Internat. J. Math. & Math. Sci.
VOL. 14 NO. 3 (1991) 463-470

GENERALIZATIONS OF THE PRIMITIVE ELEMENT THEOREM

CHRISTOS NIKOLOPOULOS and **PANAGIOTIS NIKOLOPOULOS**

Dept. of Computer Science
Bradley University
Peoria, IL 61625

Department of Mathematics
Michigan State University
E. Lansing, MI 48823

(Received July 31, 1990 and in revised form February 21, 1991)

ABSTRACT. In this paper we generalize the primitive element theorem to the generation of separable algebras over fields and rings. We prove that any finitely generated separable algebra over an infinite field is generated by two elements and if the algebra is commutative it can be generated by one element. We then derive similar results for finitely generated separable algebras over semilocal rings.

KEYWORDS AND PHRASES: Generation of algebras, separable algebras, semilocal rings.
1980 AMS subject classification code: 16,17

1. **INTRODUCTION.** It is a well known result (Nagahara, [1]) that any finitely generated separable simple algebra A over a field F is generated over F by two conjugate elements of A. It is also known that if x is an element of A which does not belong to the center of A, then there exists a unit x_1 in A such that A is generated over F by x and x_1 (Nagahara, [1]).

We present a proof of some of these results in section 2. In section 3, we examine the problem of generating separable finitely generated algebras, not necessarily simple, over infinite fields and local or semilocal rings. Namely, we show that a finitely generated separable algebra over an infinite field F is generated by two elements over F. In the case the algebra is commutative it can be generated by one element. We give a counter example to show that the condition, that the ground field is inifinite, is necessary. In section 4, we examine algebras over semilocal rings and we show that a finitely generated central separable algebra over a semilocal ring can also be generated by two elements over the ring and one element if the algebra is commutative. The condition that the algebra is central can be eliminated and the theorem still holds if the local fields of the ring, i.e. the ring modulo its maximal ideals, are infinite.

2. CONVENTIONS, RELEVANT RESULTS.

Let $A = \sum_{i,j=1}^{n} D\, e_{ij}$ be a simple ring finite over a simple subring B as left B-module where the e_{ij} are matrix units and $D = C_A(\{e_{ij}\})$ is a division ring. $C_A(S)$ is the centralizer of the subset S of A in A. Let $B_1 = B[\{e_{ij}\}] = \sum_{i,j=1}^{n} D_1\, e_{ij}$, where $D_1 = C_{B_1}(\{e_{ij}\})$ is a division ring. We prove here some basic results from [1], using a somewhat different approach.

Lemma 2.1: If D is a finitely generated separable division algebra over the field F, then there exist units u,d in D such that $D = F[u, d\, u\, d^{-1}]$.

Proof. Let M be a separable maximal subfield of D over F, then $M = F[u]$ with some u (see [1] Corollary 7.9). Let C be the center of D. Then $M = C[u]$ and D is finitely generated, central division algebra over C, with maximal subfield M. Therefore if $[D:C] = n^2$, (by [3], theorem VII 11.3), we know that there exists a unit d in D such that the set $\{u^i\, d\, u^j / i,j = 0, 1, \ldots, n-1\}$ is basis for D over C. Consequently, $D = \bigoplus_{i,j} u^i\, d\, u^j\, C = \sum_{i,j} u^i (dud^{-1})^j C = C[u, dud^{-1}]$ $= C[u][dud^{-1}] = F[u, dud^{-1}]$, which completes the proof.

Lemma 2.2: Let A, B be as in the conventions. If $D = D_1[x,y]$ with some conjugate x,y in D, then $A = B[u,v]$ for some conjugate u,v units of A.

