Reprinted from JOURNAL OF ALGEBRA
All Rights Reserved by Academic Press, New York and London

Vol. 12, No. 3, July, 1969
Printed in Belgium

Automorphisms of Cayley Algebras

MARIA J. WONENBURGER

Department of Mathematics, Indiana University, Bloomington, Indiana 47401

Communicated by Nathan Jacobson

Received October 30, 1968

DEDICATED TO THE MEMORY OF PROFESSOR
OYSTEIN ORE

The purpose of this paper is to study the decomposition of automorphisms of Cayley algebras into products of the simplest kind of automorphisms, namely, the involutory automorphisms or automorphisms of period 2. When the base field is algebrically closed of characteristic not 2 or 3, it is shown that any automorphism is the product of two involutory automorphisms (Th. 4). This result is not true for any field (Th. 3), but, if the characteristic is not 2 or 3, then any automorphism can be expressed as the product of at most 3 involutory automorphisms.

We take as a starting point N. Jacobson's study [*2*]. The reader should refer to it for the well-known results about Cayley algebras and their automorphisms that we use. The properties of Cayley algebras can also be found in [*3*].

1. A Cayley algebra C over a field F is a simple alternative algebra of dimension 8, with an identity element 1 and an involution $-$, that is, an antiautomorphism of period 2. For any $x \in C$, $x\bar{x} = \alpha 1$ where $\alpha \in F$ and the function $N(x) = \alpha$ defines a nondegenerate quadratic form with the property $N(xy) = N(x)N(y)$.

From now on we will always assume that char $F \neq 2$. So we define the bilinear form associated to N by

$$(x, y) = (1/2)(N(x + y) - N(x) - N(y)).$$

If the quadratic from has Witt index 0, then C is a division algebra. If the index is not 0, then it is equal to 4 and C is called a split Cayley algebra.

A subalgebra Q of dimension 4 is called a quaternion subalgebra if it contains 1 and the restriction of N to Q is nondegenerate, for Q is indeed a generalized quaternion algebra.

An automorphism S of C defines a rotation with respect to the bilinear form (x, y) and since it leaves 1 invariant it induces a rotation on the subspace $C_0 = (F1)^{\perp}$ the orthogonal complement of $F1$. If $S^2 = 1$, the identity mapping, but $S \neq 1$, the elements $Q = \{x \in C \mid xS = x\}$ form a quaternion subalgebra, then $C = Q \oplus Q^{\perp}$ and the orthogonal complement $Q^{\perp} = vQ$, where v is any non-isotropic vector of $Q^{\perp}$. Conversely, if Q is a quaternion subalgebra the rotation which induces the identity mapping on Q and takes the element of $Q^{\perp}$ into their negatives is an involutory automorphism of C. We will denote this automorphism by $\underset{\sim}{Q}$.

THEOREM 1. *Let C be a Cayley algebra. If S is an automorphism of C which maps a quaternion subalgebra Q into itself, then S is the product of two involutory automorphisms.*

Proof. Write $C = Q \oplus Q^{\perp}$. Since S induces an automorphism in Q, it induces a rotation in $Q^{\perp}$. Such a rotation can be decomposed into the product of two involutons H_1H_2, where H_i is the rotation of $Q^{\perp}$ which leaves invariant the vectors of a non-degenerate plane (see [5], Th. 2). Let u_i, v_i be an orthogonal basis of this plane and let Q_i be the quaternion subalgebra spanned by $1, u_i, v_i, u_iv$. Since $u_iv_i \in Q$, $\underset{\sim}{Q}_i$ agrees with H_i on $Q^{\perp}$. Hence $S = \underset{\sim}{Q}_1\underset{\sim}{Q}_2$.

COROLLARY 1. *If an automorphism S of C leaves invariant a nondegenerate plane of C_0, then it is the product of two involutory automorphisms.*

Proof. If u_1, u_2 is an orthogonal basis of the invariant nondegenerate plane

$$\begin{aligned}(u_1u_2)S &= (u_1S)(u_2S) = (\alpha_{11}u_1 + \alpha_{12}u_2)(\alpha_{21}u_1 + \alpha_{22}u_2)\\ &= (\alpha_{11}\alpha_{22} - \alpha_{12}\alpha_{21})\, u_1u_2 .\end{aligned}$$

Therefore S leaves invariant the quaternion subalgebra spanned by $1, u_1, u_2, u_1u_2$.

