GENERIC POLYNOMIALS FOR QUASI-DIHEDRAL, DIHEDRAL
AND MODULAR EXTENSIONS OF ORDER 16

ARNE LEDET

(Communicated by David E. Rohrlich)

Abstract. We describe Galois extensions where the Galois group is the quasi-
dihedral, dihedral or modular group of order 16, and use this description to
produce generic polynomials.

Introduction

Let \( K \) be a field of characteristic \( \neq 2 \). Then every quadratic extension of \( K \)
has the form \( K(\sqrt{a})/K \) for some \( a \in K^* \). Similarly, every cyclic extension of
degree 4 has the form \( K(\sqrt{r(1 + c^2 + \sqrt{1 + c^2})})/K \) for suitable \( r, c \in K^* \). In other
words: A quadratic extension is the splitting field of a polynomial \( X^2 - a \), and a
\( C_4 \)-extension is the splitting field of a polynomial \( X^4 - 2r(1 + c^2)X^2 + r^2c^2(1 + c^2) \),
for suitably chosen \( a, c \) and \( r \) in \( K \). This makes the polynomials \( X^2 - t \) and
\( X^4 - 2t_1(1 + t_2^2)X^2 + t_1^2t_2^2(1 + t_2^2) \) generic according to the following

Definition. Let \( K \) be a field and \( G \) a finite group, and let \( t_1, \ldots, t_n \) and \( X \) be
indeterminates over \( K \). A polynomial \( F(t_1, \ldots, t_n, X) \in K(t_1, \ldots, t_n)[X] \) is called
a generic (or versal) polynomial for \( G \)-extensions over \( K \), if it has the following
properties:

(1) The splitting field of \( F(t_1, \ldots, t_n, X) \) over \( K(t_1, \ldots, t_n) \) is a \( G \)-extension.

(2) If \( L/K \) is a field extension, any \( G \)-extension of \( L \) is obtained as the splitting
field of \( F(a_1, \ldots, a_n, X) \) for suitable \( a_1, \ldots, a_n \in L \).

Generic polynomials (and the closely related generic Galois extensions; cf. [Sa])
are a convenient way of describing what \( G \)-extensions look like.

In this paper, we construct generic polynomials for the quasi-dihedral, dihedral
and modular group of order 16 over fields of characteristic \( \neq 2 \). Here, the quasi-
dihedral group of order 16 is the group \( QD_8 \) with generators \( u \) and \( v \) and relations
\( u^4 = v^2 \) and \( vu = u^3v \), the dihedral group of order 16 is the group \( D_8 \) with
generators \( \sigma \) and \( \tau \) and relations \( \sigma^8 = \tau^2 = 1 \) and \( \tau\sigma = \sigma^7\tau \), and the modular
group of order 16 is the group \( M_{16} \) with generators \( u \) and \( v \) and relations \( u^8 = v^2 = 1 \)
and \( vu = u^5v \).

Received by the editors September 8, 1998.
2000 Mathematics Subject Classification. Primary 12F12.
This work was supported by a Queen’s University Advisory Research Committee Postdoctoral
Fellowship.

©2000 American Mathematical Society
The approach is as follows: We start with a Galois extension $M/K$ of degree 8, where the Galois group $G = \text{Gal}(M/K)$ is a homomorphic image of the group $E (= \mathbb{QD}_8, D_8$ or $M_{16})$ we consider. This gives us a Galois theoretical embedding problem: Can we extend this $G$-extension to an $E$-extension? And if so, how? For the embedding problems we get, the criterion for solvability is that the crossed product algebra $(M, G, c)$ splits, where $c$ is a factor system representing the group extension

$$1 \to \mu_2 \to E \to G \to 1.$$ 

For a proof of this, see e.g. [Ki]. In all three cases, this algebra is a tensor product of two quaternion algebras and a matrix algebra, meaning that the criterion can be reformulated as an equivalence of quadratic forms. Details on how to find the obstruction can be found in [Le1], and the main reference for this paper is [Le2], where conditions in terms of quadratic forms are given, and solutions to the embedding problems are constructed. 

