ON DIVISION ALGEBRAS OF DEGREE 3 WITH INVOLUTION

BY D. HAILE* AND M.-A. KNUS

Introduction. Let D be a division algebra of degree 3 over its center K and let J be an involution of the second kind on D. Let F be the subfield of K of elements invariant under J. We assume that $\mathrm{char} F \neq 3$. In the first part of this note we present a simple proof of Albert's Theorem ([A$_2$]) on the existence of a maximal subfield of D which is Galois over F with group $\mathcal{S}_3$. The first step is a construction of a subspace of elements u such that $u^3 \in F$, inspired by a similar contruction in [H$_2$] (for algebras without involution). This construction was used there to give a short elementary proof of Wedderburn's Theorem ([W]) that central division algebras of degree 3 are cyclic. In fact the argument given here yields another proof of Wedderburn's Theorem.

In [W] Wedderburn, in preparation for his result on the cyclicity of algebras of degree 3, proves that if θ is a noncentral element of D with minimal polynomial $f(X)$ (say), then there is an element $\xi \in D^\times$ such that $\xi^3 \in K$ and $f(X) = (X - \xi^{-2}\theta\xi^2)(X - \xi^{-1}\theta\xi^1)(X - \theta)$. In part 2 we prove an analogous theorem for the elements of D symmetric under J. In part 3 we apply these results to the theory of Clifford algebras. We prove that every central simple algebra of degree 3 with involution of the second kind is a homomorphic image (as algebra with involution) of the Clifford algebra of some binary cubic form with its canonical involution and then show how to classify these images for a given form.

Albert's Theorem. Let D, K, F and J be as above and let $S = (D, J)_+$ be the F-subspace of symmetric elements. Let $P_a(X)$ be the reduced characteristic polynomial of $a \in D$, let Tr be the reduced trace and N the reduced norm on D. By passing to the algebraic closure of K one easily verifies the following formula for $P_a(X)$:

$$P_a(X) = X^3 - \mathrm{Tr}(a)X^2 + \mathrm{N}(a)\mathrm{Tr}(a^{-1})X - \mathrm{N}(a)1.$$

If $a \notin K$ then $P_a(X)$ is irreducible and the minimal polynomial of a over K. It follows that $P_a^J(X) = P_{J(a)}(X)$. In particular J commutes with Tr and N and if $a \in S$, then $P_a(X) \in F[X]$.

We begin with an analog for algebras with involution of the Proposition, p. 317, in [H$_2$].

PROPOSITION 1. *Let L be a separable cubic extension of F contained in S.*
(1) There exists $d \in S \cap D^\times$ such that $\mathrm{Tr}(Ld) = 0$.

* This research was done while the first author was a visitor at the ETH, Zürich. He would like to thank the Forschungsinstitut für Mathematik for its hospitality.

(2) For d as in (1), the space $U = d^{-1}L \cap \mathrm{Ker\,Tr} = \{d^{-1}\ell \mid \ell \in L \text{ and } \mathrm{Tr}(d^{-1}\ell) = 0\}$ *is at least 2-dimensional over F and* $\mathrm{Tr}(u) = \mathrm{Tr}(u^{-1}) = 0$ *for all $u \in U \cap D^{\times}$.*
(3) The map $J' = Int(d^{-1}) \circ J$ is an involution of second kind on D and U is contained in $(D, \mathrm{Int}(d^{-1}) \circ J)_{+}$.
(4) We have $u^3 = \mathrm{N}(u) \in F$ for all $u \in U$.

