Canad. Math. Bull. Vol. **29** (2), 1986

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 $\mathrm{Aut}(A)$ denote the group of algebra automorphisms of A. We say that A has a transitive automorphism group if $\mathrm{Aut}(A)$ acts transitively on the non-zero points of A. An algebra A is said to be non-trivial if $\dim A > 1$ 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 $\mathrm{Aut}(A)$ 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 $\alpha \in \mathrm{Aut}(A)$ 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 $L_{\lambda a} = \lambda L_a$ 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 $\mathrm{Aut}(A)$ 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 μ 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 algebras.

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* $A \simeq A(n, \mu)$ *for some* $\mu \in GF(2^n)$ *and* $\mathrm{Aut}(A) \simeq C_r \rtimes C_s$ *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* σ *is the squaring map on the field* $GF(2^n)$.

PROOF: It follows from Theorem 2 that $A \simeq A(n, \mu)$ for some $\mu \in GF(2^n)$. We denote multiplication in the field by juxtaposition and multiplication in the algebra by $\circ$ where $x \circ y = \mu(xy)^{2^{n-1}}$. Let ν be any generator of the multiplicative group $GF^*(2^n)$ and T_ν be the map defined as $T_\nu(x) = \nu x$. Let σ 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 $T_\nu \in \mathrm{Aut}(A(n, \mu))$. Let $\beta \in \mathrm{Aut}(A(n, \mu))$ and let $c = \beta(1)$. Also let $\tau = T_{c^{-1}}\beta$. Now $\tau(1) = 1$ and $\tau \in \mathrm{Aut}(A(n, \mu))$ which implies that

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

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

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

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

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

Hence $\tau(ab) = \tau(a)\tau(b)$ and τ 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 $\beta = T_c\sigma^t$ and $\alpha \in \mathrm{Aut}(A(n, \mu))$ and so

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

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

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

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

$$\mathrm{Aut}(A(n, \mu)) \simeq C_r \rtimes C_s$$

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 λ to μ. Since the automorphism group of $GF(2^n)$ is generated by σ, the squaring map, $A(n, \mu)$ and $A(n, \lambda)$ will be non-isomorphic if and only if λ and μ 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 $\{\alpha, \alpha^2, \ldots, \alpha^{2^{d-1}}\}$, 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 $a^2 = 0$) is just the Kostrikin algebra with $\mu = 0$. Thus the number N_n in theorem 4 includes the trivial algebra.

REFERENCES

1. S. W. Golomb, *"Irreducible Polynomials, Synchronization Codes, Primitive Necklaces, and the Cyclotomic Algebra,"* in *Combinatorial Mathematics and its Applications* (R. C. Bose and T. A. Dowling, eds.) University of North Carolina Press, Chapel Hill, 1969.

2. F. Gross, *"Finite Automorphic Algebras over GF(2),"* Proc. A.M.S. **31** (1972), pp. 10–14.

3. D. N. Ivanov, "On Homogeneous Algebras Over GF(2)," Vestnik Mos. Unive. Matematika, **37** (1982), pp. 69–72.

4. A. I. Kostrikin, *"On Homogeneous Algebras,"* Izvestia Acad. Nauk U.S.S.R., **29** (1965), pp. 471–484.

5. E. E. Shult, *"On Finite Automorphic Algebras,"* (Illinois J. Math., **13** (1969), pp. 625–653.

6. G. J. Simmons, *"The Number of Irreducible Polynomials of Degree n over GF(p),"* Amer. Math. Monthly, **77** (1970), pp. 743–745.

7. L. G. Sweet, *"On the Triviality of Homogeneous Algebras over an Algebraically Closed Field,"* Proc. A.M.S. **48** (1975), pp. 321–324.

8. L. G. Sweet, *"On Involutions of Quasi-Division Algebras,"* Can. Math. Bull., **17**(5), (1975), pp. 723–725.

DEPARTMENT OF MATHEMATICS & COMPUTER SCIENCE
UNIVERSITY OF PRINCE EDWARD ISLAND
CHARLOTTETOWN, PRINCE EDWARD ISLAND
C1A 4P3

https://doi.org/10.4153/CMB-1986-036-1 Published online by Cambridge University Press