Advanced Studies in Pure Mathematics 17, 1989
Algebraic Number Theory — in honor of K. Iwasawa
pp. 309-330

Fine Estimates for the Growth of e_n in Z_p^d-Extensions

P. Monsky

For Professor Kenkichi Iwasawa on his seventieth birthday

Introduction

Fix a prime p and a positive integer d. Suppose that $k=k_0\subset k_1\subset\cdots$ is a tower of number fields and that k_n is Galois over k with Galois group a product of d copies of Z/p^n. Let L be the union of the k_n; it is a "Z_p^d-extension of k". We denote the exponent to which p appears in the class number of k_n by $e_n(L/k)$, or more briefly by e_n.

When $d=1$ we have Iwasawa's celebrated formula: $e_n=\mu p^n+\lambda n+\nu$, $n\gg 0$, where μ and λ are integers attached to the Iwasawa module of L/k. Suppose that $d>1$. Then in place of the Iwasawa module we have the Greenberg-Iwasawa module, X, a finitely generated torsion module over $\Lambda=Z_p[\![X_1,\cdots,X_d]\!]$, and progress towards proving analogues of Iwasawa's formula has been made by studying such modules. (See for example [1], [2], [3], [4]). The analysis started with [2], in which Cuoco treated the case $d=2$, attaching integers m_0 and l_0 to X and showing that $e_n=m_0p^{2n}+l_0np^n+O(p^n)$. This result was generalized to arbitrary d in [1]. In that paper integers $m_0=m_0(F)$ and $l_0=l_0(F)$ were attached to a non-zero $F\in\Lambda$ as follows. Let $\bar{\Lambda}=\Lambda/p\Lambda$ and $\bar{E}$ be the closed multiplicative subgroup of $\bar{\Lambda}$ generated by the $1+X_j$; it is a free rank d Z_p-module. Write $F=p^sG$ where the image, $\bar{G}$, of G in $\bar{\Lambda}$ is non-zero and write $\bar{G}$ as the product of irreducible G_i. Then $m_0(F)=s$ and $l_0(F)$ is the number of indices i for which (G_i) is the image of (X_1) under an automorphism of $\bar{\Lambda}$ transforming $\bar{E}$ to itself. The fundamental Theorem I of [1] states the following. Let $F\in\Lambda$ be the "characteristic power series" of the Greenberg-Iwasawa Λ-module, X, attached to L/k; set $m_0=m_0(F)$ and $l_0=l_0(F)$. Then $e_n(L/k)=(m_0p^n+l_0n+O(1))p^{(d-1)n}$.

Our goal in this paper is to refine the above Theorem I by proving that $e_n=(m_0p^n+l_0n+\alpha^*)p^{(d-1)n}+O(np^{(d-2)n})$ for some real α^*. There is no easy description of α^* and in particular we do not know if it is always rational. We shall show however that it is rational if either $d=2$ or if X

Received July 26, 1987.

contains no pseudo-null submodule other than (0).

Remark. Our refinement gives an almost complete answer to the question of the growth of e_n when $d=2$. For if m_0, l_0 and α^* are not all zero we have the excellent estimate $e_n = m_0 p^{2n} + l_0 n p^n + \alpha^* p^n + O(n)$. Suppose on the other hand that $m_0 = l_0 = \alpha^* = 0$. Then it follows easily from [6] that X is finite over Z_p. ($e_n(L/k) = O(n)$; consequently the p-rank of the ideal class group of k_n is $O(n)$ and Theorem 1.9 of [6] tells us that X/pX is a finite group). We conclude from Theorem II of [1] that e_n is an eventually linear function of n in this case.

We now give an outline of the paper. Until the very end we are concerned only with Λ-modules and eschew all number theory. Throughout, $\Lambda = Z_p[\![X_1, \cdots, X_d]\!]$ and $E \subset \Lambda$ is the closed multiplicative group generated by the $1+X_j$— it is a free rank d Z_p-module. In section 1 we fix an integer $r \geq 0$ and a finite subset S of $E - E^p$, and use r and S to define a sequence of ideals, J_n, of Λ. Fix a finitely generated Λ-module M such that the M/J_nM are finite groups and denote the length of $\mathrm{Tor}_i^\Lambda(M, \Lambda/J_n)$ by $l_{i,n}$. We show that the Serre intersection number $E_n(M) = \Sigma(-1)^i l_{i,n}$ of M and Λ/J_n may be expressed as an "Iwasawa sum" attached to the characteristic power series, F, of M. Such sums have been evaluated in [5], but for the convenience of the reader we calculate these sums by a simpler method. Our conclusion is that $E_n(M) = (m_0 p^n + l_0 n + \nu^*) p^{(d-1)n} + O(np^{(d-2)n})$, where $m_0 = m_0(F)$, $l_0 = l_0(F)$ and ν^* is rational.

In section 2 we bound the horizontal growth of the $\mathrm{Tor}_i^\Lambda(M, \Lambda/J_n)$ for a fixed $i \geq 1$. Let $r_{i,n}$ be the minimal number of generators of this finitely generated Z_p-module. We show that for each $i \geq 2$ the estimate $r_{i,n} = O(p^{(d-2)n})$ holds. Furthermore if M^* denotes the largest submodule of M annihilated both by a power of p and by some $h \notin (p)$ then $r_{1,n}(M/M^*) = O(p^{(d-2)n})$. We combine these bounds with bounds for the vertical growth of the $\mathrm{Tor}_i^\Lambda(M, \Lambda/J_n)$ and conclude that $l(M/J_nM)$, the length of M/J_nM, is equal to $E_n(M) + l(M^*/J_nM^*) + O(np^{(d-2)n})$. The deep results of [3] and [4] allow us to estimate $l(M^*/J_nM^*)$, and we wind up with a good estimate for $l(M/J_nM)$.

In section 3 we consider a related but more complicated problem. To each $\sigma \in S$ we attach a Λ-submodule M_σ of M, and we use the M_σ to construct a sequence of submodules A_n' of M. Then $G_n = M/A_n'$ is finite over Z_p; we denote its Z_p-rank by $r(G_n)$ and the length of its torsion subgroup by $e(G_n)$. Assuming that $r(G_n)$ does not grow too rapidly with n we obtain (with an error term that is $O(np^{(d-2)n})$) an expression for $e(G_n)$ as a sum of three contributions. The first contribution is an

Iwasawa sum attached to F, the second is connected to M^*, and the third is a fixed integer multiple of $p^{(d-1)n}$. The results of sections 1 and 2 then tell us that $e(G_n)=(m_0p^n+l_0n+\alpha^*)p^{(d-1)n}+O(np^{(d-2)n})$ for some real α^*. We conclude the paper by using the methods of [1] to deduce from this algebraic result a corresponding result for the growth of $e_n(L/k)$.

To summarize, Theorem I of [1] was based on the crude estimate $e(G_n)=$ (Iwasawa sum)$+O(p^{(d-1)n})$. Our homological argument, expressing $e(G_n)$ as the sum of three contributions, together with the estimate for the M^*-contribution coming from [3] and [4] is what underlies the improvements of this paper.

§ 1. Calculation of $E_n(M)$ via Iwasawa sums

Unless otherwise indicated d is an integer ≥ 0, Λ is the d-variable power series ring over the p-adic integers and E is the closed multiplicative subgroup of Λ generated by the $1+X_j$. E is a free rank d Z_p-module and we write the action of Z_p on E exponentially. We fix an integer $r\geq 0$ and a finite subset S of $E-E^p$.

Definition 1.1. I_n is the ideal of Λ generated by the $\sigma-1$, $\sigma\in E^{p^n}$. (Or alternatively by the $(1+X_j)^{p^n}-1$). For $n\geq r$, J_n is the ideal of Λ generated by I_n together with the $(\sigma^{p^n}-1)/(\sigma^{p^r}-1)$, $\sigma\in S$.

Remark. When $d=0$, $J_n=(0)$. When $d=1$, set $\sigma=1+X_1$. Then J_n is principal, generated by $\sigma^{p^n}-1$ when S is empty and by $(\sigma^{p^n}-1)/(\sigma^{p^r}-1)$ otherwise. When $d>1$ the situation is more complicated. J_n need not be generated by a regular sequence and Λ/J_n may have p-torsion.

Definition 1.2 W is the group of p^{th}-power roots of unity in a fixed algebraic closure of Q_p.

Definition 1.3. If ε is in W with $\varepsilon^{p^r}=1$ and $\sigma=\prod(1+X_i)^{l_i}$ is an element of S then $T_{\sigma,\varepsilon}$ is the subset of W^d consisting of all $\zeta=(\zeta_1,\cdots,\zeta_d)$ with $\prod\zeta_i^{l_i}=\varepsilon$. Set $X=\bigcup_{\sigma,\varepsilon}T_{\sigma,\varepsilon}$ and $U=W^d-X$.

Definition 1.4. R_n is the discrete valuation ring obtained from Z_p by adjoining the ε in W with $\varepsilon^{p^n}=1$. If $\zeta\in W^d$ with $\zeta^{p^n}=1$ then Q_ζ is the prime ideal of $R_n[\![X_1,\cdots,X_d]\!]$ generated by the $X_i-(\zeta_i-1)$.

Remark. If ζ is as above then each ζ_j-1 is in the maximal ideal of R_n. So it makes sense to speak of $F(\zeta-1)=F(\zeta_1-1,\cdots,\zeta_d-1)$. Note that Q_ζ is the kernel of the evaluation homomorphism $F\to F(\zeta-1)$.

We shall frequently abuse language by writing I_n and J_n for the ideals generated by I_n and J_n in $R_n[\![X_1,\cdots,X_d]\!]$.

Lemma 1.5. *In $R_n[\![X_1, \cdots, X_d]\!]$, I_n is the intersection of the ideals Q_ζ, $\zeta \in W^d$, $\zeta^{p^n}=1$.*

Proof. Consider the map $R_n[\![X_1, \cdots, X_d]\!]/I_n \to \prod_\zeta (R_n[\![X_1, \cdots, X_d]\!]/Q_\zeta)$. Using the fact that the image of $\prod_i((1+X_i)^{p^n}-1)/X_i-(\zeta_i-1))$ is nonzero in precisely one factor we find that the cokernel is annihilated by a power of p. Since $R_n[\![X_1, \cdots, X_d]\!]/I_n$ can be generated as R_n-module by p^{dn} elements while $\prod_\zeta (R_n[\![X_1, \cdots, X_d]\!]/Q_\zeta)$ has rank p^{dn} over R_n, we conclude that $R_n[\![X_1, \cdots, X_d]\!]/I_n$ is free of rank p^{dn} over R_n. At the same time we find that the above map is injective, i.e. that $I_n = \cap Q_\zeta$.

