Power Bases in Dihedral Quartic Fields

Anthony C. Kable*

Department of Mathematics, Oklahoma State University, Stillwater, Oklahoma 74078

Communicated by Alan C. Woods

Received May 23, 1998

A quartic number field, $L$, is called dihedral if the normal closure, $N$, of $L$ satisfies $\text{Gal}(N/Q) \cong D_8$. We investigate whether or not the ring of integers of such a quartic field has a power basis. When the quadratic subfield of $L$ is imaginary, the problem is completely solved. When it is real, the same method leads to a solution in many cases. Several numerical illustrations of the method are given.

A number field, $L$, is said to have a power basis if there is an algebraic integer, $\alpha$, in $L$ such that $\mathcal{O}_L = \mathbb{Z}[\alpha]$, where $\mathcal{O}_L$ denotes the ring of integers of $L$. Interest in the problem of the existence of power bases has a long history, going back at least as far as Dedekind’s well-known example of a cubic field without such a basis [4], and investigation of it lent impetus to the clarification of such basic notions as discriminant and the decomposition of primes in extensions. An effective procedure for deciding whether a particular number field has a power basis has been given by Györy [10] (it should be emphasized that Györy’s powerful results have much greater scope than has been mentioned here), but this method leads to infeasible computations for number fields of quite moderate degree and discriminant. Also, Györy’s method is unsuitable for deriving results such as Corollaries 1 and 2 below. We are thus led to seek feasible procedures in special situations.

The purpose of this work is to investigate the existence of power bases in quartic number fields whose normal closure has dihedral Galois group over $Q$ (henceforth dihedral quartic fields). This case has already received some attention in [11] and after our results have been proved we shall indicate how they relate to that work. For the special case of pure quartic fields, Funakura in [7] has solved the problem of the existence of a power basis. He relies on a direct calculation of the indicial form of the field, which would make the extension of his method to the general case quite cumbersome. We shall take a less direct route. Because of Funakura’s prior work, we shall largely ignore the pure case here.

* Current address: Department of Mathematics, Cornell University, Ithaca, New York 14853.
We begin by recalling some basic facts and establishing some notation. Let \( L \) be a dihedral quartic field. Then \( L \) has a unique quadratic subfield \( k = \mathbb{Q}(\sqrt{d}) \), where \( d \) is a square-free integer. We let \( \omega \in \mathcal{O}_k \) be \( \sqrt{d} \) when \( d \equiv 2, 3 \pmod{4} \) and \((1 + \sqrt{d})/2 \) when \( d \equiv 1 \pmod{4} \) so that \( \mathcal{O}_k = \mathbb{Z}[\omega] \).

The field \( L \) may then be expressed as \( \mathbb{Q}(\sqrt{2}) \) where \( \sqrt{2} = a + b\omega \) and \( a, b \in \mathbb{Z} \).

We let \( \mathcal{N} = \mathcal{N}_k \mathbb{Q}(\sqrt{2}) \) where \( \mathcal{N}_k \) is the norm from \( k \) to \( \mathbb{Q} \).

We shall need to identify several subfields of the normal closure, \( N \), of \( L \). The Galois group \( \text{Gal}(N/\mathbb{Q}) \) may be presented as \(_{\sigma, \tau} \) where \(_{\sigma, \tau} \) is either of the elements of \( \text{Gal}(N/\mathbb{Q}) \) of order four.

If \( H/J \) is any extension of number fields then we let \( \delta(H/J) \) (respectively \( \mathcal{D}(H/J) \)) be the relative discriminant (respectively relative different) of the extension. The absolute discriminant \( \delta(L) \) is then a distinguished generator for the ideal \( \mathcal{D}(L) \). Each number \( \cdot \in H \) has a relative discriminant \( \delta_H(\cdot) \in \mathcal{D}(H) \) and relative different \( \mathcal{D}(H/J) \) and an integer \( \cdot \in \mathcal{O}_H \) satisfies

\[
\mathcal{O}_H = \mathcal{O}_J[\cdot] \quad \text{if and only if} \quad \delta_H(\cdot) \text{ generates } \mathcal{D}(H/J).
\]

For a detailed account of the theory of different and discriminants the reader may consult [6], whose notation we are following.

