega}.$$

Then for the proof of (3) it suffices to show

$$[\bar{\Omega}: \Omega] \leqq 8,$$

i.e., the ray class number modulo 2 of Ω is not divisible by 16. Let h_2 be this ray class number; then h_2 is a divisor of $h_\Omega \cdot \phi_\Omega(2)$, where ϕ_Ω is the Euler phi function of Ω, and thus $\phi_\Omega(2) = 3 \cdot 2^2$.

It follows from [7] that the class number h_Ω of Ω is given by

$$h_\Omega = \frac{1}{2} \cdot h_{\mathbf{Q}(\sqrt{qq'})} \cdot h_{\mathbf{Q}(\sqrt{-2qq'})}$$

(as $h_{\mathbf{Q}(\sqrt{-2})} = 1$ and the unit index Q equals 1 in this case). Now, $h_{\mathbf{Q}(\sqrt{qq'})}$ is odd [4, ch. 29], and $4 \, h|_{\mathbf{Q}(\sqrt{-2qq'})}$ exactly [6, §11]; thus

$$h_\Omega = 2s$$

with $s \equiv 1 \bmod 2$, and

$$h_\Omega \cdot \phi_\Omega(2) = 2^3 \cdot 3s,$$

which was to be proved.

4. Weak decomposition laws and end of proof. The ideal class of order 2 in Ω contains an ideal which is ramified over $\mathbf{Q}(\sqrt{-2})$ [5] § 13], that is, a prime divisor of q or q'. We have q' inert in $\mathbf{Q}(\sqrt{-2})$, and the prime divisor of q' in Ω is already a prime of $\mathbf{Q}(\sqrt{qq'})$ and thus a principal prime ($h_{\mathbf{Q}(\sqrt{qq'})}$ is odd). Now, q splits in $\mathbf{Q}(\sqrt{-2})$ in the form $q = (u + v\sqrt{-2})(u - v\sqrt{-2}) = u^2 + 2v^2$ with $u, v \in \mathbf{Z}$, $u \equiv v \equiv 1 \bmod 2$, and

$$(u \pm v\sqrt{-2}) = \mathfrak{U}_\pm^2,$$

where $\mathfrak{U}_\pm$ are prime ideals of Ω which lie in the ideal class of order 2.

I have to investigate ray classes modulo 2 in Ω, and thus I will first determine generators for the prime residue classes modulo 2. Let $\mathfrak{m} = (\sqrt{-2})$ be the prime divisor of 2 in Ω and ω a primitive root modulo $\mathfrak{m}$; I may assume that ω is an integer of $\mathbf{Q}(\sqrt{qq'})$ which implies $\omega^3 \equiv 1 \bmod 2$. The association $1 + \alpha\sqrt{-2} \mapsto \alpha$ defines an isomorphism of $(1 + \mathfrak{m})/(1 + \mathfrak{m}^2)$ and the residue class field modulo $\mathfrak{m}$ (which is $\mathbf{F}_4$), so that the prime residue class group modulo 2 is of type (3, 2, 2) with generators

$$\omega, \; 1 + \sqrt{-2} \quad \text{and} \quad 1 + \omega\sqrt{-2}.$$

As $u \pm v\sqrt{-2} \equiv 1 + \sqrt{-2} \bmod 2$, I obtain the following description of the ray classes modulo 2 in Ω:

For every fractional ideal $\mathfrak{A}$ of Ω which is prime to 2 there is a representation

$$\mathfrak{A}^s = \mathfrak{A}_+^A \cdot (1 + \omega\sqrt{-2})^B \cdot (\omega^Q\alpha),$$

(4) *with uniquely determined exponents $A \in \{0, 1, 2, 3\}$, $B \in \{0, 1\}$, an (not necessarily uniquely determined) exponent $Q \in \{0, 1, 2\}$ and an $\alpha \in \Omega$ (integral with respect to $\mathfrak{m}$) with*

$$\alpha \equiv 1 \bmod 2.$$

If the fundamental unit η of $\mathbf{Q}(\sqrt{qq'})$ has half-integral coordinates, I may take $\omega = \eta$ and assume $Q = 0$.

Let S be the group of fractional ideals prime to 2 of Ω, and let

$$\kappa : S \to \mathrm{Gal}(\bar{L}/\Omega)$$

be the Artin map. As in (4), I write for an ideal $\mathfrak{A} \in S$

$$\mathfrak{A}^s = \mathfrak{A}_+^A \cdot (1 + \omega\sqrt{-2})^B \cdot (\omega^Q\alpha),$$

and then $\kappa(\mathfrak{A}) = id_{\bar{L}}$ if and only if $A = B = 0$.

As $\Omega(\sqrt{-q'}, \sqrt{-1})$ is the maximal elementary abelian extension of Ω inside $\bar{L}$, $\mathrm{Gal}(\bar{L}/\Omega(\sqrt{-q'}, \sqrt{-1})) = \{\sigma^2 | \sigma \in \mathrm{Gal}(\bar{L}/\Omega)\}$, and thus, for $\mathfrak{A} \in S$ as above, $\kappa(\mathfrak{A}) \in \mathrm{Gal}\,(\bar{L}/\Omega(\sqrt{-q'}, \sqrt{-1}))$ if and only if $A \in \{0, 2\}$ and $B = 0$.