Proof: The proof is very similar to the proof of the result of [H_2] mentioned above. For any $x \in S$, the form $f(x)(\ell) = \mathrm{Tr}(\ell x)$ has values in F since $J(\mathrm{Tr}(\ell x)) = \mathrm{Tr}(JxJ\ell) = \mathrm{Tr}(x\ell) = \mathrm{Tr}(\ell x)$. Thus we get an F-linear map $S \to L^*$, $x \mapsto f(x)$. Since $\dim_F S > \dim_F L$, there is an element d as wanted. For (2), since the form $\ell \mapsto \mathrm{Tr}(d^{-1}\ell)$ has values in F, we obviously have $\dim_F U \geq 2$ and, by the choice of d,

$$\mathrm{Tr}(d^{-1}\ell) = \mathrm{Tr}(\ell^{-1}d) = 0 \text{ for all } d^{-1}\ell \in U \cap D^{\times}.$$

To prove (3) note that $J(d^{-1}) = d^{-1}$. It follows that $Int(d^{-1}) \circ J$ is an involution of second kind on D and that the space of fixed elements under $Int(d^{-1}) \circ J$ is $d^{-1}S \supset U$. Finally we prove (4): Because the element u is fixed by the involution J', the argument presented immediately preceding the statement of the proposition shows that $P_u(X) \in F[X]$. Using the explicit form of $P_u(X)$ given there it follows from (2) that $u^3 = \mathrm{N}(u) \in F$, as desired. $\square$

Let $D[X] = D \otimes_F F[X]$. For any $\xi \in D^{\times}$, $\theta \in D$, we have

$$X - \xi^{-i}\theta\xi^{i} = \xi^{-1-i}(\xi X - \xi\theta)\xi^{i}.$$

Thus

$$(*) \qquad (X - \xi^{-2}\theta\xi^{2})(X - \xi^{-1}\theta\xi^{1})(X - \theta) = \xi^{-3}(\xi X - \xi\theta)^{3}.$$

We apply this formula to the elements $\xi = w_1$ and $\theta = w_1^{-1}w_2$, where $w_1, w_2 \in U$ are linearly independent over F. We obtain:

$$(**) \qquad (w_1 X - w_2)^3 = w_1^3(X - w_1^{-2}\theta w_1^2)(X - w_1^{-1}\theta w_1)(X - \theta).$$

LEMMA 2. *Let $\theta_1 = \theta = w_1^{-1}w_2$, $\theta_2 = w_1^{-1}\theta_1 w_1$ and $\theta_3 = w_1^{-1}\theta_2 w_1$. Then*
(1) $\mathrm{Int}(w_1^{-1})(\theta_i) = \theta_{i+1}$, i mod 3, and

$$w_1^{-3}(w_1 X - w_2)^3 = (X - \theta_3)(X - \theta_2)(X - \theta_1)$$

is the reduced characteristic polynomial of θ_i, i=1, 2, 3.
(2) $\mathrm{Tr}(\theta_i) = \theta_1 + \theta_2 + \theta_3$ and $\mathrm{N}(\theta_i) = \theta_{i+2}\theta_{i+1}\theta_i = w_1^{-3}w_2^3$.
(3) For the involution $J' = \mathrm{Int}(d^{-1}) \circ J$, where d is as in Proposition 1, we have $J'(\theta_2) = \theta_2$ and $J'(\theta_1) = \theta_3$.
(4) There exist $w_1, w_2 \in U$ linearly independent over F such that $\mathrm{Tr}(w_1^{-1}w_2) = 0$. For such a choice we have $\theta_1 + \theta_2 + \theta_3 = 0$.

Proof: The first part of (1) is clear. By Proposition 1, (4), $(w_1\alpha - w_2)^3 \in F$ for all $\alpha \in F$. Since the field F is infinite it follows that $(w_1X - w_2)^3 \in F[X]$. Because θ_1 is a root of the right hand side of $(**)$ we get the desired formula for its reduced characteristic polynomial. Thus $\mathrm{Tr}(\theta_1) = \theta_3 + \theta_2 + \theta_1$ and $\mathrm{N}(\theta_1) = \theta_3\theta_2\theta_1 = w_1^{-3}w_2^3$. Conjugating with w_1^{-i}, $i = 1, 2$, gives the other formulae of (2). The claims in (3) follow from $\theta_2 = w_1^{-3}(w_1w_2w_1)$, $\theta_1 = w_1^{-3}(w_1^2w_2)$ and $\theta_3 = w_1^{-3}(w_2w_1^2)$, because J' fixes U by Propostion 1, (3). Finally we check (4). Let w_1 be a nonzero element of U. The form $x \mapsto \mathrm{Tr}(w_1x)$ on U has values in F. Since U is at least 2–dimensional, there exists $w_2 \neq 0 \in U$ with $\mathrm{Tr}(w_1^{-1}w_2) = 0$. Since $\mathrm{Tr}(\lambda) = 3\lambda \neq 0$ for $\lambda \neq 0 \in F$, w_1 and w_2 are linearly independent over F. It then follows from (2) that $\theta_1 + \theta_2 + \theta_3 = 0$. $\square$