Proof. Since $A = \sum_{i,j=1}^{n} D\, e_{ij}$, if n=1 the lemma is trivially true. Let n>1 and $w = \sum_{i=1}^{n} e_{i,n-i+1} = w^{-1}$, $u_1 = \sum_{i=2}^{n} e_{i-1,i}$ and $v_1 = \sum_{i=2}^{n} e_{i,i-1} = w u_1 w^{-1}$. Since x and y are conjugates, we have $y = dxd^{-1}$ for some d element of D. Also, $e_{ij} = v_1^{\,i-1} u_1^{\,n-1} v_1^{\,n-1} u_1^{\,j-1}$ for i,j=1, ..., n. In case $D = D_1$ we have $B[1-u_1, w(1-u_1)w^{-1}] = B[u_1, v_1] = B[\{e_{ij}\}] = A$, and $1-u_1$ is a unit. Hence, assume that $D \neq D_1$. Examine two cases: (i) if $xy \neq 1$ and (ii) if $xy = 1$. In the first case, define u as $u_1 + x e_{n1}$, v as $v_1 + y e_{1n}$. Then $v = dwu(dw)^{-1}$ and $u^{-1} = v_1 + x^{-1} e_{1n}$ is an element of B[u]. Therefore $(x^{-1}-y)e_{1n} = u^{-1} - v$ is an element of B[u,v]. Hence $(1-xy)\, e_{nn} = u(x^{-1}-y)e_{1n}$ is an element of B[u,v] and $(1-xy)e_{in} = u^{n-i}(1-xy)e_{nn}$ and $(1-xy)e_{nj} = (1-xy)e_{nn}v^{n-j}$ are elements of B[u,v], for every i,j =1,..., n. Hence for every i,j = 1,..., n, we have $(1-xy)^2\, e_{ij}$ is in B[u,v]. Since $(1-xy)^2$ is a unit in B[u,v], we get $\{e_{ij}\}$ is a subset of B[u,v].

Also $x = u^n$, $y = \sum_{i=1}^{n} e_{il}\, v\, e_{ni}$ are in B[u,v] and therefore $B[u,v] = B[x,y,\{e_{ij}\}]$

$= D_1[x,y, \{e_{ij}\}] = D[\{e_{ij}\}] = A$. In the second case, (ii) if $xy=1$ then $D=D_1[x,y]=D_1[x]$ and since $D \neq D_1$ we get $x \neq \pm 1$ or $x^2 \neq 1$. We can now apply the first case for $y=x$ to complete the proof.

THEOREM 2.1: Any separable simple algebra finitely generated over a field is generated over the ground field by two conjugate invertible elements.

Proof. If A is separable simple finitely generated over a field F and $A = \sum_{i,j=1}^{n} De_{ij}$, then Lemma 2.1 implies $D=F[x, d\,x\,d^{-1}]$, where x is a generating element over F of a maximal subfield of D. Therefore, by Lemma 2.2 we have $A = F[u,v]$ for some conjugate u,v units in A, which completes the proof of the theorem.

Lemma 2.3: Let E a proper division subring of a division ring D and a in D with $ab \neq ba$ for some b in $D - E$. Let C the center of D. Then:

(1) There exist at most two elements c_i, $i = 1,2$ in $C \cap E$ such that $(b+c_i)a(b+c_i)^{-1} \in E$.

(2) If $a \in E$, then there exists at most one element c of the centralizer of a in E such that $(b+c)a(b+c)^{-1} \in E$.

Proof. Suppose that there exist c_1, c_2, c_3 three different elements in $C \cap E$ such that $ai=(b+c_i)a(b+c_i)^{-1}$ is contained in E, for i=1,2,3. Then $ba+c_ia= a_ib+a_ic_i$ for i=1,2,3 hence $(c_1-c_2)a=(a_1-a_2)b+(a_1c_1-a_2c_2)$ and $(c_1-c_3)a=(a_1-a_3)b+(a_1c_1-a_3c_3)$ so $a=(c_1-c_2)^{-1}(a_1-a_2)b+(c_1-c_2)^{-1}(a_1c_1-a_2c_2)$ and $a=c\,(c_1-c_3)^{-1}(a_1-a_3)b+(c_1-c_3)^{-1}(a_1c_1-a_3c_3)$. Subtracting those two, by elementary calculation we get $a_2=a_3$ which contradicts the fact that if $c_2 \neq c_3$ then $(b+c_2)a(b+c_2)^{-1} \neq (b+c_3)a(b+c_3)^{-1}$, for if $(b+c_2)\,a(b+c_2)^{-1} = (b+c_3)\,a(b+c_3)^{-1} = a'$, then $(c_2-c_3)\,a= a'(c_2-c_3)$, which gives $a=a'$. But $(b+c_2)a(b+c_2)^{-1}=a$ leads to a contradiction $ba=ab$. To prove the second assertion suppose there are two elements c_1 and c_2 in $C_R(\{a\})$ with $c_1 = c_2$ and $a_i = (b+c_i)a(b+c_i)^{-1}$ an element of F, for i=1,2. Then $b = (a_2-a_1)^{-1}[(a_1c_1-c_1\,a)-(a_2\,c_2-c_2a)] \in E$ and this is a contradiction, which proves the lemma.

