ARITHMETICAL PROPERTIES OF FINITE RINGS AND ALGEBRAS, AND ANALYTIC NUMBER THEORY

BY JOHN KNOPFMACHER

Communicated by Serge Lang, September 10, 1969

The object of this note is to state certain theorems, whose proofs together with related results will appear elsewhere. The theorems are mainly concerned with asymptotic enumeration of the isomorphism classes of finite rings or finite-dimensional algebras lying in various naturally-defined categories. Two results concern enumeration of subalgebras or subrings in a given algebra or ring. All the rings and algebras are associative, but need not necessarily have units.

1. Semisimple rings and algebras.

THEOREM 1. *Let $s(n)$ denote either the total number of nonisomorphic semisimple rings of order p^n, or the total number of nonisomorphic n-dimensional semisimple algebras over the Galois field $GF(p^r)$, p a prime. Then*

$$s(n) = \exp([\tfrac{1}{3}\pi^2 + o(1)]n^{1/2}) \quad \textit{as } n \rightarrow \infty.$$

THEOREM 2. *Let $s_{\mathfrak{R}}(n)$ denote the total number of nonisomorphic n-dimensional semisimple algebras over a real closed field $\mathfrak{R}$. Then as $n \rightarrow \infty$*

$$s_{\mathfrak{R}}(n) = \exp([b + o(1)]n^{1/3})$$

where $b = \frac{3}{4}(3+2^{1/2})^{2/3}\pi^{1/3}[\zeta(3/2)]^{2/3}$.

The proofs of these theorems, and the next one, make use of the *zeta functions* or *generating functions* of the relevant categories. In the present cases, those functions can be calculated and this is helpful in obtaining asymptotic estimates, even though usually it provides no direct asymptotic information. In particular, Theorems 1 and 2 depend on a *Tauberian theorem* of Hardy and Ramanujan [2].

The proof of Theorem 2 gives the following

COROLLARY. *Let $\pi_{\mathfrak{R}}(x)$ denote the total number of nonisomorphic*

AMS Subject Classifications. Primary 1694, 1644, 1632; Secondary 1041, 1048, 1050, 1690.

Key Words and Phrases. Finite ring, finite-dimensional algebra, Galois field, semisimple, nilpotent, asymptotic enumeration, zeta function, generating function, Tauberian theorem, abstract prime number theorems, cohomology of algebras, P. Hall's enumeration principle, Frattini subalgebra, Frattini subring.

simple algebras of dimension at most x over the real closed field $\mathcal{R}$. Then

$$\pi_{\mathcal{R}}(x) \sim \tfrac{1}{2}(3 + 2^{1/2})x^{1/2} \quad \text{as } x \to \infty.$$

We mention that, with the aid of well-known results of Hardy and Ramanujan [3], asymptotic estimates of a more precise type than above may be obtained for the categories of

(i) commutative semisimple finite p-rings,

(ii) commutative semisimple finite-dimensional algebras over some Galois field, and

(iii) semisimple finite-dimensional algebras over an algebraically closed field Λ.

Next, let $S(n)$ denote the total number of nonisomorphic semisimple finite rings of order n. Then $S(n)$ is a multiplicative arithmetical function, whose values fluctuate from 1 on square-free integers to those indicated in Theorem 1. However, 'on average' it is well behaved:

THEOREM 3. *As $x \to \infty$,*

$$\sum_{n \leq x} S(n) = \alpha_1 x + \alpha_2 x^{1/2} + O(x^{1/3}\log^2 x)$$

where $\alpha_1 = \prod_{rm^2>1} \zeta(rm^2) = 2.498 \cdots$, $\alpha_2 = \zeta(\frac{1}{2}) \prod_{rm^2>2} \zeta(\frac{1}{2}rm^2)$.

Here $\zeta(z)$ denotes the *Riemann* zeta function. The proof of this theorem employs techniques of Kendall and Rankin [5], who obtained a similar result for finite abelian groups; in particular, these techniques depend on a theorem of Landau. The main theorem of [5] also provides the 'average value' of the total number $S_c(n)$ of nonisomorphic commutative semisimple rings of order n. That result and Theorem 3 lead, via certain *abstract prime number theorems* (see Wegmann [6]), to the following

COROLLARY. (i) *Let $\pi_S(x)$ denote the total number of nonisomorphic simple finite rings of order at most x. Then*

$$\pi_S(x) \sim x/\log x \quad \text{as } x \to \infty.$$

(ii) *Let $\pi_c(x)$ denote either the total number of nonisomorphic Galois fields of order at most x, or the total number of nonisomorphic indecomposable abelian groups of order at most x. Then $\pi_c(x) \sim x/\log x$ as $x \to \infty$.*

Apart from a well-defined mean-value, the function $S(n)$ also possesses an asymptotic distribution function

$$\chi(x) = \lim_{N \to \infty} (1/N)\, \mathrm{card}\{n \leq N : S(n) \leq x\},$$

and this function is discrete. Further, for any given $\delta > 0$,

$$S(n) = o(n^{\delta}) \quad \text{as } n \to \infty.$$

Similarly for $S_c(n)$; cf. [5].

