Pacific Journal of Mathematics

A CHARACTERIZATION OF THE GROUP ALGEBRAS OF THE FINITE GROUPS

MARC A. RIEFFEL

Vol. 16, No. 2 December 1966

PACIFIC JOURNAL OF MATHEMATICS
Vol. 16, No. 2, 1966

A CHARACTERIZATION OF THE GROUP ALGEBRAS OF FINITE GROUPS

MARC A. RIEFFEL

The following is proved:

MAIN THEOREM. Let A be a finite dimensional Archemedian lattice ordered algebra which satisfies the following axioms:

MO If $f, g, h \in A$, and if $f \geqq 0$, then

(l) $f*(g \vee h) = \vee\{f_1*g + f_2*h\colon f_1 \geqq 0, f_2 \geqq 0, f_1 + f_2 = f\}$.

(r) $(g \vee h)*f = \vee\{g*f_1 + h*f_2\colon f_1 \geqq 0, f_2 \geqq 0, f_1 + f_2 = f\}$.

P If $f, g \in A$, and if $f > 0$, $g > 0$, then $f*g > 0$.

Then there exists a finite group G such that A is order and algebra isomorphic to the group algebra of G.

Some similar results are obtained for finite semigroups, and a few applications of these results are given. In particular it is shown that the second cohomology group, $H^2(S, R)$, of any finite commutative semigroup, S, with coefficients in the additive group of real numbers, R, is trivial.

It is well known that two nonisomorphic finite groups can have isomorphic group algebras (over the real or complex numbers) (see e.g. [5, p. 305]). On the other hand, Kawada [4] has shown that if the group algebra is considered as an ordered algebra (with the usual partial ordering obtained by viewing its elements as functions on the group), then if the group algebras of two groups are order as well as algebraically isomorphic, then the two groups are isomorphic (in fact Kawada proved this for the much more general case of locally compact groups). In view of this result it is natural to try to characterize those ordered algebras which occur as the group algebras of finite groups. In this paper we prove the characterization stated above.

All of our results are stated for ordered algebras over the real numbers, but with trivial modifications they apply to ordered algebras over the complex numbers. We will always denote the product of two elements, f and g, of an algebra by $f*g$.

As we will indicate in § 2, a finite dimensional Archemedian lattice ordered vector space is always boundedly lattice complete, so the right hand sides of MOl and MOr always exist.

It follows, of course, from Kawada's result that G in the Main Theorem is unique to within isomorphism.

In § 1 we will give some motivation for axiom MO.

Received August 5, 1964, and in revised form October 13, 1964.

Hewitt and Zuckerman [3, Theorem 4.2.4] have extended Kawada's result to the convolution algebras of finite semigroups. It is thus natural to try to characterize those ordered algebras which occur as the convolution algebras of finite semigroups. Unfortunately no analogue of axiom MO seems to hold in this case, and instead we have imposed an axiom which seems to us to be somewhat more artificial than axiom MO. Even then we are successful only in the commutative case (see Corollary 5.11) though we come close in the noncommutative case.

Finally, in § 6 we give several applications of some of our results. We prove here that $H^2(S, R) = 0$ for a finite commutative semigroup, S, and we give an example to show that this need not be true for noncommutative semigroups. The existence of such examples lies at the heart of our difficulties in characterizing the convolution algebras of noncommutative semigroups. However even for noncommutative finite semigroups we do show that there is a canonical way of choosing cocycle representatives for the elements of $H^2(S, R)$, which gives a convenient way of computing $H^2(S, R)$.

Throughout our paper we will use the following notation. Instead of writing "finite dimensional Archemedian lattice ordered algebra" we will write "FDALO algebra". If A and B are two ordered algebras, we will write $A \cong B$ to mean that A and B are order as well as algebraically isomorphic. If S is a finite semigroup (or group), $L(S)$ will denote its convolution algebra. There are two equivalent ways of defining the convolution algebra of a semigroup. It can be defined to be the vector space of real-valued functions on the semigroup, with convolution as multiplication, or it can be defined to be the algebra of formal linear combinations of elements in S with coefficients in the real numbers, R. We will use both definitions interchangeably, as each has certain advantages. In particular the second is functorial, whereas the first is not.

We are indebted to Calvin C. Moore for bringing to our attention the relevance of the cohomology theory of groups to our work.

1. Axiom MO. We will discuss only axiom MOl, an entirely parallel discussion applying to MOr. In § 4 we will see that the two axioms are independent.

Our motivation for conjecturing axiom MO is the Riesz decomposition of a linear functional on a partially ordered vector space into its positive and negative parts (see e.g. [2, p. 36]). For if we let $h = 0$ in MOl we obtain

1.1 $$f * g^+ = \vee \{f_1 * g \colon 0 \leqq f_1 \leqq f\} .$$

Further, in view of the relation

$$g \vee h = h + (g - h)^+ ,$$

axiom MOl is entirely equivalent to 1.1, for

$$\begin{aligned} f*(g \vee h) &= f*(h + (g-h)^+) = f*h + f*(g-h)^+ \\ &= f*h + \vee \{f_1*(g-h) \colon 0 \leqq f_1 \leqq f\} \\ &= \vee\{f_1*g + (f-f_1)*h \colon 0 \leqq f_1 \leqq f\} \\ &= \vee\{f_1*g + f_2*h \colon f_1 \geqq 0,\ f_2 \geqq 0,\ f_1 + f_2 = f\} . \end{aligned}$$

Now if we consider the operator on A consisting of multiplying elements of A on the right by g, we see that 1.1 is a formula for the positive part of this operator, which is exactly the analogue of the Riesz formula for the positive part of a linear functional.

We now show that axiom MOl holds in the group algebra of any finite group.