Using the above lemma we can prove the following:

THEOREM 2.2: If D is separable division algebra finitely generated over field F and a is an element of D such that a is not contained in the center of D, then $D = F[a, a_1]$ for some a_1 in D.

Proof. Consider M the maximal separable subfield of D. If $M = F[x]$, then theorem 2.1 implies $D=[x,y]$, for some y. By the fundamental theorem of Galois

theory for simple rings (see [1], Theorem 7.7), since $M = C_D(M)$, we have that the number of intermediate fields between M and C is equal to the number of intermediate rings between D and M. Therefore, the number of intermediate rings between D and M is finite, say $\{A_1,\ldots, A_n\}$. Now y is not contained in A_i for any i, since $F[x,y] = D$. We examine two cases:

(i) If $ay = ya$ then $a(x+y) \neq (x+y)a$, since a is not in the center of D, so $D = F[x,x+y]$ and we can apply (ii) for x, x+y.

(ii) If $ay \neq ya$, from lemma 2.3 we have that for every i, there exist at most two elements c_1, c_2 in F such that $(y+c_1)a(y+c_1)^{-1}$ is an element of A_i, and $(y+c_2)a(y+c_2)^{-1}$ is an element of A_i. Let $y_0=y+c_0$ where c_0 in F such that $y_0ay_0^{-1}$ is not contained in A_i for any i. Then $D=M[y_0ay_0^{-1}]=F[y_0ay_0^{-1},u]=F[a,y_0^{-1}uy_0]$.

THEOREM 2.3: Let A be a separable finitely generated simple algebra over a field F and a an element of A not contained in the center of A. Then $A = F[a, a_1]$ for some a_1 unit in A.

Proof. See [1], Theorem 12.1.

3. GENERATION OF ALGEBRAS OVER FIELDS.

Lemma 3.1: If S is a commutative algebra over a field F, then S is separable over F if and only if S is the direct sum of separable field extensions of F.

Proof. The proof follows since commutative separable algebras over fields are semisimple, hence S is the direct sum of field extensions of F which are separable over F since S is.

We now prove a generalization of the primitive element theorem for finitely generated commutative separable algebras.

THEOREM 3.1: If S is a finitely generated commutative separable algebra over an infinite field F, then S is generated over F by only one element, i.e. $S = F[a]$, for some a in S.

Proof. By Lemma 3.1 we have $S=F_1\oplus F_2+\ldots \oplus F_n$, with Fi a separable finite field extension of F. By the primitive element theorem, $F_i = F[x_i]$ for some x_i in S, which gives $S=F[x_1, \ldots, x_n]$. Let n=2. Then $S=F_1 \oplus F_2=F[x_1]\oplus F[x_2]$. Now, since $F_i=F[x_i]$ is a separable field extension of F, there are a finite number of fields between F_i and F. If A is a commutative separable subalgebra of S, then $A=F'_1\oplus F'_2$ with F'_i subfield of F_i and therefore there is only a finite number of commutative separable subalgebras of S. If $x=x_1+ax_2$, where a in F, then

F[x] is a commutative separable subalgebra of S and since F is infinite but there can only be a finite number of F[x]'s, there exist two different elements x', x'' of S, $x' = x_1 + a_1x_2$ and $x'' = x_1 + a_2x_2$, with a_i in F, such that F[x'] = F[x'']. Consequently, x' and x'' are contained in F[x'], which implies $x' - x'' = (a_1 - a_2)x_2$ also belongs to F[x']. Since $a_1 - a_2$ is invertible, x_2 and $x_1 = x' - a_1x_2$ belong to F[x'], which gives that $S = F[x_1, x_2]$ is contained in F[x']. Hence, $S = F[x_1, x_2] = F[x']$. An easy induction on n gives the result.

