Journal of Algebra 330 (2011) 86–102

Contents lists available at ScienceDirect

Journal of Algebra

www.elsevier.com/locate/jalgebra

On an algebra associated to a ternary cubic curve

Jung-Miao Kuo

Department of Applied Mathematics, National Chung Hsing University, Taichung, Taiwan

ARTICLE INFO

Article history:
Received 19 November 2008
Available online 1 February 2011
Communicated by Eva Bayer-Fluckiger

Keywords:
Clifford algebras
Azumaya algebras
Brauer groups
Cubic curves

ABSTRACT

In this paper we construct an algebra associated to a cubic curve C defined over a field F of characteristic not two or three. We prove that this algebra is an Azumaya algebra of rank nine. Its center is the affine coordinate ring of an elliptic curve, the Jacobian of the cubic curve C. The induced function from the group of F-rational points on the Jacobian into the Brauer group of F is a group homomorphism with image precisely the relative Brauer group of classes of central simple F-algebras split by the function field of C. We also prove that this algebra is split if and only if the cubic curve C has an F-rational point. These results generalize Haile's work on the Clifford algebra of a binary cubic form.

1. Introduction

Let f be a form of degree d in n indeterminates over a field F, and let $F\{x_1,\ldots,x_n\}$ be the free associative F-algebra in n indeterminates. The Clifford algebra A_f (usually denoted by C_f) of f is the F-algebra $A_f = F\{x_1,\ldots,x_n\}/I$, where I is the ideal generated by the relations defined by the formal identity $(\alpha_1x_1+\cdots+\alpha_nx_n)^d = f(\alpha_1,\ldots,\alpha_n)$ in the α_i. If $d=2$, this is the classical Clifford algebra of a quadratic form. If $d>2$, this is the generalized Clifford algebra and has been studied by various authors, including Heerema [10], Roby [15] and Childs [2]. Revoy [14], using results of Roby [15], exhibited an explicit F-basis for the Clifford algebra of an arbitrary form. Using this basis it is easy to see that if $d>3$ or $d=3$ and $n>2$, then the Clifford algebra contains a free F-algebra on two indeterminates. In particular, the algebra is not finitely generated over its center and hence is not Azumaya.

Haile [6] proved that if the characteristic of F is not two or three and f is a non-degenerate binary cubic form ($n=2$, $d=3$), then the Clifford algebra of f is an Azumaya algebra of rank 9 over its center, which, in turn, is the affine coordinate ring of the elliptic curve E_0 given by the Weierstrass equation $s^2=r^3-27D_f$, where D_f is the discriminant of f. The elliptic curve E_0 is in fact

E-mail address: jmkuo@amath.nchu.edu.tw.

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2010.12.021

the Jacobian of the cubic curve C_0 given by the equation $z^3 - f(x, y) = 0$. Kulkarni [11] generalized this result to binary forms f $(n = 2)$ of higher degree $d > 3$, describing the center of the Azumaya algebra $\tilde{A_f} = A_f/(\bigcap \ker \eta)$, where the intersection is taken over all the kernels of representations of dimension d, as the coordinate ring of an affine open set in the Jacobian of the projective curve $\tilde{C_0}$ given by the equation $z^d - f(x, y) = 0$. His work is in part based on Van den Burgh's results [17] which connect the Clifford algebra of a binary form f of degree d to certain vector bundles on the projective curve $\tilde{C_0}$. Up to this point, these all have the type of noncommutative linearization, in the language of Van den Bergh, of a homogeneous form. In this paper, we present a construction not of this type.

In the series of papers [6–9] on the Clifford algebra A_f of a binary cubic from f, Haile also proved that there is an induced group homomorphism from the group $E_0(F)$ of F-rational points on E_0 into the Brauer group $Br(F)$ of F [6, Theorem 1.3′] with image the relative Brauer group $Br(F(C_0)/F)$, where $F(C_0)$ denotes the function field of the curve C_0 [7, Theorem 1.2, Corollary 2.2]. Finally, he proved in [9] that the algebra A_f is split if and only if the set $C_0(F)$ of F-rational points on C_0 is nonempty. In view of the work of Haile, the Clifford algebra of the binary cubic form f reflects the nature of the cubic curve C_0. It is thus natural to ask whether there are interesting algebras associated to other cubic curves. We now generalize Haile's work to the case of certain ternary cubic forms.

From now on we assume that the characteristic of F is not two or three. Let $f(x, y) = ax^3 + 3bx^2y + 3cxy^2 + dy^3$ be a binary cubic form over F. Let $C = z^3 - exyz - f(x, y)$ be a ternary cubic form over F. We also denote by C the nonsingular cubic curve given by the equation

$$z^3 - exyz - f(x, y) = 0.$$

We will construct an F-algebra A_C associated to the cubic curve C. More precisely, the algebra A_C depends on the specific equation of the curve C given by the form f and the parameter e as above. We call A_C the (non-usual) Clifford algebra of the ternary cubic form C. Note that A_C is defined differently from the usual Clifford algebra of the form C; however, if $e = 0$, A_C is the usual Clifford algebra A_f of f, the case studied by Haile. We show that if the ternary cubic form C is irreducible over the algebraic closure $\bar{F}$ of F, then A_C is an Azumaya algebra of rank 9 (Theorem 2.15). Its center is isomorphic as an F-algebra to the affine coordinate ring of an elliptic curve E, namely the Jacobian of the curve C (Theorem 3.2). The simple homomorphic images of A_C are in one-to-one correspondence with the Galois orbits on the affine elliptic curve E_a (Corollary 3.4). The induced function Φ from the group $E(F)$ of F-rational points on E into the Brauer group $Br(F)$ of F is a group homomorphism (Theorem 4.1) with image the relative Brauer group $Br(F(C)/F)$ (Proposition 4.5). The algebra A_C is split if and only if the cubic curve C has an F-rational point (Theorem 4.6). Finally, for the diagonal case, the case when $b = 0 = c$, we present an explicit expression for the function Φ (Corollary 5.5).

We now outline the structure of this paper. In Section 2, we define the algebra A_C and then prove it is Azumaya. The center of A_C is determined in Section 3. The connection between the algebra A_C and the curve C is presented in Section 4. Finally, in Section 5, we discuss the diagonal case.

2. The algebra A_C

As in the introduction, let F be a field of characteristic not two or three, and let

$$f(x, y) = ax^3 + 3bx^2y + 3cxy^2 + dy^3$$

be a binary cubic form over F with discriminant D_f. Let C denote the ternary cubic form over F

$$C = z^3 - exyz - f(x, y).$$

We define an algebra A_C to be the free associative F-algebra on the two indeterminates x, y subject to the relations deriving from the following formal identity in α and β

$$(\alpha x+\beta y)^3 - e\alpha\beta(\alpha x+\beta y) - f(\alpha,\beta) = 0.$$

Thus

$$A_C = F\{x, y\}/I,$$

where I is the ideal generated by the elements

$$\begin{aligned}
&x^3 - a,\\
&x^2y + xyx + yx^2 - ex - 3b,\\
&xy^2 + yxy + y^2x - ey - 3c,\\
&y^3 - d.
\end{aligned}$$

Notice that when $e = 0$ in the definition of A_C, it is the usual Clifford algebra A_f of the binary cubic form f, defined as in the introduction. Abusing terminology, we call A_C the Clifford algebra of the ternary cubic form C.

