Journal de Théorie des Nombres
de Bordeaux **14** (2002), 113–149

On Galois structure of the integers in cyclic extensions of local number fields

par G. Griffith ELDER

Dedicated to Professor Manohar L. Madan

Résumé. Soit p un nombre premier, K une extension finie du corps des nombres p-adiques, et L/K une extension cyclique ramifiée de degré p^n. On suppose que le premier nombre de ramification de L/K satisfait $b_1 > 1/2 \cdot pe_0/(p-1)$ où e_0 est l'indice de ramification absolu de K. Nous déterminons explicitement la structure de l'anneau des entiers de L comme $\mathbb{Z}_p[G]$-module, où $\mathbb{Z}_p$ désigne l'anneau des entiers p-adiques et $G = \mathrm{Gal}(L/K)$ le groupe de Galois de L.

Abstract. Let p be a rational prime, K be a finite extension of the field of p-adic numbers, and let L/K be a totally ramified cyclic extension of degree p^n. Restrict the first ramification number of L/K to about half of its possible values, $b_1 > 1/2 \cdot pe_0/(p-1)$ where e_0 denotes the absolute ramification index of K. Under this loose condition, we explicitly determine the $\mathbb{Z}_p[G]$-module structure of the ring of integers of L, where $\mathbb{Z}_p$ denotes the p-adic integers and G denotes the Galois group $\mathrm{Gal}(L/K)$. In the process of determining this structure, we study various restrictions on the ramification filtration and examine the trace map relationships that result. Two of these restrictions are generalizations of *almost maximal ramification*. Our method for determining this structure is constructive (also inductive). We exhibit generators for the ring of integers of L over the group ring, $\mathbb{Z}_p[G]$ (actually over $\mathfrak{O}_T[G]$ where $\mathfrak{O}_T$ is the ring of integers in the maximal unramified subfield of K). They are determined in an essential way by their valuation. Then we describe their relations.

1. Introduction

The Normal Basis Theorem says that in a finite Galois extension of fields, L/K, there is an element whose conjugates provide a field basis for L over K. As such, this theorem explains the Galois action on fields. Restricting

Manuscrit reçu le 2 février 2001.
This research was partially supported through UCR grant no. 99-28, University of Nebraska at Omaha.

our attention to finite Galois extensions of number fields, L/K, we may ask about the Galois action on the ring of integers $\mathfrak{O}_L$ of L. This is tied to the arithmetic of the extension. By a result of E. Noether [10], we know that in order for a normal *integral* basis to exist it is necessary for the extension to be at most tamely ramified.

For local number fields, E. Noether's result is not only necessary but also sufficient. To be precise we fix a prime p, write $\mathbb{Q}_p$ for the field of p-adic numbers, let K be any finite extension of $\mathbb{Q}_p$, and suppose that L is a finite Galois extension of K with Galois group, G. The ring of integers of L has a normal basis over the ring of integers $\mathfrak{O}_K$ of K, if and only if L/K is at most tamely ramified. In other words, there is an integer $\alpha \in \mathfrak{O}_L$ whose conjugates, $\{\sigma\alpha : \sigma \in G\}$, provide a basis for $\mathfrak{O}_L$ over $\mathfrak{O}_K$, precisely when the ramification index of L/K is not divisible by p (*i.e.* $\mathfrak{P}_K \cdot \mathfrak{O}_L = \mathfrak{P}_L^e$ and $p \nmid e$ where $\mathfrak{P}$ refers to the unique prime ideal).

Outside of this situation, when the ramification index is divisible by p (*i.e.* the ramification is wild), our understanding of the Galois module structure of $\mathfrak{O}_L$ is extremely limited. To gain some control over the variety of issues that can emerge, we restrict our investigation in this paper to those extensions with cyclic Galois group. So that we may focus our attention completely on the difficulties associated with wild ramification, we assume these extensions to be totally wild. Therefore we study in this paper the Galois module structure of the integers in totally ramified, cyclic, p-extensions. Because L/K is totally ramified $\mathfrak{P}_K \cdot \mathfrak{O}_L = \mathfrak{P}_L^e$ where $e = [L : K]$. Because L/K is a p-extension $[L : K] = p^n$ for some n. Before we explain things further, we adopt some notation.

1.1. Notation.

- Fix a generator σ of $G = \mathrm{Gal}(L/K)$.
- Let K_i denote the fixed field of σ^{p^i}. Relabel $K_0 := K$, $K_n := L$.
- Let $\mathfrak{O}_i$ denote the ring of integers in K_i and $\mathfrak{P}_i$ the maximal ideal of $\mathfrak{O}_i$.
- Let π_i be a prime element in K_i, and v_i the valuation of K_i so that $v_i(\pi_i) = 1$.
- Let $b_1 < b_2 < \cdots < b_n$ denote the lower ramification numbers of K_n/K_0 [12, Ch IV].
- For $i \geq j \geq 0$ let $\mathrm{Tr}_{i,j}$ denote the relative trace from K_i to K_j and let $\lambda_{i,j}$ be the integer such that $\mathrm{Tr}_{i,j}\mathfrak{O}_i = \mathfrak{P}_j^{\lambda_{i,j}}$.
- Let T be the maximal unramified extension of $\mathbb{Q}_p$ contained in K_0, e_0 the absolute ramification index of $K_0/\mathbb{Q}_p$, and f the degree of inertia of $K_0/\mathbb{Q}_p$, so that $[K_0 : T] = e_0$, $[T : \mathbb{Q}_p] = f$.
- Let $\mathbb{F}_p$ denote the finite field of p elements.

- For $i \geq 1$ let $\Phi_{p^i}(x) = \sum_{j=0}^{p-1} x^{jp^{i-1}} = \Phi_p(x^{p^{i-1}})$ be the cyclotomic polynomial, and define $\Phi_1(x) = x - 1$.
- Let $\phi(x)$ be the Euler Phi function with $\phi(1) := 1$.
- Use $\lfloor x \rfloor$ to denote the floor function (the greatest integer less than or equal to x), while $\lceil x \rceil$ denotes the ceiling function (the least integer greater than or equal to x).

Generalizing [12, V Lem 4] (using [12, III Prop 7] and [12, IV Prop 4]) one sees that for $i \geq j$,

$$\lambda_{i,j} = \left\lfloor \frac{(b_{j+1}+1)(p^{i-j}-1) + \sum_{k=j+1}^{i-1}(b_{k+1}-b_k)(p^{i-k}-1)}{p^{i-j}} \right\rfloor . \tag{1.1}$$

While Serre's Book [12] is our primary reference for local number fields, our main reference for integral representation theory is Curtis and Reiner [2].

1.2. Structure of the Integers over the Group Ring $\mathbb{Z}_p[G]$. Motivated by the classification theorems of Integral Representation Theory, one is lead in a natural way to ask for the $\mathbb{Z}_p[G]$-module structure of $\mathfrak{O}_n$. If Noether's result is seen as a determination of $\mathfrak{O}_k[G]$-structure of $\mathfrak{O}_n$ for every subfield k of K_0, this is then one approach to generalization.

In [11] this approach was adopted by Rzedowski-Calderón, Villa-Salvador and Madan. They were motivated by Heller and Reiner's finite classification of indecomposable $\mathbb{Z}_p[C_{p^2}]$-modules [6], and sought the $\mathbb{Z}_p[G]$-module structure of $\mathfrak{O}_2$. Due to technical considerations, they did not get a complete result, finding it necessary to impose three separate restrictions on the first ramification number:

$$b_1 \geq \max\left\{\frac{e_0}{p-1}, \frac{pe_0-p+1}{2p-1}, \frac{pe_0}{p-1} - (p+1)\right\}. \tag{1.2}$$

These restrictions, in particular the second and third restriction of (1.2), have subsequently played a role in generalizations to $n > 2$.

The first of these generalizations, [5], was derived under what may be viewed principally as a slight tightening of the third part of (1.2). Under

$$b_1 \geq \max\left\{\frac{e_0}{2}, \left\lceil\frac{pe_0}{p-1}\right\rceil - p\right\}, \tag{1.3}$$

the following condition on the traces was determined:

$$\mathrm{Tr}_{t,t-2}(\mathfrak{O}_t) = \mathrm{Tr}_{t,t-2}(\mathfrak{O}_{t-1}), \quad 2 \leq t \leq n. \tag{1.4}$$

This condition restricts the number of indecomposable modules that may appear in $\mathfrak{O}_n$ to a finite set [5, Thm 4], therefore enabling the determination of the structure of $\mathfrak{O}_n$ as a $\mathbb{Z}_p[G]$-module [5, Thm 5].

The other generalization to $n > 2$ is this paper. Here we tie the second restriction in (1.2), which we call *near maximal ramification*, to a condition on the traces that may be used to greatly simplify considerations in [11]. See §2.4.1. We also introduce a new restriction on ramification, *strong ramification*, tied similarly to "trace" relations. *Strong ramification* implies *near maximal ramification*. Together they yield our main result:

Theorem 1.1. *Let p be any prime, K_0 be any finite extension of the p-adic numbers and K_n/K_0 be a fully ramified cyclic extension of degree p^n, $n \geq 1$. Assume that K_n/K_0 is strongly ramified – that its first ramification number satisfies*

$$b_1 > \frac{1}{2} \cdot \frac{pe_0}{p-1}.$$

If $G = \mathrm{Gal}(K_n/K_0)$ and H denotes the subgroup of order p, then the structure of the ring of integers, $\mathfrak{O}_n$, as a $\mathbb{Z}_p[G]$-module is determined inductively by:

$$\mathfrak{O}_n \cong \mathcal{R}_n^{\lambda_{1,0}f} \oplus \bigoplus_{i=\lambda_{n,n-1}}^{p^{n-1}e_0-1} \mathcal{R}_n(i)^f \oplus \left(\mathfrak{O}_{n-1} \ominus \bigoplus_{i=\lambda_{n,n-1}}^{p^{n-1}e_0-1} \left(\mathcal{R}_n(i)^f\right)^H \right).$$

These modules are defined in Appendix A. Other notation is defined in §1.1. Note that $\mathcal{M}^H$ denotes the submodule of $\mathcal{M}$ fixed by H, while $\ominus$ denotes the removal of a direct summand, so that $(\mathcal{M} \oplus \mathcal{N}) \ominus \mathcal{N} = \mathcal{M}$.

To put *strong ramification* in some context, note that the first lower ramification number b_1 of a cyclic p-extension is either $pe_0/(p-1)$ (if K_0 contains a p-th root of unity) or an integer which satisfies $-1 \leq b_1 < pe_0/(p-1)$ with $\gcd(b_1, p) = 1$ [12, IV §2 Ex. 3]. *Strong ramification* restricts b_1 to about one half of its possible values.

1.3. Organization of Paper. In §2, we will discuss the implications of six different restrictions on the ramification filtration, making the connection between these restrictions and trace relations our theme. Using the implications of *strong ramification*, we provide Galois generators for the ring of integers in §3. A complete description of the Galois relationships, at this point, would determine the Galois module structure. This is given in two steps. In §4 we recursively reselect the Galois generators again. This time we are careful to select them to be compatible with other previously selected Galois generators. This gives us the Galois relationships, but leaves open the possibility that they may be entangled with one another. In other words, certain Galois generators may appear in more than one Galois relationship. The second step occurs in §5 where we disentangle these Galois relationships. The section concludes with the structure of $\mathfrak{O}_3$. The dis–entanglement in §5 results however in more than the structure of $\mathfrak{O}_3$, it determines the structure of $\mathfrak{O}_n$, the main result of this paper Theorem 1.1. In §6 we provide a proof of our main result, briefly discuss its implications, and provide some corollaries, the first of which is the main result of [5]. The last section, §7, contains directions for constructing examples and some further remarks. We conclude the paper with Appendix A, an explanation of our $\mathbb{Z}_p[C_{p^n}]$-module notation.

2. Ramification restrictions and trace relations

The study of the Galois module structure of the ring of integers has been closely tied to restrictions on ramification ever since E. Noether's Normal Basis Theorem. Often the utility of a restriction on the ramification numbers emerges only after the restriction is translated into a statement about trace maps (in other words, translated into a statement concerning the existence of certain elements in the associated order). For example, tame ramification, which restricts the lower ramification numbers below 0, is equivalent to the condition $\mathrm{Tr}_{L/K}(\mathfrak{O}_L) = \mathfrak{O}_K$ (this condition was generalized to other ideals by Ullom [13]).

We begin the section with a universal trace map relationship, a relationship that holds for all cyclic p-extensions, whether ramified or not. We emphasize this fact, since the other trace relationships that we examine are all associated with restrictions on the ramification numbers. Next we discuss *stable ramification*: If the first ramification number is large enough, the other ramification numbers are determined. We also discuss *almost maximal ramification*, a condition that has played an important role in other investigations of the Galois structure of the integers in wildly ramified cyclic extensions – notably the work of Bertrandias [1] concerning structure of the integers over the associated order, and the work of Miyata [9] and Vostokov [14] concerning the structure over $\mathfrak{O}_0[G]$. Note that "tame" and "almost maximal" are two extremes of ramification – one bounds the ramification numbers from above while the other bounds the ramification numbers from below. Following our section on *almost maximal ramification* we interpret the restrictions imposed in [11] as generalizations of this condition. In the last part of this section we will study *strong ramification*:

$$\frac{1}{2} \cdot \frac{pe_0}{p-1} < b_1. \tag{2.1}$$

Since this restriction is stronger than *stable ramification* and one of the more useful generalizations of *almost maximal ramification*, namely *near maximal ramification*, we use it and its consequences to prove our main result.

2.1. A Universal Trace Relation. The family of trace map relationships described in this section hold in any cyclic p-extension, regardless of ramification. Besides their utility in our work, they have additional importance as they address the following question:

Definition: Define $\mathcal{S}_G$, the realizable indecomposables, to be the set of indecomposable $\mathbb{Z}_p[G]$-modules $\mathcal{M}$, for which there is an extension L/K with $\mathrm{Gal}(L/K) \cong G$ such that $\mathcal{M}$ appears as a $\mathbb{Z}_p[G]$-direct summand of $\mathfrak{O}_L$.

Question A: Is $\mathcal{S}_{C_{p^n}}$ equal to the set of all indecomposable $\mathbb{Z}_p[C_{p^n}]$-modules? (Because of [11, Thm 1], this question is only interesting for $n > 1$.)

The existence of these universal trace relationships enables us to answer to Question A. The answer is "no". But first we state the relationships from which we may draw this conclusion.

Lemma 2.1. *The following relationships hold in any cyclic p-extension:*

$$(\mathrm{Tr}_{j,j-1}\mathfrak{O}_j) \cap \mathfrak{O}_{j-2} \subseteq \mathrm{Tr}_{j-1,j-2}\mathfrak{O}_{j-1}, \quad j = 2, \dots, n.$$

Proof. If K_j/K_{j-2} is unramified or only partially ramified, then one has $\mathrm{Tr}_{j-1,j-2}\mathfrak{O}_{j-1} = \mathfrak{O}_{j-2}$ and the result clearly holds. If the extension is fully ramified, then this is equivalent to the statement that $\lambda_{j,j-1} \geq p\lambda_{j-1,j-2}$. This inequality may be verified as follows: If $b_{j-1} \geq p^{j-2}e_0/(p-1)$ then we have stable ramification so use (2.2) to find that $b_j = b_{j-1} + p^{j-1}e_0$, and (1.1) to evaluate the λ's. Otherwise, as one may check, $b_j \geq (p^2-p+1)b_{j-1}$ from which the statement follows. For further details, see [3, Lem 6]. □

We now turn our attention to Question A and address it for $G \cong C_{p^n}$. Note that because the answer for $n = 2$ is "no" (see below), the answer is "no" for all $n \geq 2$.

2.1.1. *Application: The Case p^2.* Based upon Lemma 2.1, we can strengthen the main result of [11]. Since $\mathrm{Tr}_{2,1}\mathfrak{O}_2 \cap \mathfrak{O}_0 \subseteq \mathrm{Tr}_{1,0}\mathfrak{O}_1$, we determine that any indecomposable summand $\mathcal{M}$ of $\mathfrak{O}_2$ must satisfy $\left(\Phi_{p^2}(\sigma)\mathcal{M}\right)^\sigma \subseteq \Phi_p(\sigma)\left(\mathcal{M}^{\sigma^p}\right)$, where $\mathcal{X}^\gamma$ denotes the submodule of $\mathcal{X}$ that is fixed by $\gamma \in G$. One may easily check that $(\mathcal{R}_2, \mathcal{Z}; 1)$ (See §A.3. The notation is from [2, Thm 34.32]) does not satisfy this condition. As a consequence, starting with [11, p. 419 (51)], setting the exponent of $(\mathcal{R}_2, \mathcal{Z}; 1)$ equal to zero, we immediately determine that:

Theorem 2.2. *If $b_1 \geq \max\{e_0/(p-1), (pe_0 - p + 1)/(2p-1)\}$, then*

$$\begin{aligned}\mathfrak{O}_2 \cong{}& \mathcal{R}_2^{\lambda_{1,0}f} \oplus \mathcal{R}_1^{(2\lambda_{1,0}-\lceil\lambda_{2,1}/p\rceil)f} \oplus \mathcal{Z}^{(\lambda_{2,0}-e_0)f} \oplus \mathcal{E}^{(\lceil\lambda_{2,1}/p\rceil-\lambda_{1,0})f} \\ &\oplus (\mathcal{R}_2, \mathcal{E}; \lambda^{p-1})^{(e_0-\lceil\lambda_{2,1}/p\rceil)f} \oplus (\mathcal{R}_2, \mathcal{Z} \oplus \mathcal{R}_1; 1, \lambda^{p-2})^{(\lambda_{1,0}-\lambda_{2,0}+e_0)f} \\ &\oplus (\mathcal{R}_2, \mathcal{R}_1; \lambda^{p-2})^{(\lambda_{2,0}-2\lambda_{1,0}-e_0+\lceil\lambda_{2,1}/p\rceil)f}\end{aligned}$$

as $\mathbb{Z}_p[G]$-modules, where these modules are described in §A.3.