We now prove that if the algebra is not commutative we can still generate the algebra from just two elements.

THEOREM 3.2: Let S be a finitely generated separable algebra over an infinite field F. Then S = F[x,y], for some x,y in S.

Proof. S separable implies S is semisimple so $S = S_1 \oplus \ldots \oplus S_n$ with S_i simple and separable over F. By Theorem 2.3 we have $S_i = F[x_i, y_i]$, x_i, y_i contained in S. Let Z_i denote the extension $F[x_i]$ of F for i=1,..., n. Then Z_i is separable over F and if $Z = Z1 \oplus \ldots \oplus Zn$ then Z is a commutative separable algebra over F. Now Theorem 3.1 implies that Z = F[x] for some x in Z. Let $y = y_1 + \ldots + y_n$. Then we have x_k is an element of F[x], for hence x_k is an element of F[x,y] for every k and $x_k^i y^j = (x_k^i e_k)\, y^j = x_k^i (e_k y^j) = x_k^i (e_k y)^j = x_k^i (e_k y_k)^j = x_k^i y_k^j$, where e_k is the identity in $F[x_k]$. So $x_k^i y_k^j$ is contained in F[x,y] hence y_k is contained in F[x,y] so $F[x_k, y_k]$ is contained in F[x,y] for every k.

Therefore $S = \bigoplus_{k=1}^{n} F[x_k, y_k]$ is contained in F[x,y], from which S = F[x,y].

This proves the theorem.

The condition that the field has to be infinite in Theorems 3.1 and 3.2 is necessary as is shown by the next example.

If F is the field with q elements, $F = \{a1 \ldots, aq\}$ and $S = \bigoplus_{i=1}^{v} Fi$, where $F_i = F$ for every i, $F \cong F[x]/(x-a_i)$. Let v>q. Then S is separable over F but cannot be generated by less than two elements since $F_1 \oplus F_2 \oplus \ldots \oplus F_{q+1} \cong F + F[x]/\prod_{i=1}^{q} (x-a_i) \cong F[x]/(x-a_i) \oplus F[x]/\prod_{i=1}^{q} (x-a_i)$ which cannot be of the form F[x]/poly(x) since $x-a_i$ is not prime to $\prod_{i=1}^{q} (x-a_i)$. In fact if v>rq, where n is the the biggest integer with that property, then S cannot be generated by less than r+1 elements.

4. GENERATION OF ALGEBRAS OVER RINGS.

In proving the following theorems we use the following form of Nakayama's Lemma: Let M be a finitely generated module over a commutative ring R. If AM = M for every maximal ideal A of R, then M = 0.

THEOREM 4.1: Let S be a commutative, finitely generated separable R-algebra, where R is a local ring with maximal ideal I, such that R/I is an infinite field. Then S = R[a], for some a in S.

Proof. By Theorem 1.11[2], we have that S/IS is commutative, finitely generated, separable over the field R/I, so by Theorem 3.1 S/IS = R/I[$\bar{a}$] with some $\bar{a}$ = a+IS contained in S/IS. We prove that IS + R[a] = S. Clearly IS + R[a] is contained in S. Also for every t contained in S we have t + IS = poly $_{R/I}(\bar{a})$ = $(r_n+I)\bar{a}^n+\ldots+(r_1+I)\bar{a}+r_0+I=(r_na^n+\ldots+r_1a+r_0)$ + IS, so t is contained in IS + R[a]. Therefore I. S/R[a] = (IS+R[a])/R[a] = S/R[a] which by Nakayama's lemma implies S = R[a].

THEOREM 4.2: Let A be a finitely generated central separable R-algebra where R is local ring. Then A = R[a,b] for some a,b in A.

Proof. Let I be the maximal ideal of R. A is central separable implies (by Theorem 3.2[2]) that A/IA is finitely generated, separable, simple over R/IS R.1 = R/I a field, therefore by Theorem 1.1 we have A/IA = R/I[$\bar{a},\bar{b}$] for some $\bar{a}$ = a+IA, $\bar{b}$ = b+IA. We show that IA + R[a,b] = A. Clearly IA + R[a,b] is a subset of A. Also for t in A we have $t+IA = \sum_{ij} \bar{a}_{ij}\,\bar{a}^i\,\bar{b}^j = \sum_{ij} a_{ij}\,a^ib^j+IA$ which is contained in R[a,b]+IA. Therefore we have that I.A/R [a,b] = (IA+R[a,b])/R [a,b] = A/R[a,b] and hence by Nakayama's lemma A = R[a,b].

