PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 49, Number 1, May 1975

ENUMERATION RESULTS IN NILPOTENT ALGEBRAS

HELMUT STRADE

ABSTRACT. We enumerate the number of subalgebras for some classes of finite nilpotent algebras. These classes are: alternative algebras over $GF(q)$, noncommutative Jordan algebras over $GF(q)$, algebras with only zero squares over some Dedekind domain.

1. **Results.** Let D denote a Dedekind domain with a prime ideal P such that D/P is a finite field $GF(q)$. An algebra A over D is a unital D-module that is also a (not necessarily associative) ring, such that $\alpha(ab) = (\alpha a)b = a(\alpha b)$ for $\alpha \in D$ and $a, b \in A$. Now let A denote a nilpotent D-algebra such that the underlying D-module A^+ is a finitely-generated P-primary torsion module. Then A is finite with q^n elements. Let X be a subalgebra in A, and let $s_m(A/X)$ denote the total number of subalgebras of index q^m in A that contain X ($s_m(A/\{0\}) = s_m(A)$). Then the following holds [3]:

$$s_m(A/X) \equiv 1 \ (q).$$

The main tool to prove this is the following

Enumeration theorem [3]. *Under the above assumptions on A, D, P suppose that the ideal $\phi(A) = A^2 + PA$ has index $[A: \phi(A)] = q^k$. Let $\mathcal{C}$ denote a set of subsets of A such that each member of $\mathcal{C}$ lies in at least one maximal subalgebra of A. Let $n(B)$ denote the total number of members of $\mathcal{C}$ contained in a given subalgebra $B \supset \phi(A)$ and let*

$$n_r(\mathcal{C}) = \sum_{B \supset \phi(A); [A:B] = q^r} n(B).$$

Then the total number of members of $\mathcal{C}$ is

$$|\mathcal{C}| = \sum_{r=1}^{k} (-1)^{r-1} q^{r(r-1)} n_r(\mathcal{C}).$$

Received by the editors October 18, 1973.
AMS (MOS) subject classifications (1970). Primary 16A22, 17B30, 17C99, 17D05.

This theorem goes back to an enumeration principle for nilpotent groups due to P. Hall [1]. In that case a much better result can be proved: the total number of subgroups of index p^m of a finite nilpotent p-group, which is not cyclic is $\equiv 1 + p \ (p^2)$ (Kulakoff's theorem). In this note we prove a similar result for some classes of algebras. The result is false for the class of algebras described above since there are counterexamples even for associative rings. The main restriction concerns the Dedekind domain.

If all squares vanish in A we call A a zsq-algebra. Algebras generated by a single element are called power algebras. zsq-algebras which are power algebras are cyclic D-modules.

In this note we prove the following:

Theorem 1. *Let A be a nilpotent finite dimensional algebra over a finite field $GF(q)$. Then the following hold:*

(i) $s_1(A) = 1 + q + q^2 + \cdots + q^{k-1}$, $k = \dim A/A^2$;

(ii) *if* $m > 1$ *then* $s_m(A) \equiv 1 + q \ (q^2)$ *if*

(a) *A is alternative,* $m < \dim A - 1$, *or*

(b) *A is a noncommutative Jordan algebra,* $m < \dim A - 2$.

Theorem 2. *Let A be a nilpotent finite dimensional algebra over a finite field $GF(q)$. Then the total number of power algebras of dimension m of A is $\equiv 0 \ (q)$ if*

(a) *A is alternative,* $m > 2$ *or*

(b) *A is a noncommutative Jordan algebra,* $m > 3$.

This theorem, too, has an analogue for nilpotent p-groups.

Theorem 3. *Under the above assumptions about A, D, P suppose that A is a zsq-algebra and P is a principal ideal. Then $s_m(A) \equiv 1 + q \ (q^2)$ if A is not cyclic. Otherwise $s_m(A) = 1$.*

2. **Proofs.** We often use the following well-known fact about nilpotent algebras [3], [4]. A is generated by r elements if and only if $\dim A/\phi(A) \leq r$ holds, especially, A is a power algebra if and only if $\dim A/\phi(A) = 1$. In this case $\phi(A) = PA + A^2$ is the unique maximal subalgebra. Further simple facts about nilpotent algebras can also be found in [4].