It should be pointed out that the obstructions to realising $\mathbb{QD}_8$ given in [Le1, Ex. 4.1] and in [Le2, 2.4] are not identical, since different maps $\mathbb{QD}_8 \to D_4$ are used. (The more natural map is the one used in [Le1], as well as in [Ki]. On the other hand, for constructing the solutions the map used in [Le2] is more convenient.) However, the obstruction in [Le2] can be obtained directly from [Le1, Prop. 4.2]. For the other two embedding problems, the obstructions in [Le1] and [Le2] are identical, although they have been rewritten slightly to accommodate the quadratic forms approach. This rewriting was done using $(a, -b) = 1$ (for $D_8$) and $(a, -1) = 1$ (for $M_{16}$). 

**Remark.** In [Bl, Thm. 4.6], Black proves the existence of generic $D_8$-extensions, although a generic polynomial is not explicitly constructed. Indeed, the idea of this paper—using the descriptions of $\mathbb{QD}_8$, $D_8$- and $M_{16}$-extensions given in [Le2] to produce generic polynomials—was directly inspired by Black’s result.

We let $D_4$ denote the dihedral group of order 8, i.e., the group with generators $\sigma$ and $\tau$ and relations $\sigma^4 = \tau^2 = 1$ and $\tau \sigma = \sigma^3 \tau$. Also, we assume all fields to have characteristic $\neq 2$. 

### The quasi-dihedral group 

Let $M/K$ be a $D_4$-extension. By [Ki, Thm. 5], we may assume

$$M = K(\sqrt{r(a + \sqrt{a})}, \sqrt{b}),$$

where $a$ and $b = a - 1$ in $K^*$ are quadratically independent, and $r \in K^*$ is arbitrary.\footnote{In [Ki], Kiming lists two kinds of $D_r$-extensions, the other being $K(\sqrt{a}, \sqrt{-1})/K$. However, the first kind, described above, covers everything.} Now, by [Le2, 2.4], $M/K$ can be embedded in a $\mathbb{QD}_8$-extension $F/K$, such that $F/K(\sqrt{b})$ is cyclic and $F/K(\sqrt{a\sqrt{b}})$ is dihedral, if and only if the quadratic forms $(b, 2ra, 2rab)$ and $(a, 2, 2a)$ are equivalent over $K$. Thus, the embedding problem is solvable for some $r \in K^*$, if and only if the quadratic form $(a, 2, 2a)$ represents $b$, i.e., if and only if

$$ax^2 + 2y^2 + 2az^2 = b = a - 1.$$
for suitable $x, y, z \in K$. Considering $y^2 + axz^2$ as a norm in the quadratic extension $K(\sqrt{-a})/K$ and multiplying $y + z\sqrt{-a}$ by a factor $(u + v\sqrt{-a})/(u - v\sqrt{-a})$, we see that we can replace $y$ and $z$ by

$$y' = \frac{(u^2 - av^2)y - 2avuz}{u^2 + av^2}, \quad z' = \frac{(u^2 - av^2)z + 2uvy}{u^2 + av^2}$$

for $u, v \in K$ with $u^2 + av^2 \neq 0$, if necessary. (The fact that $-a$ may be a square in $K$ does not change the validity of this substitution.) Thus, we may assume $1 - x^2 - 2z^2 \neq 0$ and get

$$a = \frac{1 + 2y^2}{1 - x^2 - 2z^2}.$$  

Choosing $u$ and $v$ properly, we may assume $ax^2 + 2y^2 \neq 0$ as well. Now,

$$Q'\langle a, 2, 2a \rangle Q = \langle b, 2a(ax^2 + 2y^2), 2ab(ax^2 + 2y^2) \rangle$$

for

$$Q = \begin{pmatrix} x & -2y & -2axz \\ y & ax & -2ayz \\ z & 0 & ax^2 + 2y^2 \end{pmatrix}.$$  

Also, $\det Q = b(ax^2 + 2y^2)$.