We note that if we drop the condition that A is central over R, the Theorem will still hold if R/I is an infinite field, since in the proof we can use Theorem 3.2 instead of 2.1 to get the same conclusion.

We now prove two theorems for a semilocal base ring.

THEOREM 4.3: Let S be a commutative, finitely generated separable algebra over R, where R is a semilocal ring with maximal ideals $I_1,\ldots,$ I_n such that R/I_j is infinite for every j. Then S = R[a], for some a in S.

Proof. Let radR be the radical of R. Since R/I_j infinite for every j, R/radR = $R/\bigcap_{j=1}^{n} I_j$ has to be infinite. For every j, we can show as in Theorem 2.3

that if $S/I_jS = R/I_j[\bar{a}_j], \bar{a}_j = a_j+I_jS$, then $I_jS+R[a_j] = S$. We have that $S/(\text{rad}R)S = S/\bigcap_{j=1}^{n} I_jS = R/I_1[\bar{a}_1] \oplus R \ldots \oplus R/I_n[\bar{a}_n]$ which is contained in $\bigoplus_{i=1}^{n} R/Ij$

$[\bar{a}_1,\ldots,\bar{a}_n] = R/\text{rad}R[\bar{a}_1,\ldots, \bar{a}_n]$. Therefore $S/(\text{rad}R)S = R/\text{rad}\, R[\bar{a}_1, \ldots,\bar{a}_n]$ and hence (as in Theorem 2.3) $(\text{rad}R)S+R[a_1\ldots, a_n] = S$. Consequently, $S = (\text{rad}R)S + R[a_1, \ldots, a_n] \subsetneq I_jS + R[a_1, \ldots, a_n]$ but also $I_jS + R[a_1,\ldots, a_n] \subsetneq S$, hence we get that for every j we have $I_jS + R[a_1,\ldots, a_n]= S$. Now suppose that $n = 2$. Then $S/(\text{rad}R)S = R/I_1 \cap I_2[\bar{a}_1, \bar{a}_2]$. Consider $R/I_1 \cap I_2 [\bar{a}_x]$, where $\bar{a}_x=a_1 + x\, a_2$, $x \in R/I_1 \cap I_2$. Since $R/I_1 \cap I_2[\bar{a}_1] = R/I_1[\bar{a}_1] \oplus R/I_2[\bar{a}_1]$ and the number of fields between $R/I_i[\bar{a}_1]$ and R/I_i is finite, then the number of fields between $R/I_1 \cap I_2[\bar{a}_1]$ and $R/I_1 \cap I_2$ as well as between $R/I_1 \cap I_2[\bar{a}_2]$ and $R/I_1 \cap I_2$ is finite. Therefore, since $R/I_1 \cap I_2$ is infinite, there exist elements $\bar{x}_1, \bar{x}_2$ of $R/I_1 \cap I_2$ such that $R/I_1 \cap I_2[\bar{a}'] = R/I_1 \cap I_2[\bar{a}"]$, where $\bar{a}' = \bar{a}_1 + \bar{x}_1 \bar{a}_2$, $\bar{a}" = \bar{a}_1 + \bar{x}_2 \bar{a}_2$. Since $\bar{a}'$, $\bar{a}"$ belong to $R/I_1 \cap I_2[\bar{a}']$, then $\bar{a}'-\bar{a}" = (\bar{x}_1-\bar{x}_2)\bar{a}_2$ is an element of $R/I_1 \cap I_2[\bar{a}']$. But $\bar{x}_1-\bar{x}_2$ is in $R/I_1 \cap I_2 = R/I_1 \oplus R/I_2$ and so $\bar{x}_1 - \bar{x}_2 = r_1-r_2$, with r_i element of R/I_i, therefore $\bar{x}_1-\bar{x}_2$ is a unit. Therefore $\bar{a}_2$ is contained in $R/I_1 \cap I_2[\bar{a}']$, hence $\bar{a}_1' = \bar{a}' - \bar{x}_1\bar{a}_2$ is in $R/I_1 \cap I_2[\bar{a}']$, so $R/I_1 \cap I_2[\bar{a}_1, \bar{a}_2] = R/I_1 \cap I_2[\bar{a}']$. Applying finite induction on n we get that $R/\bigcap_{j=1}^{n} I_j[\bar{a}_1,\ldots,\bar{a}_n] = R/\bigcap_{j=1}^{n} I_j[\bar{a}]$, therefore $S/(\text{rad}R)S =$