Lemma 1.6. *In $R[\![X_1, \cdots, X_d]\!]$ the prime ideals containing J_n other than the maximal ideal are just the Q_ζ, $\zeta \in U$, $\zeta^{p^n}=1$. For each such ζ, J_n generates the maximal ideal in the localization of $R_n[\![X_1, \cdots, X_d]\!]$ at Q_ζ.*

Proof. Since $J_n \supset I_n$, Lemma 1.5 shows that the only primes other than m that can contain J_n are the Q_ζ, $\zeta \in W^d$, $\zeta^{p^n}=1$. But such a Q_ζ contains J_n if and only if the image of each $(\sigma^{p^n}-1)/(\sigma^{p^r}-1)$, $\sigma \in S$, under the evaluation map $F \to F(\zeta-1)$ is zero. Since the evaluation map sends $\sigma = \prod(1+X_i)^{l_i}$ to $\prod \zeta_i^{l_i}$ it annihilates each $(\sigma^{p^n}-1)/(\sigma^{p^r}-1)$ if and only if each $(\prod \zeta_i^{l_i})^{p^r} \neq 1$; that is to say if and only if ζ is not in any $T_{\sigma,\varepsilon}$. Finally for any such ζ, Lemma 1.5 shows that I_n generates the maximal ideal in the localization of $R_n[\![X_1, \cdots, X_d]\!]$ at Q_ζ; the same is necessarily true of the larger ideal J_n.

Remark. Take a filtration of $R_n[\![X_1, \cdots, X_d]\!]/J_n$ whose quotients are cyclic with prime annihilator. It follows from Lemma 1.6 that each $R_n[\![X_1, \cdots, X_d]\!]/Q_\zeta$, $\zeta \in U$, $\zeta^{p^n}=1$, appears once as a quotient and that the remaining quotients are of finite length.

Definition 1.7. Fix a finitely generated torsion Λ-module M such that the groups M/J_nM are finite. Let $l_{i,n}$ be the length of $\mathrm{Tor}_i^\Lambda(M, \Lambda/J_n)$ and $E_n(M) = \sum(-)^i l_{i,n}$ be the "Serre intersection number" of M and Λ/J_n. (Note that the $l_{i,n}$ are finite and vanish for $i > d+1$).

Using the exact sequence of Tor we see that E_n is an additive function of M in exact sequences.

Lemma 1.8. *Let $F \in \Lambda$ be the characteristic power series of the Λ-module M. Then $E_n(M) = E_n(\Lambda/F)$.*

Proof. Take a filtration of M with quotients Λ/P_i, with P_i prime. Then $E_n(M) = \sum E_n(\Lambda/P_i)$. Furthermore, $E_n(\Lambda/F) = \sum E_n(\Lambda/P_i)$, the sum extending over those indices i for which P_i is principal. So it suffices to

show that $E_n(\Lambda/P_i)=0$ whenever P_i is non-principal. Now for such an i the sum of the Krull dimensions of Λ/P_i and Λ/J_n is $\leq(d-1)+1<$ Krull dimension Λ. The lemma on page 139 of [8] shows that the Serre intersection number of Λ/P_i and Λ/J_n vanishes for each such P_i.

Since $\mathrm{Tor}_i^{\Lambda}(\Lambda/F, \Lambda/J_n)=(0)$ for $i>1$, Lemma 1.8 gives:

Lemma 1.9. *$E_n(M)=l(\mathrm{cok}\ F)-l(\ker F)$ where F denotes the multiplication by F map $\Lambda/J_n\to\Lambda/J_n$.*

If we continue to let l denote length as Λ-module then Lemma 1.9 tells us that $E_n(M)=(\phi(p^n))^{-1}(l(\mathrm{cok}\ F)-l(\ker F))$ where F now denotes the multiplication by F map on $R_n[\![X_1, \cdots, X_d]\!]/J_n$. The remark after Lemma 1.6 shows that $E_n(M)$ is the sum of local factors $(\phi(p^n))^{-1}(l(\mathrm{cok}\ F)-l(\ker F))$, where F denotes the multiplication by F map on $R[\![X_1, \cdots, X_d]\!]/Q_\zeta$ and ζ runs over all $\zeta\in U$ with $\zeta^{p^n}=1$.

Theorem 1.10. *Let $U(n)$ consists of all $\zeta\in U$ with $\zeta^{p^n}=1$, and let* ord *be the order function attached to the p-adic valuation on $Q_p[W]$, normalized so that* ord $p=1$. *Then if $\zeta\in U$, $F(\zeta-1)\neq 0$. Furthermore $E_n(M)$ is the "Iwasawa sum" $\sum_{\zeta\in U(n)}$ ord $F(\zeta-1)$.*

Proof. $R_n[\![X_1, \cdots, X_d]\!]/Q_\zeta$ identifies with R_n, and under this identification the multiplication by F map corresponds to multiplication by $F(\zeta-1)$. Since the cokernel of this map is finite, $F(\zeta-1)\neq 0$. The local contribution to $E_n(M)$ coming from ζ is then $(\phi(p^n))^{-1}l(R_n/F(\zeta-1))$ and this is precisely ord $F(\zeta-1)$.

The explicit evaluation of Iwasawa sums was carried out in [5]; for the convenience of the reader we recall (and simplify) a portion of that article. There is a Noetherian topology on W^d in which the irreducible closed sets are the sets defined by $d-s$ equations $\phi_j(\zeta)=\varepsilon_j$, where the ϕ_j are part of a basis of the free rank d Z_p-module $\mathrm{Hom}(W^d, W)$ and the ε_j are in W. Such a set is called a "Z_p-flat" of dimension s.

Definition 1.11. If $\varepsilon\in W$, $o(\varepsilon)$ is the smallest integer n such that $\varepsilon^{p^n}=1$. Suppose that $d>0$ and let m be an integer ≥ 0. Then Γ_m is the subset of W^d consisting of all $(\zeta_1, \cdots, \zeta_d)$ satisfying the conditions $o(\zeta_1)\geq m$, $o(\zeta_2)\geq o(\zeta_1)+m$, $\cdots$, $o(\zeta_d)\geq o(\zeta_{d-1})+m$.

More generally suppose that $A=(\phi_1, \cdots, \phi_d)$ is an ordered basis of $\mathrm{Hom}(W^d, W)$. We define $\Gamma(A, m)$ to be the set of ζ satisfying the conditions $o(\phi_1(\zeta))\geq m$, $o(\phi_2(\zeta))\geq o(\phi_1(\zeta))+m$, $\cdots$. The following fundamental compactness theorem was proved in section 1 of [5]. Suppose that for each ordered basis A of $\mathrm{Hom}(W^d, W)$ an integer $m_A\geq 0$ is given. Then

W^d is covered by finitely many of the $\Gamma(A, m_A)$ together with a proper closed subset of W^d. An immediate consequence of this is:

Lemma 1.12. *Let Y be a subset of W^d. Suppose that for each invertible $T \in \mathrm{Hom}(W^d, W^d)$ there exists an integer m such that $T(Y) \cap \Gamma_m$ is empty. Then Y is contained in a proper closed subset of W^d.*

Lemma 1.13. *Suppose $F \in R_j[\![X_1, \cdots, X_d]\!]$ for some j and that $F \neq 0$. Let $Y = \{\zeta \in W^d : F(\zeta - 1) = 0\}$. Then Y is contained in a proper closed subset of W^d.*

Proof. We may assume $d > 0$. Of all the monomials $G = a \cdot \prod X_j^{c_j}$ appearing in F choose the one for which ord a is as small as possible; in case of a tie choose that G for which $(c_1, \cdots, c_d)$ comes first in lexicographic order. Choose $m > 0$ so large that $\phi(p^m) > \phi(p^t) \cdot \sum c_i$ and $p^m > \sum c_i$. Suppose that $\zeta \in \Gamma_m$ and that H is a monomial other than G appearing in F. An easy calculation shows that ord $H(\zeta - 1) >$ ord $G(\zeta - 1)$. Thus ord $F(\zeta - 1) =$ ord $G(\zeta - 1)$, $F(\zeta - 1) \neq 0$, and $Y \cap \Gamma_m$ is empty. Suppose more generally that T is an invertible element of $\mathrm{Hom}(W^d, W^d)$. Then there exists an $F' \neq 0$ in $R_j[\![X_1, \cdots, X_d]\!]$ such that $F'(\zeta - 1) = F(T^{-1}(\zeta) - 1)$ for all ζ in W^d. Clearly $F'(\zeta - 1) = 0$ if and only if $\zeta \in T(Y)$. The argument given above, applied to F', shows that $T(Y) \cap \Gamma_m$ is empty for some m and we invoke Lemma 1.12.

Theorem 1.14. *Let M be a finitely generated torsion Λ-module. Then it is possible to choose r and S so that if the J_n are as in Definition 1.1 then the groups M/J_nM are finite.*

Proof. Choose $F \neq 0$ annihilating M and let $Y = \{\zeta \in W^d : F(\zeta - 1) = 0\}$. If $\sigma \in E - E^p$ is $\prod (1 + X_i)^{l_i}$ and $\varepsilon \in W$ then the subset of W^d defined by $\sigma(\zeta - 1) = \varepsilon$ is just the $d-1$ dimensional Z_p-flat $\prod \zeta_i^{l_i} = \varepsilon$, and every $d-1$ dimensional Z_p-flat in W^d arises from some σ and ε. It follows from Lemma 1.13 that there are finitely many $\sigma_i \in E - E^p$ and $\varepsilon_i \in W$ such that Y is contained in the union of the Z_p-flats $\sigma_i(\zeta - 1) = \varepsilon_i$. Now choose r so that each $\varepsilon_i^{p^r} = 1$ and let S consist of the σ_i. Then, in the notation of Definition 1.3, $F(\zeta - 1) \neq 0$ whenever $\zeta \in U = W^d - \bigcup_{\sigma,\varepsilon} T_{\sigma,\varepsilon}$. Now $R_n[\![X_1, \cdots, X_d]\!]/J_n$ admits a filtration with quotients that are either of finite length or of the form $R_n[\![X_1, \cdots, X_d]\!]/Q_\zeta$ with $\zeta \in U$. Since $F(\zeta - 1) \neq 0$, multiplication by F has cokernel and kernel of finite length on each quotient of the filtration, and hence on $R_n[\![X_1, \cdots, X_d]\!]/J_n$ and on Λ/J_n. Thus $\Lambda/(J_n, F)$ is finite. Since (J_n, F) annihilates M/J_nM the theorem follows.