We conclude this section by strengthening Question A.

Question B: Is $\mathcal{S}_{C_{p^n}}$ finite? (This is only interesting for $n > 2$.)

This question is revised and discussed further in §7.

2.2. Stable Ramification. In this section we consider the first restriction of (1.2). Wyman proved that when a lower ramification number is large enough, subsequent ramification numbers are uniquely determined [15]:

$$(2.2)\quad b_i \geq p^{i-1}e_0/(p-1) \Longrightarrow b_j = b_i + p^i e_0(p^{j-i}-1)/(p-1),\quad i \leq j \leq n.$$

If the first ramification number is large enough, namely $b_1 \geq e_0/(p-1)$, one says that the extension is *stably ramified.*

Using (2.2) and (1.1), one may verify that under stable ramification,

$$(2.3)\qquad kp^m e_0 - \lambda_{m+k,m} = ke_0 - \lambda_{k,0},\quad 0 \leq m, m+k \leq n.$$

As a condition on the traces, this may be expressed as

$$|\mathrm{Tr}_{m+k,m}(\mathfrak{O}_{m+k})/p^k\mathfrak{O}_m| = |\mathrm{Tr}_{k,0}(\mathfrak{O}_k)/p^k\mathfrak{O}_0|.$$

If the extension is not stably ramified and K_0 contains a p-th root of unity, then the possible second lower ramification numbers, b_2, have been classified by Wyman [15, Thm 32]. A variety of second ramification numbers are possible, therefore to keep complications associated with the ramification filtration to a minimum it is prudent to assume stable ramification.

2.3. Maximal and Almost Maximal Ramification. If any of the lower ramification numbers are divisible by p, then $b_i = p^i e_0/(p-1)$ for each i [12, IV §2 Ex 3], and the extension is called *maximally ramified.* So long as the extension is *almost maximally ramified*, namely $b_1 + 1 \geq pe_0/(p-1)$, we may use [12, V §3] to find that

$$\frac{1}{p}\mathrm{Tr}_{i,i-1}(\mathfrak{O}_i) = \mathfrak{O}_{i-1},\quad i = 1, 2, \ldots, n.$$

In doing so, it is helpful to note that b_i is the ramification number of K_i/K_{i-1} [12, IV §3]. Therefore, under this condition the idempotent elements of $\mathbb{Q}_p[G]$ decompose the ring of integers:

$$\mathfrak{O}_n \cong \sum_{i=0}^{n} M_i,\ \text{ as } \mathbb{Z}_p[G]\text{-modules},$$

where $\Phi_{p^i}(\sigma)(M_i) = 0$. Each M_i may be viewed as a torsion–free module over the principal ideal domain, $R_i := \mathbb{Z}_p[G]/\langle\Phi_{p^i}(\sigma)\rangle$. Torsion–free modules over principal ideal domains are free [2, §4D] and so by checking $\mathbb{Z}_p$-ranks, we find that

$$\mathfrak{O}_n \cong \sum_{i=0}^{n} R_i^{e_0 f},\ \text{ as } \mathbb{Z}_p[G]\text{-modules}.$$

Note that under this severe restriction the ring of integers has a particularly simple Galois module structure.

Remark 2.3. As a consequence of this discussion, it only remains for us to determine the structure of the ring of integers for $b_1 < pe_0/(p-1) - 1$. Under this condition, the ramification numbers are relatively prime to p.

2.4. Generalizing "Almost Maximal": Near Maximal Ramification. The trace relationship which results from almost maximal ramification can be rewritten as $\mathrm{Tr}_{j,j-1}(\mathfrak{O}_j) = p\mathfrak{O}_{j-1}$. Since $\mathfrak{O}_{j-1} \subseteq \mathfrak{O}_j$ it is clearly always the case that $p\mathfrak{O}_{j-1} = \mathrm{Tr}_{j,j-1}(\mathfrak{O}_{j-1}) \subseteq \mathrm{Tr}_{j,j-1}(\mathfrak{O}_j)$. So if $\mathrm{Tr}_{j,j-1}(\mathfrak{O}_j) \neq p\mathfrak{O}_{j-1}$, it must be that $\mathrm{Tr}_{j,j-1}(\mathfrak{O}_j) \not\subseteq p\mathfrak{O}_{j-1}$; in other words, some of the elements in the image of the trace have valuation which is too small. To remedy this, one may increase valuation through application of $(\sigma - 1)$. This results in the following family of restrictions:

$$(\sigma-1)^t\mathrm{Tr}_{j,j-1}(\mathfrak{O}_j) \subseteq p\mathfrak{O}_{j-1}, \quad j = 1, 2, \dots, n.$$

The first case $t = 0$ is *almost maximal ramification.* The next case $t = 1$, that we call *near maximal ramification*, follows from stable ramification and $b_1 \geq (pe_0 - p + 1)/(2p-1)$.

Lemma 2.4. *Let the extension be stably ramified and let $t \geq 0$, then*

$$b_1 \geq \frac{pe_0 - p + 1}{(t+1)p - 1} \Longrightarrow (\sigma-1)^t\mathrm{Tr}_{j,j-1}(\mathfrak{O}_j) \subseteq p\mathfrak{O}_{j-1}, \quad j = 1, 2, \dots, n.$$

Remark 2.5. Compare with [11, Lem 3].

Proof. Note that the inclusion, $(\sigma-1)^t\mathrm{Tr}_{j,j-1}(\mathfrak{O}_j) \subseteq p\mathfrak{O}_{j-1}$, follows from the inequality, $\lambda_{j,j-1} + tb_1 \geq p^{j-1}e_0$. Because of (2.3) we may replace $\lambda_{j,j-1}$ in this inequality with $\lambda_{1,0} - e_0 + p^{j-1}e_0$, and work instead with $\lambda_{1,0} + tb_1 \geq e_0$. Clearly $\lambda_{1,0} = \lfloor((b_1+1)(p-1))/p\rfloor \geq e_0 - tb_1$ if and only if $((b_1+1)(p-1))/p \geq e_0 - tb_1$. One may easily check that this is equivalent to the hypothesis. □

Instead of emphasizing *near maximal ramification* as a generalization of almost maximal ramification, we can emphasize the analogy with [5]. In this section, we do for the second condition in (1.2) what [5] did for the third condition. First in Lemma 2.4, the second condition in (1.2) is interpreted as a relation among trace maps. Then we greatly simplify the argument in [11], and prove a much stronger result – already stated as Theorem 2.2. Of course, Theorem 2.2 was stated and proven earlier in this paper. The basis for that argument however, is [11, p. 419 (51)], a statement that is derived near the end of [11]. Here we outline an alternative approach which can be used to greatly simplify considerations throughout [11].

2.4.1. *Application: The Case p^2.* One may easily check that the trace relationship associated with near maximal ramification restricts the number of modules that can appear in $\mathfrak{O}_2$ from a list of $4p+1$ to the following list of nine: $\mathcal{Z}$, $\mathcal{R}_1$, $\mathcal{E}$, $\mathcal{R}_2$, $(\mathcal{R}_2, \mathcal{Z}; 1)$, $(\mathcal{R}_2, \mathcal{R}_1; \lambda^{p-2})$, $(\mathcal{R}_2, \mathcal{E}; \lambda^{p-1})$, $(\mathcal{R}_2, \mathcal{Z} \oplus$

$\mathcal{R}_1; 1, \lambda^{p-2})$, $(\mathcal{R}_2, \mathcal{Z} \oplus \mathcal{E}; 1, \lambda^{p-2})$. The notation comes from [2, Thm 34.32] and is consistent with the notation of [11]. The advantage of this restriction is clear: families of modules that arise as extensions (*e.g.* $(\mathcal{R}_2, \mathcal{R}_1; \lambda^i)$, $i = 0, 1, \ldots, p-2$) may contribute at most one member (*e.g.* $(\mathcal{R}_2, \mathcal{R}_1; \lambda^{p-2})$).

One may verify the following: if M is an indecomposable $\mathbb{Z}_p[C_{p^2}]$-module, then

$$\dim_{\mathbb{F}_p}(\Phi_p(\sigma) \cdot \mathrm{H}^{-1}(\langle \sigma^p \rangle, M)) = \begin{cases} 0 & M \not\cong \mathcal{E} \\ 1 & M \cong \mathcal{E} \end{cases} \tag{2.4}$$

where σ is a generator of C_{p^2} and $\mathrm{H}^{-1}(-,-)$ denotes Tate cohomology.

If one uses this property along with the other properties listed in [11, Table 2], one can start with the nine modules listed above and very easily derive Theorem 2.2.

2.5. Generalizing "almost maximal": rings with the same trace. Another way to express the trace relationship associated with almost maximal ramification is as $\mathrm{Tr}_{j,j-1}(\mathfrak{O}_j) = \mathrm{Tr}_{j,j-1}(\mathfrak{O}_{j-1})$. In this section we generalize this interpretation of the trace relationship. Alternatively, one may view this section as the development of a family of trace map conditions generalizing [5, Prop 1, p. 144], or as a generalization of the third restriction in (1.2).

Lemma 2.6. *Under Stable Ramification, if $b_k + 1 > p^k \lceil e_0/(p-1) \rceil - p^k$, then for all $m = 1, 2, 3, \ldots$*

1. $\lambda_{m+k+1,m} = \lambda_{m+k,m} + p^m e_0$.
2. $\mathrm{Tr}_{m+k+1,m}(\mathfrak{O}_{m+k+1}) = \mathrm{Tr}_{m+k+1,m}(\mathfrak{O}_{m+k})$.

Proof. One may easily check that these conditions are equivalent, so we need only prove 1. But first we note that $\lambda_{m+k,m} + p^m e_0 \geq \lambda_{m+k+1,m}$ regardless of ramification, since $\mathfrak{O}_{m+k} \subseteq \mathfrak{O}_{m+k+1}$ forces $\mathrm{Tr}_{m+k+1,m}(\mathfrak{O}_{m+k}) \subseteq \mathrm{Tr}_{m+k+1,m}(\mathfrak{O}_{m+k+1})$. So the restriction on the ramification numbers is only to force $\lambda_{m+k+1,m} \geq \lambda_{m+k,m} + p^m e_0$. Because of (2.3) we need only show that $\lambda_{k+1,0} \geq \lambda_{k,0} + e_0$. Using (1.1) and (2.2) one can check that $\lambda_{k+1,0} = k e_0 + b_1 + 1 + \lfloor (-b_{k+1} - 1)/p^{k+1} \rfloor$ while, $\lambda_{k,0} = (k-1)e_0 + b_1 + 1 + \lfloor (-b_k - 1)/p^k \rfloor$. Let $\delta := p^k \lceil e_0/(p-1) \rceil - (b_k + 1)$, then because of the assumption $\delta < p^k$. Therefore, we need only verify that if $q = \lceil e_0/(p-1) \rceil$ and $b_k + 1 = p^k q - \delta$ then

$$\left\lfloor \frac{-b_{k+1} - 1}{p^{k+1}} \right\rfloor \geq \left\lfloor \frac{-b_k - 1}{p^k} \right\rfloor . \tag{2.5}$$

Let $r := q(p-1) - e_0$ (so $0 \leq r \leq p-1$). Replace $-b_k - 1$ with $-p^k q + \delta$. Replace $-b_{k+1} - 1$ with $-p^k q - p^k e_0 + \delta$, and e_0 with $q(p-1) - r$. Equation (2.5) then follows immediately. □

Remark 2.7. To be able to talk about the "eventual behavior of k," consider a fully ramified $\mathbb{Z}_p$-extension. By [15], ramification in such an extension will eventually stabilize – there will be a $t \geq 0$ such that $b_t \geq p^t e_0/(p-1)$. Assuming stable ramification $b_1 \geq e_0/(p-1)$, note that as k grows the assumption $b_k + 1 > p^k \lceil e_0/(p-1) \rceil - p^k$ weakens. Once this assumption holds, note that condition 1. is equivalent to $(b_1+1)/p^k + e_0/(p-1) \cdot (1 - 1/p^{k-1}) > e_0/(p-1) \cdot (1-1/p^{k-1}) > \lceil e_0/(p-1) \rceil - 1$. This will clearly be true for large enough k. Therefore this type of condition is widespread. In any fully ramified $\mathbb{Z}_p$-extension, there is a threshold value k_0 such that for all $k \geq k_0$ and all $m \geq 1$ Condition 2. holds.

2.6. Traces on Quotient Rings: Strong Ramification. The action of $\mathrm{Tr}_{j,j-1}$ on $\mathfrak{O}_i/\mathfrak{O}_{i-1}$ is easy to describe for $j \geq i$. The trace acts via multiplication by p for $j > i$, and by 0 for $j = i$. In this section we extend this action to $j < i$. To do so, we identify $\mathrm{Tr}_{j,j-1}$ with $\Phi_{p^j}(\sigma)$ and instead study the effect of $\Phi_{p^j}(\sigma)$ upon $\mathfrak{O}_i/\mathfrak{O}_{i-1}$. The result of our study is the most important "trace" relation in our catalog. The ramification restriction associated with this relation, being stronger that others, will be called *strong ramification*.

From Remark 2.3, we may assume that all ramification numbers are relatively prime to p. Meanwhile from [12, IV §3], we know that the ramification number of K_j/K_{j-1}, is b_j. Let $\alpha \in K_n$ and $\gcd(v_n(\alpha), p) = 1$, then following [12, IV §2 Ex 3 (a)], we find that for $j < n$,

$$v_n((\sigma^{p^j} - 1)\alpha) = v_n(\alpha) + b_{j+1}. \tag{2.6}$$

Let us begin by considering the effect of $\Phi_p(\sigma)$ on $\mathfrak{O}_n$. Choose any $\alpha \in \mathfrak{O}_n$ such that $v_n(\alpha) \equiv b_1 \bmod p$. As one can easily show by repeated application of (2.6) $v_n(\Phi_p(\sigma)\alpha) = v_n((\sigma-1)^{p-1}\alpha) = v_n(\alpha) + (p-1)b_1 \equiv 0 \bmod p$. Therefore $\Phi_p(\sigma)\alpha$ may be expressed as a sum:

$$\Phi_p(\sigma)\alpha = \mu + \nu, \tag{2.7}$$

where $\mu \in \mathfrak{O}_{n-1}$, $\nu \in \mathfrak{O}_n$ and $v_n(\mu) = v_n(\Phi_p(\sigma)\alpha) < v_n(\nu)$. Assume for the purposes of this discussion that $\nu \neq 0$, so we may assume that $\gcd(v_n(\nu), p) = 1$. Since $\Phi_p(\sigma)\alpha \equiv \nu \bmod \mathfrak{O}_{n-1}$, knowing the valuation of ν means knowing the effect of the Galois action upon the valuation of $\overline{\alpha} \in \mathfrak{O}_n/\mathfrak{O}_{n-1}$. We are faced, therefore, with the following problem: How to determine the valuation of ν?

To solve this problem, we apply $(\sigma - 1)$ to both sides of (2.7), yielding

$$(\sigma^p - 1)\alpha = (\sigma - 1)\mu + (\sigma - 1)\nu.$$

Note that $v_n((\sigma^p-1)\alpha) = v_n(\alpha) + b_2$, $v_n((\sigma-1)\mu) \geq v_n(\mu) + pb_1$ and $v_n((\sigma-1)\nu) = v_n(\nu) + b_1$. If we assume that $b_2 < (2p-1)b_1$, then $v_n((\sigma^p - 1)\alpha) < v_n((\sigma-1)\mu)$, hence $v_n((\sigma^p-1)\alpha) = v_n((\sigma-1)\nu)$, and $v_n(\nu)$ is uniquely determined to be $v_n(\alpha) + (b_2 - b_1)$. Alternatively, if we assume

$b_2 > (2p-1)b_1$ and $v_n(\mu) \not\equiv 0 \bmod p^2$ so that $v_n((\sigma-1)\mu) = v_n(\mu) + pb_1$, then $v_n((\sigma^p - 1)\alpha) > v_n((\sigma-1)\mu)$, hence $v_n((\sigma-1)\mu) = v_n((\sigma-1)\nu)$, and $v_n(\nu)$ is uniquely determined to be $v_n(\alpha) + 2(p-1)b_1$. If on the other hand, neither condition is satisfied, we require additional information concerning α to determine the valuation of ν.