We again use x and y to denote the images of x and y in A_C, respectively. Let

$$\delta = \left[(xy)^2 - y^2x^2 - exy + \frac{e^2}{3}\right] + \left[(yx)^2 - x^2y^2 - eyx + \frac{e^2}{3}\right].$$

Lemma 2.1. *The element δ is in the center $Z(A_C)$ of A_C.*

Proof. Let $\delta_1 = (xy)^2 - y^2x^2 - exy + e^2/3$ and $\delta_2 = (yx)^2 - x^2y^2 - eyx + e^2/3$. It is easy to see that $\delta_1 x = x\delta_2$ and $\delta_2 y = y\delta_1$. Also,

$$\begin{aligned}
\delta_2 x &= (yxy - ey)x^2 - x^2y^2x + \frac{e^2}{3}x = \bigl(3c - xy^2 - y^2x\bigr)x^2 - x^2y^2x + \frac{e^2}{3}x\\
&= x^2\bigl(3c - xy^2 - y^2x\bigr) - xy^2x^2 + \frac{e^2}{3}x = x^2(yxy - ey) - xy^2x^2 + \frac{e^2}{3}x = x\delta_1;
\end{aligned}$$

similarly, $\delta_1 y = y\delta_2$. Thus $\delta = \delta_1 + \delta_2$ commutes with x and y. $\square$

Lemma 2.2. *The algebra A_C is generated as a module over the subring $F[\delta]$ of the center by the following* 18 *elements*:

$$\begin{aligned}
&1,\\
&x,\ y,\\
&xy,\ yx,\ x^2,\ y^2,\\
&x^2y,\ xy^2,\ y^2x,\ yx^2,\\
&x^2y^2,\ xyxy,\ xyx^2,\ y^2xy,\\
&x^2y^2x,\ xyxy^2,\\
&x^2y^2xy.
\end{aligned}$$

Proof. We observe that all the monomials of degree less than 3 are on the list. Given the monomials s of degree k on the list, for each $2 \leqslant k \leqslant 5$, we try to express the monomials of the form sx or sy as elements of the $F[\delta]$-submodule generated by elements listed above of degree at most $k+1$. In addition, we also need to check if x^2y^2xyx and $x^2y^2xy^2$ are elements of the $F[\delta]$-submodule generated by these 18 elements. These are straightforward calculations. We will only verify this when $k=5$, assuming that it has been proved true for $k \leqslant 4$. We need to consider $x^2y^2x^2$, x^2y^2xy, $xyxy^2x$, $xyxy^3$. But x^2y^2xy is on the list and $xyxy^3 = dxyx$. Moreover,

$$\begin{aligned} x^2y^2x^2 &= x^2\left((xy)^2 + (yx)^2 - x^2y^2 - exy - eyx + \frac{2e^2}{3} - \delta\right) \\ &= ayxy + x^2yxyx - axy^2 - eay - ex^2yx + \left(\frac{2e^2}{3} - \delta\right)x^2. \end{aligned}$$

Since

$$x^2yxyx = x^2\bigl(3c + ey - xy^2 - y^2x\bigr)x = 3ac + ex^2yx - ay^2x - x^2y^2x^2,$$

we get

$$x^2y^2x^2 = 3ac + \left(\frac{e^2}{3} - \frac{\delta}{2}\right)x^2 - axy^2 - ay^2x.$$

Similarly,

$$xyxy^2x = (9bc - ad) + 3ecx + \left(\frac{e^2}{3} - \frac{\delta}{2}\right)xy - 3bxy^2 - 3cyx^2 - x^2y^2xy. \qquad \square$$

Let $\bar{F}$ be a fixed algebraic closure of F and let $\omega \in \bar{F}$ be a fixed primitive cube root of unity. Throughout this paper, let $\eta = 2\omega + 1 \in \bar{F}$. To study the algebra A_C, we first assume that F contains ω. Let

$$z = yx - \omega xy - \frac{\omega^2\eta e}{3} \quad \text{and} \quad \bar{z} = yx - \omega^2 xy + \frac{\omega\eta e}{3}.$$

In general, $z\bar{z} \neq \bar{z}z$. In fact,

$$z\bar{z} - \bar{z}z = \eta(3by - 3cx).$$

Lemma 2.3. *The elements z^3 and $\bar{z}^3$ are in the center $Z(A_C)$. In fact, we have the following identities*:

$$\begin{aligned} xz &= \omega zx - 3b\omega, \qquad & x\bar{z} &= \omega^2\bar{z}x - 3b\omega^2, \\ yz &= \omega^2 zy + 3c, \qquad & y\bar{z} &= \omega\bar{z}y + 3c. \end{aligned}$$

Proof. For the first equation,

$$\begin{aligned} xz - \omega zx &= x\left(yx - \omega xy - \frac{\omega^2\eta e}{3}\right) - \omega\left(yx - \omega xy - \frac{\omega^2\eta e}{3}\right)x \\ &= -\omega\bigl(xyx + x^2y + yx^2\bigr) + \frac{(1-\omega^2)\eta e}{3}x \end{aligned}$$

$$= -\omega(ex + 3b) + \omega ex$$
$$= -3b\omega.$$

It follows that $xz^2 = \omega^2 z^2 x + 3bz$ and $xz^3 = z^3 x$. The others are similar. □

Let $\gamma \in \bar{F}$ be a fixed cube root of a. Let $F(\gamma)(T)[R]$ be the polynomial ring in the indeterminate R over the field $F(\gamma)(T)$ where T is an indeterminate. Consider the polynomial

$$h_T(R) = R^3 + \left(\frac{\omega}{\gamma}A + \frac{be}{a}\right)\frac{1}{T}R^2 - \frac{\omega e}{\gamma}TR + \left(\frac{\omega}{\gamma}A - \frac{\omega be}{a}\right)\left(\frac{\omega}{\gamma}A - \frac{\omega^2 be}{a}\right)\frac{1}{3T^2}R + T^3 + B,$$

where

$$A = 3c - \frac{3b^2}{a} \quad \text{and} \quad B = -\frac{\omega e}{3\gamma}\left(\frac{\omega}{\gamma}A + \frac{be}{a}\right) + \left(\frac{e^3}{27a} + \frac{b^3}{a^2} - d + \frac{b}{a}A\right).$$

Let K denote the ring

$$K = F(\gamma)(T)[R]/\langle h_T(R)\rangle.$$

Remark 2.4. When $e \neq 0$, it is easy to prove by contradiction that the polynomial $h_T(R)$ is irreducible over the field $F(\gamma)(T)$. When $e = 0$, $h_T(R)$ is irreducible over $F(\gamma)(T)$ if $D_f \neq 0$.

The following theorem gives an explicit model for A_C.

Theorem 2.5. *Let $\tilde{A}$ be the F-subalgebra of $M_3(K)$ generated by the matrices*

$$\tilde{x} = \begin{pmatrix} \gamma & 0 & 0 \\ 0 & \omega\gamma & 0 \\ 0 & 0 & \omega^2\gamma \end{pmatrix}$$

and

$$\tilde{y} = \begin{pmatrix} \frac{e}{3\gamma} + \frac{b}{\gamma^2} & R & T \\ T & \frac{e\omega^2}{3\gamma} + \frac{\omega b}{\gamma^2} & \omega R + \eta(\frac{\omega A}{\gamma} - \frac{\omega^2 be}{a})\frac{1}{3T} \\ \omega^2 R - \eta(\frac{\omega A}{\gamma} - \frac{\omega be}{a})\frac{1}{3T} & T & \frac{e\omega}{3\gamma} + \frac{\omega^2 b}{\gamma^2} \end{pmatrix}.$$

There is an F-algebra isomorphism from A_C onto $\tilde{A}$ sending x to $\tilde{x}$ and y to $\tilde{y}$.

We will prove Theorem 2.5 as a result of a series of lemmas.

Lemma 2.6. *There is an F-algebra homomorphism from A_C onto $\tilde{A}$ sending x to $\tilde{x}$ and y to $\tilde{y}$.*

Proof. One can check that the ideal I is in the kernel of the homomorphism from the free associative F-algebra $F\{x, y\}$ onto $\tilde{A}$ sending x to $\tilde{x}$ and y to $\tilde{y}$. □

Let $\varphi : u \mapsto \tilde{u}$ denote this F-algebra homomorphism.

