BULLETIN OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 78, Number 2, March 1972

FINITE MODULES AND ALGEBRAS OVER DEDEKIND DOMAINS AND ANALYTIC NUMBER THEORY

BY JOHN KNOPFMACHER

Communicated by H. Bass, August 10, 1971

This note states some results concerning asymptotic enumeration of the isomorphism classes of finite modules or algebras (of various types) over a Dedekind domain D. Proofs will be published elsewhere.

1. **Finite modules over a ring of algebraic integers.** Firstly, let D be the ring of integers in a finite-dimensional algebraic number field K. If M is a finitely-generated torsion module over D, then standard structure theory [**8**], [**9**] and the fact that D/P is finite for every prime ideal P implies that M is *finite in cardinal*. Further, if $\mathscr{F}(D)$ denotes the category of all such modules M and $a(n) = a_D(n)$ denotes the *total number of isomorphism classes of modules of order n in* $\mathscr{F}(D)$, then $a(n)$ is finite and "multiplicative."

Now recall that, if $N_D(x)$ denotes the total number of ideals of norm at most x in D, then $N_D(x) = \lambda_K x + O(x^\eta)$ where λ_K is an explicit positive constant depending on K and $\eta = 1 - 2/(1 + [K:Q])$ [**13**].

(1.1) THEOREM. *The function* $a(n)$ *has mean value* $\lambda_K \prod_{r=2}^{\infty} \zeta_K(r)$. *More precisely,* $\sum_{n \leqq x} a(n) = [\lambda_K \prod_{r=2}^{\infty} \zeta_K(r)]x + O(x^{1/2})$ *where* $\zeta_K(s)$ *is the Dedekind zeta function.*

When D is the ring Z of *rational integers*, $\mathscr{F}(D)$ becomes the category $\mathscr{A}$ of all ordinary *finite abelian groups*, and the theorem was first proved for this case by Erdös and Szekeres [**4**].

(1.2) COROLLARY. *Let* $\pi_{\mathscr{F}(D)}(x)$ *denote the total number of indecomposable D-modules of order at most x in* $\mathscr{F}(D)$. *Then*

$$\pi_{\mathscr{F}(D)}(x) \sim x/\log x \quad \text{as } x \to \infty.$$

Theorems 1.1 and 2.1 follow from slightly more general results about certain categories. Corollaries 1.2 and 2.2 follow with the aid of an *abstract prime number theorem*, as discussed in [**15**]; for $D = Z$, see [**10**], [**11**].

Although it has a finite mean value, $a(n)$ can be very large on prime powers: Consider a rational prime p, and define $C = C(D, p)$ by $C = \alpha_1^{-1} + \cdots + \alpha_m^{-1}$ where $(p) = P_1 \cdots P_m$ is the decomposition of (p) into prime ideals P_i in D, and P_i has norm p^{α_i}.

AMS 1970 *subject classifications.* Primary 13C10, 13E10, 13F05, 16A22, 16A40, 16A44, 16A46, 17B99; Secondary 10H25, 10H40, 10J20, 12A70, 12A75.

Key words and phrases. Module, algebra, algebraic number field, algebraic integer, Dedekind zeta function, abstract prime number theorem, partition function, semisimple algebra, nilpotent algebra, Lie algebra, quasi-finite field, Frattini subalgebra.

(1.3) THEOREM. *As* $x \to \infty$, $\sum_{n \leqq x} a(p^n) = \exp\{[\pi(2C/3)^{1/2} + o(1)]x^{1/2}\}$. *If* $\alpha_1, \ldots, \alpha_m$ *have g.c.d.* 1 *then, as* $n \to \infty$,

$$a(p^n) \sim An^{-(m+3)/4} \exp[\pi(2Cn/3)^{1/2}]$$

where $A = (\alpha_1 \cdots \alpha_m)^{1/2} 2^{-(m+2)/2} (C/6)^{(m+1)/4}$.