To prove Albert's theorem we begin with a separable cubic extension of F contained in S (for example the F–subalgebra generated by any noncentral element of S). We then obtain a space U as in Proposition 1 and choose linearly independent elements $w_1, w_2 \in U$ with $\mathrm{Tr}(w_1^{-1}w_2) = 0$, as in Lemma 2, (4). We then let $\theta_1 = \theta = w_1^{-1}w_2$, $\theta_2 = w_1^{-1}\theta_1w_1$ and $\theta_3 = w_1^{-1}\theta_2w_1$ as in Lemma 2.

THEOREM 3. *Let $E = K(\theta_2^{-1}\theta_3)$ if $\theta_2^{-1}\theta_3 \notin K$ or $E = K(\theta_2)$ if $\theta_2^{-1}\theta_3 \in K$. Then $E \subset D$ is cyclic over K and is a Galois extension over F with group $\mathcal{S}_3$.*

Proof: Assume first that $\theta_2^{-1}\theta_3 \notin K$, so that $\dim_K K(\theta_2^{-1}\theta_3) = 3$. Since

$$\mathrm{Int}(w_1^{-1})(\theta_2^{-1}\theta_3) = \theta_3^{-1}\theta_1 = -\theta_3^{-1}(\theta_3 + \theta_2) = -1 - (\theta_2^{-1}\theta_3)^{-1} \in K(\theta_2^{-1}\theta_3),$$

$\mathrm{Int}(w_1^{-1})$ restricts to a K-automorphism ρ of $K(\theta_2^{-1}\theta_3)$. If ρ is the identity, the element $\theta_2^{-1}\theta_3$ satisfies the equation $y^2 + y + 1 = 0$. The algebra D being of degree 3, this implies that $\theta_2^{-1}\theta_3 \in K$, in contradiction to the assumption. Thus ρ is nontrivial of order 3. We further have for the involution J' given in Lemma 2

$$J'(\theta_2^{-1}\theta_3) = \theta_1\theta_2^{-1} = \theta_2(\theta_2^{-1}\theta_1)\theta_2^{-1} = -\theta_2(1 + \theta_2^{-1}\theta_3)\theta_2^{-1}$$

so the involution $J'' = \mathrm{Int}(\theta_2^{-1}) \circ J'$ satisfies $J''(\theta_2^{-1}\theta_3) = -(1 + \theta_2^{-1}\theta_3)$ and so defines an automorphism of order 2 of $K(\theta_2^{-1}\theta_3)$. To show that $\mathrm{Int}(w_1^{-1})$ and J'' generate a group isomorphic to $\mathcal{S}_3$, it suffices to verify that $J'' \circ \mathrm{Int}(w_1^{-1}) = \mathrm{Int}(w_1^{-2}) \circ J''$. We check it on the generator $\theta_2^{-1}\theta_3$:

$$J'' \circ \mathrm{Int}(w_1^{-1})(\theta_2^{-1}\theta_3) = (\theta_2^{-1}\theta_3)(\theta_1^{-1}\theta_2) = (\theta_1^{-1}\theta_2)(\theta_2^{-1}\theta_3) = \theta_1^{-1}\theta_3$$

where the next to last equality follows from the fact that $\theta_1^{-1}\theta_2 = \mathrm{Int}(w_1^{-2})(\theta_2^{-1}\theta_3) \in K(\theta_2^{-1}\theta_3)$ and so commutes with $\theta_2^{-1}\theta_3$. On the other hand we have

$$\mathrm{Int}(w_1^{-2}) \circ J''(\theta_2^{-1}\theta_3) = \mathrm{Int}(w_1^{-2}\theta_2^{-1}) \circ J'(\theta_2^{-1}\theta_3) = \theta_1^{-1}\theta_3$$

as claimed.