Thus, the embdanding problem is solvable for $r = ax^2 + 2y^2$. More generally, it is solvable whenever $\langle b, 2ra, 2rab \rangle \sim \langle b, 2a(ax^2 + 2y^2), 2ab(ax^2 + 2y^2) \rangle$. By the Witt Cancellation Theorem (see e.g. [Ja, 6.5 p. 367]) this is equivalent to $\langle 2a, 2rab \rangle \sim \langle 2a(ax^2 + 2y^2), 2ab(ax^2 + 2y^2) \rangle$, i.e., to $\langle r, rb \rangle \sim \langle ax^2 + 2y^2, 1, b \rangle$. Hence, we must have $r = (ax^2 + 2y^2)(p^2 + bq^2)$ for suitable $p, q \in K$. And since we can modify $r$ by a factor from $K^* \cap (K(\sqrt{a}, \sqrt{b}))^2$ without changing $M$, we can assume $p = 1$ and $r = (ax^2 + 2y^2)(1 + bq^2)$. Then

$$Q''(a, 2, 2a)Q' = \langle b, 2ra, 2rab \rangle$$

when

$$Q' = Q \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -bq \\ 0 & q & 1 \end{pmatrix} = \begin{pmatrix} x & -2y + axz & 2(bqy - axz) \\ y & a(x - 2qyz) & -a(bqx + 2yz) \\ z & (ax^2 + 2y^2)q & (ax^2 + 2y^2)q \end{pmatrix},$$

and $\det Q' = rb$.

The construction of $QD_s$-extensions in [Lec2 2.4] uses the matrix $P = Q'^{-1}$: If $P^t(b, 2ra, 2rab)P = \langle a, 2, 2a \rangle$ and $\det P = 1/rb$, the $QD_s$-extensions we seek are

$$K(\sqrt{s\omega}, \sqrt{a})/K, \quad s \in K^*,$$

where

$$\omega = 1 + p_{11}\sqrt{b}/\sqrt{a} + \frac{1}{2}p_{22} + p_{23}/\sqrt{a} - p_{32}\sqrt{b} + p_{33}\sqrt{b}/\sqrt{a}\sqrt{r(a + \sqrt{a})}$$

$$+ \frac{1}{2}p_{22} - p_{23}/\sqrt{a} + p_{32}\sqrt{b} + p_{33}\sqrt{b}/\sqrt{a}\sqrt{r(a + \sqrt{a})},$$

Moreover, $K(\sqrt{s\omega}, \sqrt{a})/K$ is the Galois closure of $K(\sqrt{s\omega})/K$.  


Fortunately, it is easy to invert \( Q' \):

\[
P = Q'^{-1} = \langle 1/b, 1/2ra, 1/2r^2b \rangle Q'' \langle a, 2, 2a \rangle
\]

\[
= \begin{pmatrix}
ax/b & 2y/b & 2az/b \\
-(y + axz)/r & (x - 2qyz)/r & (ax^2 + 2y^2)q/r \\
(bqy - axz)/rb & -(bqx + 2yz)/rb & (ax^2 + 2y^2)/rb
\end{pmatrix}.
\]

We now have

**Theorem 1.** \( QD_8 \)-extension has the form

\[
K(\sqrt{s\omega}, \sqrt{a})/K, \quad s \in K^*,
\]

where

\[
a = \frac{1 + 2y^2}{1 - x^2 - 2z^2}
\]

for suitable \( x, y, z \in K \), such that \( a \) and \( b = a-1 \) are well-defined and quadratically independent, \( ax^2 + 2y^2 \neq 0 \), and

\[
\omega = 1 + x\sqrt{a}/\sqrt{b}
\]

\[
+ \frac{1}{2r} \left[ x - 2qyz + g(ax^2 + 2y^2) + bqz + 2yz + \frac{ax^2 + 2y^2}{\sqrt{a}} \right] \sqrt{r(a + \sqrt{a})}
\]

\[
+ \frac{1}{2r} \left[ x - 2qyz - g(ax^2 + 2y^2) - bqz - 2yz + \frac{ax^2 + 2y^2}{\sqrt{a}} \right] \sqrt{a - 1} \sqrt{r(a + \sqrt{a})}
\]

for \( q \in K \), such that \( r = (ax^2 + 2y^2)(1 + bq^2) \neq 0 \).