When $D = \boldsymbol{Z}$, this theorem follows from the Hardy-Ramanujan asymptotic formula for the partition function $p(n)$. In general, Theorems 1.3, 2.3, and 2.4 below depend on results of Brigham [**3**], Ingham [**7**], and Auluck and Haselgrove [**1**], which are also basically founded on work of Hardy and Ramanujan [**5**].

2. **Semisimple finite algebras over a ring of algebraic integers.** If D is as above, let $\mathscr{S}(D)$ denote the category of all *semisimple D-algebras* whose underlying D-modules lie in $\mathscr{F}(D)$, and let $\mathscr{S}_c(D)$ denote the subcategory of all *commutative* algebras in $\mathscr{S}(D)$. With the aid of standard structure theory [**8**], one finds that the *total number* $S(n) = S_D(n)$ *of isomorphism classes of algebras of cardinal n in* $\mathscr{S}(D)$ is finite, and the corresponding number $S_c(n)$ for $\mathscr{S}_c(D)$ coincides with $a(n)$ above. Hence *the asymptotic results of* §1 *apply directly* to $\mathscr{S}_c(D)$ also. $S(n)$ is also "multiplicative."

(2.1) THEOREM. *The function* $S(n)$ *has mean value* $\lambda_K \prod_{rm^2 > 1} \zeta_K(rm^2)$. *More precisely,* $\sum_{n \leqq x} S(n) = [\lambda_K \prod_{rm^2>1} \zeta_K(rm^2)]x + O(x^{1/2})$.

(2.2) COROLLARY. *Let* $\pi_{\mathscr{S}(D)}(x)$ *denote the total number of simple D-algebras of cardinal at most x. Then* $\pi_{\mathscr{S}(D)}(x) \sim x/\log x$ *as* $x \to \infty$.

Remainder terms can be given for Corollaries 1.2 and 2.2.

(2.3) THEOREM. *Let p be a rational prime and* $C = C(D, p)$ *as before. Then* $\sum_{n \leqq x} S(p^n) = \exp\{[\frac{1}{3}\pi^2 C^{1/2} + o(1)]x^{1/2}\}$ *as* $x \to \infty$. *If at least two integers* α_i *are coprime, then, as* $n \to \infty$,

$$S(p^n) = \exp\{[\tfrac{1}{3}\pi^2 C^{1/2} + o(1)]n^{1/2}\}.$$

When $D = \boldsymbol{Z}$, $\mathscr{S}(D)$ becomes the category of all ordinary *semisimple finite rings*, and for this case the above results were given in [**10**], [**11**]. A similar result to Theorem 2.3, using previous techniques and results of Ax [**2**] and Serre [**14**], is

(2.4) THEOREM. *Let F denote a quasi-finite field, and let* $s(n)$ *denote the total number of isomorphism classes of semisimple n-dimensional algebras over F, and* $s_c(n)$ *denote the corresponding number for the semisimple commutative n-dimensional algebras over F. Then as* $n \to \infty$,

$$s(n) = \exp\{[\tfrac{1}{3}\pi^2 + o(1)]n^{1/2}\} \text{ while } s_c(n) = p(n) \sim (4n\sqrt{3})^{-1} \exp[\pi(2n/3)^{1/2}].$$

For finite F, see [**10**], [**11**].

3. **Finite algebras over a principal ideal domain.** In this section, D denotes an arbitrary principal ideal domain with a prime ideal P such that D/P is finite. For example, D may be a special ring of algebraic integers or a special ring of integral functions of one variable over a finite field. If $D/P \cong \mathrm{GF}(q)$, and M is a finitely-generated torsion module over D such that the order ideal of each element is some power of P, then M is finite with q^n elements, for some n. If M is the underlying D-module of a D-algebra A, we shall call A a *P-primary* algebra.

Let $A(n)$, $A_c(n)$ and $A_L(n)$ denote the *total number of isomorphism classes of P-primary algebras of cardinal* q^n that are respectively *associative, commutative and associative*, or *Lie algebras*. Let $N(n)$, $N_c(n)$ and $N_L(n)$ denote the corresponding numbers for *nilpotent* algebras of these respective types.