Clearly, we should assume one of the conditions, either $b_2 < (2p-1)b_1$ or $b_2 > (2p-1)b_1$. Under stable ramification these are equivalent to $b_1 > pe_0/(2p-2)$ and $b_1 < pe_0/(2p-2)$ respectively. All other restrictions on ramification have been lower bounds, so we choose $b_1 > pe_0/(2p-2)$. We will refer to this restriction as *strong ramification.* Note that *strong* implies both *stable* and *near maximal* ramification.

This discussion is generalized in the following Lemma:

Lemma 2.8. *Assume* $\gcd(p, b_1) = 1$, $b_1 \geq pe_0/(2p-2)$ *and* $k < j \leq n$. *Given* $\alpha \in \mathfrak{O}_j$ *and* $v_j(\alpha) \equiv b_1 \bmod p$ *there exists a* ν *of* $\mathfrak{O}_j$ *with* $v_j(\nu) = v_j(\alpha) + (b_{k+1} - b_k) \equiv v_n(\alpha) \bmod p$, *such that* $\Phi_{p^k}(\sigma)\alpha \equiv \nu \bmod \mathfrak{O}_{j-1}$. *In fact,* $\Phi_{p^k}(\sigma)\alpha = \nu + \mu$ *where* $\mu \in \mathfrak{O}_{j-1}$ *and* $v_j(\nu) - (pe_0 - (p-1)b_1) = v_j(\mu)$.

Proof. If $b_1 > 1/2 \cdot pe_0/(p-1)$, then using (2.2) $b_k > 1/2 \cdot p^k e_0/(p-1) \cdot (2 - p^{1-k}) \geq 1/2 \cdot p^k e_0/(p-1)$ for $k \geq 1$. Because $b_k > 1/2 \cdot p^k e_0/(p-1)$ and $b_{k+1} = b_k + p^k e_0$ we find that $b_{k+1} > (2p-1)b_k$. If $v_j(\alpha) \equiv b_1 \bmod p$, then $v_j(\Phi_{p^k}(\sigma)\alpha) = v_j(\alpha) + (p-1)b_k \equiv 0 \bmod p$. As a consequence, there exist elements $\mu \in \mathfrak{O}_{j-1}$, $\nu \in \mathfrak{O}_j$ such that $\Phi_{p^k}(\sigma)\alpha = \mu + \nu$ where $v_j(\mu) = v_j(\alpha) + (p-1)b_k < v_j(\nu)$. Then $(\sigma^{p^k} - 1)\alpha = (\sigma^{p^{k-1}} - 1)\mu + (\sigma^{p^{k-1}} - 1)\nu$. Since $b_{k+1} < (2p-1)b_k$, $v_j((\sigma^{p^k} - 1)\alpha) < v_j((\sigma^{p^{k-1}} - 1)\mu)$. So $v_j((\sigma^{p^k} - 1)\alpha) = v_j((\sigma^{p^{k-1}} - 1)\nu)$. Clearly $\nu \neq 0$. So α may be expressed as $\mu + \nu$ where $v_j(\mu) = v_j(\alpha) + (p-1)b_k < v_j(\nu)$ and $\gcd(v_j(\nu), p) = 1$. Now because $v_j((\sigma^{p^k} - 1)\alpha) = v_j((\sigma^{p^{k-1}} - 1)\nu)$, we have $\Phi_p(\sigma^{p^k})\alpha \equiv \nu \bmod \mathfrak{O}_{j-1}$ and $v_j(\nu) = v_j(\alpha) + (b_{k+1} - b_k)$. □

3. Galois generators

As mentioned in the abstract, we shall determine the $\mathbb{Z}_p[G]$-module structure of $\mathfrak{O}_n$ by exhibiting generators and describing their relations. In this section we determine the generators. The principal mechanism whereby we may conclude that a set generates is the following basic observation.

Remark 3.1. Let $\beta_i \in \mathfrak{O}_j$ be elements subject only to the condition $v_j(\beta_i) = i$. Then the set $\{\beta_i\}_{i=0}^{p^j e_0 - 1}$ is a basis for $\mathfrak{O}_j$ over $\mathfrak{O}_T$.

As a consequence of this remark, we will work principally over $\mathfrak{O}_T$, the ring of integers in the maximal unramified subfield of K_0. The most important part of our work, especially in this section, is our development of $\mathfrak{O}_T[G]$-generators for each quotient, $\mathfrak{O}_j/\mathfrak{O}_{j-1}$, $j = 1, \ldots, n$. The $\mathfrak{O}_T[G]$-generators for $\mathfrak{O}_n$ we achieve as a byproduct.

3.1. Quotient module generators. This section is devoted to the development of $\mathfrak{O}_T[G]$-generators for $\mathfrak{O}_j/\mathfrak{O}_{j-1}$. Since $\Phi_{p^j}(\sigma)\cdot\mathfrak{O}_j/\mathfrak{O}_{j-1}=0$, we may follow the discussion in §2.3, observing that the $\mathfrak{O}_T[G]$-structure of $\mathfrak{O}_j/\mathfrak{O}_{j-1}$ is really $\mathfrak{O}_T[G]/\langle\Phi_{p^j}(\sigma)\rangle$-structure. In other words, $\mathfrak{O}_j/\mathfrak{O}_{j-1}$ may be viewed as a module over $\mathfrak{O}_T[G]/\langle\Phi_{p^j}(\sigma)\rangle\cong\mathfrak{O}_T[\zeta_{p^j}]$, where ζ_{p^j} denotes a primitive p^j–th root of unity. Now $\mathfrak{O}_T[\zeta_{p^j}]$ is a principal ideal domain and modules over principal ideal domains are free, therefore

$$\mathfrak{O}_j/\mathfrak{O}_{j-1}\cong\mathfrak{O}_T[\zeta_{p^j}]^a,$$

for some exponent a, as $\mathfrak{O}_T[G]$-modules, where σ acts upon $\mathfrak{O}_T[\zeta_{p^j}]$ via multiplication by ζ_{p^j}. To determine the exponent, compare $\mathfrak{O}_T$-ranks. One finds that $a=e_0$. So it is appropriate to talk about a basis for $\mathfrak{O}_j/\mathfrak{O}_{j-1}$ over $\mathfrak{O}_T[\zeta_{p^j}]$. Since $\mathfrak{O}_T[G]$-structure is essentially $\mathfrak{O}_T[\zeta_{p^j}]$-structure we find it convenient to blur the distinction, and refer to a $\mathfrak{O}_T[\zeta_{p^j}]$-basis as an $\mathfrak{O}_T[G]$-basis. This should not cause too much confusion.

We will use stable ramification in this section and because of Remark 2.3 assume that the ramification numbers are all relatively prime to p. Our main tools are equation (2.6), and the consequence of strong ramification, Lemma 2.8.

3.1.1. *An $\mathfrak{O}_T$-basis for $\mathfrak{O}_j$.* Let $\alpha_{m,j}\in K_j$ with $v_j(\alpha_{m,j})=b_1+pm$. We leave it to the reader to check the valuations and verify that based upon Remark 3.1 and (2.6), the following elements provide an $\mathfrak{O}_T$-basis for $\mathfrak{O}_j$: $p\alpha_{m,j},(\sigma^{p^{j-1}}-1)p\alpha_{m,j},\dots,(\sigma^{p^{j-1}}-1)^{p-1}p\alpha_{m,j}$ for $0\le p^je_0+b_1+pm$ and $p^je_0+b_1+(p-1)b_j+pm<p^je_0$, and for each value of $t=1,2,\dots p-1$, the elements, $(\sigma^{p^{j-1}}-1)^t\alpha_{m,j},\dots(\sigma^{p^{j-1}}-1)^{p-1}\alpha_{m,j},p\alpha_{m,j},(\sigma^{p^{j-1}}-1)p\alpha_{m,j},\dots(\sigma^{p^{j-1}}-1)^{t-1}p\alpha_{m,j}$ for $0\le b_1+tb_j+pm$ and $p^je_0+b_1+(t-1)b_j+pm<p^je_0$.

3.1.2. *An $\mathfrak{O}_T[\sigma^{p^{j-1}}]$-basis for $\mathfrak{O}_j/\mathfrak{O}_{j-1}$.* Implicit in the $\mathfrak{O}_T$-basis that we just listed is the $\mathfrak{O}_T[\sigma^{p^{j-1}}]$-structure of $\mathfrak{O}_j$. See [3, p 631–633] for further details. We glean from these elements the following $\mathfrak{O}_T[\sigma^{p^{j-1}}]$-basis for $\mathfrak{O}_j/\mathfrak{O}_{j-1}$:

$$B:=\left\{p\alpha_{m,j}:-p^{j-1}e_0-\left\lfloor\frac{b_1}{p}\right\rfloor\le m\le-\left\lfloor\frac{b_1+(p-1)b_j}{p}\right\rfloor-1\right\}\cup \tag{3.1}$$
$$\bigcup_{t=1}^{p-1}\left\{(\sigma^{p^{j-1}}-1)^t\alpha_{m,j}:-\left\lfloor\frac{b_1+tb_j}{p}\right\rfloor\le m\le-\left\lfloor\frac{b_1+(t-1)b_j}{p}\right\rfloor-1\right\}.$$

So far we have only used stable ramification and the fact that the ramification numbers are relatively prime to p. In the following section we will use the assumption of strong ramification.

3.1.3. *An $\mathfrak{O}_T[\sigma]$-basis for $\mathfrak{O}_j/\mathfrak{O}_{j-1}$.* The elements in (3.1) certainly span $\mathfrak{O}_j/\mathfrak{O}_{j-1}$ over $\mathfrak{O}_T[G]$ since they span $\mathfrak{O}_j/\mathfrak{O}_{j-1}$ over a sub-ring. We need to discern among them now, selecting out only those elements which are necessary. The following lemma is our principal mechanism for doing so.

Lemma 3.2. *Assume that $1/2 \cdot pe_0/(p-1) < b_1 < pe_0/(p-1)$ and $j \geq 1$. Then for each $\alpha \in K_j$ where $v_j(\alpha) = b_1 + pm$, there is an element $\nu \in K_j$ with $v_j(\nu) = p^j e_0 + tb_j + pm \equiv tb_1 \bmod p$, and an element $\mu \in K_{j-1}$ with $v_j(\mu) = v_j(\nu) - (pe_0 - (p-1)b_1) = p(m + b_j)$, such that*

$$\frac{(\sigma^{p^{j-1}} - 1)^t}{(\sigma - 1)} p\alpha = (\sigma^{p^{j-1}} - 1)^{t-1} \Phi_{p^{j-1}}(\sigma)\Phi_{p^{j-2}}(\sigma) \cdots \Phi_{p^2}(\sigma)\Phi_p(\sigma) p\alpha$$
$$= \begin{cases} \nu + \mu & \text{for } t = 1, \\ \nu & \text{for } t = 2, 3, \dots, p-1. \end{cases}$$

Proof. This result is proven by repeated application of Lemma 2.8. Let $\alpha \in K_j$ with $v_j(\alpha) \equiv b_1 \bmod p$, and let $1 \leq r, s < j$. Then by Lemma 2.8, $\Phi_{p^r}(\sigma)\alpha = \nu_1 + \mu_1$ where $v_j(\nu_1) = v_j(\alpha) + (b_{r+1} - b_r)$ and $v_j(\mu_1) = v_j(\nu_1) - (pe_0 - (p-1)b_1)$. Using Lemma 2.8 again we find that $\Phi_{p^s}(\sigma)\nu_1 = \nu_* + \mu_*$ where $v_j(\nu_*) = v_j(\nu_1) + (b_{s+1} - b_s)$ and $v_j(\mu_*) = v_j(\nu_1) + (b_{s+1} - b_s) - (pe_0 - (p-1)b_1)$. Meanwhile $v_j(\Phi_{p^s}(\sigma)\mu_1) \geq v_j(\nu_1) - (pe_0 - (p-1)b_1) + p(p-1)b_s$. One may easily verify that under stable ramification $b_{s+1} - b_s < p(p-1)b_s$, therefore by renaming $\mu_2 := \mu_* + \Phi_{p^s}(\sigma)\mu_1$ and $\nu_2 = \nu_*$ we find that $\Phi_{p^s}(\sigma)\Phi_{p^r}(\sigma)\alpha = \nu_2 + \mu_2$ where $v_j(\nu_2) = v_j(\alpha) + (b_{r+1} - b_r) + (b_{s+1} - b_s)$ and $v_j(\mu_2) = v_j(\nu_2) - (pe_0 - (p-1)b_1)$. In this way we find that $\Phi_{p^{j-1}}(\sigma)\Phi_{p^{j-2}}(\sigma) \cdots \Phi_{p^{i+1}}(\sigma)\alpha = \nu + \mu$ where $v_j(\nu) = v_j(\alpha) + (b_j - b_{i+1})$, $\mu \in K_{j-1}$ and $v_j(\mu) = v_j(\nu) - (pe_0 - (p-1)b_1)$. Since $(\sigma^{p^{j-1}} - 1)\mu = 0$, we have our result when $t > 1$. $\square$

Later we will need a partial converse to Lemma 3.2. We state and prove it now.

Lemma 3.3. *Assume that $1/2 \cdot pe_0/(p-1) < b_1 < pe_0/(p-1)$ and $j \geq 1$. Given $\mu \in K_{j-1}$ with $v_{j-1}(\mu) = b_k + m$, then there are elements $\alpha, \nu \in K_j$ such that $v_j(\alpha) = b_1 + pm$, $v_j(\nu) = p^j e_0 + pm + b_j$ and*

$$\frac{(\sigma^{p^{j-1}} - 1)^p}{(\sigma - 1)} \alpha = \nu + \mu.$$

Proof. First we extend the above Lemma and prove that given $\alpha \in K_j$ with $v_j(\alpha) = b_1 + pm$ there are elements $\mu \in K_{j-1}$ and $\nu \in K_j$ with valuations as above, such that $(\sigma^{p^{j-1}} - 1)^p/(\sigma - 1) \cdot \alpha = \nu + \mu$. Note that $(\sigma^{p^{j-1}} - 1)^p/(\sigma - 1) = (\sigma^{p^{j-1}} - 1)^{p-1}\Phi_{p^{j-1}}(\sigma) \cdots \Phi_p(\sigma)$. Using the Binomial Theorem to expand $\sigma^{p^j} = ((\sigma^{p^{j-1}} - 1) + 1)^p$ then dividing by $(\sigma - 1)$, we find that

$$(\sigma^{p^{j-1}}-1)^{p-1}=\Phi_{p^j}(\sigma)-\sum_{t=0}^{p-2}\binom{p}{t+1}(\sigma^{p^{j-1}}-1)^t.$$

So $(\sigma^{p^{j-1}}-1)^{p-1}\alpha=\Phi_{p^j}(\sigma)\alpha-p\alpha-\sum_{t=1}^{p-2}\binom{p}{t+1}(\sigma^{p^{j-1}}-1)^t\alpha$. Using Lemma 3.2 we find that $\Phi_{p^{j-1}}(\sigma)\cdots\Phi_p(\sigma)p\alpha=\mu_0+\nu_0$ where $v_j(\mu_0)=p^je_0+pm+b_j-(pe_0-(p-1)b_1)$ and $v_j(\nu_0)=p^je_0+pm+b_j$. Furthermore $\Phi_{p^{j-1}}(\sigma)\cdots\Phi_p(\sigma)\binom{p}{t+1}(\sigma^{p^{j-1}}-1)^t\alpha=\nu_t$ where $v_j(\nu_0)=p^je_0+pm+tb_j>p^je_0+pm+b_j$. Now it is easy to show by using [12, V §3 Lemma 4] that $\Phi_{p^{j-1}}(\sigma)\cdots\Phi_p(\sigma)\cdot\Phi_{p^j}(\sigma)\alpha=\mu_{p-1}\in K_{j-1}$ where $v_j(\mu_{p-1})\geq b_1+pm+(p-1)b_j+p(p-1)b_{j-1}+\cdots+p^{j-1}(p-1)b_1>v_j(\mu_0)$. So let $\mu=\mu_0+\mu_{p-1}$ and $\nu=\sum_{t=0}^{p-2}\nu_t$ and we have the desired conclusion.

We are ready to prove this lemma. To prove this we start with $\alpha_0\in K_j$ such that $v_j(\alpha_0)=v_j(\mu)-(p^je_0+b_j-(pe_0-(p-1)b_1))+b_1$, and elements $\alpha_i\in K_j$ $i=1,2,\ldots,$ such that $v_j(\alpha_i)=v_j(\alpha_0)+pi$. Then $v_j(\alpha_i)\equiv b_1 \bmod p$ for $i=0,1,\ldots,$ and using Lemma 3.2 we find that there are elements $\mu_i\in K_{j-1}$, $\nu_i\in K_j$ such that $(\sigma^{p^{j-1}}-1)^p/(\sigma-1)\cdot\alpha_i=\nu_i+\mu_i$, $v_{j-1}(\mu_i)=v_{j-1}(\mu)+i$. So there must be units $u_i\in\mathfrak{O}_0$ such that $\mu=\sum_{i=0}^{\infty}u_i\mu_i$. Let $\alpha=\sum_{i=0}^{\infty}u_i\alpha_i$ and $\nu=\sum_{i=0}^{\infty}u_i\nu_i$. The lemma follows. □

As a consequence of Lemma 3.2 we may prove the following which is the main result of this section.

