ON FINITE AUTOMORPHIC ALGEBRAS

BY

Ernest E. Shult

1. Introduction

Throughout this paper, all algebras considered are non-associative algebras, that is, not necessarily associative algebras. We say that an algebra is *automorphic* if it admits a group of automorphisms which acts transitively on its one-dimensional subspaces. We say that an algebra is finite if it contains finitely many elements.

Definition. An algebra is called a *quasi division algebra* if and only if the non-zero elements of the algebra form a multiplicative quasi-group.

The object of this paper is to show the following:

Theorem 1. *Let A be a finite automorphic algebra with ground field F. If F contains more than two elements, then either $A^2 = 0$ or A is a quasi division algebra.*

The principal application of this theorem concerns Boen's problem, and its generalizations. A finite p-group P is said to be p-automorphic if it admits a group of automorphisms G which transitively permutes the elements of order p in P. In [1], Boen considered the problem of showing that p-automorphic p-groups of odd order are abelian. Despite the efforts of several workers [1], [2], [13], [16], [17], [6], [15] this problem has remained open up to the present time.

A more natural setting of this problem is in terms of algebras. It was shown in [2] that if P is a p-automorphic p-group minimal with respect to being non-abelian, then there is associated with P, an algebra A over the field of p elements with the property that A is anticommutative and $A^2 \neq 0$. Moreover if G is the group of automorphisms which acts transitively on the elements of order p in P, then G also acts as a group of operators on the algebra A, in such manner that A and $\Omega_1(Z(P))$ are isomorphic as Z_p G-modules. Accordingly, Kostrikin introduced the notion of *homogeneous algebra*, i.e. a finite-dimensional algebra which admits a group of automorphisms transitively permuting its non-zero elements. A proof that finite homogeneous algebras over fields of odd characteristic are zero-algebras would then solve the corresponding problem on p-automorphic p-groups. In [16] Boen's problem was generalized slightly in another direction by considering *semi-p-automorphic p-groups* (spa-groups), i.e. p-groups whose cyclic subgroups of order p are transitively permuted by a group of automorphisms. The construction of an algebra canoni-

Received January 19, 1968.

TABLE 1

Type of Algebra	Author(s)	Assumptions	Reference
homogeneous	Higman	G is cyclic	[11]
"	Boen	$n < 4$	[1]
"	Boen, Rothaus and Thompson	$n < 6$	[2]
"	Boen, Rothaus and Thompson	$n^{3n^2} < q$	[2]
"	Kostrikin	$n - 6 < q$	[13]
"	Dornhoff	$2n - 3 < q$	[6]
spa-algebra	Shult	n is prime	[16]
"	Shult	G is p-solvable	[17]
"	Dornhoff	$2n - 3 < q$	[6]
"	Passman	G is p-solvable	[15]

cally associated with a minimal non-abelian spa-group still carries through and motivates the corresponding notion of *spa-algebra*, i.e. automorphic algebras which are anticommutative [16]. The fact that every finite dimensional homogeneous algebra is a spa-algebra follows from

LEMMA (Kostrikin [13]). *If A is a finite dimensional homogeneous algebra over a field of odd characteristic, then A is anticommutative.*

To show that p-automorphic p-groups of odd order are abelian, it suffices to prove that either finite homogeneous algebras or finite spa-algebras are zero-algebras if they have odd characteristic. Several authors have obtained such proofs in the presence of special additional assumptions. These results are summarized in Table 1. Throughout Table 1, A is either a homogeneous algebra or a spa-algebra. A has dimension n over $GF(q)$ where q is assumed to be odd. G denotes a group of automorphisms of A satisfying the appropriate transitivity condition. The results are listed in approximate chronological order; although the first four items were proved for q a prime, the proofs apply equally well to algebras over fields containing an odd number q of elements.

All of the results of Table 1 are contained in

COROLLARY 1. *Finite spa-algebras of odd characteristic are zero-algebras.*

More can be said about finite automorphic algebras over fields of characteristic 2. Consider

COROLLARY 2. *Let A be an automorphic algebra over $GF(q)$ and let $G = \text{Aut}(A)$. Let d be the number of G-orbits in $A^{\#} = A - (0)$. If $q - 1 > d$, then $A^2 = 0$. In particular, if $q > 2$, and A is a homogeneous algebra, then $A^2 = 0$.*

The provision that $q > 2$ in the homogeneous case is necessary, as can be seen by the following:

Example. Let $F = GF(2^n)$. Let σ denote the automorphism of F

defined by $(\alpha)^\sigma = \alpha^{2^{n-1}}$. Define a new product $\alpha \circ \beta$ on F by the rule $\alpha \circ \beta = (\alpha\beta)^\sigma$ for any α, β in F. Then it is easy to see that F becomes a quasidivision algebra over $GF(2)$ relative to the operations $\circ$ and field addition. Moreover this algebra is a homogeneous algebra since scalar multiplication by a primitive $(2^n - 1)$st root induces an automorphism of the algebra which transitively permutes the non-zero elements of F.

A number of group-theoretic corollaries follow:

COROLLARY 3. *Let P be a p-group which admits a group of automorphisms transitively permuting its subgroups of order p. Then if p is odd, P is abelian.*

COROLLARY 4. *Suppose G is a group containing one conjugate class of subgroups of odd prime order p. Then a p-Sylow subgroup S of G is abelian if and only if $\Omega_1(S) \leq Z(S)$.*

The following corollary is a generalization of a result of Gaschütz and Yen [9].

COROLLARY 5. *Let p be an odd prime. Suppose G is a p-solvable group whose subgroups of order p are conjugate in the automorphism group of G. Then G has p-length 1 and abelian p-Sylow subgroups.*

All of these corollaries are proved as consequences of Theorem 1 in Section 1 of this paper.

In Section 3 we consider algebras A over a field F and algebras $A \otimes K$ where K is a galois extension of F. The embedding $A \rightarrow A \otimes 1 \subseteq A \otimes K$ induces an injection $\mathrm{Aut}(A) \rightarrow \mathrm{Aut}(A \otimes K)$. A canonical semiautomorphism ψ of $A \otimes K$ is defined which has the property that $A \otimes 1$ comprises the fixed points of ψ in $A \otimes K$ and $\mathrm{Aut}(A)$ is isomorphic to the subgroup of $\mathrm{Aut}(A \otimes K)$ consisting of those automorphisms of $A \otimes K$ which commute with ψ. Facts concerning $\mathrm{Aut}(A)$ impose multiplicative conditions on eigenvectors for these automorphisms in $A \otimes K$. The utility of ψ lies in the fact that the multiplication table of A can then be recovered from the structure constants of $A \otimes K$. As a consequence, ψ and $A \otimes K$ provide a vehicle for deriving information concerning the algebra A from $\mathrm{Aut}(A)$. These methods can be utilized to define a class of quasidivision algebras which admit irreducible automorphisms.

In Section 4, our attention centers on elements in a linear group which have prime order and which act irreducibly on the underlying vector space. A very useful trichotomy (Theorem 3) is obtained for linear groups acting on finite vector spaces of characteristic prime to the group order.

If n denotes the dimension of the underlying space, one proves that either G is metacyclic, is a central extension of $LF(2, 2n + 1)$ (where $2n + 1$ is a prime) or that if x is an irreducible element of prime order in G, then $O(x) = n + 1$. As an application we prove an E_π-theorem which may be regarded as a modular analogue of a theorem of Blichfeldt.

Section 5 contains the main result of the paper (Theorem 4). The section then concludes with a proof of Theorem 1. The essential idea involves a shift away from automorphic algebras to a consideration of a left ideal B in an algebra A which satisfy two conditions: (i) $B^2 = 0$ and left multiplication by any element $x \in A$ induces a nilpotent transformation of B; (ii) The group H of automorphisms of A leaving B invariant acts transitively on the 1-dimensional subspaces of B. The result is that $AB = 0$. This approach admits a more powerful use of induction, leading at once to the case that H has order prime to the field characteristic. Under these conditions the trichotomy of Section 4 can be exploited.

2. Proof of the corollaries

We begin with a few basic ideas of Chevalley [4]. Let R denote the cartesian product of n copies of $GF(q)$ and let $P = GF(q)[x_1, \cdots, x_n]$ be the commutative ring of polynomials in n variables with coefficients from $GF(q)$. Any polynomial F in P can be associated with a mapping $R \to GF(q)$ by assigning values in R to the n-tuple $(x_1, \cdots, x_n)$ and evaluating F. Two polynomials in P are associated with the same mapping $R \to GF(q)$ if and only if they are congruent modulo the ideal I of P generated by $x_i^q - x_i$, $i = 1, \cdots, n$. By a process of replacing x_i^q by x_i, any polynomial F can be converted to a polynomial F such that no monomial summand of F contains a power of x_i as large as q (we say *F is in reduced form*) and $F \equiv F \bmod I$. F is unique with these properties and is called *the reduced form* of F.

LEMMA 1 (Chevalley [4]). *A polynomial in P which is in reduced form induces the zero-map $R \to 0 \in GF(q)$ if and only if it is the zero polynomial.*

This essentially asserts that the polynomials in reduced form comprise a system of distinct coset representatives of I in P.

LEMMA 2 (Chevalley [4]). *If F is a homogeneous polynomial in P having degree less than n (the number of variables) and $F(0, \cdots, 0) = 0$, then there exist an n-tuple ξ in R, such that $\xi \neq (0, \cdots, 0)$ and $F(\xi) = 0$ (i.e. F has a non-trivial zero on R).*

This is Chevalley's theorem that finite fields are quasi-algebraically closed·

Let A be a non-associative algebra. We say that A is *left (right) nil* if and only if the linear transformation L_x (R_x) of A induced by left (right) multiplication by x is a nilpotent linear transformation. We say A is a *nil algebra* if it is both left and right nil.

The following is a minor variation on a lemma of Boen, Rothaus and Thompson [2].

LEMMA 3. *If A is a finite automorphic algebra then either A is nil or A is a quasi-division algebra.*

Proof. Given any two elements a, b in A, there exists an element $g \in G = \mathrm{Aut}(A)$ and a scalar $\beta \in F$, the ground field of A, such that $a = \beta b^g$. If L_a denotes the linear transformation of A induced by left multiplication by a, then L_a and L_b are always projectively similar.

Suppose $\{a_i\}$ is an F-basis of A and let $\{\gamma_{ijk}\}$ be a fixed set of structure constants for$A$ relative to this basis. Then the transformations L_{ai} can be represented by matrices relative to the basis $\{a_i\}$ which depend only on the constants γ_{ijk}. For a general element

$$a = \lambda_1 a_1 + \cdots + \lambda_n a_n \neq 0,$$

the transformation $L_a = \lambda_1 La_1 + \cdots + \lambda_n L_{a_n}$ is represented by a matrix whose entries are linear expressions in the λ_i. It follows that all principal $j \times j$ minors of this matrix are homogeneous polynomials of degree j in the variables $\lambda_1, \cdots, \lambda_n$. If the characteristic equation of L_a is

$$x^n - C_1(\lambda_1, \cdots, \lambda_n)x^{n-1} + \cdots C_{n-1}(\lambda_1, \cdots, \lambda_n)x + C_n(\lambda_1, \cdots, \lambda_n)$$

then each C_j, being a linear combination of these principal $j \times j$ minors, is a homogeneous polynomial of degree j in the λ_i. Moreover, if we write $(\lambda_1, \cdots, \lambda_n)^g$ for $(\lambda_1', \cdots, \lambda_n')$ whenever $a^g = \sum \lambda_i' a_i$, we have that

$$C_j(\lambda_1, \cdots, \lambda_n) = C_j((\lambda_1, \cdots, \lambda_n)^g)$$

for each $q \in G$ and$n$-tuple $(\lambda_1, \cdots, \lambda_n)$ in $F \times \cdots \times F$, since the similarity of L_a and L_{a^g} forces them to have identical characteristic equations. For any other element $b \in A$, L_b is projectively similar to L_a. Thus for any second n-tuple $(\alpha_1, \cdots, \alpha_n)$ there exists a scalar β such that

$$\beta^j C_j(\lambda_1, \cdots, \lambda_n) = C_j(\alpha_1, \cdots, \alpha_n) \quad \text{for } j \leq n.$$

Thus if there exists a choice for $(\lambda_1, \cdots, \lambda_n) \neq (0, \cdots, 0)$ which is a zero for C_j, then C_j vanishes for all n-tuples in $F \times \cdots \times F$. By Lemma 2, such a choice exists for each$j < n$. Thus either L_a has characteristic equation $x^n = 0$ for each $a \in A$, or else L_a has characteristic equation $x^n - C_n(a)$ for each $a \in A$ where $C_n(a) \neq 0$ for all $a \in A - (0)$. Thus either L_a is nilpotent for all $a \in A$ or L_a is non-singular for each $a \in A - (0)$. A similar dichotomy holds among the set of right multiplications. If A is left (right) nil, then some right (left) multiplication is singular and so A is also right (left) nil. Thus either A is nil or $A - (0)$ is a quasi group.