First we treat a special case. Let A be a nilpotent noncommutative Jordan algebra over $GF(q)$ of dimension $n > 4$ or alternative of dimension $n > 3$. Moreover let there exist a maximal subalgebra B generated by a single element b. Since A is nilpotent, $A^2 \subset B$ and $\dim B = n - 1 > 3$ (resp. > 2) holds. A noncommutative Jordan algebra is power associative,

so B is associative in both cases. Thus

$$B = \left\{ \sum_{i=1}^{n-1} \alpha_i b^i, \ \alpha_i \in GF(q) \right\}, \qquad b^n = 0.$$

Lemma 1. *There exists* $a \in A \setminus B$ *such that*

(i) $A = B + GF(q)a$;

(ii) $aA, Aa \subset B^3$.

Proof. (1) Let A be a noncommutative Jordan algebra and $n > 4$. Choose $a' \in A \setminus B$. From $a'b \in A^2 \subset B$ we get $a'b = \alpha b + f(b)b$. A is nilpotent, so $\alpha = 0$ and $a = a' - f(b) \in A \setminus B$ fulfills (i). Moreover $ab = 0$. In a noncommutative Jordan algebra the following identities hold [5]:

$$(x^i y)x = x^i(yx), \qquad (yx^i)x = (yx)x^i, \qquad x^i(xy) = x(x^i y), \qquad i \in N.$$

If $b^i a = \sum_{j=2}^{n-1} \alpha_{ij} b^j$ it follows that

$$0 = b^i(ab) = (b^i a)b = \sum_{j=2}^{n-1} \alpha_{ij} b^{j+1}$$

and $\alpha_{ij} = 0$ if $j \neq n-1$. We have proved $Ba \subset B^{n-1}$. In the same manner we prove $aB \subset B^{n-1}$.

Let $a^2 - \alpha b - \beta b^2 \in B^3$. From the Jordan identity

$$(a + tb)((a + tb)^2(sa + b)) = (a + tb)^2((a + tb)(sa + b)), \qquad s, t \in GF(q),$$

follows

$$b^{n-1}(t^2 + \beta)\alpha_{3,n-1} - b^4(t^2 + \beta)\beta s - b^3(t^2 + 2\beta)\alpha s - b^2\alpha^2 s \equiv 0 \ (b^5).$$

So $\alpha = \beta = 0$ since b^2, b^3, b^4 are linearly independent.

(2) If A is alternative the proof is analogous. A is indeed associative since it is generated by 2 elements, and we only have to use other identities. Q.E.D.

Lemma 2. *There are exactly* q *maximal subalgebras which are power algebras. They are generated by elements* $b + ra$, $r \in GF(q)$.

Proof. Each maximal power algebra B' is generated by an element $ra + sb + bf(b)$. It contains $A^2 \supset B^2$ and therefore $ra + sb$. If $s = 0$, then by Lemma 1 $(ra + bf(b))^2 \in B^3$ holds. But then the codimension of B' in A is not 1, so we can assume $s = 1$. On the other hand, $b + ra$ generates a subalgebra B_r and the following hold:

(a) $(b + ra)^i \equiv b^i \ (B^{i+1})$ if $1 < i < n - 1$;

(b) if $n > 4$ then

$$(b + ra)^{n-1} = (b + ra)^{n-3}(b + ra)^2 = (b^{n-3} + b^{n-3}g(b))(b^2 + b^2h(b)) = b^{n-1};$$

(c) if $n = 4$ (then A is associative) then

$$(b + ra)^3 = b^3 + r(ba^2 + bab + ab^2) + r^2(a^2b + aba + ba^2) + r^3a^3 = b^3.$$

This implies $B_r^2 = B^2$. Since B is a power algebra, $\dim B_r = \dim B_r^2 + 1 = \dim B^2 + 1 = \dim A - 1$ holds. So B_r is maximal; $B_r = B'$. Q.E.D.

We now turn to the general case. The number of subalgebras $B \supset A^2 + PA$ of index q^r in A is denoted by $\phi_{k,r}$, where k is the index of $A^2 + PA$ in A. $\phi_{k,r}$ is the number of vector spaces of codimension $k - r$ in a k-dimensional vector space. Therefore $\phi_{k,1} = \sum_{r=0}^{k-1} q^r$ and $\phi_{k,2} \equiv 1 \ (q^2)$ if $k > 2$.

Proof of Theorem 1. (i) The result about $s_1(A)$ is well known.