Lemma 3.4. *Assume that $1/2\cdot pe_0/(p-1)<b_1<pe_0/(p-1)$ and $j\geq 1$. Let*

$$\mathcal{B}_{j,0}:=\left\{p\alpha_{m,j}:-p^{j-1}e_0-\left\lfloor\frac{b_1}{p}\right\rfloor\leq m\leq-\left\lfloor\frac{b_1+(p-1)b_j}{p}\right\rfloor-1\right\},$$
$$\mathcal{B}_{j,t}:=\left\{(\sigma^{p^{j-1}}-1)^t\alpha_{m,j}:-\left\lfloor\frac{b_1+tb_j}{p}\right\rfloor\leq m\leq-\left\lfloor\frac{tb_j}{p}\right\rfloor-1\right\}.$$

Then the union of these sets, namely $\mathcal{B}_j:=\bigcup_{t=0}^{p-1}\mathcal{B}_{j,t}$, is an $\mathfrak{O}_T[G]$-basis for $\mathfrak{O}_j/\mathfrak{O}_{j-1}$. Furthermore if $\beta\in\mathcal{B}_{j,t}$, then $v_j(\beta)\equiv(t+1)b_1 \bmod p$ and

$$\frac{(\sigma^{p^{j-1}}-1)^{p-1}}{(\sigma-1)}\cdot\beta=\begin{cases}\nu+\mu & \text{for } \beta\in\mathcal{B}_{j,1}\\ \nu & \text{for } \beta\in\mathcal{B}_{j,t}, t\notin\{0,1\}\end{cases}$$

where $\nu\in\mathfrak{O}_j$, $\mu\in\mathfrak{O}_{j-1}$, $v_j(\nu)=v_j(\beta)+p^je_0-b_1$ and $v_j(\mu)=v_j(\nu)-(pe_0-(p-1)b_1)$.

Proof. From our earlier discussion, we know to look among the elements of (3.1) for e_0 elements which form a basis for $\mathfrak{O}_j/\mathfrak{O}_{j-1}$ over $\mathfrak{O}_T[G]/\langle\Phi_{p^j}(\sigma)\rangle$.

Note that any element of $\beta \in B$ such that

$$(\sigma-1)^{\phi(p^j)-1}\beta \equiv \frac{(\sigma^{p^{j-1}}-1)^{p-1}}{(\sigma-1)}\beta \equiv 0 \bmod (\mathfrak{O}_{j-1}+p\mathfrak{O}_j)$$

can not be in this basis. We combine this observation and Lemma 3.2 now. Considering those elements in B of the form $p\alpha_{m,j}$, we easily eliminate all elements except those in $\mathcal{B}_{j,0}$. Now we consider those elements of the form $(\sigma^{p^{j-1}}-1)^t\alpha_{m,j} \in B$. Using the Binomial Theorem as we did in the proof of Lemma 3.3, we find that $(\sigma^{p^{j-1}}-1)^{p-1} = \Phi_{p^j}(\sigma) + \sum_{i=1}^{p-1}\binom{p}{i}(\sigma^{p^{j-1}}-1)^{i-1}$. So to determine the effect of $(\sigma^{p^{j-1}}-1)^{p-2}\Phi_{p^{j-1}}(\sigma)\cdots\Phi_p(\sigma)$ on $(\sigma^{p^{j-1}}-1)^t\alpha_{m,j} \in \mathfrak{O}_j/\mathfrak{O}_{j-1}$, it is clear that we need only determine $(\sigma^{p^{j-1}}-1)^{t-1}\Phi_{p^{j-1}}(\sigma)\cdots\Phi_p(\sigma)p\alpha_{m,j} \in \mathfrak{O}_j/\mathfrak{O}_{j-1}$. Because of this and Lemma 3.2 we eliminate all elements $(\sigma^{p^{j-1}}-1)^t\alpha_{m,j} \in B$, except for those listed in $\mathcal{B}_{j,t}$. The Lemma now follows, as it is easily shown that the elements which remain, namely $\mathcal{B}_j$, continue to span $\mathfrak{O}_j/\mathfrak{O}_{j-1}$ over $\mathfrak{O}_T[G]$; furthermore, exactly e_0 elements remain. □

3.2. Galois generators for the ring of integers. This section summarizes our accomplishments thus far. For each $0 \le m \le e_0-1$ choose an $\alpha \in \mathfrak{O}_0$ with $v_0(\alpha)=m$. Let the set of such α be called $\mathcal{B}_0$.

Proposition 3.5. *Assume that $1/2\cdot pe_0/(p-1) < b_1 < pe_0/(p-1)$, and that the sets $\mathcal{B}_j$ for $j=1,2,\dots,n$ are defined as in* Lemma 3.4. *Then $\mathcal{B}=\cup_{j=0}^n\mathcal{B}_j$ generates $\mathfrak{O}_n$ over $\mathfrak{O}_T[G]$:*

$$\mathfrak{O}_n = \sum_{\beta\in\mathcal{B}}\mathfrak{O}_T[G]\cdot\beta.$$

Proof. This is clear. □

4. Galois relationships

From the previous section we inherit $\mathfrak{O}_T[G]$-generators for $\mathfrak{O}_n$. These generators are not yet, however, completely suited to our needs. When selecting these elements, we did not consider Galois inter–relationships. In fact, they were selected based upon their valuation alone. To remedy this fact, in this section we choose certain of these elements again, this time paying attention to Galois relationships. When we are done, we will not only have $\mathfrak{O}_T[G]$-generators for $\mathfrak{O}_n$, but also have their $\mathfrak{O}_T[G]$-relationships.

4.1. Galois relationships: outline of approach. We proceed inductively, first assuming that the Galois relationships among the elements of $\mathfrak{O}_{n-1}$ are known, then determining the Galois relationships among the elements of $\mathfrak{O}_n$. As there are a number of issues associated with illuminating and then disentangling these Galois relationships, we discuss the process first.

4.1.1. *Form of Galois relation.* Consider the canonical short–exact sequence

$$0 \longrightarrow \mathfrak{O}_{n-1} \xrightarrow{i} \mathfrak{O}_n \xrightarrow{\pi} \mathfrak{O}_n/\mathfrak{O}_{n-1} \longrightarrow 0,$$

where i refers to the injection and π refers to the natural projection. Since $\mathfrak{O}_n/\mathfrak{O}_{n-1}$ is free over $\mathfrak{O}_T[G]/\langle\Phi_{p^n}(\sigma)\rangle$, the elements of $\mathfrak{O}_n/\mathfrak{O}_{n-1}$, namely $\pi(\alpha)$ for $\alpha \in \mathfrak{O}_n$, satisfy the equation $\Phi_{p^n}(\sigma)\pi(\alpha) = 0$. Meanwhile since the generators of $\mathfrak{O}_n/\mathfrak{O}_{n-1}$, $\alpha \in \mathcal{B}_n$, are also a basis they satisfy only this one equation. Now $\Phi_{p^n}(\sigma)\alpha \in \mathfrak{O}_{n-1}$ and assuming that we can express any element of $\mathfrak{O}_{n-1}$ in terms of the generators of $\mathfrak{O}_{n-1}$, the Galois relationships among the elements of $\mathfrak{O}_n$ which are not already in $\mathfrak{O}_{n-1}$ will all be expressions of the form

$$\Phi_{p^n}(\sigma)\alpha = \sum_{j=0}^{n-1}\sum_{\beta\in\mathcal{B}_j} f_\beta(\sigma)\beta \text{ for some } f_\beta(\sigma) \in \mathfrak{O}_T[G]. \tag{4.1}$$

Since $\Phi_{p^n}(\sigma)\mathfrak{O}_{n-1} = p\mathfrak{O}_{n-1}$, a change of a generator α by an element of $\mathfrak{O}_{n-1}$ will change the right–hand–side of (4.1) by an element of $p\mathfrak{O}_{n-1}$ and so these expressions are only significant modulo $p\mathfrak{O}_{n-1}$. However if for each $\alpha \in \mathcal{B}_n$, the right–hand–side of this expression was determined modulo $p\mathfrak{O}_{n-1}$, the Galois module structure of $\mathfrak{O}_n$ would be completely determined by induction.

4.1.2. *Valuation and the Galois relations.* In this section we assume that the ramification numbers are relatively prime to p and describe a process whereby the right–hand–sides of the expressions in (4.1) may be determined.

Based upon their expression in Lemma 3.4, it is clear that all elements of $\mathcal{B}_n$ besides those in $\mathcal{B}_{n,0}$ map to zero under the trace; thus resulting in trivial right–hand–sides. This leaves us to determine the right–hand–side of (4.1) for each $\alpha \in \mathcal{B}_{n,0}$. But if for each $\lambda_{n,n-1} \le i \le p^{n-1}e_0 - 1$ we had Galois expressions for elements $\nu_i \in \mathfrak{O}_{n-1}$ with $v_{n-1}(\nu_i) = i$, then we could use the following result, Lemma 4.1, to choose the elements of $\mathcal{B}_{n,0}$ again. In other words, we can first determine the right–hand–sides for (4.1) and then find α to provide the left–hand–side of the equation.

Lemma 4.1. *Given any element $\nu \in K_{j-1}$ with valuation, $v_{j-1}(\nu) = i$, there is an element $\alpha \in K_j$ with valuation, $v_j(\alpha) = pi - (p-1)b_j$, such that $\mathrm{Tr}_{j,j-1}(\alpha) = \nu$.*

Proof. The ramification number of K_j/K_{j-1} is b_j. Use this, the fact that the trace maps fractional ideals of $\mathfrak{O}_j$ to fractional ideals of $\mathfrak{O}_{j-1}$ [12, V §3 Lem 4], and the lemma follows. $\square$

Based upon this observation, we are left to find expressions, in terms of the Galois generators of $\mathfrak{O}_{n-1}$, for each valuation i in $\lambda_{n,n-1} \leq i \leq p^{n-1}e_0 - 1$.

4.1.3. *Preview: expressing ν_i.* The observations in this subsection depend explicitly upon *strong ramification*, and implicitly upon *near maximal ramification*. Note that near maximal ramification means that $(\sigma-1)\cdot\mathrm{Tr}_{n,n-1}\alpha \in p\mathfrak{O}_{n-1}$ for every $\alpha \in \mathcal{B}_n$. Hence $(\sigma-1)\nu_i \in p\mathfrak{O}_{n-1}$, and so $\overline{\nu_i} \in \mathfrak{O}_{n-1}/p\mathfrak{O}_{n-1}$ must lie in the submodule of $\mathfrak{O}_{n-1}/p\mathfrak{O}_{n-1}$ killed by $(\sigma-1)$. What are the generators of that submodule?

We turn to the consequence of near maximal ramification, Proposition 3.5, and the generators of $\mathfrak{O}_{n-1}$ to address this question. Certainly the elements $(\sigma^{p^j}-1)^{p-1}/(\sigma-1)\cdot\overline{\beta}$ for $\beta \in \mathcal{B}_{j,t}$ where $t \neq 0$ lie in this module. Meanwhile the elements $\Phi_{p^j}(\sigma)\cdot\overline{\beta}$ for $\beta \in \mathcal{B}_{j,0}$ also lie in this module. So we might expect that ν_i be expressible in terms of

$$\bigcup_{j=1}^{n-1}\left(\bigcup_{t\neq 0}\frac{(\sigma^{p^{j-1}}-1)^{p-1}}{(\sigma-1)}\cdot\mathcal{B}_{j,t}\cup\Phi_{p^j}(\sigma)\mathcal{B}_{j,0}\right). \tag{4.2}$$

However the $\Phi_{p^j}(\sigma)\cdot\beta$ for $\beta \in \mathcal{B}_{j,0}$ are, in turn, expressible in terms of the Galois generators of $\mathfrak{O}_{j-1}$, and so expressions of the form $\Phi_{p^j}(\sigma)\mathcal{B}_{j,0}$ are not necessary and may be eliminated from this union.

To determine which of the members of (4.2) explicitly appear in the description of a particular ν_i we make use of *strong ramification*. But first note that since elements in $\mathfrak{O}_{n-2}$ have valuation, v_{n-1}, equivalent to zero modulo p, it might seem that the residue class modulo p of i should influence our expression for ν_i. Indeed it does; our expression for ν_i will depend initially upon one of the following three conditions: $i \equiv 0 \bmod p$, $i \equiv b_1 \bmod p$, and $i \not\equiv 0, b_1 \bmod p$. Ultimately, it will depend upon a partial p-adic expansion for i.

Of the three conditions, the last is most easily explained. Using *strong ramification* and its consequence Lemma 3.2, ν_i may be chosen to be $(\sigma^{p^{n-1}}-1)^{p-1}/(p-1)\beta$ for some $\beta \in \cup_{t=1}^{p-1}\mathcal{B}_{n-1,t}$. This may be accomplished without placing any additional restriction on β besides valuation. The condition $i \equiv 0 \bmod p$ is also easily explained. Because of Lemma 2.1 there is an element of $\mathrm{Tr}_{n-1,n-2}(\mathfrak{O}_{n-1})$ with valuation, v_{n-1}, equal to i. Therefore, by induction we may assume that there is an expression in terms of the Galois generators for $\mathfrak{O}_{n-2}$ with valuation i. Use this expression for ν_i.

This leaves the condition $i \equiv b_1 \bmod p$. Because of Lemma 3.2, there is an element $\beta \in \mathcal{B}_{n-1,1}$ such that $(\sigma^{p^{n-1}}-1)^{p-1}/(p-1)\beta = \mu + \nu$ where ν has valuation i. So we may choose $\nu_i := \nu$. We need to tidy up one loose end. What is the expression in terms of Galois generators for μ? We know that $\mu \in \mathfrak{O}_{n-2}$. If we had an expression in $\mathfrak{O}_{n-2}$ with the same valuation as μ (call the expression μ'), then we could use Lemma 3.3, to replace β with a new Galois generator, β', for $\mathfrak{O}_{n-1}/\mathfrak{O}_{n-2}$ and replace ν_i with another element, ν_i', of equivalent valuation so that $\nu_i' = (\sigma^{p^{n-1}}-1)^{p-1}/(p-1)\beta'+\mu'$. At that point, we would have an element with valuation i which is expressed in terms of a new set of Galois generators for $\mathfrak{O}_{n-1}$.

Of course, we still need to find an expression among the Galois generators of $\mathfrak{O}_{n-2}$ with the same valuation as μ. As it turns out this expression depends on the residue class of its valuation. In fact, there are three cases. As one might imagine, when $v_{n-2}(\mu) \equiv b_1 \bmod p$, we will need to express μ itself in terms of a sum – one of these terms expressed in terms of a Galois generator for $\mathfrak{O}_{n-2}/\mathfrak{O}_{n-3}$, the other term an element of $\mathfrak{O}_{n-3}$. At this point it is clear that the ν_i could have a rather long expression as a sum of generators from different quotient rings, the coefficients of which are of the form: $(\sigma^{p^j}-1)^{p-1}/(p-1)$ for some j.

4.2. The Recursive selection of the Galois generators. Consider the sequence with t–th term:

$$s_t(j) := \frac{1}{p^t}\left[p^{j-1+t}e_0 - 1 + \frac{p^t-1}{p-1}(pe_0-(p-1)b_1)\right]. \tag{4.3}$$

Recall that by Remark 2.3 we may assume that $b_1 < pe_0/(p-1)$. Since $pe_0-(p-1)b_1 > 0$, it is easily shown that the sequence, $\{s_t(j) : t = 1, \dots\}$, decreases as t increases with limit $s_\infty(j) := p^{j-1}e_0 + b_1 - pe_0/(p-1)$. Therefore $s_\infty(j) < s_1(j)$. The significance of this sequence will be made clear later. For now note that under stable ramification, $0 \le s_\infty(j)$ for $j \ge 1$.

In this section, our goal is the following: To determine for each integer i with $s_\infty(j) < i < p^{j-1}e_0$ an element ν_i with valuation $v_{j-1}(\nu_i) = i$ along with its explicit expression in terms of our generators (*i.e* an explicit linear combination of elements from $\cup_{k=0}^{j-1}\mathcal{B}_k$ along with with coefficients from $\mathfrak{O}_T[G]$).

For emphasis, we state this again. We would like to prove that:

Statement 4.2. For each integer i with $s_\infty(j) < i < p^{j-1}e_0$ there is an element $\nu_i \in \mathfrak{O}_{j-1}$ with valuation $v_{j-1}(\nu_i) = i$, and an explicit linear combination of elements from $\cup_{k=0}^{j-1}\mathcal{B}_k$ with coefficients from $\mathfrak{O}_T[G]$ that equals ν_i.

Clearly Statement 4.2 holds for $j = 1$: For each integer i with $s_\infty(1) < i < e_0$ there is an element α of $\mathcal{B}_0$ with valuation $v_0(\alpha) = i$. To prove the Statement 4.2 holds for $j > 1$ and to provide these explicit linear combinations, we proceed inductively. Note that at each step, we may need to re–select certain elements of $\mathcal{B}_j$, based upon previous selections (*i.e.* the elements of $\cup_{k=0}^{j-1}\mathcal{B}_k$).