LEMMA 4. *Let F be a finite field and let R be the vector space of n-tuples with entries from F. Let p be a homogeneous polynomial of degree n in $F[x_1, \cdots, x_n]$. Suppose G is a group of linear transformations of R which acts transitively on the one-dimensional subspaces of R and suppose*

$$p(v) = p(v^g)$$

for every $v \in R$ and $g \in G$. Then either

(i) $p(v) = 0$ *for all* $v \in R$ *or*

(ii) *the stabilizer in* G *of a one-dimensional subspace of* R *fixes every vector in that subspace*;

i.e. for any $v \in R$, $g \in G$, $v^g = \lambda v$ *for some* $\lambda \in F$ *implies* $\lambda = 1$ *or* $v = 0$.

Proof. Let d be the number of G-orbits on $R - (0)$; let L be the subspace

$$\{(\lambda, 0, \cdots, 0) \mid \lambda \in F\}$$

of R, and let H be the stabilizer in G of L. Then, because G is transitive on the 1-dimensional subspaces of R, d also represents the number of H-orbits on $L - (0)$. For any $u \in L - (0)$ and $h \in H, u^h = \lambda(h)u$ for some scalar $\lambda(h) \in F$ depending on h and independent of u. It is easy to see that $\lambda(h_1)\lambda(h_2) = \lambda(h_1 h_2)$ for $(h_1, h_2) \in H \times H$ and so λ defines a homomorphism $\lambda: H \rightarrow F^*$, the multiplicative group of non-zero elements of F. Thus for all $u \in L - (0)$, the H-orbit $u^H = \{\lambda(h)u \mid h \in H\}$ has cardinality independent of u. As there are d such orbits and F^* is cyclic of order $q - 1$, we have

$$\lambda(H) \simeq Z_{(q-1)/d}.$$

Now suppose p does not vanish on R. Then for some $v \in R$, $p(v) \neq 0$. We can find $g \in G$ and $\beta \in F^*$ such that $v^g = (\beta, 0, \cdots, 0)$ and so

$$\begin{aligned} 0 = p(\beta, 0, \cdots, 0) &= p((\beta, 0, \cdots, 0)^h) \\ = p(\lambda(h)\beta, 0, \cdots, 0) &= \lambda(h)^n p(\beta, 0, \cdots, 0) \end{aligned}$$

for every $h \in H$ since p is homogeneous of degree n. Thus $\lambda(h)^n = 1$ for all $h \in H$ so $(q - 1)/d$ divides n, or $(q - 1)$ divides nd.

We now show that $(p(x_1, \cdots, x_n))^d$ is constant on $R - (0)$. Set

$$k = (p(1, 0, \cdots, 0))^d.$$

For any $v \in R - (0)$ there exists $(\beta, g) \in F^* \times G$ such that $v^g = (\beta, 0, \cdots, 0)$. Then

$$(p(v))^d = (p(\beta, 0, \cdots, 0))^d = \beta^{nd}k = k, \quad \text{independent of } v,$$

since $\beta \neq 0$ and $q - 1$ divides nd. Set

$$f = k(1 - \textstyle\prod_{i=1}^{n} (1 - x_i^{q-1})).$$

Then both f and p^d have value k on $R - (0)$ and value zero on $(0, \cdots, 0)$. It follows from Lemma 1, that since f is in reduced form, it *is* the reduced form of p^d. Thus

$$nd = \deg(p^d) \geq \deg(f) = n(q - 1)$$

so $d \geq q - 1$. Since d divides $q - 1$, $d = q - 1$ and (ii) holds.

LEMMA 5. *If* A *is a finite automorphic algebra, then either* A *is nil, or* $G = \mathrm{Aut}(A)$ *does not move an element of* A *to a distinct scalar multiple of itself* *(i.e. $d = q - 1$ where q is the cardinality of the ground field of A and d is the number of G-orbits on $A - (0)$.).*

Proof. From Lemma 3, if $\{a_i\}$ is an F-basis for A and $a = \sum \lambda_i a_i$, $\lambda_i \in F$, then the characteristic equation of L_a has the form

$$x^n - C_n(\lambda_1, \cdots, \lambda_n) = 0.$$

IfA is not nil, $C_n(\lambda_1, \cdots, \lambda_n) = p(a)$ is not zero for all $z \in A$. Now p satisfies the conditions on p in Lemma 4 and so (ii) holds for G and A.

We can now prove all the corollaries assuming Theorem 1 as a hypothesis.

Proof of Corollary 1. If A is a finite spa-algebra, anticommutativity and odd characteristic force $a^2 = 0$ for each $a \in A$. Then if $A \neq (0)$ then A contains at least three elements and A is not a quasi-division algebra. As A is automorphic, and the ground field is not Z_2, the result follows from Theorem 1.

Proof of Corollary 2. If $q - 1 > d$, by Lemma 5, A is nil. By Theorem 1, since A is not a quasi-division algebra $A^2 = 0$.

Proof of Corollary 3. Let P be a p-group of odd order chosen minimally with respect to being non-abelian and satisfying the hypothesis of Corollary 3. Then the Frattini subgroup $D(P)$, and $P/\Omega_1(Z(P))$ are both homocyclic abelian p-groups. Thus $[P, P] = \Omega_1(Z(P))$ is elementary and so p-th powers are central and generate $D(P)$. Then there exists a power mapping $\bar{P} = P/D(P) \rightarrow \Omega_1(Z(P))$ which is a G-isomorphism μ between these spaces viewed as G-modules. Since $D(P) = Z(P)$, commutation defines a skew-symmetric bilinear mapping

$$\gamma: \bar{P} \times \bar{P} \rightarrow \Omega_1(Z(P)).$$

Setting $A = \bar{P}$, a G-module, the composition of the G-homomorphism

$$A \times A = \bar{P} \times \bar{P} \xrightarrow{\gamma} \Omega_1(Z(P)) \xrightarrow{\overset{-1}{\mu}} \bar{P} = A$$

defines a product$A \times A \rightharpoonup A$ relative to which A is a non-associative algebra and G is an operator group. Thus, since $A \simeq \Omega_1(Z(P))$ A is a spa-algebra. Since $A^2 = 0$ by Corollary 1, the mapping γ is the zero map and so P is abelian. This contradicts the choice of P and proves the corollary.

Proof of Corollary 4. Suppose $\Omega_1(S) \leq Z(S)$. By Burnside's fusion theorem and the hypothesis of this corollary, a p-complement Q of S in $N_G(S)$ acts as a group of operators of the p-group S transitively permuting its subgroup of order p. As S is odd, S is abelian by Corollary 2. The converse part is trivial.

Proof of Corollary 5. Clearly we may assume $O_{p'}(G) = 1$. Let S be a p-Sylow subgroup of G and set $P = O_p(G)$. We may assume $P > 1$. Then $\Omega_1(S) = \Omega_1(P)$. Next we observe that the semidirect product $H = \text{Aut}(G)\ G$

is a group of operators of P transitively acting on its subgroups of order P. Thus P is abelian. Let Q be a p-complement in $O_{pp'}(G)$. By a Frattini argument we may write $H = N_H(Q)P$. If $S = P$ we are done. Assuming $S > P$, we have $Q > 1$. Then

$$N_H(Q) \cap \Omega_1(P) = Z(O_{pp'}(G)) \cap \Omega_1(P)$$

is an H-invariant subgroup of $\Omega_1(P)$ which is clearly an irreducible H-module. Thus either $\Omega_1(P) \leq C_H(Q)$ or $N_H(Q) \cap \Omega_1(P) = 1$. In the former case, by a theorem of Huppert [12], since P is abelian, P is centralized by Q. This is contrary to Lemma 1.2.3 of Hall and Higman [10]. Thus $N_H(Q)$ is a complement in H to P. Since $\Omega_1(S) \leq P$, $N_G(Q)$ is a p'-group; hence $P = S$, and the proof is complete.

3. The canonical semi-automorphism group

Recall that if V is a vector space over a field K, a mapping

$$f: V \rightharpoonup V$$

is called a semi-linear transformation of V if and only if $f(u + v) = f(u) + f(v)$ for all $u, v \in V$ and there exists $\sigma \in \operatorname{Aut}(K)$ such that $f(\alpha u) = \alpha^\sigma f(u)$ for all $u \in V$ and $\alpha \in K$.

Definition. Let B be an algebra over the field K. A mapping

$$f: B \rightharpoonup B$$

is called a *semi-automorphism* of B if and only if $f(a)f(b) = f(ab)$ for all a, $f \in B$ and f is a semi-linear transformation of B.

If A is an algebra over a field K and F is a subfield of K, then the set $S_F(A)$ of semi-automorphisms f of A satisfying $f(\alpha a) = \alpha f(a)$ for all $a \in A$ and scalars α lying in the subfield F, forms a group. Clearly $\operatorname{Aut}(A) = S_K(A)$ and is a normal subgroup of $S_F(A)$. If P is the prime subfield of K, $S_P(A)$ is the full semi-automorphism group of A. Moreover if $F \subseteq L \subseteq K$ where L is a normal extension of F, then $S_L(A) \trianglelefteq S_F(A)$ and $S_F(A)/S_L(A)$ is a subgroup of the Galois group $G(L/F)$.

Now suppose A is an algebra over F and K is an extension field of F. In the usual way $A \otimes K$ can be endowed with the structure of a K-algebra by asserting that

$$(a \oplus \alpha)(b \otimes \beta) = (ab) \otimes (\alpha\beta)$$

for all $a, b \in A$ and $\alpha, \beta \in K$. Then the mapping

$$a \rightharpoonup a \otimes 1$$

induces an embedding $A \rightharpoonup A \otimes K$ as algebras over F. There is also an embedding

$$\mu: \operatorname{Aut}(A) \rightharpoonup \operatorname{Aut}(A \otimes K)$$

uniquely defined by the requirement that $(a \otimes \alpha)^{(g)} = a^g \otimes \alpha$ for all $g \in G$, $a \in A$ and $\alpha \in K$.

In this paragraph we assume that K is a finite normal separable extension of F. We now define in a canonical way a finite subgroup, $Y(A, K)$ of $S_F(A \otimes K)$ with the properties

(1) $Y(A, K) \simeq G(K/F)$,
(2) $Y(A, K) \cap \text{Aut}\ (A \otimes K) = 1$,
(3) $Y(A, K)\ \text{Aut}\ (A \otimes K) = S_F(A \otimes K)$.