The proof of the following result (being entirely analogous to that of Lemma 1.13) is left to the reader. We shall use the result to simplify the evaluation of Iwasawa sums carried out in [5].

Lemma 1.15. *Suppose $G \in R_j[\![X_1, \cdots, X_d]\!]$ for some j, and that there is a co-efficient of G that is a unit in R_j. Let Y consist of all $\zeta \in W^d$ for which either $G(\zeta-1)=0$, $G(\zeta^p-1)=0$ or $\operatorname{ord} G(\zeta^p-1) \neq p \operatorname{ord} G(\zeta-1)$. Then Y is contained in a proper closed subset of W^d.*

Definition 1.16. $\mathscr{S}_d$ is the Q-vector space of functions spanned by the p^{ax}, $0 \leq a \leq d$, and the xp^{ax}, $0 \leq a \leq d-1$. $\mathscr{S}_d^*$ is the Q-vector space spanned by the p^{ax} and the xp^{ax}, $0 \leq a \leq d-1$.

Note that $\mathscr{S}_d \supset \mathscr{S}_d^* \supset \mathscr{S}_{d-1}$. Furthermore if $f(x) \in \mathscr{S}_d^*$ then $f(x+1) - p^{d-1}f(x)$ is in $\mathscr{S}_{d-1}$. Indeed $f \to f(x+1) - p^{d-1}f(x)$ maps $\mathscr{S}_d^*$ onto $\mathscr{S}_{d-1}$ with kernel consisting of rational multiples of $p^{(d-1)x}$.

Definition 1.17. If $U \subset W^d$, $U(n)$ consists of all $\zeta \in U$ with $\zeta^{p^n}=1$. Suppose that $F \in R_j[\![X_1, \cdots, X_d]\!]$ for some j, and that U is a subset of W^d such that $F(\zeta-1) \neq 0$ for each $\zeta \in U$. The "Iwasawa sum", $\sum(F, U, n)$, is $\sum_{\zeta \in U(n)} \operatorname{ord} F(\zeta-1)$. Let $g \in \mathscr{S}_d$. We shall say that $\sum(F, U, n)$ is "eventually equal to g" if $\sum(F, U, n) = g(n)$ for $n \gg 0$. Furthermore by the co-efficient of p^{an} (or np^{an}) in $\sum(F, U, n)$ we mean the co-efficient of p^{ax} (or xp^{ax}) in g.

Lemma 1.18. Let Y be a closed subset of W^d, $Y \neq W^d$. Then there are integers c_i such that the cardinality of $Y(n)$ is $\sum_0^{d-1} c_i p^{in}$ for $n \gg 0$.

Proof. Suppose first that Y is irreducible. We may assume without loss of generality that it is defined by $\zeta_i = \varepsilon_i$ $(1 \leq i \leq d-s)$; then the cardinality of $Y(n)$ is p^{sn} for large n. Suppose now that Y is the union of two smaller closed subsets Y_1 and Y_2. By Noetherian induction we may assume the result holds for Y_1, Y_2 and $Y_1 \cap Y_2$; it then evidently holds for Y.

Theorem 1.19. *Suppose that $F \in R_j[\![X_1, \cdots, X_d]\!]$ and that U is an open subset of W^d such that $F(\zeta-1) \neq 0$ for each $\zeta \in U$. Then $\sum(F, U, n)$ is eventually equal to some $f \in \mathscr{S}_d$.*

Proof. We argue by induction on d, the case $d=0$ being trivial. Suppose $d>0$. We make the following observation. Suppose that V and V' are non-empty open subsets of W^d such that $F(\zeta-1) \neq 0$ for each ζ in V and each ζ in V'. Then $\sum(F, V, n) - \sum(F, V', n)$ is eventually equal to an element of $\mathscr{S}_{d-1}$. It suffices to establish the observation

when $V \supset V'$, and this amounts to showing that $\sum(F, \mathscr{Z} \cap V, n)$ is eventually equal to an element of $\mathscr{S}_{d-1}$ where $\mathscr{Z} = W^d - V'$. We shall show that this in fact is true of an arbitrary closed $\mathscr{Z} \neq W^d$ in W^d, arguing by Noetherian induction on $\mathscr{Z}$. Suppose first that $\mathscr{Z}$ is irreducible. We may assume without loss of generality that it is defined by $\zeta_i = \varepsilon_i$, $s+1 \leq i \leq d$ where $s \leq d-1$. Let F^* be the s-variable power series obtained from F by substituting $\varepsilon_i - 1$ for X_i whenever $i > s$; note that F^* has co-efficients in some R_k. Projection on the first s co-ordinates identifies $\mathscr{Z}$ with W^s and $\mathscr{Z} \cap V$ with an open subset V^* of W^s. Then for n large, $\sum(F, \mathscr{Z} \cap V, n) = \sum(F^*, V^*, n)$— by the induction hypothesis it is eventually equal to an element of $\mathscr{S}_s$. But $\mathscr{S}_s \subset \mathscr{S}_{d-1}$. Finally if $\mathscr{Z}$ is a union of two smaller closed subsets we argue as in the proof of Lemma 1.18.

To prove the theorem we may assume U is non-empty. Then $F \neq 0$ and we write $F = \alpha G$ where $\alpha \in R_j$ and some co-efficient of G is a unit in R_j. Lemma 1.18 shows that there are integers c_i such that $\sum(F, U, n) - \sum(G, U, n) = (\operatorname{ord} \alpha)(p^{dn} - \sum_0^{d-1} c_i p^{in})$ for $n \gg 0$. So it suffices to show that $\sum(G, U, n)$ is eventually equal to an element of $\mathscr{S}_d^*$. Now let Y be the set of Lemma 1.15; choose finitely many $\sigma_i \in E - E^p$ and $\varepsilon_i \in W$ such that Y is contained in the union of the Z_p-flats $\sigma_i(\zeta - 1) = \varepsilon_i$. Choose r so that each $\varepsilon_i^{p^r} = 1$. Set $V^* = \{\zeta \in W^d;\ \text{no}\,(\sigma_i(\zeta-1))^{p^r} = 1\}$ and $U^* = \{\zeta \in W^d : \text{no}\,(\sigma_i(\zeta-1))^{p^{r+1}} = 1\}$. Then for each $\zeta \in U^*$, $G(\zeta - 1) \neq 0$, $G(\zeta^p - 1) \neq 0$ and $\operatorname{ord} G(\zeta^p - 1) = p \operatorname{ord} G(\zeta - 1)$. We wish to show that $\sum(G, U, n)$ is eventually equal to an element of $\mathscr{S}_d^*$; in light of the observation it suffices to prove this result for $\sum(G, U^*, n)$.

Now $\zeta \to \zeta^p$ maps W^d onto itself with fibers of cardinality p^d, and the complete inverse image of V^* is U^*. Thus $\zeta \to \zeta^p$ maps $U^*(n+1)$ onto $V^*(n)$ with each fiber of cardinality p^d. Now

$$\sum(G, U^*, n+1) = \sum_{\zeta \in U^*(n+1)} p^{-1} \operatorname{ord} G(\zeta^p - 1).$$

It follows that $\sum(G, U^*, n+1) = p^{d-1} \sum(G, V^*, n)$. The observation now shows that there is an $h \in \mathscr{S}_{d-1}$ such that $\sum(G, U^*, n+1) - p^{d-1} \sum(G, U^*, n) = h(n)$ for all $n \geq$ some fixed N. Choose g in $\mathscr{S}_d^*$ such that $g(x+1) - p^{d-1} g(x) = h(x)$. Modifying g by a rational multiple of $p^{(d-1)x}$ we may also assume that $g(N) = \sum(G, U^*, N)$. Then $g(n) = \sum(G, U^*, n)$ for all $n \geq N$, completing the proof.

Theorem 1.20. *Suppose that $F \neq 0$ is in $Z_p[\![X_1, \cdots, X_d]\!]$, $d \geq 1$, and that U is a non-empty open subset of W^d such that $F(\zeta - 1) \neq 0$ for each $\zeta \in U$. Then the co-efficients of p^{dn} and $np^{(d-1)n}$ in $\Sigma(F, U, n)$ are the non-negative integers $m_0(F)$ and $l_0(F)$ described in the second paragraph of the introduction.*

Proof. The observation made in the course of the proof of Theorem 1.19 shows that these co-efficients are independent of the choice of U. Now $F=p^{m_0}G$ where $m_0=m_0(F)$ and the image, $\bar{G}$, of G in $\Lambda/p\Lambda$ is non-zero. Then $\sum(F, U, n)=m_0(p^{dn}-\sum_0^{d-1} c_i p^{in})+\sum(G, U, n)$ for $n\gg 0$. Since the co-efficient of p^{dn} in $\sum(G, U, n)$ is zero, (see the proof of Theorem 1.19), the co-efficient of p^{dn} in $\sum(F, U, n)$ is m_0. At the same time we see that $np^{(d-1)n}$ has the same co-efficient in $\sum(F, U, n)$ that it does in $\sum(G, U, n)$.

To evaluate this co-efficient we take σ_i, r, U^* and V^* as in the proof of Theorem 1.19. We may assume that no two σ_i generate the same Z_p-submodule of E; at the same time we may assume that if $\sigma \in E-E^p$ with $\overline{\sigma-1}$ dividing $\bar{G}$ in $\bar{\Lambda}$ then σ generates the same Z_p-submodule of E as does one of the σ_i. Let S be the set consisting of the σ_i and define $T_{\sigma,\varepsilon}$, $\sigma \in S$, $\varepsilon \in W$ as in definition 1.3. By our hypotheses the $T_{\sigma,\varepsilon}$ are distinct Z_p-flats. Furthermore, $V^*=W^d-\cup T_{\sigma,\varepsilon}$, $(\sigma \in S, \varepsilon^{p^r}=1)$, while $U^*=W^d-\cup T_{\sigma,\varepsilon}$ $(\sigma \in S, \varepsilon^{p^{r+1}}=1)$. For $\sigma \in S$ let l_σ be the exponent to which $\overline{\sigma-1}$ appears in the factorization of $\bar{G}$. Then $l_0(F)=l_0(G)=\sum l_\sigma$ and we are reduced to showing that the co-efficient of $np^{(d-1)n}$ in $\sum(G, U^*, n)$ is $\sum l_\sigma$.

