When Is the Clifford Algebra of a Binary Cubic Form Split?

DARRELL E. HAILE

Department of Mathematics, Indiana University,
Bloomington, Indiana 47405

Communicated by Susan Montgomery

Received March 13, 1990

Let \( f(u, v) \) be a nondegenerate binary form over a field \( F \) of characteristic not two or three. We prove that the Clifford algebra of \( f(u, v) \) over \( F \) is split if and only if the ternary form \( w^3 - f(u, v) \) has a nontrivial \( F \)-rational point.

1. INTRODUCTION

Let \( F \) be a field and let \( f \) be a form of degree \( n \) in \( m \) variables over \( F \). The Clifford algebra of \( f \) over \( F \) is defined to be the algebra \( C_f = F(x_1, x_2, \ldots, x_m)/I \), where \( F(x_1, x_2, \ldots, x_m) \) is the free \( F \)-algebra in \( m \) variables and \( I \) is the ideal generated by

\[
\{(\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_m x_m)^n - f(\alpha_1, \alpha_2, \ldots, \alpha_m) | \alpha_1, \alpha_2, \ldots, \alpha_m \in F\}.
\]

If \( n = 2 \) then this is the classical Clifford algebra of a quadratic form. For forms of higher degree the algebra has been studied by Childs [2], Revoy [7], and Roby [8], among others.

In this paper we are interested in the case of a binary cubic form. This case has been studied in Heerema [6] and Haile [4, 5]. Assume \( F \) is a field of characteristic not two or three and let \( f(u, v) \) be a nondegenerate binary cubic form over \( F \). It was shown in [4] that \( C_f \) is an Azumaya algebra of rank nine over its center and its center is the affine ring of a certain elliptic curve (depending on \( f \)—the center was also determined in some special cases by Heerema in [6]). It should be recalled that for binary quadratic forms there is an analogous result, namely the Clifford algebra of a binary quadratic over \( F \) is an Azumaya algebra of rank four over its center. Of course in that case the center is the field \( F \) itself and so the Clifford algebra is a central simple \( F \)-algebra of degree two, that is, a quaternion algebra.
An Azumaya algebra over a commutative ring $R$ is said to be \textit{split} if there is a finitely generated, projective $R$-module $P$ such that $A$ is isomorphic as an $R$-algebra to $\text{End}_R(P)$. In fact one can introduce an equivalence relation on Azumaya algebras over $R$ for which the classes have a natural group structure (the Brauer group of $R$) and for which the split algebras form a single class, the identity of the group $[1]$. It is natural to ask for conditions on the binary cubic form $f(u, v)$ that determine whether or not the Clifford algebra $C_2$ is split. Again in the case of a binary quadratic form such a condition is well known. In that case the Clifford algebra is split (that is, isomorphic to $M_2(F)$, the ring of $2 \times 2$ matrices over $F$) if and only if there are elements $\alpha, \beta \in F$ such that $f(\alpha, \beta) = 1$. Because a quadratic form that has a nontrivial zero necessarily represents every element of the field, it is easy to see that the condition on $f$ is equivalent to requiring that the ternary quadratic form $w^2 - f(u, v)$ represent 0 nontrivially over $F$, that is, have a nontrivial $F$-rational point.

We can now state the main result.

**Theorem.** Let $f(u, v)$ be a nondegenerate binary cubic form over a field $F$ of characteristic not two or three. The Clifford algebra $C_2$ of $f$ over $F$ is a split algebra if and only if the ternary form $w^3 - f(u, v)$ has a nontrivial $F$-rational point.

We will prove this theorem in the next section. In the third section we give two applications to explicit examples.