(ii) If A is a power algebra generated by an element a, then A^2 is the unique maximal subalgebra, which is not a power algebra, since a^2, a^3 are linearly independent. Then $s_m(A) = S_{m-1}(A^2)$. So we come down to the case that A is not a power algebra. In that case there are subalgebras of codimension 2 containing A^2. We apply the enumeration theorem and use induction on m. Let $\mathcal{C}$ be the class of subalgebras of codimension m.

$$m = 2\colon\ s_2(A) \equiv |\mathcal{C}| \equiv \sum_{\text{Codim } B=1;\, A^2 \subset B} n_1(B) - q \cdot \sum_{\text{Codim } B=2;\, A^2 \subset B} n_2(B) \ (q^2).$$

Let A contain a power algebra B of codimension 1. From $m = 2$ follows $\dim A > 3$ (resp. $\dim A > 4$). By Lemma 2 there are exactly q power algebras of codimension 1.

$$s_2(A) \equiv \sum_{\text{Codim } B=1;\, A^2 \subset B} s_1(B) - q \cdot \sum_{\text{Codim } B=2;\, A^2 \subset B} s_0(B)$$

$$\equiv (1 + q)(\phi_{k,1} - q) + q - q\phi_{k,2} \equiv 1 + q \ (q^2).$$

If A contains no power algebra of codimension 1 then, by (i), $s_2(A) \equiv (1 + q)\phi_{k,1} - q\phi_{k,2} \equiv 1 + q \ (q^2)$.

$m > 2$: By induction follows

$$s_m(A) \equiv \sum_{\text{Codim } B=1;\, A^2 \subset B} s_{m-1}(B) - q \cdot \sum_{\text{Codim } B=2;\, A^2 \subset B} s_{m-2}(B).$$

$$\equiv (1 + q)\phi_{k,1} - q\phi_{k,2} \equiv 1 + q \ (q^2).$$

Proof of Theorem 2. Let $\mathcal{C}$ be the class of power algebras of codimension m. The case $m = 1$ is proved by Lemma 2. Now we apply the enumeration theorem and use induction on m.

Proof of Theorem 3. If A is cyclic, that is $A = Du$, then Pu is the unique subalgebra of index q. But Pu is cyclic; $Pu = D(pu)$ since P is principal.

Now assume that A is not cyclic. The result about $s_1(A)$ is well known. Suppose $m \geq 2$ and let $\mathcal{C}$ be the class of subalgebras of index q^m. Then

$$s_m(A) \equiv \sum_{[A:B]=q;\, A^2 \subset B} n_1(B) - q \cdot \sum_{[A:B]=q^2;\, A^2 \subset B} n_2(B)$$

$$\equiv \sum_{[A:B]=q;\, A^2 \subset B} s_{m-1}(B) - q \cdot \sum_{[A:B]=q^2;\, A^2 \subset B} s_{m-2}(B) \quad (q^2).$$

If all subalgebras of index q are not cyclic the proof is done by hypothesis on $m - 1$. So suppose that A contains a maximal subalgebra Dv, that is, $A = Du + Dv$, $A^2 + PA \subset Dv$. If $pu = sv$, $s \notin P$, then A is cyclic, generated by v. Therefore $s = s'p$ holds. So P annihilates $u' = u - s'v$. The subalgebras $D(v + iu')$, $i \in D/P$, are exactly the maximal cyclical ones. There are q of that kind. By hypothesis on $m - 1$ we conclude

$$s_m(A) \equiv (1 + q)(\phi_{k,1} - q) + q - q\phi_{k,2} \equiv 1 + q \quad (q^2).$$

REFERENCES

1. P. Hall, *A contribution to the theory of groups of prime power order*, Proc. London Math. Soc. (2) 36 (1934), 29–95.

2. J. Knopfmacher, *Arithmetical properties of finite rings and algebras, and analytic number theory*, J. Reine Angew. Math. 252 (1972), 16–43. MR 47 #1769.

3. J. Knopfmacher and G. E. Burger, *Submodules, subalgebras and ideals in finite modules or nilpotent algebras over Dedekind domains*, J. London Math. Soc. (2) 5 (1972), 681–690. MR 47 #1852.

4. R. L. Kruse and D. T. Price, *Nilpotent rings*, Gordon and Breach, New York, 1969. MR 42 #1858.

5. H. Braun and M. Koecher, *Jordan Algebren*, Die Grundlehren der math. Wissenschaften in Einzeldarstellungen mit besonderer Berücksichtigung der Anwendungsgebiete, Band 128, Springer-Verlag, Berlin and New York, 1966. MR 34 #4310.

UNIVERSITÄT HAMBURG, 2 HAMBURG 13, WEST GERMANY