Lemma 2.7. *The element $\tilde{\delta}$ is transcendental over F.*

Proof. By direct computation,

$$\tilde{\delta} = 2\omega\gamma^2\left(3RT + \frac{\omega A}{\gamma} + \frac{be}{a}\right). \tag{1}$$

Thus $\tilde{\delta}$ is transcendental over F. $\square$

Lemma 2.8. *The field $F(\tilde{\delta}, T^3)$ is a quadratic extension of $F(\tilde{\delta})$.*

Proof. Since $T^6 - (R^3 + T^3)T^3 + (RT)^3 = 0$, it follows from the choice of $h_T(R)$ that T^3 satisfies the following polynomial in X:

$$X^2 + \left(B - \frac{\omega e}{\gamma}RT\right)X + \left(\frac{\omega}{\gamma}A + \frac{be}{a}\right)(RT)^2 + \left(\frac{\omega}{\gamma}A - \frac{\omega be}{a}\right)\left(\frac{\omega}{\gamma}A - \frac{\omega^2 be}{a}\right)\frac{RT}{3} + (RT)^3,$$

which, in turn by Eq. (1), equals

$$X^2 + \left(\frac{e^3}{27a} + \frac{b^3}{a^2} - d + \frac{b}{a}A - \frac{e}{6a}\tilde{\delta}\right)X + \frac{1}{216a^2}\tilde{\delta}^3 - \frac{beA}{18a^2}\tilde{\delta} - \frac{1}{27a}\left(A^3 + \frac{b^3e^3}{a^2}\right).$$

Thus the result follows. $\square$

Throughout this paper, if $\omega \in F$, let $(\alpha, \beta)_F$ denote the 9-dimensional symbol algebra over F with generators u, v and relations $u^3 = \alpha$, $v^3 = \beta$, and $vu = \omega uv$.

Lemma 2.9. *The algebra $\tilde{A}$ is a free $F[\tilde{\delta}]$-module of dimension* 18.

Proof. Let $\xi = z - \omega^2\eta(b/a)x^2$. Then

$$x\xi = \omega\xi x \quad \text{and} \quad \xi^3 = z^3 + 3\eta\frac{b^3}{a} \in Z(A_C).$$

A direct computation shows that

$$\tilde{z}^3 = 3\eta\left(aT^3 - \frac{b^3}{a}\right), \quad \text{so } \tilde{\xi}^3 = 3\eta a T^3. \tag{2}$$

Thus the $F(\tilde{\delta}, T^3)$-subalgebra of $\tilde{A}F(\tilde{\delta}, T^3)$ generated by $\tilde{x}$ and $\tilde{\xi}$ is the symbol algebra $(3\eta aT^3, a)_{F(\tilde{\delta}, T^3)}$. It follows that

$$\dim_{F(\tilde{\delta}, T^3)} \tilde{A}F\big(\tilde{\delta}, T^3\big) \geqslant 9$$

and hence by Lemma 2.8,

$$\dim_{F(\tilde{\delta})} \tilde{A}F\big(\tilde{\delta}, T^3\big) = \dim_{F(\tilde{\delta}, T^3)} \tilde{A}F\big(\tilde{\delta}, T^3\big) \cdot \dim_{F(\tilde{\delta})} F\big(\tilde{\delta}, T^3\big) \geqslant 18.$$

But by Eq. (2) and Lemma 2.8 again, $\tilde{A}F(\tilde{\delta}, T^3) = \tilde{A}F(\tilde{\delta})$. Moreover, by Lemma 2.2, $\tilde{A}$ as an $F[\tilde{\delta}]$-module is generated by 18 elements. Therefore these generators, regarded as elements in $\tilde{A}F(\tilde{\delta})$, form an $F(\tilde{\delta})$-basis, and hence the result follows. □

From the proof of Lemma 2.9, we conclude the following result.

Lemma 2.10. *The $F(\tilde{\delta}, T^3)$-subalgebra $\tilde{A}F(\tilde{\delta}, T^3)$ of $M_3(K)$ is the* 9*-dimensional symbol algebra* $(3\eta aT^3, a)_{F(\tilde{\delta},T^3)}$ *with generators $\tilde{\xi}$ and $\tilde{x}$. In particular, $Z(\tilde{A}) \subseteq F(\tilde{\delta}, \tilde{\xi}^3)$.*

We now can prove Theorem 2.5.

Proof of Theorem 2.5. Since by Lemma 2.2 A_C is an $F[\delta]$-module generated by 18 generators, it then follows from Lemma 2.9 that the homomorphism φ from A_C onto $\tilde{A}$ sends these generators to an $F[\tilde{\delta}]$-basis of $\tilde{A}$. But by Lemma 2.7, the restriction of φ to $F[\delta]$ is an isomorphism onto $F[\tilde{\delta}]$. Hence the homomorphism φ itself is injective, and we are done. □

Remark 2.11. It follows from Theorem 2.5 and Lemma 2.10 that $Z(A_C) \subseteq F(\delta, \xi^3)$.

Here let F be an arbitrary field, and let A be an F-algebra. An *l-dimensional representation* of A is an F-algebra homomorphism $\phi : A \to M_l(L)$, where L is an extension field of F. A representation is *algebraic* if L is an algebraic extension of F. Now as usual again, let F be a field of characteristic of not 2 or 3.

Example 2.12. The homomorphism φ gives rise to a 3-dimensional non-algebraic representation of the F-algebra A_C when $e \neq 0$.

Proposition 2.13. *Suppose the form C is irreducible over $\bar{F}$. Then the dimension of every algebraic representation of the Clifford algebra A_C is at least* 3.

Proof. Let $\phi : A_C \to M_l(L)$ be an arbitrary algebraic representation of A_C, and let X, Y be the images of x, y, respectively. Let α, β be two indeterminates over L. Then $(\alpha X + \beta Y)^3 - e\alpha\beta(\alpha X + \beta Y) = f(\alpha, \beta)$. Hence $\alpha X + \beta Y \in M_l(L(\alpha, \beta))$ satisfies the polynomial

$$h(t) = t^3 - e\alpha\beta t - f(\alpha, \beta) \in L(\alpha, \beta)[t],$$

which is irreducible over $L(\alpha, \beta)$, for otherwise, $h(t)$ as a polynomial in $L[\alpha, \beta, t]$ would be reducible over L, a contradiction to the irreducibility of C over $\bar{F}$. Hence $h(t)$ is the minimal polynomial of $\alpha X + \beta Y$ over $L(\alpha, \beta)$, and so l is at least 3. □

Corollary 2.14. *Every simple homomorphic image of the Clifford algebra A_C has degree at least* 3.

Proof. Let R be an arbitrary simple homomorphic image of A_C, and let $Z(R)$ denote the center of R. It is well known that there exists a finite field extension L of $Z(R)$ which splits R; that is, $R \otimes_{Z(R)} L \cong M_l(L)$, where $l = \deg R$. Hence we obtain a representation of A_C into $M_l(L)$. By Proposition 2.13 it suffices to prove that $Z(R)$ is an algebraic extension of F. Recall that A_C is finitely generated as a module over $F[\delta]$. Hence R, isomorphic to A_C/m for some maximal ideal m of A_C, is also finitely generated as a module over $F[\delta]/(F[\delta] \cap m)$. Thus R, and hence $Z(R)$, is integral over $F[\delta]/(F[\delta] \cap m)$. Since $F[\delta] \cap m$ is a prime ideal of $F[\delta]$, and so it is generated by an irreducible polynomial over F, it follows that $F[\delta]/(F[\delta] \cap m)$ is a finite field extension of F. As a result, $Z(R)$ is algebraic over F. □

We are now ready to prove the main theorem.

Theorem 2.15. *Suppose the form C is irreducible over $\bar{F}$. Then the Clifford algebra A_C of the ternary cubic form C is an Azumaya algebra of rank* 9 *over its center.*

Proof. We first assume that $\omega \in F$. Then by the Artin–Procesi theorem on polynomial identities (cf. Rowen [16, Theorem 6.1.35]), it follows from Theorem 2.5 and Corollary 2.14 that A_C is an Azumaya algebra of rank 9. Now let F be an arbitrary field of characteristic not 2 or 3. Notice that the construction of the Clifford algebra A_C is functorial in F; that is, for any field extension L/F, $A_C^L = A_C \otimes_F L$ is the Clifford algebra of the form C regarded as over L. If $L = F[\omega]$, we have seen that A_C^L is an Azumaya algebra of rank 9. As a result, A_C is an Azumaya algebra of rank 9 (cf. DeMeyer and Ingraham [4, p. 45]). □

Remark 2.16. When $e = 0$, it is easily checked that C is irreducible over $\bar{F}$ if and only if $D_f \neq 0$, the assumption used in *Haile* [6].