LEMMA 1.2. *Let A be any boundedly lattice complete lattice ordered algebra. If $f, g, h \in A$ and if $f \geqq 0$ then*

1.3 $$f*(g \vee h) \geqq \vee\{f_1*g + f_2*h \colon f_1 \geqq 0,\ f_2 \geqq 0,\ f_1 + f_2 = f\} .$$

Proof. We note that the right hand side always exists since for such f_1 and f_2

$$f_1*g + f_2*h \leqq f*|g| + f*|h| .$$

As indicated in the discussion above it is sufficient to show that

$$f*g^+ \geqq \vee\{f_1*g \colon 0 \leqq f_1 \leqq f\} .$$

But this is clear from the fact that if $0 \leqq f_1 \leqq f$, then

$$f_1*g = f_1*g^+ - f_1*g^- \leqq f_1*g^+ \leqq f*g^+ .$$

PROPOSITION 1.4. If G is a finite group then $L(G)$ satisfies axiom MO.

Proof. It is clear that $L(G)$ is boundedly lattice complete so that Lemma 1.2 applies. Then, as indicated above, it is sufficient to show that if $f, g \in A$ and if $f \geqq 0$ then

1.5 $$f*g^+ \leqq \vee\{f_1*g \colon 0 \leqq f_1 \leqq f\} .$$

Now for any $t \in G$ define an element, f_t, of $L(G)$ by

$$f_t(s) = \begin{cases} f(s) \text{ if } g(s^{-1}t) \geqq 0 \\ \ \ 0 \text{ if } g(s^{-1}t) < 0 . \end{cases}$$

Then it is clear that $0 \leqq f_t \leqq f$. Furthermore it is trivial to check that $(f_t * g)(t) = (f * g^+)(t)$, and 1.5 follows immediately.

2. Pure elements.

We now begin the proof of the Main Theorem.

The first fact which we will need is that any Archemedian vector lattice of finite dimension n is order and vector space isomorphic to R^n, the n-fold Cartesian product of real lines, with the usual product partial order (see [1, p. 240] where this fact is attributed to M. Mannos; see also [2, p. 39]). As a first consequence, any finite dimensional Archemedian vector lattice is boundedly lattice complete. In particular, as in Lemma 1.2 the right hand sides of axiom MO always exist.

Now if the group algebra, $L(G)$, of a finite group, G, is viewed as the algebra of formal linear combinations of elements of G, then there is a natural embedding of G into $L(G)$. Under this embedding the elements of G become elements of $L(G)$ of the following type.

DEFINITION 2.1. An element, f, of a partially ordered vector space is said to be *pure* if $f > 0$ and if whenever $f \geqq g \geqq 0$ it follows that $g = af$ for some real number a.

Then if we wish to find a group associated with an algebra satisfying the conditions of the Main Theorem we would hope in some way to find its elements among the pure elements of A. Now it is clear that in R^n the pure elements are exactly the positive elements all but one of whose coordinates are zero. Since A is isomorphic as a vector lattice to R^n it follows that A has a sufficient number of pure elements, in the sense that we can choose a basis for A consisting of pure elements, or, more generally, given any family of linearly independent pure elements of A it can be extended to a basis for A by adjoining pure elements.

Now if A is to be isomorphic to a group algebra, it should be the case that the product of pure elements of A is pure. We now show that this is implied by either of axioms MOl or MOr in the presence of axiom P. We will actually prove this only for axiom MOl, but of course an entirely parallel discussion applies to axiom MOr.

LEMMA 2.2. *Let A be a lattice ordered algebra satisfying axiom* MOl. *Then if f is a pure element of A it follows that for any $g, h \in A$*

2.3 $$f*(g \vee h) = (f*g) \vee (f*h)$$

and

2.4 $$f*(g \wedge h) = (f*g) \wedge (f*h) ,$$

that is, left multiplication by f is a lattice homomorphism.

Proof. If $f_1 + f_2 = f$ where $f_1 \geqq 0$, $f_2 \geqq 0$ then since f is pure there is a real number, a, $0 \leqq a \leqq 1$, such $f_1 = af$ and $f_2 = (1-a)f$. Then

$$\begin{aligned} f*(g \vee h) &= \vee\{af*g + (1-a)f*h\colon 0 \leqq a \leqq 1\} \\ &\leqq \vee\{a[(f*g) \vee (f*h)] + (1-a)[(f*g) \vee (f*h)]\colon 0 \leqq a \leqq 1\} \\ &= (f*g) \vee (f*h) \leqq f*(g \vee h)\ , \end{aligned}$$

and 2.3 follows. Then 2.4 follows from the relation

$$g \wedge h = -[(-g) \vee (-h)]\ .$$

We remark that if A satisfies all the hypotheses of the Main Theorem, in particular both axioms MOl and MOr, then it can be shown that property 2.3 characterizes the pure elements of A. In the absence of either axiom MOl or MOr we have examples to show that this is no longer true.

PROPOSITION 2.5. Let A be a FDALO algebra satisfying axioms MOl and P. Then the product of pure elements is pure.

Proof. Suppose that for two (possibly equal) pure elements f and f_1 of A it happens that $f*f_1$ is not pure, so that $f*f_1 = g_0 + g_1$ where $g_0 \wedge g_1 = 0$, $g_0 > 0$ and $g_1 > 0$. Let the dimension of A be n, and let $f_2, \cdots, f_n$ be pure elements of A such that $f_1, \cdots, f_n$ forms a basis for A. This can be done according to the remarks following Definition 2.1. Let $g_k = f*f_k$ for $k = 2, \cdots, n$. Then by axiom P each $g_k > 0$. Since A is of dimension n, $g_0, \cdots, g_n$ can not be linearly independent. Then $g_0, \cdots, g_n$ can not be mutually disjoint, for if they were, that is, if $g_i \wedge g_j = 0$ for $i \neq j$, then a routine argument would show that they were linearly independent. Thus $(f*f_i) \wedge (f*f_j) \neq 0$ for some $i, j, i \neq j$. But by Lemma 2.2 $(f*f_i) \wedge (f*f_j) = f*(f_i \wedge f_j) = f*0 = 0$, and so we have a contradiction.