Assume now that $\theta_2^{-1}\theta_3 = y \in K$. By Lemma 2, (2), we must have $y^3 = 1$. If $y = 1$, we get $\theta_2 = \theta_3 = \theta_1$, a contradiction to $\theta_2 + \theta_3 + \theta_1 = 0$. Thus $y \in K$ is a primitive cubic root of 1. It follows from $\theta_3 = y\theta_2$ that $\theta_1 = y\theta_3$ and $\theta_2 = y\theta_1$. Thus

$\mathrm{N}(\theta_2) = \theta_1\theta_3\theta_2 = \theta_2^3$ and $\theta_2^3 \in K$. Since $J'(\theta_2) = \theta_2$, we even have $\theta_2^3 \in F$. Further we deduce from $J'(\theta_1) = \theta_3$ and $\theta_1 = y\theta_3$ that $\theta_3 = J'(y)\theta_1$, so that $J'(y) = y^2$ and $K = F(y)$. Thus we have $K(\theta_2) = K(\theta_3) = K(\theta_1)$ and the restriction ρ of $\mathrm{Int}(w_1^{-1})$ to $K(\theta_2)$ is given by $\theta_2 \mapsto \theta_3 = y\theta_2$. It is then easy to check that $\{J', \rho\}$ generates a group of automorphisms of $K(\theta_2)$ isomorphic to $\mathcal{S}_3$. □

Remarks. (1) The argument used in the proof of Theorem 3 is largely inspired by the very last part of Albert's proof in ([A$_2$]). The use of Lemma 2 allows to avoid most of the computations in the first part of his proof.
(2) As we remarked in the introduction the analog of Proposition 1 given in [H$_2$] is used to give a proof of Wedderburn's Theorem on the cyclicity of a central division algebra of degree 3 (without involution) over K. In fact, Albert's Theorem also holds (with the same proof) for D of the form $A \times A^{\mathrm{op}}$, A a central division algebra over F with the twist involution, so that Wedderburn's Theorem can be viewed a special case of Albert's Theorem. Thus we get another elementary proof of Wedderburn's Theorem. A similar remark applies to the next proposition.

Wedderburn Factorization of symmetric elements. Let D, K, J, S and F be as above. We want to show that one can obtain the full "symmetric" version of Wedderburn's Factorization Theorem (described in the introduction).

Proposition 4. *Let $\theta \in D - F$ with minimal polynomial $f \in F[X]$. There is an involution J' on D such that $\theta \in S' = (D, J')_+$ and there is an element $\xi \in S'$ such that $\xi^3 \in F^\times$ and*

$$f(X) = (X - \xi^{-2}\theta\xi^2)(X - \xi^{-1}\theta\xi^1)(X - \theta).$$

Proof: We first show there is an involution fixing θ. This is a special case of a result of Albert ([A$_1$],p. 157). For completeness we provide a proof. The elements θ and $J(\theta)$ have the same minimal polynomials, hence are conjugates in D. Let $J(\theta) = \mathrm{Int}(g)(\theta)$. If $g + J(g) \neq 0$, then $\mathrm{Int}(g + J(g))(\theta) = J(\theta)$ and so the involution $J'' = \mathrm{Int}((g + J(g))^{-1}) \circ J$ fixes θ. If $g = -J(g)$, then $J'' = \mathrm{Int}(g^{-1}) \circ J$ fixes θ.