As $\Omega(\sqrt{-q'})/\Omega$ is unramified and $h_\Omega \equiv 2 \bmod 4$, $\Omega(\sqrt{-q'})$ is the Hilbert 2-class field and thus for $\mathfrak{A} \in S$, as above, $\kappa(\mathfrak{A}) \in \mathrm{Gal}(\bar{L}/\Omega(\sqrt{-q'}))$ if and only if $A \in \{0, 2\}$, i.e., $\mathfrak{A}^s$ is a principal ideal.

For the proof of the Theorem I have to show (2). So let p be a rational prime which splits completely in $\Omega(\sqrt{-q'}, \sqrt{-1})$; then p also splits completely in Ω and in $\Omega(\sqrt{-q'})$. Let $\mathfrak{p}$ be a prime divisor of p in Ω; then $\mathfrak{p}^s = (\Pi)$ with $\Pi \in \Omega$, $N_{\Omega/\mathbf{Q}}(\Pi) = p^s$, and $\kappa(\mathfrak{p}) \in \mathrm{Gal}(\bar{L}/\Omega(\sqrt{-q'}, \sqrt{-1}))$, i. e.

$$(\Pi) = (u + v\sqrt{-2})^C \cdot (\omega^Q\alpha)$$

with $C \in \{0, 1\}$, $Q \in \mathbf{Z}$ and $\alpha \equiv 1 \bmod 2$. Furthermore, $\mathfrak{p}$ splits completely in $\bar{L}$ if and only if $\kappa(\mathfrak{p}) = id_{\bar{L}}$, i.e., if and only if

$$(\Pi) = (\omega^Q\alpha)$$

with $\alpha \equiv 1 \bmod 2$. The units of Ω are already in $\mathbf{Q}(\sqrt{qq'})$ (see [7]), and so they are congruent to some power of ω modulo 2. Thus it remains to show:

Let $\Pi \in \Omega$ be integral and

$$\Pi \equiv \omega^Q \cdot (1 + \sqrt{-2})^C \bmod 2$$

with $C \in \{0, 1\}$ and $Q \in \mathbf{Z}$; then there is a representation

(5)
$$N_{\Omega/\mathbf{Q}}(\Pi) = x^2 + 8qq'y^2 = c^2 + 8d^2$$

with $x, y, c, d \in \mathbf{Z}$ and

$$y + d \equiv C \bmod 2.$$

To see (5), set

$$\omega^{-Q}\Pi = (1 + \sqrt{-2})^C + 2\beta$$

with $\beta \in \Omega$, β integral with respect to 2; from [9] it follows that

$$\beta = \frac{1}{2}(b_0 + b_1\sqrt{qq'} + b_2\sqrt{-2} + b_3\sqrt{-2qq'}),$$

with $b_i \in \mathbf{Q}$, b_i integral for 2 and $b_0 \equiv b_1 \bmod 2$, $b_2 \equiv b_3 \bmod 2$. Taking norms I obtain

$$N_{\Omega/\mathbf{Q}(\sqrt{-2qq'})}(\Pi) = x + 2y\sqrt{-2qq'},$$

$$N_{\Omega/\mathbf{Q}(\sqrt{-2})}(\Pi) = c + 2d\sqrt{-2},$$

with $x, y, c, d \in \mathbf{Z}$ and

$$y + d \equiv C \bmod 2.$$

Taking further norms to $\mathbf{Q}$ gives the assertion.

References

1. F. Halter-Koch, *Binäre quadratische Formen und rationale Zerlegungsgesetze I*, to appear in J. of Number Theory.

2. F. Halter-Koch, *Arithmetische Theorie der Normalkörper von 2-Potenzgrad mit Diedergruppe*, J. Number Theory **3** (1971), 412–443.

3. F. Halter-Koch, P. Kaplan and K. S. Williams, *An Artin character and representations of primes by binary quadratic forms II*, Manuscripta Math. **37** (1982), 357–381.

4. H. Hasse, *Number Theory*. Springer 1980.

5. H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, T. Ia. Physica-Verlag, Würzburg 1965.

6. P. Kaplan, *Sur le 2-groupe des classes d'ideaux des corps quadratique*, J. f. reine und Angew. Math. **283/284** (1976), 313—363.

7. Kubota, *Über den bizyklischen biquadratischen Zahlkörper*, Nagoya Math. J. **10** (1956), 65–85.

8. P. A. Leonard and K. S. Williams, *The quadratic and quartic character of certain quadratic units II*, Rocky Mountain J. of Math. **9** (1979), 683—692.

9. K. S. Williams, *Integers of biquadratic fields*, Canadian Math. Bull. **13** (1970), 519–526.

FRANZ HALTER-KOCH, MATHEMATISCHES INSTITUT DER UNIVERSITAT GRAZ, HALBÄRTHGASSE 1/1, A-8010 GRAZ