DEFINITION 2.6. An ordered algebra A will be said to satisfy axiom Q if the products of pure elements of A are pure.

The next step in our proof of the Main Theorem is to investigate the FDALO algebras which satisfy axiom Q. Since it is easily seen that the convolution algebra of any finite semigroup is such an algebra, we can expect this investigation to lead towards characterization of these convolution algebras.

3. Cocycles. Let A be a FDALO algebra of dimension n, which

satisfies axiom Q, and let E be the set of pure elements of A. Then axiom Q says that E is closed with respect to the multiplication in A and so forms a semigroup. Further, the group R^+ of positive real numbers under multiplication acts on E, and the action is compatible with the multiplication in E so that the quotient, $S = E/R^+$, is again a semigroup. The elements of S are just the semirays of pure elements in A, and, from the fact that A is isomorphic as a vector lattice to R^n, it is clear that there are exactly n such semirays, so that S is a finite semigroup of order n. We might hope that A would be isomorphic to the convolution algebra of S. To show this it would be sufficient to show that for each element of S, that is, for each equivalence class of elements of E, we can pick a representative in E such that this set of representatives is closed under multiplication. It turns out that this can not always be done, and the investigation of when it can be done is most conveniently viewed as a problem in cohomology with coefficients in R^+. For completeness we will now define the concepts from cohomology theory which we will need.

Let S be a finite semigroup (as always, we do not assume that it has a unit element). For any positive integer n, by a (positive) n-cochain we will mean any function on S^n with values in R^+. The n-cochains form a group, $C^n(S, R^+)$, under pointwise multiplication. By a 2-cocycle we mean any element, z, of $C^2(S, R^+)$ which satisfies the "cocycle identity"

3.1 $$z(rs, t)z(r, s) = z(r, st)z(s, t) .$$

The 2-cocycles form a subgroup, $Z^2(S, R^+)$, of $C^2(S, R^+)$. Given any 1-cochain, c, the coboundary, dc, of c is defined to be the 2-cochain

$$dc(s, t) = c(s)c(t)/c(st) .$$

It is easily checked that coboundaries are cocycles, and that d is a group homomorphism of $C^1(S, R^+)$ into $Z^2(S, R^+)$, so that the coboundaries form a subgroup, $B^2(S, R^+)$, of $Z^2(S, R^+)$. The factor group,

$$H^2(S,R^+) = Z^2(S, R^+)/B^2(S, R^+) ,$$

is the second cohomology group of S with coefficients in R^+. The second cohomology group is a functor on the category of finite semigroups and their homomorphisms.

If S is a finite semigroup and if $z \in Z^2(S, R^+)$, then, as usual, one can define an algebra, $zT(S)$, the z-twisted algebra over S, as follows: the elements of S will form a basis for $zT(S)$ over R, and the product in $zT(S)$, $s *_z t$, or if no confusion arises, just $s * t$, of two of these basis elements, s and t, is defined by

3.2 $$s *_z t = z(s, t)st$$

where st is the product of s and t in S. This product extends by linearity to a product in all of $zT(S)$. Alternatively we can define $zT(S)$ to be the vector space of real-valued functions on S with multiplication defined by the twisted convolution

$$(f *_z g)(t) = \sum \{z(r, s)f(r)g(s)\colon rs = t\} .$$

The fact that z satisfies the cocycle identity is exactly what is needed to ensure that the product in $zT(S)$ is associative. With the obvious partial ordering it is easily seen that any such twisted algebra is a FDALO algebra which satisfies axiom Q. The ordinary convolution algebra of a semigroup is just the z-twisted algebra for which $z \equiv 1$.

In view of these remarks it is reasonable to try to show that any FDALO algebra satisfying axiom Q is isomorphic to a twisted algebra over some finite semigroup. We now show that this is true.

THEOREM 3.3. *Let A be a FDALO algebra satisfying axiom Q. Then there exists a finite semigroup, S, and a $z \in Z^2(S, R^+)$ such that $A \cong zT(S)$.*

Proof. Let $S = E/R^+$ as defined at the beginning of this section. If f is any element of E, we will denote by $\bar{f}$ the corresponding element of $S = E/R^+$. For each element $\bar{f}$ of S choose a representative for $\bar{f}$ in E. We denote this representative by $(\bar{f})_0$ or just f_0. For any two elements $\bar{f}$ and $\bar{g}$ of S with representatives f_0 and g_0, the element $f_0 * g_0$ will be a representative of the element $\bar{f}\bar{g}$ of S, and so is some multiple of $(\bar{f}\bar{g})_0$. We define the cochain z to be this multiple, that is, z is defined by the relation

3.4 $$f_0 * g_0 = z(\bar{f}, \bar{g})(\bar{f}\bar{g})_0 .$$

The cochain z defined by 3.4 is a cocycle, for given any $\bar{f}, \bar{g}, \bar{h} \in G$

$$z(\bar{f}, \bar{g})z(\bar{f}\bar{g}, \bar{h})[(\bar{f}\bar{g})\bar{h}]_0 = z(\bar{f}, \bar{g})[(\bar{f}\bar{g})_0 * h_0] = (f_0 * g_0) * h_0 .$$

Similarly, associating the other way,

$$z(\bar{g}, \bar{h})z(\bar{f}, \bar{g}\bar{h})[\bar{f}(\bar{g}\bar{h})]_0 = f_0 * (g_0 * h_0) ,$$

so that z satisfies the cocycle identity.