The final preliminary observation we require concerns the signature of \( L \). The field \( L \) may have four distinct embeddings into the real numbers, in which case we call it \textit{totally real}, or it may have no embeddings into the real numbers, in which case we call it \textit{totally complex}, or it may have precisely two distinct embeddings into the real numbers, in which case we call it \textit{mixed}. It is well-known (see [6, II.1, p. 52]) that \( \delta_L \) is positive when \( L \) is totally real or totally complex and negative when \( L \) is mixed. We claim that \( \cdot \) always has the same sign as \( \delta_L \); unfortunately, this must be verified by a consideration of cases. If \( k \) is an imaginary quadratic field then \( L \) must be totally complex and so \( \delta_L \) is positive and \( \cdot \), being a norm from \( k \), is also positive. If \( k \) is a real quadratic field then \( L \) is totally real when both \( \delta^2 \) and \( (\delta')^2 \) are positive, totally complex when both \( \delta^2 \) and \( (\delta')^2 \) are negative and mixed when these two numbers have opposite signs. Since \( \cdot = \delta^2(\delta')^2 \), in each of these situations \( \cdot \) has the same sign as \( \delta_L \). This verifies our claim.

\textbf{Theorem 1.} Let \( \cdot = x + y\sqrt{d} \in L \) with \( x, y \in k \) and define \( C = \mathcal{N}_k(2y) \) and \( A = (x-x')^2 - \text{Tr}_{k/\mathbb{Q}}(y^2\delta') \), where \( \text{Tr}_{k/\mathbb{Q}} \) denotes the trace from \( k \) to \( \mathbb{Q} \). Then \( \mathcal{O}_L = \mathbb{Z}[\cdot] \) if and only if the following conditions hold:

\[
\langle \sigma, \tau | \sigma^2 = \tau^4 = 1, \sigma \tau = \tau^3 \rangle,
\]

where \( \text{Gal}(N/L) \) is generated by \( \sigma \) and \( \tau \) is either of the elements of \( \text{Gal}(N/\mathbb{Q}) \) of order four. Then \( \text{Gal}(N/k) = \langle \sigma, \tau^2 \rangle \) and so \( \tau \) induces the non-trivial automorphism of \( k \). We shall denote by \( k' \) (respectively \( F \)) the quadratic (respectively biquadratic) field fixed by the subgroup \( \langle \sigma, \tau^2 \rangle \) (respectively \( \langle \tau^2 \rangle \)). The field \( F \) is the compositum of \( k \) and \( k' \).

Theorem 1. Let \( \gamma = x + y\sqrt{d} \in L \) with \( x, y \in k \) and define \( C = \mathcal{N}_k(2y) \) and \( A = (x-x')^2 - \text{Tr}_{k/\mathbb{Q}}(y^2\delta'), \) where \( \text{Tr}_{k/\mathbb{Q}} \) denotes the trace from \( k \) to \( \mathbb{Q} \). Then \( \mathcal{O}_L = \mathbb{Z}[\cdot] \) if and only if the following conditions hold:
(a) \( \alpha \in \mathcal{O}_L \),
(b) \( v d_k^2 C^2 = d_L \),
(c) With the appropriate choice of sign, \( 4A^2 = C^2 v \pm 4 d_k \).

