CAYLEY SYMMETRIES IN ASSOCIATIVE ALGEBRAS

EARL J. TAFT

1. Introduction. Let A be a finite-dimensional associative algebra over a field F. Let R denote the radical of A. Assume that A/R is separable. Then it is well known (the Wedderburn principal theorem) that A possesses a Wedderburn decomposition $A = S + R$ (semi-direct), where S is a separable subalgebra isomorphic with A/R. We call S a Wedderburn factor of A.

Now let G be a set of linear transformations of the underlying vector space of A. If there exists a Wedderburn factor S of A which is sent into itself by each element of G, we say that S is a G-invariant Wedderburn factor of A. In **(2)**, it is shown that if G is a fully reducible group of automorphisms of the algebra A, and if the characteristic of F is zero, then A possesses G-invariant Wedderburn factors. In **(3)** it is shown that if G is a finite group each of whose elements is either an automorphism or an anti-automorphism of the algebra A, and if the characteristic of F is not a divisor of the order of G, then A possesses G-invariant Wedderburn factors.

By the well-known Malcev theorem (see **1**), any two Wedderburn factors of A are conjugate by an inner automorphism of A given by conjugation by an element $1 + z$, where $z \in R$. In this paper, we discuss the uniqueness question for G-invariant Wedderburn factors, where G is as in **(3)** and as described in the last sentence of the preceding paragraph. In **(4)**, we showed that if G is a finite group of automorphisms and anti-automorphisms of the algebra A, and if the characteristic of F is zero, then any two G-invariant Wedderburn factors are conjugate by a G-orthogonal element $\exp z$, where z is a G-symmetric element of R. (See **4** for an explanation of the terminology.) It was conjectured in **(4)** that if G is as described here, and if the characteristic of F is not a divisor of the order of G, then any two G-invariant Wedderburn factors of A are conjugate by an inner automorphism of A given by conjugation by a G-orthogonal element of A. Here we shall answer this conjecture in the affirmative (see Theorem 2 and Corollary 1) under the additional hypothesis that the characteristic of F be different from two. This will generalize the result for characteristic zero **(4)** mentioned above.

2. Preliminaries. Let A be a finite-dimensional associative algebra over a field F of characteristic $\neq 2$, and let R denote the radical of A. Let G be a set of non-singular linear transformations of the underlying vector space of

Received March 5, 1962. This paper was sponsored by a grant from the Research Council of Rutgers, The State University, while the author was in residence at Yale University.

A, each element of which is either an automorphism or an anti-automorphism of the algebra A. (If A is commutative, then we regard each element of G as an automorphism of A.)

Let A_1 denote the algebra obtained from A by adjunction of an identity (if necessary). Then the elements of G induce mappings of A_1 (where $t(c) = c$ for $t \in G$, $c \in F$).

DEFINITION 1. *An element z in A is called G-symmetric if z is left fixed by the automorphisms in G, and z is sent into $-z$ by the anti-automorphisms in G.*

It is easy to see that the G-symmetric elements of A form a Lie algebra over F. The G-symmetric elements of R will also form a Lie algebra over F.

DEFINITION 2. *An element w of A_1 is called G-orthogonal if w is regular (has a two-sided inverse in A_1), if w is left-fixed by the automorphisms in G, and if w is sent into w^{-1} by the anti-automorphisms of G.*

It is easy to check that the G-orthogonal elements of A_1 form a multiplicative group (a subgroup of the group of all regular elements of A_1).

DEFINITION 3. *An inner automorphism of A given by conjugation by a G-orthogonal element of A_1 is called a G-orthogonal conjugacy of A.*

By the remark following Definition 2, it follows that the G-orthogonal conjugacies of A form a group (a subgroup of the group of all automorphisms of the algebra A). It is easy to see that any G-orthogonal conjugacy of A commutes with each element of G. Hence if S is a G-invariant subalgebra of A, then the image of S under any G-orthogonal conjugacy of A will also be a G-invariant subalgebra of A.