We proceed as in the proof of Proposition 1 to find a 2–dimensional subspace W of $L = F(\theta) \subset S'' = (D, J'')_+$ and $d \in S'' \cap D^\times$ such that $y^3 \in F$ for all $y \in d^{-1}W$. Let $Y = F + F\theta \subset L$. We claim that there exists $\ell \in L$ such that $\ell W = Y$. In fact it was shown in [H$_2$] that for any 2-dimensional subspaces U_1 and U_2 of L, there is $\ell \in L$ such that $\ell U_1 = U_2$. Again for completeness we recall the argument: let $f, g \in L^*$ be such that $U_1 = \mathrm{Ker}\ f$ and $U_2 = \mathrm{Ker}\ g$. The claim then follows from the fact that L^* is a 1–dimensional L–space (through the operation $(f\ell)(x) = f(\ell x)$). So let $\ell \in L$ be such that $\ell W = Y$ and let $\xi = (\ell d)^{-1}$; then $\xi Y = d^{-1}\ell^{-1}Y = d^{-1}W$, so that $x^3 \in F$ for all $x \in \xi Y$. As in the proof of Lemma 2, (1), it follows that $(\xi X - \xi\theta)^3 \in F[X]$ and hence, applying $(*)$, that $(X - \xi^{-2}\theta\xi^2)(X - \xi^{-1}\theta\xi^1)(X - \theta)$ is the reduced characteristic polynomial of θ. It follows that $f(X) = (X - \xi^{-2}\theta\xi^2)(X - \xi^{-1}\theta\xi^1)(X - \theta)$. Moreover $J' = \mathrm{Int}(\ell) \circ J''$ fixes θ and ξ. □

Clifford Algebras. The foregoing results may be applied to the theory of Clifford algebras of binary cubic forms. Recall that if $g(u_1, \ldots, u_m)$ is a form of degree d in m

variables over a field F, then the Clifford algebra C_g of g is the algebra $F\{X_1,\ldots,X_m\}/I$ where $F\{X_1,\ldots,X_m\}$ is the free algebra on m variables and I is the ideal generated by the set

$$\{(\alpha_1 X_1+\ldots\alpha_m X_m)^d - g(\alpha_1,\ldots,\alpha_m),\ \alpha_1,\ldots,\alpha_m\in F\}$$

(See Roby [Ro], Revoy [Re_1], Childs [C]). If g is a binary cubic form it has been shown (Heerema [He], Revoy [Re_2], Haile [H_1]) that C_g is an Azumaya algebra over its center Z and that Z is isomorphic to the affine coordinate ring $F[E]$ of the elliptic curve E given by the equation $S^2=R^3-27\delta$ where $\delta\in F$ is the discriminant of g. In particular each simple image A of C_g is of degree 3 over its center and the simple images with center F are in one-to-one correspondence with the F-rational points on E. This correspondence gives rise to a function from $E(F)$, the group of F-rational points on E, to $B(F)$, the Brauer group of F, and it is shown in Haile [H_1], that this map is a group homomorphism.

Now let $g(u,v)$ be a binary cubic form over F. The free algebra $F\{X,Y\}$ admits a unique involution fixing X and Y and this involution preserves I. We let $*$ denote the induced involution on C_g and call it the *canonical* involution on C_g.

PROPOSITION 5. Let A be a simple algebra of degree 3 with involution of the second kind having fixed field F. There is an involution J on A and a binary form $g(u,v)$ over F such that (A,J) is a homomorphic image of $(C_g,*)$. Moreover, if A is a division algebra and $f(x)\in F[x]$ is irreducible of degree 3 with a root $\theta\in D$, then there is an element $a\in F^\times$ and an involution J on D such that $(C_g,*)$ maps onto (D,J), where $g(u,v)=av^3f(u/v)$.

