PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 79, Number 2, June 1980

ON FINITE DIVISION RINGS

ROBERT H. OEHMKE

ABSTRACT. Herein it is shown that the set of right powers of a generic element of a finite division ring contains a basis of the ring as an algebra over a prime field. This result is then applied to finite flexible division rings of characteristic not 2 to obtain commutativity.

A finite division ring (or semifield [4]) is a finite algebraic system containing at least two distinguished elements 0 and 1. A division ring $\mathfrak{A}$ possesses two binary operations, addition and multiplication, designated in the usual notation and satisfying the following axioms:

(i) $(\mathfrak{A}, +)$ is a group with identity 0.

(ii) If $a, b \in \mathfrak{A}$ and $ab = 0$ then $a = 0$ or $b = 0$.

(iii) If $a, b, c \in \mathfrak{A}$ then $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.

(iv) The element 1 satisfies the relationship $1 \cdot a = a \cdot 1 = a$ for all a in $\mathfrak{A}$.

It is seen easily that there are unique solutions to the equations $ax = b$ and $xa = b$ for every nonzero a and every b in $\mathfrak{A}$. It also follows easily that addition is commutative. In fact it can be seen that $\mathfrak{A}$ is a vector space over some prime field $F = GF(p)$ and that $\mathfrak{A}$ has p^n elements where n is the dimension of $\mathfrak{A}$ over F [4].

Let $u_1, \ldots, u_n$ be a basis of $\mathfrak{A}$ over F and let $\delta_1, \ldots, \delta_n$ be a set of n algebraically independent elements over F. Let $K = F(\delta_1, \ldots, \delta_n)$. As usual the algebra $\mathfrak{A}_K$ is the tensor product over F of $\mathfrak{A}$ and K. $\mathfrak{A}_K$ can be considered as a vector space over K with basis $u_1, \ldots, u_n$. Thus

$$x = \delta_1 u_1 + \cdots + \delta_n u_n$$

is an element of $\mathfrak{A}_K$ and is called the generic element of $\mathfrak{A}$ [3].

For any y in $\mathfrak{A}_K$ we shall write $y^l = y^{l-1} \cdot y$, $y^0 = 1$ and $y^1 = y$ if $l \geq 2$ for the right powers of the element y. If R_y designates the linear transformation induced by right multiplication by y then $y^l = 1 \cdot R_y^l$. If x_0 is an element of $\mathfrak{A}$ and is written as $x_0 = \delta_{10} u_1 + \cdots + \delta_{n0} u_n$ where $\delta_{i0} \in F$ we shall call x_0 a specialization of x.

Now R_x as a linear transformation on the vector space $\mathfrak{A}_K$ over K has a characteristic polynomial $m_x(\lambda)$ of degree n. If S_x is the matrix representation of R_x with respect to the basis $u_1, \ldots, u_n$ then $m_x(\lambda) = |\lambda I - S_x|$. But clearly, S_x has entries that are linear over F in the variables $\delta_1, \ldots, \delta_n$. Thus $m_x(\lambda)$ is a homogeneous polynomial in $F[\lambda, \delta_1, \ldots, \delta_n]$. We can write $m_x(\lambda) = \Sigma \sigma_i(x) \lambda^i$ where $\sigma_i(x)$ is a homogeneous polynomial in $F[\delta_1, \ldots, \delta_n]$ of degree $n - i$.

We let R_{x_0} designate the linear transformation induced by right multiplication by x_0 in $\mathfrak{A}$. Then R_{x_0} is represented by the matrix S_{x_0} with respect to the basis

Received by the editors May 11, 1979.
AMS (MOS) subject classifications (1970). Primary 17A01, 51A05.

0002-9939/80/0000-0253/$01.75

$u_1, \ldots, u_n$ where S_{x_0} is the specialization of S_x; i.e., where the variables $\delta_1, \ldots, \delta_n$ occurring in S_x are replaced by $\delta_{10}, \ldots, \delta_{n0}$. Since the entries of S_x are polynomials this specialization is always well defined. We further extend K to a field L which contains a new variable δ and the roots of the polynomials $m_{x_0}(\lambda)$ and $\delta - \mu_{x_0}(\lambda)$ in λ where $\mu_{x_0}(\lambda)$ is the minimal polynomial satisfied by R_{x_0}. We can write

$$m_{x_0}(\lambda) = \prod_j (\lambda - \xi_j), \quad \delta - \mu_{x_0}(\lambda) = \prod_i (\lambda - \beta_i).$$

We borrow generously from Braun and Koecher [2, p. 102] in proving the following result.

