BULL. AUSTRAL. MATH. SOC. 16A68
VOL. 25 (1982), 433-440.

GENERATORS OF SIMPLE ALGEBRAS

DAVID CHOATE

It is shown that simple algebras of characteristic not equal to 2 , which contain non-trivial elements that satisfy $x^n = x$ for some fixed, minimal integer $n > 1$, are generated by these elements.

1. Introduction

In the study of simple rings idempotents play an important role. For example, it is known that simple algebras which contain non-trivial idempotents are generated by their idempotents (with some exceptions in characteristic two). We will generalize this result by relaxing the hypothesis of a theorem of Jacobson which says that if R is a ring in which $a^n = a$ (with $n > 1$ an integer depending on a) for every $a \in R$ then R must be commutative. We require only that there exists a non-trivial element a such that $a^n = a$ for some integer $n > 1$. With this we can show that some simple algebras at least are "more nearly commutative" in the sense that the commutator $[R, R]$ is contained in a subset of a set which is known to contain it.

2. Definitions

We call an element a an *n-potent* provided $a^n = a$ but $a^t \neq a$ for $1 < t < n$. An n-potent is *non-trivial* provided $a^{n-1} \neq 1, 0$. Observe that a^{n-1} is a non-trivial idempotent since

Received 6 January 1982.

$$(a^{n-1})^2 = a^{2n-2} = a^n a^{n-2} = a^{n-1} .$$

By E_n^{n-1} we mean the additive group generated by the $(n-1)$st powers of non-trivial n-potents. It is clear from the above that $E_n^{n-1} \subset E = E_2^1$.

3. The Lie ideal E_n^{n-1}

LEMMA 1. *If* a *is a non-trivial* n*-potent in a ring* R *, then so are* $a + a^{n-1}r - a^{n-1}ra^{n-1}$ *and* $a + ra^{n-1} - a^{n-1}ra^{n-1}$ *for every* $r \in R$.

Proof. We first show that

$$(a+a^{n-1}r-a^{n-1}ra^{n-1})^k = a^{k-1}(a+a^{n-1}r-a^{n-1}ra^{n-1})$$

by induction. This equation is clearly true for $k = 1$. Assume it is true for some $k \geq 1$. Then

$$\begin{aligned}
&(a+a^{n-1}r-a^{n-1}ra^{n-1})^{k+1} \\
&\quad = (a+a^{n-1}r-a^{n-1}ra^{n-1})^k(a+a^{n-1}r-a^{n-1}ra^{n-1}) \\
&\quad = a^{k-1}(a+a^{n-1}r-a^{n-1}ra^{n-1})(a+a^{n-1}r-a^{n-1}ra^{n-1}) \\
&\quad = a^{k-1}\big((a^2+a^n r-a^n ra^{n-1})+(a^{n-1}ra+a^{n-1}ra^{n-1}r-a^{n-1}ra^{n-1}ra^{n-1}) \\
&\qquad\qquad +(-a^{n-1}ra^n-a^{n-1}ra^{2n-2}r+a^{n-1}ra^{2n-2}ra^{n-1})\big) \\
&\quad = a^k(a+a^{n-1}r-a^{n-1}ra^{n-1})
\end{aligned}$$

since a^{n-1} is an idempotent.

So if $k = n$,

$$(a+a^{n-1}r-a^{n-1}ra^{n-1})^n = a^{n-1}(a+a^{n-1}r-a^{n-1}ra^{n-1}) = a + a^{n-1}r - a^{n-1}ra^{n-1} .$$

Moreover if

$$(a+a^{n-1}r-a^{n-1}ra^{n-1})^t = a + a^{n-1}r - a^{n-1}ra^{n-1}$$

for some t , $1 < t < n$, we have

$$a^{t-1}(a+a^{n-1}r-a^{n-1}ra^{n-1}) = a + a^{n-1}r - a^{n-1}ra^{n-1} .$$

Multiplying from the right by a^{n-1} , we have $a^{t-1}a^n = a^n$, or $a^t = a$. But this is impossible since a is an n-potent. So

$a + a^{n-1}r - a^{n-1}ra^{n-1}$ is an n-potent.

Now if

$$0 = \left(a+a^{n-1}r-a^{n-1}ra^{n-1}\right)^{n-1} = a^{n-2}\left(a+a^{n-1}r-a^{n-1}ra^{n-1}\right) ,$$

we can multiply from the right by a^{n-1} to obtain

$$0 = a^{n-2}a^{n} = a^{n-2}a = a^{n-1} .$$

But this is impossible since a is non-trivial.