In particular, we get a \( QD_8 \)-extension over \( K(x, y, z, q, s) \), when we consider \( x, y, z, q \) and \( s \) as indeterminates. This gives us our generic polynomial for \( QD_8 \)-extensions:

**Theorem 2.** Let \( x, y, z, q \) and \( s \) be indeterminates over the field \( K \). Then the polynomial

\[
F(x, y, z, q, s, T) = (T^2 - s)^4 + s^2c_2(T^2 - s)^2 + s^3c_1(T^2 - s) + s^4c_0
\]

in \( K(x, y, z, q, s, T) \) is a generic polynomial for \( QD_8 \)-extensions over \( K \), when

\[
a = \frac{1 + 2y^2}{1 - x^2 - 2z^2}, \quad b = a - 1, \quad r = (ax^2 + 2y^2)(1 + bq^2),
\]

\[
h = p_{23} + ap_{32} - p_{33}, \quad k = p_{22} - p_{32} + p_{33},
\]

\[
a = r(h^2 + ak^2 + 2hk)/4, \quad \beta = r(h^2 + ak^2 + 2ahk)/4a,
\]

\[
c_2 = -2(ax^2/b + 2\alpha), \quad c_1 = 2rx(p_{23} + ap_{32} - ap_{22} - bp_{33})
\]

\[
-2ap_{23}p_{33} + 2ap_{23}p_{32} - 2p_{23}p_{33} + 2ap_{22}p_{32}
\]

\[
c_0 = a^2x^4/b^2 + 2(\alpha^2 + a\beta^2) - 4ax^2\alpha/b - 2(\alpha^2 - a\beta^2)
\]

and the \( p_{ij} \)'s are the entries in the matrix \( P \) above. Specifically, \( QD_8 \)-extensions are obtained by specialisations such that \( a \) and \( b \) are well-defined and quadratically independent, and \( r \) and \( s \) are \( \neq 0 \).
We notice that the coefficients in degrees 0 and 2 are expressed in terms of $h$.

Calculations (performed in Maple V) show that

$$f(T) = T^4 + c_2 T^2 + c_1 T + c_0$$

is the minimal polynomial for $\omega - 1$, where $\omega$ is as in Theorem 1. It follows that $F(x, y, z, q, s, T)$ is the minimal polynomial for $\sqrt{s \omega}$.

Remark. A few observations about the calculation of $f(x, y, z, q, T)$ are in order:

Since $\theta = \omega - 1$ has degree 4 and is a primitive element for the $C_2 \times C_2$-extension $M/K(\sqrt{a})$, we are left with calculating minimal polynomials in $C_2 \times C_2$-extensions:

Let $L/k = k(\sqrt{A, B})/k$ be a $C_2 \times C_2$-extension, and let $\theta = a_1 \sqrt{A} + a_2 \sqrt{B} + a_3 \sqrt{A \sqrt{B}, a_1, a_2, a_3 \in k}$, have degree 4. Then the minimal polynomial for $\theta$ over $k$ is

$$f(T) = T^4 - 2(a_1^2 A + a_2^2 B + a_3^2 AB)T^2 - 8a_1a_2a_3ABT$$

$$+ (a_1^4 A^2 + a_2^4 B^2 + a_3^4 AB^2 - 2a_1^2 a_2^2 AB - 2a_2^2 a_3^2 AB^2).$$

We notice that the coefficients in degrees 0 and 2 are expressed in terms of $a_1' = a_1^2 A$, $a_2' = a_2^2 B$ and $a_3' = a_3^2 AB$.

In the case of Theorem 2, we have $L/k = M/K(\sqrt{a})$, $A = b$ and $B = r(a + \sqrt{a})$. Also,

$$a_1 = p_{11}/\sqrt{a},$$

$$a_2 = \frac{1}{2}(p_{22} + p_{23}/\sqrt{a})\sqrt{a - 1} + p_{33}(\sqrt{a - 1})/\sqrt{a},$$

and

$$a_3 = \frac{1}{2}(p_{22}/b - p_{23}/\sqrt{a})\sqrt{a - 1}/b\sqrt{a} - p_{32} + p_{33}/\sqrt{a}. $$

Calculations (performed in Maple V) show that $a_2' = r(1 + \sqrt{a})(h + k\sqrt{a})^2/4$ and $a_3'$ are conjugate in $K(\sqrt{a})/K$. This simplifies the expressions for $c_0$ and $c_2$.