We must now show that $A \cong zT(S)$. We define a linear map, F, of $zT(S)$ into A as follows. The elements of S form a basis for $zT(S)$. We define F on this basis by

$$F(\bar{f}) = (\bar{f})_0 \quad \text{for each} \quad \bar{f} \in S,$$

and we extend F to all of $zT(S)$ by linearity. We now show that F is an order and algebra isomorphism of $zT(S)$ onto A.

Since as $\bar{f}$ ranges over S the $(\bar{f})_0$ are mutually disjoint, they are linearly independent and so form a basis for A. Thus F is bijective.

That F is an order isomorphism follows by a routine argument using the fact that the elements of S and the $(\bar{f})_0$ form bases of mutually disjoint positive elements for $zT(S)$ and A respectively.

Finally, to show that F is an algebra isomorphism it is sufficient to show that

$$F(\bar{f} *_z \bar{g}) = F(\bar{f}) * F(\bar{g}) \quad \text{for all } \bar{f}, \bar{g} \in S.$$

But

$$F(\bar{f} *_z \bar{g}) = F(z(\bar{f}, \bar{g})\bar{f}\bar{g}) = z(\bar{f}, \bar{g})(\bar{f}\bar{g})_0 = f_0 * g_0 = F(\bar{f}) * F(\bar{g}) .$$

This concludes the proof of Theorem 3.3.

We now show that the isomorphism classes of twisted algebras over a fixed semigroup, S, depend only on the cohomology classes of the cocycles involved (we will consider the converse question in Theorem 6.5).

PROPOSITION 3.5. *Let S be a finite semigroup, and let $w, z \in Z^2(S, R^+)$. Suppose also that w and z are homologous, that is, $z = (dc)w$ for some $c \in C^1(S, R^+)$. Then $wT(S) \cong zT(S)$.*

Proof. We define a linear map, F, of $zT(S)$ into $wT(S)$ as follows. The algebra $zT(S)$ has as a basis the elements of S. We define F on this basis by

$$F(s) = c(s)s$$

where we view $c(s)s$ as an element of $wT(S)$, and we extend F to all of $zT(S)$ by linearity. As in the proof of Theorem 3.3 it is evident that F is bijective and is an order isomorphism. All that remains to be shown is that F is multiplicative, and it is sufficient to show this on the basis of $zT(S)$ consisting of the elements of S. Given $s, t \in S$,

$$\begin{aligned} F(s *_z t) &= z(s, t)F(st) = [(dc)w](s, t)c(st)st \\ &= [c(s)c(t)/c(st)]w(s, t)c(st)st \\ &= w(s, t)c(s)c(t)st = F(s) *_w F(t) . \end{aligned}$$

4. Cancellation laws. Continuing the proof of the Main Theorem, we show that if the algebra A satisfies axiom MOl (resp. MOr) then the semigroup S found in Theorem 3.3 must satisfy the left (resp. right) cancellation law.

PROPOSITION 4.1. Let S be a finite semigroup, and let $z \in Z^2(S, R^+)$. Then $zT(S)$ satisfies axiom MOl (resp. MOr) if and only if S satisfies the left (resp. right) cancellation law.

Proof. Even if S does not satisfy a cancellation law, Lemma 1.2 applies so that $zT(S)$ satisfies inequality 1.3.

Suppose that S satisfies the left cancellation law. As indicated in § 1 we need only show that if $f, g \in zT(S)$ and if $f \geqq 0$, then

4.2 $$f *_z g^+ \leqq \vee\{f_1 *_z g\colon\ 0 \leqq f_1 \leqq f\} .$$

Now the left cancellation law implies that for any two elements, s, t, of S there is at most one $r \in S$ such that $sr = t$ (and, of course, the finiteness of S then implies that such an r exists). Thus the following definition makes sense: for each $t \in S$ define an element, f_t, of $zT(S)$ by

$$f_t(s) = \begin{cases} f(s) & \text{if } \ g(r) \geqq 0 \quad \text{where } \ sr = t \\ 0 & \text{if } \ g(r) < 0 \quad \text{where } \ sr = t . \end{cases}$$

Then it is clear that $0 \leqq f_t \leqq f$ and it is trivial to check that $(f_t * g)(t) = (f * g^+)(t)$. Inequally 4.2 follows immediately.

Conversely, suppose that the left cancellation law does not hold in S, so that we can find $r_1, r_2, s \in S$ such that $sr_1 = sr_2$ but $r_1 \neq r_2$. Assume that r_1 and r_2 are ordered so that $z(s, r_1) \geqq z(s, r_2)$. Let $f = s$ and $g = r_1 - r_2$. Then $g^+ = r_1$ so that $f * g^+ = z(s, r_1)sr_1$, whereas it is easily checked that

$$\vee\{f_1 * g\colon\ 0 \leqq f_1 \leqq f\} = [z(s, r_1) - z(s, r_2)]sr_1$$

so that inequality 4.2 fails.

A parallel argument applies to axiom MOr.

It is then clear that if we apply Theorem 3.3 to the algebra A of the Main Theorem, the finite semigroup, S, found in Theorem 3.3 satisfies both the left and right cancellation laws and so is a group.

The remaining step in the proof of the Main Theorem is to show that the cocycle, z, found in Theorem 3.3 is a coboundary if A satisfies either axiom MOl or MOr. We do this by showing that if S is a finite semigroup satisfying either the left or right cancellation law then every positive 2-cocycle on S is a coboundary.