Also if

$$1 = \left(a+a^{n-1}r-a^{n-1}ra^{n-1}\right)^{n-1} = a^{n-2}\left(a+a^{n-1}r-a^{n-1}ra^{n-1}\right) ,$$

we can multiply from the left by a^2 to get

$$\begin{aligned} a^2 &= a^n\left(a+a^{n-1}r-a^{n-1}ra^{n-1}\right) \\ &= a\left(a+a^{n-1}r-a^{n-1}ra^{n-1}\right) \\ &= a^2 + a^{n-1}r - a^{n-1}ra^{n-1} . \end{aligned}$$

Subtracting a^2 we find that $a^{n-1}r - a^{n-1}ra^{n-1} = 0$. Substituting this in the first equation, we have $1 = a^{n-1}$, a contradiction.

Therefore $a + a^{n-1}r - a^{n-1}ra^{n-1}$ is a non-trivial n-potent. In a similar manner we can show that $a + ra^{n-1} - a^{n-1}ra^{n-1}$ is also a non-trivial n-potent.

THEOREM 1. *Let R be a ring with a non-trivial n-potent. Then E_n^{n-1} is a Lie ideal of R .*

Proof. Since a is a non-trivial n-potent, so are $a + a^{n-1}r - a^{n-1}ra^{n-1}$ and $a + ra^{n-1} - a^{n-1}ra^{n-1}$ by Lemma 1. Therefore

$$\left(a+a^{n-1}r-a^{n-1}ra^{n-1}\right)^{n-1} = a^{n-2}\left(a+a^{n-1}r-a^{n-1}ra^{n-1}\right) = a^{n-1} + a^{n-2}r - a^{n-2}ra^{n-1}$$

and

$$\left(a+ra^{n-1}-a^{n-1}ra^{n-1}\right)^{n-1} = a^{n-1} + ra^{n-2} - a^{n-1}ra^{n-2}$$

https://doi.org/10.1017/S0004972700005475 Published online by Cambridge University Press

are elements of E_n^{n-1} for each element $r \in R$. Replacing r with ar in tne first and r with ra in the second, we find that
$a^{n-1} + a^{n-1}r - a^{n-1}ra^{n-1}$ and $a^{n-1} + ra^{n-1} - a^{n-1}ra^{n-1}$ are elements of E_n^{n-1} . Since E_n^{n-1} is an additive group, it contains

$$a^{n-1}r - ra^{n-1} = \left(a^{n-1}+a^{n-1}r-a^{n-1}ra^{n-1}\right) - \left(a^{n-1}+ra^{n-1}-a^{n-1}ra^{n-1}\right) .$$

Since E_n^{n-1} is generated by the a^{n-1}'s , E_n^{n-1} is a Lie ideal of R .

COROLLARY 1.1. *Let A be a simple algebra of characteristic not equal to 2 having a non-trivial n-potent. Then* $[A, A] \subset E_n^{n-1}$.

Proof. Since E_n^{n-1} is a Lie ideal of A , we know by a celebrated theorem of Herstein [1, Theorem 1.5] that if A is a simple algebra either E_n^{n-1} is contained in the center of A or $[A, A] \subset E_n^{n-1}$ unless A is of characteristic 2 . The first possibility can be eliminated since the center of A is a field and E_n^{n-1} contains non-trivial idempotents.

COROLLARY 1.2. *Let A be a simple algebra of characteristic not equal to 2 having a non-trivial n-potent. Then the subring generated by its n-potents is A .*

Proof. Let S be the subring generated by the non-trivial n-potents. Then $S \supset E_n^{n-1} \supset [A, A]$ by Corollary 1.1. By a corollary to Herstein's theorem we know that the subring generated by $[A, A]$ is A . So S contains A .

It is natural to ask if E_n^{n-1} can be properly contained in E . The following example shows that this can happen when n is 1 more than an odd prime.

EXAMPLE 1. Let R be the set of $(p+1) \times (p+1)$ matrices over the rational numbers. We first show that $E_{p+1}^{p} \neq \emptyset$. If

https://doi.org/10.1017/S0004972700005475 Published online by Cambridge University Press

$$\begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & & & & \vdots \\ 0 & 0 & 0 & \dots & 1 \\ 0 & +1 & 0 & \dots & 0 \end{pmatrix}_{(p+1)\times(p+1)} = a ,$$

then a is the companion matrix of the polynomial $f(x) = -x + x^{p+1}$. Since f is the minimal polynomial for a, a is a $(p+1)$-potent. If $a^p = 1$, a is invertible. But this is impossible since a has a column of zeros. If $a^p = 0$, $a = a^{p+1} = 0$. So a is a non-trivial $(p+1)$-potent. This means $a^p \in E^p_{p+1}$.