DEFINITION 4. *Two G-invariant subalgebras S and T of A are said to be G-orthogonally conjugate if there exists a G-orthogonal conjugacy of A which carries S onto T.*

By the remark following Definition 3, it follows that the relation of G-orthogonal conjugacy is an equivalence relation among the G-invariant subalgebras of A.

If z is a G-symmetric element of R, then it is clear that $1 + z$ is regular in A_1, and that $(1 - z)(1 + z)^{-1}$ is G-orthogonal. It is this type of G-orthogonal element that will be useful in discussing (in § 3) the uniqueness problem mentioned in the introduction. The following computational lemmas and theorem are a generalization to the present setting of the algebraic techniques involved in the Cayley parametrization of (a part of) the orthogonal group acting on Euclidean n-space (see **5**, Chapter II, Section 10, and Chapter X, Section 5).

LEMMA 1. *Let z be an element of R. Then z is G-symmetric if and only if $(1 - z)(1 + z)^{-1}$ is G-orthogonal. Furthermore,*

$$1 + (1 - z)(1 + z)^{-1} = 2(1 + z)^{-1}$$

is regular, and

$$z = \{1 - (1 - z)(1 + z)^{-1}\}\{1 + (1 - z)(1 + z)^{-1}\}^{-1}.$$

Proof. The first assertion is easy to check. The second one is obtained by multiplying $(1+z)+(1-z) = 2$ by $(1+z)^{-1}$, and the last assertion may be verified by inserting $(1 + z)(1 + z)^{-1}$ between the brackets on the right-hand side of the equation.

LEMMA 2. *Let w be a G-orthogonal element of A_1 such that $1 + w$ is regular. Then $(1 - w)(1 + w)^{-1}$ is G-symmetric. Furthermore, if $1 - w$ is also in R, then $1 + (1 - w)(1 + w)^{-1}$ is regular, and*

$$w = \{1 - (1 - w)(1 + w)^{-1}\}\{1 + (1 - w)(1 + w)^{-1}\}^{-1}.$$

Proof. It is clear that $(1 - w)(1 + w)^{-1}$ is left-fixed by the automorphisms in G. Let t be an anti-automorphism in G. Then

$$\begin{aligned} t\{(1 - w)(1 + w)^{-1}\} &= (1 + t(w))^{-1}(1 - t(w)) \\ &= (1 + w^{-1})^{-1}(1 - w^{-1}) = (1 + w^{-1})^{-1}w^{-1}w(1 - w^{-1}) \\ &= (1 + w)^{-1}(w - 1) = -(1 - w)(1 + w)^{-1}. \end{aligned}$$

This proves the first assertion. The second assertion is clear. The proof of the last assertion is similar to the proof of the last assertion of Lemma 1.

THEOREM 1. *Let A be a finite-dimensional associative algebra over a field F of characteristic $\neq 2$, and let R be the radical of A. Let G be a set of non-singular linear transformations of A, each element of which is either an automorphism or an anti-automorphism of the algebra A. Let $C(G)$ denote the subset of A_1 consisting of elements of the form $(1 - z)(1 + z)^{-1}$, where z is a G-symmetric element of R. Then $C(G)$ is a subgroup of the multiplicative group of G-orthogonal elements of A_1.*

Proof. Let x and y be G-symmetric elements of R and let

$$u = (1 - x)(1 + x)^{-1} \quad \text{and} \quad v = (1 - y)(1 + y)^{-1}$$

be elements of $C(G)$. Then $uv = (1 - x)(1 + x)^{-1}(1 - y)(1 + y)^{-1}$. Since $(1 + x)^{-1}$ and $(1 + y)^{-1}$ are polynomials in x and y, respectively, with constant term 1, we may write $uv = 1 + r$, where $r \in R$. Then $1 - uv = -r$ is in R. Also $1 + uv = 2 + r = 2(1 + \frac{1}{2}r)$ is regular. It is clear that uv is G-orthogonal. Hence, by Lemma 2, $(1 - uv)(1 + uv)^{-1}$ is a G-symmetric element of R and

$$uv = \{1 - (1 - uv)(1 + uv)^{-1}\}\{1 + (1 - uv)(1 + uv)^{-1}\}^{-1}.$$

Hence uv is in $C(G)$. The remaining group properties are clear. This completes our proof.