Corollary 2.17. *Each simple homomorphic image of the Clifford algebra A_C is a central simple algebra of degree* 3*.*

We now prove that the irreducibility over $\bar{F}$ of $C = z^3 - exyz - f(x, y)$ is a necessary condition for the Clifford algebra A_C to be Azumaya.

Proposition 2.18. *If the Clifford algebra A_C of the ternary cubic form C is Azumaya, then the form C is irreducible over $\bar{F}$.*

Proof. Suppose $C = z^3 - exyz - f(x, y) \in F[x, y, z]$ is reducible over $\bar{F}$. Then there exist $u, v, w \in \bar{F}[x, y]$ such that

$$z^3 - exyz - f(x, y) = \big(z + u(x, y)\big)\big(z^2 + v(x, y)z + w(x, y)\big).$$

Hence $f(x, y) = -(u(x, y))^3 + exyu(x, y)$ and so $u(x, y) = \mu x + \nu y$ for some $\mu, \nu \in \bar{F}$. Thus there exists a surjective F-algebra homomorphism from A_C onto $F(\mu, \nu)$ sending x to $-\mu$ and y to $-\nu$. Let K be the ring defined as right before Remark 2.4 with F replaced by $F(\omega)$. Let $\tilde{x}$ and $\tilde{y}$ be defined as in the statement of Theorem 2.5, and let $\tilde{A}$ be the F-subalgebra of $M_3(K)$ generated by $\tilde{x}$ and $\tilde{y}$. There is an F-algebra homomorphism from A_C onto $\tilde{A}$ sending x to $\tilde{x}$ and y to $\tilde{y}$. Since $\tilde{A}$ is noncommutative and hence so is A_C, it follows that A_C is not Azumaya, for otherwise, $\operatorname{rank}_{Z(A_C)} A_C > 1$ would force $\operatorname{rank}_{Z(R)} R > 1$ for any simple homomorphic image R, contradicting the case when $R = F(\mu, \nu)$. □

Corollary 2.19. *The Clifford algebra A_C of the ternary cubic form C is Azumaya if and only if the form C is irreducible over $\bar{F}$.*

3. The center of A_C

From now on, we assume that the form $C = z^3 - exyz - f(x, y) \in F[x, y, z]$ is irreducible over $\bar{F}$. Let C also denote the nonsingular cubic curve given by the equation

$$z^3 - exyz - f(x, y) = 0.$$

In this section we determine the center $Z(A_C)$ of A_C.

Throughout this section, let

$$A = 3c - \frac{3b^2}{a} \quad \text{and} \quad D = \frac{e^3}{27a} + \frac{b^3}{a^2} - d + \frac{b}{a}A.$$

Lemma 3.1. *Assume that F contains ω. Let $\bar{\xi} = \bar{z} + \omega\eta(b/a)x^2$, where $\bar{z}$ is defined as right before Lemma* 2.3. *Then $\bar{\xi}x = \omega x\bar{\xi}$ and*

$$\left(\bar{\xi}^3 + \frac{\eta e}{2}\frac{\delta}{2} - \frac{3}{2}\eta aD\right)^2 = \left(\frac{\delta}{2}\right)^3 - \frac{3e^2}{4}\left(\frac{\delta}{2}\right)^2 + \left(\frac{9e}{2}aD - 3ebA\right)\frac{\delta}{2} - \frac{27}{4}a^2D^2 - a\left(A^3 + \frac{b^3e^3}{a^2}\right).$$

Proof. The first equation is straightforward. Consider $\tilde{\bar{\xi}}$, the homomorphic image of $\bar{\xi}$ under the isomorphism φ defined as right before Lemma 2.7. A direct computation shows that

$$\tilde{\bar{\xi}}^3 = -3\eta a\left[R^3 + \left(\frac{\omega}{\gamma}A + \frac{be}{a}\right)\frac{R^2}{T} + \left(\frac{\omega}{\gamma}A - \frac{\omega be}{a}\right)\left(\frac{\omega}{\gamma}A - \frac{\omega^2 be}{a}\right)\frac{R}{3T^2}\right]. \tag{3}$$

Then by the choice of $h_T(R)$, defined as right before Remark 2.4, and Eq. (1),

$$\begin{aligned}\tilde{\bar{\xi}}^3 &= -3\eta a\left[\frac{\omega e}{\gamma}RT + \frac{\omega e}{3\gamma}\left(\frac{\omega}{\gamma}A + \frac{be}{a}\right) - D - T^3\right] \\ &= -\eta e\frac{\tilde{\delta}}{2} + 3\eta aD + 3\eta aT^3. \end{aligned}\tag{4}$$

Combining Eqs. (3) and (4), we have

$$\begin{aligned}\tilde{\bar{\xi}}^3\tilde{\bar{\xi}}^3 = {}&\left[-\eta e\frac{\tilde{\delta}}{2} + 3\eta aD\right]\tilde{\bar{\xi}}^3 \\ &+ 27a^2\left[(RT)^3 + \left(\frac{\omega}{\gamma}A + \frac{be}{a}\right)(RT)^2 + \left(\frac{\omega}{\gamma}A - \frac{\omega be}{a}\right)\left(\frac{\omega}{\gamma}A - \frac{\omega^2 be}{a}\right)\frac{RT}{3}\right].\end{aligned}\tag{5}$$

But by Eq. (1) again,

$$\tilde{\delta}^3 = 216a^2\left[(RT)^3 + \left(\frac{\omega A}{\gamma} + \frac{be}{a}\right)(RT)^2 + \left(\frac{\omega A}{\gamma} + \frac{be}{a}\right)^2\left(\frac{RT}{3}\right) + \left(\frac{\omega A}{3\gamma} + \frac{be}{3a}\right)^3\right]. \tag{6}$$

Therefore, it follows from Eqs. (1), (5) and (6) that

$$\begin{aligned}&\left(\tilde{\bar{\xi}}^3 + \frac{\eta e}{2}\frac{\tilde{\delta}}{2} - \frac{3}{2}\eta aD\right)^2 \\ &= 27a^2\left[\frac{\tilde{\delta}^3}{216a^2} - \left(\frac{\omega A}{3\gamma} + \frac{be}{3a}\right)^3 - \left(\frac{\omega A}{\gamma}\right)\left(\frac{be}{a}\right)\left(\frac{RT}{3}\right)\right] + \left(\frac{\eta e}{2}\frac{\tilde{\delta}}{2} - \frac{3}{2}\eta aD\right)^2 \\ &= \left(\frac{\tilde{\delta}}{2}\right)^3 - \frac{3e^2}{4}\left(\frac{\tilde{\delta}}{2}\right)^2 + \left(\frac{9e}{2}aD - 3ebA\right)\frac{\tilde{\delta}}{2} - \frac{27}{4}a^2D^2 - a\left(A^3 + \frac{b^3e^3}{a^2}\right). \qquad \square\end{aligned}$$

Theorem 3.2. *The center of A_C is isomorphic as an F-algebra to the affine coordinate ring of the elliptic curve E given by the Weierstrass equation*

$$E_a\colon\quad s^2 = r^3 - \frac{3}{4}e^2r^2 + \left(\frac{9e}{2}aD - 3ebA\right)r - \frac{27}{4}a^2D^2 - a\left(A^3 + \frac{b^3e^3}{a^2}\right).$$