We now show $E^p_{p+1} \subsetneq E$ for every odd prime p. Suppose $E = E^p_{p+1}$. Then if we call e the $(p+1) \times (p+1)$ matrix with 1 as the 1×1 entry and 0's elsewhere, we have $e = a_1^p + \dots + a_k^p$ where k is an integer greater than 1 and each a_i is a non-trivial $(p+1)$-potent. Note that the a_i's are not necessarily distinct. Since each a_i^p is an idempotent, the trace of a_i^p, $\mathrm{tr}\left(a_i^p\right)$, is a positive integer. Note that if $k > 1$, $1 = \mathrm{tr}(e) = \mathrm{tr}\left(a_1^p\right) + \dots + \mathrm{tr}\left(a_k^p\right) > 1$. Therefore $e = a^p$ where $a = \left(\alpha_{ij}\right)$ is a non-trivial $(p+1)$-potent. Multiplying by a we have $ea = a$. After equating entries, we get $\alpha_{ij} = 0$ for $i \geq 2$. Remembering that $a^p = e$ we can equate 1×1 entries to obtain $\alpha_{11}^p = 1$. Now if $\alpha_{11} = 1$, $e = a^p = a$. But this means $a^2 = a$ which is impossible since a is a $(p+1)$-potent. Therefore $\alpha_{11}^{p-1} + \dots + \alpha_{11} + 1 = 0$. This means Q splits $x^{p-1} + \dots + x + 1$, a contradiction when $p \geq 3$. So $E^p_{p+1} \subsetneq E$.

EXAMPLE 2. Let R be a simple ring whose center is the field F. It is easy to show that $E_4^3 = E$ whenever F splits $x^2 + x + 1$ and

https://doi.org/10.1017/S0004972700005475 Published online by Cambridge University Press

char $F \neq 3$. For if there exists an $f \in F$ such that $f^2 + f + 1 = 0$, then we know that $f \neq 1$ since char $F \neq 3$. If e is a non-trivial idempotent of A , then $(fe)^4 = f^4e^4 = fe$. Now if $(fe)^2 = fe$, then $f^2 - f = 0$. Since $f \neq 1$, $f = 0$ which implies $1 = 0$, a contradiction. Note that for any element a such that $a^4 = a$ and $a^2 \neq a$ we know that $a^3 \neq a$. So fe is a 4-potent. Therefore for any $e \in E$, $e = (fe)^3 \in E_4^3$. So $E \subset E_4^3$.

4. Another set of generators

If $n > 1$ is the smallest integer such that $a + a^2 + \ldots + a^{n-1} = 0$ for some $a \in R$, then we call a a pseudo-n-potent. Observe that if a is a pseudo-n-potent *non-trivial* provided $a^{n-1} \neq 1, 0$. By P_n^{n-1} we mean the additive group generated by the $(n-1)$st powers of non-trivial pseudo-n-potents. We do not have to go far to find a ring with $P_n^{n-1} \neq \emptyset$ as the next example shows.

EXAMPLE 3. Let R be the ring of $(n-1) \times (n-1)$ matrices over a field. Consider the matrix

$$a = \begin{pmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \vdots & & & & \vdots \\ 0 & 0 & 0 & \ldots & 1 \\ 0 & -1 & -1 & \ldots & -1 \end{pmatrix}_{(n-1)\times(n-1)}$$

which is the companion matrix to $f(x) = x + x^2 + \ldots + x^{n-1}$. Since f is the minimal polynomial for a , a is a pseudo-n-potent. Clearly $a^{n-1} \neq 1$ since a has a column of zeros; and as before $a^{n-1} = 0$ implies $a = 0$ which is impossible if $n > 2$.