The proof of Theorem 1.19 shows that

$$\sum(G, U^*, n+1)-p^{d-1}\sum(G, U^*, n)=p^{d-1}\sum(G, V^*-U^*, n).$$

It follows easily that the co-efficient of $np^{(d-1)n}$ in $\sum(G, U^*, n)$ is equal to the co-efficient of $p^{(d-1)n}$ in $\sum(G, V^*-U^*, n)$. Now $V^*-U^*=\mathscr{Z}\cap V^*$ where $\mathscr{Z}$ is the union of the $T_{\sigma,\lambda}(\sigma \in S, o(\lambda)=r+1)$. Since these $T_{\sigma,\lambda}$ are distinct the co-efficient of $p^{(d-1)n}$ in $\sum(G, \mathscr{Z}\cap V^*, n)$ is just the sum of the co-efficients of $p^{(d-1)n}$ in the various $\sum(G, T_{\sigma,\lambda}\cap V^*, n)$, $(\sigma \in S, o(\lambda)=r+1)$. So if we can show that the contribution from each such pair (σ, λ) is $(\phi(p^{r+1}))^{-1}$. l_σ we'll be done.

We may assume without loss of generality that r is large and that $\sigma=1+X_d$, so that $T_{\sigma,\lambda}$ consists of all $\zeta \in W^d$ with last co-ordinate λ. Set $G'=G(X_1, \cdots, X_{d-1}, \lambda-1)$ and let V' be the image of $T_{\sigma,\lambda}\cap V^*$ under the projection map $(\zeta_1, \cdots, \zeta_d)\to(\zeta_1, \cdots, \zeta_{d-1})$. Then the co-efficient of $p^{(d-1)n}$ in $\sum(G, T_{\sigma,\lambda}\cap V^*, n)$ is equal to the co-efficient of $p^{(d-1)n}$ in $\sum(G', V', n)$. Now V' is a non-empty open subset of W^{d-1}. Furthermore using the fact that $r+1=o(\lambda)$ is large we see easily that $G=G(X_1, \cdots, X_{d-1}, \lambda-1)=(\lambda-1)^a\cdot H$, where a is the exponent to which X_d appears in the factorization of $\bar{G}$, and some co-efficient of H is a unit in R_{r+1}. It follows that the co-efficient of $p^{(d-1)n}$ in $\sum(G', V', n)$ is $\operatorname{ord}((\lambda-1)^a)=l_{1+X_d}\cdot(\phi(p^{r+1}))^{-1}$, establishing the theorem.

Theorem 1.21. *Suppose $d \geq 2$ and let M be a finitely generated torsion Λ-module such that the groups M/J_nM are finite. Let F be the characteristic power series of M, $m_0 = m_0(F)$ and $l_0 = l_0(F)$. Then there is a rational ν^* such that $E_n(M) = (m_0 p^n + l_0 n + \nu^*) p^{(d-1)n} + O(np^{(d-2)n})$.*

Proof. By Theorem 1.10 there is a non-empty open subset U of W^d such that $E_n(M) = \Sigma(F, U, n)$. Now apply Theorems 1.19 and 1.20.

§ 2. Estimates for $l(M/J_nM)$

Unless otherwise indicated we assume for the rest of the paper that no two elements of S generate the same Z_p-submodule of E, and that $d \geq 2$. By the p-rank of a finitely generated Z_p-module G we mean the minimal number of generators of G over Z_p. (This is not to be confused with the Z_p-rank which is the dimension of $G \otimes_{Z_p} Q_p$ over Q_p).

Definition 2.1. Let M be a finitely generated Λ-module. $r_{i,n}(M)$ is the p-rank of $\mathrm{Tor}_i^{\Lambda}(M, \Lambda/J_n)$.

In particular $r_{1,n}(\Lambda/p)$ is just the Z/p-dimension of the p-torsion subgroup of Λ/J_n. In order to bound $r_{i,n}(M)$ for $i \geq 1$ and arbitrary M we first bound $r_{1,n}(\Lambda/p)$.

Lemma 2.2. *Fix an integer $r \geq 0$ and elements $\sigma_1, \cdots, \sigma_s$ and τ of E, not in E^p. Let $\bar{I}_n$ be the image of I_n in $\bar{\Lambda} = \Lambda/p$, and $\bar{J}_n^*$ be the ideal of $\bar{\Lambda}$ generated by $\bar{I}_n$ and the $(\overline{\sigma_i - 1})^{p^n - p^r}$. Suppose that the Z_p-submodule of E generated by τ is not equal to the submodule generated by any σ_i. Then the cokernel of the multiplication by $(\overline{\tau - 1})^{p^r}$ map $\bar{J}_n^*/\bar{I}_n \to \bar{J}_n^*/\bar{I}_n$ has Z/p-dimension that is $O(p^{(d-2)n})$, and the same is true of the kernel.*

Proof. We shall prove the result for the cokernel—note that cokernel and kernel have the same dimension. Set $\bar{\mathcal{O}} = \bar{\Lambda}/((\overline{\tau - 1})^{p^r}, \prod (\overline{\sigma_i - 1})^{p^r})$. Our hypotheses tell us that each $\bar{\Lambda}/(\overline{\tau - 1}, \overline{\sigma_i - 1})$ has Krull dimension $\leq d-2$; the same is therefore true of $\bar{\mathcal{O}}$. Now the cokernel of our map is an $\bar{\mathcal{O}}$-module that is annihilated by $\bar{I}_n$ and can be generated by s elements. Thus its Z/p-dimension is $\leq s \cdot \dim(\bar{\mathcal{O}}/\bar{I}_n\bar{\mathcal{O}})$. Now $\bar{I}_n = (X_1^{p^n}, \cdots, X_d^{p^n}) \supset (X_1, \cdots, X_d)^{dp^n}$. The theory of the Hilbert polynomial then tells us that the Z/p-dimension of $\bar{\mathcal{O}}/\bar{I}_n\bar{\mathcal{O}}$ is $O(p^{(d-2)n})$.

Lemma 2.3. *Let $\bar{I}_n$ and $\bar{J}_n$ be the images of I_n and J_n in $\bar{\Lambda}$. Then the Z/p-dimension of $\bar{J}_n/\bar{I}_n$ is $|S| \cdot p^r \cdot p^{(d-1)n} + O(p^{(d-2)n})$ where $|S|$ is the cardinality of S.*

Proof. We argue by induction on $|S|$. We may assume that $S = \{\sigma_1, \cdots, \sigma_s, \tau\}$; let $S^* = \{\sigma_1, \cdots, \sigma_s\}$ and J_n^* be the ideal generated by I_n and

the $(\sigma_i^{p^n}-1)/(\sigma_i^{p^r}-1)$. It will suffice to show that the Z/p-dimension of $\bar{J}_n/\bar{J}_n^*$ is $p^r \cdot p^{(d-1)n}+O(p^{(d-2)n})$. Consider the multiplication by $(\overline{\tau-1})^{p^r}$ map $\bar{\Lambda}/\bar{I}_n \to \bar{\Lambda}/\bar{I}_n$. It is easily seen that the kernel of this map is generated by $(\overline{\tau-1})^{p^n-p^r}$ and has Z/p-dimension equal to $p^r \cdot p^{(d-1)n}$.

Let Q_n'', Q_n and Q_n' be the kernels of the multiplication by $(\overline{\tau-1})^{p^r}$ map on $\bar{J}_n^*/I_n$, $\bar{\Lambda}/\bar{I}_n$ and $\bar{\Lambda}/\bar{J}_n^*$, and let C_n'', C_n and C_n' be the corresponding cokernels. Then the exact sequence $(0)\to \bar{J}_n^*/\bar{I}_n \to \bar{\Lambda}/\bar{I}_n \to \bar{\Lambda}/\bar{J}_n^* \to (0)$ gives rise to an exact sequence $(0)\to Q_n'' \to Q_n \to Q_n' \to C_n'' \to C_n \to C_n' \to (0)$. It follows from Lemma 2.2 that the kernel and cokernel of $Q_n \to Q_n'$ have Z/p-dimensions that are $O(p^{(d-2)n})$. The remark at the end of the last paragraph then tells us that the Z/p-dimension of the image of Q_n in Q_n' is $p^r \cdot p^{(d-1)n}+O(p^{(d-2)n})$, and that this image identifies with $((\overline{\tau-1})^{p^n-p^r}, \bar{J}_n^*)/\bar{J}_n^*$ — that is to say with $\bar{J}_n/\bar{J}_n^*$.

Theorem 2.4.

(a) *The Z_p-rank of J_n/I_n is $|S|\cdot p^r \cdot p^{(d-1)n}+O(p^{(d-2)n})$.*

(b) *$r_{1,n}(\Lambda/p)$ is $O(p^{(d-2)n})$.*

Proof. The Z_p-rank of Λ/J_n is equal to the R_n-rank of $R_n[\![X_1, \cdots, X_d]\!]/J_n$. The remark after Lemma 1.6 shows that this is the cardinality of $U(n)$ where $U=W^d-X$, and X is the union of the $T_{\sigma,\varepsilon}$, $\sigma \in S$, $\varepsilon^{p^r}=1$. Thus the Z_p-rank of J_n/I_n is the cardinality of $X(n)$. Since the elements of S generate distinct Z_p-submodules of E, the $T_{\sigma,\varepsilon}$ are distinct $d-1$ dimensional Z_p-flats and there are precisely $|S|\cdot p^r$ of them. The proof of Lemma 1.18 shows that $T_{\sigma,\varepsilon}(n)$ has cardinality $p^{(d-1)n}$ for $n \gg 0$; (a) follows easily. To prove (b) note that we have just shown that the Z_p-rank of Λ/J_n is $p^{dn}-|S|\cdot p^r \cdot p^{(d-1)n}+O(p^{(d-2)n})$. On the other hand Lemma 2.3 shows that the Z/p-dimension of the mod p reduction, $\bar{\Lambda}/\bar{J}_n$, of Λ/J_n is also $p^{dn}-|S|\cdot p^r \cdot p^{(d-1)n}+O(p^{(d-2)n})$. Thus the dimension of the p-torsion subgroup of Λ/J_n is $O(p^{(d-2)n})$.

The following two lemmas, whose proof uses the Frobenius functor, are the key to bounding the growth of $r_{i,n}(M)$ for a fixed $i \geq 2$. They do not require $d \geq 2$.