The dihedral group

Again, we look at a $D_4$-extension $M = K(\sqrt{r(a + \sqrt{a}), \sqrt{b}})$, where $b = a - 1$. By [L62] 3.3, $M/K$ can be embedded in a $D_8$-extension $F/K$, such that $F/K(\sqrt{b})$ is cyclic, if and only if the quadratic forms $(b, ra, rab)$ and $(ab, 2a, 2b)$ are equivalent over $K$, and if $P$ is a $3 \times 3$ matrix over $K$ with $P^t(b, ra, rab)P = (ab, 2a, 2b)$ and $\det P = 2/r$, the $D_8$-extensions in question are

$$K(\sqrt{s \omega}, \sqrt{b})/K, \quad s \in K^*,$$

where

$$\omega = 1 - p_{11}/\sqrt{a}$$

$$+ \frac{1}{2}(p_{33} + p_{23}/\sqrt{a})\sqrt{r(a + \sqrt{a})} + \frac{1}{2}(p_{22}/b - p_{33}/\sqrt{a})(\sqrt{a - 1})\sqrt{r(a + \sqrt{a})}.$$

Also, $K(\sqrt{s \omega}, \sqrt{b})/K$ is the Galois closure of $K(\sqrt{s \omega})/K$.

The embedding problem is solvable for some $r \in K^*$ if and only if $(ab, 2a, 2b)$ represents $b$, i.e., if and only if the quadratic form $(ab, 2a, 2b, -b)$ is isotropic. Multiplying by $2ab$ and removing square factors, we see that this is equivalent to $(2, b, a, -2a)$ being isotropic, or to $(a, 2, -2a)$ representing $-b$:

$$ax^2 + 2y^2 - 2az^2 = -b = 1 - a$$
for suitable $x, y, z \in K$. We may assume $1 + x^2 - 2z^2 \neq 0$ and get

$$a = \frac{1 - 2y^2}{1 + x^2 - 2z^2}.$$ 

Modifying $y$ and $z$ properly, we may assume $z$ and $b + 2y^2$ to be non-zero as well. Now, returning to the first criterion given,

$$Q'(ab, 2a, 2b)Q = (b, a(b + 2y^2), ab(b + 2y^2))$$

for

$$Q = \begin{pmatrix} y/az & -1 & -xy/z \\ b/2az & y & -bx/2z \\ x/2z & 0 & (b + 2y^2)/2z \end{pmatrix},$$

Also, $\det Q = (b + 2y^2)/2$.

Thus, the embedding problem is solvable for $r = b + 2y^2$, and more generally whenever $\langle r, rb \rangle \sim (b + 2y^2, b(b + 2y^2))$. Hence, we must have $r = (b+2y^2)(p^2 + bq^2)$ for suitable $p, q \in K$. Again, we can assume $p = 1$ and thus $r = (b + 2y^2)(1 + bq^2)$. Then

$$Q'^t(ab, 2a, 2b)Q' = (b, ra, rab)$$

when

$$Q' = Q \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -bq \\ 0 & q & 1 \end{pmatrix} = \begin{pmatrix} y/az & -(z + qxy)/z & (bqz - xy)/z \\ b/2az & (2yz - bqz)/z & -(2qyz + x)b/2z \\ x/2z & (b + 2y^2)q/2z & (b + 2y^2)/2z \end{pmatrix},$$

and $\det Q' = r/2$.

We need to invert $Q'$, and again this is easy:

$$P = Q'^{-1} = (1/b, 1/ra, 1/rab)Q^t(ab, 2a, 2b)$$

$$= \begin{pmatrix} y/z & 1/z & x/z \\ -b(z + qxy)/rz & (2yz - bqz)/rz & (b + 2y^2)q/raz \\ (bqz - xy)/rz & -(x + 2qyz)/rz & (b + 2y^2)/raz \end{pmatrix}.$$ 