Since any orthogonal transformation of an anisotropic space of dimension $n \geqslant 2$ over a real closed field leaves invariant a plane, we have proved

COROLLARY 2. *If C is a Cayley division algebra over a real closed field, any automorphism of C is the product of two involutory automorphisms.*

2. To deal with split Cayley algebras we find it useful to work with standard bases. For the convenience of the reader we proceed to obtain one. First, let us recall that if a_1, a_2 are two orthogonal non-isotropic vectors in C_0 and $a_3 \in Q^{\perp}$, where Q is the quaternion subalgebra spanned by $1, a_1, a_2, a_1a_2$, then $(a_1a_2)a_3 = -a_1(a_2a_3)$.

Let z be a vector in C_0 such that $N(z) = -1$, that is, such that $\frac{1}{2}(1 - z)$ and $\frac{1}{2}(1 + z)$ are idempotents. If v_i is any non-isotropic vector of C_0 orthogonal to z, the subspace spanned by $1, z, v_1, v_1z$ is a split quaternion subalgebra Q and the vectors $u_1 = v_1 + v_1z$ and $w_1 = v_1 - v_1z$ are isotropic and the product $u_1w_1 = -2N(v_1)(1 - z)$.

Let now v_2 be any non-isotropic vector in $Q^{\perp}$ and $v_3 = 2v_1v_2$. Then z, u_i, w_i, $i = 1, 2, 3$, is a basis of C_0, where $u_i = v_i + v_iz$, $w_i = v_i - v_iz$ are isotropic vectors and $(u_i, w_j) = -2\delta_{ij}N(v_i)$, δ_{ij} being the Kronecker delta. Now, if $i \neq j$,

$$u_iu_j = (v_i + v_iz)(v_j + v_jz) = 2v_iv_j - 2(v_iv_j)z.$$

Choosing $N(v_1) = N(v_2) = 1/4$, which is always possible, we get $2v_2v_3 = 4v_2(v_1v_2) = v_1$, $2v_3v_1 = 4(v_1v_2)\,v_1 = v_2$. Therefore

$$u_iu_j = \begin{cases} w_k \text{ if } (i, j, k) \text{ is an even permutation of } (1, 2, 3) \\ -w_k \text{ if } (i, j, k) \text{ is an odd permutation of } (1, 2, 3). \end{cases} \tag{1}$$

Changing z into $-z$, we see that

$$w_iw_j = \operatorname{sig}(i, j, k)\, u_k \tag{2}$$

where sig (i, j, k) is the signature of the permutation (i, j, k).

Moreover,

$$u_iw_j = -\tfrac{1}{2}\delta_{ij}(1 - z) \qquad \text{and} \qquad w_iu_j = -\tfrac{1}{2}\delta_{ij}(1 + z) \tag{3}$$

$$u_iz = u_i \qquad \text{and} \qquad w_iz = -w_i . \tag{4}$$

That is, u_1, u_2, u_3, span the 3 dimensional space of C_0 consisting of vectors annihilated by left multiplication by the indempotent $\frac{1}{2}(1 - z)$. Similarly, $[w_1, w_2, w_3]$, the subspace spanned by w_1, w_2, w_3, is the subspace of C_0 annihilate by right multiplication by $(1 - z)$.Hence these subspaces are uniquely determined by z.

Now $(u_i, w_j) = -\frac{1}{2}\delta_{ij}$, and for any $u \in [u_1, u_2, u_3]$ and any $w \in [w_1, w_2, w_3]$, $uw = (u, w)(1 - z)$ and $wu = (u, w)(1 + z)$.

Notice that the subspace $[1, u_1 + w_1, u_2 + w_2, u_3 + w_3] = Z$ is a quaternion subalgebra. The automorphism $\underset{\sim}{Z}$ takes z into $-z$, u_i into w_i, and w_i into u_i.

If an automorphism S of the split Cayley algebra C leaves invariant the vector z it must induce linear transformations in $[u_1, u_2, u_3]$ and $[w_1, w_2, w_3]$. So let

$$u_iS = \Sigma\alpha_{ij}u_j \qquad \text{and} \qquad w_iS = \Sigma\beta_{ij}w_j . \tag{5}$$

Since S induces an orthogonal transformation on the subspace spanned by the u_i, w_i, $i = 1, 2, 3$, we must have that the matrix

$$(\beta_{ij}) = ((\alpha_{ij})^t)^{-1} \tag{6}$$

where $(\alpha_{ij})^t$ denotes the transpose of (α_{ij}).