Lemma 2.5. *Let N be a finitely generated $\bar{\Lambda}$-module of Krull dimension $\leq a$ and $\bar{I}_n$ be the ideal of $\bar{\Lambda}$ generated by the $X_i^{p^n}$. Then the Z/p-dimension of* $\mathrm{Tor}_i^{\bar{\Lambda}}(N, \bar{\Lambda}/\bar{I}_n)$ *is $O(p^{an})$.*

Proof. Let $N_{(n)}$ be the $\bar{\Lambda}$-module that is N as additive group but with $\bar{\Lambda}$ acting via the endomorphism $x \to x^{p^n}$ of $\bar{\Lambda}$. $\mathrm{Tor}_i^{\bar{\Lambda}}(N, \bar{\Lambda}/\bar{I}_n)$ is just the i^{th} homology group of the Koszul complex on N built from the multiplication by $X_j^{p^n}$ operators. As vector space over Z/p this identifies

with the i^{th} homology group of the Koszul complex on $N_{(n)}$ built from the multiplication by X_j operators; that is to say with $\mathrm{Tor}_i^{\bar{\Lambda}}(N_{(n)}, Z/p)$. We prove that the dimension of this last space is $O(p^{an})$ by induction on a. By dévissage we may assume that N is cyclic with prime annihilator P of coheight a. The case $a=0$ is trivial. If $a>0$, $N_{(1)}$ is annihilated by P and has rank p^a as $\bar{\Lambda}/P$-module. It follows that $N_{(1)}$ has a filtration in which p^a of the quotients are isomorphic to N, and each remaining quotient has Krull dimension $\leq a-1$. Applying the exact functor $M \to M_{(n)}$ to this filtration and using the induction assumption we find that $\dim(\mathrm{Tor}_i^{\bar{\Lambda}}(N_{(n+1)}, Z/p)) \leq p^a \dim(\mathrm{Tor}_i^{\bar{\Lambda}}(N_{(n)}, Z/p)) + cp^{(a-1)n}$ for some fixed c. The rest is easy.

Remark. Seibert [7] proves more precise results in a more general setting.

Lemma 2.6. *Let N be as in Lemma* 2.5, *and r be a fixed integer* ≥ 0. *Then the Z/p-dimension of* $\mathrm{Tor}_i^{\bar{\Lambda}}(N, \bar{\Lambda}/(X_1^{p^n}, X_2^{p^n}, \cdots, X_d^{p^r}))$ *is* $O(p^{an})$.

Proof. By dévissage we may assume that $r=0$ and that either X_d is not a zero-divisor on N or that X_d annihilates N. Set $\bar{\Lambda}' = \bar{\Lambda}/X_d$. In the first case the group we are studying identifies with $\mathrm{Tor}_i^{\bar{\Lambda}'}(N/X_dN, \bar{\Lambda}'/(X_1^{p^n}, \cdots, X_{d-1}^{p^n}))$, while in the second case it is an extension of $\mathrm{Tor}_{i-1}^{\bar{\Lambda}'}(N, \bar{\Lambda}/(X_1^{p^n}, \cdots, X_{d-1}^{p^n}))$ by $\mathrm{Tor}_i^{\bar{\Lambda}'}(N, \bar{\Lambda}'/(X_1^{p^n}, \cdots, X_{d-1}^{p^n}))$. Now apply Lemma 2.5 with $\bar{\Lambda}$ replaced by $\bar{\Lambda}'$.

Theorem 2.7. *Let M be a finitely generated Λ-module and i an integer* ≥ 0.

(a) *If M has Krull dimension $\leq d-2$ and $pM=(0)$ then $r_{i,n}(M) = O(p^{(d-2)n})$.*

(b) *The same estimate holds if M is Z_p-flat with characteristic power series* 1.

(c) *The same estimate holds if M is arbitrary, provided $i \geq 2$.*

Proof. To prove (a) we need to show that the Z/p-dimension of $\mathrm{Tor}_i^{\Lambda}(M, \Lambda/J_n)$ is $O(p^{(d-2)n})$. It suffices to prove this result with Λ/J_n replaced by Λ/I_n and by J_n/I_n. Now $\mathrm{Tor}_i^{\Lambda}(M, \Lambda/I_n)$ is the i^{th} homology group of a Koszul complex on M built from the multiplication by $X_j^{p^n}$ operators. It follows that it identifies with $\mathrm{Tor}_i^{\bar{\Lambda}}(M, \bar{\Lambda}/\bar{I}_n)$ and Lemma 2.5 with $a=d-2$ bounds the dimension of this space.

Let S_n be the product of the $\Lambda/(I_n, \sigma^{p^r}-1)$, $\sigma \in S$. There is a map of S_n onto J_n/I_n whose restriction to $\Lambda/(I_n, \sigma^{p^r}-1)$ is multiplication by $(\sigma^{p^n}-1)/(\sigma^{p^r}-1)$. S_n is a free Z_p-module of rank $|S| \cdot p^r \cdot p^{(d-1)n}$; it follows from Theorem 2.4 that the kernel, K_n, of $S_n \to J_n/I_n$ is free over Z_p of

rank $O(p^{(d-2)n})$. To bound the dimension of $\mathrm{Tor}_i^{\Lambda}(M, J_n/I_n)$ it suffices to bound the dimensions of $\mathrm{Tor}_{i-1}^{\Lambda}(M, K_n)$ and $\mathrm{Tor}_i^{\Lambda}(M, S_n)$. Now using the exact sequence $0\to K_n \xrightarrow{p} K_n \to K_n/pK_n \to 0$ we find that $\mathrm{Tor}_{i-1}^{\Lambda}(M, K_n)$ embeds in $\mathrm{Tor}_{i-1}^{\Lambda}(M, K_n/pK_n)$. Since K_n/pK_n admits a filtration of $O(p^{(d-2)n})$ steps with quotients isomorphic to Z/p the length of this last module is $O(p^{(d-2)n})$. To conclude the proof of (a) it suffices to show that for each $\sigma \in S$ the dimension of $\mathrm{Tor}_i^{\Lambda}(M, \Lambda/(I_n, \sigma^{p^r}-1))$ is $O(p^{(d-2)n})$. We may assume that $n \geq r$ and that $\sigma = 1+X_d$. Then $(I_n, \sigma^{p^r}-1)$ is generated by the $(1+X_i)^{p^n}-1$, $i<d$, together with $(1+X_d)^{p^r}-1$. So the group $\mathrm{Tor}_i^{\Lambda}(M, \Lambda/(I_n, \sigma^{p^r}-1))$ is just the i^{th} homology group of the Koszul complex on M built from the operators $X_1^{p^n}$, $X_2^{p^n}$, $\cdots$ and $X_d^{p^r}$. Now apply Lemma 2.6.

Suppose that M satisfies the hypotheses of (b). Using the exact sequence $0\to M \xrightarrow{p} M \to M/pM \to 0$ we see that the reduction mod p of $\mathrm{Tor}_i^{\Lambda}(M, \Lambda/J_n)$ embeds in $\mathrm{Tor}_i^{\Lambda}(M/pM, \Lambda/J_n)$. So it suffices to show that the Z/p-dimension of this last space is $O(p^{(d-2)n})$. By the hypotheses of (b) M has Krull dimension $\leq d-1$. As p is not a zero-divisor on M it is in no minimal prime of Ann M, and the Krull dimension of M/pM is $\leq d-2$. The desired bound then follows from (a).

By dévissage it suffices to prove (c) when M is cyclic with prime annihilator P. We may assume that P is non-principal since otherwise $r_{i,n}(M)=0$ for $i \geq 2$. Suppose first that $p \in P$. If M has Krull dimension $d-1$ then $P=(p, g)$ for some g with $\bar{g} \neq 0$. Then the $\mathrm{Tor}_i^{\Lambda}(M, \Lambda/J_n)$ are the homology groups of the Koszul complex on Λ/J_n built from multiplication by p and by g. Thus $\mathrm{Tor}_i^{\Lambda}(M, \Lambda/J_n)$ vanishes for $i>2$ while $\mathrm{Tor}_2^{\Lambda}(M, \Lambda/J_n)$ is contained in the p-torsion subgroup of Λ/J_n and so has dimension that is $O(p^{(d-2)n})$. Suppose next that $p \in P$ but that M has Krull dimension $<d-1$. Then (a) gives the desired result. Finally if $p \notin P$ we may apply (b).

Definition 2.8. If M is a finitely generated Λ-module then M^* is the largest submodule of M annihilated both by a power of p and by some $h \notin (p)$.

Theorem 2.9. *Let M be a finitely generated torsion Λ-module. Suppose that $M^*=(0)$ and the M/J_nM are finite groups. Then $r_{1,n}(M)$ is $O(p^{(d-2)n})$.*

Proof. There exist cyclic Λ-modules M_i with prime annihilators (f_i) and a map $\phi: M \to \prod M_i$ whose kernel and cokernel have trivial characteristic power series. Then the characteristic power series of M is $\prod f_i$;

it follows that each M_i/J_nM_i is finite. Let K, M' and C denote the kernel, image and cokernel of ϕ, so that we have exact sequences $(0)\to K \to M\to M'\to(0)$ and $(0)\to M'\to\prod M_i\to C\to(0)$. Then $r_{1,n}(M)\leq r_{1,n}(K) + r_{1,n}(M')\leq r_{1,n}(K)+r_{2,n}(C)+\sum_i r_{1,n}(M_i)$. Since K has characteristic power series (1) it is annihilated by some $h\notin(p)$. Thus the p-torsion subgroup of K is contained in M^*. But $M^*=(0)$. So K is flat over Z_p and Theorem 2.7 (b) shows that $r_{1,n}(K)$ is $O(p^{(d-2)n})$. Theorem 2.7 (c) gives the same estimate for $r_{2,n}(C)$. Finally $\mathrm{Tor}_1^{\Lambda}(M_i, \Lambda/J_n)$ identifies with the kernel of the multiplication by f_i map $\Lambda/J_n\to\Lambda/J_n$. But since M_i/J_nM_i which is the cokernel of this map is finite, the same is true of the kernel. So $\mathrm{Tor}_1^{\Lambda}(M_i, \Lambda/J_n)$ identifies with a finite subgroup of Λ/J_n—we conclude from Theorem 2.4 that $r_{1,n}(M_i)$ is $O(p^{(d-2)n})$.

We next wish to show that the exponent of the p-power torsion subgroup of $\mathrm{Tor}_i^{\Lambda}(M, \Lambda/J_n)$ is $O(n)$. Essential to this are the following lemmas from [5] whose proofs we repeat. The lemmas do not require $d\geq 2$.

Lemma 2.10. *Suppose $F\in R_j[\![X_1, \cdots, X_d]\!]$, $F\neq 0$. Then there is a non-empty open subset of W^d on which the function $\zeta\to$ord $F(\zeta-1)$ is bounded.*

Proof. We may assume that some co-efficient of F is a unit. Let $Y=\{\zeta\in W^d: F(\zeta-1)=0$ or ord $F(\zeta-1)\geq 1\}$. Arguing as in the proof of Lemma 1.13 we find that Y is contained in a proper closed subset of W^d.