4.2.1. *Selection of the elements of* $\mathcal{B}_{j,t}$. For emphasis, we point out that the elements in $\mathcal{B}_{j,t}$ for $t = 2, 3, \dots, p-1$ are chosen based upon valuation alone. There is no need to replace the elements given in §3.

The first elements that we replace are those in $\mathcal{B}_{j,0}$. We do so based upon a subset of the elements provided by Statement 4.2, namely those $\nu_i \in \mathfrak{O}_{j-1}$ with $\lambda_{j,j-1} \le i < p^{j-1}e_0$. Note that $s_\infty(j) \le \lambda_{j,j-1}$. We use Lemma 4.1. Based upon ν_i we choose $p\alpha_{j,m} \in \mathcal{B}_{j,0}$ where $m = i - b_1 - 2p^{j-1}e_0 + e_0$. Is is easily checked that these bounds on i correspond with the bounds on m in Lemma 3.4.

Now, we choose elements in $\mathcal{B}_{j,1}$, based upon the ν_i provided by Statement 4.2 with $s_\infty(j) < i < s_1(j)$. Our main tool is Lemma 3.3. Since the notation used in this lemma refers to the elements in $\mathfrak{O}_{j-1}$ as μ's, we relabel our elements in $\mathfrak{O}_{j-1}$ referring to them as μ_i instead of ν_i. So we may say that we replace elements of $\mathcal{B}_{j,1}$ based upon the $\mu_i \in \mathfrak{O}_{j-1}$ given by Statement 4.2 with $v_{j-1}(\mu_i) = i$ and $s_\infty(j) < i < s_1(j)$. Given a μ_i, Lemma 3.3 provides elements α and $\nu \in \mathfrak{O}_j$ such that $v_j(\alpha) = b_1 + pm$, $v_j(\nu) = p^j e_0 + pm + b_j$, and

$$\frac{(\sigma^{p^{j-1}} - 1)^{p-1}}{(\sigma - 1)} \cdot (\sigma^{p^{j-1}} - 1)\alpha = \nu + \mu_i,$$

where $m = i - b_j$. In this way the elements $(\sigma^{p^{j-1}} - 1)\alpha_{m,j} \in \mathcal{B}_{j,1}$ are defined for $s_\infty(j) - b_j < m \le -\lfloor b_j/p \rfloor - 1$. For emphasis, we repeat this. Only those elements $(\sigma^{p^{j-1}} - 1)\alpha_{m,j} \in \mathcal{B}_{j,1}$ with

$$-\left\lfloor \frac{b_j + b_1}{p} \right\rfloor \le -\left\lfloor \frac{p^{j-1}e_0}{p-1} \right\rfloor \le m \le -\left\lfloor \frac{b_j}{p} \right\rfloor - 1$$

are redefined. All other elements in $\mathcal{B}_{j-1}$ are left as they were in §3. One may check that since $b_1 > 1/2 \cdot pe_0/(p-1)$, $s_\infty(j) - b_j > -\lfloor (b_1 + b_j)/p \rfloor - 1$, so this really refers to a subset of $\mathcal{B}_{j,1}$.

We have defined all of the elements in $\mathcal{B}_{j,0}$ and some of the elements in $\mathcal{B}_{j,1}$ again in terms of elements in $\mathfrak{O}_{j-1}$. In the following lemma we show that the elements in $\mathfrak{O}_{j-1}$ which give rise to $\mathcal{B}_{j,0}$ are disjoint from the elements that give rise to $\mathcal{B}_{j,1}$. In other words, $s_1(j) < \lambda_{j,j-1}$.

Lemma 4.3. *If* $e_0/(p-1) \le b_1 < pe_0/(p-1)$ *then* $p^j e_0 - (pe_0 - (p-1)b_1) < p\lambda_{j,j-1}$.

Proof. From (2.3) $\lambda_{j,j-1} = p^{j-1}e_0 - e_0 + \lambda_{1,0}$. This lemma is therefore equivalent to the statement that $(p-1)b_1 < p\lambda_{1,0}$. Since $\lambda_{1,0} = b_1 - \lfloor b_1/p \rfloor$, the lemma reduces to $\lfloor b_1/p \rfloor < b_1/p$, which is clear, since $p \nmid b_1$. $\square$

4.2.2. *Proof that* Statement 4.2 *holds with j instead of $j-1$.* First consider those $i \equiv 0 \bmod p$ with $p^je_0 + b_1 - pe_0/(p-1) < i < p^je_0$. Let $i = pj$, then $p^{j-1}e_0 - (pe_0/(p-1) - b_1) < p^{j-1}e_0 - (pe_0/(p-1) - b_1)/p < j < p^{j-1}e_0$, and if Statement 4.2 holds for $j-1$, then there are elements in $\mathfrak{O}_{j-1} \subseteq \mathfrak{O}_j$ with valuation j expressed in terms of the Galois generators of $\mathfrak{O}_{j-1}$.

The only new expressions occur when $i \not\equiv 0 \bmod p$. Based upon Lemma 3.4, as long as $i \not\equiv 0, b_1 \bmod p$, there is an element $\beta \in \cup_{t=2}^{p-1}\mathcal{B}_{j,t}$ so that $(\sigma^{p^{j-1}}-1)^{p-1}/(p-1)\beta$ has valuation i. Observe that $\{v_j((\sigma^{p^{j-1}}-1)^{p-1}/(p-1)\beta) : \beta \in \cup_{t=2}^{p-1}\mathcal{B}_{j,t}\}$ is the set of all integers $i \not\equiv 0, b_1 \bmod p$, $p^je_0 - b_1 < i < p^je_0$. Because $b_1 > 1/2 \cdot pe_0/(p-1)$, $p^je_0 - b_1 < p^je_0 + b_1 - pe_0/(p-1)$.

We have expressed all integers $i \not\equiv b_1 \bmod p$ in the range $p^je_0 + b_1 - pe_0/(p-1) < i < p^je_0$ in terms of the Galois generators for $\mathfrak{O}_j$. But we have not as yet created any new Galois expressions based upon the old ones provided by Statement 4.2. Now consider $i \equiv b_1 \bmod p$. One may check that for each such integer there are elements $\beta \in \mathcal{B}_{j,0}$ and $\mu \in \mathfrak{O}_{j-1}$ such that the expression for μ in terms of the Galois generators of $\mathfrak{O}_{j-1}$ is given, and $\nu = (\sigma^{p^{j-1}} - 1)^{p-1}/(p-1)\beta - \mu$.

4.3. Description of the Galois relationships. Now that we have recursively defined the elements of $\mathcal{B}$ to be compatible, we describe their relationships. Given an element $\nu_i \in \mathfrak{O}_{n-1}$ with $v_{n-1}(\nu_i) = i$ where $\lambda_{n,n-1} \leq i < p^{n-1}e_0$, we find that there are basically two different ways of expressing ν_i in terms of the Galois generators for $\mathfrak{O}_n$. One of these expressions is in terms of the $\mathcal{B}_{j,t}$ where $t \neq 0$, while the other expression is in terms of the $\mathcal{B}_{j,0}$. The complexity of each expression depends on the p-adic expansion of i.

4.3.1. *Expressing ν_i in terms of the $\mathcal{B}_{j,t}$ where $t \neq 0$.* We proceed now and describe the expression for a given $\nu_i \in \mathfrak{O}_{n-1}$ with $v_{n-1}(\nu_i) = i$ where $\lambda_{n,n-1} \leq i < p^{n-1}e_0$. First we examine the p-adic expansion of i. We are interested in only certain of its features, and so we express this p-adic expansion in a particular way.

Let $\mathfrak{b} = pe_0 - (p-1)b_1$. Note $\mathfrak{b} \equiv b_1 \bmod p$. Let $\overline{\mathfrak{b}}$ be the least nonnegative residue of $\mathfrak{b}$ modulo p, and let A be the usual set of residues modulo p, except $\overline{\mathfrak{b}}$ is replaced with $\mathfrak{b}$. So $A := \big(\{0, 1, 2, \dots, p-1\} - \{\overline{\mathfrak{b}}\}\big) \cup \{\mathfrak{b}\}$. Each integer $i \geq 0$ has a unique finite p-adic representation with coefficients in A:

$$i = c_0 + c_1p + c_2p^2 + \cdots + c_jp^j,\ c_k \in A,\ c_j \neq 0.$$

Let m be the smallest subscript with $c_m \notin \{0, \mathfrak{b}\}$ or $n-1$, whichever is smaller. In other words, let

$$m = \min\left(\{k : c_k \notin \{0, \mathfrak{b}\}\} \cup \{n-1\}\right).$$

We now have a special p-adic expression for i:

$$i = c_0 + c_1 p + c_2 p^2 + \cdots + c_{m-1} p^{m-1} + C p^m, \tag{4.4}$$

where each c_k belongs to $\{0, \mathfrak{b}\}$, and $C \not\equiv 0, b_1 \bmod p$ unless $m = n-1$ in which case there is no restriction on C.

Now that we have a p-adic expression associated with i, we will use it to associate with i an element $\nu_i \in \mathfrak{O}_n$, where $v_n(\nu_i) = i$. We will do so in such a way that the expression for ν_i in terms of our Galois basis is transparent. Our conclusions are captured in the following lemma:

Lemma 4.4. *For each integer i with $\lambda_{n,n-1} \leq i \leq p^{n-1}e_0$ there are elements $\beta_{n-k-1} \in \mathcal{B}_{n-k-1}$ and $f_k(\sigma) \in \mathbb{Z}_p[G]$ so that*

$$\nu_i =: \sum_{k=0}^{m} f_k(\sigma) \cdot \beta_{n-k-1} \text{ has valuation } v_{n-1}(\nu_i) = i.$$

These elements are determined by the p-adic expression for i given in (4.4). *For $k < m$, either $c_k = \mathfrak{b}$ and β_{n-k-1} lies in $\mathcal{B}_{n-k-1,1}$, or $c_k = 0$ and $\beta_{n-k-1} = 0$. For $k = m$, either $m = n-1$ and β_0 lies in $\mathcal{B}_0$ without restriction, or $m < n-1$ and β_{n-m-1} lies in $\mathcal{B}_{n-m-1,t}$ for some $t \notin \{0,1\}$. Meanwhile $f_{n-1}(\sigma) := 1$ and $f_k(\sigma) := (\sigma^{p^{n-k-2}} - 1)^{p-1}/(\sigma - 1)$ for $k < n-1$.*

Proof. This sum is clearly what we were referring to at the end of §4.1.3. The only question which we must answer, now, is whether we recursively defined, back in §4.2, enough of the elements of $\mathcal{B}_{j,1}$ for $j = 1, \ldots, n-1$. The limit, $s_\infty(j)$, of the sequence (4.2) was instrumental in our recursive definition, although its significance was not explained. We correct that omission now.

Consider the situation where all the coefficients in the p-adic expression for i are $\mathfrak{b}$, $i = \sum_{k=0}^{m} \mathfrak{b} p^k$. In a sense, this is the worst case. Since ν_i lies non–trivially in the image of the trace, $\mathrm{Tr}_{n,n-1}\mathfrak{O}_n$, we have $\lambda_{n,n-1} \leq i < p^{n-1}e_0$. Because of Lemma 4.3 we find that $p^n e_0 - 1 - \mathfrak{b} < pi < p^n e_0$. Since $i \equiv b_1 \bmod p$, $\nu_i = (\sigma^{p^{n-1}} - 1)^{p-1}/(\sigma - 1)\beta + \mu_{n-2}$ for some $\beta \in \mathcal{B}_{n-1,1}$ and $\mu_{n-2} \in \mathfrak{O}_{n-2}$. The valuation of $v_{n-2}(\mu_{n-2}) \equiv b_1 \bmod p$ and $s_\infty(n-1) < s_2(n-1) = p^{-2}(p^n e_0 - 1 - \mathfrak{b} - p\mathfrak{b}) < v_{n-2}(\mu_{n-2}) < p^{n-2}e_0$. So because of our recursive definition, there are elements $\beta \in \mathcal{B}_{n-2,1}$ and $\mu_{n-3} \in \mathfrak{O}_{n-3}$ such that $\mu_{n-2} = (\sigma^{p^{n-2}} - 1)^{p-1}/(\sigma - 1)\beta + \mu_{n-3}$. Furthermore $s_\infty(n-2) < s_3(n-2) = p^{-3}(p^n e_0 - 1 - \mathfrak{b} - p\mathfrak{b} - p^2\mathfrak{b}) < v_{n-3}(\mu_{n-3}) < p^{n-3}e_0$, and $v_{n-3}(\mu_{n-3}) \equiv b_1 \bmod p$, and so μ_{n-3} is expressed similarly. Based upon this discussion, the significance of the sequence, $s_t(j)$, is clear. Moreover the lemma is clear. □

4.3.2. *Expressing ν_i in terms of $\mathcal{B}_{j,0}$.* We have observed earlier that if $i \equiv 0 \bmod p$ then we may choose, $\nu_i \in \mathfrak{O}_{n-2}$. Because of the Universal Trace Relation described in Lemma 2.1, we may assume that ν_i is $\mathrm{Tr}_{n-1,n-2}\beta_{n-1}$

for some $\beta_{n-1} \in \mathcal{B}_{n-1,1}$. So $\mathrm{Tr}_{n,n-1}\beta_n = \mathrm{Tr}_{n-1,n-2}\beta_{n-1} = \nu_i$ for some $\beta_n \in \mathcal{B}_{n,1}$. Furthermore, if $i \equiv 0 \bmod p^2$ then we may choose, $\nu_i \in \mathfrak{O}_{n-3}$. In this case, because of Lemma 2.1 there will be elements $\beta_n \in \mathcal{B}_{n,1}$, $\beta_{n-1} \in \mathcal{B}_{n-1,1}$ and $\beta_{n-2} \in \mathcal{B}_{n-2,1}$, such that $\mathrm{Tr}_{n,n-1}\beta_n = \mathrm{Tr}_{n-1,n-2}\beta_{n-1} = \mathrm{Tr}_{n-2,n-3}\beta_{n-2} = \nu_i$. Indeed, the following lemma is true:

Lemma 4.5. *Let* $M_i := \min(\{n-1\} \cup \{j : p^j \mid i, p^{j+1} \nmid i\})$. *Then there are elements* $\beta_n, \beta_{n-1}, \dots, \beta_{n-M_i}$ *where* $\beta_j \in \mathcal{B}_{j,1}$ *such that*

$$\left.\begin{array}{r} \mathrm{Tr}_{n,n-1}\beta_n \\ \mathrm{Tr}_{n-1,n-2}\beta_{n-1} \\ \vdots \\ \mathrm{Tr}_{n-M_i,n-M_i-1}\beta_{n-M_i} \end{array}\right\} = \nu_i.$$

Proof. This is clear based upon the recursive generation of the $\mathcal{B}_{j,1}$ and repeated application of Lemma 2.1. $\square$

Based upon this Lemma, we can associate to any given ν_i a set of elements which map to ν_i under a trace. If $p \nmid i$ the set contains only one element, but if $p^{n-1} \mid i$ the set will have n elements.

4.3.3. *Combining these expressions for* ν_i *in a* $\mathbb{Z}_p[G]$*-module.* There are many issues that we have not as yet addressed, so it would be premature for us to begin now to describe the Galois module structure of $\mathfrak{O}_n$. In particular, we still need to disentangle the expressions for different i. This will of course be closely associated with the process of decomposing the module, $\mathfrak{O}_n$. Nevertheless, we can at this point examine the Galois expressions associated with a particular value of i and by focusing only on the Galois generators which are involved in these expressions, describe our prototype $\mathbb{Z}_p[G]$-module.

If we combine the expressions in Lemmas 4.4 and 4.5, we get

$$\left.\begin{array}{r} \Phi_{p^n}(\sigma)\beta_n \\ \Phi_{p^{n-1}}(\sigma)\beta_{n-1} \\ \vdots \\ \Phi_{p^{n-M_i}}(\sigma)\beta_{n-M_i} \end{array}\right\} = \sum_{j \geq M_i} \frac{(\sigma^{p^{n-j-1}} - 1)^{p-1}}{(\sigma - 1)} \cdot \beta_{n-j},$$

where, possibly, some of the β_{n-j} are zero. Compare the module generated by these β's subject to this relations with the module $\mathcal{R}_n(i)$ described in §A.2.

5. Galois structure

We first determine the structure of $\mathfrak{O}_1$ and $\mathfrak{O}_2$. Then before we proceed to our inductive step, we use our method to determine the structure of $\mathfrak{O}_3$. While this step is not necessary for induction, it does help motivate some of the technicalities.