On the other hand $(u_iS)(u_jS) = \operatorname{sig}(i, j, k,)\, w_kS$ shows that β_{ij} is the cofactor A_{ij} of α_{ij} in (α_{ij}). But from (6) we know that

$$\beta_{ij} = A_{ij}(\det(\alpha_{ij}))^{-1}.$$

Hence $\det(\alpha_{ij}) = 1$. Now it is immediately seen that if $\det(\alpha_{ij}) = 1$, taking (β_{ij}) as in (6), equations (5) together with $1S = 1$, $zS = z$, define an automorphism of C.

Any automorphism T of C which takes z into $-z$ is of the form $S\bar{Z}$. Therefore

$$u_iT = \Sigma\alpha_{ij}w_j , \qquad w_iT = \Sigma\beta_{ij}u_j$$

where the matrices (α_{ij}) and (β_{ij}) are unimodular and satisfy (6). Moreover such automorphism will be involutory if and only if $(\alpha_{ij})(\beta_{ij}) = I$, the identity matrix. Because of (6) this holds if and only if (α_{ij}) is symmetric.

It is well-known that given a matrix A there exists a symmetric matrix S such that $SAS^{-1} = A^t$. Then $AS^{-1} = S^{-1}A^t = (AS^{-1})^t$ is also symmetric, hence $A = (AS^{-1})S$ is the product of two symmetric matrices. Conversely, if $A = S_1S_2$, S_1, S_2 symmetric, then $A^t = S_2S_1 = S_2AS_2^{-1}$. When the minimum polynomial of A equals the characteristic polynomial, any other matrix B such that $BAB^{-1} = A^t$ is of the form $B = Sp(A)$, where $p(A)$ is a polynomial in A, and any such B is symmetric (see [4]).

If T is an automorphism of C, such that $zT = z$, $u_iT = \Sigma\alpha_{ij}u_j$ and we can decompose $A = (\alpha_{ij})$ into the product of two unimodular symmetric matrices, say $A = S_1S_2$, where $S_h = (s_{ij}^h)$, then if $\bar{Q}_j$, $j = 1, 2$, are the involutory automorphisms defined by $z\bar{Q}_j = -z$ and $u_i\bar{Q}_1 = \Sigma s_{ij}^1 w_j$ and $w_i\bar{Q}_2 = \Sigma s_{ij}^2 u_j$, we get $T = \bar{Q}_1\bar{Q}_2$.

THEOREM 2. *Let C be a Cayley algebra over a field K in which every element has a cubic root. Then any automorphism T of C which leaves invariant a vector $z \in C_0$ such that $N(z) = -1$, is the product of two involutory automorphisms.*

Proof. We have just seen that if $u_iT = \Sigma\alpha_{ij}u_j$, we only need to find two unimodular symmetric matrices S_1, S_2 satisfying $S_1S_2 = (\alpha_{ij})$. We know that there always exist two symmetric matrices S_1', S_2' whose product $S_1'S_2' = (\alpha_{ij})$. Since they are nonsingular and in K every element has a cubic root, we take $S_1 = \alpha S_1'$, $S_2 = \alpha^{-1}S_2'$, where $\alpha \in K$ satisfies the condition $\alpha^3 = (\det S_1)^{-1}$.

Suppose that $K = Q(\omega)$ is the quadratic extension of the field of rational numbers Q by a complex cubic root ω of 1. Let A be a 3×3 matrix whose minimum polynomial is $(x - \omega)^3$. Suppose $A = S_1S_2$, the product of two unimodular symmetric matrices, then let $B = CAC^{-1}$, where $C = \operatorname{diag}\{\alpha^{-1}, 1, 1\}$, now $B = (CS_1C)(C^{-1}S_2C^{-1})$ and $\det(C^{-1}S_2C^{-1}) = \alpha^2$. We have recalled above that any other symmetric matrix appearing as the second factor in such decomposition is of the form $C^{-1}S_2C^{-1}p(B)$. Now $\det p(B) = p(\omega)^3$, hence if $x^3 - \alpha^2$ is an irreducible polynomial B *is not the product of two unimodular symmetric matrices*. The same argument can be applied to a finite field F containing a root of $x^2 + x + 1$, since in this case we also have elements $\alpha \in F$ such that $x^3 - \alpha^2$ is an irreducible polynomial in $F[x]$.