### 2. Proof of Main Theorem

We proceed to the proof of the theorem. Let $f(u, v) = a_1 u^3 + a_2 u^2 v + a_3 u v^2 + a_4 v^3$. As we stated above $C_2 = F[x, y] / I$, where $I$ is the ideal generated by the elements $(ax + by)^3 - f(\alpha, \beta)$ for all $\alpha, \beta \in F$. It is shown in [4] that $I$ is a finitely generated ideal, generated by the following four elements:

\[
\begin{align*}
x^3 - a_1 \\
x^2 y + xy x + y x^2 - a_2 \\
y^2 x + y x y + x y^2 - a_3 \\
y^3 - a_4.
\end{align*}
\]

Let $Z$ denote the center of $C_2$. As we noted above $C_2$ is Azumaya of rank nine over $Z$. Moreover $Z$ is the affine ring of the elliptic curve given by the equation $S^3 = R^3 - 27D$, where $D$ is the discriminant of $f$ [4]. In particular $Z$ is a Dedekind domain. Let $L$ denote the field of fractions of $Z$ and let $\Sigma_2 = C_2 \otimes_Z L$. The algebra $\Sigma_2$ is a central simple $L$-algebra of degree three.
Because $Z$ is Dedekind, the canonical homomorphism of Brauer groups $B(Z) \to B(L)$ is injective [1]. Hence $C_f$ is split if and only if $\Sigma_f$ is split, that is if and only if $\Sigma_f \cong M_3(L)$.

Now assume that that form $w^3 - f(u, v)$ has a nontrivial $F$-rational point. It follows easily that either the form $f(u, v)$ represents 1 in $F$ or $f(u, v)$ represents 0 nontrivially in $F$. If there exist $\alpha, \beta \in F$ such that $f(\alpha, \beta) = 1$, then $(\alpha x + \beta y)^3 = 1$. But $\alpha x + \beta y \notin Z$: If $\alpha x + \beta y \in Z$ then it follows that $xy = yx$, so $C_f$ is commutative. But it is easy to see that this contradicts the relations given above (because $f$ is assumed nondegenerate). Hence $ax + \beta y \in \Sigma_f$ is a noncentral cube root of one. Letting $t = ax + \beta y$ we see that $(t - 1)(t^2 + t + 1) = 0$. If $\Sigma_f$ is a division algebra, then, because $t$ is not in $F$, we infer that $t^2 + t + 1 = 0$. Hence either $t$ satisfies a linear polynomial over $F$, contradicting the fact that $t \notin F$, or the minimal polynomial of $t$ over $F$ is of degree 2, contradicting the fact that $\Sigma_f$ has degree three over $F$. Hence $\Sigma_f$ is not a division algebra and so must be split. Hence $C_f$ is split. Similarly if $f$ represents zero nontrivially then $C_f$ contains a nonzero nilpotent element. It follows that $\Sigma_f$ contains a nonzero nilpotent element. Thus $\Sigma_f$, and so $C_f$, is split.

We now proceed to the converse. We consider first the special case in which $f(u, v)$ is diagonal and $F$ contains a primitive third root of one, $\omega$. Let $f(u, v) = au^3 + bv^3$, where $a, b \in F$. In this case $D = -a^2b^2/4$ and $-27$ is a square in $F$, so the center $Z$ is given by the equation $S^2 = R^3 + d^2$, where $d = ab/2$. This affine curve is an affine piece of the elliptic curve $E$ given by the cubic form $S^2T - R^3 - d^2T$. The field of fractions $L$ is the function field $F(E)$ of $E$ over $F$. It is shown in [4] that if we let $\mu = yx - \omega xy$ in $C_f$, then $\mu^3 = S + d$ (so in particular $\mu^3 \in Z$) and $\mu x = \omega xy \mu$. Hence the central simple $F(E)$-algebra $\Sigma_f$ is the symbol algebra $(a, S + d)_{F(E),\omega}$.