Suppose $[K:F] = n$ and let $\{\varepsilon_\sigma\}$, $\sigma \in G(K/F)$ be a normal F-basis of K. Since

(4) $A \otimes K = A \otimes \varepsilon_1 \oplus \cdots \oplus A \otimes \varepsilon_n$,

where $\{\sigma_i\} = G(K/F)$, the mapping $\psi_\sigma : a \otimes \epsilon_{\sigma_i} \rightharpoonup a \otimes \epsilon_{(\sigma_i \sigma)}$ for all $a \in A$ and fixed $\sigma \in G(K/F)$ can be extended F-linearly to $A \otimes K$, permuting the subsets $A \otimes \varepsilon_{\sigma_i}$ as wholes. Clearly each ψ_σ is a semi automorphism of $A \otimes K$ satisfying $\psi_\sigma(\alpha a) = \alpha^\sigma \psi_\sigma(a)$ for all $a \in A, \alpha \in K$. Since $\psi_\sigma \psi_\tau = \psi_{\sigma\tau}$ (viewing $S_p(A \otimes K)$ as a right operator group), the set

$$\{\psi_\sigma \mid \sigma \in G(K/F)\}$$

forms a group $Y(A, K)$. Clearly $1 = \psi_1$ is the only element in $Y(A, K) \cap \text{Aut}\ (A \otimes K)$. If $f \in S_F(A \otimes K)$ then $f(\alpha a) = \alpha^\tau f(a)$ for all $a \in A$, $\alpha \in K$ and some fixed $\tau \in G(K/F)$ independent of a and α. Clearly $f\psi_{\tau^{-1}}$ and $\psi_{\tau^{-1}} f$ both belong to Aut $(A \otimes K)$ and so

$$Y(A, K)\ \text{Aut}\ (A \otimes K) = S_F(A \otimes K).$$

We can now prove

THEOREM 2. *Suppose A is an algebra over F and K is a normal separable finite extension of F. Then*

(5) $A \otimes 1 = C_{A \otimes K}(Y(A, K))$

Moreover,

(6) $\text{Aut}\ (A) \simeq C_{\text{Aut}(A \otimes K)}(Y(A, K))$

Proof. Suppose $a \in A \otimes K$ is an element fixed by $Y(A, K)$. Then the decomposition (4) yields

$$a = \textstyle\sum_{\sigma \in G(K/F)} a_\sigma \otimes \varepsilon_\sigma , \qquad a_\sigma \in A$$

and for $\psi_\sigma \in Y(A, K)$, $(a_\tau \otimes \varepsilon_\tau)^{\psi_\sigma} = a_\tau \otimes \varepsilon_{\tau\sigma}$ whence the a_σ are all equal. Thus a has the form $a_1 \otimes \sum \varepsilon_\sigma \in A \otimes 1$, from the separability of K/F. Obviously $(a \otimes 1)\psi_\sigma = a \otimes 1$ is a fixed point of $Y(A, K)$ and so (5) holds.

Suppose $g \in \text{Aut}\ (A)$ and $\psi_\sigma \in Y(A, K)$. Then for any $a \in A$,

$$(a \otimes \varepsilon_\tau)^{\mu(g)\psi_\sigma} = (a^g \otimes \varepsilon_\tau)^{\psi_\sigma} = a^g \otimes \varepsilon_{\tau\sigma} = (a \otimes \varepsilon_\tau)^{\psi_\sigma \mu(g)}.$$

Since $\mu(g)$ and ψ_σ are F-linear maps which commute when restricted to the $a \otimes \varepsilon_\tau$ whose F-span is $A \otimes K$, $\mu(\text{Aut}\ (A))$ is centralized by $Y(A, K)$. Now suppose ζ is an automorphism of $A \otimes K$ which commutes with all semi-automorphisms in $Y(A, K)$. Then ζ induces an automorphism on the fixed point set $A \otimes 1$. Thus $(a \otimes 1)^\zeta = a^g \otimes 1$ for some $g \in \text{Aut}\ (A)$ and all $a \in A$. Since ζ is K-linear, $(a \otimes \alpha)^\zeta = a^g \otimes \alpha$ whence $\zeta = \mu(g)$. Thus we see from (1), (2), and (3) that $Y(A, K)$ normalizes the subgroup Aut $(A \otimes K)$ of $S_F(A \otimes K)$ and this group for fixed points of $Y(A, K)$ in Aut $(A \otimes K)$ is precisely $\mu(\text{Aut}\ (A))$. Thus (6) holds.

The next two lemmas will be required for Section 4.

LEMMA 6. *Suppose A is a finite algebra over F. Let g be an element of order m in* Aut (A) *where* char F *does not divide m. If U is a g-irreducible subspace of A and K is an extension of F containing m-th roots, then $U \otimes K$ has a basis of eigenvectors for $\mu(g)$ which are transitively permuted by $Y(A, K)$.*

Proof. Set $|F| = q$. There exists an m-th root θ and an eigenvector $u_0 \in U \otimes K$, such that $(u_0)^{\mu(g)} = \theta u_0$. $Y(A, K) \simeq G(K/F)$ is cyclic, and is generated by an element ψ such that $\psi(\alpha a) = \alpha^q \psi(a)$. Setting $d = \dim U$, the eigenroots for g are $\theta, \theta^q, \cdots, \theta^{q^{d-1}}$, and so setting $u_i = u_0^{\psi^i}$, $i = 0, \cdots, d-1$, the u_i generate $U \otimes K$ and $\psi^d(u_0) = \beta u_0$ for some $\beta \in K$. If q has exponent n mod m, d divides n and $\psi^n = 1$. Thus

$$u_0^{\psi^n} = u_0^{(\psi d)n/d} = \beta\beta^{q^d}\beta^{q^{2d}} \cdots \beta^{q^{n-d}} u_0 .$$

Since $1 + q^d + q^{2d} + \cdots + q^{n-d}$ divides $(q^n - 1)/(q^d - 1)$, it follows that β is a $(q^d - 1)$st power. Hence we can find $\gamma \in K$ such that $\gamma^{q^{d-1}} = \beta^{-1}$. It follows that ψ^d fixes γu_0 and we may use the ψ-orbit of γu_0, as the desired eigenbasis of $U \otimes K$.

LEMMA 7. *Suppose A is a finite algebra over F with left ideal B and suppose $x \in$* Aut (A) *has order m, prime to* char F *and that x leaves B invariant and acts faithfully and irreducibly on B. Let U be an x-irreducible subspace of A different from B and let K be an extension field of F containing primitive m-th roots of unity. Form $U \otimes K$ and $B \otimes K$ and let $u_0, \cdots, u_{d-1}$ be an eigenbasis of $U \otimes K$ relative to the transformation x. Suppose $u_0(B \otimes K)$ is one-dimensional. Then left multiplication of B by any non-zero element $u \in U$, induces a linear transformation of B which is similar to a semilinear transformation of K. In particular, such a transformatiin is non-singular and so $uB = B$ for $0 \neq u \in U$.*

Proof. Set $F = q$, $\dim_F B = n$ and let θ be a primitive m-th root of unity. Then x acts on $B \otimes K$, with n distinct eigenvalues $\theta, \theta^q, \cdots, \theta^{q^{n-1}}$ and q has exponent n modulo m. Similarly x acts with eigenvalues $\theta^k, \theta^{kq}, \cdots, \theta^{kq^{d-1}}$ where $kq^d \equiv 1 \bmod m$. Let ψ generate $Y(A, K)$ where $\psi(\alpha a) = \alpha^q \psi(a)$ for all $\alpha \in K$ and $a \in A$. By Lemma 6, there exist eigenbases $u_0, \cdots, u_{d-1}$ and $b_0, \cdots, b_{n-1}$ of $U \otimes K$ and $B \otimes K$ respectively. By hypothesis $u_0(B \otimes K)$ has dimension 1. On the other hand, for some c and e, $u_0 b_c = \gamma b_e \neq 0$ and

$u_0 b_i = 0$ for $i \neq c$. This forces $k + q^c \equiv q^e \bmod m$. If

$$u = \textstyle\sum_0^{d-1} \alpha_i u_i$$

is fixed by ψ, then $\alpha_0 = \alpha_{d-1}^q = \alpha_{d-2}^{q^2} = \cdots = \alpha_1^{q^{d-1}} = \alpha_0^{q^d}$. Thus if L is an intermediate field such that $F \subseteq L \subseteq K$ and $[L:F] = d$, then for each $\alpha \in L$ we may associate a unique element $u(\alpha) = \sum \alpha^{q^i} u_i$ in $U \otimes 1$, the fixed points of ψ in $U \otimes K$. Similarly for each $\beta \in K$, we may uniquely associate the element

$$b(\beta) = \textstyle\sum_0^{n-1} \beta^{q^i} b_i$$

in $B \otimes 1$, the fixed points of ψ in B. Then

$$\begin{aligned} u(\alpha)b(\beta) &= \textstyle\sum_{i=0}^{d-1} \sum_{j=0}^{n-1} \alpha^{q^i} \beta^{q^j} u_i b_j \\ &= \textstyle\sum_{i=0}^{d-1} \alpha^{q^i} u_i (\beta^{q^{i+c}} b_{i+c} + \beta^{q^{i+d+c}} b_{i+d+c} + \cdots + \beta^{q^{i+(u-d)+c}} b_{i+(n-d)+c} \\ &= \textstyle\sum_{j=0}^{n-1} \alpha^{q^j} \beta^{q^{j+c}} \gamma^{q^j} b_{j+e} \\ &= b(\beta^{q^{c-e}} (\alpha\gamma)^{q^{u-e}}) \end{aligned}$$

Thus left multiplication of B by $u = u(\alpha)$ in $U = U \otimes 1$, corresponds to the transformation

$$\beta \longrightarrow \beta^{q^{c-e}} (\alpha\gamma)^{q^{u-e}} \qquad \text{for all} \quad \beta \in K$$

which is semilinear. The conclusions of the lemma now follow.

The essential result of the previous lemma can be used for the construction of finite quasi-division algebras which admit an automorphism which acts irreducibly on the algebra.

Suppose q is a fixed prime power and that q has exponent n modulo some integer m prime to q. Suppose there exists a congruence of the form $1 + q^a \equiv q^b \bmod m$. Set $F = GF(q)$, $K = GF(q^n)$ and let V be an n-dimensional vector space over K. We may regard V as $U \otimes K$ where U is an n-dimensional space over F. Then there is an irreducible linear transformation x on U satisfying $x^n = 1$, and we can let x' denote its extension to V. Regarding both U and V as algebras for the moment, the mapping corresponding to the semiautomorphism ψ satisfying $\psi(\alpha v) = \alpha^q \psi(v)$ for all $\alpha \in K$, $v\ E\ V$ can be defined. There exists a ψ-invariant eigenbasis $v_0, \cdots, v_{n-1}$ of V relative to x'. We convert V to a non-trivial algebra A by defining $v_0 v_a = \gamma v_b$ for some fixed $\gamma \in K$ and setting

$$v_i v_{i+a} = \gamma^{q^i} v_{i+b}$$

where the subscripts are read modulo n. Then $x' \in \text{Aut}(A)$, and ψ generates $S_F(A) \bmod \text{Aut}(A)$. It follows that U is a subalgebra over F. In fact U is isomorphic to the following algebra U':

As a vector space over F identify U' with K. For any two elements α and β in K define a product $\alpha \circ \beta$ by the equation

$$\alpha \circ \beta = \alpha^{q^{n-b}} \beta^{q^{a-b}} \gamma^{q^{n-b}}$$

where juxtaposition denotes field multiplication. This algebra $U' \simeq U$ admits x' so that it induces an automorphism corresponding to the linear transformation x in U. In U' it corresponds to scalar multiplication by a primitive m-th root in K.

The quasidivision algebra mentioned in Section 1 corresponds to the case that $q = 2$, $a = 0$, $b = 1$ and x is scalar multiplication by a $(2^n - 1)$-st root.

4. The trichotomy

Let $V(n, p^s)$ denote the n-dimensional vector space over the field $GF(p^s)$ and let G be a linear group acting on $V(n, p^s)$. If p does not divide G, the Brauer character of the representation of G on $V(n, p^s)$ is an ordinary character and many of the facts concerning G can be learned from this character. As useful as this procedure may be, many facts concerning the action of G *qua* linear group are lost in passing to the ordinary complex character. In particular we lose information concerning which subgroups of G act irreducibly on $V(n, p^s)$. We shall recoup some of this in Theorem 3 below.

We begin with a standard

LEMMA 8. *Let $\phi_n(x)$ denote the cyclotomic polynomial whose roots are the primitive n-*th *roots of unity and let k be an integer. Then*

$$\phi_n(k) = r^e p_1^{a_1} \cdots p_t^{a_t} \tag{7}$$

where $n = r^\lambda n_1$, and $r \equiv 1 \bmod n_1$ (which makes r the largest prime divisor of n) and $p_i \equiv 1 \bmod n$. Moreover, p_i does not divide $\phi_m(k)$ for any $m < n$. If $n > 2$, $e = 0$ or 1.

Proof. This is essentially the content of Theorems 94 and 95 of Nagell's book [14].

The primes $p_1, \cdots, p_t$ occurring in equation (7) are hereafter denoted the *normal prime divisors* of $\phi_n(q)$.

Now suppose x is an element of prime order p_i, lying in $GL(n, p^s)$where $n > 1$. Then x acts irreducibly on $V(n, p^s)$ if and only if p^s has exponent $n \bmod p_i$. It follows that p_i divides $\phi_n(p^s)$, that $p_i \equiv 1 \bmod n$ and that any other element of order p_i in $GL(n, p^s)$ also acts irreducibly on $V(n, p^s)$.