**Proof.** We first suppose that \( \mathcal{O}_L = \mathbb{Z}[\alpha] \). Then certainly \( \alpha \in \mathcal{O}_L \). Moreover, \( \mathcal{O}_L = \mathcal{O}_L[\{\alpha\}] \) and so \( A_{L,q}(\alpha) \) generates \( \mathfrak{b}(L/k) \). Since \( \text{Gal}(L/k) = \langle \tau^2 \rangle \) and \( \tau^2 = -\tau \) we have

\[
\mathfrak{b}(L/k) = (A_{L,q}(\alpha)) = (N_{L,q}(\alpha - \alpha^\tau)) = (N_{L,q}(2\gamma)) = (4\gamma^2) = d_k^2 \]

where \( (\beta) \) denotes the principal ideal generated by \( \beta \). But then, from the general behavior of discriminants in towers of extensions (see [6, III.2.15]), we have

\[
\mathfrak{b}(L/\mathbb{Q}) = N_{k/\mathbb{Q}}(\mathfrak{b}(L/k)) \cdot \mathfrak{b}(k/\mathbb{Q})^2 = (16 N_{k/\mathbb{Q}}(\gamma)^2 v d_k^2) = (v d_k^2 C^2).
\]

Now \( d_L \) also generates \( \mathfrak{b}(L/\mathbb{Q}) \) and, by the remarks preceding the statement of the Theorem, \( d_L \) and \( v \) have the same sign. It follows that \( d_L = v d_k^2 C^2 \) and hence condition (b) is satisfied.

Next observe that

\[
A_{L,q}(\alpha) = N_{L,q}(\delta_{L,q}(\alpha)) = N_{L,q}((\alpha - \alpha')(\alpha - \alpha^\tau)(\alpha - \alpha^\tau)) = N_{L,q}(2\gamma) N_{L,q}((\alpha - \alpha')(\alpha - \alpha^\tau)) = 16 N_{L,q}(\gamma)^2 N_{L,q}(\delta^2) N_{L,q}((\alpha - \alpha')(\alpha - \alpha^\tau)) = C^2 N_{L,q}((\alpha - \alpha')(\alpha - \alpha^\tau))
\]

and so, in the presence of condition (b),

\[
d_k^2 A_{L,q}(\alpha) = d_L N_{L,q}((\alpha - \alpha')(\alpha - \alpha^\tau)).
\]

This equation implies, still in the presence of (b), that an integer \( \alpha \) satisfies \( \mathcal{O}_L = \mathbb{Z}[\alpha] \) if and only if

\[
N_{L/q}((\alpha - \alpha')(\alpha - \alpha^\tau)) = \pm d_k^2.
\]
Since \((\alpha - \alpha^\tau)(\alpha - \alpha^{\tau^*}) \in \mathcal{L}\), (1) is trivially equivalent to
\[
N_{\mathbb{N}/\mathbb{Q}}((\alpha - \alpha^\tau)(\alpha - \alpha^{\tau^*})) = d_k^2.
\] (2)

Since the inner automorphism of \(\text{Gal}(\mathbb{N}/\mathbb{Q})\) induced by \(\sigma\) interchanges \(\tau\) and \(\tau^\ast\), we have
\[
N_{\mathbb{N}/\mathbb{Q}}(\alpha - \alpha^\tau) = N_{\mathbb{N}/\mathbb{Q}}(\alpha - \alpha^{\tau^*})
\]
and hence (2) is equivalent to
\[
N_{\mathbb{N}/\mathbb{Q}}(\alpha - \alpha^\tau) = \pm d_k^2.\] (3)

We now wish to calculate \(N_{\mathbb{N}/\mathbb{Q}}(\alpha - \alpha^\tau)\) by making use of the tower of fields \(\mathbb{N} \supset F \supset k' \supset \mathbb{Q}\) introduced in the preliminary discussion. We begin by calculating \(N_{\mathbb{N}/F}(\alpha - \alpha^\tau)\). Since \(\text{Gal}(\mathbb{N}/F) = \langle \tau^2 \rangle\), \(\tau^2\) is central in \(\text{Gal}(\mathbb{N}/\mathbb{Q})\) and \(\beta^{r^2} = -\beta\) we have
\[
N_{\mathbb{N}/F}(\alpha - \alpha^\tau) = [(x - x^\tau) + (y\beta - y^\tau\beta^\tau)][(x - x^\tau) + (y\beta - y^\tau\beta^\tau)]^{\tau^2}
= [(x - x^\tau) + (y\beta - y^\tau\beta^\tau)][(x - x^\tau) - (y\beta - y^\tau\beta^\tau)]
= (x - x^\tau)^2 - (y\beta - y^\tau\beta^\tau)^2
= (x - x^\tau)^2 - \text{Tr}_{k'/\mathbb{Q}}(y^2\beta^2) + (C/2) \beta \beta^\tau
= A + (C/2) \sqrt{r},
\]
where at the last step we have used the fact that \((\beta \beta^\tau)^2 = N_{\mathbb{K}/\mathbb{Q}}(\beta^2) = v\).

