

Author: Giorgos Siligardos

Title: Numerical Approach to an Embedding Problem Concerning Dihedral class fields of order 16

Abstract: Let q be a prime number with $q \equiv 5 \pmod{8}$. If ϵ is the fundamental unit of $(2)q$ and $(2)q = -$, then exactly one of $4(2\epsilon), (8\epsilon)q$ is embedded in a dihedral extension of which is cyclic and unramified outside 2 over q . In this paper we show how we can find which field has the embedding property using numerical procedures.

Creator: HDML

Numerical Approach to an Embedding Problem Concerning Dihedral Class Fields of Order 16

Giorgos Siligardos

Abstract

Let q be a prime number with $q \equiv 5 \pmod{8}$. If ϵ is the fundamental unit of $\mathbb{Q}(\sqrt{2q})$ and $k = \mathbb{Q}(\sqrt{-2q})$, then exactly one of $k(\sqrt[4]{2\epsilon})$, $k(\sqrt[4]{8\epsilon})$, is embedded in a dihedral extension of \mathbb{Q} which is cyclic and unramified outside 2-over k . In this paper we show how we can find which field has the embedding property using numerical procedures.

2000 *Mathematics subject classification*: 11Z05

1. Notation and Preliminaries

Let q be a prime number with $q \equiv 5 \pmod{8}$. We set $D_0 = -8q$, so that D_0 is the fundamental discriminant of $\mathbb{Q}(\sqrt{-2q})$. Let $D_s = 2^{2s}D_0$ and let $H(D_s)$ be the class group of primitive positive definite binary quadratic forms of discriminant D_s . $H_2(D_s)$ will denote the 2-Sylow part of $H(D_s)$ and h will denote the odd part of the class number of $H(D_s)$. By Theorem 3 of [1] we have that $H_2(D_0)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Also, by [3] there is an exact sequence

$$1 \longrightarrow (2^s) \longrightarrow H_2(D_s) \longrightarrow (2) \longrightarrow 1 \quad (1)$$

where (2^s) and (2) denote cyclic groups of order 2^s and 2 respectively. The ambiguous classes of $H_2(D_s)$ for $s \geq 1$ are

$$I_s = [1, 0, 2^{2s+1}q], [4, 4, 1 + 2^{2s-1}q], [q, 0, 2^{2s+1}], \text{ and } [4q, 4q, q + 2^{2s-1}]$$

(where $[a, b, c]$ $a, b, c \in \mathbb{Z}$, denotes the class of the quadratic form $ax^2 + bxy + cy^2$). For $s \geq 1$, $H_2(D_s)$ is not cyclic and so (1) implies that $H_2(D_s)$ is of type $(2^s, 2)$. Let $H_2(D_s) = \langle A_s, B_s \rangle$, where $A_s^{2^s} = B_s^2 = I_s$. The ambiguous classes of $H_2(D_s)$ can be distributed in two genera: $\mathcal{G}_1 = \{I_s, A_s^{2^{s-1}}\}$, $\mathcal{G}_2 = \{B_s, A_s^{2^{s-1}}B_s\}$ and

$$\begin{aligned} I_s &= [1, 0, 2^{2s+1}q], & A_s^{2^{s-1}} &= [4, 4, 1 + 2^{2s-1}q], \\ B_s &= [q, 0, 2^{2s+1}], & A_s^{2^{s-1}}B_s &= [4q, 4q, q + 2^{2s-1}]. \end{aligned}$$

It is easy to see that $I_s, A_s^{2^{s-1}}$ represent numbers m such that $m \equiv 1 \pmod{8}$ and that $B_s, A_s^{2^{s-1}}B_s$ represent numbers n such that $n \equiv 5 \pmod{8}$. We shall denote by k the quadratic field $\mathbb{Q}(\sqrt{-2q})$ and by $k(D_s)$ the Ring Class Field modulo 2^s over k . Also, $k_2(D_s)$ will denote the maximum 2-extension of \mathbb{Q} inside $k(D_s)$ and finally, for a subgroup H of $H_2(D_s)$ we shall denote by L_H the corresponding subfield of $k_2(D_s)$ via the Artin isomorphism. (Note that the notation of this paper is in fully agreement with the notation in [3] for convenience.) By [3] we have that there is an epimorphism