In this section, π will denote the set of primes dividing the order of G such that if x is an element of prime order, r, in G, then x acts irreducibly on $V(n, p^s)$ if and only if $r \in \pi$. It is easily seen that if π_0 is the set of *normal prime divisors* of $\phi_n(p^s)$ then π is the subset of those primes in π_0 which divide the group order.

LEMMA 9. *Assume n and $q = p^s$ fixed. Then π_0 is empty only if $n \leq 2$ or else $n = 6$, and $q = 2$ (so $\phi_n(q) = 3$).*

Proof. This standard result is Theorem 6 of [5].

LEMMA 10. *Let G be a linear group on $V(n, p^s)$ and let π be the set of primes indicated above, i.e. $\pi = \pi(G) \cap \pi_0$. If $r \in \pi$, let S be an S_r-subgroup of G.*

Then

(a) $C_G(\Omega_1(S))$ *is cyclic and is* $C_G(S)$.

(b) $N_G(\Omega_1(S)) = N_G(S)$ *and* $[N_G(S):C_G(S)]$ *divides* n.

(c) S *is a TI set in* G.

(d) $\Omega_1(S)$ *centralizes every* $\{p, r\}'$*-subgroup of odd order in* G *which it normalizes. A similar conclusion holds with* S *replacing* $\Omega_1(S)$.

Proof. Since all parts of the lemma hold for $n = 1$, assume $n \geq 2$.

Let x be an element of order r lying in the center of S. Let θ be a primitive r-th root, set

$$K = GF(p^{ns}) = GF(p^s)(\theta) \quad \text{and} \quad V = V(n, p^s) \otimes K.$$

Then x acts on V as a matrix similar to diag $(\theta, \theta^q, \cdots, \theta^{q^{n-1}})$, and has distinct eigenvalues. It follows that the centralizer of x in $GL(n, K)$ consists of diagonal matrixes and so $C_G(x)$ is an irreducible abelian subgroup of $GL(n, p^s)$. As a result, $C_G(x)$ is cyclic. From our choice of x, $C_G(x)$ centralizes S and so (a) holds.

Since $\Omega_1(S)$ is characteristic in S, $N_G(S) \leq N_G(\Omega_1(S))$. The latter normalizes $C_G(\Omega_1(S))$ and its characteristic subgroup S. Thus $N_G(\Omega_1(S)) = N_G(S)$. Since Aut $(\Omega_1(S))$ is cyclic, so is $N_G(\Omega_1(S))/C_G(\Omega_1(S))$. Thus $N_G(\Omega_1(S))$ induces a cyclic $\frac{1}{2}$-transitive permutation group on the eigenvalues θ^{q^i} and so the order of this cyclic group divides $\dim_K V = n$, and (b) holds.

If $1 < L = S \cap S^x$, for some $x \in G$ then $\Omega_1(S) \leq L$ so both S and S^x centralize $\Omega_1(S)$. As S is the only S_r-subgroup of $C_G(\Omega_1(S))$, $S = S^x$. Thus (c) holds.

Let N be a $\{p, r\}'$-subgroup of G which is normalized by $\Omega_1(S)$ and suppose N is not centralized by $\Omega_1(S)$. Since S and N have coprime orders, for each prime t dividing $|N|$, N contains an S_t-subgroup normalized by $\Omega_1(S)$. We can find a prime such that the normalized S_t-subgroup of N is not centralized by $\Omega_1(S)$. Choose T minimal in this subgroup with respect to being normalized but not centralized by $\Omega_1(S)$. Then T is a special t-group whose Frattini factor group has order t^m and is acted on irreducibly by $\Omega_1(S)$. Form the p'-subgroup $H = \Omega_1(S)T$ and view $V_0 = V(n, p^s)$ as an H-module. Then V_0 has an absolutely irreducible constituent V_{00} whose kernel H_1 does not contain T. If $H_0 = D(T)$, H/H_0 is Frobenius, and $\dim V_{00} = r \leq \dim V_0 = n$. This contradicts $r \equiv 1 \bmod n$. Thus $T/T \cap H_0$ is extraspecial and so $\dim V_{00} = t^{1/2m} < n$. Since r is a prime exceeding $n + 1$ and r divides $t^m - 1$, r equals $t^{1/2m} + 1$. Since $n \geq 2$ and $r \in \pi_0$, r is odd. Then $r = t^{1/2m} + 1$ forces $t = 2$ contrary to the hypothesis of (d). Thus (d) holds, completing the proof of the lemma.

The following lemma concerns TI sets and ordinary complex characters.

LEMMA 11. *Let* H *be a TI set in* G. *Suppose* H *is abelian and that* H *is embedded in* G *so that*

(a) $H^x \leq N_G(H)$ *implies* $H^x = H$,

(b) $1 < H_0 \leq H$ *implies* $C_G(H_0) = C_G(H)$.

If G *has a faithful character of degree* $\leq |H|^{1/2} - 1$ *then* $H \trianglelefteq G$.

Proof. If $H \leq L \leq G$, then the hypotheses of the pair (H, G) inherit to the pair (H, L). Thus if $H \trianglelefteq L < G$, by induction, $H \trianglelefteq L$. Thus we may assume that $N_G(H)$ is the unique maximal subgroup of G containing H. Now suppose $H \leq N \triangleleft G$. Then $H^x \leq N \leq N_G(H)$ for all $x \in G$. By (a), this implies $H \triangleleft G$ and we are done. Thus H is not contained in any proper normal subgroup of G. Now set $H^{\#} = H - \{1\}$, and set

$$N_0 = \{\cup_{x \in H} C_G(x)\} - Z(G) = C_G(H) - Z(G) \quad \text{by (b)}.$$

If $x \in N_0 \cap N_0^g$, both H and H^g lie in $C_G(H)$. Thus either $N_0 \cap N_0^g = N_0$ or $\emptyset$. Now set $N_1 = N_G(N_0)$. Then $N_1 = N_G(C_G(H))$. Clearly, $N_G(H)$ normalizes $C_G(H)$ so $N_G(H) \leq N_1$. For any $y \in N_1$, $H^y \leq C_G(H)$ so $H^y = H$ by (a). Thus $N_1 = N_G(G)$. We have thus verified the hypotheses 24.1 of [7]. It now follows from Theorem 24.3 of [7] that $\chi(1) > |H|^{1/2} - 1$ for every faithful character of G. As this is a contradiction, $H \trianglelefteq G$.

LEMMA 12. *If S is an S_r-subgroup of a linear group G acting on $V(n, p^s)$ then S satisfies the conditions* (a) *and* (b) *of Lemma* 11.

Proof. For any $x \in G$, $S^x \leq N_G(S)$ implies $S = S^x$ since S is the unique S_r-subgroup of $N_G(S)$.

Also if $1 < S_0 \leq S$, then $\Omega_1(S) \leq S_0$. Thus $C_G(S) \leq C_G(S_0) \leq C_G(\Omega_1(S))$ and all three are equal by Lemma 10, part (a).

THEOREM 3. *Let G be a linear group on $V(n, p^s)$ and let π be the set of primes $\pi(G) \cap \pi_0$. If $p \nmid |G|$, then one of the following three cases holds*:

(a) *G contains a normal irreducible cyclic subgroup C of index dividing n*;

(b) *G is a central extension of $LF(2, 2n + 1)$ and $\pi = \{2n + 1\}$ or $\{n + 1, 2n + 1\}$*;

(c) *π contains at most the single prime $n + 1$, where $(n + 1)^2 \nmid |G|$.*

Proof. Suppose $r \in \pi$. Let Σ be the Brauer character of the representation of G on $V(n, p^s)$. Then Σ is a faithful ordinary complex character of G of degree n. Let S be an S_r-subgroup of G. If $|S|^{1/2} - 1 \geq n$, $S \trianglelefteq G$ by Lemmas 11 and 12. Then $G = N_G(S)$ and so (a) holds by Lemma 10. Now $r \equiv 1 \bmod n$, by the definition of π_0. If $r > 2n + 1$, again $S \trianglelefteq G$ and (a) holds by a fundamental theorem of Feit and Thompson [8]. Thus $r = 2n + 1$ or $n + 1$. If $r = 2n + 1$, r divides $|G|$ to the first power only and (b) holds, by a deep theorem of Brauer [3]. Thus we may assume $\pi = \{r\} = \{n + 1\}$. Suppose $S = r^a$ where $a \geq 2$. Then $|S|^{-/2} \geq q = n + 1$ so $|S|^{1/2} - 1 \geq n$ contrary to what we know about S. Thus (c) is proved.

To illustrate the usefulness of the trichotomy of Theorem 3, we include as an easy application, an

E_π-THEOREM. *Suppose G is a p'-group acting on $V(n, p^s)$. Let π be defined as in Lemma 9. Then either G contains a π-Hall subgroup or both $n + 1$ and $2n + 1$ are primes and G is a central extension of $LF(2, 2n + 1)$.*

Proof. We may assume $|\pi| \geq 2$. Theorem 3 applies to force case (b).

If $\pi = \pi_0$, case (c) of Theorem 3 holds when $\pi_0 = \{n + 1\}$ and $(n + 1)^2$ does not divide $\phi_n(p^s)$. It will be useful to us to determine at just what values of p^s and n this can occur.

LEMMA 13. *Suppose k is an integer greater than 2, and suppose n is a positive integer. Let r be the largest prime dividing n. Then if $b = 0$ or 1, we have*

$$\phi_n(k) = r^a(n + 1)^b$$

only in the following cases:

$$\begin{aligned} &n = 2, \quad k \text{ any integer of the form } 2^a - 1 \text{ or } 3\cdot 2^a - 1;\\ &n = 4, \quad k = 3, \quad r^a(n + 1)^b = 10;\\ &n = 6, \quad k = 3, \quad a = 0, \quad b = 1;\\ &\qquad\quad k = 5, \quad a = b = 1.\end{aligned}$$

Proof. The proof proceeds by a series of short steps.

(a) *Let r_1 and r_2 be primes. Then $r_1^{r_2-1} \geq \max(r_1, r_2)$.*

If $r_1 \geq r_2$, $r_1^{r_2-1} \geq r_1 = \max(r_1, r_2)$, and if $r_1 < r_2$ then $r_1^{r_2-1} \geq 2_1^{r_2-1} > r_2$.

(b) *Suppose $n = n_1 n_2$ where $(n_1, n_2) = 1$ and $n_1 > n_2 > 2$. Let r, r_1 and r_2 be the largest prime divisors of n, n_1 and n_2 respectively. Then $r = \max(r_1, r_2)$. If*

$$(k - 1)^{\phi(n_1)} > r_1(n_1 + 1)$$

then $(k - 1)^{\phi(n)} > r(n + 1)$.

Clearly

$$\begin{aligned}(k - 1)^{\phi(n)} &= ((k - 1)^{\phi(n_1)})^{\phi(n_2)} > r_1^{r_2-1}(n_1 + 1)^2\\ &\geq \max(r_1, r_2)(n_1 n_2 + 1) = r(n + 1).\end{aligned}$$

(c) *Let q be a prime number. Then if $k \geq 3$*

$$(k - 1)^{(q-1)q^{a-1}} > q(q^a + 1)$$

unless $q^a = 2$ and $k \leq 7$, $q^a = 3, 4$ and $k \leq 4$ or $q^a = 5$ or 8 and $k = 3$.

First we directly verify the inequality when $q^a = 2^4, 3^2, 5^2$ and $k = 3$, when $q^a = 2^3, 5$ and $k = 4$, or $q^a = 2^2, 3$ and $k = 5$. If $q^a = 2$, it is easily seen that the inequality implies $k > 6$. Now suppose for some value of b and k that

$$(k - 1)^{(q-1)q^{b-1}} > q(q^b + 1).$$

Then raising both sides to the q-th power

$$(k - 1)^{(q-1)q^b} > (q)q^b + 1))^q > q^q(q^{q^b} + 1^q) > q(q^{b+1} + 1).$$

Thus (c) holds by induction, if we can prove the inequality for $a = 1$, $q > 5$. It suffices to show this when $k = 3$, $q \geq 7$. But in general if $s \geq 7$, then

$2^{s-1} > s(s+1)$ since this holds for $s = 7$, and if it holds for $s = t$, then $2^{(t+1)-1} = 2\cdot 2^{t-1} > 2t(t+1) > t(t+1) + 2(t+1) = (t+1)(t+2)$ and it holds for $t+1$. Thus (c) is proved.