PROPOSITION 4.3. If S is a finite semigroup satisfying the left or right cancellation law then $H^2(S, R^+) = \{1\}$.

Proof. We show that the usual averaging argument for groups (we are indebted to C. C. Moore for bringing this argument to our attention) works even in this case.

Suppose that S satisfies the left cancellation law, and that $z \in Z^2(S, R^+)$. Define $c \in C^1(S, R^+)$ by

$$c(s) = \Pi\{z(s, r) : r \in S\} .$$

Then

$$\begin{aligned} dc(s, t) &= [\Pi_r z(s, r)\Pi_r z(t, r)]/\Pi_r z(st, r) \\ &= \Pi_r\{[z(s, r)z(t, r)z(s, t)]/z(st, r)z(s, t)\} \\ &= \Pi_r\{[z(s, r)z(t, r)z(s, t)]/z(s, tr)z(t, r)\} \\ &= [z(s, t)]^n \Pi_r\{z(s, r)/z(s, tr)\} , \end{aligned}$$

where n is the order of S. Now the left cancellation law and the finiteness of S imply that as r ranges over S so does tr for fixed t. Thus

$$\Pi_r z(s, tr) = \Pi_r z(s, r)$$

so that $dc(s, t) = [z(s, t)]^n$. Then if we define a new 1-cochain, c', by $c'(t) = [c(t)]^{1/n}$, since d is a homomorphism it is clear that $dc'(s, t) = z(s, t)$ as desired.

A parallel argument applies for the right cancellation law except that c must be defined by

$$c(s) = \Pi_r z(r, s) .$$

We now obtain.

THEOREM 4.4. *Let A be a FDALO algebra satisfying axiom* MOl *(resp.* MOr*) and axiom P. Then there exists a finite semigroup, S, satisfying the left (resp. right) cancellation law such that $A \cong L(S)$.*

Proof. By Theorem 3.3 there exists a finite semigroup S and a $z \in Z^2(S, R^+)$ such that $A \cong zT(S)$. By Proposition 4.1 the semigroup S satisfies the left (resp. right) cancellation law. By Proposition 4.3 z is homologous to 1, and so by Proposition 3.5 $zT(S) \cong L(S)$. Thus $A \cong L(S)$.

The Main Theorem is an immediate corollary of Theorem 4.4 and Proposition 4.1.

5. Semigroups. One way of viewing the Main Theorem is as follows. It says that if a FDALO algebra satisfying axiom Q also satisfies axiom MO then it is possible to choose a (necessarily unique) basis consisting of pure elements which is closed under multiplication (and in fact forms a group under multiplication). We will now show that for an arbitrary FDALO algebra satisfying axiom Q there is a canonical way of choosing a basis consisting of pure elements which enjoys quite special properties. In particular, if the algebra is commutative this basis will be closed under multiplication, though this need not be true otherwise. If we use this canonical basis as the basis used in the proof of Theorem 3.3 then the cocycle, z, of the theorem will also enjoy quite special properties, and we thus obtain the following strengthened form of Theorem 3.3.

THEOREM 5.1. *Let A be a FDALO algebra satisfying axiom Q. Then there exists a finite semigroup, S, and a $z \in Z^2(S, R^+)$ satisfying*

(a) *$z(s, t) = z(t, s)$ for all $s, t \in S$,*

(b) *if $s, t \in S$ and if $st = ts$ then $z(s, t) = 1$,*

such that $A \cong zT(S)$.

Proof. Let $S = E/R^+$ as in the proof of Theorem 3.3. We will need two results concerning finite semigroups which we now present.

LEMMA 5.2. *Let S be a finite semigroup, and let $s \in S$. Then there exist (strictly) positive integers j and p such that $s^{j+p} = s^j$. If j and p are the smallest positive integers with this property, then for any positive integers k and l with $k > l$ we will have $s^k = s^l$ if and only if $l \geqq j$ and $k = l + np$ for some positive integer n.*

This is just Remark 2.6.1 of [3].

LEMMA 5.3. *Let S be a finite semigroup, let $s, t \in S$, and let j, k, p, q be the smallest positive integers such that $(st)^{j+p} = (st)^j$ and $(ts)^{k+q} = (ts)^k$. Then $p = q$ and $k + 1 \geqq j \geqq k - 1$.*

Proof. $(st)^{k+q+1} = s(ts)^{k+q}t = s(ts)^k t = (st)^{k+1}$ so that by Lemma 5.2 $k + 1 \geqq j$ and $k + q + 1 = k + 1 + mp$ for some positive integer m. Similarly $(ts)^{j+p+1} = (ts)^{j+1}$ so that $j + 1 \geqq k$ and $j + p + 1 = j + 1 + nq$ for some positive integer n. Thus $q = mp = nmq$, so $q = p$.

We remark that the relation between j and k cannot be improved as can be seen by considering semigroup 3 of order 3 in [3, p. 114].

We now continue with the proof of Theorem 5.2. Given any element $\bar{f}$ of S, by Lemma 5.2 there exist positive integers, j and p, such that $(\bar{f})^{j+p} = (\bar{f})^j$. We will now show that there exists a unique element, f_0, in $\bar{f}$ such that $(f_0)^{j+p} = (f_0)^j$. This will give us a canonical way of choosing representatives for the elements of S.

DEFINITION 5.4. An element, f, of A will be called *basic* if it is pure and if there exist positive integers j, p such that $f^{j+p} = f^j$.