(3.1) THEOREM. *As* $n \to \infty$, $q^{[4/27+O(n^{-1})]n^3} \leqq N(n) \leqq q^{[1/3+O(n^{-1})]n^3}$ *while* $A(n) \leqq q^{[1+O(n^{-1})]n^3}$.

(3.2) THEOREM. *As* $n \to \infty$, $q^{[2/27+O(n^{-1})]n^3} \leqq N_c(n), N_L(n) \leqq q^{[1/6+O(n^{-1})]n^3}$ *while* $A_c(n), A_L(n) \leqq q^{[1/2+O(n^{-1})]n^3}$.

The proofs of these results follow a pattern of Higman's for finite p-groups [**6**], and make use of the *Frattini subalgebra.* In fact, the lower bounds are obtainable when D is a general Dedekind domain (with D/P finite) and it seems reasonable to *conjecture* that they provide correct asymptotic estimates even for such a general Dedekind domain. (With regard to Theorem 3.1 *when* D is $\mathrm{GF}(q)$ or $\boldsymbol{Z}$, compare [**12**, Chapter 5]; however, we remark that the proofs of 5.2.4 and 5.2.5 in [**12**] do not seem to cover the following rings in all respects: consider the additive group $\boldsymbol{Z}/(27)$ together with (i) usual multiplication, (ii) multiplication $\bar{r}\cdot\bar{s} = \overline{3rs}$ where $\bar{a}$ denotes the coset of $a \in \boldsymbol{Z}$. With regard to Theorem 3.2 *when* D is $\mathrm{GF}(q)$ or $\boldsymbol{Z}$, we understand that R. L. Kruse has similar results for Lie algebras (unpublished); compare also [**10**], [**11**] in the commutative case.)

ADDED IN PROOF. The results of §3 hold over any Dedekind domain D with D/P finite. For such D and P, generalizations of Theorems 6, 7 of [**10**] to finite nilpotent P-primary D-algebras and to finite P-primary bimodules over nilpotent associative D-algebras will appear shortly in a joint paper by the author and G. E. Burger.

REFERENCES

1. F. C. Auluck and C. B. Haselgrove, *On Ingham's Tauberian theorem for partitions*, Proc. Cambridge Philos. Soc. **48** (1952), 566–570. MR **14**, 138.

2. J. Ax, *Elementary theory of finite fields*, Ann. of Math. (2) **88** (1968), 239–271. MR **37** #5187.

3. N. A. Brigham, *A general asymptotic formula for partition functions*, Proc. Amer. Math. Soc. **1** (1950), 181–191. MR **11**, 582.

4. P. Erdös and G. Szekeres, *Über die Anzahl der Abelschen Gruppen gegebener Ordnung und über ein verwandtes zahlentheoretisches Problem*, Acta Sci. Math. Szeged **7** (1935), 95–102.

5. 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.

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

7. A. E. Ingham, *A Tauberian theorem for partitions*, Ann. of Math. (2) **42** (1941), 1075–1090. MR **3**, 166.

8. N. Jacobson, *Theory of rings*, Math. Surveys, no. 2, Amer. Math. Soc., Providence, R.I., 1943. MR **5**, 31.

9. I. Kaplansky, *Modules over Dedekind rings and valuation rings*, Trans. Amer. Math. Soc. **72** (1952), 327–340. MR **13**, 719.

10. J. Knopfmacher, *Arithmetical properties of finite rings and algebras, and analytic number theory*, Bull. Amer. Math. Soc. **76** (1970), 830–833.

11. ———, *Arithmetical properties of finite rings and algebras, and analytic number theory*, J. Reine Angew. Math. (to appear).

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

13. E. Landau, *Einführung in die elementare und analytische Theorie der algebraischen Zahlen und der Ideale*, Chelsea, New York, 1949. MR **11**, 85.

14. J.-P. Serre, *Corps locaux*, Actualités Sci. Indust., no. 1296, Hermann, Paris, 1962. MR **27** #133.

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

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF THE WITWATERSRAND, JOHANNESBURG, SOUTH AFRICA