

# On Quadratic and Quartic Characters of Quadratic Units

メタデータ	言語: English 出版者: 公開日: 2017-10-03 キーワード (Ja): キーワード (En): 作成者: Furuta, Yoshiomi, Kaplan, Pierre, 古田, 孝臣 メールアドレス: 所属:
URL	<a href="https://doi.org/10.24517/00011226">https://doi.org/10.24517/00011226</a>

This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 3.0 International License.



## On Quadratic and Quartic Characters of Quadratic Units

Yoshiomi Furuta and Pierre Kaplan

*Department of Mathematics, Faculty of Science, Kanazawa University*  
*U. E. R Sciences Mathématiques, Université de Nancy I*

(Received October 27, 1981)

**Abstract.** Prime decomposition criteria in non-abelian normal extensions  $L$  of degree 8 are studied, where  $L$  is obtained by adjoining a square root or a quartic root of the fundamental unit of a quadratic field according as the norm of the unit is equal to  $-1$  or  $1$ .

### §1. Introduction

Let  $m$  be a positive square free rational integer. In this paper we give an expression to the  $2^n$  ( $n=1$  or  $2$ ) residue symbol of the fundamental unit  $\varepsilon_m$  of the quadratic field  $k = \mathbb{Q}(\sqrt{m})$ , relative to certain primes  $q$ .

If the norm of  $\varepsilon_m$  is  $-1$  we consider the quadratic character of  $\varepsilon_m$ . This case has been already studied, for example in [1], [4]. If the norm of  $\varepsilon_m$  is  $+1$  we consider its biquadratic character. This case has been studied in [5], [6], and later in [3] so as to include also the case where the norm of  $\varepsilon_m$  is  $-1$ . Here we apply the methods and results of [2] to the construction of [3]; this will give for certain  $q$  an expression of  $(\frac{\varepsilon_m}{q})_{2n}$  by certain prime decomposition symbols defined in [2].

We set  $\eta = R + S\sqrt{m}$ , where  $(R, S)$  is the minimum positive solution of

$$(1.1) \quad R^2 - mS^2 = 1.$$

By [3, Lemma 1] there exists a unique decomposition  $m = de$ ,  $d, e > 0$ , a unique pair of positive integers  $V, W$  and a unique number  $t = 1$  or  $2$  such that  $t = 1$  if  $m \not\equiv 1 \pmod{4}$ ,  $(t, d) \neq (1, 1)$  and that

$$(1.2) \quad t = dV^2 - eW^2, \quad \eta = \varepsilon^2,$$

where

$$(1.3) \quad \varepsilon = \frac{V\sqrt{dt} + W\sqrt{et}}{t}.$$

If  $N(\varepsilon_m) = -1$ ,  $\varepsilon = \varepsilon_m^3$  or  $\varepsilon_m$  and if  $N(\varepsilon_m) = +1$ ,  $\varepsilon^2 = \varepsilon_m^3$  or  $\varepsilon_m$  according as the

diophantine equation  $r^2 - ms^2 = 4$  has or has not odd solutions  $(r, s)$ .

The prime decomposition symbol we will consider is  $[dt, -et, q]$ , as defined in [2, Definition 1. 1 and Definition 5. 2] .

Let  $m = p_1 p_2 \cdots p_r$  the decomposition of  $m$  in a product of prime numbers. We consider odd primes  $q$  such that

$$(1. 4) \quad \left(\frac{-1}{q}\right) = \left(\frac{t}{q}\right) = \left(\frac{p_i}{q}\right) = 1 \quad (i=1, \dots, r)$$

Then  $\varepsilon$  can be interpreted as an integer modulo  $q$ , the quadratic residue symbol  $\left(\frac{\varepsilon}{q}\right)$  is well defined, and equal to  $\left(\frac{\varepsilon}{\mathfrak{q}}\right)$  where  $\mathfrak{q}$  is a prime ideal (of degree 1) divisor of  $q$  in any subfield of  $\mathbb{Q}(\sqrt{-1}, \sqrt{t}, \sqrt{p_1}, \dots, \sqrt{p_r})$ .