Proof: Let K denote the center of A. First assume A is a division algebra. By Proposition 4 there is a involution J' such that $J'(\theta)=\theta$ and an element $\xi\in A$ fixed by J' such that $\xi^3=a\in F^\times$ and

$$f(X)=(X-\xi^{-2}\theta\xi^2)(X-\xi^{-1}\theta\xi^1)(X-\theta)=a^{-1}(\xi X-\xi\theta)^3.$$

Hence the binary cubic form $g(u,v)=av^3f(u/v)$ satisfies $g(u,v)=(u\xi+v(-\xi\theta))^3\in A[u,v]$. If we let $J=\mathrm{Int}(\xi)\circ J'$, then $J(\xi)=\xi$, $J(\xi\theta)=\xi\theta$. Hence the map $X\mapsto\xi$, $Y\mapsto\xi\theta$ induces a homomorphism from $(C_g,*)$ onto (A,J).

If $A=M_3(K)$, let $J'=\mathrm{Int}(u)\circ\tau$ with $u=\mathrm{diag}(1,\left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right))$, $\tau(x_{ij})=(\bar{x}_{ij})^t$, where $x\mapsto\bar{x}$ is conjugation in K and t is transpose. If $K=F(\beta)$ with $\beta^2=a$, let $g(u,v)=(u-v)(u^2-av^2)$. There is a homomorphism ϕ of $(C_g,*)$ onto $(M_3(K),J)$ sending

$$X \quad\text{to}\quad \begin{pmatrix}0&0&1\\1&0&0\\0&1&0\end{pmatrix} \quad\text{and}\quad Y\quad\text{to}\quad \begin{pmatrix}0&0&-\beta\\1&0&0\\0&\beta&0\end{pmatrix},$$

where $J=\mathrm{Int}(\phi(X))\circ J'$. □

If A is a simple image of C_g arising from the maximal ideal m of Z then $*$ will induce an involution on A if and only if $m^*=m$. Moreover, because the center of A is Z/m we see that the fixed field of $*$ on A is F if and only if m has residue degree 2. In fact we can describe such maximal ideals quite precisely:

THEOREM 6. The simple images of C_g on which $*$ induces an involution of the second kind with fixed field F are in one to one correspondence with the pairs of points $(r, \pm s)$ on the curve $S^2 = R^3 - 27\delta$ such that $r \in F, s \notin F$. The center of the resulting algebra is $F(s)$, a quadratic extension of F.

Proof: Let $C_g = F\{X, Y\}/I$. We use the results of the discussion beginning section 2 of [H$_3$]. By making a linear change of variables we may assume that $g(u, v) = au^3 + 3cuv^2 + dv^3$ in $F[u, v]$. Let $r = ac, 2s = ad, t = -c^2$, and $\delta = s^2 - rt = \frac{a^2d^2}{4} + ac^3$, the discriminant of g. Let $L = F[\sqrt{\delta}, \omega]$ where ω is a primitive third root of one. Let $\overline{X} = (\sqrt{\delta}+s)X - rY$ and $\overline{Y} = (\sqrt{\delta}-s)X + rY$ in $C_g \otimes_F L$, the Clifford algebra of g over L. If we let $\mu = \overline{Y}\,\overline{X} - \omega\overline{X}\,\overline{Y}$ and $\nu = \overline{Y}\,\overline{X} - \omega^2\overline{X}\,\overline{Y}$, then the elements $\mu\nu$, $\sqrt{\delta}(\mu^3+\nu^3)$ are in C_g and $Z = F[\mu\nu, \sqrt{\delta}(\mu^3+\nu^3)]$. Morever Z is isomorphic to the coordinate ring of $E : S^2 = R^3 - 27\delta$ via the map

$$R \mapsto \frac{\mu\nu}{4r^2\delta}, \quad S \mapsto \frac{\sqrt{\delta}(\mu^3 + \nu^3)}{16r^3\delta^2}.$$

Now the map $* \otimes 1$ is the canonical involution on $C_g \otimes L$ and an easy computation shows that $\mu^{*\otimes 1} = -\omega\nu$. It follows that $\mu\nu$ in C_g is fixed by $*$. Hence the action of $*$ on $Z = F[E]$ is given by $R^* = R$ and $S^* = -S$.