2. **Nilpotent algebras and rings.** Now let $N(n)$ denote the total number of nonisomorphic nilpotent n-dimensional algebras over the Galois field $GF(q)$, q a prime-power, and let $N_c(n)$ denote the corresponding number for commutative nilpotent algebras.

THEOREM 4. *The numbers $N(n)$, $N_c(n)$ satisfy the inequalities*

$$q^{[4/27+o(1)]n^3} \leqq N(n) \leqq q^{n^3/3}$$

and

$$q^{[2/27+o(1)]n^3} \leqq N_c(n) \leqq q^{n^3/6}$$

as $n \to \infty$, the upper bounds being true for all n.

These inequalities are analogous to ones of Higman [4] for finite p-groups, but the present proofs depend largely on a quantitative application of the *cohomology theory of algebras*. The exponents in the upper bounds neglect $O(n^2)$ terms, but in any case the dominant terms are probably not best possible. Theorem 4 yields the lower bounds of the next theorem, but the upper bounds there now depend on some preliminary, and apparently new, propositions concerning nilpotent finite rings.

THEOREM 5. *Let $\hat{N}(n)$ denote the total number of nonisomorphic nilpotent finite rings of order p^n, p a prime, and let $\hat{N}_c(n)$ denote the corresponding number for commutative nilpotent rings. Then*

$$p^{[4/27+o(1)]n^3} \leqq \hat{N}(n) \leqq p^{n^3/3}$$

and

$$p^{[2/27+o(1)]n^3} \leqq \hat{N}_c(n) \leqq p^{[1/6+o(1)]n^3}$$

as $n \to \infty$, the first upper bound being true for all n.

These results show that nilpotent algebras and rings form a substantial proportion out of all finite algebras and rings, while the semisimple ones have asymptotic density zero.

3. **Subalgebras and subrings.** The final results to be stated here concern enumeration of the subalgebras in a given finite-dimensional nilpotent algebra A over the Galois field $GF(q)$, q a prime-power, or of the subrings in a finite nilpotent ring R of order p^n, p a prime.

THEOREM 6. *Let $s_m(A)$ denote the total number of subalgebras of codimension m in the given algebra A above, and let* $k=\operatorname{codim} A^2$ *in A. Then*:

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

(ii) *if* $0<m\leqq k$ *then* $s_m(A)=\psi(k,m)+aq^{k-m+1}$ *for some* $a\geqq 0$, *where*

$$\psi(k,m)=\frac{(q^k-1)(q^k-q)\cdots(q^k-q^{m-1})}{(q^m-1)(q^m-q)\cdots(q^m-q^{m-1})};$$

(iii) *in general,* $s_m(A)\equiv 1 \pmod q$.

These results, which are analogous to well-known ones about finite p-groups, may be obtained from an analogue for finite nilpotent algebras of *P. Hall's enumeration principle for finite p-groups* [1]. They make use, however, of some preliminary propositions about finite-dimensional nilpotent algebras over arbitrary fields. The last theorem is obtained in a similar way, and also depends on certain apparently new preliminary results. The concept of the *Frattini subalgebra or subring* is useful for the preliminary propositions referred to in each case.

THEOREM 7. *Let R be a finite nilpotent ring of order p^n, p a prime. Let $s_m(R)$ denote the total number of subrings of order p^{n-m} in R, and suppose that R^2+pR has order p^{n-k} in R. Then*:

(i) $s_1(R)=1+p+p^2+\cdots+p^{k-1}$;

(ii) *if* $0<m\leqq k$ *then* $s_m(R)=\phi(k,m)+ap^{k-m+1}$ *for some* $a\geqq 0$, *where*

$$\phi(k,m)=\frac{(p^k-1)(p^k-p)\cdots(p^k-p^{m-1})}{(p^m-1)(p^m-p)\cdots(p^m-p^{m-1})};$$

(iii) *in general,* $s_m(R)\equiv 1 \pmod p$.

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. G. H. Hardy and S. Ramanujan, *Asymptotic formulae concerning the distribution of integers of various types*, Proc. London Math. Soc. (2) **16** (1917), 112–132.

3. ———, *Asymptotic formulae in combinatory analysis*, Proc. London Math. Soc. (2) **17** (1918), 75–115.

4. G. Higman, *Enumerating p-groups*. I: *Inequalities*, Proc. London Math. Soc. (3) **10** (1960), 24–30. MR **22** #4779.

5. D. G. Kendall and R. A. Rankin, *On the number of Abelian groups of a given order*, Quart. J. Math. Oxford Ser. **18** (1947), 197–208. MR **9**, 226.

6. H. Wegmann, *Beiträge zur Zahlentheorie auf freien Halbgruppen*. I, II, J. Reine Angew. Math. **221** (1965), 20–43; 150–159. MR **32** #4097; MR **32** #4098.

UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG, SOUTH AFRICA