Lemma 2.11. *Suppose $F\in R_j[\![X_1, \cdots, X_d]\!]$. Make the convention that* ord $0=0$. *Then the function $\zeta\to$ord $F(\zeta-1)$ is bounded on W^d.*

Proof. By induction on d, the case $d=0$ being trivial. By Lemma 2.10 the function $\zeta\to$ord $F(\zeta-1)$ is bounded on the complement of a union of finitely many $d-1$ dimensional Z_p-flats. So it suffices to show that $\zeta\to$ord $F(\zeta-1)$ is bounded on any such Z_p-flat, T. We may assume that T is defined by $\zeta_d=\varepsilon$. Set $F^*=F(X_1, \cdots, X_{d-1}, \varepsilon-1)$ so that F^* has co-efficients in some R_k. By the induction assumption $\zeta\to$ord $F^*(\zeta-1)$ is bounded on W^{d-1}, and we conclude that $\zeta\to$ord $F(\zeta-1)$ is bounded on T.

Theorem 2.12. *Let M be a finitely generated Λ-module. Then there is a constant c such that for each n the p-power torsion subgroup of M/J_nM is annihilated by p^{dn+n+c}.*

Proof. A detailed proof of a somewhat more general result is given in section 4 of [1]. We briefly sketch the specialization of that proof to

our case. In Lemma 1.5 we constructed an imbedding of

$$R_n[\![X_1, \cdots, X_d]\!]/I_n \quad \text{into} \quad \prod(R_n[\![X_1, \cdots, X_d]\!]/Q_\zeta),$$

the product extending over all $\zeta \in W^d(n)$. It's easy to see that the cokernel C_n of the imbedding is annihilated by p^{dn}. Consider the map

$$(M/J_nM) \underset{\Lambda}{\otimes} (R_n[\![X_1, \cdots, X_d]\!]/I_n) \to \prod((M/J_nM) \underset{\Lambda}{\otimes} (R_n[\![X_1, \cdots, X_d]\!]/Q_\zeta)).$$

The kernel of this map is a homomorphic image of $\mathrm{Tor}_1^\Lambda(M/J_nM, C_n)$ and so is annihilated by p^{dn}.

Now let $X = \bigcup_{\sigma,\varepsilon} T_{\sigma,\varepsilon}$ and $U = W^d - X$ be as in Definition 1.3. We make the following claims. First, if $\zeta \in X(n)$ then $(M/J_nM) \otimes_\Lambda (R_n[\![X_1, \cdots, X_d]\!]/Q_\zeta)$ is annihilated by p^{n-r}. Second, if $\zeta \in U(n)$ then the p-power torsion subgroup of $(M/J_nM) \otimes_\Lambda (R_n[\![X_1, \cdots, X_d]\!]/Q_\zeta)$ is annihilated by some p^a, independent both of n and of $\zeta \in U(n)$. Suppose we grant the claims. Then it follows from the paragraph above that the p-power torsion subgroup of $(M/J_nM) \otimes_\Lambda (R_n[\![X_1, \cdots, X_d]\!]/I_n)$ is annihilated by p^{dn+n-r} for large n. But as I_n annihilates M/J_nM this tensor product identifies with $(M/J_nM) \otimes_{R_n} Z_p$, a product of copies of M/J_nM.

It remains to establish the claims. The first is easy. If $\zeta \in T_{\sigma,\varepsilon}(n)$ then $(\sigma^{p^n} - 1)/(\sigma^{p^r} - 1)$ annihilates M/J_nM while $\sigma^{p^r} - 1$ annihilates $R_n[\![X_1, \cdots, X_d]\!]/Q_\zeta$. Since the tensor product is annihilated by each of these elements it is annihilated by p^{n-r}. Suppose now that $\zeta \in U(n)$. As we have seen in Lemma 1.6, $Q_\zeta \supset J_n$. Thus the tensor product identifies with $M \otimes_\Lambda (R_n[\![X_1, \cdots, X_d]\!]/Q_\zeta)$. Now choose a presentation $\Lambda^s \to \Lambda^t \to M \to (0)$ of M with matrix $|F_{ij}|$, and let $\{H_\alpha\}$ be the set of determinants of the finitely many square submatrices of $|F_{ij}|$. Then $M \otimes_\Lambda (R_n[\![X_1, \cdots, X_d]\!]/Q_\zeta)$ is the cokernel of a mapping $(R_n)^s \to (R_n)^t$ whose matrix is $|F_{ij}(\zeta - 1)|$. It follows from this that the p-power torsion subgroup of the cokernel is annihilated by some non-zero $H_\alpha(\zeta - 1)$. By Lemma 2.11 all the ord $H_\alpha(\zeta - 1)$ are bounded by some integer a independent of α and ζ. We conclude that p^a annihilates the p-power torsion subgroup of each $M \otimes_\Lambda (R_n[\![X_1, \cdots, X_d]\!]/Q_\zeta)$.

Corollary 2.13. *Let M be a finitely generated Λ-module and $i \geq 0$ an integer. Then there is a constant c such that for each n the p-power torsion subgroup of* $\mathrm{Tor}_i^\Lambda(M, \Lambda/J_n)$ *is annihilated by p^{dn+n+c}.*

Proof. For $i = 0$ this Theorem 2.12. For $i > 0$ map a finite free Λ-module onto M with kernel K, note $\mathrm{Tor}_i^\Lambda(M, \Lambda/J_n)$ embeds in $\mathrm{Tor}_{i-1}^\Lambda(K, \Lambda/J_n)$, and argue by induction.

Combining the above corollary with Theorems 2.7 and 2.9 we get:

Theorem 2.14. *Let M be a finitely generated torsion Λ-module such that the M/J_nM are finite. Suppose that $M^*=(0)$. Then for each $i\geq 1$, $l_{i,n}(M)=O(np^{(d-2)n})$. In particular $l(M/J_nM)=E_n(M)+O(np^{(d-2)n})$.*

We next study what happens when the assumption $M^*=(0)$ is dropped. First we show that $l(J_nM^*/I_nM^*)$ is $O(p^{(d-2)n})$.

Lemma 2.15. *Let N be a Λ-module annihilated both by some p^t and some $h\notin(p)$. Suppose $\sigma\in S$. Then there exists a $G\in\Lambda$, with $\overline{\sigma-1}$ not dividing $\bar{G}$, such that G annihilates $((\sigma^{p^n}-1)/(\sigma^{p^r}-1))N$ for large n.*

Proof. Modulo p, $h\equiv(\sigma-1)^\lambda g$ where $\overline{\sigma-1}$ does not divide $\bar{g}$. Set $G=g^t$. Since $g\cdot(\sigma-1)^\lambda$ annihilates N/pN, $G\cdot(\sigma-1)^{t\lambda}$ annihilates N. Now $(\sigma^{p^n}-1)/(\sigma^{p^r}-1)$ is in the ideal $(\sigma-1,p)^{n-r}$. So for n large it's in the ideal $((\sigma-1)^{t\lambda},p^t)$— the lemma follows.

Lemma 2.16. *Let N be a finitely generated Λ-module annihilated both by some p^t and some $h\notin(p)$. Then $l(J_nN/I_nN)$ is $O(p^{(d-2)n})$.*

Proof. It suffices to show that $l((I_n,(\sigma^{p^n}-1)/(\sigma^{p^r}-1))N/I_nN)$ is $O(p^{(d-2)n})$ for each $\sigma\in S$. Choose G as in Lemma 2.15 and set $\mathcal{O}=\Lambda/(G,\sigma^{p^r}-1,p^t)$. Then $\bar{\mathcal{O}}=\bar{\Lambda}/(\bar{G},\overline{\sigma-1}^{p^r})$ has Krull dimension $\leq d-2$. The argument of Lemma 2.2 shows that $l(\bar{\mathcal{O}}/\bar{I}_n\bar{\mathcal{O}})$ is $O(p^{(d-2)n})$, and since $l(\mathcal{O}/I_n\mathcal{O})\leq t\cdot l(\bar{\mathcal{O}}/\bar{I}_n\bar{\mathcal{O}})$, the same estimate holds for $l(\mathcal{O}/I_n\mathcal{O})$. Now for large n, $((I_n,(\sigma^{p^n}-1)/(\sigma^{p^r}-1))N)/I_nN$ is an $\mathcal{O}$-module annihilated by I_n. Since the number of generators of this module is independent of n we get the lemma.

Theorem 2.17. *Let M be a finitely generated torsion Λ-module such that the M/J_nM are finite, and let $M^*\subset M$ be as in Definition* 2.8. *Then $l(M/J_nM)=E_n(M)+l(M^*/I_nM^*)+O(np^{(d-2)n})$.*

Proof. Set $M'=M/M^*$. There is an exact sequence $\mathrm{Tor}_1^\Lambda(M',\Lambda/J_n)\to M^*/J_nM^*\to M/J_nM\to M'/J_nM'\to(0)$. Theorem 2.14 tells us that $l_{1,n}(M')=O(np^{(d-2)n})$ while $l(M'/J_nM')=E_n(M')+O(np^{(d-2)n})$. Since M and M' have the same characteristic power series, $E_n(M')=E_n(M)$. We conclude that $l(M/J_nM)=E_n(M)+l(M^*/J_nM^*)+O(np^{(d-2)n})$; Lemma 2.16 applied to M^* completes the proof.

To apply Theorem 2.17 we need good estimates both for $E_n(M)$ and $l(M^*/I_nM^*)$. The first is provided by Theorem 1.21. For the second we use the following deep results from [3] and [4].

Theorem 2.18. *Let N be a finitely generated Λ-module of Krull dimension $\leq a$ annihilated by p^{t+1} for some t. Then:*

(1) *If $a=1$ there is an $\alpha \in p^{-t}Z$ such that $l(N/I_nN)=\alpha p^n+O(1)$.*

(2) *In general there is a real α such that $l(N/I_nN)=\alpha p^{an}+O(p^{(a-1)n})$.*

Remarks. For the first result see Theorems 8.1 and 8.3 of [3]; the precise definition of α is given in Definition 2.3 of that paper. We shall only need (1) in the case $d=2$, which allows the unpleasant calculations of sections 4–6 of [3] to be simplified, but the proof is still messy.

The second result makes heavy use of the Frobenius functor; see Theorem 3.9 of [4]. In [4] we produce α as the limit of a Cauchy sequence; we do not know if it is always rational.

Corollary 2.19. *$l(M^*/I_nM^*)=\alpha p^{(d-1)n}+O(p^{(d-2)n})$ for some real α. When $d=2$, $\alpha \in Z[1/p]$.*

Proof. Since M^* is annihilated by some $h \notin (p)$, M^*/pM^* is a torsion module over $\bar{\Lambda}$ and so has Krull dimension $\leq d-1$. So the same is true of M^*, and we may apply Theorem 2.18 with $N=M^*$ and $a=d-1$.

