REFERENCES

1. A. A. Albert, *Quasigroups*. I, Trans. Amer. Math. Soc. vol. 54 (1943) pp. 507–519.
2. ———, *Quasigroups*. II, Trans. Amer. Math. Soc. vol. 55 (1944) pp. 401–419.
3. O. Ore, *Chains in partially ordered sets*, Bull. Amer. Math. Soc. vol. 49 (1943) pp. 558–566.

UNITED STATES NAVAL ACADEMY, POSTGRADUATE SCHOOL

TWO ELEMENT GENERATION OF A SEPARABLE ALGEBRA

A. A. ALBERT

The *minimum rank* of an algebra A over a field F is defined to be the least number $r=r(A)$ of elements $x_1, \cdots, x_r$ such that A is the set of all polynomials in $x_1, \cdots, x_r$ with coefficients in F. In what follows we shall assume that A is an *associative algebra of finite order* over an *infinite* field F.

It is well known that $r(A)=1$ if A is a separable field over F and that $r(A)=2$ if A is a total matric[1] algebra over F. Over fourteen years ago I obtained but did not publish the result that $r(A)=2$ if A is a central division algebra over F. The purpose of this note is to provide a brief proof of the generalization which states that if A is any *separable* algebra over F then $r(A)=1$ or 2 according as A is or is not commutative.

We observe first that a commutative separable[2] algebra Z is a direct sum of separable fields and that there exists a scalar extension K over F such that Z_K has a basis $e_1, \cdots, e_n$ over F for pairwise orthogonal idempotents e_i. If $u_1, \cdots, u_n$ is a basis of Z over F and $x=a_1u_1+\cdots+a_nu_n$ the powers x^i have the form

$$x^i = \sum_{j=1}^{n} b_{ij}u_j \qquad (i = 1, \cdots, n),$$

where the determinant

$$d(a_1, \cdots, a_n) = |b_{ij}|$$

is a polynomial in the parameters $a_1, \cdots, a_n$. If $c_1, \cdots, c_n$ are any

Received by the editors April 13, 1944.

[1] See page 95 of my *Modern higher algebra*.

[2] The definition of a separable algebra given below reduces to a direct sum of fields in the commutative case. When F is nonmodular the concept of semisimple algebra and separable algebra coincide.

distinct elements of K the quantity $x_0 = c_1e_1 + \cdots + c_ne_n$ is known[1] to generate the diagonal algebra Z_K, that is $Z_K = F[x_0]$ has a basis $x_0, x_0^2, \cdots, x_0^n$. If we express the quantities $e_1, \cdots, e_n$ linearly in terms of $u_1, \cdots, u_n$ we see that x_0 is a value of x for values a_{i0} of the a_i in K. The linear independence of $x_0, x_0^2, \cdots, x_0^n$ implies that $d(a_{10}, \cdots, a_{n0}) \neq 0$. Then $d(a_1, \cdots, a_n)$ is not identically zero and thus there exists a quantity x in Z such that Z has a basis $x, x^2, \cdots, x^n$ over F, $Z = F(x)$, $r(Z) = 1$.

An algebra A is called a separable[2] algebra if A is a direct sum of simple components A_k such that the center of every A_k is a separable field over F. If x and y are in A we define

$$F[x, y]$$

to mean the set of all polynomials

$$\sum_{i=1,\cdots,m}^{j=1,\cdots,q} a_{ij}x^iy^j \qquad (a_{ij} \text{ in } F).$$

Only a finite number of the power products x^iy^j are linearly independent and each $F[x, y]$ is a linear subspace of A, m and q may be be selected so that $F[x, y]$ has order mq over F.

A separable algebra has a unity quantity e and if $A = F[x]$ then A has a basis $x^0 = e, x, \cdots, x^{n-1}$ over F, $A = F[x, e]$. Also A is commutative. If A is not commutative and $A = F[x, y]$ then $e = x[f(x, y)]y$ and thus x and y must be nonsingular. Note then that A has a basis of power products x^iy^j where $i = 0, \cdots, m-1$ and $j = 0, \cdots, q-1$. We use these results in the proof of our principal

THEOREM. *If A is a separable algebra which is not commutative then $r(A) = 2$, $A = F[x, y]$ for nonsingular elements x and y such that $F[x]$ is separable.*

We first study the case where A is the direct product of a total matric algebra M of degree g and a division algebra D of degrees s over a separable center C over F. It is well known[3] that D contains a maximal separable subfield $W = C[x_0]$ of degree s over C and that $W = F[x_0]$. The algebra $Q = (e_{11}, \cdots, e_{gg})$, whose basis consists of a set of primitive idempotents of M whose sum is its unity element e, has the property that $Z \neq Q \times W$ is separable and commutative, and so $Z = F[x]$. If K is a scalar splitting field over C of D the algebra Z_K contains $n = gs$ primitive pairwise orthogonal idempotents whose sum

[3] See Theorem 4.18 of my *Structure of algebras*, Amer. Math. Soc. Colloquium Publications, vol. 24, New York, 1939.

is the unity element e of the total matric algebra A_K of degree n over K. Also $Z=C[x]$, $Z_K=K[x]$ and it is known[1] that there exists a quantity y_0 in A_K such that

$$A_K = K[x, y_0],$$

that is, the power products $x^i y_0^j$ taken for $i, j=1, \cdots, n$ are linearly independent in K. If $p=n^2$ and $u_1, \cdots, u_p$ are a basis of A over C we may write $y=a_1u_1+ \cdots +a_pu_p$ and express the powers x^iy^j in the form

$$z_k = x^iy^j = \sum_{h=1} b_{kh}u_h \qquad (k = i + jn - n;\ i, j = 1, \cdots, n),$$

for b_{kh} in F. The determinant $d(a_1, \cdots, a_p)=|b_{kh}|$ is a polynomial in $a_1, \cdots, a_p$ with coefficients in C which is not identically zero since it is not zero for values $a_{10}, \cdots, a_{j0}$ which define y_0. It follows that $A=C[x, y]$. But $C[x]=F[x]$ so that $A=F[x, y]$.

We finally consider a separable algebra A which is the direct sum of simple components $A_1, \cdots, A_t$. By the proofs above every component $A_k=F[x_k, y_k]$, where y_k is the unity quantity e_k of A_k when A_k is commutative, $Z_k=F[x_k]$ is separable. The algebra Z which is the direct sum of $Z_1, \cdots, Z_t$ is a commutative separable algebra and so $Z=F[x]$. Let $y=y_1+ \cdots +y_t$. Since $F[x]$ contains every x_k the linear space $F[x, y]$ contains $x_k^iy^j=x_k^iy_k^j$. For $x_k^i=x_k^ie_k$ and $e_ky^j=(e_ky)^j=y_k^j$. It follows that $F[x, y]$ contains every A_k and that $F[x, y]=A$.

THE UNIVERSITY OF CHICAGO