The elliptic curve E is the Jacobian of the nonsingular cubic curve C given by the equation

$$z^3 - exyz - f(x, y) = 0.$$

Proof. Assume first that $\omega \in F$. Let $\bar{\xi}$ be defined as in the statement of Lemma 3.1. Then by Theorem 2.5 and Eqs. (2) and (4), $\bar{\xi}^3 = -\eta e\delta/2 + 3\eta aD + \xi^3 \in Z(A_C)$, and so by Remark 2.11, $Z(A_C) \subset F(\delta, \bar{\xi}^3)$. Let $F[E_a]$ denote the affine coordinate ring of the elliptic curve E. Then $F[E_a] = F[r, s]$ is a Dedekind domain, where r and s are the Weierstrass coordinate functions on E. Let $F[\delta, \bar{\xi}^3]$ be the F-subalgebra of A_C generated by δ and $\bar{\xi}^3$. Then

$$F\left[\delta, \bar{\xi}^3\right] \subset Z(A_C) \subset F\left(\delta, \bar{\xi}^3\right).$$

By Lemma 3.1, we have a surjective F-algebra homomorphism from $F[E_a]$ onto $F[\delta, \bar{\xi}^3]$ sending

$$r \mapsto \frac{\delta}{2},$$
$$s \mapsto \bar{\xi}^3 + \frac{\eta e}{2}\frac{\delta}{2} - \frac{3}{2}\eta aD.$$

Since every nonzero prime ideal of $F[E_a]$ is maximal and $F[\delta, \bar{\xi}^3]$ is not a field, this homomorphism must be an isomorphism. In particular, $F[\delta, \bar{\xi}^3]$ is integrally closed. But it follows from Lemma 2.2 that A_C, and hence its center $Z(A_C)$, is integral over $F[\delta, \bar{\xi}^3]$. As a result, $Z(A_C) = F[\delta, \bar{\xi}^3] \cong F[E_a]$.

Suppose now that $\omega \notin F$. Let $L = F[\omega]$. Let σ be an F-automorphism of L sending ω to ω^2, so that $\mathrm{Gal}(L/F) = \langle\sigma\rangle$. Then A_C may be identified as the algebra of fixed elements in $A_C \otimes_F L$ under the automorphism $1 \otimes \sigma$. In particular,

$$Z(A_C) = Z(A_C \otimes_F L)^{1\otimes\sigma} = L\left[\delta, \bar{\xi}^3\right]^{1\otimes\sigma}.$$

But it is easy to see that δ and $\bar{\xi}^3 + (\eta e/2)(\delta/2) - (3/2)\eta aD$ are fixed by $1 \otimes \sigma$. Hence $Z(A_C) = F[\delta, \bar{\xi}^3 + (\eta e/2)(\delta/2) - (3/2)\eta aD]$, which is isomorphic as an F-algebra to $F[E_a]$ by an argument like the above.

The explicit Weierstrass equation of the Jacobian of a nonsingular plane cubic curve can be found in An et al. [1, Section 3.2, (3.8)]. Their computations show that the elliptic curve E is the Jacobian of the curve C. $\square$

Corollary 3.3. *Let $F(E)$ be the function field of the elliptic curve E, and let $\Sigma_C = A_C \otimes_{F[E_a]} F(E)$. Then Σ_C is an $F(E)$-central simple algebra of degree 3. Furthermore, if $\omega \in F$, then Σ_C is the symbol algebra $(a, s - (\eta e/2)r + (3/2)\eta aD)_{F(r,s)}$ with generators x and $\bar{\xi}$, where r and s are the Weierstrass coordinate functions on E.*

I am indebted to Prof. Adrian Wadsworth for pointing out the following fact: Let R be an integrally closed integral domain with quotient field K and let L be a normal field extension of K, possibly of infinite degree. Let G be the group of K-automorphisms of L and let T be the integral closure of R in L. Then every automorphism in G maps T to itself and permutes the maximal ideals of T. Moreover, G acts transitively on the set of maximal ideals of T contracting a given maximal ideal of R (cf. [13, Theorem 9.3(iii), p. 66]). Therefore, the orbits under the action of G on the maximal ideals of T are in one-to-one correspondence with the maximal ideals of R. Applying this to our case with $R = F[E_a]$ and $T = \bar{F}[E_a]$, we derive the following corollary:

Corollary 3.4. *There is a one-to-one correspondence between the simple homomorphic images of A_C and the Galois orbits of the set of points in $\bar{F} \times \bar{F}$ on the affine elliptic curve*

$$E_a: \quad s^2 = r^3 - \frac{3}{4}e^2 r^2 + \left(\frac{9e}{2}aD - 3ebA\right)r - \frac{27}{4}a^2 D^2 - a\left(A^3 + \frac{b^3 e^3}{a^2}\right).$$

The correspondence is given as follows: Each Galois orbit containing the point $p = (r_0, s_0)$ *on the affine curve* E_a *determines a maximal ideal* m_p *in the center of* A_C*, and the algebra* $A_C/m_p A_C$ *with center* $F(r_0, s_0)$ *is then the corresponding central simple algebra of degree* 3*.*

Proof. Since A_C is Azumaya, its simple homomorphic images are in one-to-one correspondence with maximal ideals of its center $F[E_a]$. Thus the result follows. □

4. A_C and the curve C

Define a function Φ from the group $E(F)$ of F-rational points on the elliptic curve E, the Jacobian of the cubic curve C, into the Brauer group of F by sending the point O at infinity to 1 and sending $p \in E_a(F)$ to the Brauer class of the specialization of A_C at the point p, $A_C/m_p A_C$, where m_p is the maximal ideal of $Z(A_C)$ determined by p as described in Corollary 3.4. We shall prove that Φ is a group homomorphism.

Theorem 4.1. *The function* $\Phi : E(F) \to Br(F)$*, sending*

$$p \in E_a(F) \mapsto [A_C/m_p A_C],$$
$$\textit{the point } O \textit{ at infinity} \mapsto 1,$$

is a group homomorphism.

It was first proved true in [12] for the diagonal case (when $b = 0 = c$) by direct computation. Here we apply a result of Ciperiani and Krashen [3, Theorem 2.3.1] to give a proof for any case. We first present a brief description of their result: Let k be a field with $\bar{k}$ a fixed separable closure of k. Let X be a smooth projective curve over k, and let $\mathcal{P}ic_X$ be the Picard variety of X. If $x \in X(k)$, let $Br(X, x)$ denote the subgroup of the Brauer group $Br(X)$ consisting of classes whose specialization at x is trivial. Then there is a natural isomorphism $\mathcal{A}: H^1(k, \mathcal{P}ic_X(\bar{k})) \to Br(X, x)$, and in the case that $X = \mathcal{E}$ is an elliptic curve, and $x = O_{\mathcal{E}}$ is the origin of the curve, the map

$$H^1\big(k, \mathcal{E}(\bar{k})\big) \times \mathcal{E}(k) \to Br(k),$$
$$(\alpha, p) \mapsto \mathcal{A}(\alpha)|_p$$

coincides with the Tate paring. If we can extend the Clifford algebra A_C to a Brauer class in $Br(E)$ and then show that the class has trivial specialization at the point O at infinity, then by this result, the specialization map of the class, exactly the function Φ, is a group homomorphism.

We now proceed to prove that the Clifford algebra A_C over the affine part E_a of the elliptic curve E can be extended to a Brauer class in $Br(E)$. I am indebted to Prof. Daniel Krashen for suggesting the approach given as below for the following more general result.

Proposition 4.2. *Suppose that* X *is a smooth projective curve over the field* k*. Let* $\alpha \in Br(k(X))$*, where* $k(X)$ *is the function field of the curve* X*. If* α *is unramified except possibly at a single* k*-rational point* x*, then* α *is unramified.*

To prove this proposition, we begin with some background. Let $K = k(X)$, $\bar{k}$ be a fixed separable closure of k, $\bar{K} = \bar{k}(X) = \bar{k} \otimes_k k(X)$ and $G = \mathrm{Gal}(\bar{k}/k)$. Recall that for a k-rational point P on X, the usual ramification map $\mathrm{ram}_P : Br(X) \to H^1(G, \mathbb{Q}/\mathbb{Z})$ is defined via the composition

$$H^2\big(G, \bar{K}^\times\big) \xrightarrow{\mathrm{val}_P} H^2(G, \mathbb{Z}) \xrightarrow{\cong} H^1(G, \mathbb{Q}/\mathbb{Z}),$$

where val_P is induced from the valuation on $\bar{K}^\times$ corresponding to the point P, and the isomorphism is induced from the short exact sequence

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0. \tag{7}$$

In the case when we have a point P on X which is closed but not k-rational; that is, the residue field of P, $\kappa(P)$, is not equal to k, let $H_P = \mathrm{Gal}(\bar{k}/\kappa(P))$. We define the ramification map at P, ram_P, via the composition

$$H^2\big(G, \bar{K}^\times\big) \xrightarrow{\mathrm{res}} H^2\big(H_P, \bar{K}^\times\big) \xrightarrow{\mathrm{val}_{\tilde{P}}} H^2(H_P, \mathbb{Z}) \xrightarrow{\cong} H^1(H_P, \mathbb{Q}/\mathbb{Z}),$$

where $\tilde{P}$ can be chosen to be any $\kappa(P)$-point lying over P.