5.1. The Structure of $\mathfrak{O}_1$. From Proposition 3.5, we know that $\mathcal{B}_0 \cup \mathcal{B}_1$ generates $\mathfrak{O}_1$ over $\mathfrak{O}_T[G]$. Furthermore, we know all the Galois relationships: $\Phi_p(\sigma)\beta = 0$ for all $\beta \in \cup_{t\neq 0}\mathcal{B}_{1,t}$, while for each $\beta \in \mathcal{B}_{1,0}$, there is a unique $\alpha \in \mathcal{B}_0$ such that $\Phi_p(\sigma)\beta = \alpha$. As a consequence each $\beta \in \mathcal{B}_{1,0}$ gives rise to f direct summands of $\mathcal{R}_{1:0}$. See the Appendix A for the module notation. Each $\beta \in \mathcal{B}_{1,t}$ for $t = 1, \dots p-1$ gives rise to f copies of $\mathcal{R}_1$ while each $\alpha \in \mathcal{B}_0$ with $0 \leq v_0(\alpha) < \lambda_{1,0}$ gives rise to f direct summands of $\mathcal{R}_0$ in $\mathfrak{O}_1$. Therefore

$$\mathfrak{O}_1 \cong (\mathcal{R}_0 \oplus \mathcal{R}_1)^{\lambda_{1,0}f} \oplus \mathcal{R}_{1:0}^{(e_0-\lambda_{1,0})f}, \tag{5.1}$$

as $\mathbb{Z}_p[G]$-modules. Using notation as in [11] (see §A.3) this expression reads, $\mathfrak{O}_1 \cong (\mathcal{Z} \oplus \mathcal{R}_1)^{\lambda_{1,0}f} \oplus \mathcal{E}^{(e_0-\lambda_{1,0})f}$.

5.2. The Structure of $\mathfrak{O}_2$. From Proposition 3.5, we know that the elements of $\mathcal{B}_0 \cup \mathcal{B}_1 \cup \mathcal{B}_2$ generate $\mathfrak{O}_2$ over $\mathfrak{O}_T[G]$. Meanwhile from the previous section, we have the Galois relationships among the elements of $\mathcal{B}_0$ and $\mathcal{B}_1$. And so to determine the decomposition of $\mathfrak{O}_2$, we must determine the Galois relationships in $\mathfrak{O}_2$ that involve elements of $\mathcal{B}_2$.

First note that $\Phi_{p^2}(\sigma)\beta = 0$ for every $\beta \in \cup_{t\neq 0}\mathcal{B}_{2,t}$. Since, as one may notice, no other Galois relation (listed in this section) involves one of these β, each such β generates an $\mathfrak{O}_T[G]$-summand of $\mathfrak{O}_2$. Therefore each $\beta \in \cup_{t\neq 0}\mathcal{B}_{2,t}$ corresponds with the appearance of f copies of $\mathcal{R}_2$ in the $\mathbb{Z}_p[G]$-decomposition of $\mathfrak{O}_2$.

This leaves us to list the Galois relationships that involve $\beta \in \mathcal{B}_{2,0}$. But based upon the discussion in §4.1.2, this is done once an expression is determined, in terms of $\mathcal{B}_0$ and $\mathcal{B}_1$, for each valuation i, $\lambda_{2,1} \leq i < pe_0$.

First we consider those $i \equiv 0 \bmod p$ in $\lambda_{2,1} \leq i \leq pe_0 - 1$. Each such i is the valuation of an element in $\mathfrak{O}_0$. Let us refer to such an element as $\beta_0 \in \mathfrak{O}_0$. Because of Lemma 2.1, β_0 also lies in the image of the trace from $\mathfrak{O}_1$. There are two elements which map onto β_0: an element β_2 in $\mathcal{B}_{2,0}$ (via $\mathrm{Tr}_{2,1}$) and an element β_1 in $\mathcal{B}_{1,0}$ (via $\mathrm{Tr}_{2,1}$). So

$$\Phi_{p^2}(\sigma)\beta_2 = \Phi_p(\sigma)\beta_1 = \beta_0.$$

As one will notice these elements will not be involved in any other Galois relation (listed in this section). Therefore $\beta_0, \beta_1, \beta_2$ generated an $\mathfrak{O}_T[G]$-summand of $\mathfrak{O}_2$. And consequently, each $i \equiv 0 \bmod p$ in $\lambda_{2,1} \leq i \leq pe_0 - 1$ is associated with the appearance of f copies of $\mathcal{R}_{2,1:0}$ in $\mathfrak{O}_2$. We would like however to proceed inductively – knowing the structure of $\mathfrak{O}_1$, we determine the structure of $\mathfrak{O}_2$. Therefore we observe that part of this particular Galois relation, namely $\Phi_p(\sigma)\beta_1 = \beta_0$, was listed in §5.1 and associated with the appearance of an $\mathfrak{O}_T[G]$-summand of $\mathfrak{O}_1$. What was once associated with a summand of $\mathfrak{O}_1$ is now part of a larger module, part of a collection of terms associated with a summand of $\mathfrak{O}_2$. However each $i \equiv 0 \bmod p$ in

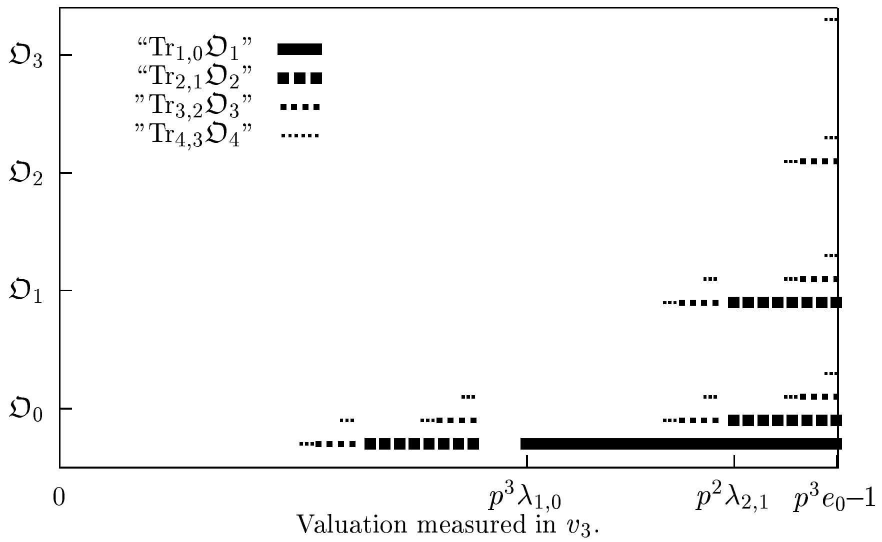
$p\lambda_{1,0} \le i \le \lambda_{2,1} - 1$ is still the valuation of a $\beta_0 \in \mathfrak{O}_0$ that is mapped to only from an element β_1 in $\mathcal{B}_{1,0}$. These elements are not involved in any further Galois relation. Therefore each $i \equiv 0 \bmod p$ in $p\lambda_{1,0} \le i \le \lambda_{2,1} - 1$ is associated with a $\mathfrak{O}_T[G]$-summand of $\mathfrak{O}_2$ or f copies of $\mathcal{R}_{1:0}$ in the $\mathbb{Z}_p[G]$-decomposition of $\mathfrak{O}_2$. Note that this yields a count of $\mathcal{R}_{1:0}$ in $\mathfrak{O}_2$ that is the count of $\mathcal{R}_{1:0}$ in $\mathfrak{O}_1$ minus the count of $\mathcal{R}_{2,1:0}$ in $\mathfrak{O}_2$. In other words, if we assume (wrongly so) that the count of $\mathcal{R}_{1:0}$ given in (5.1) is also the count of $\mathcal{R}_{1:0}$ in $\mathfrak{O}_2$; then each $i \equiv 0 \bmod p$ with $\lambda_{2,1} \le i \le pe_0 - 1$ is associated with the appearance (in our formula for the structure of $\mathfrak{O}_2$) of f copies of $\mathcal{R}_{2,1:0}$, along with the removal of f copies of $\mathcal{R}_{1:0}$. Now count the number of these i and note that this is consistent with the count of $\mathcal{R}_{2,1:0}$ in Theorem 2.2. Meanwhile what is left in our count (from (5.1)) of $\mathcal{R}_{1:0}$ is also consistent with Theorem 2.2.

We have taken some time to communicate the process whereby the structure of $\mathfrak{O}_n$ is determined once the structure of $\mathfrak{O}_{n-1}$ is known and the expressions (in terms of Galois generators) are known for each valuation in $\lambda_{n,n-1} \le i \le p^{n-1}e_0 - 1$. Now that the underlying process is clear, we sketch the rest of the details for $\mathfrak{O}_2$ below:

First assume (wrongly so) that the counts of $\mathcal{R}_0$ and $\mathcal{R}_1$ in (5.1) are also correct for $\mathfrak{O}_2$. And now let us consider those $i \not\equiv 0, b_1 \bmod p$ in $\lambda_{2,1} \le i \le pe_0 - 1$. In this case there is an element $(\sigma - 1)^{p-2}\beta$ where $\beta \in \cup_{t=2}^{p-1}\mathcal{B}_{1,t}$ with valuation i. Therefore each such $i \not\equiv 0, b_1 \bmod p$ is accompanied by the appearance of f copies of $\mathcal{R}_{2:1}$ in $\mathfrak{O}_2$, along with the disappearance of f of the copies of $\mathcal{R}_1$. Finally, consider $i \equiv b_1 \bmod p$. In this case, there is an element $\beta \in \mathcal{B}_{1,1}$ and $\alpha \in \mathfrak{O}_0$ with $v_0(\alpha) < \lambda_{1,0}$) (so that α gave rise to f copies of $\mathcal{R}_0$ in $\mathfrak{O}_1$), such that $(\sigma - 1)^{p-2}\beta - \alpha$ has valuation i. Therefore for each $i \equiv b_1 \bmod p$, one must remove f copies of $\mathcal{R}_0$ and f copies of $\mathcal{R}_1$, and add f copies of $\mathcal{R}_{2:1,0}$. Count and compare all this with Theorem 2.2.

Note that Theorem 2.2 was proven under a condition weaker than strong ramification. This indicates that the structure provided by our theorems may continue to hold outside strong ramification.

5.3. A visual–aid. As has become evident from our determination of the structure of $\mathfrak{O}_2$, the p-adic expressions for the i where $\lambda_{n,n-1} \le i < p^{n-1}e_0$ need to be disentangled before we can be sure of the structure of $\mathfrak{O}_n$. In other words, we need to be sure that Galois generators do not belong to more than one module. When we dealt with $\mathfrak{O}_1$ and $\mathfrak{O}_2$ we could afford to be a little sloppy, as we knew the structure beforehand. We have no such luxury now. To help keep the myriad of facts straight, we introduce a picture in this section. Disentangling the expressions for i then is simply a matter of showing that apparently disjoint features of this picture are indeed disjoint.



5.3.1. *Explanation of graph.* First note that this graph assumes that we are in the process of determining the structure of $\mathfrak{O}_4$. Nevertheless, as a mental image, it is useful as we determine the structure of other $\mathfrak{O}_n$.

Consider the following partition of the set of integers, $\{0, 1, \ldots, p^{n-1}e_0 - 1\}$: For each $j = 0, \ldots, n-2$, let $\mathcal{I}_j$ denote the set of nonnegative integers less than $p^{n-1}e_0$ which are exactly divisible by p^j, $\mathcal{I}_j := \{i \in \mathbb{Z} : 0 \le i < p^{n-1}e_0, p^j \mid i, p^{j+1} \nmid i\}$. Let $\mathcal{I}_{n-1}$ be the integers which remain, $\mathcal{I}_{n-1} := \{i \in \mathbb{Z} : 0 \le i < p^{n-1}e_0, p^{n-1} \mid i\}$.

We may associate via valuation, v_{n-1}, each subset $\mathcal{I}_j$ for $j = 0, 1, \ldots n-2$ with the elements of $\mathfrak{O}_{n-j-1}$ which do not belong to $\mathfrak{O}_{n-j-2}$. The elements of $\mathfrak{O}_0$ are associated with $\mathcal{I}_{n-1}$. Imagine plotting these sets separately at different levels. Plot $\mathcal{I}_0$ at the highest level and on down until the integers in $\mathcal{I}_{n-1}$ are plotted at the lowest level. We have not explicitly plotted these sets in our picture, nevertheless they should be understood to exist and are represented implicitly by the levels, $\mathfrak{O}_3$, $\mathfrak{O}_2$, $\mathfrak{O}_1$ and $\mathfrak{O}_0$.

Now any integer i such that $\lambda_{n,n-1} \le i \le p^{n-1}e_0 - 1$ inherits from §4.3.1 a p-adic expression. In fact we may assume by recursion that each $i = p^j t$ such that $\lambda_{n-j,n-j-1} \le p^j t \le p^{n-1}e_0 - 1$ also has a p-adic expression. Based upon these p-adic expressions we may associate to i a path through the integers $0, 1, \ldots, p^n e_0 - 1$. The nodes of this path are the p-adic tails of i, the set one gets by dropping, in sequence, the initial terms in its p-adic expansion,

$$\mathcal{N}_i = \{i, i - c_0, \dots, c_{m-1}p^{m-1} + Cp^m, Cp^m\}. \tag{5.2}$$

Arrange the elements of $\mathcal{N}_i$ in decreasing order, and connect each element with the next element. No element should be connected to itself. In this way we create a path beginning with i and ending with Cp^m.

Imagine plotting such paths on the graph. Clearly each path will have no more than one node in each set $\mathcal{I}_i$. But where in each $\mathcal{I}_i$ may these nodes appear? This question is addressed by the placement of various *bars* on our graph. These bars represent intervals in which nodes may appear. In fact they represent intervals where nodes from paths associated with particular types of p-adic expressions may appear.

For example, because an integer i such that $\lambda_{4,3} \leq i \leq p^3e_0 - 1$ may belong to any one of the sets $\mathcal{I}_j$, $j = 0, 1, 2, 3$; we have plotted dotted bars associated with $\mathrm{Tr}_{4,3}\mathfrak{O}_4$ at each of the four levels. Each bar begins at $\lambda_{4,3}$ and ends at $p^3e_0 - 1$. Since we are also interested in the image of the trace $\mathrm{Tr}_{3,2}\mathfrak{O}_3$, there are three bars that begin at $p\lambda_{3,2}$ and end at $p^3e_0 - 1$. Note that we are measuring, in this particular graph, in terms of the valuation v_3. In general, because of stable ramification, in particular (2.3), the bands associated with $\mathrm{Tr}_{i,i-1}\mathfrak{O}_i$ are exactly p times as long as the bands associated with $\mathrm{Tr}_{i+1,i}\mathfrak{O}_{i+1}$. This is illustrated in the graph.

But there are 15 bars associated with $\mathrm{Tr}_{4,3}\mathfrak{O}_4$, what do the other 11 represent? They represent the potential appearance of a node in a path starting at i where $\lambda_{4,3} \leq i \leq p^3e_0 - 1$. If $i \equiv b_1 \bmod p$ then the second node in the path starting at i is $\mathfrak{b} = pe_0 - (p-1)b_1$ to the left of i. To illustrate this, we have placed bars at the $\mathfrak{O}_2$, $\mathfrak{O}_1$ and $\mathfrak{O}_0$-levels which begin at $\lambda_{4,3} - \mathfrak{b}$ and end at $p^3e_0 - 1 - \mathfrak{b}$. If $i - \mathfrak{b} \equiv pb_1 \bmod p^2$, then there will be another node to the left of this one, so we place bars at the $\mathfrak{O}_1$ and $\mathfrak{O}_0$-levels which begin at $\lambda_{4,3} - (1+p)\mathfrak{b}$ and end at $p^3e_0 - 1 - (1+p)\mathfrak{b}$. The recursive nature of this process should be clear.

So that we may be specific when we reference these bars, we name them now. We will refer to a band associated with $\mathrm{Tr}_{j+1,j}\mathfrak{O}_{j+1}$ as $l(j, *x)$, where the variable expression x is a potentially empty binary string referring to location. The pattern is as follows: At the $\mathfrak{O}_j$-level there is one bar associated with $\mathrm{Tr}_{j+1,j}\mathfrak{O}_{j+1}$. We will refer to this bar with the expression $l(j,*)$. At the $\mathfrak{O}_{j-k}$-level there are 2^k bars associated with $\mathrm{Tr}_{j+1,j}\mathfrak{O}_{j+1}$. From right to left they are $l(j, *0\cdots00)$, $l(j, *0\cdots01)$, $l(j, *0\cdots10)$, $\dots$, $l(j, *x)$, $\dots$, $l(j, *1\cdots11)$. The x's are the binary expressions for the integers $0, 1, \dots, 2^k - 1$ written in increasing order.

At this point we have paths which begin at each level, beginning with some integer p^ki, $(i,p) = 1$ for $p^k\lambda_{n-k,n-k-1} \leq p^ki \leq p^{n-1}e_0 - 1$, or beginning and ending at integers $p^{n-1}i$ with $p^{n-1}\lambda_{1,0} \leq p^{n-1}i \leq p^{n-1}e_0 - 1$.

For example, consider two integers i and j with $\lambda_{4,3} \leq i, j \leq p^3 e_0 - 1$ with p-adic expressions $i = \mathfrak{b} + \mathfrak{b}p + \mathfrak{b}p^2 + Cp^3$, $j = \mathfrak{b} + Dp^3$, for some integers C and D. The nodes of i lie under $l(3, *)$, $l(3, *0)$, $l(3, *00)$, $l(3, *000)$, while the nodes of j lie under $l(3, *)$ and $l(3, *101)$. Consider pi with $p\lambda_{3,2} \leq pi \leq p^3 e_0 - 1$ with p-adic expression $pi = \mathfrak{b}p + Cp^2$ where $C \not\equiv 0, b_1 \bmod p$ then the path associated with pi begins under $l(2, *)$, and ends under $l(2, *0)$.