THEOREM 3. *For some fields K there exist automorphisms of the split Cayley algebra over K which can not be expressed as the product of two involutory automorphisms.*

Proof. Let K be a field which contains matrices $B = (\beta_{ij})$ as above, that is, have minimum polynomial $(x - \omega)^3$ and are not expressible as the product of two unimodular symmetric matrices. Let T be an automorphism such that $zT = z$, $u_iT = \Sigma\beta_{ij}u_j$. Then $[z]$ is the subspace of C_0 consisting of vectors invariant under T. If $T = \bar{Q}_1\bar{Q}_2$ any vector in $\bar{Q}^{\perp} \cap \bar{Q}_2^{\perp}$ is invariant under T. Since $\dim Q_i^{\perp} = 4$ and $Q_i^{\perp} \subset C_0$ of dimension 7, we have $Q_1^{\perp} \cap Q_2^{\perp} \neq 0$, therefore $Q_1^{\perp} \cap Q_2^{\perp} = [z]$. But then the automorphisms $\bar{Q}_i$ must take z into $-z$ and we have just seen that this, being equivalent to decomposing B into the product of two unimodular symmetric matrices, is impossible.

3. Let us recall now some properties of the orthogonal transformations of a vector space V relative to a nongenerate symmetric bilinear form in char $\neq 2$. If $c(x)$ is the characteristic polynomial of an orthogonal transformation, then any root of $c(x)$ appears with the same multiplicity that its inverse, hence $c(x) = \pm x^n c(x^{-1})$. In [5] departing slightly from the classical terminology we have called such polynomials self-reciprocal. We can factorize $c(x)$ in the form

$$c(x) = (x - 1)^r (x + 1)^{r'}\, p_1(x)^{r_1} \cdots p_h(x)^{r_h}$$

where $p_i(1) \neq 0 \neq p_i(-1)$, the $p_i(x)$ are distinct and irreducible self-reciprocal in the sense that they are self-reciprocal and can not be expressed as the product of two self-reciprocal polynomials. Then the $p_i(x)$ are pairwise coprime and have even degree.

The direct sum decomposition of the vector space into invariant subspaces $V = V_+ \oplus V_- \oplus V_1 \oplus \cdots \oplus V_h$ where the characteristic polynomial of the restriction of the transformation to V_+, V_-, V_i is a power of $x + 1$, $x - 1$, $p_i(x)$ respectively, is an orthogonal direct sum (cf. [5], Corollary to Prop.) If the transformation is a rotation r' is even.

In our case, if S is an automorphism of a Cayley algebra, the restriction of S to C_0 is a rotation and therefore $r = 1, 3, 5$ or 7.

We want to study the automorphisms S with the property that the characteristic polynomial of the restriction of S to C_0 has 1 as a multiple root. We have then three possibilities, namely, $r = 3, 5, 7$. By studying each one of these cases we are going to establish the following theorem.

THEOREM 4. *Let K be any field of* char $\neq 2, 3$. *If S is an automorphism of a Cayley algebra over K, such that the characteristic polynomial of the restriction of S to C_0 is divisible by $(x - 1)^2$, then S is the product of two involutory automorphisms.*

Case 1. $r = 3$. Then the subspace V_+ is a nondegenerate 3 dimensional space. The invariant factors of the restriction of S to V_+ must have one of the following forms,

(a) $x - 1, x - 1, x - 1$

(*b*) $(x - 1)^2, x - 1$

(c) $(x - 1)^3$.

If (a) holds V_+ consist of invariant vectors and by Corollary 1 to Theorem 1, $S = \bar{Q}_1\bar{Q}_2$.

(b) is impossible, because then S induces in V_+ a rotation which leaves invariant every vector of a hyperplane, hence it must be the identity (see [*1*], Th. 3.17).

Assume then that $(x - 1)^3$ is the minimum plynomial. Then we will show that the subspace $K.1 \oplus V_+$ is a quaternion subalgebra, therefore by Th. 1 $S = \bar{Q}_1\bar{Q}_2$.

