ON THE TRIVIALITY OF FINITE AUTOMORPHIC ALGEBRAS

BY
ERNEST E. SHULT

Introduction

A non-associative algebra A is called *automorphic* if it admits a group of automorphisms G which transitively permutes its one-dimensional subspaces. The following result was announced in [1] and proved in [2].

PROPOSITION. *Let A be a finite-dimensional automorphic algebra with ground field $GF(q)$. If $q > 2$ then either $A^2 = 0$ or A has no zero divisors.*

The object of this note is to clarify the conclusion of the proposition by proving the following:

THEOREM. *Let A be a finite automorphic algebra over $GF(q)$ and suppose $q > 2$. Then either $A^2 = 0$ or A is $GF(q)$ itself.*

Since it was shown in [2] that if $q = 2$, there exists an automorphic algebra without zero divisors of every dimension, the above theorem gives a best-possible criterion on dim (A) and q that a finite automorphic algebra be a zero algebra.

We require a few introductory lemmas.

LEMMA 1. *If A is a finite automorphic algebra over $GF(q)$, and A admits an automorphism which takes some element in A to a distinct scalar multiple of itself, then A has zero divisors.*

Proof. This is Lemma 5 of [2].

LEMMA 2. *If A is a finite automorphic algegra over $GF(q)$ and $A^2 \neq 0$, then*

$$(q - 1, |\operatorname{Aut}(A)|) = 1. \tag{1}$$

Proof. Suppose r were a prime divisor of $q - 1$ and g was an automorphism of A having order r. Then A has a basis of g -eigenvectors. Since $g \neq 1$, by Lemma 1, A has zero divisors. Since $2 \leq r \leq q - 1$, $q > 2$; by the proposition $A^2 = 0$, against hypothesis. Thus (1) holds.

Proof of the theorem

From this point onward we shall assume that A is a finite automorphic algebra over $GF(q)$ satisfying the following hypotheses:

(i) $A^2 \neq 0$,
(ii) $q > 2$,
(iii) $A \neq GF(q)$.

Received February 29, 1968.

To prove the theorem it suffices to show that no such algebra A satisfying (i), (ii), and (iii) exists. We shall achieve this by deducing from hypotheses (i), (ii) and (iii) a series of results ((A) through (E) below) which are incompatible.

(A) *A has no zero divisors and equation* (1) *holds.*

Proof. The first clause follows from hypothesis (i) and Lemma 2. The second follows from (i), (ii), and the proposition.

(B) Aut (A) *contains no subgroup which is transitive on the* 1*-dimensional subspaces of A and has order prime to q.*

Proof. Set $q = p^s$ and $n = \dim(A)$. Let us assume $G \leq \mathrm{Aut}(A)$ is a p'-group transitive on the 1-dimensional subspaces of A. We shall achieve a contradiction by a series of short steps.

(a) $(q - 1, n) = 1$

Suppose a prime t divides $q - 1$ and n. Since A is automorphic, $|G|$ is divisible by the number of 1-dimensional subspaces $1 + q + \cdots + q^{n-1} \equiv n \equiv 0 \bmod t$, so t divides $|G|$. This contradicts (1) and so (a) holds.

(b) $n > 2$

Suppose $\dim(A) = 1$. For nonzero $a \in A$, $a^2 = \alpha a$, for some α in $GF(q)$. From (A), $\alpha \neq 0$. Set $\epsilon = \alpha^{-1}a$. Then $e^2 = e$ and $\gamma \to \gamma\epsilon$ defines an isomorphism $GF(q) \to A$. This contradicts (iii).