(d) *If $k \geq 3$, the inequality*

$$(k-1)^{\phi(n)} > r(n+1) \tag{8}$$

holds except possibly when n has the form $2\cdot q^a$, where $q^a > 5$ and q is an odd prime, or when n has the form $n = 2^a 3^b 5^c$ where $0 \leq b, c \leq 1$ and $0 \leq a \leq 3$.

This is a consequence of combining (b) and (c).

(e) *The inequality* (8) *holds if $n = 2q^a$ where $(q-1)q^{a-1} \geq 6$ and $a > 1$*.

We apply the inequality $2^{s-1} > s(s+1)$ established in the proof of (c). Thus if $(q-1)q^{a-1} \geq 6$,

$$2^{(q-1)q^{a-1}} > (q-1)^2 q^{2a-2} + 3(q-1)q^{a-1} + 2.$$

Since $q \geq 3$, $q^2 + 1 > 4q$ or $(q-1)^2 > 2q$. Thus

$$\begin{aligned} 2^{(q-1)q^{a-1}} &> 2q^{2a-1} + 3(q-1)q^{a-1} + 2 \\ &> 2q^{a+1} + q = q(2q^a + 1) = r(n+1) \end{aligned}$$

if $a \geq 2$.

(f) *The inequality* (8) *holds if $n = 2q$ where q is a prime > 7.*

First, $2^8 > 161 = 9(2\cdot 9 + 1)$. If $2^{t-1} > t(2t+1)$ then

$$2^t > t(2t+1) + 3(2t+t) > t(2t+1) + 4t + 3 \quad \text{if} \quad t \geq 3.$$

(g) *If $n \equiv 0 \bmod 15$, then* (8) *holds.*

If $n = 30$, or 15, $(k-1)^{\phi(n)} \geq 2^8 = 256$ while $r = 5$ and $r(n - 1 = 80$ or 155. From (b) with $n_1 = 15$, the cases $n = 60$ and 120 are also covered.

(h) *If $k \geq 3$, $\phi_n(k) > r(n+1)$ unless $n = 8, 10, 12,$ or 14 with $k = 3$, $n = 3$ or 4 with $k \leq 4$, $n = 2$ with $k \leq 7$, or $n = 6$, with $k \leq 5$.*

$$\phi_n(k) = \textstyle\prod_{i=1}^{\phi(n)} |(k - \omega_i)| \geq (k-1)^{\phi(n)}$$

where ω_i ranges over the primitive n-th roots of unity (equality holds only when $n = 1$). But the right side exceeds $r(n+1)$ except possibly when $n = 14$ (from (f)), when $n = 5, 8$ (with $k = 3$), $n = 3, 4$ (with $k \leq 4$), when $n = 6, 12, 24$ or $n = 10, 20$ or 40 with $k = 3$ (from (g)). If $n = 5$, $\phi_5(k) \geq \phi_5(3) = 131$ and this exceeds $5(5+1) = 30$. If $n = 20$ or 40, $2^{\phi(n)} > 2^8 > 5\cdot 41$. If $n = 24$, $2^{\phi(n)} = 2^8 > 3\cdot 25 = 75$. The possibilities are thus those specified in (h). The bounds on k are determined from $2^{\phi(n)} \leq r(n+1)$ in each case.

We are now in a position to prove the lemma. From Theorems 94–95 of

[14], if $n > 2$, the exponent of r in $\phi_n(k)$ is at most 1, and all other prime divisors are congruent to unity modulo n. Thus if $(n + 1)$ occurs as a factor, $n + 1$ is a prime number. Thus in the case that $n = 3$, 8 or 14, we have $\phi_n(k) = 3$, 2 or 7, respectively. For $n = 3$, this would imply $k = 1$. If $n = 8$ or 14, $\phi_n(k) \geq 2^{\phi(n)} > 2^4 > \max(2, 7)$, and so these cases are impossible. If $n = 2$, the equation reads $k - 1 = 2^a \cdot 3^b$ so any $k \equiv 1 \bmod 2^a$ or $3 \cdot 2^a$ provides a solution. If $n = 10$, or 12, either $\phi_n(k) = 5$ or 3, 11 or 13, or else $\phi_n(k) = r(n + 1) = 55$ or 39. In the former case, $\phi_n(k) > 2^{\phi(n)} > 2^4 > 13$ and so the equation cannot hold. Thus $\phi_{10}(3) = 55$ or $\phi_{12}(3) = 39$, since $k = 3$ in these cases in order to avoid the inequality (8). But $\phi_{10}(3) \geq 55$ so the inequality in (b) holds. Similarly $\phi_{12}(3) = 3^4 - 3^2 + 1 = 73 \neq 39$. Thus $n = 10$ and 12 are excluded. Now suppose $n = 4$. We then have $k^2 + 1 = r^a(n + 1)^b = 2^a 5^b$. The only possible solution here is $k = 3$, $a = 1 = b$. Finally if $n = 6$, we have $k^2 - k + 1 = 3^a \cdot 7^b \leq 21$. Here we obtain a solution when $k = 5$, $a = b = 1$, or $k = 2$, $a = 1$, $b = 0$, against $k \geq 3$.

In the proof of the main theorem of the next section, we require two minor number-theoretic results.

Lemma 14. *If $n > 14$ and $q > 2$, then*

$$q^{3/4n} \leq \frac{1}{n}\left(\frac{q^n - 1}{q - 1}\right)$$

Proof. Suppose $n > 14$. Then from

$$\left(\frac{n+1}{n}\right)^4 \leq \left(\frac{16}{15}\right)^4 < 3 \quad \text{and} \quad 15^4 \leq 3^{11}$$

we obtain from $q > 2$ that $n^4 \leq 3^{n-4} \leq q^{n-4}$. Thus $n \leq (q^{1/4n} - 1)/(q - 1)$ and the result follows.

Lemma 15. *If $n \geq 12$, $3^{n-1} > (2n + 1)^3$.*

Proof. This follows at once from $(27/25)^3 < 3$.

5. The main theorem

The title of this section refers to

Theorem 4. *Let A be a finite-dimensional algebra over $GF(q)$ and let B be a left ideal in A with the property that $B^2 = 0$. Then left multiplication of all the elements of B by a fixed element a in A induces a linear transformation $L_a: B \rightarrow B$. Suppose L_a is nilpotent for every a in A and suppose A admits a group of automorphisms G which leaves B invariant and acts transitively on the one-dimensional subspaces of B. If $q > 2$, then $AB = 0$.*

Proof. First we replace A by another algebra A^* also satisfying the hypotheses of this theorem, and such that the conclusion of the theorem holds for A if and only if it holds for A^*. Let $W = A/B$ as a $GF(q)G$-module and formally set $A^* = W \oplus B$ as G-modules. We define multiplication as follows. Set $W^2 = B^2 = BW = 0$. For $b \in B$ and $w \in W$ we have that w is a coset $a + B$, and that in A the products $(a + B)b = a\,b$, is a unique element of B, since $B^2 = 0$. Thus if $w = a + B$, and $b \in B$, we may unambiguously define the product wb in A^* to be ab. It is now clear that A^* is a non-associative algebra, containing B as a left (indeed 2-sided) ideal and that as a G-module, A^* admits G as a group of operators preserving all algebraic operations in A^*. Clearly $A^*B = 0$ if and only if $WB = 0$ if and only if $AB = 0$. If

$$\bar{G} = G/(C_G(A/B) \cap C_G(B))$$

(G mod the stabilizer of the chain $A \geq B \geq 0$) then $\bar{G}$ acts as a group of automorphisms of A^*, transitively permuting the one-dimensional subspaces of its left ideal B. Thus without loss of generality we may assume the following

HYPOTHESES. (i) *A is a non-associative finite algebra over $GF(q)$.*

(ii) *$A = W \oplus B$ where $W^2 = B^2 = BW = 0$ and $0 \neq WB \leq B$.*

(iii) *A admits a group of automorphisms G leaving both subalgebras W and B invariant, and acting transitively on the 1-dimensional subspaces of B.*

(iv) *For each $w \in W$, the mapping $L_w : B \rightarrow B$ defined by $b \rightarrow wb$ for all $b \in B$, is a nilpotent transformation of B.*

(v) *$q > 2$.*

The proof now proceeds by a series of short steps utilizing induction on dim A.

(a) *If $w \in W$ and $wB = 0$, then $w = 0$.*

If $W_0 = \{w \mid w \in W,\ wB = 0\}$ then W_0 is a G-invariant subspace of W. By (ii) $W_0 < W$. Then $A_1 = (W/W_0) \oplus B$ is a well-defined algebra admitting $G = G/(C_G(W/W_0) \cap C_G(B))$ as a group of automorphisms. Clearly hypotheses (i) through (v) hold with A_1, W/W_0, B and G in the roles of A, W, B, and G, respectively. If $W_0 > 0$, $\dim A_1 < \dim A$ and induction applies to force $(W/W_0)B = 0$. Thus $WB = 0$ against (ii). Thus $W_0 = 0$ and (a) holds.

(b) *W is an irreducible G-module.*

If W is not irreducible, we can find a non-trivial submodule U. Since $W^2 = 0$, $U \oplus B$ is a proper subalgebra of A, admitting G as a group of operators, in such manner that $U \oplus B$, U, B and $G_1 = G/C_G(U \oplus B)$ satisfy the roles of A, W, B and G in hypotheses (i) through (iv). By induction, $UB = 0$. By (a), $U = (0)$, contrary to the choice of U. Thus (b) holds.

(c) *G acts faithfully on B.*

Let $H = C_G(B)$ so $H \trianglelefteq G$. Then for any $h \in H$, $w \in W$ and $b \in B$ we have

$wb = (wb)^h = w^h b$ so $(w^h - w)b = 0$ so $w^h = w$ by (a). Thus H fixes *both* W and B. Whence H consists of the identity automorphism alone. Thus (c) holds.

(d) *G is a p'-group, where p is the characteristic of $GF(q)$.*

Suppose G has a non-trivial S_p-subgroup P. Set

$$Z_1 = \{b \mid b^x = b \quad \text{for all} \quad x \in P\}$$

and inductively define

$$Z_i = \{b \mid b^x - b \in Z_{i-1} \quad \text{for all} \quad x \in P\}.$$

We thus form a "central series"

$$0 < Z_1 < Z_2 < \cdots < Z_m = B.$$

Since $P > \langle 1 \rangle$, and (c) implies that P acts non-trivially on B, we have $m > 1$. Form a similar "central series"

$$0 < U_1 < U_2 < \cdots < U_k + W$$

for W. Then

$$U_1 \oplus Z_1 = \{a \mid a \in A, a^x = a \quad \text{for all} \quad x \in P\}$$

and clearly forms a subalgebra of A, and Z_1 is an ideal in $U_1 \oplus Z_1$. From a theorem of Burnside, $N_G(P) = PQ$ acts transitively on the one-dimensional subspaces of Z_1, so that $U_1 \oplus Z_1$, U_1, Z_1 and $Q/C_Q(U_1 \oplus Z_1)$ satisfy the roles of A, W, B and G in hypotheses (i) through (iv). (Note that for $u \in U_1$, the restriction of L_u to Z_1 is still nilpotent.) Since $Z_1 < B$, induction applies to yield $U_1 Z_1 = 0$. Now suppose for some integer j, such that $0 < j < m$, we have $U_j Z_1 = 0$. Then for any $u \in U_{j+1}$, $z_1 \in Z_1$ $x \in P$,

$$(uz_1)^x = u^x Z_1 = uz_1 + (u^x - u)Z_1 = uz_1$$

since $u^x - u \in Z_j$ and $Z_j B = 0$. Thus $uz_1 \in Z_1$. Then $U_{j+1} \oplus Z_1$ is a subalgebra of A and $U_{j+1} \oplus Z_1$, U_{j+1}, Z_1, $Q/C_Q(U_{j+1} \oplus Z_1)$ satisfy the roles of A, W, B and G in hypotheses (i) through (iv). Since $Z_1 < B$, induction on $\dim A$ applies to force $U_{j+1} Z_1 = 0$. Mathematical induction on j now yields $WZ_1 = U_k Z_1 = 0$. By (iii), $Z_1^G = \langle Z_1^g \mid g \in G \rangle = B$ and so $WB = 0$ against (ii). This contradiction forces $P = 1$ so (d) holds.