$$\Phi_s : H_2(D_{s+1}) \longrightarrow H_2(D_s) : [a, 2b, 4c] \longrightarrow [a, b, c]$$

which is induced by the restriction epimorphism of Galois groups:

$$G(k_2(D_{s+1})/k) \longrightarrow G(k_2(D_s)/k).$$

It is easy to see that $\Phi_s(B_{s+1}) = B_s$ and that we may choose the A_s in such a way that $\Phi_s(A_{s+1}) = A_s$. Obviously, if $H_{s+1} \leq H_2(D_{s+1})$ and $\Phi_s(H_{s+1}) = H_s$, then $L_{H_s} \subseteq L_{H_{s+1}}$ and particularly for $s \geq 2$ and $\ell, j \in \mathbb{Z}$ such that $\ell, j \geq 0$ it holds that $L_{\langle A_s^{2^\ell}, B_s^j \rangle} = L_{\langle A_{s+1}^{2^\ell}, B_{s+1}^j \rangle}$ since these two fields have the same degree over k .

For an integer m and an element C of $H_2(D_s)$ we shall use the notation $C \longrightarrow m$ to show that C represents properly m (that is, there is a quadratic form $f \in C$ and $x, y \in \mathbb{Z}$ with $(x, y) = 1$ such that $f(x, y) = m$).

For this paper we shall need the following two propositions:

Proposition 1 Let p be a prime odd number ($p \neq q$) and $C \in H_2(D_s)$ ($s \in \mathbb{Z}, s \geq 1$) with $C^4 = 1$. It holds that $C \longrightarrow p^h$ if and only if the decomposition field of p in $k_2(D_s)$ is $L_{\langle C \rangle}$. \square

Proposition 2 Let $k \in \mathbb{Z}, k \geq 1$. Every unramified outside 2 cyclic extension of k of degree 2^k which is dihedral over \mathbb{Q} is contained in $k_2(D_k)$. \square

(Remark : Proposition 1 is lemma 1 of [3] and Proposition 2 is implied by Satz 11 of [4] and the structure of $H_2(D_s)$.)

2. Elementary Aspects

In this section we shall state two propositions which show the inductive representation ability of p^h by B_s and $A_s^{2^{s-1}}B_s$, for an odd prime p and an integer s with $s \geq 1$.

Proposition 3 Let $s \in \mathbb{Z}, s \geq 1$.

1. If $B_s \longrightarrow p^h$ with solution (x, y) (that is $p^h = qx^2 + 2^{2s+1}y^2$, $x, y \in \mathbb{Z}$, $(x, y) = 1$), then:

(a) x is odd.

- (b) If y is even, then $B_{s+1} \rightarrow p^h$ with solution $(x, \frac{y}{2})$.
- (c) If y is odd, then $A_{s+1}^{2^{(s+1)-1}} B_{s+1} \rightarrow p^h$ with solution $(\frac{x-y}{2}, y)$.
2. If $B_{s+1} \rightarrow p^h$ with solution (x, y) , then $B_s \rightarrow p^h$ with solution $(x, 2y)$.
3. If $A_{s+1}^{2^{(s+1)-1}} B_{s+1} \rightarrow p^h$ with solution (x, y) , then $B_s \rightarrow p^h$ with solution $(2x + y, y)$. \square

The proof of Proposition 3 is an elementary exercise. Now, since for $s \geq 1$, B_s and $A_s^{2^{s-1}} B_s$ generate different subgroups of $H_2(D_s)$, Proposition 1 implies that if p^h is represented by one of them, then it is represented by exactly one. This result along with Proposition 3 enables us to state the following Proposition:

Proposition 4

1. If $B_s \rightarrow p^h$ or $A_s^{2^{s-1}} B_s \rightarrow p^h$, for $s \geq 1$, then it also holds that $B_1 \rightarrow p^h$. (That is there are $x, y \in \mathbb{Z}$, $(x, y) = 1$, such that $p^h = qx^2 + 8y^2$).
2. If there are $x, y \in \mathbb{Z}$, $(x, y) = 1$, with $p^h = qx^2 + 8y^2$, then if one sets $y = 2^{s_0} r$, with $s_0 \geq 0$ and r odd, then for $s \in \mathbb{Z}$, $s \geq 1$ it holds:
- $B_s \rightarrow p^h$ if and only if $1 \leq s \leq s_0 + 1$ (with solution: $(x, \frac{y}{2^{s-1}})$);
 - $A_s^{2^{s-1}} B_s \rightarrow p^h$ if and only if $s = s_0 + 2$ (with solution: $(\frac{x-r}{2}, r)$). \square