THEOREM 1. *The irreducible factors of* $\mu_{x_0}(\lambda)$ *are the same as the irreducible factors of* $m_{x_0}(\lambda)$.

PROOF.

$$\begin{aligned}\prod_j (\delta - \mu_{x_0}(\xi_j)) &= \prod_j \prod_i (\xi_j - \beta_i) = \pm \prod_i \prod_j (\beta_i - \xi_j) \\ &= \pm \prod_i |\beta_i I - S_{x_0}| = \pm \left| \prod_i (\beta_i I - S_{x_0}) \right| \\ &= \pm \left| \prod_i (S_{x_0} - \beta_i I) \right| = |\delta I - \mu(S_{x_0})|.\end{aligned}$$

But $\mu(S_{x_0}) = 0$. Therefore the above polynomial in δ is δ^n. Therefore $\mu_{x_0}(\xi_j) = 0$ for all ξ_j and the theorem follows.

Now R_{x_0} is nonsingular on the vector space $\mathfrak{A}$ due to the definition of a division ring. Thus none of the ξ_j's can be 0. It now follows that the constant term of $m_x(\lambda)$ is a homogeneous form in $\delta_1, \ldots, \delta_n$ not representing 0 nontrivially.

Let V_x be the subspace of $\mathfrak{A}_K$ generated by the right powers of x over K and $\bar{R}_x$ the restriction of R_x to V_x. Assume V_x is of dimension m. The characteristic polynomial, $\varepsilon_x(\lambda)$, of $\bar{R}_x$ is of degree m and must divide $m_x(\lambda)$. Therefore $\varepsilon_x(\lambda)$ must be homogeneous in $\lambda, \delta_1, \ldots, \delta_n$ and hence is a polynomial in λ with polynomial coefficients in the δ_i's [5, p. 127]. Therefore the "constant term" of $\varepsilon_x(\lambda)$ is a form of degree m in $\delta_1, \ldots, \delta_m$ that divides the "constant term" of $m_x(\lambda)$. But then the "constant term" of $\varepsilon_x(\lambda)$ is a form in n variables and of degree m that does not represent 0 nontrivially. By the Artin-Chevalley Theorem [5, p. 140] we see that $m = n$. Therefore

THEOREM 2. $V_x = \mathfrak{A}_K$ *and* $1, x, \ldots, x^{n-1}$ *is a basis of* $\mathfrak{A}_K$.

Following a similar argument as above and assuming $\mathfrak{A}$ is strictly power associative, McCrimmon [6] gave an alternate proof to Albert's result [1] that such $\mathfrak{A}$'s were fields. We shall give another application of this result to flexible algebras.

A flexible algebra is an algebra for which $a(ba) = (ab)a$ for all a and b in $\mathfrak{A}$. If L_a and R_a denote the linear transformations induced by left multiplication and right multiplication respectively then the flexible identity is equivalent to $R_a L_a = L_a R_a$ for all $a \in \mathfrak{A}$. The flexible identity can be linearized to

$$a(bc) + c(ba) = (ab)c + (cb)a. \tag{1}$$

If the characteristic is not 2 then (1) implies $a(ba) = (ab)a$. Thus in the characteristic not 2 case the flexible identity extends to all scalar extensions of $\mathfrak{A}$, in particular to $\mathfrak{A}_K$. In $\mathfrak{A}_K$ let W be the set of all vectors w such that $w(R_x - L_x) = 0$. Clearly $1 \in W$. If $\mathfrak{A}$ is flexible then W is an R_x invariant subspace of $\mathfrak{A}$ and must be V_x. But $V_x = \mathfrak{A}_K$. Therefore

THEOREM 3. *If $\mathfrak{A}$ is a flexible division ring of characteristic not 2 then $\mathfrak{A}$ is commutative.*

REFERENCES

1. A. A. Albert, *On nonassociative division algebras*, Trans. Amer. Math. Soc. **72** (1952), 296–309.
2. H. Braun and M. Koecher, *Jordan-Algebren*, Springer-Verlag, Berlin, 1966.
3. N. Jacobson, *Structure and representations of Jordan algebras*, Amer. Math. Soc. Colloq. Publ., vol. 39, Amer. Math. Soc., Providence, R. I., 1968.
4. D. Knuth, *Finite semifields and projective planes*, J. Algebra **2** (1965), 182–217.
5. S. Lang, *Algebra*, Addison-Wesley, Reading, Mass., 1965.
6. K. McCrimmon, *A note on finite division rings*, Proc. Amer. Math. Soc. **17** (1966), 1173–1177.

DEPARTMENT OF MATHEMATICS, THE UNIVERSITY OF IOWA, IOWA CITY, IOWA 52242