Choosing an appropriate basis in V_+ we have

$$uS = u, \qquad zS = z + \alpha u, \qquad vS = v + \beta z + \gamma u$$

where u and v form a hyperbolic pair and Kz is the orthogonal complement in V_+ of $[u, v]$ (see [*1*], p. 133).

Now $(uz)S = u(z + \alpha u) = uz$. Hence $uz = \delta u$. Also

$$(uv)S = u(v + \beta z + \gamma u) = uv + \beta uz,$$

that is, $(uv)(S - 1)^2 = 0$; therefore $uv \in K.1 + V_+$. Finally

$$(zv)S = (z + \alpha u)(v + \beta z + \gamma u) = zv + \alpha uv + \beta z^2 + (\alpha - \gamma)\, uz,$$

which implies that $(zv)(S - 1)^3 = 0$. Hence $zv \in K1 \oplus V_+$ and this subspace is a quaternion subalgebra.

Case 2. $r = 5$. Then the orthogonal complement in C_0 of V_+ is a nondegenerate invariant plane, thus by Cor. 1 to Th. 1, $S = \bar{Q}_1\bar{Q}_2$. A closer study will show that this case can *not* appear.

Case 3. $r = 7$. To dispose of this case we are going to divide it into two subcases.

(a) $(x - 1)^7$ is the minimum polynomial of the restriction of S to C_0.

(b) $(x - 1)^7$ is not the minimum polynomial.

Let us take subcase (a). Notice first that the subspace of invariant vectors of C_0 has dimension 1 and must be isotropic. We may assume that $u_1S = u_1$, where u_1 belongs to a standard basis.

If u_{1r} denotes the linear transformation of C, $u_{1r} : y \to yu_1$, we see that its kernel is $[u_1, w_2, w_3, 1 - z]$ and $\operatorname{Ker} u_{1r} \cap C_0 = [u_1, w_2, w_3]$. Since $u_1S = u_1$, these subspaces are invariant under S, therefore $[u_1, w_2, w_3]$ and $[u_1, w_2, w_3, z]$ are the kernels of the transformations $(S - 1)^3$ and $(S - 1)^4$ restricted to C_0.

We want to take a standard basis adapted to our transformation. For this purpose let w_3' be any element of $\operatorname{Ker}(S - 1)^3$ not in $\operatorname{Ker}(S - 1)^2$ and write $w_3'S = w_3' + w_2'$, $w_2'S = w_2' + u'$. Then $u'S = u'$ and $w_2'w_3' = \alpha u' \neq 0$. We define a new basis where $w_3 = \alpha^{-1}w_3'$, $w_2 = \alpha^{-1}w_2'$, $u_1 = \alpha^{-1}u$. Then $w_2w_3 = u_1$ and $u_1S = u_1$, $w_2S = w_2 + u_1$, $w_3S = w_3 + w_2$.

We can choose now our $z \in \operatorname{Ker}(S - 1)^4 \cap C_0$ in such a way that $u_1z = u_1$, $w_iz = w_i$ and complete u_1, w_2, w_3, z to a standard basis.

Since S is an automorphism we have

$$(u_1S)(zS) = u_1S, \qquad (w_2S)(zS) = -w_2S, \qquad (w_3S)(zS) = -w_3S$$

which give

$$zS = z - 2w_3 - 2w_2 + 2\delta u_1$$

In the same way we can find, in the order given below

$$\begin{aligned} u_3S &= u_3 - z + w_3 + (1 + \delta)w_2 + \mu u_1 \\ u_2S &= u_2 - u_3 - \delta w_3 - \delta w_2 + \nu u_1 \\ w_1S &= w_1 - u_2 + u_3 - z - (\mu + \delta)w_3 - (\mu + \delta + \nu)w_2 - (\nu + \delta)u_1 \\ &= (u_2S)(u_3S) \end{aligned}$$

Now if we try to decompose S into $\bar{Q}_1\bar{Q}_2$ we know that $[u] = Q_1^{\perp} \cap Q_2^{\perp}$, hence $u\bar{Q}_i = -u$. An automorphism which takes u into $-u$ must leave invariant the subspaces $[u, w_2, w_3]$ and $[u, w_2, w_3, z]$. Hence the restriction of $\bar{Q}_2$ to $[u_1, w_2, w_3]$ relative to this basis has a matrix of the form

$$A = \begin{pmatrix} -1 & 0 & 0 \\ \alpha & \beta & \gamma \\ \alpha' & \beta' & \gamma' \end{pmatrix} \qquad \text{with} \qquad A^2 = I$$

Moreover, the equation $w_2 w_3 = u_1$ gives

$$(\alpha u_1 + \beta w_2 + \gamma w_3)(\alpha' u_1 + \beta' w_2 + \gamma' w_3) = -u_1$$

which implies $\beta\gamma' - \gamma\beta' = -1$. Hence A must have the characteristic roots $-1, -1, 1$.