We now have

**Theorem 3.** A $D_s$-extension has the form

$$K(\sqrt{sw}, \sqrt{b})/K, \quad s \in K^*,$$

where

$$a = \frac{1 - 2y^2}{1 + x^2 - 2z^2}$$

for suitable $x, y, z \in K$, such that $a$ and $b = a - 1$ are well-defined and quadratically independent, $z$ and $b + 2y^2$ are non-zero, and

$$\omega = 1 - \frac{y}{z\sqrt{a}} - \frac{2ayz(1 + bq) + ab(1 - q)x + (b + 2y^2)b}{2rabz} \sqrt{r(a + \sqrt{a})}$$

$$+ b(b + 2y^2)(1 + bq) + a^2(2yz - bqz)}{2rabz\sqrt{a} \sqrt{r(a + \sqrt{a})}}$$

for $q \in K$, such that $r = (b + 2y^2)(1 + bq^2) \neq 0$.

Considering $x, y, z, q$ and $s$ as indeterminates, we get our generic polynomial for $D_s$-extensions:
Theorem 4. Let $x, y, z, q$ and $s$ be indeterminates over the field $K$. Then the polynomial

$$G(x, y, z, q, s, T) = (T^2 - s)^4 + s^2d_2(T^2 - s)^2 + s^3d_1(T^2 - s) + s^4d_0$$

in $K(x, y, z, q, s, T)$ is a generic polynomial for $D_8$-extensions, when

$$a = \frac{1 - 2y^2}{1 + 2z^2}, \quad b = a - 1, \quad r = (b + 2y^2)(1 + bq),$$

$$\alpha = -y/az, \quad \beta = -(2ayz(1 + bq) + ab(1 - q)x + (b + 2y^2)b)/2rabz,$$

$$\gamma = (b(b + 2y^2)(1 + bq) + a^2(2yz - bx))/(2ra^2b),$$

$$d_2 = -2a(\alpha^2 + r\beta^2 + ra\gamma^2 + 2r\beta\gamma),$$

$$d_1 = -4raa(\alpha^2 + 2a\beta^2 + 2a\gamma^2) \quad \text{and}$$

$$d_0 = a(\alpha^4 + r^2\beta^4 + r^2a^2\gamma^4 - 2r\alpha^2\beta^2 - 2r^2a^2\beta^2 - 2r^2a^2\gamma^2)$$

$$-2r^2ab\beta^2\gamma^2 + 2r^2a^3\gamma - 4ra^2\beta\gamma).$$

Specifically, $D_8$-extensions are obtained by specialisations such that $a$ and $b$ are well-defined and quadratically independent, and $r$ and $s$ are $\neq 0$.

Proof. $g(x, y, z, q, T) = T^4 + d_2T^2 + d_1T + d_0$ is the minimal polynomial for $\omega - 1$, where $\omega$ is as in Theorem 3.

Remark. If $L/k = k(\sqrt{r(a + \sqrt{a})})$ is a $C_4$-extension, the minimal polynomial for an element

$$\theta = \alpha\sqrt{a} + \beta\sqrt{r(a + \sqrt{a})} + \gamma\sqrt{a}\sqrt{r(a + \sqrt{a})} \in M$$

degree 4 is

$$f(T) = T^4 - 2a(\alpha^2 + r\beta^2 + ra\gamma^2 + 2r\beta\gamma)T^2$$

$$-4raa(\beta^2 + a\gamma^2 + 2a\beta\gamma)T + a(\alpha^2 + r^2\beta^4 + 2r^2\beta^2\gamma^4 + 2r^2\beta^2\gamma^2 + 2r^2a\beta^2\gamma^2 - 4ra\beta\gamma).$$

In the case of Theorem 4, our $C_4$-extension is $L/k = M/K(\sqrt{b})$, and we let $\theta = \omega - 1$ and $c = \sqrt{b}$. This gives us the minimal polynomial for $\omega - 1$ over $K(\sqrt{b})$, and since $c = \sqrt{b}$ only occurs to the second power, the polynomial is in fact the minimal polynomial over $K$. Computing the minimal polynomial for $s\omega$ over $K$ is then trivial.