Thus \(N_{\mathbb{N}/F}(\alpha - \alpha^\tau)\) actually lies in \(k'\) and we have
\[
N_{\mathbb{N}/\mathbb{Q}}(\alpha - \alpha^\tau) = N_{k'/\mathbb{Q}}(N_{\mathbb{N}/F}(\alpha - \alpha^\tau))^2
= N_{k'/\mathbb{Q}}(A + (C/2) \sqrt{r})^2
= (A^2 - (C^2/4) v)^2.
\]

Thus Equation (3) is equivalent to
\[
A^2 - (C^2/4) v = \pm d_k
\] (4)

which is condition (c) of the statement.

To summarize, we have shown that, in the presence of condition (b), an integer \(\alpha\) satisfies \(\mathcal{C}_u = \mathbb{Z}[\alpha]\) if and only if condition (c) holds. Since we have also shown that \(\mathcal{C}_u = \mathbb{Z}[\alpha]\) leads to condition (b), this completes the proof of the Theorem.
Corollary 1. Let $L$ be a dihedral quartic field containing the quadratic field $k$. If $L$ has a power basis then, with a suitable choice of sign, $d_L \pm 4d_k^3$ is a square.

Proof. Combining conditions (b) and (c) of the Theorem we obtain

$$4d^2_k A^2 = d_L \pm 4d_k^3$$

and since $A$ is a rational number the conclusion follows.

Corollary 2. Let $L$ be a mixed dihedral quartic field containing the quadratic field $k$. If $L$ has a power basis then $|d_L| \leq 4d_k^3$. In particular, there are only finitely-many mixed dihedral quartic fields having a power basis and containing a given real quadratic field.

Proof. Since $L$ is mixed, $d_L$ is negative. The previous Corollary implies that $d_L + 4d_k^3 \geq 0$ and the inequality follows. It is well-known that there are only finitely-many number fields with a given discriminant and from this the finiteness statement follows.

It is instructive to compare Corollary 2 with Theorem 2 of [11]. It is there shown that every quadratic field, $k$, is contained in infinitely-many dihedral quartic fields with a power basis. The question of signature is not considered, but it is easy to verify from the proof that the dihedral quartic fields constructed by Huard et al. are totally real when $k$ is a real quadratic field. Thus the finiteness statement of Corollary 2 is confined to mixed fields. This connection between the signature of $L$ and the existence of a power basis in $L$ seems surprising (at least to the author). Since earlier work in which the existence of power bases has been extensively studied has focussed on normal extensions of $\mathbb{Q}$, all of which are either totally real or totally complex, there is currently insufficient evidence from which to guess whether this is an isolated phenomenon. (For examples of this work, the reader may consult [1, 3, 8, 9, 12].)

In order to make effective use of Theorem 1 we need to determine the conditions imposed on $x, y \in k$ by the condition $x + y\mathfrak{d} \in \mathcal{O}_L$. This information could be extracted from the tables in [11] but it seems easier to obtain it directly.

Lemma 1. Suppose that $x, y \in k$ and $x + y\mathfrak{d} \in \mathcal{O}_L$. Then $2x \in \mathcal{O}_k$. If the prime (ideal) factorization of $\mathfrak{d}^2 \mathfrak{c}_k$ in $\mathcal{O}_k$ is square-free then $2y \in \mathcal{O}_k$ also. In general, $2my \in \mathcal{O}_k$, where $m^2$ is the greatest square divisor of $d(a, b)^2$ if $d \equiv 1 \pmod{4}$ and of $2d(a, b)^2$ if $d \equiv 2, 3 \pmod{4}$.