LEMMA 5.5. *If f is basic and if $(\bar{f})^{k+q} = (\bar{f})^k$ for some positive integers k and q, then $f^{k+q} = f^k$.*

Proof. Since f is basic, $f^{j+p} = f^j$ for some positive integers j and p. By hypothesis $f^{k+q} = af^k$ for some $a \in R^+$. Then

$$(f^{k+q})^{j+p} = (af^k)^{j+p} = a^{j+p}f^{kj}$$

and

$$(f^{k+q})^{j+p} = (f^j)^{k+q} = (f^{k+q})^j = (af^k)^j = a^j f^{kj} .$$

Thus $a^{j+p} = a^j$ so that $a = 1$.

LEMMA 5.6. *In each element, $\bar{f}$, of S there is a unique basic element. If f is any representative of $\bar{f}$, and if $f^{j+p} = af^j$ for any positive integers j, p and for $a \in R^+$, then this basic element is $a^{-1/p}f$.*

Proof. Let $\bar{f} \in S$ with representative f. Then by Lemma 5.2 there exist integers j, p such that $(\bar{f})^{j+p} = (\bar{f})^j$, that is, $f^{j+p} = af^j$ for some $a \in R^+$.

Now suppose that j, p are any positive integers such that $f^{j+p} = af^j$ for some $a \in R^+$. Let $b = a^{-1/p}$ and let $g = bf$, so $g \in \bar{f}$. Then

$$g^{j+p} = b^{j+p}f^{j+p} = b^j a^{-1} af^j = g^j$$

so that g is basic. Thus each element of S contains at least one basic element.

To show that this element is unique, suppose that there is another element, h, in $\bar{f}$ which is basic, so that $h^{k+q} = h^k$ for positive integers k and q. Then clearly $(\bar{f})^{k+q} = (\bar{f})^q$, that is, $(\bar{g})^{k+q} = (\bar{g})^k$ so that by Lemma 5.5 $g^{k+q} = g^k$. Furthermore $h = cg$ for some $c \in R^+$. Then

$$c^{k+q}g^k = c^{k+q}g^{k+q} = h^{k+q} = h^k = c^k g^k$$

so that $c = 1$ and $h = g$.

This unique basic element in $\bar{f}$ is the one we will now denote by $(\bar{f})_0$ or just f_0.

LEMMA 5.7. *If f and g are basic, and if $f*g = g*f$ then $f*g$ is basic.*

Proof. If $f^{j+p} = f^j$ and $g^{k+q} = g^k$ then a routine calculation shows that $(f*g)^{jk+pq} = (f*g)^{jk}$.

This last lemma shows that if the algebra A is commutative, then the basis consisting of basic elements is closed under multiplication.

Now that we have shown how to choose a unique basic representative for each element of S we use these representatives to define a cocycle on S, just as we did in Theorem 3.3, by the relation

5.8 $$f_0 * g_0 = z(\bar{f}, \bar{g})(\bar{f}\bar{g})_0 .$$

It then follows exactly as in the proof of Theorem 3.3 that $A \cong zT(S)$. To conclude the proof of Theorem 5.1 we need only show that z satisfies properties (a) and (b).

LEMMA 5.9. *The z defined by* 5.8 *satisfies property* (a) *of Theorem* 5.1, *that is,*

$$z(\bar{f}, \bar{g}) = z(\bar{g}, \bar{f}) \text{ for all } \bar{f}, \bar{g} \in S.$$

Proof. Given $\bar{f}, \bar{g} \in S$, let j, k, p, q be the least positive integers such that

$$(\bar{f}\bar{g})^{j+p} = (\bar{f}\bar{g})^{j} \text{ and } (\bar{g}\bar{f})^{k+q} = (\bar{g}\bar{f})^{k} .$$

Then by Lemma 5.3 $p = q$ and $k + 1 \geqq j \geqq k - 1$. Further $f_0 * g_0$ is a representative of $\bar{f}\bar{g}$ and $g_0 * f_0$ is a representative of $\bar{g}\bar{f}$, so there exist $a, b \in R^+$ such that

$$(f_0 * g_0)^{j+p} = a(f_0 * g_0)^{j}, \quad \text{and} \quad (g_0 * f_0)^{k+q} = b(g_0 * f_0)^{k} .$$

Then by Lemma 5.6

$$(\bar{f}\bar{g})_0 = a^{-1/p}(f_0 * g_0), \quad \text{and} \quad (\bar{g}\bar{f})_0 = b^{-1/q}(g_0 * f_0) ,$$

so that $z(\bar{f}, \bar{g}) = a^{1/p}$ and $z(\bar{g}, \bar{f}) = b^{1/q}$. Since $p = q$, it is sufficient for us to show that $a = b$.

If $j = k + 1$ then

$$\begin{aligned} a(f_0 * g_0)^{j} &= (f_0 * g_0)^{k+1+p} = f_0 * (g_0 * f_0)^{k+p} * g_0 \\ &= f_0 * b(g_0 * f_0)^{k} * g_0 = b(f_0 * g_0)^{j} , \end{aligned}$$

so that $a = b$. A parallel argument works if $k = j + 1$.

If $k = j$ then

$$\begin{aligned} a(f_0 * g_0)^{j+1} &= (f_0 * g_0)^{j+p+1} = f_0 * (g_0 * f_0)^{k+p} * g_0 \\ &= f_0 * b(g_0 * f_0)^{k} * g_0 = b(f_0 * g_0)^{j+1} \end{aligned}$$

so that $a = b$.