Now suppose $n = 2$. By (a), q is a power of 2 and $q + 1$ is divisible by an odd prime r. Lemma 10 (part (a)) of [2] shows that G contains a cyclic irreducible S_r-subgroup S of order r^k dividing $q + 1$. A generator g of S also acts on the algebra $A \otimes K$ with eigenbasis $\{u_0, u_1\}$ where u_i is associated with the root θ^{q^i}, $i = 0, 1$, θ is a primitive r^k-th root, and $K = GF(q)(\theta)$. The products $u_i u_j$ are also g-eigenvectors with roots $\theta^{q^i+q^j}$. Since $\theta^q \cdot \theta = \theta^{1+q}$ is not θ or θ^q, $u_0 u_1 = 0$. Since $A^2 \neq 0$, $(A \otimes K)^2 \neq 0$ so one of u_0^2 and u_1^2 is nonzero. In either case the equation $\theta^2 = \theta^q$ is forced, so $q \equiv 2 \bmod r^k$. But $q \equiv -1 \bmod r^k$ whence $r^k = 3$. It follows that $q + 1$ is a power of 3 so $q = 2$ or 8. By (ii), $q = 8$, so 9 divides $|G|$ and this contradicts $r^k = 3$.

(c) *G contains a normal irreducible self-centralizing cyclic subgroup C whose index divides n.*

Let π be the set of prime divisors of $|G|$ for which elements of prime order r in G act irreducibly on A. Then if G contains a normal S_r-subgroup S for $r \in \pi$, then $C = C_G(S_r)$ satisfies the role of C in (c) by Lemma 10 of [2]. Thus we may assume G contains no normal S_r-subgroups for $r \in \pi$. By the fundamental trichotomy in Theorem 3 of [2], either $G/Z(G) \simeq LF(2, n + 1)$ where $2n + 1$ is a prime or π contains at most the prime $n + 1$. In the former case $|G|$ is even so by (1) q is even. In this case (A) holds. In the latter

case, by (b) and Lemma 13 of [2], $n = 4$ and $q = 3$ or else $n = 6 \equiv$ and $q = 3$ or 5. All of these contradict (a). Thus (c) holds.

(d) *Let* $c = |C|$. *There exist integers* a, b, *with* $0 \leq a \leq (n/2)$, $0 \leq b \leq n - 1$, *such that* $1 + q^a \equiv q^b \bmod c$. q *has exponent* $n \bmod c$.

Let x_1 generate C, let θ_1 be a primitive c-th root of unity, and let $K_1 = GF(q)(\theta_1)$. Since x_1 acts irreducibly on A, the action of x_1 on $A \otimes K_1$ involves a full set of algebraically conjugate eigenroots $\theta_1^{q^i}$, $i = 0, \cdots n - 1$. Thus q has exponent $n \bmod c$. Since (i) forces $(A \otimes K_1)^2 \neq 0$, the product of at least two x_1-eigenvectors is non-zero. This forces the congruence $1 + q^a \equiv q^b \bmod c$. By multiplying through by q^{n-a} if necessary, we may assume $a \leq n/2$.

(e) $|C|$ *is not divisible by* $1 + q + \cdots + q^{n-1}$; *viz.* $C \neq G$.

Let c be a multiple of $1 + q + \cdots + q^{n-1}$. Let a and b be defined as in (d). If $1 + q^a = q^b$ then $a = 0$ and $q = 2$ against (ii). Thus the congruence in (d) involves distinct integers. It follows that one of them exceeds c. Since $b \leq n - 1$, $q^b < c$, by (b). Thus $1 + q^a > c$, against $a \leq n/2$.

(f) *Set* $d = \gcd(n, 1 + q + \cdots + q^{n-1})$. *Then*

(f-1) c *is a multiple of* $(1/d)(1 + q + \cdots + q^{n-1})$
(f-2) $d > q$.
(f-3) n *is not a prime.*

Since C is a normal cyclic subgroup of G, C is $(\frac{1}{2})$-transitive on the 1-dimensional subspaces of A. Since $(q - 1, |C|) = 1$ by (a), c divides $1 + q + \cdots + q^{n-1}$. Since $[G:C]$ divides n, $c = (1/m)(1 + q + \cdots + q^{n-1})$ where m divides n. Since c is an integer, m divides $1 + q + \cdots + q^{n-1}$ so m divides d. Thus (f-1) holds.

Since $q \neq 2$ forces $1 + q^a = q^b$ one of $1 + q^a$ and q^b exceeds

$$(1/d)(1 + q + \cdots + q^{n-1}).$$

Thus either $d(1 + q^a)$ or dq^b exceeds $1 + q + \cdots + q^{n-1}$. Since $\max(a, b) \leq n - 1$, we have $d \geq q$. If $d = q$, (A) holds. Thus $d > q$.