(e) *Let π_0 be the set of prime divisors of $\phi_n(q)$ which are prime to n, where $n = \dim B$ and $\phi_n(x)$ is the cyclotomic polynomial for n-th roots of unity. Then if $n > 1$ all primes in π_0 divide $|G|$, and one of the following hold:*

(i) *G contains a normal S_r-subgroup, for some $r \in \pi_0$.*

(ii) *$\pi_0 = \{n + 1, 2n + 1\}$ or $\{2n + 1\}$, G is a central extension of $LF(2, 2n + 1)$ where $2n + 1$ is a prime.*

(iii) *π_0 is empty or consists of the prime $n + 1$ alone. In the latter case $(n + 1)^2$ does not divide $|G|$.*

Since G acts transitively on the $(q^n - 1)/(q - 1)$ one-dimensional subspaces of B, $\phi_n(q)$ divides $|G|$ or $n = 1$. The last part follows from the trichotomy theorem (Theorem 3).

(f) $n > 2$.

If $n = 1$, L_w being nilpotent implies $wB = 0$ for all $w \varepsilon W$. This contradicts hypothesis (ii).

Suppose $n = 2$. Select $w_1 \epsilon W$, $w_1 \neq 0$. Then as $w_1 B \neq 0$, there exists $b \epsilon wB$ such that $w_1 b = 0$ and $b \neq 0$. Since $W(w_1 B) = 0$ implies $WB = 0$ (against (ii)), we have $W(w_1 B) \neq 0$ so $w_2(wb) \neq 0$ for some $w_2 \epsilon W$. (Clearly w_1 and w_2 are linearly independent.) Nilpotence of L_{w_1} now shows that $w_2 w_1 b \notin wB$. Thus $\{w_2 w_1 b, w_1 b\}$ is a basis for B and regarding the L_w as left operators of B we have relation to this basis,

$$L_{w_1} = \begin{pmatrix} 0 & 0 \\ \alpha_1 & 0 \end{pmatrix}, \quad L_{w_2} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \qquad \text{where } \alpha_1 \neq 0.$$

Clearly $L_{w_1+w_2}$ is non-singular, against (iii).

(g) $\pi_0 \neq \emptyset$.

By (v), $q > 2$. If π_0 were empty, $\phi_n(q)$ is a power of the largest prime divisor of n by step (f) and Lemma 8. Since $q > 2$, Lemma 9 applies to force $n = 2$ and q a Mersenne prime. This is excluded by (f) so π_0 is not empty.

This step shows that G contains elements of prime order which act irreducibly on B. The next two steps concern the action of irreducible cyclic subgroups of G.

(h) *If C is an abelian subgroup of G with distinct absolutely irreducible constituents on B (e.g., if C is cyclic and acts irreducibly on B), then C is fixed point free on W.*

Suppose W' is the set of fixed points of C in W. Then as C is irreducible on B and acts faithfully there (by (c)), $|C| = c$ is a divisor of $q^n - 1$. Let K be a splitting field for C over $GF(q)$ and form the algebra

$$A \otimes K = (W \otimes K) \oplus (B \otimes K).$$

Then C acts on $B \otimes K$ as a sum of n dictinct (if C is $GF(q)$-irreducible, algebraically conjugate) absolutely irreducible representations. Since any $w' \otimes 1 \epsilon W' \otimes 1 < A \otimes K$ generates a C-submodule of $W \otimes K$ affording the trivial representation, left multiplication of $B \otimes K$ by this element is representable as a diagonal matrix similar (in GLn, K)) to $L_{w'}$ (as a linear transformation of B). Since the latter is nilpotent and the former is diagonal, similarity forces both to be the 0-transformation (or matrix). Thus $w'B = 0$ so $w' = 0$ by (a). Thus $W' = 0$, proving (h).

(i) *Suppose C is a cyclic subgroup of G having order c and acting irreducibly on B. Then there exist at least two distinct residues b_1, b_2* mod n *and residues a_1, a_2* mod n *such that the congruence*

$$(9) \qquad 1 + q^{b_1+a_2-a_1} = q^{a_2-a_1} + q^{b_2} \mod c$$

holds with $a_2 \not\equiv a_1$ (mod n). (*Here q has exponent n* mod c.)

Let W_1 be any C-irreducible subspace of W and let $K = GF(q^n)$. Define the integer k by letting $\theta, \theta^q, \cdots, \theta^{q^{n-1}}$ be the eigenvalues on $B \otimes K$ and $\theta^k, \theta^{kq}, \cdots, \theta^{kq^{d-1}}$ be the eigenvalues on $W_1 \otimes K$ of the transformations induced by a generator, y, of C. (Here θ is a primitive c-th root in K since C acts faithfully on B, although not necessarily faithfully on W_1.)

Let $B \otimes K = \langle z_0, \cdots, z_{n-1}\rangle$ where z_j is an eigenvector of y for the root θ^{q^j}. If no residue a_1(mod n) exists such that

$$(10) \qquad \theta^{kq^{a_1}} \cdot \theta = \theta^{q^{b_1}}$$

for some b_1, then $(W_1 \otimes K)\langle z_0\rangle = 0$ as a set of products in $A \otimes K$. Let ψ be a generator of the canonical group of semiautomorphisms of $A \otimes K$ defined in the remarks preceding Theorem 2, whose fixed points comprise $A \otimes 1$. We can then choose the z_i in such manner that they are transitively permuted by ψ. Since $W_1 \otimes K$ is ψ-invariant, iteration of ψ forces $(W_1 \otimes K)\langle z_i\rangle = 0$ for $i = 0, \cdots, n-1$. It follows that $W_1 B = 0$ (in A) against (a) and our choice of W_1.

Suppose only one pair of eigenvalues θ^{kq^a} and θ^{q^b} exists such that $\theta^{kq^a} \cdot \theta = \theta^{q^b}$. Then only one product between z_0 and an eigenvector w_a in $W_1 \otimes K$ can be non-zero. Under these circumstances, Lemma 7 shows that in A, for any $w \in W_1$, L_w is a linear transformation of B which is similar (as a $GF(q)$-linear mapping) to a semilinear transformation of $GF(q^n)$. In particular, L_w is non-singular for all non-zero w in W_1. This contradicts hypothesis (iv).

Thus at least two *distinct* pairs of eigenvalues $(\theta^{kq^{a_i}}, \theta^{q^{b_i}})$ $i = 1, 2$ can be found satisfying (10). The two congruences

$$1 + kq^{a_1} \equiv q^{b_1} \bmod c, \qquad 1 + kq^{a_2} \equiv q^{b_2} \bmod c$$

follow upon equating exponents (mod c). Multiplying the congruences through by q^{n-a_i}, $i = 1, 2$, respectively, and equating the expressions for k which result yields (9). (Note: If $b_1 \equiv b_2$, then $kq^{a_1} \equiv kq^{a_2}$ mod c and the two pairs of eigenvalues would agree. Also $b_1 \not\equiv b_2$ implies $a_1 \not\equiv a_2$ mod n.)

A number of troublesome special cases are eliminated in the following two steps.

(j) *Suppose C is a self-centralizing subgroup of G which is not at π_0'-group. Then $[N_G(C):C] < n$.*

Let S be an S_r-subgroup of C where $r \in \pi_0 \cap \pi(C)$. Then S acts irreducibly on B, and $C_G(S) \geq C_{N_G(C)}(S) \geq C$, where, by Lemma 10, all three members of this chain are cyclic. Since C is self centralizing, $C = C_{N_G(C)}(S)$. Also $N_G(S) \geq N_G(C)$. Now $N_G(C)$ induces a cyclic group of automorphisms of S, and we can find an element of y such that $\langle y, C \rangle = N_G(C)$. Suppose $[N_G(C):C] = n$. Then B is an absolutely irreducible module for $N_G(C)$ and y^n lies in its center. It follows that y^n acts as multiplication by a scalar $\omega \in GF(q)$. Since $C_{N_G(C)}(S) = C$, and $(n, r) = 1$, $\langle y, S \rangle / \langle y^n \rangle$ is a Frobenius group. For every $w \in W$ and $b \in B$, $(wb)^{y^n} = w^{y^n} b^{y^n} = \omega(w^{y^n} b) = \omega(wb)$ since $wb \in B$. Thus $(w^{y^n} - w)B = 0$ and so $w^{y^n} = w$. Since $\Omega_1(S)$ acts irreducibly on B, S acts faithfully on W, by (h). It follows that $\langle y, S \rangle$ is represented as a Frobenius group on W and so y fixes a non-trivial element w_0 of W. But y has p'-order (by (d)) and B restricted to $\langle y \rangle$ affords the representation induced from the irreducible representation of its subgroup $\langle y^n \rangle$ defined by $y^n \rightharpoonup \omega$. It follows that $\langle y \rangle$ is represented on B with absolutely irreducible constituents which are distinct. It follows from (h) that y acts without fixed points on W, a contradiction.

(k) *n is not a prime number.*

Suppose $n = s$ is a prime number. By Lemma 10, part (b), for each $r \in \pi_0$ and S_r-subgroup S of G, $[N_G(S):C_G(S)]$ divides n and so is 1 or n. Since $C_G(S)$ is self-centralizing, (j) implies $N_G(S) = C_G(S)$. By Burnside's transfer theorem, S has a normal complement in G. Applying this result for each prime in π_0, a chain of Frattini arguments shows that G has a cyclic π_0-Hall subgroup H and a normal π_0-complement N. If T is a t-subgroup of N chosen minimally with respect to being normalized by a S_r-subgroup S in H but not centralized by $\Omega_1(S)$, then T is a special t-group, and every absolutely irreducible representation of ST over a field of characteristic relatively prime to ST either (a) has T in its kernel, (b) has degree greater than $r - 1$ or (c) has degree $r - 1$. Case (c) holds only when $r - 1 = [T:D(T)]^{1/2}$. Since T acts faithfully on B, $(q, |ST|) = 1$, and $\dim B = n$, absolutely irreducible ST-constituents of B have degree $\leq n$ which divides $r - 1$. But now n and $r = n + 1$ are both primes. This forces $n = 2$, against (f). Thus $\Omega_1(S)$ centralizes every t-subgroup of N which S normalizes. A Frattini argument coupled with the use of the Schür-Zassenhaus theorem shows that S normalizes at least one S_t-subgroup of N for each t dividing $|N|$. Thus N and H both lie in $C_G(\Omega_1(S))$, which by Lemma 10, part (a), is cyclic.

Since G is now a B-irreducible cyclic subgroup of G, by (i) there exist integers c_1, c_2, c_3 (where c_1 is distinct from c_2 and c_3) such that for each integer k such that $0 \leq k \leq n - 1$,

$$q^k + q^{c_1+k} \equiv q^{c_2+k} + q^{c_3+k} \mod |G|. \tag{11}$$

Also $|G| \geq 1 + q + \cdots + q^{n-1}$. When all exponents are reduced mod n, both sides of (11) represent distinct integers, one of which necessarily exceeds $|G|$. Since $n > 2$, it follows that this integer is exactly $2q^{n-1}$. With

$k = 0$, this forces $c_2 = c_3 = n - 1$. Similarly, with $k = 1$, we have $q + q^{c_1+k} \equiv 2$ forcing $2q^{n-1} = q + q^{c_1+k}$ so $n = 2$, against (f).

(l) *If case* (i) *of step* (e) *holds, then G contains a normal cyclic subgroup C of order a multiple of $(d/n)(1 + q + \cdots + q^{n-1})$ where d is a divisor of n and $d \geq 2$. Moreover $n \leq 14$ in this case.*

Case (i) of step (e) implies the normality of an S_r-subgroup S for some $r \in \pi_0$. Set $C = C_G(S)$. Then C is cyclic, is its own centralizer, and $G/C = N_G(S)/C_G(S)$ is a proper divisor n/d of n by Lemma 10(b), and step (j). Since G acts transitively on the $1 + q + \cdots + q^{n-1}$ one-dimensional subspaces of B, $(d/n)(1 + q + \cdots + q^{n-1})$ divides $|C|$.