§ 3. Estimates for $e(G_n)$ and $e_n(L/k)$

If G is a finitely generated Z_p-module denote the Z_p-rank of G by $r(G)$ and the length of the p-power torsion subgroup of G by $e(G)$. We wish to generalize Theorem 2.17 by estimating the growth of $e(G_n)$ for a sequence, G_n, defined as follows:

(1) M is a finitely generated torsion Λ-module; for each $\sigma \in S$, M_σ is a submodule of M containing $(\sigma^{p^r}-1)M$.

(2) For $n \geq r$, $A'_n=I_nM+\sum_{\sigma \in S}((\sigma^{p^n}-1)/(\sigma^{p^r}-1))M_\sigma$, and $G_n=M/A'_n$.

Throughout we shall assume that $r(G_n)=O(p^{(d-2)n})$. We begin the calculation of $e(G_n)$ by showing that for an appropriate λ the replacement of each M_σ by $M_\sigma+p^\lambda M$ changes $e(G_n)$ by at most $O(np^{(d-2)n})$. This requires several lemmas.

Lemma 3.1. *$r(M/(M_\sigma+I_nM))$ is $O(p^{(d-2)n})$.*

Proof. Because $r(M/A'_n)$ is $O(p^{(d-2)n})$ it's enough to show that $r((M_\sigma+A'_n)/(M_\sigma+I_nM))$ is $O(p^{(d-2)n})$. This reduces to showing that the Z_p-rank of $(M_\sigma+I_nM+((\tau^{p^n}-1)/(\tau^{p^r}-1))M_\tau)/(M_\sigma+I_nM)$ is $O(p^{(d-2)n})$ for each $\tau \in S$. We may assume $\tau \neq \sigma$. Since $M_\sigma \supset (\sigma^{p^r}-1)M$, the

module we're studying is annihilated by $\sigma^{p^r}-1$ as well as by $\tau^{p^r}-1$ and by I_n. Set $\mathcal{O}=\Lambda/(\sigma^{p^r}-1, \tau^{p^r}-1)$. Since no two elements of S generate the same Z_p-submodule of E the argument of Lemma 2.2 shows that the Z/p-dimension of $\bar{\mathcal{O}}/\bar{I}_n\bar{\mathcal{O}}$ is $O(p^{(d-2)n})$; the same estimate then holds for $r(\mathcal{O}/I_n\mathcal{O})$. But the $\mathcal{O}/I_n\mathcal{O}$-module we're studying is generated by a fixed number of elements, independent of n.

Lemma 3.2. *The characteristic power series, g, of M/M_σ is trivial.*

Proof. By Lemma 3.1 the R_n-rank of $(M/M_\sigma)\otimes_\Lambda(R_n[\![X_1, \cdots, X_d]\!]/I_n)$ is $O(p^{(d-2)n})$. Suppose that $(g)\neq(1)$. We shall derive a contradiction by showing that for $n\geq r$ the above R_n-rank is $\geq p^{(d-1)n}$. Note first that $\sigma^{p^r}-1$ annihilates M/M_σ. It follows that g factors in $R_r[\![X_1, \cdots, X_d]\!]$ into a product of linear factors of the form $\sigma-\varepsilon$ with $\varepsilon^{p^r}=1$. Fix one such factor, $\sigma-\varepsilon$, and suppose that $\zeta\in W^d(n)$ with $\sigma(\zeta-1)$ equal to this ε. The characteristic power series of the $R_n[\![X_1, \cdots, X_d]\!]$-module $(M/M_\sigma)\otimes_\Lambda R_n[\![X_1, \cdots, X_d]\!]$ is g. Thus the prime ideal $(\sigma-\varepsilon)$ is in the support of this module, and since $Q_\zeta\supset(\sigma-\varepsilon)$ the same is true of Q_ζ. Now $Q_\zeta\supset I_n$ as well and so is in the support of $(M/M_\sigma)\otimes_\Lambda(R[\![X_1, \cdots, X_d]\!]/I_n)$. So if we take a filtration of this last module in which the quotients are cyclic with prime annihilator, then each $R_n[\![X_1, \cdots, X_d]\!]/Q_\zeta$ for which $\zeta^{p^n}=1$ and $\sigma(\zeta-1)=\varepsilon$ occurs at least once as a quotient. Since the number of such ζ is $p^{(d-1)n}$ we have the desired contradiction.

Lemma 3.3. *Choose λ so large that p^λ annihilates the p-power torsion in each M/M_σ. Then the Z_p-module $(A'_n+p^\lambda J_nM)/A'_n$ can be generated by $O(p^{(d-2)n})$ elements.*

Proof. Set $D_\sigma=p^\lambda(M/M_\sigma)$. Then D_σ is flat over Z_p; by Lemma 3.2 it has Krull dimension $\leq d-1$. So D_σ/pD_σ has Krull dimension $\leq d-2$, and an argument familiar by now shows that D_σ/I_nD_σ can be generated by $O(p^{(d-2)n})$ elements as Z_p-module. Now D_σ/I_nD_σ identifies with $(p^\lambda M+M_\sigma)/(p^\lambda I_nM+M_\sigma)$. Thus we get a map from $\prod_\sigma(D_\sigma/I_nD_\sigma)$ to M/A'_n whose restriction to D_σ/I_nD_σ is induced by multiplication by $(\sigma^{p^n}-1)/(\sigma^{p^r}-1)$. The image of this map is evidently $(A'_n+p^\lambda J_nM)/A'_n$, giving the lemma.

Lemma 3.4. *There is a constant c such that for each n both the p-power torsion subgroup of M/A'_n and the p-power torsion subgroup of $M/(A'_n+p^\lambda J_nM)$ are annihilated by p^{dn+n+c}.*

Proof. For M/A'_n this slight generalization of Theorem 2.12 may be proved by a similar technique; for details see section 4 of [1]. The

result for $M/(A'_n+p^\lambda J_nM)$ follows on replacing each M_σ by $M_\sigma+p^\lambda M$; this has the effect of replacing A'_n by $A'_n+p^\lambda J_nM$.

Theorem 3.5. *Choose λ as in Lemma* 3.3 *and set $H_n=M/(A'_n+p^\lambda J_nM)$. Then $|e(G_n)-e(H_n)|$ is $O(np^{(d-2)n})$.*

Proof. Suppose we have an onto map $\phi: G\to H$ of finitely generated Z_p-modules with the following properties: the p-power torsion subgroups of G and H are each annihilated by p^A and the kernel K of ϕ can be generated by B elements over Z_p. We claim that $|e(G)-e(H)|\leq AB$. To see this note the exact sequence

$$(0)\to {}^tK\to {}^tG\to {}^tH\to K/p^AK\to G/p^AG\to H/p^AH\to(0)$$

where ${}^tK$, ${}^tG$ and ${}^tH$ are the torsion subgroups of K, G and H. The sequence shows that both the kernel and cokernel of ${}^tG\to {}^tH$ are annihilated by p^A and generated by B or fewer elements over Z_p, establishing the claim. Now apply this result to the projection map $G_n\to H_n$ with kernel $(A'_n+p^\lambda J_nM)/A'_n$. Since Lemma 3.3 shows that this kernel can be generated by $O(p^{(d-2)n})$ elements, and Lemma 3.4 that both ${}^tG_n$ and ${}^tH_n$ are annihilated by p^{dn+n+c}, the theorem follows.

We now proceed to estimate $e(G_n)$ with an error term no worse than $O(np^{(d-2)n})$. We assume in the following definition and lemmas that the M/J_nM are finite groups—this restriction is very easy to get rid of. In view of Theorem 3.5 we may replace each M_σ by $M_\sigma+p^\lambda M$. So we shall assume that $M_\sigma\supset p^\lambda M$ for some λ. Then p^λ annihilates J_nM/A'_n, the M/A'_n are finite groups, and $e(G_n)$ is just $l(G_n)$.

Definition 3.6.

(1) $X_\sigma=M/(\sigma^{p^r}-1, p^\lambda)M$, $Y_\sigma=M_\sigma/(\sigma^{p^r}-1, p^\lambda)M$.

(2) $N_\sigma=X_\sigma/Y_\sigma=M/M_\sigma$.

(3) J'_n is the ideal $I_n+p^\lambda J_n$ of Λ.

Besides the obvious maps $\prod_\sigma(Y_\sigma/I_nY_\sigma)\to\prod_\sigma(X_\sigma/I_nX_\sigma)$ we have for each $n\geq r$ a map $\prod_\sigma(X_\sigma/I_nX_\sigma)\to M/J'_nM$ whose restriction to X_σ/I_nX_σ is induced by multiplication by $(\sigma^{p^n}-1)/(\sigma^{p^r}-1)$. Composing, we get maps $\prod_\sigma(Y_\sigma/I_nY_\sigma)\to M/J'_nM$. The following observation is clear.

Lemma 3.7. *The cokernels of the maps $\prod(Y_\sigma/I_nY_\sigma)\to\prod(X_\sigma/I_nX_\sigma)$, $\prod(X_\sigma/I_nX_\sigma)\to M/J'_nM$, and $\prod(Y_\sigma/I_nY_\sigma)\to M/J'_nM$ identify respectively with $\prod(N_\sigma/I_nN_\sigma)$, M/J_nM and M/A'_n.*

Lemma 3.8. *Let N be a finitely generated Λ-module annihilated by $(\sigma^{p^r}-1, p^\lambda)$ for some $\sigma\in S$. Then there is an integer $\alpha=\alpha(N)$ such that*

$l(N/I_nN)=\alpha p^{(d-1)n}+O(p^{(d-2)n})$. *In particular,* $l(N_\sigma/I_nN_\sigma)=\alpha(N_\sigma)p^{(d-1)n}+O(p^{(d-2)n})$.