**§2. Calculation of  $[dt, -et, q]$**

We apply [2, Theorem 5. 1] with  $d_1 = dt$  and  $d_2 = -et$ . As  $t^2 = dtV^2 - etW^2$ , the number  $m$  of [2, Theorem 5. 1] is equal to 1. Also the number  $d$  of [2, Theorem 5. 1] is equal to our number  $t$ . Thus we obtain :

PROPOSITION. *Let  $q$  be a prime number satisfying (1. 4), and congruent to 1 modulo 8 if  $t$  is even or if  $m$  is even and  $d$  or  $-e \equiv -1 \pmod{4}$ . Then*

$$[dt, -et, q] = \left(\frac{dt}{b}\right) = \left(\frac{-et}{b}\right),$$

where  $b, X, Y$  is any solution of the following diophantine equation such that

$$(b, x, y) = 1 \text{ and } (b, 2m) = 1 :$$

- a)  $qb^2 = X^2 + XY + \frac{m+1}{4} Y^2$  if  $m \equiv -1 \pmod{4}$ ,  $d \equiv -e \equiv 1 \pmod{4}$ ,  $t=1$  ;
- b)  $qb^2 = X^2 + mY^2$  if  $m \not\equiv -1 \pmod{4}$ ,  $d$  or  $-e \equiv 1 \pmod{8}$ ,  $t=1$  ;
- c)  $qb^2 = X^2 + 4mY^2$   $\left\{ \begin{array}{l} \text{if } m \equiv -1 \pmod{4}, d \equiv -e \equiv -1 \pmod{4}, t=1, \\ \text{if } m \not\equiv -1 \pmod{4}, d \text{ or } -e \equiv 5 \pmod{8}; \end{array} \right.$
- d)  $qb^2 = X^2 + 16mY^2$  if  $m \equiv 2 \pmod{4}$ ,  $d$  or  $-e \equiv -1 \pmod{4}$  ;
- e)  $qb^2 = (b + 8X + 4Y)^2 + 16mY^2$  if  $m \equiv -1 \pmod{4}$ ,  $t=2$ .

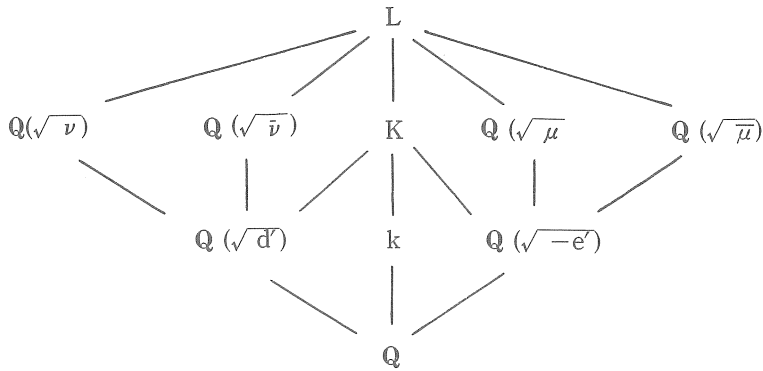
**§3. Determination of  $\left(\frac{\varepsilon}{q}\right)$**

As in [3] we set  $d' = dt$ ,  $e' = et$ ,  $\mu = t - W\sqrt{-e'}$ ,  $\bar{\mu} = t + W\sqrt{-e'}$ ,  $\nu = 2t + 2V\sqrt{d'}$ ,  $\bar{\nu} = 2t - 2V\sqrt{d'}$  and define the following fields :

$$(3. 1) \quad k = \mathbb{Q}(\sqrt{-m}), K = \mathbb{Q}(\sqrt{d'}, \sqrt{-e'}), L = K(\sqrt{\mu}).$$

Then, as  $\mu\bar{\mu} = V^2d'$ ,  $L$  is a dihedral extension of  $\mathbb{Q}$  whose subfield structure is as

follows :



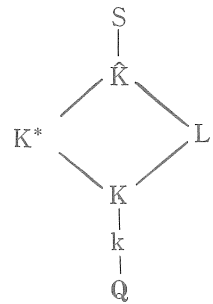
As  $(d', e')=1$  or  $2$  and as  $\nu$  and  $\mu$  are prime to one another up to a square factor in  $K$ , the only ideals which can ramify in  $L/k$  lie above  $2$ . Therefore the conductor  $\mathfrak{f}$  of  $L/k$  is a power of  $2$ .

Let  $S$  be the ray class field modulo  $\mathfrak{f}$  above  $k$ , and let  $\hat{K}$  and  $K^*$  respectively the central class field and the genus field above  $K$  relative to  $S/Q$ .

Then  $L \subset S$ , and, as  $\text{Gal}(L/K)$  belongs to the center of  $\text{Gal}(L/Q)$ ,  $L \subset \hat{K}$ . As  $L/Q$  is non abelian,  $L \not\subset K^*$ , so that  $[\hat{K} : K^*]=2$ .