Now assume $C_f$ is split. Let $K = F(\alpha)$, where $\alpha^3 = a$. If $\alpha \in F$ then the form $w^3 - au^3 - bv^3$ has a nontrivial rational point. Hence we may assume $\alpha \notin F$. Then $K/F$ is a Galois extension and $G = \text{Gal}(K/F)$ is cyclic of order three. Let $K(E)$ denote the function field of $E$ over $K$. Let $P(E_K)$, $\text{Div}(E_K)$, and $\text{Pic}(E_K)$ denote the group of principal divisors on $E_K$, the group of divisors on $E_K$, and the Picard group of $E_K$, respectively. The group $G$ acts on all of these objects in the obvious ways and we have the following short exact sequences of $G$-modules (see [9]):

$$0 \to K^\times \to K(E)^\times \to P(E_K) \to 0$$
$$0 \to P(E_K) \to \text{Div}(E_K) \to \text{Pic}(E_K) \to 0$$
$$0 \to \text{Pic}_0(E_K) \to \text{Pic}(E_K) \to Z \to 0.$$
norm map, $\sigma$ is a generator for $G$, $B_N = \{b \in B | N(b) = 0\}$, $B^{1-\sigma} = \{b - \sigma(b) | b \in B\}$, and $B^G$ is the subgroup of elements fixed by $G$. Looking at the long exact sequences in cohomology associated with the sequences above we obtain the following diagram with exact rows and columns:

$$
0 \rightarrow H^1(G, \text{Pic}_0(E_K)) \rightarrow H^1(G, \text{Pic}(E_K)) \rightarrow 0
$$

$$
H^2(G, K^\times) \rightarrow H^2(G, K(E)^\times) \rightarrow H^2(G, P(E_K)) \rightarrow 0
$$

$$
H^2(G, \text{Div}(E_K)).
$$

The exactness of the column follows from the fact that $H^1(G, \text{Div}(E_K)) = 0$. The surjectivity of $\gamma$ follows from the fact that $H^1(G, \mathbb{Z}) = 0$. The injectivity follows from the observation that the map $H^0(G, \text{Pic}(E_K)) \rightarrow H^0(G, \mathbb{Z})$ is surjective because $E$ has an $F$-rational point (at infinity, for example). Finally because $G$ is cyclic we have $H^3(G, K^\times) = H^1(G, K^\times)$ and this latter group is trivial by Hilbert’s Theorem 90. This demonstrates the exactness of the second row.

The group $H^2(G, K(E)^\times)$ is the relative Brauer group $B(K(E)/F(E))$ and contains the class of the symbol algebra $\Sigma_f$. In fact, $H^2(G, K(E)^\times) = F(E)^\times / N(K(E)^\times)$ and the class of $\Sigma_f$ corresponds to the coset $\mu^3[N(K(E))^\times]$. The image of this coset in $H^2(G, P(E_K)) = P(E_K)/N(P(E_K))$ is the coset of the principal divisor $(\mu^3)$, which we now compute: a straightforward computation shows that the ideal $(\mu^3)$ in $F[R, S]$ is the cube of the maximal ideal $(R, S + d)$. Hence the divisor determined by the function $\mu^3$ is $3\mathcal{P} - 3\infty$, where $\mathcal{P}$ is the divisor corresponding to the maximal ideal $(R, S + d)$ and $\infty$ denotes the point at infinity.

Now consider the divisor class of $\mathcal{P} - \infty$ in $\text{Pic}_0(E_K)$, where we are using $\mathcal{P}$ to denote the maximal ideal generated by $R$ and $S + d$ in both $F[R, S]$ and $K[R, S]$. Because both $\mathcal{P}$ and $\infty$ are fixed by $G$, we see that $N(\mathcal{P} - \infty) = 3(\mathcal{P} - \infty)$, which as we have seen is the principal divisor $(\mu^3)$ and so lies in the trivial class. Hence the divisor class of $\mathcal{P} - \infty$ lies in $H^1(G, \text{Pic}_0(E_K)) = [\text{Pic}_0(E_K)] / [\text{Pic}_0(E_K)]^{1-\sigma}$. The image of this element under $\rho$ is the coset $(\mathcal{P} - \infty)[\text{Pic}(E_K)]^{1-\sigma}$ and in turn the image of this coset via the connecting homomorphism $\delta$ is the coset $3(\mathcal{P} - \infty)[N(\text{Div}(E_K))]$. Hence we see that $\rho(\Sigma_f) = 3\gamma(\mathcal{P} - \infty)$.

