# FERMAT'S THEOREM FOR ALGEBRAS

GORDON L. WALKER

**1. Introduction.** Let $A$ be an algebra over the field $F$ and let $F[x_1, \cdots, x_n]$ be a free algebra over $F$ generated by indeterminates $x_1, \cdots, x_n$; then

$$f(x_1, \cdots, x_n) \in F[x_1, \cdots, x_n]$$

is a *polynomial identity* for $A$ if $f \not\equiv 0$ and $f(a_1, \cdots, a_n) = 0$ for all $a_1 \in A$. Some of the recent investigations [2; 3] of polynomial identities have been concerned with those that are linear in each indeterminate, and for certain algebras all such polynomial identities are known.

In the following we obtain other information on polynomial identities by investigating those in a single indeterminate. Our results provide a generalization of the Fermat theorem when this is formulated as: $x^{p^n} - x$ is a polynomial identity for the field of $p^n$ elements. Other generalizations have been given [4] that determine the least common multiple of the orders of the nonsingular elements of a total matrix algebra over a finite field.

**2. An ideal of polynomial identities.** If $A$ is an algebra over $F$, and $x$ an indeterminate, let $\mathfrak{J}(A)$ be the set of all $f(x)$ in $F[x]$ such that $f(a) = 0$ for all $a \in A$. We then clearly have:

LEMMA 1. *$\mathfrak{J}(A)$ is a principal ideal in $F[x]$.*

THEOREM 1. *If $A$ is a total matrix algebra of order $m^2$ over $GF(p^n)$, then $\mathfrak{J}(A)$ is the principal ideal generated by $f(m, p^n, x)$, the monic least common multiple of all polynomials of degree $m$ in $GF(p^n)[x]$.*

*Proof.* $f(m, p^n, x) \in \mathfrak{J}(A)$ since it is divisible by the minimal polynomial of every element of $A$. If $g(x) \in \mathfrak{J}(A)$ then it is a multiple of $f(m, p^n, x)$, for if $h(x)$ is any monic polynomial of degree $m$ in $GF(p^n)[x]$ there exists $a \in A$ so that $h(x)$ is the minimal polynomial of $a$ over $GF(p^n)$ [5, p. 148].

To extend this result we use:

Received March 15, 1953.
*Pacific J. Math.* 4 (1954), 317-320