DEFINITION 5. *We call $C(G)$ the Cayley subgroup of the group of G-orthogonal elements of A_1. A G-orthogonal conjugacy of A given by conjugation by an element of $C(G)$ will be called a Cayley-symmetry of A. Two G-invariant subalgebras S and T of A will be said to be Cayley-equivalent if there exists a Cayley symmetry of A which maps S onto T.*

By Theorem 1, the Cayley symmetries of A form a group, and hence the relation of Cayley-equivalence is an equivalence relation among the G-invariant subalgebras of A.

3. Cayley-equivalence of G-invariant Wedderburn factors. In this section, we prove the conjecture made in **(4)**, and described in the Introduction.

THEOREM 2. *Let A be a finite-dimensional associative algebra over a field F of characteristic $\neq 2$. Let R be the radical of A, and let A/R be separable. Let G be a finite group, each element of which is either an automorphism or an anti-automorphism of A, and whose order is not a multiple of the characteristic of F. Let $A = T + R$ be a G-invariant Wedderburn decomposition of A (i.e., T is a G-invariant Wedderburn factor of A). Let S be any G-invariant separable subalgebra of A. Then S is Cayley-equivalent to a subalgebra of T.*

Proof. We first note that if A is commutative, then by the result in **(1)**, there exists a unique Wedderburn factor, so that the result is trivial (the identity mapping will suffice), Hence we may assume that A is not commutative, so that each element in G is either an automorphism or an anti-automorphism of A, but not both.

Case 1. We first assume that $R^2 \neq 0$.

We proceed by induction on the F-dimension of A and assume the result to be true for algebras whose dimension is less than that of A. If B is a subset of A, let $\bar{B}$ denote the image of B under the natural homomorphism of A onto A/R^2. Each element of G will induce an automorphism or an anti-automorphism of $\bar{A}$. $\bar{A} = \bar{T} + \bar{R}$ is a G-invariant Wedderburn decomposition of $\bar{A}$, and $\bar{S}$ is a G-invariant separable subalgebra of $\bar{A}$. Hence, by induction, there is an element x in R such that $\bar{x}$ is G-symmetric in $\bar{R}$, and such that

$$(\bar{1} + \bar{x})(\bar{1} - \bar{x})^{-1}\bar{S}(\bar{1} - \bar{x})(\bar{1} + \bar{x})^{-1} \subseteq \bar{T}.$$

Now set

$$y = \frac{1}{n} \sum_{t \in G} (-1)^{\operatorname{sgn} t}\, t(x),$$

where n is the order of G, and sgn t is $+1$ if t is an automorphism, and -1 if t is an anti-automorphism. Clearly y is in R. Since G is a group, y is G-symmetric by the laws governing the multiplication of automorphisms and anti-automorphisms. Furthermore,

$$\bar{y} = \frac{1}{n} \sum_{t \in G} (-1)^{\operatorname{sgn} t} t(\bar{x}) = \frac{1}{n} \sum_{t \in G} \bar{x} = \bar{x}$$

since $\bar{x}$ is G-symmetric. Hence, if we set

$$S_1 = (1 + y)(1 - y)^{-1} S (1 - y)(1 + y)^{-1},$$

then we have

$$\bar{S}_1 = (\bar{1} + \bar{x})(\bar{1} - \bar{x})^{-1} \bar{S} (\bar{1} - \bar{x})(\bar{1} + \bar{x})^{-1} \subseteq \bar{T},$$

so that $S_1 + R^2 \subseteq T + R^2$.