LEMMA 5.10. *The z defined by* 5.8 *satisfies property* (b) *of Theorem* 5.1, *that is, if $\bar{f}, \bar{g} \in S$ and if $\bar{f}\bar{g} = \bar{g}\bar{f}$ then $z(\bar{f}, \bar{g}) = 1$.*

Proof. From the hypotheses it follows that $(\bar{f}\bar{g})_0 = (\bar{g}\bar{f})_0$, and from Lemma 5.9 $z(\bar{f}, \bar{g}) = z(\bar{g}, \bar{f})$. Thus

$$f_0 * g_0 = z(\bar{f}, \bar{g})(\bar{f}\bar{g})_0 = z(\bar{g}, \bar{f})(\bar{g}\bar{f})_0 = g_0 * f_0$$

so that f_0 and g_0 commute. Then by Lemma 5.7 $f_0 * g_0$ is basic, that is,

$$(\bar{f}\bar{g})_0 = f_0 * g_0 = z(\bar{f}, \bar{g})(\bar{f}\bar{g})_0\ ,$$

so that $z(\bar{f}, \bar{g}) = 1$.
This concludes the proof of Theorem 5.1.

We can now give our characterization of the convolution algebras of finite commutative semigroups.

COROLLARY 5.11. *Let A be a commutative FDALO algebra which satisfies axiom Q. Then there exists a finite commutative semigroup, S, such that $A \cong L(S)$.*

Proof. Applying Theorem 5.1 to A, we obtain the semigroup $S = E/R^+$ and a cocycle z on S which satisfies properties (a) and (b) such that $A \cong zT(S)$. Since A is commutative so is E and thus so is S. Thus by property (b) $z \equiv 1$. Thus $zT(S) = L(S)$.

DEFINITION 5.12. For reasons which will be apparent in Theorem 6.2 we will call a cocycle which satisfies properties (a) and (b) *a fundamental* cocycle.

6. Applications.

As an application of some of the above results we will show how the use of the fundamental cocycles defined above gives a convenient method for computing $H^2(S, R^+)$. As a corollary we will obtain the fact that if S is commutative then $H^2(S, R^+) = \{1\}$.

To do this we need to extend Hewitt and Zuckerman's theorem which states that semigroups with isomorphic convolution algebras are isomorphic [3, Theorem 4.2.4], to the case of twisted algebras. To do this we will need to recall a few facts about the functorial behavior of cohomology groups. Let S and S' be two finite semigroups and let i be a homomorphism of S into S'. Then i induces a map, $\hat{i}$, of $C^n(S', R^+)$ into $C^n(S, R^+)$ for any integer n by assigning to any $c \in C^n(S', R^+)$ the cochain $\hat{i}(c)$ defined by

$$\hat{i}(c)(s_1, \cdots, s_n) = c(i(s_1), \cdots, i(s_n))$$

for $s_1, \cdots, s_n \in S$. It is easily checked that $\hat{i}$ is a homomorphism which carries $Z^2(S', R^+)$ into $Z^2(S, R^+)$, commutes with the boundary operator, d, and so carries $B^2(S', R^+)$ into $B^2(S, R^+)$. Thus $\hat{i}$ induces a homomorphism, which we will also denote by $\hat{i}$, of $H^2(S', R^+)$ into $H^2(S, R^+)$. If for any $z \in Z^2(S', R^+)$ we denote its cohomology class by $\bar{z}$, then we have

$$\hat{i}(\bar{z}) = (\hat{i}(z))^- .$$

THEOREM 6.1. *Let S and S' be finite semigroups, and let $z \in Z^2(S, R^+)$ and $w \in Z^2(S', R^+)$. Suppose that $zT(S) \cong wT(S')$. Then there exists an isomorphism, i, of S onto S' such that $\hat{i}(\bar{w}) = \bar{z}$.*

Proof. Let F be an isomorphism of $zT(S)$ onto $wT(S')$. We define i and a 1-cochain, c, as follows: For $s \in S$, if s is viewed as an element of $zT(S)$, it is pure, and so $F(s)$ is pure, and so is of the form $c(s)i(s)$ for $c(s) \in R^+$, $i(s) \in S'$. Then for any $s, t \in S$

$$\begin{aligned} z(s, t)c(st)i(st) &= F(z(s, t)st = F(s *_z t) \\ &= F(s) *_w F(t) = c(s)c(t)w(i(s), i(t))i(s)i(t) . \end{aligned}$$

Thus $i(st) = i(s)i(t)$, so that i is a homomorphism, and

$$z(s, t) = [c(s)c(t)/c(st)]w(i(s), i(t)) ,$$

so that $\bar{z} = \hat{i}(\bar{w})$. Furthermore, i is injective, for if $s, t \in S$ and $s \neq t$, then, viewed as elements of $zT(S)$, $s \wedge t = 0$, so $F(s) \wedge F(t) = 0$, so $i(s) \neq i(t)$. Finally, since $zT(S)$ and $wT(S')$ are isomorphic they have the same dimension, and so S and S' have the same number of elements. Thus i must be subjective, and so is an isomorphism.

THEOREM 6.2. *Let S be a finite semigroup. Then in each cohomology class of $H^2(S, R^+)$ there is exactly one fundamental cocycle. Further, the fundamental cocycles form a subgroup of $Z^2(S, R^+)$ which is isomorphic to $H^2(S, R^+)$. This shows that the exact sequence*

$$1 \rightarrow B^2(S, R^+) \rightarrow Z^2(S, R^+) \rightarrow H^2(S, R^+) \rightarrow 1$$

splits.

Proof. Let $z \in Z^2(S, R^+)$. Then $zT(S)$ satisfies the hypotheses of Theorem 5.1 and so there exists a finite semigroup S' and a fundamental cocycle, w, such that $zT(S) \cong wT(S')$. By Theorem 6.1 there is an isomorphism, i, of S onto S' such that $\bar{z} = \hat{i}(\bar{w})$. But it is easy to check that if w is fundamental, then so is $\hat{i}(w)$. This shows that there exists at least one fundamental cocycle in each cohomology class.