So we try the following matrix of square equal 1

$$A = \begin{pmatrix} -1 & 0 & 0 \\ \alpha & 1 & 0 \\ \dfrac{\alpha\beta}{2} & \beta & -1 \end{pmatrix}$$

Since $S\bar{Q}_2 = \bar{Q}_1$ should also be an involution we know that

$$\begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} -1 & 0 & 0 \\ \alpha & 1 & 0 \\ \dfrac{\alpha\beta}{2} & \beta & -1 \end{pmatrix} = \begin{pmatrix} -1 & 0 & 0 \\ \alpha - 1 & 1 & 0 \\ \dfrac{2\alpha + \alpha\beta}{2} & \beta + 1 & -1 \end{pmatrix}$$

must have square equal I. Hence $\beta = -(1 + \alpha)$.

We are going to find first all the automorphisms T of C whose restriction to $[u_1, w_2, w_3]$ relative to this basis is given by the matrix A with $\beta = -(1 + \alpha)$. That is,

$$u_1 T = -u_1, \qquad w_2 T = w_2 + \alpha u_1,$$
$$w_3 T = w_3 - (1 + \alpha) w_2 - \tfrac{1}{2}\alpha(1 + \alpha) u_1$$

As before we can find zT, then $u_3 T$, then $u_2 T$ and finally $w_1 T = (u_2 T)(u_3 T)$. We obtain

$$\begin{aligned} zT &= z - 2\alpha w_3 - \alpha(1 + \alpha) w_2 + D u_1 \\ u_3 T &= -u_3 + \alpha z - \alpha^2 w_3 - \tfrac{1}{2}(D + \alpha^2(1 + \alpha)) w_2 + \beta u_1 \\ u_2 T &= u_2 - (1 + \alpha) u_3 + \frac{1}{2}\alpha(1 + \alpha) z - \frac{1}{2}(D + \alpha^2(1 + \alpha)) w_3 \\ &\quad - \frac{1 + \alpha}{4}(2D + \alpha^2(1 + \alpha)) + \gamma u_1 \end{aligned}$$

Now we want to see for which values of D, β, γ, this T is an involutory automorphism. We get $xT^2 = x$ for $x = u_1, w_2, w_3, z$ and

$$u_3 T^2 = u_3 + (\tfrac{1}{2}\alpha D - 2\beta) u_1 .$$

Hence

$$\beta = \tfrac{1}{4}\alpha D \tag{7}$$

and with this value of β we find $u_2 T^2 = u_2$.

Since α and D can be arbitrary, we want, if possible, to choose them so that $ST = T'$ is also an involutory automorphism.

We already know that $u_1 T' = -u_1$, $w_2 T' = w_2 + (\alpha - 1) u_1$ and $w_3 T' = -w_3 - \alpha w_2 - \frac{1}{2}\alpha(\alpha - 1) u$, and by direct computation we find

$$\begin{aligned} zT' &= z - 2(\alpha - 1) w_3 - \alpha(\alpha - 1) w_2 + (\alpha(\alpha - 1) + D - 2\delta u_1 \\ u_3 T' &= -u_3 + (\alpha - 1) z - (\alpha^2 - 2\alpha + 1) w_3 \\ &\quad - \tfrac{1}{2}(D - 2\delta + \alpha^3 - \alpha^2) w_2 + \tfrac{1}{4}(\alpha D - 4D - 4\mu + 2\alpha - 2\alpha^2 + 4\alpha\delta) u_1 \end{aligned}$$

Since this is an automorphism of the same form that T with α replaced by $\alpha - 1$, D by $\alpha(\alpha - 1) + D - 2\delta$, and β by $\alpha D - 4D - 4\mu + 2\alpha - 2\alpha^2 + 4\alpha\delta$ it will be involutory if the equivalent of condition (7) holds. So we obtain

$$\alpha^3 - \alpha - 6\alpha\delta + 2\delta + 3D + 4\mu = 0$$

Hence if the characteristic of the basic field is not 3 we can take

$$D = -\tfrac{1}{3}(\alpha^3 - \alpha - 6\alpha\delta + 2\delta + 4\mu)$$

and when the characteristic is 3 we get the relation $\alpha^3 - \alpha + 2\delta + \mu = 0$ which may not have a solution if the field is not algebraically closed.