3. The Embedding Problem and Study of the Subfields Involved

We start this section with a Definition and a Lemma:

Definition 1 Let $n \in \mathbb{Z}$, $n \geq 2$. We shall say that a field M is a $\mathcal{DF}(n)$ field when the following hold:

- $k \subseteq M$ and M/k is unramified outside 2;
- The Galois group $G(M/k)$ is cyclic of order n ;
- The Galois group $G(M/\mathbb{Q})$ is the dihedral group of order $2n$. \square

(Remark : Note that, by Proposition 2, for every $k \in \mathbb{Z}$, all $\mathcal{DF}(2^k)$ fields are contained in $k_2(D_k)$.)

Lemma 1 Let ϵ be the fundamental unit of $\mathbb{Q}(\sqrt{2q})$. The following hold:

1. $k(\sqrt{\epsilon})$ and $k(\sqrt{2\epsilon})$ are $\mathcal{DF}(4)$ fields not equal.

2. $k(\sqrt[4]{2\epsilon})$ and $k(\sqrt[4]{8\epsilon})$ are $\mathcal{DF}(8)$ fields not equal. \square

Proof Using (1.1) of [6] we may easily see that ϵ has norm -1 over \mathbb{Q} . Also, by Lemma 1 of [2], we have that $k(\sqrt[4]{2\epsilon})$ is a $\mathcal{DF}(8)$ field and that $G(k(\sqrt[4]{2\epsilon})/\mathbb{Q}) = \langle \sigma, \tau \rangle$ with:

$$\sigma(\sqrt{2q}) = -\sqrt{2q}, \quad \sigma(i) = -i, \quad \sigma(\sqrt[4]{2\epsilon}) = \frac{1-i}{\sqrt[4]{2\epsilon}}$$

$$\tau(\sqrt{2q}) = \sqrt{2q}, \quad \tau(i) = -i, \quad \tau(\sqrt[4]{2\epsilon}) = \sqrt[4]{2\epsilon}$$

and $\sigma^8 = \tau^2 = 1$, $\tau\sigma = \sigma^7\tau$. This proves that $k(\sqrt[4]{2\epsilon})$ is a $\mathcal{DF}(8)$ field. Similarly, we may prove that $k(\sqrt[4]{8\epsilon})$ is a $\mathcal{DF}(8)$ field with $G(k(\sqrt[4]{8\epsilon})/\mathbb{Q}) = \langle \sigma_1, \tau_1 \rangle$ such that:

$$\sigma_1(\sqrt{2q}) = -\sqrt{2q}, \quad \sigma_1(i) = -i, \quad \sigma_1(\sqrt[4]{8\epsilon}) = \frac{2(1-i)}{\sqrt[4]{8\epsilon}}$$

$$\tau_1(\sqrt{2q}) = \sqrt{2q}, \quad \tau_1(i) = -i, \quad \tau_1(\sqrt[4]{8\epsilon}) = \sqrt[4]{8\epsilon}$$

and $\sigma_1^8 = \tau_1^2 = 1$, $\tau_1\sigma_1 = \sigma_1^7\tau_1$. Moreover, $k(\sqrt[4]{2\epsilon}) \neq k(\sqrt[4]{8\epsilon})$ because $\sqrt{2} \notin k(\sqrt[4]{2\epsilon})$ ($k(i)$ is the only intermediate extension of $k(\sqrt[4]{2\epsilon})/k$). The first part of the Lemma concerning $k(\sqrt{\epsilon})$ and $k(\sqrt{2\epsilon})$ is an easy exercise using Satz 1 of [5]. \blacksquare