Now suppose $n > 14$. By Lemma 14, for all $q > 2$,

$$q^{(3/4)n} \leq \frac{1}{n}\left(\frac{q^n - 1}{q - 1}\right). \tag{12}$$

By step (i), there exist integers b_1, a_2 and b_2 such that

$$q^k + q^{k+b_1+a_2-a_1} \equiv q^{k+a_2-a_1} + q^{k+b_2} \mod |C|, \tag{13}$$

for $k = 0, 1, \cdots, n - 1$. For each integer a let $\bar{a}$ (also denoted a^-) be defined by $a \equiv \bar{a} \bmod n$ and $0 \leq \bar{a} < n$. If we rewrite equation (13) with exponents replaced by the "barred" value of these integers, then both sides of (13) represent *distinct integers* (since $(0, (b_1 + a_2 - a_1)^-)$ and $((a_2 - a_1)^-, (b_2))$ represent distinct pairs of residues mod n) which are congruent mod $|C|$. It follows that one of the integers exceeds $|C|$, and hence by (12), exceeds $2q^{3/4n}$. Thus for every value of k, one of the four exponents

$$(\bar{k}, (k + b_1 - a_1)^-, (k + a_2 - a_2 - a_1)^-, (k + b_2)^-)$$

represents value between $(\frac{3}{4})n$ and $n - 1$ (inclusively). Put another way, when the four values, 0, $(b_1 + a_2 - a_1)^-$, $(a_2 - a_1)^-$ and $\bar{b}_2$ are placed on the circle of residues mod n, no gap can occur between adjacent members of the quartette which exceeds one-fourth of the circle. Thus n is divisible by 4 and for some k, the four exponents are congruent to 0, $(\frac{1}{4})n$, $(\frac{1}{2})n$, $(\frac{3}{4})n$ (mod n) some order. In that case,

$$q^{(3/4)n} + q^{(1/2)n} > |C| \geq 2q^{(3/4)n},$$

an impossibility.

(m) *Case* (i) *of step* (e) *does not hold.*

Suppose case (i) of step (e) holds. By steps (f), (k) and (l) we may assume $4 \leq n \leq 14$ and that n is not a prime number. Thus we have $n = 4, 6, 8, 9, 10, 12$ or 14. By (i) we have a congruence

$$\begin{gathered} 1 + q^a \equiv q^b + q^c \mod |C|, \\ (\max\ (a, b, c) < n,\ a \notin \{b, c\} \text{ and } \min\ (b, c(> 0) \end{gathered} \tag{14}$$

where $|C| \geq (2/n)(1 + q + \cdots + q^{n-1})$. By multiplying congruence (14) through by q^{n-a} if necessary, we may assume without loss of generality that $a < \frac{1}{2}n$.

Suppose $n = 4$. Since $q \geq 3$, $2q^2 \leq \frac{1}{2}(1 + q + q^2 + q^3)$. Since one side of the congruence (14) must represent an integer exceeding the modulus $|C|$, one of the exponents is at least 3. Since $a < \frac{1}{2}n$, without loss of generality we may assume $c = 3$. Multiplying (14) through by q, (14) becomes

$$q + q^{a+1} \equiv 1 + q^{b+1}.$$

Then either $(a + 1)^-$ or $(b + 1)^-$ is 3. Thus either

(i) $q + q^2 \equiv 1 + q^3$,
(ii) $2q \equiv 1 + q^3$
(iii) $q + q^3 \equiv 1 + q^2$, or
(iv) $q + q^3 \equiv 2$,

mod $|C|$. Case (iv) yields $1 + q^2 \equiv 2q$ and case (ii) yields $2q^2 \equiv 1 + q$ and in both congruences neither side can represent an integer exceeding $\frac{1}{2}(1 + q + q^2 + q^3)$. In (i), $q^2 + q^3 \equiv 1 + q$ so

$$(q^2 - 1)(1 + q) \equiv 0 \mod |C|$$

and this holds mod r for some prime $r \in \pi_0$. This contradicts the fact that q has exponent 4 modulo such an r. In case (iii),

$$(q^2 + 1)(q - 1) \equiv 0 \mod |C|$$

and so $(q^2 + 1)(q - 1)$ is a multiple $\frac{1}{2}(1 + q + q^2 + q^3)$. Since $(q^2 + 1)(q - 1)$ is positive and less than $1 + q + q^2 + q^3$, $k = 1$. Then $2q^3 + 2q^2 - 2q - 2 = 1 + q + q^2 + q^3$ so $q^3 + q^2 = 3(1 + q)$ so $q^2 = 3$, an impossibility.

Suppose $n = 6$. Then $|C| \geq (1 + q + \cdots + q^5)/3$, and since $q \geq 3$ implies $3q^3 + 3q^4 \leq 1 + q + \cdots + q^5$, and in the congruence (14), $a \leq \frac{1}{2}n = 3$, we may assume $c = \max(b, c) \geq 4$, with equality holding only if also $b = 4$. Multiplying the congruence through by q^2 and reducing exponents mod n, the right side is at most $q + q$, an integer less than $|C|$. The left side is $q^2 + q^{2+a}$ and so $a = 3$. Multiplying again by q, we have $q^3 + 1 \equiv q^{(b+3)^-} + q^{(c+3)^-}$ and since $(b + 3)^- \leq (c + 3)^- \leq 2$, neither side represents an integer exceeding the modulus. Since $a \notin \{b, c\}$, it cannot also represent an equation between integers; hence the congruence (14) cannot hold.

Suppose $n = 8$. Here

$$|C| \geq (\tfrac{1}{4})(1 + q + \cdots + q^7).$$

Since $8q^5 < (1 + 3 + 3^2)q^5 \leq q^5 + q^6 + q^7$ we have $q^5 + q^5 < |C|$. Thus if the sum of two powers of q exceed $|C|$, at least one exponent is 6 or 7. In congruence (14), we have $a < (\frac{1}{2})n = 4$ and $b \leq c$, so we may assume $c \geq 6$. In addition $1 + q \geq 4$ yields $4(q^4 + q^6) \leq q^4 + q^5 + q^6 + q^7$ and so $q^4 + q^6 < |C|$. Thus $q^6 + q^f$ exceeds $|C|$ only if $f = 5$ or 6. Now if $c = 7$, $q + q^{a+1} \equiv 1 + q^{b+1}$ and since $a + 1 \leq 5$, $b + 1 = 7$. Then $q^2 + q^{a+2} \equiv$

$1 + q \bmod |C|$, and this is a contradiction. Thus $c = 6$, and $q^2 + q^{a+2} \equiv 1 + a^{(b+2)^-}$. Then $a + 2 \leq 6$ forces $(b + 2)^- = 7$. Then $q^3 + q^{a+3} \equiv 1 + q$ so $a + 3 = 7$. This finally yields $q^4 + 1 \equiv q + q^2 \bmod |C|$, an impossibility.

Suppose $n = 9$. Then $|C| \geq (\frac{1}{3})(1 + q + \cdots + q^8)$. Then $q^6 + q^7 < |C|$ and $c \geq 7$. If $c = 8$, $q + q^{a+1} \equiv 1 + q^{b+1}$ forcing $b + 1 = 8$. This yields $q^2 + q^{a+2} \equiv 1 + q \bmod |C|$, which is impossible. Hence $c = 7$, $b = 7$, whence $q^3 + q^{a+3} \equiv 2 \bmod |C|$, another impossibility.

If $n = 10$,

$$|C| \geq (\tfrac{1}{5})(1 + q + \cdots + q^9) \quad \text{and} \quad 10q^7 \leq (1 + q + q^2)q^7$$

so in congruence (14), $c \geq 8$. If $c = 9$, $q + q^{a+1} \equiv q^{b+1} + 1$ so (since $a + 1 \leq 5$), $b + 1 > 8$ forcing $q^2 + q^{a+2} \equiv 1 + q$ or $q^3 + q^{a+3} \equiv 1 + q^2$. This means $a + 3 \geq 8$, an impossibility. If $c = 8$, $q^2 + q^{a+2} \equiv q^{b+2} + 1$ so $b + 2 \geq 8$. Then $q^4 + q^{a+4} \equiv q^{(b+4)^-} + q^2$ where $(b + 4)^- = 0$ or 1. This forces $a + 4 = 8$ (since $a \leq 4$). Then $q^6 + 1 \equiv q^{(b+6)^-} + q^4 \bmod |C|$, which is impossible since $(b + 6)^- \leq 7$.

If $n = 12$, $|C| \geq (\frac{1}{6})(1 + q + \cdots + q^{11})$. Since $q \geq 3$, $1 + q + q^2 \geq 12$ so $12q^9 \leq q^9 + q^{10} + q^{11}$. Thus $q^e + q^f > (\frac{1}{6})(1 + \cdots + q^{11})$ implies $\max(\bar{e}, \bar{f}) \geq 10$. Thus in (14), $c \geq 10$, so

$$q^2 + q^{a+2} \equiv q^{b+2} + q^{(c+2)^-} \mod |C|$$

where $(c + 2)^- = 0$ or 1. Then $a + 2 \leq 7$ forces $b + 2 = 10$ or 11 so $q^4 + q^{a+4} \equiv q^{(b+4)^-} + q^{(c+2)^-}$ where $0 \leq (b + 4)^- < (c + 4)^- \leq 5$. Thus $a + 4 \geq 10$ against $a \leq 5$.

Suppose $n = 14$. Now

$$7q^{10} + 7q^{11} \leq q^2(q^{10} + q^{11}) < 1 + q + \cdots + q^{13}.$$

Thus if $0 \leq e \leq f \leq 13$ and $q^e + q^f > (\frac{1}{7})(1 + q + \cdots + q^{13})$, then $f \geq 11$ and if $f = 11$, then $e = 11$ also. Thus in (14) $c \geq 11$. If $c = 12$ or 13, $q^2 + q^{a+2} \equiv q^{b+2} + q^{(c+2)^-}$ forcing $b + 2 \geq 12$. Then $q^4 + q^{a+4} \equiv q^{(b+4)^-} + q^{(c+4)^-}$ where $0 \leq (\mathrm{b} + 4)^- < (c + 4)^- \leq 5$. This forces $a + 4 > 11$ against $a \leq 6$. Otherwise, $b = c = 11$, so $q^3 + q^{a+3} \equiv 2$ forcing $a + 3 \geq 12$, another contradiction. This completes step (m).

(n) *Case* (ii) *of step* (*f*) *does not hold.*

Suppose case (ii) holds. Then $2n + 1$ is prime and $G/Z(G) \simeq LF(2, 2n + 1)$. Moreover, B is an absolutely irreducible G-module. Thus $Z(G)$ acts on B as scalar multiplication by elements of $GF(q)$. As a result, $Z(G)$ stabilizes every one-dimensional subspace of B and so the number of one-dimensional subspaces of B divides the order of the central factor group of G, i.e.

$$(15) \qquad 1 + q + \cdots + q^{n-1} \quad \text{divides} \quad 2n(n + 1)(2n + 1).$$

By Lemma 15, if $n \geq 12$, $q^{n-1} \geq 3^{n-1} > (2n + 1)^3$ and (15) is impossible.

From the above, and steps (f) and (k) we have $4 \leq n < 12$, $2n + 1$ a prime and n composite. This leaves $n = 6$, 8 or 9.

If $n = 6$, $[G:Z(G)] = 12 \cdot 7 \cdot 13$ is a multiple of

$$(q + 1)(q^2 + q + 1)(q^2 - q + 1).$$

Clearly $q^5 < 12 \cdot 7 \cdot 13$ so $q^4 < 4 \cdot 7 \cdot 13$ so $q < 5$. Thus $q = 3, 4$. If $q = 4$, $q + 1 = 5$, which doesn't divide $12 \cdot 7 \cdot 13$ as it should. And $q = 3$ is impossible because 3 does not have exponent 6 mod 13.

If $n = 8$, $[G:Z(G)] = 16 \cdot 9 \cdot 17 < 11^5$ so $q < 11$. Also q has exponent 8 mod 17 so 17 divides $q^4 + 1$. Thus $q = 2$, 8 or 9 or 15. $q = 2$ or 15 are ruled out. If $q = 8$, $q^2 + 1 = 5 \cdot 13$ must divide $16 \cdot 9 \cdot 17$ while if $q = 9$, $q + 1 = 2 \cdot 5$ divides $16 \cdot 9 \cdot 17$, both absurdities.

If $n = 9$, $[G:Z(G)] = 2^2 \cdot 3^2 \cdot 5 \cdot 19$. If $q^2 \geq 19$, then

$$1 + q + \cdots + q^8 > q^6 \geq 19^3 = (2n + 1)^3 > 2n(n + 1)(2n + 1)$$

and (15) cannot hold. Thus $q = 3$ or 4. If $q = 4$, $1 + q + q^2 = 3 \cdot 7$ must divide $[G:Z(G)] \not\equiv 0 \bmod 7$. But $q \neq 3$, since 3 does not have exponent 9 mod 19 ($\phi_9\ (3) \not\equiv O(19)$). This concludes step ($n$).

