PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 31, No. 1, January 1972

FINITE AUTOMORPHIC ALGEBRAS OVER GF(2)

FLETCHER GROSS[1]

ABSTRACT. If A is a finite nonassociative algebra over GF(2) and G is a group of automorphisms of A such that G transitively permutes the nonzero elements of A, then it is shown that either $A^2 = 0$ or the nonzero elements of A form a quasi-group under multiplication. Under the additional hypothesis that G is solvable, the algebra A is completely determined.

All algebras considered in this paper are nonassociative. Shult **[5]** proved that if A is a finite automorphic algebra over GF(q) and $q > 2$, then either $A^2 = 0$ or A is a quasi division algebra. Here an automorphic algebra is one in which the automorphisms of the algebra transitively permute the one-dimensional subspaces. A quasi division algebra is an algebra in which the nonzero elements form a quasi-group under multiplication. One of the purposes of the present paper is to show that the restriction $q > 2$ in Shult's Theorem is unnecessary. Actually a great deal of Shult's argument still applies when $q = 2$. Where Shult's proof breaks down for $q = 2$, the Feit-Thompson Theorem, a theorem on solvable transitive linear groups, and a number theoretic result of Shaw **[4]** combine to finish the proof.

If A is a finite automorphic algebra over GF(q), $q > 2$, and $A^2 \neq 0$, then Shult **[6]** showed that $A = \mathrm{GF}(q)$. For $q = 2$, we prove the weaker result that if A is a finite algebra over GF(2), $A^2 \neq 0$, and G is a *solvable* group of automorphisms of A such that G transitively permutes the nonzero elements of A, then A is isomorphic to the algebra $A(n, \mu)$ for some positive integer n and some nonzero element μ in GF(2^n). Kostrikin **[2]** obtained the same conclusion under the assumption that G is cyclic.

The algebra $A(n, \mu)$ referred to above is defined as follows: Let $K = \mathrm{GF}(2^n)$ and let μ be a fixed nonzero element of K. For x and y in K, define $[x, y]$ by the rule $[x, y] = \mu(xy)^{2^{n-1}}$. Then $A(n, \mu)$ is the algebra over GF(2) obtained from K by replacing multiplication by [,]. $A(n, \mu)$

Received by the editors February 12, 1971.
AMS 1970 *subject classifications*. Primary 17A99; Secondary 20B25.
Key words and phrases. Finite automorphic algebra.
[1] Research supported in part by NSF Grant GP-12028.

is an automorphic algebra since if λ is any nonzero element of K, then the mapping $x \to \lambda x$ for all $x \in K$ is an automorphism of $A(n, \mu)$. (With $\mu = 1$, the algebras $A(n, \mu)$ also occur as examples in [**6**].)

Before proceeding to our main theorems, we require some preliminary results.

LEMMA 1. *If n, r, and a are nonnegative integers such that $2^n \equiv 1 \pmod{r}$, $rn \equiv 0 \pmod{2^n - 1}$, and $2^a \equiv 1 \pmod{r}$, then $a \equiv 0 \pmod{n}$.*

This is proved by Shaw [**4,** Lemma 4].

LEMMA 2. *If n, r, a, b, c, and d are nonnegative integers such that $2^n \equiv 1 \pmod{r}$, $rn \equiv 0 \pmod{2^n - 1}$, and $2^a + 2^b \equiv 2^c + 2^d \pmod{r}$, then $a + b \equiv c + d \pmod{n}$.*

PROOF. This is certainly true if the sets $\{a, b\}$ and $\{c, d\}$ are the same modulo n. If they are not, then it follows from [**4,** Lemma 5] that $n = 6$. In this case, the lemma is established by a straightforward examination of the possible values (mod n) of a, b, c, and d.

LEMMA 3. *Let $K = \mathrm{GF}(2^n)$ and for $0 \neq \lambda \in K$, let T_λ be the mapping of K defined by $xT_\lambda = \lambda x$. Let R be the mapping $xR = x^2$. Let T be the group consisting of all T_λ for $0 \neq \lambda \in K$, let U be the cyclic group generated by R, and let $L = TU$. Next suppose μ is a fixed nonzero element of K and define $[x, y]$ for x and y in K by the rule $[x, y] = \mu(xy)^{2^{n-1}}$. If $S \in L$ and $ST_\mu = T_\mu S$, then $[xS, yS] = [x, y]S$ for all x and y in K.*

PROOF. Let C be the subgroup of L consisting of those elements of L which commute with T_λ. Clearly C contains T and it is easily verified that $[x, y]S = [xS, yS]$ for all $S \in T$. Thus, to prove the lemma it suffices to show that $[x, y]S = [xS, yS]$ if $S \in C \cap U$. If $S \in C \cap U$, then we must have $\mu S = \mu$. But then, since S is an automorphism of K, the desired result follows immediately.