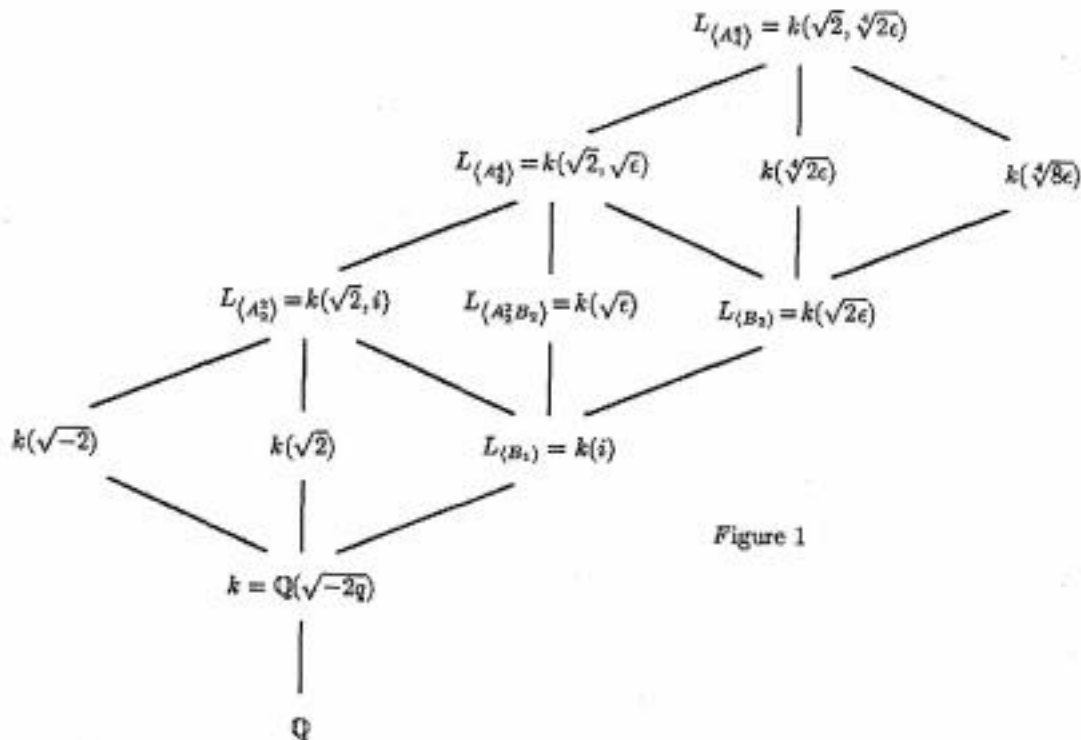


Figure 1

We now proceed to the study of the class subfields (see Figure 1). By Proposition 2 and the group structure of $H_2(D_8)$ we induce that amongst the $\mathcal{DF}(2)$ fields: $L_{\langle B_1 \rangle}$, $L_{\langle A_1 B_1 \rangle}$ and $L_{\langle A_1 \rangle}$, only $L_{\langle B_1 \rangle}$ is embedded in a $\mathcal{DF}(4)$ field and moreover, there are only two $\mathcal{DF}(4)$ extensions of $L_{\langle B_1 \rangle}$ which are: $L_{\langle B_2 \rangle}$, and $L_{\langle A_2^2 B_2 \rangle}$. Since $k(i)$ is a $\mathcal{DF}(2)$ field and it is contained in both $k(\sqrt{\epsilon})$ and $k(\sqrt{2\epsilon})$ (which, by Lemma 1, are $\mathcal{DF}(4)$ fields) we have that

$$L_{\langle B_1 \rangle} = k(i) \quad \text{and} \quad \{L_{\langle B_2 \rangle}, L_{\langle A_2^2 B_2 \rangle}\} = \{k(\sqrt{\epsilon}), k(\sqrt{2\epsilon})\}.$$

Going one step further, of the two $L_{\langle B_2 \rangle}, L_{\langle A_2^2 B_2 \rangle}$, only $L_{\langle B_2 \rangle}$ is embedded in a $\mathcal{DF}(8)$ field and moreover there are exactly two $\mathcal{DF}(8)$ extensions of $L_{\langle B_2 \rangle}$ which are: $L_{\langle B_3 \rangle}$ and $L_{\langle A_3^2 B_3 \rangle}$. Since, by Lemma 1, $k(\sqrt[4]{2\epsilon}), k(\sqrt[4]{8\epsilon})$ are $\mathcal{DF}(8)$ extensions containing $k(\sqrt{2\epsilon})$, we conclude that:

$$L_{\langle B_2 \rangle} = k(\sqrt{2\epsilon}) \quad \text{and} \quad \{L_{\langle B_3 \rangle}, L_{\langle A_3^2 B_3 \rangle}\} = \{k(\sqrt[4]{2\epsilon}), k(\sqrt[4]{8\epsilon})\}.$$