In general, suppose that i is such that $\lambda_{n,n-1} \leq i \leq p^{n-1}e_0 - 1$, then if $(p^{k+1}, i) = p^k$ then the first node associated with i lies under

$$l(n-1, *\overbrace{11\cdots 1}^{k}).$$

Now we illustrate the recursive process whereby one may determine based upon a node which bar the next node will lie under. Suppose now that i has a node under $l(n-1, *x)$ (where x is a potentially empty binary string), the integer value of the node being $\mathfrak{n}$. Now $(\mathfrak{n}, p^{s+1}) = p^s$ for some $s < n-1$ (unless the $p^{n-1} \mid \mathfrak{n}$ in which case it is the final node in the path anyhow). Unless $\mathfrak{n} \equiv p^s\mathfrak{b} \bmod p^{s+1}$ the path terminates at $\mathfrak{n}$, so what happens for $\mathfrak{n} \equiv p^s\mathfrak{b} \bmod p^{s+1}$? Clearly $(\mathfrak{n} - p^s\mathfrak{b}, p^{s+2+t}) = p^{s+1+t}$ for some value of t. Let $r = \min\{t, n-s-2\}$, then the next node lies under the bar labeled

$$l(n-1, *\overbrace{11\cdots 1}^{r}0x).$$

5.3.2. *Distinct paths are disjoint.* Recall that our purpose in presenting this picture is to help us disentangle the expressions for the elements ν_i with $v_{n-1}(\nu_i) = i$ and $\lambda_{n,n-1} \leq i \leq p^{n-1}e_0 - 1$ in terms of our Galois generators for $\mathfrak{O}_{n-1}$ from one another. This is equivalent to a disentangling of the paths, $\mathcal{N}_i$.

Lemma 5.1. *Let $\mathcal{N}_i$ be defined as in* (5.2)*. If $\mathcal{N}_i \cap \mathcal{N}_j \neq \emptyset$, then $\mathcal{N}_i \subseteq \mathcal{N}_j$ or $\mathcal{N}_j \subseteq \mathcal{N}_i$.*

Proof. Suppose that $i \neq j$ but that i and j have the same type of p-adic expression so that their nodes therefore lie under the same bars. Since $i \neq j$, these p-adic expressions must therefore differ only in the final term. Since we get these sets, $\mathcal{N}_i$, $\mathcal{N}_j$, from subtracting off the same amount from i that we do from j, clearly $\mathcal{N}_i \cap \mathcal{N}_j = \emptyset$.

Suppose that i and j have p-adic expressions that are initially alike, we can use the previous discussion to show that their initial nodes are disjoint. This leaves us to consider what happens with their tails or what happens when their entire p-adic expressions differ in form. If the picture is an accurate reflection of the general situation, then we need not worry because bars which sit side–by–side do not overlap.

First note that there is a certain self-similarity in this picture. Whatever collection of bars occurs at the $k+1$–st level, that same collection appears twice at the k–th level. The reason for this is clear. A node may either be 0 or congruent to $p^s\mathfrak{b} \pmod{p^{s+1}}$ for some integer s. In the first case, we plot the integer immediately below. In the second case we plot the integer $p^s\mathfrak{b}$ to the left.

Now to know that the picture accurately reflects the general situation we need to check two things.

1. Do any of the $l(k,*), l(k+1,*0), l(k+2,*00), \dots, l(k+t,*\overbrace{00\cdots 0}^{t})$ overlap?
2. Do the bars denoted by $l(k+1,*), l(k+2,*1), l(k+3,*10), \dots, l(k+t,*1\overbrace{00\cdots 0}^{t-2})$ really lie over $l(k,*)$? More accurately, we need to check whether the elements of $\mathcal{I}_{n-k-1}$ which lie under one of the bars, $l(k+1,*), l(k+2,*1), \dots$, really also lie under $l(k,*)$.

We address the first issue: Because of the self–similarity in this picture, if any of

$$l(k+1,*0), l(k+2,*00), l(k+3,*000), \dots, l(k+t,*\overbrace{00\cdots 0}^{t})$$

overlap, then there is an overlap among

$$l(k+1,*), l(k+2,*0), l(k+3,*00), \dots, l(k+t,*\overbrace{00\cdots 0}^{t-1}).$$

This recursive problem therefore boils down to whether $l(k+1,*0)$ is really completely to the left of $l(k,*)$. This is addressed by Lemma 4.3.

We address the second issue: Since the bars

$$l(k+1,*), l(k+2,*1), l(k+3,*10), \dots, l(k+t,*1\overbrace{00\cdots 0}^{t-2})$$

all lie side by side, we would be done, if we could prove that any element of $\mathcal{I}_{n-k-1}$ which is strictly less than the the left–most end value of $l(k+t,*100\cdots 0)$ is also strictly less than the left–most end point of $l(k,*)$. This is proven in the following lemma. $\square$

Lemma 5.2. *If $e_0/(p-1) \le b_1 < pe_0/(p-1) - 1$ then for $k \ge t$,*

$$p^{k-t+1}(\lambda_{t,t-1} - 1) < \lambda_{k+1,k} - \left(\frac{p^{k-t}-1}{p-1}\right)(pe_0 - (p-1)b_1).$$

Proof. Using (2.3) replace $\lambda_{t,t-1}$ and $\lambda_{k+1,k}$ with $p^{t-1}e_0 - e_0 + \lambda_{1,0}$ and $p^k e_0 - e_0 + \lambda_{1,0}$ respectively. The inequality then reduces to

$$(5.3) \quad (p^{k-t+1} - 1)(e_0 - \lambda_{1,0}) + p^{k-t+1} > \left(\frac{p^{k-t}-1}{p-1}\right)(pe_0 - (p-1)b_1).$$

If $p = 2$, (5.3) is actually, $(2^{k-t+1} - 1)(e_0 - (b_1 + 1)/2) + 2^{k-t+1} > (2^{k-t} - 1)(2e_0 - b_1)$. This reduces to $b_1 < 2e_0 + 2^{k-t+1} + 1$ which is clearly true.

Suppose that p is odd. Note that inequality in (5.3) follows immediately from $(p^{k-t+1} - 1)(e_0 - \lambda_{1,0}) \geq (p^{k-t} - 1)(pe_0 - (p-1)b_1)/(p-1)$, which is equivalent to

$$\frac{e_0 - \lambda_{1,0}}{e_0 - (p-1)b_1/p} \geq \frac{p(p^{k-t} - 1)}{(p-1)(p^{k-t+1} - 1)}.$$

To verify this equation, we establish the following inequalities:

$$\frac{e_0 - \lambda_{1,0}}{e_0 - (p-1)b_1/p} \geq \frac{1}{2} > \frac{p(p^{k-t} - 1)}{(p-1)(p^{k-t+1} - 1)}.$$

First we establish the left inequality. Note that this is equivalent to $e_0 \geq \lambda_{1,0} + (b_1/p - \lfloor b_1/p \rfloor)$. Since $b_1 + 1 < pe_0/(p-1)$ we have $e_0 \geq \lambda_{1,0} + 1$, so the inequality obviously holds. The second inequality is equivalent to $p^{k-t+1}(p-3) + p + 1 > 0$ and since $p \geq 3$, it holds. □

5.4. The Structure of $\mathfrak{O}_3$. As we noted earlier while determining the structure of $\mathfrak{O}_1$ and $\mathfrak{O}_2$, because of Proposition 3.5 , $\mathcal{B}_0 \cup \mathcal{B}_1 \cup \mathcal{B}_2 \cup \mathcal{B}_2$ generates $\mathfrak{O}_3$ over $\mathfrak{O}_T[G]$. Since $\Phi_{p^3}(\sigma)\beta = 0$ for all $\beta \in \cup_{t \neq 1} \mathcal{B}_{3,t}$, each such β will correspond to the appearance of f copies of $\mathcal{R}_3$ in the $\mathbb{Z}_p[G]$-direct sum decomposition of $\mathfrak{O}_3$.

All that remains for a determination of the structure of $\mathfrak{O}_3$ is a catalog of the expressions for i, $\lambda_{3,2} \leq i < p^2 e_0$, in terms of the Galois generators of $\mathfrak{O}_2$.

Suppose that $i \equiv 0 \bmod p$, then each such i coincides with the appearance of f copies of $\mathcal{R}_{3,2:1,0}$ along with the disappearance of f copies of $\mathcal{R}_{2:1,0}$, or the appearance of $\mathcal{R}_{3,2:1}$ and the disappearance of $\mathcal{R}_{2:1}$, or the appearance of $\mathcal{R}_{3,2,1:0}$ and the disappearance of $\mathcal{R}_{2,1:0}$. Which occurs depends upon whether $i \equiv \mathfrak{b}p \bmod p^2$, $i \not\equiv 0, \mathfrak{b}p \bmod p^2$ or $i \equiv 0 \bmod p^2$, respectively.

If $i \equiv \mathfrak{b} \bmod p$ then i coincides with the appearance of f copies of $\mathcal{R}_{3:2,1,0}$ along with the disappearance of f copies of $\mathcal{R}_2 \oplus \mathcal{R}_1 \oplus \mathcal{R}_0$, or the appearance of $\mathcal{R}_{3:2,1}$ and the disappearance of $\mathcal{R}_2 \oplus \mathcal{R}_1$, or the appearance of $\mathcal{R}_{3,1:2,0}$ and the disappearance of $\mathcal{R}_2 \oplus \mathcal{R}_{1:0}$. Which occurs depends upon whether $i \equiv \mathfrak{b} + \mathfrak{b}p \bmod p^2$, $i \not\equiv \mathfrak{b}, \mathfrak{b} + \mathfrak{b}p \bmod p^2$ or $i \equiv \mathfrak{b} \bmod p^2$, respectively.

If $i \not\equiv 0, \mathfrak{b} \bmod p$ then i coincides with the appearance of f copies of $\mathcal{R}_{3:2}$ along with the disappearance of f copies of $\mathcal{R}_2$. All this is expressed in the following Theorem:

Theorem 5.3. *Let p be any prime. If $b_1 > pe_0/(2p-2)$ then*

$$\begin{aligned}\mathfrak{O}_3 \cong \mathcal{R}_0^{(\lambda_{1,0}-b-x)\cdot f} &\oplus \mathcal{R}_1^{(\lambda_{1,0}-c-a-x)\cdot f} \oplus \mathcal{R}_2^{(\lambda_{1,0}-d)\cdot f} \oplus \mathcal{R}_3^{\lambda_{1,0}\cdot f}\\ &\oplus \mathcal{R}_{1:0}^{(a+b-y)\cdot f} \oplus \mathcal{R}_{2:1}^{(a-c+w)\cdot f} \oplus \mathcal{R}_{3:2}^{a\cdot f}\\ &\oplus \mathcal{R}_{2:1,0}^{(b-w)\cdot f} \oplus \mathcal{R}_{3:2,1}^{(b-x)\cdot f} \oplus \mathcal{R}_{2,1:0}^{(c-z)\cdot f} \oplus \mathcal{R}_{3,2:1}^{(c-w)\cdot f}\\ &\oplus \mathcal{R}_{3,2:1,0}^{w\cdot f} \oplus \mathcal{R}_{3:2,1,0}^{x\cdot f} \oplus \mathcal{R}_{3,1:2,0}^{y\cdot f} \oplus \mathcal{R}_{3,2,1:0}^{z\cdot f},\end{aligned}$$

as $\mathbb{Z}_p[G]$-modules, where $\mathfrak{b} = pe_0-(p-1)b_1$, $a+b+c = e_0-\lambda_{1,0}$, $d = a+b+y$, $b = e_0 - \lceil \mathfrak{b}/p\rceil - \lceil(\lambda_{2,1}-\mathfrak{b})/p\rceil = \lambda_{1,0} - \lambda_{2,0} + e_0$, $c = e_0 - \lceil \lambda_{2,1}/p\rceil$, $w = e_0 - \lceil \mathfrak{b}/p\rceil - \lceil(\lambda_{3,2}-p\mathfrak{b})/p^2\rceil$, $x = e_0 - \lceil(\mathfrak{b}+p\mathfrak{b})/p^2\rceil - \lceil(\lambda_{3,2}-\mathfrak{b}-p\mathfrak{b})/p^2\rceil$, $y = e_0 - \lceil \mathfrak{b}/p^2\rceil - \lceil(\lambda_{3,2}-\mathfrak{b})/p^2\rceil$, $z = e_0 - \lceil\lambda_{3,2}/p^2\rceil$. These modules are described in Appendix A.

6. The Galois structure of the ring of integers

In this section we collect the observations of the previous section into a proof of the main result of the paper, Theorem 1.2. The proof is followed by a discussion of the result.

Proof. (Theorem 1.2) From §3 we know that $\mathfrak{O}_n$ is generated over $\mathfrak{O}_T[G]$ by $\cup_{i=0}^n \mathcal{B}_i$. As one may check, each element of $\cup_{t\neq 0}\mathcal{B}_{n,t}$ contributes a copy of $\mathfrak{O}_T \otimes_{\mathbb{Z}_p} \mathcal{R}_n$ to the $\mathfrak{O}_T[G]$-direct decomposition of $\mathfrak{O}_n$ (or f copies of $\mathcal{R}_n$ to the $\mathbb{Z}_p[G]$-direct decomposition). Meanwhile based upon §4 each i for $\lambda_{n,n-1} \le i \le p^{n-1}e_0 - 1$ corresponds to the occurrence of $\mathfrak{O}_T \otimes_{\mathbb{Z}_p} \mathcal{R}_n(i)$ as a $\mathfrak{O}_T[G]$-submodule of $\mathfrak{O}_n$. Because of §5, in particular §5.3 and Lemma 5.1, we know that the elements of $\cup_{i=0}^n \mathcal{B}_i$ which generate $\mathfrak{O}_T \otimes_{\mathbb{Z}_p} \mathcal{R}_n(i)$ are disjoint from the elements which generate $\mathfrak{O}_T \otimes_{\mathbb{Z}_p} \mathcal{R}_n(j)$ for $i \neq j$. Furthermore the elements of $\cup_{i=0}^k \mathcal{B}_i$ which generate $\mathfrak{O}_T \otimes_{\mathbb{Z}_p} \mathcal{R}_k(j)$ are either disjoint or are entirely contained in the set of elements which generate $\mathfrak{O}_T \otimes_{\mathbb{Z}_p} \mathcal{R}_n(i)$, for $k < n$. As a consequence, we are justified in expressing the structure of $\mathfrak{O}_n$ as a direct sum of $\mathcal{R}_n(i)$'s and the summands of $\mathfrak{O}_{n-1}$ that do not interact with any $\mathcal{R}_n(i)$. This is represented in the statement of our theorem. $\square$

6.1. Discussion of result and corollaries. Notice the difference in flavor between Theorem 5.3 and Theorem 1.1. The first result is explicit, specifying the modules and determining their exponents. The second result is implicit, essentially providing an algorithm from which the modules and their exponents can be determined. Clearly using Theorem 1.1 we may state results like Theorem 5.3 for $n = 4$, for $n = 5$ and so forth. These results however rapidly exceed a single page in length. Therefore we refrain from doing so, leaving it to the interested reader.

However if we impose stricter restrictions on ramification we should be able to state explicit results that are easily confined to a single page and yet hold without restriction on n, results similar to [5, Thm 5]. Indeed imposing (1.3), the restriction used in [5], we find that the type of p-adic expression for i in $\lambda_{n,n-1} \le i < p^{n-1}e_0$ is restricted to a very narrow range of possibilities, thus providing an entirely new proof for [5, Thm 5].

Define

$$A = e_0 - \lambda_{1,0}.$$

Corollary 6.1. *Let p be any prime (odd or even) and $b_1 > pe_0/(2p-2)$. If $b_1 + 1 > p\lceil e_0/(p-1)\rceil - p$ then:*

$$\mathfrak{O}_n \cong \mathcal{R}_0^{\lambda_{1,0}\cdot f} \oplus \sum_{i=1}^{n-1} \mathcal{R}_i^{(\lambda_{1,0}-A)\cdot f} \oplus \mathcal{R}_n^{\lambda_{1,0}\cdot f} \oplus \sum_{i=1}^{n} \mathcal{R}_{i:i-1}^{A\cdot f}$$

Proof. The p-adic expressions for the i such that $\lambda_{n,n-1} \le i < p^{n-1}e_0$ determine the modules. Any restriction of the type of p-adic expression that may appear thereby restricts the Galois module structure.