The modular group

Let $M/K$ be a $C_4 \times C_2$-extension. It is well-known that $C_4$-extensions have the form $K(\sqrt{r(a + \sqrt{a})})/K$, where $a = 1 + c^2, c \in K^*$, is not a square, and $r \in K^*$ is arbitrary. Thus, we can write $M = K(\sqrt{r(a + \sqrt{a}), \sqrt{b}})$, where $a = 1 + c^2$ and $b \in K^*$ in $K^*$ are quadratically independent, and $r \in K^*$.

By $[Le2] 3.5$, $M/K$ can be embedded in an $M_{16}$-extension $F/K$, such that $F/K(\sqrt{a})$ is not cyclic, if and only if the quadratic forms $\langle 1, 2rab, 2rab \rangle$ and $\langle a, 2b, 2ab \rangle$ are equivalent over $K$. So, in order for the embedding problem to
be solvable for some $r \in K^*$, it is necessary and sufficient that the quadratic form $\langle a, 2b, 2ab \rangle$ represents 1, i.e.,

$$ax^2 + 2by^2 + 2abz^2 = 1$$

for suitable $x, y, z \in K$. We must have $y^2 + az^2 \neq 0$, since otherwise $ax^2 = 1$, and so

$$b = \frac{1 - ax^2}{2(y^2 + az^2)}.$$  

Modifying $y$ and $z$ if necessary, we may assume $z$ and $ax^2 + 2b(y/z)^2$ to be non-zero, and replacing $b$ by $bz^2$, $y$ by $y/z$ and $z$ by 1, we get

$$b = \frac{1 - ax^2}{2(y^2 + a)}$$

and $ax^2 + 2by^2 \neq 0$. Now,

$$Q'(a, 2b, 2ab)Q = \langle 1, 2ab(ax^2 + 2by^2), 2ab(ax^2 + 2by^2) \rangle$$

for

$$Q = \begin{pmatrix} x & -2by & -2abx \\ y & ax & -2aby \\ 1 & 0 & ax^2 + 2by^2 \end{pmatrix}$$

and $\det Q = ax^2 + 2by^2$.

Thus, the embedding problem is solvable for $r = ax^2 + 2by^2$, and more generally for $r = (ax^2 + 2by^2)(p^2 + q^2)$ for $p, q \in K$ with $p^2 + q^2 \neq 0$. We can assume $p = 1$ and $r = (ax^2 + 2by^2)(1 + q^2)$. Then

$$Q''(a, 2b, 2ab)Q' = \langle 1, 2rab, 2rab \rangle$$

when

$$Q' = Q \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -q \\ 0 & q & 1 \end{pmatrix} = \begin{pmatrix} x & -2b(y + ax) & 2b(qy - ax) \\ y & a(x - 2by) & -a(qx + 2by) \\ 1 & (ax^2 + 2by^2)q & ax^2 + 2by^2 \end{pmatrix},$$

and $\det Q' = r$.

Using [3, 3.5], we get the $M_{16}$-extensions

$$K(\sqrt{s \omega}, \sqrt{\omega})/K, \quad s \in K^*,$$

where

$$\omega = 1 + p_{11}/\sqrt{a} + \frac{1}{2}[p_{22} + p_{23}/\sqrt{a} - p_{32} + p_{33}/\sqrt{a}]\sqrt{r(a + \sqrt{a})}$$

$$+ \frac{1}{2}[p_{22} - p_{23}/\sqrt{a} + p_{32} + p_{33}/\sqrt{a}]\sqrt{\frac{a - 1}{c}}\sqrt{r(a + \sqrt{a})},$$

where

$$P = Q'^{-1} = \langle 1, 1/2rab, 1/2rab \rangle Q''(a, 2b, 2ab)$$

$$= \begin{pmatrix} ax & 2by & 2ab \\ -(y + ax)/r & (x - 2by)/r & (ax^2 + 2by^2)q/r \\ (qy - ax)/r & -(qx + 2by)/r & (ax^2 + 2by^2)/r \end{pmatrix}.$$  

Also, $K(\sqrt{s \omega}, \sqrt{b})/K$ is the Galois closure of $K(\sqrt{s \omega})/K$.  