If n is a prime, $d = 1$ or n. $d = 1$ contradicts (f-2) so $d = n$. Since d divides $1 + q + \cdots + q^{n-1}$, $q^n \equiv 1 \bmod n$. Also $q^{\phi(n)} = q^{n-1} \equiv 1 \bmod n$. Thus $q \equiv 1 \bmod n$ since $\gcd(n, n - 1) = 1$. Thus $q > n \geq d$ against (f-2). Hence (f-3).

(g) $n \leq 14$.

Lemma 14 of [2] asserts that if $q > 2$ and $n > 14$ then

$$q^{(3/4)n} \leq (1/n)(1 + q + \cdots + q^{n-1}). \tag{2}$$

Thus if we suppose n > 14, it follows that since $d > 1$, (by (f-2)),

$$q^{m_1} + q^{m_2} > (1/d)(1 + q + \cdots + q^{n-1})$$

implies $\max(m_1, m_2) \geq (\frac{3}{4})n$ whenever $0 \leq m_i \leq n-1$, $i = 1, 2$. For any integer m, let $\bar{m}$ be defined by $0 \leq \bar{m} \leq n-1$, $m \equiv \bar{m} \bmod n$. From (d) and (f-1), for each $k = 0, 1, \cdots, n-1$,

$$q^{\bar{k}} + q^{(k+a)^-} \equiv q^{(b+k)^-} \mod c.$$

Since $n > 14$, this implies that for each k, one of the exponents $(\bar{k}, (k+a)^-, (b+k)^-)$ lies in the inverval $[(\frac{3}{4})n, n-1]$. As $n > 14$ and only three exponents are involved, this is clearly impossible for some k. Hence (g).

(h) $n \leq 14$.

By (b) and (f-3), n is a composite integer between 4 and 14, so $n = 4$, 6, 8, 9, 10, 12 or 14.

If $n = 4$, by (ii) and (f-2), $q = 3$. This contradicts (a).

If $n = 6$, $q = 3$, 4 or 5. All contradict (a).

If $n = 8$, $q = 4$ by (ii) and (f-2). Then $1 + q + \cdots + q^7$ is odd so $d = 1$ against (f-2).

If $n = 9$, $q = 3$, 5, 8 by (ii) and $n > q$. If $q = 3$, $d = 1$ against (f-2). If $q = 5$ or 8, and 3 divides d, then $q^9 \equiv 1 \equiv q^2 \bmod 3$ so $q \equiv 1 \bmod 3$, against $d > q$ (f-2). Thus $d = 1$ against (f-2).

If $n = 10$, by (ii), (a) and $n > q$, $q = 4$ or 8. Then d is odd, so $d = 5$. Since $q^{10} \equiv 1 \equiv q^{\phi(d)} = q^4 \bmod d$, $q^2 \equiv 1 \bmod d$ so $q = 4$. Then

$$1 + q^a \equiv q^b \mod (\tfrac{1}{5})(1 + q + \cdots + q^9)$$

where $a \leq 5$. Then as $5(1 + q^a) < q^6 + q^7$, we have

$$5q^b > 1 + q + \cdots + q^9.$$

This forces $b = 9$ and so

$$q + q^{a+1} \equiv 1 \mod (\tfrac{1}{5})(1 + q + \cdots + q^9).$$

This is an absurdity as both sides are less than the modulus.

If $n = 12$, q is a power of 2 between 4 and 12 such that $q - 1$ is prime to 12. Thus $q = 8$. Then as d is an odd divisor of 12 and $d \neq 1$, $d = 3$. Then

$$q^{m_1} + q^{m_2} > (\tfrac{1}{3})(1 + q + \cdots + q^{11})$$

and $q = 8$, forces $\max(m_1, m_2) = 10$ or 11. Since $\{k, (k+a)^-, (k+b)^-$ does not contain the residues 10 or 11 for all k, the congruence in (d) cannot hold.