(o) *Case* (iii) *of* (e) *cannot hold.*

Here π_0 consists of $n + 1$ alone. Moreover, $(n + 1)^2 \nmid |G|$, since otherwise G has a normal π_0-Hall subgroup and case (i) of (e) obtains, against (m). Thus $\phi_n(q) = r^e(n + 1)$ where r is the largest prime dividing n. From Lemma 13, $n = 2$, 4 or 6. But $n \neq 2$, by (f). If $n = 4$, $\phi_4(q) = 5$ and $q = 2$, an excluded case, or else $\phi_4(q) = 10$ and $q = 3$. If $n = 6$, $\phi_n(q) = 7$ or 21 which occurs with $q = 3$ or 5. We examine these cases separately.

First suppose $\phi_4(q) = 10$, $q = 3$. Here, B contains 40 one-dimensional subspaces, so $40 \mid |G|$. Suppose $13 \mid |G|$. Let R be a 13-Sylow subgroup of G. Then R acts on B with an irreducible 3-dimensional subspace $[B, R] = \langle b - b^x \mid x \in R \rangle$ and $C_B(R) = GF(3)$ as an additive group. Since $G \leq GL(4, 3)$, which has order $2^9 3^6 5 \cdot 13$, and since G is a $3'$-group by step (d), it follows that $N_G(R)$ is a $\{2, 13\}$-group. Since R is irreducible on the 3-dimensional space $[B, R]$ stabilized by $N_G(R)$, it follows that $N_G(R)/C_G(R)$ is a subgroup of Z_3. Since $3 \nmid |G|$, $N_G(R) = C_G(R)$, and so R has a normal complement in G. Since $5 \mid |G|$, a Frattini argument shows that G must contain a cyclic subgroup of order 65. This is impossible since such a group does not lie in $GL(4, 3)$. Thus 13 does not divide $|G|$. It follows that G divides $2^9 5$ and so, by a famous theorem of Burnside, G is solvable.

By Lemma 10 (d), a 5-Sylow subgroup S of G centralizes $O_2(G)$. Thus $O_{2,2'}(G) = S + O_2(G)$ and so S is normal in G. By Lemma 10 (a), $C = C_G(S)$ is cyclic, and acts semiregularly on the one-dimensional subspaces of B. Since G/C is a subgroup of Z_4 and $40 \mid |G|$, we see that C has even order. An involution in C is necessarily acting as scalar multiplication by -1, Let G_1 be the subgroup of G which stabilizes a one dimensional subspace of B.

Then any element x in $G_1 \cap C$ stabilizes all of the 5 or more lines lying in some C-orbit of the one-dimensional subspaces, and acts on these lines as scalar-multiplication by a common scalar $\alpha(x)$. It follows that $G_1 \cap C = Z_2$. Since G/C is abelian, G_1 has a normal supplement N such that $N \cap G_1 = C \cap G_1$. Then, since N is itself transitive on the one-dimensional subspaces of B, we may assume $N = G$ and that $G_1 = G_1 \cap C$ is generated by the transformation of scalar multiplication by -1. Thus $|G| = 80$ and regularly permutes the 80 non-zero elements of B. Thus a 2-Sylow subgroup T of G has a unique involution. Moreover 20 divides $|C|$.

Now suppose $|C| = 20$. Then T possesses a factor group which is cyclic of order 4 and so cannot be generalized quaternion. Thus T is cyclic and

$$G = \text{grp}\,\langle a, x \mid a^5 = 1 = x^{16}, x^{-1}ax = a^2\rangle.$$

At this point, no help can be gained from the congruence of step (i) since solutions exist modulo 20 as well as modulo 16, the orders of the maximal cyclic subgroups of G. Instead, we argue that G is not a subgroup of $GL(4, 3)$, i. e. that G cannot act on B (recall from step (c) that G acts faithfully on B). Let K be the field $GF(3^4) = GF(3)(\theta, \mu)$ where θ and μ are primitive 5-th and 4-th roots of unity. Then $B \otimes K$ is a KG-module. Suppose U is an irreducible KG-submodule of $B \otimes K$. Then U is a sum of homogeneous KG-components $U = U_0 + U_1 + U_2 + U_3$ in which a generator x^4a of $\langle x^4a\rangle = C$ acts on U_i as scalar multiplication by $\mu\theta^{3^i}$. The U_i are transitively permuted by x and so x^4 acts on U as scalar multiplication by μ. Since $\dim_K(B \otimes K) = \dim B = 4$, $U = B \otimes K$. But this is impossible since $[x^4] \simeq Z_4$ and acts on B as two irreducible $GF(3)\langle x^4\rangle$-modules B_1 and B_2 of dimension 2. Thus $B \otimes K$ contains at least two distinct algebraically conjugate $K\langle x^4\rangle$-modules associated with the two primitive 4-th roots μ and $\mu^3 = \mu^{-1}$. This contradicts the action of x^4 forced above by the defining relations of G. Thus G cannot act on B and so we may dispense with this case.

Thus $|C| = 40$ or 80. In either case, we must obtain a solution (a, b_1, b_2) of the congruence

$$1 + 3^a \equiv 3^{b_1} + 3^{b_2} \mod 40$$

with $a \leq 2$, $0 \neq b_1 \leq b_2 \leq 3$. Since $1 + 3^a < 40$, $3^{b_1} + 3^{b_2}$ must exceed 40. Since the b_i are less than 4, this can only occur if $b_1 = b_2 = 3$. In that case $1 + 3^a = 54 - 40 = 14$, which has no solution for a. Thus $|C| = 40$ or 80 is impossible, and the case $n = 4$, $q = 3$ cannot occur.

Suppose $n = 6$ and $q = 3$. Then $13 \mid |G|$. Then by a theorem of Brauer [3], either G contains a normal 13-Sylow subgroup or else G is a central extension of $LF(2, 13)$. In the latter case $q = 3 \mid |G|$ against (d). Thus G contains a normal subgroup of order 13 or 13^2. By Lemma 10, part (d), this group is centralized by the 7-Sylow subgroup of G, and so G contains a cyclic subgroup of order 91 which acts irreducibly on B. Thus by step (i) we obtain a congruence of the form

$$1 + 3^{a_1} \equiv 3^{b_1} + 3^{b_2} \quad \text{mod } 91$$

where $a_1 = 0$, 1 or 2, $b_2 \leq b_1 \leq 5$, and $\{0, a_1\} \cap \{b_1, b_2\}$ is empty. Then $3^{b_1} + 3^{b_2}$ exceeds 91. If b_1 is 5, then $3 + 3^{a_1+1} \equiv 1 + 3^{b_2+1}$, so $a_1 + 1 \leq 3$ implies $b_2 + 1 = 5$. Then $9 + 3^{a_1+2} \equiv 4$ mod 91, which is impossible since the left side is 18, 36 or 90. Thus $b_1 \leq 4$ and $9 + 3^{a_1+2} \equiv 1 + 3^{b_2+2}$. Since the left side of this congruence is at most 90, the right side must exceed 91 whence $b_2 + 2 = 5$. The original equation is then $1 + 3^{a_1} \equiv 3^3 + 3^4 \equiv 17$ mod 91, which is impossible since $a_1 = 0$, 1 or 2.

Now suppose $n = 6$ and $q = 5$. Then by a theorem of Feit and Thompson [8], G contains a normal 31-Sylow subgroup, normalized by a 7-Sylow subgroup of G. By Lemma 10 (d), G contains a cyclic subgroup of order 217, which acts irreducibly on B. Again, we have a congruence

$$1 + 5^{a_1} \equiv 5^{b_1} + 5^{b_2} \quad \text{mod } 217$$

with $a_1 = 0$, 1 or 2, $b_2 \leq b_1 \leq 5$ and $\{b_1, b_2\} \cap \{0, a_1\}$ empty. The right side must exceed 217 and so either $b_1 = b_2 = 3$ or $b_1 \geq 4$. Suppose $b_1 = b_2 = 3$. Then $5^3 + 5^{a_1+3} \equiv 2$. This is impossible since the possible residues for the left side are 33, 99, or 214. Now suppose $b_1 = 4$. Then $5^2 + 5^{a_1+2} \equiv 1 + 5^{b_2+2}$. The left side of this congruence yields residues 50, 150, or 216. This excludes $b_2 = 0$ or 4 so $b_2 = 1, 2$ or 3, yielding 126, 200 or 90 as possible residues. Thus $b_1 = 5$ and $5 + 5^{a_1+1} \equiv 1 + b^{b_2+1}$ and so $4 \leq b_2 + 1 \leq 5$. Then $1 + 5^{b_2+1} \equiv 192$ or 88 mod 217. Since $5 + 5^{a_1+1} = 10, 30$ or 130 the congruence is impossible.

The theorem now follows from the patent incompatibility of (f), (m), (n) and (o).

We conclude with the

Proof of Theorem 1. Let A be a finite automorphic algebra which is not a quasidivision algebra (this includes the assertion that $A \neq \{0\}$) and assume the ground field contains $q > 2$ elements. By Lemma 3, A is a nil algebra. Let $G = \text{Aut}(A)$. Construct a G-module $A_1 \oplus A_2$ where $\mu_i : A \rightarrow A_i$ is an isomorphism as G-modules. Convert $A_1 \oplus A_2$ into an algebra by setting $A_1^2 = 0 = A_2^2 = A_2 A_1$ and defining products $A_1 A_2$ by setting

$$\mu_1(a)\mu_2(b) = \mu_2(ab) \in A_2 \quad \text{for all } a, b \in A.$$

Then G acts as a group of automorphisms of $A_1 \oplus A_2$, A_2 is a left ideal, and as A is a nil algebra, left multiplications induced nilpotent transformations of A_2. Thus $A_1 \oplus A_2$, A_2 and G satisfy the roles of A, B and G in Theorem 4. This forces $A_1 A_2 = 0$ and so $\mu_2(ab) = 0$ for all $a, b \in A$, As μ_2 is monic, $A_2 = 0$.

REFERENCES

1. J. Boen, *On p-automorphic p-groups*, Pacific J. Math., vol. 12 (1962), pp. 813–816.

2. J. Boen, O. Rothaus and J. Thompson, *Further results on p-automorphic p-groups*, Pacific J. Math., vol. 12 (1962), pp. 817–821.

3. R. Brauer, *On groups whose order contains a prime to the first power*, II, Amer. J. Math., vol. 64 (1942), pp. 421–440.
4. C. Chevalley, *Demonstration d'une hypothese de M. Artin*, Abh. Math. Sem. Univ. Hamburg, vol. 11 (1936), pp. 73–75.
5. L. E. Dickson, *On the cyclotomic function*, Amer. Math. Monthly, vol. 12 (1905), pp. 85–89.
6. L. Dornhoff, *p-automorphic p-groups and homogeneous algebras*, preprint, Yale University.
7. W. Feit. *Characters of finite groups*, Yale University Notes, 1965.
8. W. Feit and J. Thompson, *Groups which have a faithful character of degree less than* $(p - 1)/2$, Pacific J. Math., vol. 11 (1961), pp. 1257–1262.
9. W. Gaschutz and T. Yen, *Groups with an automorphism group which is transitive on the elements of prime orde1*, Math. Zeitschrift, vol. 86 (1964), pp. 123–127.
10. P. Hall and G. Higman, *On the p-length of p-solvable groups and reduction theorems for the Burnside problem*, Proc. London Math. Soc. (3), vol. 6 (1956), pp. 1–42.
11. G. Higman, *Suzuki* 2-*groups*, Illinois J. Math., vol. 7 (1963), pp. 73–96.
12. B. Huppert, *Zweifach transitive auflösbare Permutationsgruppen*, Math. Zeitschrift, vol. 68, pp. 126–150.
13. A. I. Kostrikin, *On homogeneous algebras*. Izvestia Acad. Nauk SSSR, vol. 29 (1965), pp. 471–483.
14. T. Nagell, *Introduction to number theory*, 2nd ed., Chelsea, New York, 1964.
15. D. Passman, personal communication, fall, 1967.
16. E. Shult, *On semi-p-automorphic groups, I*, multilithed notes.
17. ——— . *On semi-p-automorphic groups, II*, multilithed notes.

Southern Illinois University
Carbondale, Illinois