Going one more step further, of the two $L_{\langle B_3 \rangle}, L_{\langle A_3^2 B_3 \rangle}$, only $L_{\langle B_3 \rangle}$ is embedded in a $\mathcal{DF}(16)$ field and moreover there are exactly two $\mathcal{DF}(16)$ extensions of $L_{\langle B_3 \rangle}$ which are: $L_{\langle B_4 \rangle}$ and $L_{\langle A_4^4 B_4 \rangle}$. This last result defines the embedding problem for the fields $k(\sqrt[4]{2\epsilon})$ and $k(\sqrt[4]{8\epsilon})$ (see Figure 1). In the next section we shall see a numerical way for the determination of $L_{\langle B_3 \rangle}$.

4. Main results

In the previous section we saw that $L_{\langle B_1 \rangle} = k(i)$. So, Proposition 1 implies that for an odd prime number p with $p \neq q$ it holds:

$$p^h = qx^2 + 8y^2, (x, y) = 1 \text{ is solvable in } \mathbb{Z} \Leftrightarrow \left(\frac{-2q}{p}\right) = 1 \text{ and } p \equiv 5 \pmod{8}. \quad (2)$$

Moreover, assume that p is an odd prime number satisfying the conditions given above. Since $L_{\langle B_2 \rangle} = k(\sqrt{2\epsilon})$, Propositions 1 and 4 imply that

$$y \text{ is even in (2)} \Leftrightarrow \left(\frac{2\epsilon}{p}\right) = 1. \quad (3)$$

Now, if y is even, we may write $y = 2z$, $z \in \mathbb{Z}$, and again since $\{L_{\langle B_3 \rangle}, L_{\langle A_3^4 B_3 \rangle}\} = \{k(\sqrt[4]{2\epsilon}), k(\sqrt[4]{8\epsilon})\}$, Propositions 1 and 4 imply the following Theorem:

Theorem 1 Let q be an odd prime number with $q \equiv 5 \pmod{8}$ and ϵ be the fundamental unit of $\mathbb{Q}(\sqrt{2q})$. Let also $k = \mathbb{Q}(\sqrt{-2q})$. For an odd prime p with $p \neq q$ such that $p^h = qx^2 + 32z^2$ for some $x, z \in \mathbb{Z}$, $(x, z) = 1$, it holds that:

$$k(\sqrt[4]{2\epsilon}) \text{ is contained in a } \mathcal{DF}(16) \text{ field if and only if } s_p = (-1)^z.$$

Where

$$s_p = \begin{cases} 1, & \text{if } p \text{ splits completely in } k(\sqrt[4]{2\epsilon}) \\ -1, & \text{otherwise. } \square \end{cases}$$

So, a proper choice of p can determine the solution of the embedding problem. In Table (I) there are numerical examples for various q . The primes p are chosen to be the minimum primes satisfying:

$$p \equiv 5 \pmod{8}, \left(\frac{-2q}{p}\right) = \left(\frac{2\epsilon}{p}\right) = 1$$

so that there are $x, z \in \mathbb{Z}$, $(x, z) = 1$, with $p^h = qx^2 + 32z^2$.