Theorem 5. An \( M_{16} \)-extension has the form
\[
K(\sqrt{s\omega}, \sqrt{b})/K, \quad s \in K^*,
\]
where
\[
b = \frac{1 - ax^2}{2(y^2 + a)}
\]
for suitable \( c, x, y \in K \), such that \( a = 1 + c^2 \) and \( b \) are well-defined and quadratically independent, \( ax^2 + 2by^2 \neq 0 \), and
\[
\omega = 1 + x\sqrt{a}
\]
\[
+ \frac{1}{2r} \left[ (x(1 + q) + 2by(1 - q) + \frac{(ax^2 + 2by^2)(1 + q)}{\sqrt{a}}) \sqrt{r(a + \sqrt{a})} \right.
\]
\[
+ \frac{1}{2r} \left[ (x(1 - q) - 2by(1 + q) + \frac{(ax^2 + 2by^2)(1 - q)}{\sqrt{a}}) \sqrt{\frac{a - 1}{c} \sqrt{r(a + \sqrt{a})}} \right]
\]
for \( q \in K \), such that \( r = (ax^2 + 2by^2)(1 + q^2) \neq 0 \).

Treating \( c, x, y, q \) and \( s \) as indeterminates, we then have

Theorem 6. Let \( c, x, y, q \) and \( s \) be indeterminates over the field \( K \). Then the polynomial
\[
H(c, x, y, q, s, T) = (T^2 - s)^4 + e_2(T^2 - s)^2 + e_1(T^2 - s) + e_0
\]
in \( K(c, x, y, q, s, T) \) is a generic polynomial for \( M_{16} \)-extensions, when
\[
a = 1 + c^2, \quad b = \frac{1 - ax^2}{2(y^2 + a)}, \quad r = (ax^2 + 2by^2)(1 + q^2),
\]
\[
\beta = ((cx + 2by)(1 + q) + (ax^2 + 2by^2 + 2bcy - x)(1 - q))/2rc,
\]
\[
\gamma = ((acx^2 + 2bcy^2 - 2aby)(1 + q) + (ax(1 - x) - 2by^2)(1 - q))/2rac,
\]
\[
e_2 = -2a(x^2 + r\beta^2 + r\alpha^2 + 2r\beta\gamma),
\]
\[
e_1 = -4rax(3\beta^2 + 2r\alpha^2 + 2a\beta\gamma) \quad \text{and}
\]
\[
e_0 = a(ax^4 + r^2b\beta^4 + r^2a^2\beta^4 - 2rax^2\beta^2 - 2ra^2x^2\gamma^2
\]
\[
-2r^2ab\beta^2\gamma^2 + 2r^2a\beta^3\gamma - 4r^2x^2\beta\gamma).
\]

Specifically, \( M_{16} \)-extensions are obtained by specialisations such that \( a \) and \( b \) are well-defined and quadratically independent, and \( r \) and \( s \) are \( \neq 0 \).

Proof. \( h(c, x, y, q, T) = T^4 + e_2T^2 + e_1T + e_0 \) is the minimal polynomial for \( \omega - 1 \), where \( \omega \) is as in Theorem 5. \( \square \)

Remark. In [Le2], a description of \( C_8 \)-extensions is produced from the description of \( QD_{21} \)-extensions by, essentially, letting \( b \) be a square. However, Saltman proves in [Sa, Thm. 5.11] that there is no generic \( C_8 \)-extension over the rational numbers, and—by implication—no generic polynomial for \( C_8 \)-extensions in that case either. The reason the construction of generic polynomials works for \( QD_{5} \), \( D_{8} \) and \( M_{16} \), but not for \( C_8 \), is the extra degree of freedom obtained by introducing \( b \): If we try to carry through the calculations for \( C_8 \), we get a condition of the type \( a - 1 = (1 + 2y^2)/(1 - x^2 - 2z^2) - 1 = c^2 \), and it is not clear how to ensure that \( a - 1 \) is a
square, while at the same time getting enough $a$’s. (Indeed, by Saltman’s result it is impossible.) Thus, paradoxically, the larger groups $QD_8$, $D_8$ and $M_{16}$ are easier to handle than the smaller group $C_8$.

References


Department of Mathematics and Statistics, Queen’s University, Kingston, Ontario, Canada K7L 3N6

E-mail address: ledet@math.queensu.ca