Proof. The number $x + y\mathfrak{d}$ is an integer if and only if $\text{Tr}_{L/k}(x + y\mathfrak{d}) = 2x$ and $\text{N}_{L/k}(x + y\mathfrak{d}) = x^2 - y^2\mathfrak{d}^2$ are both integers. Thus if $x + y\mathfrak{d} \in \mathcal{O}_L$ then
any gives rise to a power basis and set 2. Then for each number field \(L\) containing \(k\), we shall now describe a method by which all these classes may be determined for any dihedral quartic field. Suppose that \(\alpha = x + y\beta\) gives rise to a power basis and set \(2x = z_1 + z_2\beta\) and \(2ny = z_3 + z_4\beta\), where \(m\) is the integer defined in Lemma 1 (if \(\beta^2\) happens to be square-free then we may take \(m = 1\) instead). Then \(z_j \in \mathbb{Z}\) for \(j = 1, ..., 4\). The discriminant \(d_k\) has been calculated in [11] and using it we may determine the possible values of \(A\) and \(C\) in Theorem 1. Then \(z_3\) and \(z_4\) must satisfy the equation

\[ N_{k/\mathbb{Q}}(z_3 + z_4\beta) = m^2C \]  

(7) and, since \(z_3\) and \(z_4\) are integers and \(k\) is imaginary, this equation has finitely-many solutions and they may be effectively determined. Passing to an integer equivalent to \(\alpha\), we may assume without loss of generality that \(z_1 = 0\) or \(z_1 = 1\). Finally, the equation

\[ m^2z_3^2(\alpha - \beta)^2 = 4m^2A + Tr_{k/\mathbb{Q}}(z_3 + z_4\beta)^2 \beta^2 \]  

(8) (which comes from the definition of \(A\)) determines the possible values for \(z_2\). For each possible quadruple \((z_1, z_2, z_3, z_4)\) we then need only check whether the corresponding \(x\) is integral. In this way a complete set of representatives for the classes of integers which give rise to a power basis will be obtained. This method may also be applied when \(k\) is a real quadratic field,
but need not succeed, since, in this case, (7) always has infinitely-many solutions if it has one. Never the less, the author has been unable to discover an example of a dihedral quartic field containing a real quadratic subfield for which the method described here fails to determine whether it has a power basis.

As an illustration, let us consider the fields $L_1$ and $L_2$ generated over $\mathbb{Q}$ by $\theta_1$ and $\theta_2$, where $\theta_1^2 = 11 + 2\sqrt{-3}$ and $\theta_2^2 = (23 + \sqrt{-3})/2$. These fields both contain $k = \mathbb{Q}(\sqrt{-3})$ and we set $\omega = (1 + \sqrt{-3})/2$, as usual. Both $\theta_1^2$ and $\theta_2^2$ have norm $133 = 7 \cdot 19$ and Theorem 1 of [11] implies that $d_{L_1} = d_{L_2} = 3^2 \cdot 7 \cdot 19$. To satisfy the conditions of Theorem 1, we must have $C = 1$ and $A = \pm 11/2$. We may take $m = 1$ and the equation

$$N_{k/\mathbb{Q}}(z_3 + z_4\omega) = 1$$

has solutions $(z_3, z_4) = (\pm 1, 0), (0, \pm 1), (1, -1)$ and $(-1, 1)$. For each of these we have to solve (8), which becomes

$$-3z_3^2 = \pm 22 + \text{Tr}_{k/\mathbb{Q}}((z_3 + z_4\omega)^2 \theta_1^2)$$

(9) for $j = 1$ or 2. It is only here that the difference between $L_1$ and $L_2$ appears.