On the other hand, for each $i \geqslant 0$, the divisor map induces maps

$$H^i\big(G, \bar{K}^\times\big) \xrightarrow{\mathrm{div}} H^i\big(G, \mathrm{Div}(X)\big).$$

Note that as G-modules, we have

$$\mathrm{Div}(X) = \bigoplus_{P \in X_0} \bigg(\bigoplus_{Q \mapsto P} \mathbb{Z} \bigg),$$

where X_0 denotes the set of closed points on X, and the notation $Q \mapsto P$ stands for the closed points Q on X lying over P. Thus for each $i \geqslant 0$,

$$H^i\big(G, \mathrm{Div}(X)\big) = \bigoplus_{P \in X_0} H^i\bigg(G, \bigoplus_{Q \mapsto P} \mathbb{Z}\bigg), \tag{8}$$

for cohomology commutes with direct sums. Also,

$$M^G_{H_P}(\mathbb{Z}) = \mathrm{Hom}_{H_P}\big(\mathbb{Z}[G], \mathbb{Z}\big) \cong \bigoplus_{Q \mapsto P} \mathbb{Z} \tag{9}$$

as G-modules. But Shapiro's lemma states that for each $i \geqslant 0$,

$$H^i\big(G, M^G_{H_P}(\mathbb{Z})\big) \cong H^i(H_P, \mathbb{Z}). \tag{10}$$

Thus by combining Eqs. (8), (9) and (10), we may rewrite each div map as

$$H^i\big(G, \bar{K}^\times\big) \to \bigoplus_{P \in X_0} H^i(H_P, \mathbb{Z}).$$

But $H^i(H_P,\mathbb{Z})\cong H^{i-1}(H_P,\mathbb{Q}/\mathbb{Z})$ for each $i\geqslant 2$, induced again from the short exact sequence in (7). Therefore we get, for each $i\geqslant 2$ and $P\in X_0$, a map

$$r_P: H^i\big(G,\bar{K}^\times\big)\to H^{i-1}(H_P,\mathbb{Q}/\mathbb{Z}),$$

called the residue map associated with P (cf. Gille and Szamuely [5, Section 6.4]).

We are now ready to prove Proposition 4.2.

Proof of Proposition 4.2. Consider the corestriction maps

$$\mathrm{Cor}_P: H^{i-1}(H_P,\mathbb{Q}/\mathbb{Z})\to H^{i-1}(G,\mathbb{Q}/\mathbb{Z})$$

for each closed point P. By [5, Theorem 6.4.4], we have complexes for all $i\geqslant 1$

$$H^i\big(G,\bar{K}^\times\big)\xrightarrow{\ \sum r_P\ }\bigoplus_{P\in X_0}H^{i-1}(H_P,\mathbb{Q}/\mathbb{Z})\xrightarrow{\ \sum \mathrm{Cor}_P\ }H^{i-1}(G,\mathbb{Q}/\mathbb{Z}).$$

One can show that when $i=2$, the residue map r_P is precisely the ramification map ram_P for each closed point P. Thus the composition

$$H^2\big(G,\bar{K}^\times\big)\xrightarrow{\ \sum \mathrm{ram}_P\ }\bigoplus_{P\in X_0}H^{1}(H_P,\mathbb{Q}/\mathbb{Z})\xrightarrow{\ \sum \mathrm{Cor}_P\ }H^{1}(G,\mathbb{Q}/\mathbb{Z})$$

is zero. Suppose that the class α is unramified everywhere possibly except at the k-rational point x. Since Cor_x is simply the identity map, it then follows that α must also be unramified at x. □

Corollary 4.3. *The Brauer class of A_C in $Br(F(E))$ is unramified everywhere. In particular, the Clifford algebra A_C can be extended to a Brauer class in $Br(E)$.*

Proof. Identify $Br(F[E_a])$ with a subgroup of $Br(F(E))$. This is immediate from Proposition 4.2, since the only possible ramification of the Brauer class of A_C in $Br(F(E))$ is at the point O at infinity, for it is the only point not on E_a. □

Proposition 4.4. *The Brauer class of A_C in $Br(E)$ has trivial specialization at the point O at infinity.*

Proof. Let $\Sigma_C=A_C\otimes_{F[E_a]}F(E)$. We may assume that $\omega\in F$. Then by Corollary 3.3, Σ_C is the symbol algebra $(a, s-(\eta e/2)r+(3/2)\eta aD)_{F(r,s)}=(a,t)_{F(r,s)}$, where $t=(s-(\eta e/2)r+(3/2)\eta aD)r^3/s^3$. Let v be the discrete valuation on $F(E)$ corresponding to the point O at infinity. Then $v(r)=-1$, and hence $v(s)=-3/2$ by the Weierstrass equation E_a of E. Since $v(a)=v(t)=0$, the specialization of Σ_C at O is $(a,\bar{t})_F$, where $\bar{t}$ is the image of t in the residue field of O. But

$$\begin{aligned}t&=\left(s-\frac{\eta e}{2}r+\frac{3}{2}\eta aD\right)\frac{r^3}{s^3}\\&=\left(1-\frac{\eta e}{2}\frac{r}{s}+\frac{3}{2}\eta aD\frac{1}{s}\right)\left(1+\frac{3}{4}e^2\frac{r^2}{s^2}-D_1\frac{r}{s^2}-D_2\frac{1}{s^2}\right),\end{aligned}$$

where D_1 and D_2 are the coefficient of r and the constant, respectively, in the Weierstrass equation E_a. Thus $\bar{t}=1$, and hence the specialization at O of the class of A_C is trivial. □

We now conclude Theorem 4.1.

Proof of Theorem 4.1. As mentioned right below the statement of Theorem 4.1, it follows from Corollary 4.3 and Proposition 4.4 that the function Φ is a group homomorphism. □

Next we prove that the image of this group homomorphism Φ is precisely the relative Brauer group $Br(F(C)/F)$.

Proposition 4.5. *A central division algebra D over F is a homomorphic image of A_C if and only if D is split by the function field of the curve C. Consequently, the image of the group homomorphism $\Phi : E(F) \to Br(F)$ is $Br(F(C)/F)$.*

Proof. Let D be an F-central division algebra. Let λ be an indeterminate over F and let $D(\lambda) = D \otimes_F F(\lambda)$. Suppose D is a homomorphic image of A_C. Then D is of degree 3 by Corollary 2.17. Let the map from A_C onto D be denoted by $u \mapsto \bar{u}$. Let $d(\lambda) = \bar{x}\lambda + \bar{y} \in D(\lambda)$. The defining relations for A_C imply that $d(\lambda)$ satisfies the polynomial in t over $F(\lambda)$, $h(t) = t^3 - e\lambda t - f(\lambda, 1)$. But $h(t)$ is irreducible over $F(\lambda)$. It then follows that $F(\lambda)(d(\lambda))$ is a maximal subfield of the division algebra $D(\lambda)$. As a result, $F(C) \cong F(\lambda)(d(\lambda))$ splits D.