$R/\text{rad}R[\bar{a}]$ from which we get $(\text{rad}R)\, S + R[a] = S = I_jS + R[a]$. So for every I_j maximal ideal we have I_j. $S/R[a] = (I_jS+R[a])/R[a] = S/R[a]$ which by Nakayama's lemma gives $S = R[a]$.

THEOREM 4.4: Let S be a finitely generated central separable R-algebra, where R semilocal ring with maximal ideas $I_1,\ldots,I_n$ such that R/I_j infinite for every j. Then $S = R[a,b]$, for some a,b in S.

Proof. For every j, S/I_jS is central separable over the field R/I_j (therefore simple), and hence by Section I we have $S/I_jS = R/I_j[\bar{a}_j, \bar{b}_j]$, with $a_j + I_jS$ unit in S/I_jS. As in Theorem 3.3 we can show $I_jS + R[a_j, b_j] = S$ for every $j=1\ldots,n$. Also as in 3.5 $S/(\text{rad}R)S = \bigoplus_{j=1}^{n} R/I_j[\bar{a}_j,\bar{b}_j] = R/\text{rad}R[\bar{a}_1,\ldots, \bar{a}_n, \bar{b}_1,\ldots, \bar{b}_n]$. By Theorem 3.5 we get that $Z = \bigoplus_{j=1}^{n} R/\bigcap I_j[\bar{a}_j] = R/\bigcap I_j[\bar{a}_1,\ldots,\bar{a}_n] = R/$

$\bigcap_{j=1}^{n} I_j[\bar{a}]$. Let $\bar{b} = \bar{b}1+\ldots \bar{b}_n$. Then for every k, $\bar{a}_k$ we have $R/\bigcap_{j=1}^{n} I_j[\bar{a}] \subseteq R/\bigcap_{j=1}^{n} I_j[\bar{a},\bar{b}]$, and $\bar{a}_k{}^i\bar{b}^j = (\bar{a}_k{}^i\bar{e}_k)\bar{b}^j = \bar{a}_k{}^i(\bar{e}_k\bar{b})^j = \bar{a}_k{}^i\bar{b}_k{}^j$, where $\bar{e}_k$ is the unit of kth summand. Therefore $\bar{a}_k{}^i\bar{b}_k{}^j$ is contained in $R/\bigcap_{j=1}^{n} I_j[\bar{a},\bar{b}]$, so $\bar{b}_k$ is contained in $R/\bigcap_{j=1}^{n} I_j[\bar{a},\bar{b}]$, and consequently for every k we have that $R/\mathrm{rad}R[\bar{a}_k,\bar{b}_k]R/\mathrm{rad}R[\bar{a},\bar{b}]$. Hence $S/(\mathrm{rad}R)S = R/\mathrm{rad}R[\bar{a},\bar{b}]$ with $\bar{a} = a + (\mathrm{rad}R)S$, $\bar{b} = b + (\mathrm{rad}R)S$. So for every maximal ideal I_j of R we have $I_jS/R[a,b] = (I_jS+R[a,b])/R[a,b] = S/R[a,b]$ which gives $S = R[a,b]$ and completes the proof.

REFERENCES

[1] H. TOMINAGA and T. NAGAHARA, Galois theory of simple rings, Okayama University, Japan, 1970.

[2] F. DeMEYER and E. INGRAHAM, Separable algebras over commutative rings, 181 Springer-Verlag 1971.

[3] N. JACOBSON, Structure of rings, Amer. Math. Soc. Colloq., Publ. 37, 1956.

[4] F. KASCH, Uber den Satz vom primitiven Element bei Schiefkorper, J. reine und angew. Math., 180 (1951), 150-159.

[5] A. A. ALBERT, Modern Higher Algebra, The Univ. of Chicago Press, 1937.