For $L_1$, (9) is

$$-3z_3^2 = \pm 22 + 22z_3^2 + 10z_3z_4 - 17z_4^2,$$

which has solutions $(z_2, z_3, z_4) = (0, \pm 1, 0), (\pm 3, 1, -1)$ and $(\pm 3, -1, 1)$. Testing these solutions with $z_1 = 0$ and $z_1 = 1$, we find that $z_1 = 1$ yields an integer in every case. Hence there are six integers representing the equivalence classes of power bases in $L_1$. However, they are themselves equivalent in pairs and we are left with three equivalence classes of integers giving rise to power bases. They may be taken as

$$x_{11} = \frac{1}{4}(1 + \theta_1),$$

$$x_{12} = \frac{1}{4}[(1 + 3\omega) + (1 - \omega) \theta_1],$$

and

$$x_{13} = \frac{1}{4}[(1 - 3\omega) + (1 - \omega) \theta_1].$$

For $L_2$, (8) says

$$-3z_3^2 = \pm 22 + 23z_3^2 + 20z_3z_4 - 13z_4^2,$$

which has no solutions. We conclude that $L_2$ does not have a power basis.

As has been indicated above, finding a complete set of representatives for the equivalence classes of integers which give rise to power bases in a
dihedral quartic field containing a real quadratic field requires more information than Theorem 1 alone provides. In order to give a concrete example of the problems which occur, we shall determine all integers which give rise to power bases in the field $L$ obtained by adjoining a square-root of the golden ratio to $k = \mathbb{Q}(\sqrt{5})$. We begin with some necessary preliminaries.

Let $\{F_n\}_{n \in \mathbb{Z}}$ and $\{L_n\}_{n \in \mathbb{Z}}$ be, respectively, the (extended) Fibonacci and Lucas sequences, which may be defined by Binet's formulae

\[
F_n = \frac{1}{\sqrt{5}} (\omega^n - (\omega^*)^n),
\]
\[
L_n = \text{Tr}_{k/\mathbb{Q}}(\omega^n),
\]
where $\omega = (1 + \sqrt{5})/2$ is the golden ratio.

**Lemma 2.** The only integer solutions to the equation $L_n = 5c^2 - 1$ are $(n, c) = (-1, 0), (3, \pm 1)$. The only integer solution to the equation $L_n = 5c^2 + 1$ is $(n, c) = (1, 0)$.

**Proof.** The method we use is inspired by that of [5] and relies on Cohn's determination of the Fibonacci squares in [2]. Cohn showed that the only squares in the Fibonacci sequence are $F_0 = 0, F_1 = F_2 = 1$ and $F_{12} = 144$. Since $F_{-m} = (-1)^m F_m$, it follows that the only indices, $n$, for which $F_n$ is plus or minus a square are $n = 0, \pm 1, \pm 2$ and $\pm 12$. If $(u, v)$ is an integer solution to the equation

\[
u^2 - 5c^2 = \pm 4, \tag{10}\]

then the standard theory of Pell's equation implies that

\[
\frac{u + v\sqrt{5}}{2} = \pm \omega^n = \pm \frac{L_n + F_n\sqrt{5}}{2}
\]
and so $F_n = \pm c^2$. Since $L_0 = 2, L_1 = 1, L_2 = 3, L_{12} = 322$ and $L_{-m} = (-1)^m L_m$, it follows that the only integer solutions to (10) are

\[(u, v) = (\pm 2, 0), \quad (\pm 1, \pm 1), \quad (\pm 3, \pm 1), \quad (\pm 322, \pm 12). \tag{11}\]