Recall that we are assuming $C_f$ is split. Hence $\Sigma_f$ is split and so represents the trivial class in $H^2(G, K(E)^\times)$. Thus $0 = \rho(\Sigma_f) = 3\gamma(\mathcal{P} - \infty)$. 

481/146/9.18
But the map $\delta_\gamma$ is injective, so we infer that the class of $P - \infty$ in $H^1(G, \text{Pic}_0(E_K))$ is trivial. Because $E$ is an elliptic curve, we have $\text{Pic}_0(E_K) \cong E(K)$, the group of $K$-rational points, where the map sends any point $P$ in $E(K)$ to the class of the divisor $P - \infty$. Hence $H^1(G, \text{Pic}_0(E_K)) \cong H^1(G, E(K))$ and under this isomorphism the class of $P - \infty$ corresponds to the point $P$, that is to the point $(0, -d, 1)$ on $E$, where we are writing the variables in the order $R, S, T$.

The group $H^1(G, E(K))$ is a piece of the Weil–Chatelet group of the elliptic curve $E$ over $F$. Each element corresponds to a curve which is a homogeneous space for $E$. The element is trivial if and only if the corresponding curve has an $F$-rational point (see [11, Chap. 10] for the basic properties of the Weil–Chatelet group). We claim that the curve corresponding to the point $(0, -d, 1)$ is the curve given by the equation $w^3 - au^3 - bv^3$. If so then $C_f$ being split implies that this curve has a rational point, so we are done.

To prove our claim we follow the recipe of part (c) of [11, Chap. 10, Theorem 2.2]. The point $(0, -d, 1)$ has order three in $E(K)$. There is an action of $\mathbb{Z}_3$ on the function field $K(R, S)$ obtained by using the Galois action on $K$ and translation by the point $(0, -d)$: More precisely if the point $(r, s)$ lies on $E$ then one computes that $(r, s) + (0, -d) = [2dr/(s - d), d - 2d(s + d)/(s - d)]$. Hence the action of $\mathbb{Z}_3$ on $K(R, S)$ is given by sending the rational function $g(R, S)$ to $g^2([2dR/(S - d), d - 2d(S + d)/(S - d)])$. The function field of the homogeneous space corresponding to $(0, -d, 1)$ is precisely the fixed field of this action.

Let $\eta = 2\omega + 1$. Then $\eta^2 = -3$. Assume $\sigma(x) = \omega x$. It is then routine to check that the elements $B = \alpha(S + \eta d)/R$ and $D = \alpha^2(S - \eta d)/R$ are fixed under this action. It follows easily that the fixed field is $F(B, D)$. But $a^{-1}B^3 - a^{-2}D^3 = 6\eta d = 3\eta ab$ and $3\eta = (-\eta)^3$ is a cube in $F$. Hence $a(B/D)^3 + b(\eta aD^{-1})^3 = 1$, that is the fixed field is the function field of the curve $w^3 - au^3 - bv^3$, as desired.

We now do the general case. Let $f(u, v)$ be a nondegenerate binary cubic form. Let $H$ denote the projective curve given by the equation $w^3 - f(u, v)$. Let $D$ denote the discriminant of $f$. The curve $H$ is a homogeneous space for its Jacobian $J(H)$ which is an elliptic curve over $F$ ([11, Chap. 10]; in fact, $J(H)$ is given by the equation $S^2T = R^3 - 27DT^3$ which determines the center of $C_f$, but we will not use this fact). The period of $H$ is its order in $H^1(G(\overline{F}/F), J(H))$, where $\overline{F}$ is the algebraic closure of $F$ [11, p. 321]. Applying the usual restriction–corestriction relation for group cohomology, one sees that if $L/F$ is a finite extension such that $H$ has an $L$-rational point, then the period of $H$ divides $[L : F]$.