Let  $q$  be a rational prime congruent to  $1$  modulo  $4$  and decomposed in  $K^*$  in ideals of the first degree. From [2] we have

$$(3.2) \quad [d', -e', q] = \left( \frac{\hat{K}/K^*}{q} \right) = \left( \frac{L/K}{N_{K^*/K} q} \right) = \left( \frac{\mu}{q} \right) = \left( \frac{\nu}{q} \right),$$



where  $q$  and  $\mathfrak{q}$  are prime ideal factor of  $q$  in  $K^*$  and  $K$  respectively.

According to [2, Theorem 4.3], the field  $K^*$  is given as

$$(3.3) \quad K^* = k_0^* Q(\sqrt[f]{T}),$$

where  $k_0^*$  is the ordinary genus field of  $k$ , and  $f$  is a positive rational integer, which can be calculated from the conductor  $\mathfrak{f}$  of the extension  $L/k$ . As  $f$  and  $\mathfrak{f}$  have the same prime factors,  $f$  is a power of  $2$ . Therefore the primes  $q \equiv 1 \pmod{4}$  completely decomposed in  $K^*$  are the primes satisfying (2.1) and, in the case where  $f > 4$

$$(3.4) \quad q \equiv 1 \pmod{f}.$$

From the value of  $\mathfrak{f}$  given in [3], we deduce the value of  $f$ . Both of them are listed in the following table :

Table 1

m	t, d, e	f	f
$m \equiv 1 \pmod{4}$	$e \equiv 1 \pmod{4}$	1 or 2	1 or 4
	$-e \equiv 1 \pmod{4}$	4	8
$m \equiv -1 \pmod{4}$	$t=2$	16	16
	$t=1, d \equiv -e \equiv -1 \pmod{4}$	16	16
	$t=1, d \equiv -e \equiv 1 \pmod{4}, W$ odd	8	8
	$t=1, d \equiv -e \equiv 1 \pmod{4}, W$ even	1 or 4	1 or 4
$m \equiv 2 \pmod{4}$	$d \equiv 2, -e \equiv -1 \pmod{4}$	4	8
	$d \equiv -1, e \equiv 2 \pmod{4}$	4	8
	$d \equiv 2 \pmod{4}, -e \equiv 1 \pmod{8}$	1 or 2	1 or 4
	$d \equiv 1 \pmod{8}, e \equiv 2 \pmod{4}$	1 or 2	1 or 4

Now, using (1. 2) and (1. 3) we obtain

$$(3. 5) \quad \varepsilon \nu = t(\varepsilon + 1)^2,$$

so that  $(\frac{\varepsilon}{q}) = (\frac{t}{q}) (\frac{\nu}{q})$ . Using (3. 2), and noting that  $f=16$  if  $t=2$ , we see that we have the following :

**THEOREM.** *Let  $m$  be a square free positive rational integer,  $m = p_1 p_2 \cdots p_r$  its decomposition in prime factors. Let  $\varepsilon$  be defined by (1. 3), and  $q$  a prime number satisfying (1. 4) and (3. 4) where  $f$  is given in Table 1. Then*

$$(3. 6) \quad \left(\frac{\varepsilon}{q}\right) = [dt, -et, q] .$$

**COROLLARY.** *If  $m$  and  $q$  satisfy the conditions of the Theorem, then*

$$(3. 7) \quad \left(\frac{\varepsilon}{q}\right) = \left(-\frac{dt}{b}\right) = \left(\frac{-et}{b}\right),$$

where  $b$  is defined in the Proposition.

#### References

- [1] Y. Furuta, Norm of units of quadratic fields, J. Math. Soc. Japan, **11** (1959), 139-145.
- [2] ———, A prime decomposition symbol for a non-abelian central extension which is abelian over a bicyclic biquadratic field, Nagoya Math. J., **79** (1980), 79-109.
- [3] F. Halter-Koch, P. Kaplan and K. S. Williams, An Artin character and representations of primes by binary quadratic forms II (to appear).
- [4] P. Kaplan and K. S. Williams, An Artin character and representations of primes by binary quadratic forms, Manuscripta Math., **33** (1981), 339-356.
- [5] E. Lehmer, On the quartic character of quadratic units, J. reine und angew. Math., **268/269** (1974), 294-301.
- [6] P. A. Leonard and K. S. Williams, The quartic characters of certain quadratic units, J. Number Theory **12** (1980), 106-109.