Now suppose that $L_n = 5c^2 \pm 1$. We have $L_n \equiv L_{n+4} \pmod{5}$ and, in addition to the values given above, $L_3 = 4$. Thus $n$ must be odd and we have the well-known relation

\[L_n^2 + 4 = 5F_n^2.\]
Factoring the left hand side of this equation in \( \mathbb{Z}[i] \) we get
\[
(5c^2 + 1 + 2i)(5c^2 + 1 - 2i) = 5F_n^2,
\]
which, since \( 5 = (1+2i)(1-2i) \), may be expressed as
\[
((1-2i)c^2 + 1)((1+2i)c^2 + 1) = F_n^2
\]
with the plus sign or
\[
((1+2i)c^2 - 1)((1-2i)c^2 - 1) = F_n^2
\]
with the minus sign. The greatest common divisor of the two factors on the left hand side of (12) divides \((1+i)^3\) and so we must have \((1-2i)c^2 + 1 = r(1+i)^r \beta^2\) where \( r = 0 \) or \( 1 \), \( s \geq 0 \) and \( \beta \in \mathbb{Z}[i] \) is relatively prime to \((1+i)\). Equation (12) then forces \( s \) to be even and so we have
\[
(1-2i)c^2 + 1 = (a + bi)^2
\]
or
\[
(1-2i)c^2 + 1 = i(a + bi)^2.
\]
Equation (15) leads to \((a+2b)^2 - 5b^2 = -2\), which is congruentially impossible modulo 4. Thus (14) holds and leads to
\[
c^2 = ab
\]
\[
c^2 + 1 = a^2 - b^2.
\]
Therefore \( a^2 - ab - b^2 = 1 \) and so \( a \) and \( b \) are relatively prime and (16) implies that \( b = \pm v^2 \) for some \( v \in \mathbb{Z} \). Making this substitution and completing the square we obtain \((2a-b)^2 - 5v^4 = 4\), so that (11) gives us all possible values for \((2a-b, v)\). Examining each possibility, we find that only \((a, b) = (\pm 1, 0)\) gives a solution to (16) and (17) and this solution has \( c = 0 \). This proves the second claim. We may analyze (13) similarly. It leads to \((a+2b)^2 - 5v^4 = -4\) and then to \( c = 0 \) or \( \pm 1 \). This establishes the first claim.

**Theorem 2.** Let \( L = \mathbb{Q}(\mathfrak{a}) \) where \( \mathfrak{a}^2 = (1 + \sqrt{5})/2 \). A complete set of representatives for the equivalence classes of integers in \( L \) giving rise to power bases is \( \{ \mathfrak{a}, -\mathfrak{a} + \mathfrak{a}^3, \mathfrak{a}^2 + \mathfrak{a}^3, -\mathfrak{a}^2 + \mathfrak{a}^3 \} \).

**Proof.** Using [11], we obtain \( d_L = -400 \) and so to satisfy the conditions of Theorem 1 we must have \( A = \pm 1 \) and \( C = \pm 4 \). Since \( \mathfrak{a} \) is square-free
indeed a unit) we may take $m = 1$. If $N_{\mathbb{Q}(2)}(z_3 + z_4 \omega) = \pm 4$ then $z_3 + z_4 \omega = \pm 2\omega^n$ for some $n \in \mathbb{Z}$. Thus $z_2$ must satisfy

$$5z_2^2 = \pm 4 + \text{Tr}_{\mathbb{Q}(4)}(4\omega^{2n+1})$$

$$= 4(\pm 1 + L_{2n+1})$$

and so $L_{2n+1} \pm 1$ must be five times a square. From Lemma 2, this implies that $n = -1$, 0 or 1. If $n = -1$ or 0 then $z_2 = 0$ and if $n = 1$ then $z_2 = \pm 2$. We may take $z_1 = 0$ in every case and we obtain the integers $\pm \omega^{-1}3$, $\pm 3$ and $\pm \omega \pm \omega 3$. Now $\omega^{-1} = \omega - 1$ and so, up to equivalence, we are left with $(\omega - 1)3 = -3 + 3^2$, $3\omega + \omega 3 = 3^2 + 3^3$ and $-3 + \omega 3 = -3^2 + 3^3$, as claimed.

Remarkably, all the integers found in Theorem 2 are units of $L$. This may be seen most easily by observing that

$$\mathcal{O}(3^2 + 3^3) = 1$$

and

$$(3^2 + 3^3)(-3^2 + 3^3) = \omega.$$