Conversely, suppose the F-central division algebra D is split by $F(C)$. Then $F(C) \cong F(\lambda, \nu)$, where $\nu^3 - e\lambda\nu - f(\lambda, 1) = 0$, is a cubic extension of $F(\lambda)$ that splits $D(\lambda)$. Hence $D(\lambda)$ is an $F(\lambda)$-central division algebra of degree 3 and $F(C)$ is isomorphic to a maximal subfield of $D(\lambda)$. Thus there exists some $d(\lambda) \in D(\lambda)$ such that $d(\lambda)^3 - e\lambda d(\lambda) - f(\lambda, 1) = 0$; that is, $d(\lambda)$ is a root of $h(t)$. Then the $F[\lambda]$-subalgebra $F[\lambda][d(\lambda)]$ of $D(\lambda)$ as an $F[\lambda]$-module is finitely generated. Let B be a maximal $F[\lambda]$-order in $D(\lambda)$ containing $F[\lambda][d(\lambda)]$. Since $D[\lambda] = D \otimes_F F[\lambda]$ is also a maximal $F[\lambda]$-order in $D(\lambda)$, and all maximal $F[\lambda]$-orders are conjugate, then $D[\lambda]$ also contains a root of $h(t)$, say $a(\lambda)$. Notice that $a(\lambda)$ must be linear because D is a division algebra. Let $a(\lambda) = d_1\lambda + d_2$, where $d_1, d_2 \in D$ with $d_1 \neq 0$. We have a homomorphism from A_C into D sending x to d_1 and y to d_2. Since D is of degree 3, then by Corollary 2.17 again, this homomorphism is surjective. The last statement of the proposition follows immediately. □

We now recall that an Azumaya algebra A over a commutative ring R is said to be split if there exists a finitely generated, faithful projective R-module P such that $A \cong \mathrm{End}_R(P)$. As mentioned in the introduction, it was proved in Haile [9] that the usual Clifford algebra A_f of the non-degenerate binary cubic form f is split if and only if the curve C_0, given by $z^3 - f(x, y) = 0$, has an F-rational point. We also extend this result to the Clifford algebras A_C.

Theorem 4.6. *The Clifford algebra A_C is split if and only if the cubic curve C has an F-rational point.*

It was first proved true in [12] for the diagonal case. To prove this theorem holds in any case, recall the result of Ciperiani and Krashen [3, Theorem 2.3.1] as described right below the statement of Theorem 4.1. A useful consequence is as follows: Suppose $[\mathcal{C}] \in H^1(k, \mathcal{E}(\bar{k}))$. If $[\mathcal{C}] \neq 0$, then $Br(\mathcal{C}_{k(\mathcal{E})}/k(\mathcal{E})) \neq 0$, where $\mathcal{C}_{k(\mathcal{E})}$ denotes the homogeneous space $\mathcal{C}$ regarded as over $k(\mathcal{E})$. This is part of [3, Corollary 2.3.2].

Proof of Theorem 4.6. Suppose that the curve C has an F-rational point; $C(F) \neq \emptyset$. Since every F-central division algebra split by $F(C)$ is also split by the residue fields of points on C, it then follows that $Br(F(C)/F) = 0$, and hence by Proposition 4.5, the specialization of A_C at any F-rational point on E is split. As mentioned in the proof of Theorem 2.15, the construction of the Clifford algebra A_C is functorial in F. Thus for any field extension L/F, the specialization of $A_C^L = A_C \otimes_F L$ at any L-point on E is split. Now, let $L = F(E)$. By considering the generic point of the curve E as an L point on E extended to the function field L, we conclude that $\Sigma_C = A_C \otimes_{F[E_a]} F(E)$, isomorphic to $A_C^L \otimes_{L[E_a]} L$, is split. Therefore, the algebra A_C itself is split, since the canonical homomorphism of Brauer groups $Br(F[E_a]) \to Br(F(E))$ is injective, for $F[E_a]$ is a Dedekind domain.

Conversely, if A_C is split, then so is A_C^L for any field extension L of F. Applying Proposition 4.5 to the Clifford algebra A_C^L, we see that the relative Brauer group $Br(L(C)/L)$ is trivial. Again, let $L = F(E)$. Since the curve C is a homogeneous space for the elliptic curve E, it then follows from [3, Corollary 2.3.2] that the curve C must have an F-rational point. □

5. The diagonal case

In this short section we focus on the special case when the binary cubic form f is diagonal; that is, $b = 0 = c$. We will present explicit formulas for the group homomorphism $\Phi : E(F) \to Br(F)$ defined as in the beginning of Section 4.

Throughout this section we also assume that $e^3 \neq 27ad$, which is the necessary and sufficient condition for the form $C = z^3 - exyz - ax^3 - dy^3$ to be irreducible over $\bar{F}$. Assume that F contains ω. As defined in Section 2, let $z = yx - \omega xy - \omega^2\eta e/3$ and $\bar{z} = yx - \omega^2 xy + \omega\eta e/3$. Let $\zeta = z\bar{z}$. We shall see that ζ plays the same role as δ in the diagonal case. In fact, the following lemma shows that $\delta = 2\zeta$.

Lemma 5.1. *We have the following identities*:

$$\begin{gathered} xz = \omega zx, \qquad x\bar{z} = \omega^2 \bar{z}x, \\ yz = \omega^2 zy, \qquad y\bar{z} = \omega\bar{z}y, \\ (xy)(yx) = (yx)(xy). \end{gathered}$$

In particular, z^3, $\bar{z}^3$ and ζ are in the center $Z(A_C)$ of A_C, $z\bar{z} = \bar{z}z$ and

$$\zeta = (xy)^2 - y^2x^2 - exy + \frac{e^2}{3} = (yx)^2 - x^2y^2 - eyx + \frac{e^2}{3}.$$

Proof. These are straightforward calculations; the first four identities are immediate from Lemma 2.3 by letting $b = 0 = c$. □

Recall the isomorphism $\varphi : A_C \to \tilde{A}$, $u \mapsto \tilde{u}$, where $\tilde{A}$ is defined as in Theorem 2.5. In the diagonal case, we have the following result.

Proposition 5.2. *Let R be a simple homomorphic image of A_C, and let $u \mapsto \hat{u}$ denote the homomorphism. Then R is the symbol algebra $(\hat{z}^3, a)_{Z(R)}$ or $(a, \hat{\bar{z}}^3)_{Z(R)}$, where $Z(R)$ is the center of R.*

Proof. By Lemma 5.1, $\hat{z}^3$ and $\hat{\zeta}$ are in the center $Z(R)$ of R, and $\hat{x}\hat{z} = \omega\hat{z}\hat{x}$. Suppose $\hat{z}^3 \neq 0$. Note that $\hat{\zeta} = \hat{z}\hat{\bar{z}} = \hat{z}(\hat{z} + \eta\hat{x}\hat{y} - \eta e/3)$. Thus

$$\hat{y} = -\frac{1}{3}\eta\hat{x}^{-1}\left(\hat{z}^{-1}\hat{\zeta} - \hat{z} + \frac{\eta e}{3}\right).$$

It follows that R is generated over its center by $\hat{x}$ and $\hat{z}$. Hence R is the symbol algebra $(\hat{z}^3, a)_{Z(R)}$. A similar argument shows that if $\hat{\bar{z}}^3 \neq 0$, R is the symbol algebra $(a, \hat{\bar{z}}^3)_{Z(R)}$. Now it suffices to show that $\hat{z}^3$ and $\hat{\bar{z}}^3$ cannot both be zero.