So we have shown that if (a) holds the automorphism $S = \bar{Q}_1 \bar{Q}_2$ when the characteristic is not three.

In order to discuss subcase (b) we will first prove the following.

LEMMA. *If $(x - 1)^7$ is the characteristic polynomial of the automorphism S, but not its minimum polynomial, then S either leaves invariant a quaternion subalgebra or there exists two linearly independent isotropic vectors u and w invariant under S and such that $uw = 0$.*

Proof. If there exists an invariant non-degenerate plane in C_0 we already know that there exists an invariant quaternion subalgebra and therefore $S = \bar{Q}_1 \bar{Q}_2$. On the other hand since $(x - 1)^7$ is not the minimum polynomial there exist at least two linearly independent invariant vectors.

Suppose then that the plane spanned by these two vectors is degenerate. If the radical of the restriction of the bilinear form to this plane has dimension 1, there exists an orthogonal basis u, z such that $N(u) = 0$, $N(z) \neq 0$. Then if $uz \notin [u]$, the vectors u, uz satisfy the conditions. Should $uz = \alpha u$, then $\alpha \neq 0$ and $uz^2 = (uz) z = \alpha^2 u$, so $z^2 = \alpha^2.1$ and $N(\alpha^{-1} z) = -1$. Hence S leaves invariant a vector of norm -1 and the restriction of S to the subspace $U = \{x \in C_0 \mid x(\alpha^{-1} z) = x\}$ has 1 as a characteristic root since $u \in U$, and we know that the same is true of the restriction of S to $V = \{x \in C_0 \mid x(\alpha^{-1} z) = -x\}$. Let $v \in V$ such that $vS = v$, since $uv = (u, v)(1 - \alpha^{-1} z)$ if $(u, v) \neq 0$, the vectors $1, u, v, z$ span an invariant quaternion subalgebra and if $(u, v) = 0$, the pair u, v satisfies the condition stated in the lemma.

If the invariant plane is totally isotropic, let u, v be a basis. Then if $uv = 0$ we are done and if $uv \neq 0$, the pair u, uv satisfies the requirements. This completes the proof of the lemma.

So it remains to show that if S leaves invariant two linearly independent isotropic vectors whose product is 0, S is the product of two involutory automorphisms. Such two vectors can be taken as the u_1 and w_2 of an appropriate standard basis, and the most general automorphism leaving these two vectors invariant is of the following form

$$
\begin{aligned}
u_1S &= u_1 , \qquad w_2S = w_2 , \qquad w_3S = w_3 + \alpha w_2 + \beta u_1 \\
zS &= z + 2\beta w_2 + 2\mu u_1 , \qquad u_3S = u_3 + \mu w_2 + \gamma \mu_1 \\
u_2S &= u_2 - \alpha u_3 + \beta z - \mu w_3 + (\beta^2 - \alpha\mu)\, w_2 + \delta u_1 \\
w_1S &= w_1 - \beta u_3 + \mu z - \gamma w_3 - (\delta + \alpha\gamma - \beta\mu)\, w_2 + (\mu^2 - \beta\gamma)\, u_1
\end{aligned}
$$

One also finds that the most general automorphism which takes u_1 and w_2 into their negatives is the following,

$$
\begin{aligned}
u_1T &= -u_1 , \qquad w_2T = -w_2 \\
w_3T &= w_3 + Aw_2 + Bu_1 \\
zT &= z + 2Bw_2 + 2Mu_1 \\
u_3T &= u_3 + Mw_2 + Cu_1 \\
u_2T &= -u_2 + Au_3 - B_z + Mw_3 + (AM - B^2)\, w_2 + Du_1 \\
w_1T &= (u_2T)(u_3T)
\end{aligned}
$$