Proof. Without loss of generality we may assume that $\sigma=1+X_d$. Set $\Lambda'=Z_p[\![X_1, \cdots, X_{d-1}]\!]$ and let I'_n be the ideal of Λ' generated by the $(1+X_j)^{p^n}-1$ for $j<d$. Then N is a finitely generated Λ'-module annihilated by p^λ: let p^α be its characteristic power series as Λ'-module. For $n\geq r$, $N/I_nN=N/I'_nN$. We can now argue as in sections 1 and 2 with d replaced by $d-1$ to conclude that $l(N/I'_nN)=\alpha p^{(d-1)n}+O(p^{(d-2)n})$. Or more simply we can proceed as follows. There exist cyclic Λ'-modules N_i with annihilators (p^{n_i}), $\sum n_i=\alpha$, and maps $\phi: N\to\prod N_i$, $\phi^*: \prod N_i\to N$ whose cokernels C and C^* are annihilated by some $h\notin(p)$. Then C/I'_nC and C^*/I'_nC^* are modules over $\Lambda'/(h, p^\lambda)$, a local ring of Krull dimension $\leq d-2$. It follows in the usual way that $l(C/I'_nC)$ and $l(C^*/I'_nC^*)$ are each $O(p^{(d-2)n})$, and consequently that $l(N/I'_nN)$ and $\sum l(N_i/I'_nN_i)$ differ by $O(p^{(d-2)n})$. But since Λ'/I'_n is a free Z_p-module of rank $p^{(d-1)n}$, the length of N_i/I'_nN_i is $n_ip^{(d-1)n}$. Now use the fact that $\sum n_i=\alpha$.

Lemma 3.9. *Suppose that* $M^*=(0)$. *Then each of the maps of Lemma* 3.7 *has kernel of length* $O(p^{(d-2)n})$.

Proof. To prove the result for the first map it suffices to show that the length of the kernel of $Y_\sigma/I_nY_\sigma\to X_\sigma/I_nX_\sigma$ is $O(p^{(d-2)n})$; this is in fact true without the restriction $M^*=(0)$. We may assume that $\sigma=1+X_d$. There is an exact sequence $Y_\sigma/I_nY_\sigma\to X_\sigma/I_nX_\sigma\to N_\sigma/I_nN_\sigma\to(0)$. Up to an error term of $O(p^{(d-2)n})$ the lengths of Y_σ/I_nY_σ, X_σ/I_nX_σ and N_σ/I_nN_σ are given by $\alpha(Y_\sigma)p^{(d-1)n}$, $\alpha(X_\sigma)p^{(d-1)n}$ and $\alpha(N_\sigma)p^{(d-1)n}$. But the explicit description of α given in the proof of Lemma 3.8 shows that $\alpha(X_\sigma)=\alpha(Y_\sigma)+\alpha(N_\sigma)$—the desired estimate follows.

It remains to prove the result for the map $\prod(X_\sigma/I_nX_\sigma)\to M/J'_nM$, under the assumption that $M^*=(0)$. Take $S_n=\prod_\sigma\Lambda/(\sigma^{p^r}-1, I_n)$ as in the proof of Theorem 2.7. Note that $\prod(X_\sigma/I_nX_\sigma)=\prod(M/(\sigma^{p^r}-1, I_n, p^\lambda)M)=M\otimes_\Lambda(S_n/p^\lambda S_n)$. Now the exact sequence $(0)\to K_n\to S_n\to J_n/I_n\to(0)$ of the proof of Theorem 2.7 yields, on reduction modulo p^λ, an exact sequence $K_n/p^\lambda K_n\to S_n/p^\lambda S_n\to J_n/J'_n\to(0)$. Thus the kernel of the map $M\otimes_\Lambda(S_n/p^\lambda S_n)\to M\otimes_\Lambda(J_n/J'_n)$ is a homomorphic image of $M\otimes_\Lambda(K_n/p^\lambda K_n)$ and so has length that is $O(p^{(d-2)n})$. Furthermore the kernel of the map $M\otimes_\Lambda(J_n/J'_n)\to M/J'_nM$ is a homomorphic image of $\mathrm{Tor}_1^\Lambda(M, \Lambda/J_n)$, and is annihilated by p. Under the assumption $M^*=(0)$, Theorem 2.9 shows that the length of this kernel is $O(p^{(d-2)n})$. So the length of the kernel of the composite map $M\otimes_\Lambda(S_n/p^\lambda S_n)\to M/J'_nM$ is also $O(p^{(d-2)n})$, establishing the lemma.

Lemma 3.10. *Suppose that $M^*=(0)$. Then there is an integer β such that $l(G_n)=l(M/J_nM)+\beta p^{(d-1)n}+O(p^{(d-2)n})$.*

Proof. By Lemmas 3.7 and 3.9, $l(M/A'_n)-l(M/J_nM)-\sum l(N_\sigma/I_nN_\sigma)$ is $O(p^{(d-2)n})$. Now apply Lemma 3.8.

Theorem 3.11. *Let F be the characteristic power series of M. Suppose that the G_n are defined as at the beginning of this section and that $r(G_n)=O(p^{(d-2)n})$. The there is a non-empty open subset U of W^d and an integer β such that $e(G_n)=\sum(F, U, n)+l(M^*/I_nM^*)+\beta p^{(d-1)n}+O(np^{(d-2)n})$.*

Proof. We first prove the theorem under the hypothesis that the M/J_nM are finite. Then Theorem 3.5 allows us to assume that $M_\sigma \supset p^\lambda M$ for some fixed integer λ. Replacing M by $M'=M/M^*$ and each M_σ by its image in M/M^*, and applying Lemma 3.10 we find that $l(M/(M^*+A'_n))=l(M'/J_nM')+\beta p^{(d-1)n}+O(p^{(d-2)n})$ for some integer β. If we take U as in Definition 1.3, then Theorems 1.10 and 2.14 applied to M' tell us that $l(M'/J_nM')=\sum(F, U, n)+O(np^{(d-2)n})$. It remains to show that $l(M/A'_n)=l(M/(M^*+A'_n))+l(M^*/I_nM^*)+O(p^{(d-2)n})$. Since the cokernel of the map $M^*/I_nM^*\to M/A'_n$ identifies with $M^*/(M^*+A'_n)$ it's enough to show that the length of the kernel is $O(p^{(d-2)n})$. As M/A'_n maps onto M/J_nM it suffices to prove this result for the kernel of $M^*/I_nM^*\to M/J_nM$. But this last map factors through M^*/J_nM^*. Since the kernel of $M^*/J_nM^*\to M/J_nM$ is a homomorphic image of $\mathrm{Tor}_1^A(M/M^*, A/J_n)$, and is annihilated by a fixed power of p, Theorem 2.9 shows that its length is $O(p^{(d-2)n})$. Finally we see from Lemma 2.16 that the length of the kernel of $M^*/I_nM^*\to M^*/J_nM^*$ is also $O(p^{(d-2)n})$.

We now show how to remove the assumption that the M/J_nM are finite. In view of Theorem 1.14 we can find an $r'\geq r$ and an $S'\supset S$ so that if we use r' and S' to define ideals J'_n, $n\geq r'$, as in Definition 1.1 then the M/J'_nM are finite. For each $\sigma\in S'$ we define a submodule M'_σ of M as follows. If $\sigma\in S$, $M'_\sigma=((\sigma^{p^{r'}}-1)/(\sigma^{p^r}-1))M_\sigma$, while if $\sigma\notin S$ then $M'_\sigma=(\sigma^{p^{r'}}-1)M$. Then for $n\geq r'$ the A'_n defined from r', S' and the M'_σ is the same as the A'_n defined from r, S, and the M_σ. So $e(G_n)$ is unchanged when r, S and M_σ are replaced by r', S' and M'_σ, and we may apply the result of the last paragraph.

Using Theorems 1.19 and 1.20 to estimate $\sum(F, U, n)$ and Corollary 2.19 to handle $l(M^*/I_nM^*)$ we get:

Theorem 3.12. *Situation as in as in Theorem* 3.11. *Let $m_0=m_0(F)$ and $l_0=l_0(F)$. Then there is a real number α^* such that $e(G_n)=m_0p^{dn}+l_0np^{(d-1)n}+\alpha^*p^{(d-1)n}+O(np^{(d-2)n})$. If either $M^*=(0)$ or $d=2$ then α^* is rational.*

We now use the method of [1] to deduce the number-theoretic results of the introduction from Theorem 3.12. Namely let L/k be a Z_p^d-extension with $d \geq 2$, let M_L be the maximal unramified abelian pro-p extension of L and set $X = G(M_L/L)$. Then the free rank d Z_p-module $G(L/k)$ acts on X by conjugation. Let Λ and E be as in section 1 and fix an isomorphism between $G(L/k)$ and E. Then E acts on X and we may use this action to make X into a Λ-module, the "Greenberg-Iwasawa" module of L/k. As in the case $d=1$, treated by Iwasawa, X is finitely generated and torsion over Λ, and one can essentially recover the Galois group of the maximal unramified abelian p-extension of k_n, and hence $e_n(L/k)$, from X together with its Λ-module structure.

To be precise, the following result is proved in Theorems 5.11 and 5.12 of [1]. *There is an integer $r \geq 0$ and a finite set of pairs (τ_i, M_i), $\tau_i \in E - E^p$, M_i a Λ-submodule of X, such that if we set $A_n' = I_n X + \sum_i ((\tau_i^{p^n} - 1)/(\tau_i^{p^r} - 1))M_i$ then the $r(X/A_n'))$ are bounded and $|e_n(L/k) - e(X/A_n')| = O(n)$.* Now without changing the A_n' we may assume that $M_i \supset (\tau_i^{p^r} - 1)X$ and that the τ_i generate distinct Z_p-submodules of E. But we are now in precisely the algebraic situation treated in this section, and Theorem 3.12 gives:

Theorem 3.13. *Let L/k be a Z_p^d-extension of a number field, $d \geq 2$, X the Greenberg-Iwasawa module of the extension, and F the characteristic power series of X. Set $m_0 = m_0(F)$, $l_0 = l_0(F)$. Then there is a real number α^* such that $e_n(L/k) = (m_0 p^n + l_0 n + \alpha^*)p^{(d-1)n} + O(np^{(d-2)n})$. When $d=2$, α^* is rational.*

References

[1] Cuoco, A., Monsky, P., Class numbers in Z_p^d-extensions, Math. Ann., **255** (1981), 235–258.

[2] ——, Some contributions to the theory of Z_p^2-extensions, Brandeis University thesis (1979).

[3] Monsky, P., Class numbers in Z_p^d-extensions, III, Math. Z., **193** (1986), 491–514.

[4] ——, Class numbers in Z_p^d-extensions, IV, Math. Z., **196** (1987), 547–572.

[5] ——, On p-adic power series, Math. Ann., **255** (1981), 217–227.

[6] ——, p-Ranks of class groups in Z_p^d-extensions, Math. Ann., **263** (1983), 509–514.

[7] Seibert, G., Complexes with homology of finite length and Frobenius functors, J. Algebra, to appear.

[8] Serre, J. P., Algèbre Locale Multiplicités. Lecture Notes in Mathematics **11**, p. 139. Berlin Heidelberg New York: Springer 1975.

Department of Mathematics
Brandeis University
Waltham, MA 02254
U.S.A.