Pacific Journal of Mathematics

FERMAT'S THEOREM FOR ALGEBRAS

GORDON L. WALKER

Vol. 4, No. 2 June 1954

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 $a_i \in A$. 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 $\mathfrak{I}(A)$ 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. *$\mathfrak{I}(A)$ 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 $\mathfrak{I}(A)$ 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. $f(m, p^n, x) \in \mathfrak{I}(A)$ since it is divisible by the minimal polynomial of every element of A. If $g(x) \in \mathfrak{I}(A)$ 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

LEMMA 2. *If A is a subalgebra of B then $\mathfrak{I}(A) \supseteq \mathfrak{I}(B)$.*

LEMMA 3. *If A_1, A_2 are algebras over F then*

$$\mathfrak{I}(A_1 \oplus A_2) = \mathfrak{I}(A_1) \cap \mathfrak{I}(A_2).$$

Proof. Lemma 2 is trivial, and this implies

$$\mathfrak{I}(A_1 \oplus A_2) \subseteq \mathfrak{I}(A_1) \cap \mathfrak{I}(A_2).$$

If $a \in A_1 \oplus A_2$ then

$$a = a_1 + a_2,$$

where $a_1 a_2 = 0$ and $a_i \in A_i$, so that

$$a^k = a_1^k + a_2^k$$

for all integers k. Thus

$$f(a) = f(a_1) + f(a_2)$$

for all $f(x) \in F[x]$, and

$$\mathfrak{I}(A_1) \cap \mathfrak{I}(A_2) \subseteq \mathfrak{I}(A_1 \oplus A_2).$$

We now have:

THEOREM 2. *If $A = A_1 \oplus \cdots \oplus A_k$, where each A_i is a total matrix algebra of order m_i^2 over $GF(p^n)$, and*

$$m_1 \leq m_2 \leq \cdots \leq m_k,$$

then $\mathfrak{I}(A)$ is the principal ideal generated by $f(m_k, p^n, x)$.

3. A determination of $f(m, p^n, x)$. The following theorem with Theorem 1 becomes the Fermat theorem in case $m = 1$.

THEOREM 3. $f(m, p^n, x) = (x^{p^n} - x)(x^{p^{2n}} - x) \cdots (x^{p^{mn}} - x)$.

This follows by induction from:

LEMMA 4. $f(m, p^n, x) = (x^{p^{mn}} - x) f(m-1, p^n, x)$.

To show this we let $\mu[g(x), h(x)]$, where $g(x), h(x) \in GF(p^n)[x]$, denote the multiplicity (including zero) of $g(x)$ as a factor of $h(x)$; because the unique factorization property holds, we have only to show

$$(1) \quad \mu[g_k(x), f(m, p^n, x)] = \mu[g_k(x), x^{p^{mn}} - x] + \mu[g_k(x), f(m-1, p^n, x)]$$

for all irreducible monic polynomials $g_k(x)$ of degree $k \leqq m$ in $GF(p^n)[x]$. But

$$\mu[g_k(x), f(m, p^n, x)] \text{ is } \mu[g_k(x), f(m-1, p^n, x)]$$

when k does not divide m, and is $\mu[g_k(x), f(m-1, p^n, x)] + 1$ when k divides m. Thus (1) holds, since $x^{p^{mn}} - x$ is the product of all $g_k(x)$ such that k divides m [**1**, p. 17].

4. Further results concerning $\mathfrak{J}(A)$. The preceding results together with the structure theorem for semi-simple algebras imply:

THEOREM 4. *If A is a semi-simple algebra of characteristic* p, *and the simple components of A have orders $m_1^2, \cdots, m_k^2$ over their centers $GF(p^{n_1}), \cdots, GF(p^{n_k})$, respectively, then $\mathfrak{J}(A)$ is the principal ideal generated by the least common multiple of*

$$f(m_1, p^{n_1}, x), \cdots, f(m_k, p^{n_k}, x).$$

A further extension is provided by:

THEOREM 5. *If A is an algebra over F with radical N, if*

$$\mathfrak{J}(A - N) = (f), f \in F[x],$$

and if $\mathfrak{J}(N) = (x^r)$, that is, index $N = r$, *then*

$$(g_1) \supseteq \mathfrak{J}(A) \supseteq (g_2),$$

where g_1 is the least common multiple of x^r and $f(x)$, and $g_2 = [f(x)]^r$.

Proof. From $f(x) \in \mathfrak{J}(A - N)$ we deduce $f(a) \in N$ for every $a \in A$, so

$$\mathfrak{J}(A) \supseteq (g_2).$$

From Lemma 2 we have both $\mathfrak{J}(A - N)$ and $\mathfrak{J}(N)$ including $\mathfrak{J}(A)$, so their intersection (g_1) includes $\mathfrak{J}(A)$.

REMARK. The following example shows that the bounds on $\mathfrak{I}(A)$ in Theorem 5 cannot be improved without further hypothesis. If e_{ij} $(i, j = 1, 2)$ are matrix units, and $F = GF(2)$, let A_1 be the algebra with basis e_{11}, e_{12} over F, and let A_2 be the algebra with basis e_{11}, e_{12}, e_{22} over F. Both algebras have radicals of index 2, and $f(x) = x^2 - x$; but

$$\mathfrak{I}(A_1) = (g_1), \qquad \mathfrak{I}(A_2) = (g_2),$$

where

$$g_1 = x^3 - x^2, \; g_2 = x^4 - x^2 = (x^2 - x)^2,$$

so that $(g_1) \neq (g_2)$.

REFERENCES

1. L. E. Dickson, *Linear groups with an exposition of the Galois field theory*, Teubner, Leipzig, 1901.

2. I. Kaplansky, *Rings with a polynomial identity*, Bull. Amer. Math. Soc. **54** (1948), 575-580.

3. J. Levitzki, *A theorem on polynomial identities*, Proc. Amer. Math. Soc. **1** (1950), 334-341.

4. I. Niven, *Fermat's theorem for matrices*, Duke Math. J. **15** (1948), 823-826.

5. S. Perlis, *Theory of matrices*, Addison-Wesley, Cambridge, 1952.

PURDUE UNIVERSITY

PACIFIC JOURNAL OF MATHEMATICS

Mathematical papers intended for publication in the *Pacific Journal of Mathematics* should be typewritten (double spaced), and the author should keep a complete copy. Manuscripts may be sent to any of the editors. Manuscripts intended for the outgoing editors should be sent to their successors. All other communications to the editors should be addressed to the managing editor, E.G. Straus, at the University of California Los Angeles 24, California.

50 reprints of each article are furnished free of charge; additional copies may be obtained at cost in multiples of 50.

The *Pacific Journal of Mathematics* is published quarterly, in March, June, September, and December. The price per volume (4 numbers) is $12.00; single issues, $3.50; back numbers (Volumes 1, 2, 3) are available at $2.50 per copy. Special price to individual faculty members of supporting institutions and to individual members of the American Mathematical Society: $4.00 per volume; single issues, $1.25.

Subscriptions, orders for back numbers, and changes of address should be sent to the publishers, University of California Press, Berkeley 4, California.

Printed at Ann Arbor, Michigan. Entered as second class matter at the Post Office, Berkeley, California.

*To be succeeded in 1955, by H.L. Royden, Stanford University, Stanford, California.

**To be succeeded in 1955, by E.G. Straus, University of California, Los Angeles 24, Calif.

UNIVERSITY OF CALIFORNIA PRESS · BERKELEY AND LOS ANGELES

Pacific Journal of Mathematics
Vol. 4, No. 2 June, 1954