We will show $H$ has period one. By [11, Chap. 10, Proposition 3.3], it will follow that $H$ has an $F$-rational point, as desired. First let $L$ be the field
extension of \( F \) obtained by adjoining \( \omega \) and \( \sqrt{D} \) to \( F \). Then \([L : F]\) divides four. The algebra \( C_f \otimes_F L \) is the Clifford algebra of \( f \) viewed as a form over \( L \). Now over \( L \) the form \( f \) can be diagonalized \([3, \text{p. 17}]\). Because equivalent forms have isomorphic Clifford algebras and \( C_f \) is split, we infer from the first part of the proof that \( w^3 - f(u, v) \) has an \( L \)-rational point. Thus the period of \( H \) divides four.

Next consider the polynomial \( g(\lambda) = f(\lambda, 1) \). If \( g(\lambda) \) is reducible over \( F \) then \( g(\lambda) \) has a root \( \alpha \) in \( F \). In that case \( u = \alpha, v = 1, w = 0 \) is a nontrivial \( F \)-rational point on \( H \). Hence we may assume \( g(\lambda) \) is irreducible. Let \( K \) be the field obtained by adjoining a root of \( g(\lambda) \) to \( F \). Then \([K : F] = 3\) and the argument we just gave shows that \( H \) has a \( K \)-rational point. Hence the period of \( H \) divides three.

We conclude that the period of \( H \) is one, and so \( H \) has an \( F \)-rational point.

3. Applications

We give two applications of this criterion to explicit examples. Both are examples of forms for which the Clifford algebra is nonsplit but every simple homomorphic image of the Clifford algebra is split. For the first consider the form \( f(u, v) = xu^3 + x^2v^3 \) over the rational function field \( \mathbb{C}(x) \). It is an easy exercise to see that the form \( w^3 - xu^3 - x^2v^3 \) has no \( \mathbb{C}(x) \)-rational point. Hence by the theorem \( C_f \) is not split and so \( \Sigma_f \) is a division algebra. We have seen that in this case the algebra \( \Sigma_f \) is the symbol algebra \( (x, S + (x^3/2))_{\mathbb{C}(x)(E), w^3} \), where \( E \) is the elliptic curve with equation \( S^2 = R^3 - x^6/4 \). However, every simple homomorphic image of \( C_f \) has center a finite extension of \( \mathbb{C}(x) \) \([4]\) and so is split by Tsen's theorem \([12]\).

The second example displays the same phenomenon, now over \( \mathbb{Q} \). Let \( f(u, v) = (4/3)u^3 + (5/3)v^3 \). It has been shown by Selmer \([10]\) that the curve \( w^3 - (4/3)u^3 + (5/3)v^3 \) has point locally everywhere but has no point over \( \mathbb{Q} \). By the theorem the Clifford algebra \( C_f \) is not split. The center is given by \( S^2 = R^3 - 100/3 \). Let \( A \) be a simple homomorphic image of \( C_f \). The center of \( A \) will be a finite extension \( K \) of \( \mathbb{Q} \). For each prime \( P \) of \( K \), the algebra \( A_P = A \otimes_K K_P \) is a homomorphic image of the Clifford algebra of the form \( f \) viewed over the local field \( \mathbb{Q}_P \cap \mathbb{Q} \). Because \( w^3 - (4/3)u^3 + (5/3)v^3 \) has local points everywhere, we see that \( A_P \) is split for all primes \( P \) of \( K \). By the Hasse principle we infer that \( A \) is also split. Hence every simple homomorphic image of \( C_f \) is split.
REFERENCES