This automorphism T is involutory if and only if

$$
AC - MB - 2D = 0 \tag{8}
$$

Hence we can take any A, B, C and M, then D is determined by (8). As for the automorphism $T' = ST$ we get

$$
\begin{aligned}
u_1T' &= -u_1' , \qquad w_2T' = -w_2' \\
w_3T' &= w_3 + (A - \alpha)\, w_2 + (B - \beta)\, u_1 \\
2T' &= z + 2(B - \beta)\, w_2 + 2(M - \mu)\, u_1 \\
u_3T' &= u_3 + (M - \mu)\, w_2 + (C - \gamma)\, u_1 \\
u_2T' &= -u_2 + (A - \alpha)\, u_3 - (B - \beta)\, z + (M - \mu)\, w_3 \\
&\quad + ((A - \alpha)(M - \mu) - (B - \beta)^2)\, w_2 \\
&\quad + (D - \delta - \alpha C + 2\beta M - \mu B)\, u_1
\end{aligned}
$$

Therefore T' will be involutory if

$$
(A - \alpha)(C - \gamma) - (M - \mu)(B - \beta) - 2(D - \delta - \alpha C + 2\beta M - \mu B) = 0
$$

If T is involutory, that is, if (8) holds, this reduces to

$$
\alpha C - \gamma A + 3\mu B - 3\beta M + \alpha\gamma - \mu\beta + 2\delta = 0
$$

When char $K \neq 3$ we can find values of A, B, C and M satisfying this equation unless $\alpha = \gamma = \mu = \beta = 0$ and $\delta \neq 0$. But in the latter case the quaternion subalgebra $[1, u_3 , w_3 , z]$ is invariant under S. So in subcase (b) it is also true that $S = \bar{Q}_1\bar{Q}_2$ and the theorem is proved.

4. Let K be an algebraically closed field of characteristic $\neq 2, 3$. Then if the hypothesis of Theorem 4 does not hold for an automorphism S, the subspace of C_0 consisting of invariant vectors has dimension one and is nondegenerate, hence it contains a vector of norm -1 and we can apply Theorem 2. So our results give the following.

THEOREM 4. *Let C be a Cayley algebra over an algebraically closed field of characteristic $\neq 2, 3$. Then any automorphism of C is the product of two involutory automorphisms.*

We have already seen that if we do not impose any conditions on the field the result does not hold. For the general case the best result is given by

THEOREM 5. *Let C be a Cayley algebra over a field of characteristic $\neq 2, 3$. Any automorphism of C can be expressed as the product of at most three involutory automorphisms.*

Proof. If the hypothesis of Theorem 3 does not hold, let v be an invariant non-isotropic vector in C_0. Let t be non-isotropic and orthogonal to v. Take t' non-isotropic an orthogonal to $[1, v, t, vt]$. Then $Q_3 = [1, t, t', tt']$ is a quaternion subalgebra which defines an automorphism which takes v into $-v$ and induces a reflection on the subspace $[1, v]^\perp$. Since the automorphism $S\bar{Q}_3$ induces a reflection in this subspace it leaves invariant a nonzero vector $v' \in [1, v]^\perp$. If v' is non-isotropic then $S\bar{Q}_3 = \bar{Q}_1\bar{Q}_2$, because it leaves invariant the quaternion subalgebra $[1, v, v', vv']$. Should v' be isotropic, then $S\bar{Q}_3$ satisfies the hypothesis of Theorem 3, so we get again $S\bar{Q}_3 = \bar{Q}_1\bar{Q}_2$, that is, $S = \bar{Q}_1\bar{Q}_2\bar{Q}_3$.

REFERENCES

1. ARTIN, E. "Geometric Algebra." Interscience, New York, 1957.
2. JACOBSON, N. Composition algebras and their automorphisms. Rendiconti del Circolo Matematico di Palermo, 1958, pp. 55–80.

3. Schafer, R. D. "An Introduction to Non-Associative Algebras." Academic Press, New York, 1966.
4. Taussky, O. and Zassenhaus, H. On the similarity transformation between a matrix and its transpose. *Pacific J. Math.* **9**, 893–896 (1959).
5. Wonenburger, M. Transformations which are products of two involutions. *J. Math. Mech.* **16** (1966), 327–338.

PRINTED IN BRUGES, BELGIUM, BY THE ST. CATHERINE PRESS, LTD