ALGEBRAS WITH TRANSITIVE AUTOMORPHISM GROUPS

BY

L. G. SWEET AND J. A. MACDOUGALL*

Abstract. Let \( A \) be a finite dimensional algebra (not necessarily associative) over a field, whose automorphism group acts transitively. It is shown that \( K = GF(2) \) and \( A \) is a Kostrikin algebra. The automorphism group is determined to be a semi-direct product of two cyclic groups. The number of such algebras is also calculated.

All algebras are assumed to be finite dimensional but not necessarily associative. If \( A \) is an algebra over a field \( K \) let \( Aut(A) \) denote the group of algebra automorphisms of \( A \). We say that \( A \) has a transitive automorphism group if \( Aut(A) \) acts transitively on the non-zero points of \( A \). An algebra \( A \) is said to be non-trivial if \( \text{dim} \ A > 1 \) and \( A^2 \neq 0 \).

We show that if \( A \) is a non-trivial algebra with a transitive automorphism group then \( K = GF(2) \), \( A \) is a Kostrikin algebra and \( Aut(A) \) is the semi-direct product of two finite cyclic groups.

Theorem 1: If \( A \) is a non-trivial algebra with transitive automorphism group over a field \( K \) then \( K = GF(2) \).

Proof: First assume that \( K \) is infinite. Let \( a, b \in A \setminus \{0\} \). Then there exists an \( \alpha \in Aut(A) \) such that \( \alpha(a) = b \) and this implies that \( \alpha L_a \alpha^{-1} = L_b \) where \( L_a \) and \( L_b \) indicate left multiplication by \( a \) and \( b \) respectively in \( A \). That is, \( L_a \) and \( L_b \) are similar. But in particular, we may allow \( b = \lambda a \) for any nonzero \( \lambda \in K \). Now comparing the characteristic polynomials of \( L_a \) and \( L_b = \lambda L_a \) it is easy to show that \( L_a \) is nilpotent. Similarly \( R_a \) is nilpotent and so \( A \) is a special nil algebra as defined in [7]. It follows from Theorem 2 of the above paper that \( A^2 = 0 \).

Now assume that \( K \) is finite. Then \( Aut(A) \) certainly acts transitively on the one dimensional subspaces of \( A \) and so the results of Shult [5] imply that \( K = GF(2) \).

Definition: Let \( K = GF(2^n) \) and \( \mu \) be any fixed element in \( K \). Let \( \circ : K \times K \to K \) be the map defined by \( x \circ y = \mu(xy)^{2^n-1} \). Let \( A(n, \mu) \) denote the algebra over \( GF(2) \) obtained from \( K \) by replacing the usual multiplication in \( K \) by the map \( \circ \).

We call \( A(n, \mu) \) a Kostrikin Algebra since these algebras were investigated by Kostrikin in [4].

* This research was supported by NSERC grant A5232.

Received by the editors December 24, 1984 and, in revised form, March 27, 1985.

AMS 1980 Subject Classification: primary 17A99, secondary 20B25.

Key Words and Phrases. Transitive groups, automorphism groups, Kostrikin algebras, homogeneous algebras, automorphic algebra.

Theorem 2: If $A$ is a non-trivial algebra with transitive automorphism group then $A$ is a Kostrikin Algebra.

Proof: By Theorem 1, $K = GF(2)$. Let $n = \dim A$. If $n$ is odd then the result was proved by Sweet [8] and finally Ivanov [3] proved that the result was true for any finite $n$.

Theorem 3: Let $A$ be a non-trivial algebra of dimension $n$ with transitive automorphism group. Then $A = A(n, \mu)$ for some $\mu \in GF(2^n)$ and $\text{Aut}(A) = C_r \rtimes C_s$ where $r = 2^n - 1$ and $s = n/\gcd(n, m)$ where $m$ is the smallest positive integer such that $\sigma^m(\mu) = \mu$ and $\sigma$ is the squaring map on the field $GF(2^n)$.

Proof: It follows from Theorem 2 that $A = A(n, \mu)$ for some $\mu \in GF(2^n)$. We denote multiplication in the field by juxtaposition and multiplication in the algebra by $\circ$. Let $\nu$ be any generator of the multiplicative group $GF^*(2^n)$ and $T_\nu$ be the map defined as $T_\nu(x) = \nu x$. Let $\sigma$ be the map defined as $\sigma(x) = x^2$ and $\alpha = \sigma^m$, where $m$ is the smallest positive integer such that $\sigma^m(\mu) = \mu$.