LEMMA 4. *Let K, T_λ, and T have the same meaning as in Lemma 3. Suppose that H is a subgroup of T such that $|T/H|$ divides n. If R is any nonzero homomorphism of the additive group of K into itself such that R commutes with all elements of H, then $R \in T$.*

PROOF. Since $R \neq 0$, there is an element x in K such that $xR \neq 0$. Let $\lambda = x^{-1}(xR)$. Then $(R - T_\lambda)$ commutes with all elements of H and has nonzero kernel. By Lemma 1, H acts irreducibly on the additive group of K. Schur's Lemma now implies that $R - T_\lambda = 0$. Therefore $R \in T$.

THEOREM 1. *Let A be a finite algebra over* GF(2) *and assume that B is a left ideal in A such that $B^2 = 0$. Assume that for each $x \in A$, the linear* *transformation L_x of B defined by $L_x y = xy$ for $y \in B$ is a nilpotent transformation. Suppose further that G is a group of automorphisms of A such that B is G-invariant and G acts transitively on the nonzero elements of B. Then $AB = 0$.*

PROOF. This corresponds to Theorem 4 of [**5**]. As in the proof of that theorem we may assume that there is a minimal counterexample A satisfying (in addition to the hypothesis of the theorem) the following:

(i) As a G-module, A is the direct sum of the G-invariant subspaces W and B.

(ii) $W^2 = B^2 = BW = 0 \neq WB$.

Proceeding exactly as in [**4,** steps (a) through (d)] we find that

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

(b) W is an irreducible G-module.

(c) B is a faithful G-module.

(d) G has odd order.

It follows from (d) and the Feit-Thompson Theorem [**1**] that G is solvable. If $|B| = 2^n$, then Theorem 19.9 of [**3**] now implies that G has a normal cyclic subgroup C of order r where $2^n \equiv 1 \pmod r$ and $rn \equiv 0 \pmod{2^n - 1}$. By Lemma 1, C acts irreducibly on B. As in step (h) of Shult's proof, we conclude that C acts in a fixed-point-free manner on W. Next, Shult's proof of step (i) is applicable and so there are nonnegative integers a_1, a_2, b_1, b_2 such that $a_1 \not\equiv a_2 \pmod n$, $b_1 \not\equiv b_2 \pmod n$, but $2^{a_1} + 2^{b_1+a_2} \equiv 2^{a_2} + 2^{b_2+a_1} \pmod r$. Lemma 2 now yields $a_1 + b_1 + a_2 \equiv a_2 + b_2 + a_1 \pmod n$ which contradicts $b_1 \not\equiv b_2 \pmod n$. Thus Theorem 1 is proved.

THEOREM 2. *If A is a finite automorphic algebra over* GF(2), *then either $A^2 = 0$ or A is a quasi division algebra.*

PROOF. This is derived from Theorem 1 by exactly the same process Shult uses to derive his Theorem 1 from his Theorem 4.

For the rest of this paper, with the exception of Theorem 4, we make the following assumptions: A is a finite algebra over GF(2), $A^2 \neq 0$, and G is a (not necessarily solvable) group of automorphisms of A which acts transitively on the nonzero elements of A. If x and y belong to A, the product of x and y will be denoted by $[x, y]$. S will denote the mapping $x \to [x, x]$ for $x \in A$. C will be the set of all homomorphisms of A into itself where A is considered as a G-module. By Schur's Lemma, C is a division ring. Since C is finite, C is a field of characteristic 2. Finally let $|A| = 2^n$.

LEMMA 5. $[x, y] = [y, x]$ *for all x and y in A. If $T \in C$, then* $[x, yT] = [xT, y]$.

PROOF. Suppose $T \in C$ and define $x \circ y$ by the rule $x \circ y = [xT, y] + [yT, x]$. Using this operation instead of multiplication we obtain a new algebra B. If $R \in G$, then $(x \circ y)R = (xR) \circ (yR)$ for all x and y in A. Hence B is an automorphic algebra. But $x \circ x = 0$ for all x since we are working over a field of characteristic 2. It now follows from Theorem 2 that $x \circ y = 0$ for all x and y. Thus $[xT, y] = [yT, x]$. With $T = 1$, we obtain $[x, y] = [y, x]$ and the lemma follows.

COROLLARY. $S \in C$.

PROOF. $(x + y)S = xS + yS + [x, y] + [y, x] = xS + yS$. Clearly. $(xS)T = (xT)S$ for all $T \in G$.

LEMMA 6. *If $T \in C$, then $[x, y]T = [xT, yT]$ for all x and y in A. Thus the nonzero members of C are automorphisms of A as an algebra.*

PROOF. Define $x \circ y$ by the rule $x \circ y = [x, y]T + [xT, yT]$. Using this instead of multiplication, we obtain a new algebra B. B is an automorphic algebra since $(x \circ y)R = (xR) \circ (yR)$ for all $R \in G$. Now $x \circ x = xST + xTS$. But, since C is a field, $ST = TS$. Thus $x \circ x = 0$. Theorem 2 implies that $x \circ y = 0$ for all x and y in A. Therefore, Lemma 6 is proved.

