ON NAKAYAMA'S EXTENSION OF THE $x^{n(x)}$ THEOREMS

ALEX ROSENBERG AND DANIEL ZELINSKY

In [6] Nakayama proved that if A is a division ring with center Z such that every element a of A satisfies

$$f(a) = a^{n_1(a)}\alpha_1 + \cdots + a^{n_r(a)}\alpha_r \in Z \tag{1}$$

where the α_i are r fixed nonzero elements of Z, and $0 < n_1(a) < n_i(a)$ $(i = 2, \cdots, r)$, then $A = Z$. In [**3**, Theorem 11; **5**; **2**; **1**] specialized forms of (1) (e.g. $a^{n(a)} \in Z$, $a^{n(a)} - a \in Z$) are shown to imply commutativity at least for semi-simple rings. It is natural therefore to seek an extension of Nakayama's result to semi-simple rings. Since a semi-simple ring is a subdirect sum of primitive rings and (1) is preserved under homomorphism we first study primitive rings satisfying (1).

If A is such a ring it may be identified with a dense ring of linear transformations on a vector space $\mathfrak{M}$ over a division ring D. Since D is the ring of endomorphisms of $\mathfrak{M}$ that commute with A, Z is in D and in fact in the center of D. We may assume that there are at least two independent vectors x, y in $\mathfrak{M}$. If $\lambda \in D$ there is an element a in A such that $xa = 0$, $ya = y\lambda$. Now $ya^n = y\lambda^n$ so that if $f(a) \in Z$ is the relation of type (1) that a satisfies, we have $xf(a) = 0$, $yf(a) = yf(\lambda)$. Since $f(a) \in Z \subset D$ this makes $f(a) = 0$ so that $yf(\lambda) = 0$, $f(\lambda) = 0$, and by Nakayama's result $D = Z$. Thus the center of a primitive ring satisfying (1) is a field.

Moreover, we have proved that each element in this field satisfies a polynomial equation of the form $f(a) = 0$ with f as in (1). Let P be the prime subfield of Z and Q be the field obtained by adjoining to P a maximal, algebraically independent set from among $\alpha_1, \cdots, \alpha_r$. Assuming that Z is not absolutely algebraic[1] of prime characteristic, Lemmas 1 and 2 of [6] show that Z is purely inseparable over Q or $Z = Q$. In the former case $f(a)^{p^k} = 0$ is an equation with coefficients in the rational function field Q; thus in either case every nonzero rational function λ would satisfy an equation

$$\beta_1 + \beta_2\lambda^{n_2(\lambda)} + \cdots + \beta_r\lambda^{n_r(\lambda)} = 0$$

with $n_i(\lambda) \geqq 1$ and the β_i fixed polynomials. [If $Q = P =$ the rationals we take the β_i to be integers.] However the ring of polynomials in several variables [the ring of integers] is a unique factorization do-

Presented to the Society, June 20, 1953; received by the editors May 27, 1953.

[1] Algebraic over its prime subfield.

main and so the numerator of λ would have to divide β_1 for every λ in Q, which is impossible. Hence Z is an absolutely algebraic field of characteristic p.

Thus a primitive ring satisfying (1) is an algebraic algebra over an absolutely algebraic field of characteristic p; this automatically makes it an algebraic algebra over $GF(p)$. Conversely, every algebraic algebra over $GF(p)$ satisfies a very special form of (1). For if a is an element of A, there is a polynomial f over $GF(p)$ such that $f(a) = 0$. The splitting field of f is a finite field, so that for some $q = p^s$, each linear factor of f divides $x^q - x$. If m is a power of p larger than the multiplicity of each root of f, then f divides $x^{mq} - x^m$. Hence a satisfies $a^{mq} - a^m = 0$. We have

THEOREM 1. *A noncommutative primitive ring satisfies* (1) *if and only if it is an algebraic algebra over its center*[2] *and this center is an absolutely algebraic field of prime characteristic. In this case, the condition* (1) *implies* $a^{n(a)} - a^{m(a)} = 0$, $0 < n(a) < m(a)$.