Now it is easy to check that $T_\nu \in \text{Aut}(A(n, \mu))$. Let $\beta \in \text{Aut}(A(n, \mu))$ and let $c = \beta(1)$. Also let $\tau = T_\nu^{-1}\beta$. Now $\tau(1) = 1$ and $\tau \in \text{Aut}(A(n, \mu))$ which implies that

$$\tau(a \circ b) = \tau(\mu(ab)^{2^{n-1}}) = \mu(\tau(a) \tau(b))^{2^{n-1}}$$

Let $S: A(n, \mu) \to A(n, \mu)$ be the mapping defined as $S(x) = x \circ x$. Then $S = T_\mu$ and $S \in \text{Aut}(A(n, \mu))$. In fact, it is easy to show that $S$ belongs to the centre of $\text{Aut}(A(n, \mu))$ which implies that (1) can be written as

$$\tau(\mu(ab)^{2^{n-1}}) = \mu(\tau(ab)^{2^{n-1}}) = \mu(\tau(a) \tau(b))^{2^{n-1}}$$

If we let $b = 1$ we conclude that $\tau \circ^1 = \sigma^{-1} \tau$ and (2) implies that

$$\tau(a^{-1}(ab)) = \sigma^{-1}(\tau(ab)) = \sigma^{-1}(\tau(a) \tau(b))$$

Hence $\tau(ab) = \tau(a) \tau(b)$ and $\tau$ is a field automorphism of $GF(2^n)$. It is well known that $\tau = \sigma^t$ for some integer $t$. In fact $t$ must be a multiple of $m$ since $\tau(\mu) = \mu$. Now $\beta = T_\nu \sigma^t$ and $\alpha \in \text{Aut}(A(n, \mu))$ and so

$$\text{Aut}(A(n, \mu)) = \langle T_\nu, \alpha \rangle$$

where $T_\nu$ is of order $2^n - 1$ and $\alpha$ is of order $s = n/\gcd(n, m)$. Finally observe that $\alpha^{-1} T_\nu \alpha = T_\nu^{2^{m-1}}$ and so

$$\text{Aut}(A(n, \mu)) = \langle T_\nu, \alpha | T_\nu^s = \alpha^s = 1, \alpha^{-1} T_\nu \alpha = T_\nu^{2^{m-1}} \rangle.$$ 

Clearly $\langle T_\nu \rangle$ is a normal subgroup of $\text{Aut}(A(n, \mu))$ and it is easy to show that $\langle T_\nu \rangle \cap \langle \alpha \rangle = 1$ and so

$$\text{Aut}(A(n, \mu)) \cong C_r \rtimes C_s$$

where $r = 2^n - 1$ and $s = n/\gcd(n, m)$. 


Theorem 4: The number of non-isomorphic Kostrikin algebras of dimension $n$ is given by

$$N_n = \frac{1}{n} \sum_{d|n} \phi(d) 2^{n/d}$$

Proof: Theorem 4 of [2] states that the algebras $A(n, \mu)$ and $A(n, \lambda)$ are isomorphic if and only if there is an automorphism of $GF(2^n)$ mapping $\lambda$ to $\mu$. Since the automorphism group of $GF(2^n)$ is generated by $\sigma$, the squaring map, $A(n, \mu)$ and $A(n, \lambda)$ will be non-isomorphic if and only if $\lambda$ and $\mu$ belong to different orbits of $GF(2^n)$. But, $GF(2^n)$ partitions into the sets of roots of all the irreducibles over $GF(2)$ of degrees dividing $n$ (see [6]). Further, the roots of an irreducible of degree $d$ are $\{\alpha, \alpha^2, \ldots, \alpha^{2^{n-1}}\}$, that is, an orbit of $GF(2^n)$. Thus the number of Kostrikin algebras of dimension $n$ is equal to the number of irreducible polynomials over $GF(2)$ of a degree which divides $n$, and this number is given in [1] as the $N_n$ above.

It should be noted that the trivial algebra (in which $\alpha^2 = 0$) is just the Kostrikin algebra with $\mu = 0$. Thus the number $N_n$ in theorem 4 includes the trivial algebra.

References


Department of Mathematics & Computer Science
University of Prince Edward Island
Charlottetown, Prince Edward Island
C1A 4P3