Now $T + R^2$ is a G-invariant Wedderburn decomposition of $T + R^2$. Also, S_1 is a G-invariant separable subalgebra of $T + R^2$ by the remarks following Definition 3. Finally, the dimension of $T + R^2$ is less than the dimension of $A = T + R$. Applying the induction hypothesis again, we conclude that there is an element z in R^2 (and hence in R) such that z is G-symmetric, and such that $(1 + z)(1 - z)^{-1} S_1 (1 - z)(1 + z) \subseteq T$. Then it is clear (using Theorem 1) that $(1 - y)(1 + y)^{-1}(1 - z)(1 + z)^{-1}$ is an element in $C(G)$, conjugation by which maps S into T.

Case 2. Now assume that $R^2 = 0$.

In this case, we use the result in **(4)**. Although the result is stated there for characteristic 0, the only restriction necessary is that one be able to divide by the factorials of the positive integers less than the index of nilpotency of the radical. Hence, the result there is valid if the characteristic of F is greater than or equal to the index of nilpotency of R. In particular, if $R^2 = 0$, then for z in R, $\exp(\operatorname{Ad} z) = I + \operatorname{Ad} z$ is conjugation by $\exp z = 1 + z$, and there is no restriction necessary on the characteristic of F (except in relation to the order of G).

Therefore, we conclude that there exists a G-symmetric element z in R such that conjugation by $\exp z = 1 + z$ maps S into T. But since $R^2 = 0$ and the characteristic of F is not 2, the element

$$1 + z = (1 + \tfrac{1}{2}z)^2 = (1 + \tfrac{1}{2}z)(1 - \tfrac{1}{2}z)^{-1}$$

is in $C(G)$, since clearly $-\frac{1}{2}z$ is a G-symmetric element of R. This completes the proof of Theorem 2.

Theorem 2 has the following two corollaries.

COROLLARY 1. *Let A and G be as stated in the hypothesis of Theorem* 1. *Then any two G-invariant Wedderburn factors of A are Cayley-equivalent.*

COROLLARY 2. *Let A and G be as stated in the hypothesis of Theorem* 1. *Let S be a G-invariant separable subalgebra of A. Then S may be embedded in a G-invariant Wedderburn factor of A.*

4. The case of characteristic zero. As mentioned in the introduction. Theorem 2 and Corollary 1 generalize the result for characteristic zero in **(4)**.

(Indeed, the latter result is used in Case 2 of the proof of Theorem 2.) In this section, we note that a Cayley-symmetry may be written in the exponential form obtained in **(4)** if F has the characteristic zero.

Let z be a G-symmetric element of R. Then the Cayley-symmetry given by conjugation by $(1 - z)(1 + z)^{-1}$ may be considered as conjugation by $\exp[\log\{(1 - z)(1 + z)^{-1}\}]$, and this conjugation is the same as

$$\exp\{\mathrm{Ad}(\log[(1 - z)(1 + z)^{-1}])\}.$$

But,

$$\begin{aligned}\log\{(1 - z)(1 + z)^{-1}\} &= \log(1 - z) - \log(1 + z)\\ &= \left(-z - \frac{z^2}{2} - \frac{z^3}{3} - \dots\dots\right) - \left(z - \frac{z^2}{2} + \frac{z^3}{3} - \dots\dots\right)\\ &= -2\left(z + \frac{z^3}{3} + \frac{z^5}{5} + \dots\dots\right)\end{aligned}$$

is a G-symmetric element of R, since it involves only odd powers of z.

References

1. A. Malcev, *On the representation of an algebra as a direct sum of the radical and a semi-simple algebra*, Dokl. Akad. Nauk. S.S.S.R. (N.S.), *36* (1942), 42–45.

2. G. D. Mostow, *Fully reducible subgroups of algebraic groups*, Amer. J. Math., *78* (1956), 200–221.

3. E. J. Taft, *Invariant Wedderburn factors*, Illinois J. Math., *1* (1957), 565–573.

4. ——— *Uniqueness of invariant Wedderburn factors*, Illinois J. Math., *6* (1962), 353–356.

5. H. Weyl, *The classical groups* (Princeton, 1946).

Yale University