Next, the fact that the fundamental cocycles form a subgroup of $Z^2(S, R^+)$ is easily checked. Finally, if w and z are two fundamental cocycles such that $\bar{w} = \bar{z}$, then w/z is a coboundary and is a fundamental cocycle, so that $w/z = dc$ for some $c \in C^1(S, R^+)$. Let $s \in S$. Then for any positive integers m and n the elements s^m and s^n commute, so by property (b) of fundamental cocycles

$$1 = w/z(s^m, s^n) = c(s^m)c(s^n)/c(s^{m+n}) .$$

This says that c is a homomorphism of the finite commutative subsemigroup of S generated by s into R^+. Since no element of R^+ is of bounded order except 1, and since s is of bounded order this means that $c(s) = 1$. Since this is true for all s, $c \equiv 1$ and hence $w/z \equiv 1$, so $w = z$.

Thus, to determine $H^2(S, R^+)$ for a given finite semigroup S, we need only determine the group of fundamental cocycles of S. In particular, we obtain.

COROLLARY 6.3. *Let S be a finite commutative semigroup. Then* $H^2(S, R^+) = \{1\}$.

Proof. If z is a fundamental cocycle, then, from property (b) of fundamental cocycles and from the fact that S is commutative, it follows that $z \equiv 1$. Thus the group of fundamental cocycles is $\{1\}$.

We now give an example to show that if S is not commutative then $H^2(S, R^+)$ need not be trivial.

EXAMPLE 6.4. Let S be the "box" semigroup consisting of the four points of the plane $(0, 0), (0, 1), (1, 0), (1, 1)$, with product defined by $(x_1, y_1)(x_2, y_2) = (x_1, y_2)$. For each real number, b, we can define an element, z_b, of $C^2(S, R^+)$ by

$$z_b((x_1, y_1), (x_2, y_2)) = \exp\,[b(x_1 - x_2)(y_1 - y_2)] .$$

It is easily verified that for each b the cochain z_b is in fact a fundamental cocycle, and that every fundamental cocycle of S is of this form. It is also clear that this group of fundamental cocycles is isomorphic to R. Thus

$$H^2(S, R^+) = R .$$

From Theorem 6.1 it is clear that if $b \neq 0$ then $z_bT(S)$ is not isomorphic to the convolution algebra of any finite semigroup. If we wish to characterize the convolution algebras of arbitrary finite semigroups, we must find an axiom which will distinguish between these convolution algebras and those twisted algebras which are essentially different, such as those exhibited directly above. We have not found a suitable such axiom.

Finally, we return to the question of what can be said about two cohomology classes on a finite semigroup, S, if the corresponding twisted algebras are isomorphic. Let I be the group of automorphisms of S. Then, since cohomology is a contravariant functor, the opposite group, I^*, acts as a group of automorphisms of $H^2(S, R^+)$. It is not difficult to prove that the answer to our question is

THEOREM 6.5. *Let S be a finite semigroup, and let $\bar{w}$ and $\bar{z} \in H^2(S, R^+)$. Then $\bar{w}T(S) \cong \bar{z}T(S)$ if and only if $\bar{w}$ and $\bar{z}$ are in the same orbit of $H^2(S, R^+)$ under the action of I^*.*

COROLLARY 6.6. *Let S be a finite semigroup with automorphism group I. Then there is a natural bijection between the isomorphism classes of twisted algebras over S and the orbits of $H^2(S, R^+)$ under the action of I^*.*

The author is indebted to the referee for suggesting a rearrangement of the material of this paper which permitted a considerably clearer and swifter proof of the main theorem.

Added in proof. W. W. Adams has pointed out to us that the proof of uniqueness for Theorem 6.2 shows that property (a) for fundamental cocycles follows from property (b).

REFERENCES

1. G. Birkhoff, *Lattice theory*, Amer. Math. Soc., Providence, 1948.
2. N. Bourbaki, *Eléménts de Mathématique, Livre VI, Intégration*, Ch. II, Act. Sci. et Ind., 1175, Hermann, Paris, 1952.
3. E. Hewitt and H. Zuckerman, *Finite dimensional convolution algebras*, Acta Math. **93** (1955), 67-119.
4. Y. Kawada, *On the group ring of a topological group*, Math. Japonicae, **1** (1948), 1-5.
5. J. G. Wendel, *On isometric isomorphism of group algebras*, Pacific J. Math. **1** (1951), 305-311.

UNIVERSITY OF CALIFORNIA, BERKELEY

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be typewritten (double spaced). The first paragraph or two must be capable of being used separately as a synopsis of the entire paper. It should not contain references to the bibliography. Manuscripts may be sent to any one of the four editors. All other communications to the editors should be addressed to the managing editor, Richard Arens at the University of California, Los Angeles, California 90024.

50 reprints per author of each article are furnished free of charge; additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is published monthly. Effective with Volume 16 the price per volume (3 numbers) is $8.00; single issues, $3.00. Special price for current issues to individual faculty members of supporting institutions and to individual members of the American Mathematical Society: $4.00 per volume; single issues $1.50. Back numbers are available.

Subscriptions, orders for back numbers, and changes of address should be sent to Pacific Journal of Mathematics, 103 Highland Boulevard, Berkeley 8, California.

Printed at Kokusai Bunken Insatsusha (International Academic Printing Co., Ltd.), No. 6, 2-chome, Fujimi-cho, Chiyoda-ku, Tokyo, Japan.

PUBLISHED BY PACIFIC JOURNAL OF MATHEMATICS, A NON-PROFIT CORPORATION

The Supporting Institutions listed above contribute to the cost of publication of this Journal, but they are not owners or publishers and have no responsibility for its content or policies.

* Paul A. White, Acting Editor until J. Dugundji returns.

Pacific Journal of Mathematics

Vol. 16, No. 2 December, 1966