THEOREM 3. *If G is solvable, then A is isomorphic to $A(n, \mu)$ for some nonzero element μ in* $\mathrm{GF}(2^n)$.

PROOF. If G is solvable, then we may identify the additive group of A with $\mathrm{GF}(2^n)$ such that G is a subgroup of L where L has the same meaning as in Lemma 3. Let K, T_λ, and T have the same meaning as in Lemma 3 and let $H = G \cap T$. Since $|L/T| = n$, $|G/H| = |TG/T|$ divides n. $(2^n - 1)$ divides $|G|$ since G transitively permutes the $(2^n - 1)$ nonzero elements of K. Hence $|T/H| = (2^n - 1)/|H|$ divides $|G/H|$ which divides n. Lemma 4 now implies that every nonzero element of C belongs to T. Therefore $S = T_\mu$ for some nonzero μ in K. Now for x and y in K, define $x \circ y$ by the rule $x \circ y = [x, y] + \mu(xy)^{2^{n-1}}$. Since $T_\mu = S$ commutes with all elements of G, Lemma 3 implies that $(x \circ y)R = (xR) \circ (yR)$ for all $R \in G$. Therefore, replacing [,] by $\circ$, we obtain a new automorphic algebra B. Since for all x, $x \circ x = xS + \mu(x^2)^{2^{n-1}} = xT_\mu + xT_\mu = 0$, B cannot be a quasi division algebra. Thus, Theorem 2 implies that $x \circ y = 0$ for all x and y in K. An immediate consequence of this is that A is isomorphic to $A(n, \mu)$.

It is natural to ask whether $A(n, \mu)$ and $A(m, \lambda)$ could be isomorphic. This is answered by our final result.

THEOREM 4. *$A(m, \lambda)$ and $A(n, \mu)$ are isomorphic if, and only if, $m = n$ and there is an automorphism S of* $\mathrm{GF}(2^n)$ *such that $\lambda S = \mu$.*

PROOF. Since $A(m, \lambda)$ has order 2^m, $A(m, \lambda)$ and $A(n, \mu)$ cannot be isomorphic if $m \neq n$. Now let $K = \mathrm{GF}(2^n)$ and assume that λ and μ are two nonzero elements of K. Let $[x, y] = \lambda(xy)^{2^{n-1}}$ and $x \circ y = \mu(xy)^{2^{n-1}}$ for all x and y in K. Then $A(n, \lambda)$ and $A(n, \mu)$ are isomorphic if, and only if, there is a mapping S of K onto K such that $(x + y)S = xS + yS$ and $[x, y]S = (xS) \circ (yS)$ for all x and y in K. If S is an automorphism of K such that $\lambda S = \mu$, then S has the above properties and $A(n, \lambda)$ and $A(n, \mu)$ are isomorphic. Conversely, suppose S is a mapping of K onto K satisfying the above. If T_α is the mapping $x \to \alpha x$, then ST_α also satisfies the above properties. Thus, without loss of generality, we may assume that $1S = 1$. From $[1, 1]S = (1S) \circ (1S) = 1 \circ 1$, we obtain $\lambda S = \mu$. From $[x, x]S = (xS) \circ (xS)$, we find that $(\lambda x)S = \mu(xS)$ for all x in K. Next $[x^2, 1]S = (x^2S) \circ (1S)$ implies that $(\lambda x)S = \mu(x^2S)^{2^{n-1}}$. Therefore, $(x^2S)^{2^{n-1}} = xS = ((xS)^2)^{2^{n-1}}$. Since we are working over a field of characteristic 2, this implies that $(x^2)S = (xS)^2$ for all $x \in K$. Finally, it follows from $[x^2, y^2]S = (x^2S) \circ (y^2S) = (xS)^2 \circ (yS)^2$ that $(\lambda xy)S = \mu((xy)S) = \mu(xS)(yS)$. An immediate consequence of this is that S is an automorphism of K which proves the theorem.

REFERENCES

1. W. Feit and J. Thompson, *Solvability of groups of odd order*, Pacific J. Math. **13** (1963), 775–1029. MR **29** #3538.

2. A. I. Kostrikin, *On homogeneous algebras*, Izv. Akad. Nauk SSSR Ser. Mat. **29** (1965), 471–484; English transl., Amer. Math. Soc. Transl. (2) **66** (1968), 130–144. MR **31** #219.

3. D. Passman, *Permutation groups*, Benjamin, New York, 1968. MR **38** #5908.

4. D. Shaw, *The Sylow 2-subgroups of finite, soluble groups with a single class of involutions*, J. Algebra **16** (1970), 14–26.

5. E. E. Shult, *On finite automorphic algebras*, Illinois J. Math. **13** (1969), 625–653. MR **40** #1441.

6. ———, *On the triviality of finite automorphic algebras*, Illinois J. Math. **13** (1969), 654–659. MR **40** #1442.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF UTAH, SALT LAKE CITY, UTAH 84112