Notice that when $b = 0 = c$, the polynomial $h_T(R) = R^3 - (\omega e/\gamma)TR + T^3 + D$ with $D = e^3/27a - d$. Since $\tilde{z}^3 = 3\eta a T^3$, $\tilde{\bar{z}}^3 = \tilde{\bar{\xi}}^3 = -3\eta a R^3$ and $\tilde{\zeta} = \tilde{\delta}/2 = 3\omega\gamma^2 RT$ by Eqs. (2), (3) and (1), respectively, we then have $\tilde{z}^3 - \tilde{\bar{z}}^3 = \eta e\tilde{\zeta} - 3\eta a(e^3/27a - d)$. Thus via the isomorphism φ, $z^3 - \bar{z}^3 = \eta e\zeta - 3\eta a(e^3/27a - d)$, so $\hat{z}^3$, $\hat{\bar{z}}^3$ and $\hat{\zeta}$ satisfy

$$\hat{z}^3 - \hat{\hat{z}}^3 = \eta e \hat{\zeta} - 3\eta a\left(\frac{e^3}{27a} - d\right).$$

Assume $\hat{z}^3 = 0 = \hat{\hat{z}}^3$. Then $\hat{\zeta}^3 = (\hat{z}\hat{\hat{z}})^3 = \hat{z}^3\hat{\hat{z}}^3 = 0$ and hence $\hat{\zeta} = 0$, since $\hat{\zeta} \in Z(R)$, which is a field. But then $e^3 = 27ad$, a contradiction. □

Remark 5.3. The previous proposition does not hold in the non-diagonal case, even with $\hat{z}, \hat{\hat{z}}$ replaced by $\hat{\xi}, \hat{\hat{\xi}}$, respectively. In the diagonal case, we can use Proposition 5.2 to replace Corollary 2.14 in the proof of Theorem 2.15.

The elliptic curve E for the center $Z(A_C)$ in the diagonal case is given by the Weierstrass equation

$$E_a:\quad s^2 = r^3 - \frac{3}{4}e^2r^2 + \frac{e}{6}\left(e^3 - 27ad\right)r - \frac{(e^3 - 27ad)^2}{108}.$$

Let $\theta = \eta e/2$ and $\varepsilon = (3/2)\eta a(e^3/27a - d)$. Then we have E_a: $s^2 = r^3 + (\theta r - \varepsilon)^2$.

We now express the correspondence in Corollary 3.4 explicitly in the diagonal case.

Proposition 5.4. *Given the point (r_0, s_0) on E_a, the corresponding simple homomorphic image is the symbol algebra $(s_0 - \varepsilon + \theta r_0, a)_{F(r_0,s_0)}$ if $(r_0, s_0) \neq (0, \varepsilon)$, and $(a, 2\varepsilon)_{F(r_0,s_0)}$ if $(r_0, s_0) = (0, \varepsilon)$.*

Proof. In the proof of Theorem 3.2, we have taken the relations $r = \delta/2$ and $s = \bar{\xi}^3 + (\eta e/2)(\delta/2) - (3/2)\eta aD$. When $b = 0 = c$, $\delta = 2\zeta$, $\bar{\xi} = \bar{z}$ and $z^3 - \bar{z}^3 = \eta e\zeta - 3\eta aD$ with $D = e^3/27a - d$. Thus the relations in the diagonal case are as follows:

$$r = \zeta,$$
$$s = z^3 + \varepsilon - \theta r.$$

Given the point (r_0, s_0) on E_a, one can easily check that $s_0 - \varepsilon + \theta r_0 = 0$ if and only if $r_0 = 0$ and $s_0 = \varepsilon$. Therefore the result follows from Proposition 5.2. □

As a consequence, we have the following result for the function Φ defined as in the beginning of Section 4.

Corollary 5.5. *The function $\Phi : E(F) \to Br(F)$ in the diagonal case can be expressed explicitly as follows*:

$$(r_0, s_0) \mapsto \begin{cases} [(s_0 - \varepsilon + \theta r_0, a)_F] & \text{if } (r_0, s_0) \neq (0, \varepsilon), \\ [(a, 2\varepsilon)_F] & \text{if } (r_0, s_0) = (0, \varepsilon), \end{cases}$$
$$O \mapsto 1.$$

If we take the relations $r = \zeta$ and $s = z^3 + \varepsilon$, then the corresponding elliptic curve E' which determines the center $Z(A_C)$ is given by E'_a: $s^2 - 2\theta rs = r^3 - 2\theta\varepsilon r + \varepsilon^2$. It was proved in [12] by direct computation that the function $\Psi : E'(F) \to Br(F)$, given by

$$(r_0, s_0) \mapsto \begin{cases} [(s_0 - \varepsilon, a)_F] & \text{if } (r_0, s_0) \neq (0, \varepsilon), \\ [(a, 2\varepsilon)_F] & \text{if } (r_0, s_0) = (0, \varepsilon), \end{cases}$$
$$O \mapsto 1,$$

is a group homomorphism. It follows that the function Φ is a group homomorphism, since $\Phi = \Psi \circ \iota$, where $\iota : E \to E'$ sending $[r, s, u]$ to $[r, s + \theta r, u]$ is an isogeny; that is, a morphism between two elliptic curves sending O to O.

To conclude the function Φ is a group homomorphism without the assumption that F contains ω, the following commutative diagram was considered in [12]:

$$\begin{tikzcd} E(L) \arrow[r] & Br(L) \\ E(F) \arrow[r] \arrow[u] & Br(F) \arrow[u] \end{tikzcd}$$

where $L = F[\omega]$. Since the top map is a homomorphism, and the restriction homomorphism $Br(F) \to Br(L)$ is injective on the image of $E(F)$ in $Br(F)$, for $[L : F]$ is relatively prime to 3, it then follows that the bottom map $E(F) \to Br(F)$ is a homomorphism.

Acknowledgments

I would like to thank my doctoral advisor, Darrell Haile, for all of his thoughtful comments and suggestions at various stages of the writing of the paper. Thanks are also dedicated to Adrian Wadsworth and Daniel Krashen for their insightful comments. I am also grateful to Nikolaus Vonessen for his careful reading. Finally, I am grateful to the referee, who helps clarify the work with the suggested approaches for Theorem 4.1 and Theorem 4.6, which extend the results in the earlier version of the paper. This paper is based on my PhD thesis. Extensions of the original results were carried out while I was supported by NSC of Taiwan.

References

[1] S.Y. An, S.Y. Kim, D. Marshall, S. Marshall, W. McCallum, A. Perlis, Jacobians of genus one curves, J. Number Theory 90 (2001) 304–315.
[2] L. Childs, Linearizing of n-ic forms and generalized Clifford algebras, Linear Multilinear Algebra 5 (1978) 267–278.
[3] M. Ciperiani, D. Krashen, Relative Brauer groups of genus 1 curves, preprint, arXiv:math/0701614v2, 2007.
[4] F. DeMeyer, E. Ingraham, Separable Algebras Over Commutative Rings, Lecture Notes in Math., vol. 181, Springer-Verlag, 1971.
[5] Philippe Gille, Tamás Szamuely, Central Simple Algebras and Galois Cohomology, Cambridge Stud. Adv. Math., vol. 101, Cambridge University Press, Cambridge, 2006.
[6] D. Haile, On the Clifford algebra of a binary cubic form, Amer. J. Math. 106 (1984) 1269–1280.
[7] D. Haile, On the Clifford algebras, conjugate splittings, and function fields of curves, Israel Math. Conf. Proc. 1 (1989) 356–361.
[8] D. Haile, On Clifford algebras and conjugate splittings, J. Algebra 139 (1991) 322–335.
[9] D. Haile, When is the Clifford algebra of a binary cubic form split?, J. Algebra 146 (1992) 514–520.
[10] N. Heerema, An algebra determined by a binary cubic form, Duke Math. J. 21 (1954) 423–444.
[11] R.S. Kulkarni, On the Clifford algebra of a binary form, Trans. Amer. J. Math. 355 (2003) 3181–3208.
[12] J.-M. Kuo, The Clifford algebra of a cubic form, PhD thesis, Indiana University, 2008.
[13] H. Matsumura, Commutative Ring Theory, Cambridge Stud. Adv. Math., vol. 8, Cambridge University Press, 1989.
[14] P. Revoy, Algèbres de Clifford et algèbres extérleures, J. Algebra 46 (1977) 268–277.
[15] N. Roby, Algèbres de Clifford des formes polynomes, C. K. Acad. Sci. Paris A 268 (1969) 484–486.
[16] L.H. Rowen, Ring Theory, vol. II, Pure Appl. Math., vol. 128, Academic Press, Inc., 1988.
[17] M. Van den Bergh, Linearisations of binary and ternary forms, J. Algebra 109 (1987) 172–183.