If $n = 14$, then $q = 14$ and $d = 7$. Then

$$q^{m_1} + q^{m_2} > (\tfrac{1}{7})(1 + q + \cdots + q^{13})$$

forces $\max(m_1, m_2) = 12$ or 13, since $14^{q^{11}} < q^{13}$. Again since $\{k, (k+a)^-$, $(k+b)^-\}$ does not have non-empty intersection with $\{12, 13\}$ for all $k = 0$, $1, \cdots, 13$, the congruence in (d) cannot hold.

This final contradiction between (g) and (h) proves (B).

(C) *The square of every element in A is a scalar multiple of itself.*

Proof. By (B), $G = \mathrm{Aut}(A)$ has a non-trivial S_p-subgroup S, where $p^s = q$. Then $A_1 = C_A(S)$ is a non-trivial subalgebra of A. By the Burnside fusion theorem, if Q is a p-complement in $N_G(S)$, then Q induces a p'-group of automorphisms of the subalgebra A_1 which acts transitively on its 1-dimensional subspaces. Since by (A), A has no zero divisors, neither does A_1. Thus A_1 satisfies (i) and (ii). It now follows from the fact that (i), (ii), and (iii) imply (B) that the algebra A_1 cannot satisfy all three hypotheses. Hence (iii) fails for A_1 and so $\dim A_1 = 1$. Since A is automorphic, every 1-dimensional subspace is a subalgebra and (C) holds.

(D) *A is not commutative.*

Proof. By (C), for any non-zero $x \in A$ there exists a scalar α_x such that $x^2 = \alpha_x x$. By replacing x by an appropriate scalar multiple of itself, we may suppose x is an idempotent (this is the argument in (A) part (a) applied to the subalgebra $GF(q)x$). By (iii) $\dim A \geq 2$. Thus we can find two linearly independent idempotents x, y in A, and from (C).

$$(3) \qquad (x + \theta y)^2 = x + \theta^2 y + \theta(xy + yx) = \alpha_{x+\theta y}(x + \theta y)$$

for any $\theta \in GF(q)$.

Now suppose A were commutative. Putting $\theta = 1$ in equation (3), we see that $2xy$ is a multiple of $x + y$. Putting $\theta = -1$ in (3), $(x - y)^2$ is a scalar multiple of both $x + y$ and $x - y$. It follows from the linear independence of x and y that $GF(q)$ has characteristic 2. Then (3) yields $x + \theta^2 y$ is a scalar multiple of $x + \theta y$ forcing $\theta = 1$ or 0. As θ is an arbitrary element of $GF(q)$ $q = 2$ contradicting (ii). Thus A is non-commutative.

The final contradiction now occurs in

(E) *A is commutative.*

Proof. Define a new algebra $B = A(+, \circ)$ where $B = A$ as vector spaces over $GF(q)$ and a new product $\circ$ is defined by

$$(4) \qquad x \circ y = xy + yx.$$

Then B is a non-associative algebra satisfying (ii) and (iii). It is easily verified that if $g \in \mathrm{Aut}(A)$, then $(x \circ y)^g = x^g \circ y^g$ and so there is an embedding $\mathrm{Aut}(A) \to \mathrm{Aut}(B)$. Thus B is also a finite automorphic algebra. If hypothesis (i) also held for B, then by (D), B would be non-commutative. Since B is patently commutative, (i) must fail. Thus $B^2 = 0$. This forces A to be anticommutative. Now if $GF(q)$ were odd, $x^2 = -x^2 = 0$ for all $x \in A$, contradicting (A). Thus $GF(q)$ has characteristic 2 and this now makes A commutative.

The contradiction between (D) and (E) exhibits the incompatibility of hypotheses (i), (ii), and (iii) and completes the proof of the theorem.

Remark. The proof does not utilize induction at any point.

References

1. E. Shult, *The solution of Boen's problem,* Bull. Amer. Math. Soc., vol. 74 (1968), pp. 268–270.
2. ———, *On finite automorphic algebras,* Illinois J. Math., vol. 13 (1969), pp. 625–653 (this issue).

Southern Illinois University
Carbondale, Illinois