Now let A be a simple image of C_g on which $*$ induces an involution of second kind with fixed field F. As we have seen $A = C_g/mC_g$ where m is a maximal ideal of Z of residue degree 2 such that $m^* = m$. Let $K = Z/m$. The involution $*$ induces the nontrivial automorphism of K over F. Hence in the coordinate ring $K[E]$ there are 2 maximal ideals lying over m in $F[E]$. These maximal ideals are given by K-rational points and are conjugate under $*$. If (r, s) is one such point we have seen that $r^* = r$ and $s^* = -s$. Hence $r \in F, s \notin F$ and $K = F(s)$.

Conversely, if (r, s) is a point on E such that $r \in F, s \notin F$ then $K = F(s)$ is a quadratic extension of F. Moreover $(r, -s)$ is another point on E and these two points lie over the same maximal ideal m of $F[E]$. Clearly $m^* = m$ and m has residue degree 2, so, as we have seen, $*$ induces an involution of the second kind on C_g/mC_g with fixed field F. □

COROLLARY 7. Let $K = F(\gamma), \gamma^2 \in F$ be a quadratic extension of F. The simple images of C_g with center K on which $*$ induces an involution of second kind with fixed field F are in one to one correspondence with the pairs $(\alpha, \pm\beta)$ of F–rational points on the elliptic curve $S^2 = R^3 - 27(\delta/\gamma^3)$.

Proof: By the theorem the simple images of C_g with center K on which $*$ induces an involution of second kind with fixed field F are in one to one correspondence with the pairs of points $(r, \pm s)$ on the curve $S^2 = R^3 - 27\delta$ such that $r \in F$ and $F(s) = K$. Since $s^2 = r^3 - 27\delta \in F$, it follows that $s/\gamma \in F$. But then the points $(r/\gamma^2, \pm s/\gamma^3)$ are F–rational and lie on $S^2 = R^3 - 27(\delta/\gamma^3)$. Conversely if $(\alpha, \pm\beta)$ are F–rational points on $S^2 = R^3 - 27(\delta/\gamma^3)$, then the points $(\alpha\gamma^2, \pm\beta\gamma^3)$ lie on $S^2 = R^3 - 27\delta$ and satisfy $\alpha\gamma^2 \in F$, $F(\beta\gamma^3) = K$. □

References

[A_1] A.A. Albert, *Structure of Algebras*, Colloqium Publ. 24, Amer. Math. Soc. New York, 1939

[A_2] A.A. Albert, On involutorial associative division algebras, Scripta Mathematica 26 (1963), 309-316

[C] L. Childs, Linearizing of n-ic forms and generalized Clifford algebras, Linear and Multilinear Alg. 5 (1978), 267-278

[H_1] D.E. Haile, On the Clifford algebra of a binary cubic form, Amer. J. Math. 106 (1984), 12-69-1280

[H_2] D.E. Haile, A useful proposition for division algebras of small degree, Proc. Amer. Math. Soc. 106 (1989), 317-319

[H_3] D.E. Haile, On Clifford algebras and conjugate splittings, J. Algebra 139 (1991), 322-335

[He] N. Heerema, An algebra determined by a binary cubic form, Duke Math. J. 21 (1954), 423-444

[Re_1] Ph. Revoy, Algèbres de Clifford et algèbres extérieures, C.R. Acad. Sci. Paris 277A (1973), 655-657

[Re_1] Ph. Revoy, Sur certaines algèbres de Clifford, Communications in Alg. 11 (1983), 1877-1891

[Ro] N. Roby, Algèbres de Cliford des formes polynômes, C.R. Acad. Paris 268A (1969), 484-486

[W] J.H.M. Wedderburn, On division algebras, Trans. Amer. Math. Soc. (1921), 129-135

Darrell E. Haile
Department of Mathematics
Indiana University
Bloomington, IN 47405
USA
haile ucs.indiana.edu

Max-Albert Knus
Departement Mathematik
ETH-Zentrum
CH-8092 Zürich
Switzerland
knus math.ethz.ch