From Table (I) and other numerical examples a conjecture may be stated. If we write $\epsilon = u + v\sqrt{2q}$ with $u, v \in \mathbb{Z}$, then, since $u^2 - 2qv^2 = -1$, we have that u is odd and so v is odd (take $u^2 - 2qv^2 = -1$ modulo 8) which means that $(u+v) \equiv 0 \pmod{2}$. Now, we may look at the examples in Table (I) to see the following conjecture being accomplished:

Conjecture 1 Let q be an odd prime number with $q \equiv 5 \pmod{8}$ and $\epsilon = u + v\sqrt{2q}$ be the fundamental unit of $\mathbb{Q}(\sqrt{2q})$, with $u, v \in \mathbb{Z}$. For $k = \mathbb{Q}(\sqrt{-2q})$, the following equivalence holds:

$$k(\sqrt[4]{2\epsilon}) \text{ is contained in a } \mathcal{DF}(16) \text{ field} \Leftrightarrow \frac{u+v}{2} \equiv 0 \pmod{2}. \square$$

Table (I)

q	k	(u, v)	p	$*p$	(s, e)	$\frac{(u+v)}{2} \pmod{2}$	Embedded Field
5	1	(3,1)	37	-1	(1,1)	0	$k(\sqrt[3]{27})$
13	3	(5,1)	37	-1	(41,30)	1	$k(\sqrt[3]{87})$
29	1	(99,13)	61	-1	(3,1)	0	$k(\sqrt[3]{27})$
37	5	(43,5)	5	+1	(9,2)	0	$k(\sqrt[3]{27})$
53	5	(4005,389)	101	+1	(51,167)	1	$k(\sqrt[3]{87})$
61	5	(11,1)	29	-1	(471,467)	0	$k(\sqrt[3]{27})$
101	3	(3141,221)	53	-1	(3,68)	1	$k(\sqrt[3]{87})$
109	5	(251,17)	13	-1	(23,99)	0	$k(\sqrt[3]{27})$
149	3	(409557,23725)	13	-1	(1,8)	1	$k(\sqrt[3]{87})$
157	13	(443,25)	5	+1	(1317,5444)	0	$k(\sqrt[3]{27})$
173	5	(93,5)	5	+1	(3,7)	1	$k(\sqrt[3]{87})$
181	9	(19,1)	53	-1	(2191455,8715137)	0	$k(\sqrt[3]{27})$
197	5	(395023035,19900975)	13	-1	(5,107)	0	$k(\sqrt[3]{27})$
249	3	(69051,2977)	101	+1	(8221,1764)	0	$k(\sqrt[3]{27})$
277	11	(174293,7405)	5	+1	(387,479)	1	$k(\sqrt[3]{87})$
293	9	(4115086707,169999665)	5	-1	(81,31)	0	$k(\sqrt[3]{27})$
317	7	(65999458125,2621173333)	29	+1	(9949,7791)	1	$k(\sqrt[3]{87})$
373	13	(3534843,202645)	5	+1	(1896,46)	0	$k(\sqrt[3]{27})$
389	7	(54610269,1957873)	29	+1	(5543,12867)	1	$k(\sqrt[3]{87})$
401	9	(419288307,13808525)	13	+1	(2575,15358)	0	$k(\sqrt[3]{27})$
541	11	(1262101,38369)	13	+1	(20443,221323)	1	$k(\sqrt[3]{87})$
701	7	(930015700509,24857960029)	61	+1	(65325,68899)	1	$k(\sqrt[3]{87})$

References

- [1] E. Brown, *The Power of 2 Dividing the Class Number of a Binary Quadratic Discriminant*, Journal of Number Theory, **5**, (1973), 413-419
- [2] F. Halter Koch, *Ring Class Fields modulo 8 of $\mathbb{Q}(\sqrt{-m})$ and the quartic character of units of $\mathbb{Q}(\sqrt{m})$ for $m \equiv 1 \pmod{8}$* , Osaka J. Math., **26** (1989), 625-646
- [3] F. Halter Koch, *Representation of Primes by Binary Quadratic Forms of Discriminant $-256q$ and $-128q$* , Glasgow Math. J., **35** (1993), 261-268
- [4] F. Halter Koch, *Arithmetische Theorie der Normalkörper von 2-Potenzgrad mit Diedergruppe*, Journal Of Number Theory **33** (1971), 412-443
- [5] F. Halter Koch, *Konstruktion von Klassenkörpern und Potenzrestkriterien für quadratische Einheiten*, Manuscripta Math., **54** (1986), 453-492

- [6] F. Halter Koch, P. Kaplan, K.
tions of Primes by Binary Q
357-381

◇ Giorgos Siligardos

Department of Applied Mathematics
Univeristy of Crete
Heraclion, GREECE
siligard@math.uoc.gr