Next, if A is a semi-simple ring satisfying (1) with α_1 in no primitive ideal, it is clear that A will be a subdirect sum of rings C and A_p, where C is a commutative semi-simple ring and each A_p is a subdirect sum of noncommutative primitive algebraic algebras over $GF(p)$. However, not every subdirect sum of this last form will satisfy (1): A complete direct sum of an infinite number of copies of the ring of 2×2 matrices over the algebraic closure of $GF(p)$ does not satisfy any condition of type (1). We can also see that (1) cannot always be replaced by $a^{n(a)} - a^{m(a)} = 0$ in such an A_p. To obtain an example, let Z_i be the algebraic closure of $GF(p)$, A_i the ring of all 2×2 matrices over Z_i, and A the local direct sum[3] of the A_i with respect to the Z_i. Then for each a in A, $a^{n(a)} - a^{m(a)}$ is in the center of A, but A is clearly not algebraic over any field. In general we do not know whether (1) can always be replaced by the condition $a^{n(a)} - a^{m(a)}$ in the center. However, if the $n_i(a)$ are bounded we can settle the question; in fact:

THEOREM 2. *Let A be a semi-simple ring satisfying* (1) *with α_1 in no primitive ideal and with bounded $n_i(a)$. Then A is a subdirect sum of a commutative ring and total matrix algebras with a bounded number of*

---

[2] We remark that Theorem 1 and its proof remain true verbatim if we replace the center of A throughout by the centroid of A—the ring of endomorphisms of the additive group of A which commute with the left and right multiplications [4, p. 236].

[3] Each element of A is an element of the Cartesian product of the A_i having its ith component in Z_i for all but a finite number of i's.

elements. Furthermore, A satisfies the condition $a^n - a^m \in Z$ with n and m fixed, unequal positive integers.

Proof. Let k be a bound for $n_i(a)$ and r be as in (1). We show that every noncommutative primitive image B of A has $\leqq l$ elements, where l is a function of k and r alone. By our previous arguments each element η of the center Y of B satisfies an equation $f(\eta) = 0$ with f as in (1). Since the degree of f is $\leqq k$ there are at most k^r such polynomials. Let g be their product; its degree is at most $s = k^{r+1}$, and every element of Y is a root of g. Hence Y is a field with at most s elements. Now B is a primitive algebraic algebra of degree $\leqq k$ over Y and so by [**3**, Theorems 5 and 8] it is a total matrix algebra of degree $\leqq k$ over Y. Thus B has at most $l = s^{k^2}$ elements.

Hence B is an algebraic algebra over $GF(p)$ of dimension $< l$. Therefore every element b of B satisfies a polynomial equation of degree $< l$ and with coefficients in $GF(p)$. The remarks immediately preceding Theorem 1 then show that there exist positive integers u, v depending only on l and p such that $b^u - b^v = 0$ for all b in B. If we write A as a subdirect sum of the rings C and A_p as before, each A_p will satisfy a polynomial identity $a^u - a^v = 0$. Since the noncommutative primitive summands are of bounded size, at most a finite number of distinct A_p's can occur. To complete the proof it suffices to choose positive, unequal integers m, n such that $x^n - x^m$ is divisible by each of the finite number of polynomials $x^u - x^v$.

References

1. I. N. Herstein, *A generalization of a theorem of Jacobson* III, Amer. J. Math. vol. 75 (1953) pp. 105–111.

2. M. Ikeda, *On a theorem of Kaplansky*, Osaka Math. J. vol. 4 (1952) pp. 235–240.

3. N. Jacobson, *Structure theory for algebraic algebras of bounded degree*, Ann. of Math. vol. 46 (1945) pp. 695–707.

4. N. Jacobson, *Structure theory of simple rings without finiteness assumptions*, Trans. Amer. Math. Soc. vol. 57 (1945) pp. 228–245.

5. I. Kaplansky, *A theorem on division rings*, Canadian Journal of Mathematics vol. 3 (1951) pp. 290–292.

6. T. Nakayama, *On the commutativity of certain division rings*, Canadian Journal of Mathematics vol. 5 (1953) pp. 242–244.

Northwestern University