THEOREM 2. *Let R be a ring having a non-trivial pseudo-n-potent. Then P_n^{n-1} is a Lie ideal of R .*

Proof. Let a be a non-trivial pseudo-n-potent in R . From Lemma 1 we learned that

$$\left(a+a^{n-1}r-a^{n-1}ra^{n-1}\right)^k = a^{k-1}\left(a+a^{n-1}r-a^{n-1}ra^{n-1}\right) = a^k + a^{n+k-2}r - a^{n+k-2}ra^{n-1}$$

whenever $a^n = a$. If we sum over k from 1 to $n - 1$, we have

$$\begin{aligned}\left(a+a^{n-1}r-a^{n-1}ra^{n-1}\right) + \left(a+a^{n-1}r-a^{n-1}ra^{n-1}\right)^2 + \ldots + \left(a+a^{n-1}r-a^{n-1}ra^{n-1}\right)^{n-1} \\ = \left(a + a^2 + \ldots + a^{n-1}\right) + \left(a^{n-1} + a + a^2 + \ldots + a^{n-2}\right)r \\ - \left(a^{n-1} + a + a^2 + \ldots + a^{n-2}\right)ra^{n-1} \\ = 0 + 0 - 0 = 0 .\end{aligned}$$

To show n is minimal we suppose there exists a positive integer $t < n - 1$ such that

$$\begin{aligned}0 &= \left(a+a^{n-1}r-a^{n-1}ra^{n-1}\right) + \left(a+a^{n-1}r-a^{n-1}ra^{n-1}\right)^2 + \ldots + \left(a+a^{n-1}r-a^{n-1}ra^{n-1}\right)^t \\ &= \left(a + a^2 + \ldots + a^t\right) + \left(a^{n-1} + a + a^2 + \ldots + a^{t-1}\right)r \\ &\quad - \left(a^{n-1} + a + a^2 + \ldots + a^{t-1}\right)ra^{n-1} .\end{aligned}$$

Multiplying from the right by the idempotent a^{n-1} , we have

$$0 = \left(a + a^2 + \ldots + a^t\right)a^{n-1} = a^n + a^{n+1} + \ldots + a^{t+n-1} = a + a^2 + \ldots + a^t$$

which is a contradiction. Therefore $a + a^{n-1}r - a^{n-1}ra^{n-1}$ is a pseudo-n-potent for every $r \in R$. To show that $a + a^{n-1}r - a^{n-1}ra^{n-1}$ is non-trivial we can use the same argument used in Lemma 1. This means that

$$\left(a+a^{n-1}r-a^{n-1}ra^{n-1}\right)^{n-1} = a^{n-1} + a^{n-2}r - a^{n-2}ra^{n-1}$$

is a generator of P_n^{n-1} . If we replace r with ar , we find that $a^{n-1} + a^{n-1}r - a^{n-1}ra^{n-1}$ is a generator of a^{n-1} for every $r \in R$. In a similar manner we can show that $a^{n-1} + ra^{n-1} - a^{n-1}ra^{n-1}$ is a generator of P_n^{n-1} for every $r \in R$. Since P_n^{n-1} is an additive group we know that

$$ra^{n-1} - a^{n-1}r = \left(a^{n-1}+ra^{n-1}-a^{n-1}ra^{n-1}\right) - \left(a^{n-1}+a^{n-1}r-a^{n-1}ra^{n-1}\right) \in P_n^{n-1} .$$

So P_n^{n-1} is a Lie ideal of R .

COROLLARY 2. *Let* A *be a simple algebra of characteristic not equal to* 2 *having a non-trivial pseudo-n-potent. Then the subring generated by its pseudo-n-potents is* A .

Proof. Follow the same argument used in the proof of Corollary 1.2.

We close with a conjecture.

CONJECTURE. Let A be a simple algebra with a rational center. Let $a \in A$ such that $a^3 \neq 1, 0$. Then either a, a^2 and a^3 are linearly independent over the center, or A contains a non-trivial pseudo-4-potent.

The proof of this conjecture will depend on a number theoretic problem. For if $\beta_1 a + \beta_2 a^2 + \beta_3 a^3 = 0$ where the β_i's are rational numbers, we can assume the β_i's are integers after clearing the equation of denominators. If we multiply this equation by a and a^2 , we get a homogeneous system whose coefficient matrix has determinant $\beta_1^2 + \beta_2^2 + \beta_3^2 - 3\beta_1\beta_2\beta_3$ which must be zero. If in turn this implies $\beta_1 = \beta_2 = \beta_3$, we would know that A contains a non-trivial pseudo-n-potent.

Reference

[1] I.N. Herstein, *Topics in ring theory* (University of Chicago Press, Chicago and London, 1965).

Department of Mathematics,
University of Southwestern Louisiana,
Lafeyette,
Louisiana 70504,
USA.