Let $q = \lceil e_0/(p-1)\rceil$ so that $e_0 = q(p-1) - r$ for some $r = 0, 1, \ldots, p-1$. The restriction on ramification may then be rewritten as $b_1 > pq - (p+1)$. In other words, $b_1 = pq - v$ for some $0 \le v < p+1$, or $0 \le v \le p$. But we may assume that $b_1 \not\equiv 0 \bmod p$, so $1 \le v \le p-1$. Now it may be shown that $\lambda_{1,0} = q(p-1) - v + 1 = e_0 + r - v + 1$. So $v = e_0 - \lambda_{1,0} + r + 1 > e_0 - \lambda_{1,0}$. Using (2.3), $\lambda_{n,n-1} > p^{n-1}e_0 - v$. So for $n > 1$, since $p^{n-1}e_0 - v > p^{n-1}e_0 - p$ and $p^{n-1} - v \equiv b_1 \bmod p$ we find that $i \not\equiv 0, b_1 \bmod p$ for every i in $\lambda_{n,n-1} \le i < p^{n-1}e_0$. The corollary follows then because every i such that $\lambda_{n,n-1} \le i < p^{n-1}e_0$ is associated with the appearance of an $\mathcal{R}_{n:n-1}$. $\square$

Only two families of modules appear in this corollary: the family of irreducible modules, $\mathcal{R}_i$, and the family of modules represented by $\mathcal{R}_{i:i-1}$. Since each of these modules appear in the structure of $\mathfrak{O}_1$, the structure in this corollary may be understood as a generalization of the structure of $\mathfrak{O}_1$. To generalize this discussion, we require the following definition:

Definition 6.2. Let $\mathcal{R}_{A:B}$ be a module as described in §A.1, so A, B are sets of integers. Let $A(i) = \{a+i : a \in A\}$ and $B(i) = \{a+i : a \in B\}$. Then the family of modules containing $\mathcal{R}_{A:B}$ is the set of modules, $\mathcal{R}_{A(i):B(i)}$, with $i \in \mathbb{Z}$ (so long as the module is defined).

Our original intent in developing Lemma 2.6 was to provide a sequence of ever weaker restrictions on ramification resulting in ever looser trace relations. The hope was that these trace relations would restrict the type of module that may appear in $\mathfrak{O}_n$ to those families that are already represented in $\mathfrak{O}_1$, then in $\mathfrak{O}_2$, and then in $\mathfrak{O}_3$, etc. This does not happen.

Although the first restriction in Lemma 2.6 does restrict the modules to those families which are already represented in $\mathfrak{O}_1$, the second restriction in Lemma 2.6 does not restrict the modules to those that are already represented in $\mathfrak{O}_2$, namely the families containing $\mathcal{R}_0$, $\mathcal{R}_{1:0}$, $\mathcal{R}_{2,1:0}$, and $\mathcal{R}_{2:1,0}$. We explain this now.

For the second restriction in Lemma 2.6, namely $b_2+1 > p^2\lceil e_0/(p-1)\rceil - p^2$, to determine a structure for $\mathfrak{O}_n$ in terms of modules from the four families of modules already represented in the structure of $\mathfrak{O}_2$, we would have to show that based upon this restriction, the only p-adic expressions appearing among the i in $\lambda_{n,n-1} \le i \le p^{n-1}e_0 - 1$ are those of the form: C, pC, and $\mathfrak{b}+pC$ where $C \not\equiv 0, b_1 \bmod p$. These i would then correspond to the appearance of the modules: $\mathcal{R}_{n:n-1}$, $\mathcal{R}_{n,n-1:n-2}$, and $\mathcal{R}_{n:n-1:n-2}$, respectively. Along with the irreducible modules, $\mathcal{R}_n$, these would be the four families appearing in $\mathfrak{O}_n$. This however is not possible, other p-adic expressions can appear. One can show that based upon the restriction $b_2+1 > p^2\lceil e_0/(p-1)\rceil - p^2$, there is no integer in $\lambda_{n,n-1} \le i \le p^{n-1}e_0 - 1$ which is equivalent to 0 or even $\mathfrak{b}+p\mathfrak{b}$ modulo p^2, but one cannot show that there is no integer equivalent to $\mathfrak{b}$ or $p\mathfrak{b}$ modulo p^2. This is with good reason. Modules such as $\mathcal{M} = \mathcal{R}_{n,n-2,n-4,\dots,n-(2k):n-1,n-3,n-5,\dots,n-(2k+1)}$ satisfy the restriction $\mathrm{Tr}_{t,t-3}(M^{\sigma^t}) = \mathrm{Tr}_{t,t-3}(M^{\sigma^{t-1}})$ for each $t = 3, 4, \dots, n$. And so there are a number of families which satisfy the second trace relation provided by Lemma 2.6, yet do not appear in $\mathfrak{O}_2$. One has to imagine, then, that the variety of modules satisfying subsequent trace relations proliferate. Our plan then to control the type of module by the imposition of lower bounds on ramification must therefore be amended.

To control the statements in our corollaries, we require an alternative restriction on ramification. We require one that is not merely a lower bound on the ramification numbers but one that strictly controls the variety of p-adic expressions that may appear in $\lambda_{n,n-1} \le i \le p^{n-1}e_0 - 1$.

Fortunately there is a certain stability inherent in the statement of our main theorem. This results from the fact that for $n \ge k$, the intervals $\lambda_{n,n-1} \le i < p^{n-1}e_0 - 1$ and $\lambda_{k,k-1} \le i < p^{k-1}e_0 - 1$ have the same length. Therefore the only residues modulo p^{k-1} that appear among the integers $\lambda_{n,n-1} \le i \le p^{n-1}e_0 - 1$ are residues that appear among the integers $\lambda_{k,k-1} \le j \le p^{k-1}e_0 - 1$. Assume then that the p-adic expressions for the j in $\lambda_{k,k-1} \le j \le p^{k-1}e_0 - 1$ all end with m (as in (4.4)) strictly less that $k-1$. This would force each C to be distinct from 0 and $b_1 \bmod p$. Consequently, the only p-adic expressions that appear at the n–th level are those that already have appeared at the k–th level.

Corollary 6.3. *Let K_n/K_0 be a cyclic fully ramified extension of degree p^n with $b_1 > pe_0/(2p-2)$. If the only module families which appear in $\mathfrak{O}_k$*

are those that appear in $\mathfrak{O}_{k-1}$, then only those module families appear in $\mathfrak{O}_t$ for $t = k, k+1, \dots, n$.

Proof. If the only module families which appear in $\mathfrak{O}_k$ are those which appear in $\mathfrak{O}_{k-1}$, then the only p-adic expressions that appear in $\lambda_{k,k-1} \leq i \leq p^{k-1}e_0 - 1$ are those that appear in $\lambda_{k-1,k-2} \leq i \leq p^{k-2}e_0 - 1$. In particular, the p-adic expressions that occur in $\lambda_{k,k-1} \leq i \leq p^{k-1}e_0 - 1$ must terminate before the p^{k-1}–st term. Since $p^{k-1}e_0 - a \equiv p^{t-1}e_0 - a \bmod p^{k-1}$ for $t \geq k$, the p-adic expressions that appear in $\lambda_{t,t-1} \leq i \leq p^{t-1}e_0 - 1$ are exactly those that appear in $\lambda_{k,k-1} \leq i \leq p^{k-1}e_0 - 1$. □

Based upon this corollary we can generalize Corollary 6.1 as follows. First, we define some more constants:

$$\mathfrak{b} = pe_0 - (p-1)b_1,$$
$$B_0 = e_0 - \left\lceil \frac{\lambda_{2,1}}{p} \right\rceil, B_1 = e_0 - \left\lceil \frac{\mathfrak{b}}{p} \right\rceil - \left\lceil \frac{\lambda_{2,1} - \mathfrak{b}}{p} \right\rceil = \lambda_{1,0} - \lambda_{2,0} + e_0.$$

Corollary 6.4. *Let p be any prime (odd or even) and $b_1 > pe_0/(2p-2)$. If $n > 2$ and every integer i in $\lambda_{3,2} \leq i < p^2 e_0$ is expressed p-adically as C, pC, or $\mathfrak{b} + pC$ where $C \not\equiv 0, b_1 \bmod p$, then:*

$$\mathfrak{O}_n \cong \mathcal{R}_0^{a_0 \cdot f} \oplus \sum_{i=1}^{n-2} \mathcal{R}_i^{a \cdot f} \oplus \mathcal{R}_{n-1}^{a_{n-1} \cdot f} \oplus \mathcal{R}_n^{\lambda_{1,0} \cdot f} \oplus \mathcal{R}_{1:0}^{c_1 \cdot f} \oplus \sum_{i=2}^{n-1} \mathcal{R}_{i:i-1}^{c \cdot f} \oplus \mathcal{R}_{n:n-1}^{c_n \cdot f}$$
$$\oplus \sum_{i=2}^{n} \mathcal{R}_{i,i-1:i-2}^{B_0 \cdot f} \oplus \sum_{i=2}^{n} \mathcal{R}_{i:i-1,i-2}^{B_1 \cdot f}$$

where $a_0 = \lambda_{1,0} - B_1$, $a = \lambda_{1,0} - A + B_0 - B_1$, $a_{n-1} = \lambda_{1,0} - A + B_0$, $c_1 = A - B_0$, $c = A - 2B_0 - B_1$, $c_n = A - B_0 - B_1$.

Proof. This corollary follows from Corollary 6.3 and counting. □

To indicate how this may be generalized further we list one more corollary. To do so, we require some additional constants:

$$C_0 = e_0 - \left\lceil \frac{\lambda_{3,2}}{p^2} \right\rceil, C_1 = e_0 - \left\lceil \frac{\mathfrak{b}}{p^2} \right\rceil - \left\lceil \frac{\lambda_{3,2} - \mathfrak{b}}{p^2} \right\rceil,$$
$$C_2 = e_0 - \left\lceil \frac{p\mathfrak{b}}{p^2} \right\rceil - \left\lceil \frac{\lambda_{3,2} - p\mathfrak{b}}{p^2} \right\rceil, C_3 = e_0 - \left\lceil \frac{\mathfrak{b} + p\mathfrak{b}}{p^2} \right\rceil - \left\lceil \frac{\lambda_{3,2} - \mathfrak{b} - p\mathfrak{b}}{p^2} \right\rceil.$$

Corollary 6.5. *Let p be any prime (odd or even) and $b_1 > pe_0/(2p-2)$. If $n > 3$ and every integer i in $\lambda_{4,3} \leq i < p^3 e_0$ is expressed p-adically as C, pC, p^2C, $\mathfrak{b} + pC$ $\mathfrak{b} + p^2C$, $p\mathfrak{b} + p^2C$ or $\mathfrak{b} + p\mathfrak{b} + p^2C$ where $C \not\equiv 0, b_1 \bmod p$, then:*

$$\begin{aligned}\mathfrak{O}_n \cong & \mathcal{R}_0^{a_0\cdot f} \oplus \sum_{i=1}^{n-3} \mathcal{R}_i^{a\cdot f} \oplus \sum_{i=n-2}^{n-1} \mathcal{R}_i^{a_i\cdot f} \oplus \mathcal{R}_n^{\lambda_{1,0}\cdot f} \oplus \mathcal{R}_{1:0}^{c_1\cdot f} \oplus \sum_{i=2}^{n-2} \mathcal{R}_{i:i-1}^{c\cdot f} \\ & \oplus \sum_{i=n-1}^{n} \mathcal{R}_{i:i-1}^{c_i\cdot f} \oplus \mathcal{R}_{2,1:0}^{d_2\cdot f} \oplus \sum_{i=3}^{n-1} \mathcal{R}_{i,i-1:i-2}^{d\cdot f} \oplus \mathcal{R}_{n,n-1:n-2}^{d_n\cdot f} \\ & \oplus \mathcal{R}_{2:1,0}^{e_2\cdot f} \oplus \sum_{i=3}^{n-1} \mathcal{R}_{i:i-1,i-2}^{e\cdot f} \oplus \mathcal{R}_{n:n-1,n-2}^{e_n\cdot f} \oplus \sum_{i=3}^{n} \mathcal{R}_{i,i-1,i-2:i-3}^{C_0\cdot f} \\ & \oplus \sum_{i=3}^{n} \mathcal{R}_{i,i-2:i-1,i-3}^{C_1\cdot f} \oplus \sum_{i=3}^{n} \mathcal{R}_{i,i-1:i-2,i-3}^{C_2\cdot f} \oplus \sum_{i=3}^{n} \mathcal{R}_{i:i-1,i-2,i-3}^{C_3\cdot f}\end{aligned}$$

where $a_0 = \lambda_{1,0} - B_1 - C_3$, $a = \lambda_{1,0} - A + B_0 - B_1 + C_1 - C_3$, $a_{n-2} = \lambda_{1,0} - A + B_0 - B_1 + C_1$, $a_{n-1} = \lambda_{1,0} - A + B_0$, $c_1 = A - B_0 - C_1$, $c = A - 2B_0 - B_1 + C_0 - C_1 + C_2$, $c_{n-1} = A - 2B_0 - B_1 + C_0 + C_2$, $c_n = A - B_0 - B_1$, $d_2 = B_0 - C_0$, $d = B_0 - 2C_0 - C_2$, $d_n = B_0 - C_0 - C_2$, $e_2 = B_1 - C_2$, $e = B_1 - C_1 - C_2 - C_3$, $e_n = B_1 - C_1 - C_3$.

Proof. This corollary follows from Corollary 6.3 and counting. □

We could proceed further by writing down corollaries of this sort. As this is simply a computational process, we leave it to the interested reader.

7. Examples and remarks

7.1. Examples. The results of [7] and [8] may be used as they were in [5] to exhibit extensions with prescribed ramification to which we may apply our main result. We leave this exercise to the reader.

7.2. Remarks. Recall Question B from §2.1. Based upon work in that section, we know that for $n \geq 2$, $\mathcal{S}_{C_{p^n}}$ is proper in the set of all $\mathbb{Z}_p[C_{p^n}]$-indecomposables. But one might wish for more, perhaps $\mathcal{S}_{C_{p^n}}$ is very small, or at least finite. This is in general too much to hope for, see [4] where the set $\mathcal{S}_G$ is is shown to be infinite for G the Klein 4-group. But still, the integral representations of cyclic groups seem to be simpler in nature than the representations of other groups. And so we may continue to ask whether $\mathcal{S}_{C_{p^n}}$ be finite. This is a difficult open question. As a result, we revise the question and answer the revision.

Definition: Define the set of x–restricted realizable indecomposables, $\mathcal{S}_G(x)$, to be the set of indecomposable $\mathbb{Z}_p[G]$-modules $\mathcal{M}$, for which there is an extension L/K with $\mathrm{Gal}(L/K) \cong G$ and first ramification number $b_1 \geq x$, such that $\mathcal{M}$ appears as a $\mathbb{Z}_p[G]$-direct summand of $\mathfrak{O}_L$. Let $s_G = \inf\{x : |\mathcal{S}_G(x)| < \infty\}$.

Question C: What is $s_{C_{p^n}}$?

Note that $s_{C_{p^n}}$ is bounded trivially by $-1 \leq s_{C_{p^n}} \leq pe_0/(p-1)$, and that $\mathcal{S}_{C_{p^n}}$ is finite if and only if $s_{C_{p^n}} = -1$. Therefore the answer to Question B is "yes" if $s_{C_{p^n}} = -1$. While we are not able to answer Question C; we can, using Theorem 1.2, provide a non-trivial upper bound:

$$s_{C_{p^n}} \leq pe_0/(2p-2).$$

It is reasonable to expect that one might, by extending the methods of this paper, derive similar inductive descriptions of the ring of integers without strong ramification, perhaps reducing the upper bound on $s_{C_{p^n}}$ to $\max\{e_0/(p-1), (pe_0-p+1)/(2p-1)$. Indeed, in §2.6 we made a choice between two restrictions on b_1: *strong ramification* and $b_1 < (1/2)pe_0/(p-1)$. Had we chosen to work with $b_1 < (1/2)pe_0/(p-1)$ instead, we would have already determined the effect of $\Phi_p(\sigma)$ on any $\alpha \in \mathfrak{O}_n$ with $v_n(\alpha) \not\equiv 0 \bmod p$ and $v_n(\alpha)+(p-1)b_1 \not\equiv 0 \bmod p^2$, needing only to extend this effect to those α with $v_n(\alpha)+(p-1)b_1 \equiv 0 \bmod p^2$. Certainly there are many other details to consider, but still it is reasonable to expect that our results under strong ramification generalize. We noted at the end of §5.2, that for C_{p^2}-extensions, our result extends (using other methods) to the weaker restriction $b_1 \geq \max\{e_0/(p-1), (pe_0-p+1)/(2p-1)$. This investigation is certainly worth pursuing.

There are two other directions of generalization to consider. First, one might apply the methods of this paper to the Galois module structure of other fractional ideals besides $\mathfrak{O}_n$. We have restrained from developing our results in this generality because of the impact of the additional details on the exposition. Secondly, one might derive a result generalizing Yokoi [16] (for example, [5, Thm 6]). However, this merely translates our results into another language.

Appendix A. The modules

In this section, we describe the modules that are used in our structure theorems. First we describe a broad class of module. Then we specialize to those modules that actually appear. In the final part of this section, we provide a brief dictionary to facilitate translation between our notation and the notation used in [11] and [2].

A.1. A general class of module. We assume throughout that σ, the generator of G, acts via multiplication by x. First we introduce the irreducible modules:

$$\mathcal{R}_i := \frac{\mathbb{Z}_p[x]}{\langle \Phi_{p^i}(x) \rangle}.$$

The other modules all arise as extensions of these irreducible modules. To facilitate their description, define

$$\mathcal{E}_i := \frac{\mathbb{Z}_p[x]}{\langle x^{p^i} - 1\rangle}.$$

These are the regular representations of the group quotients.

Let $A = \{a_1, a_2, \dots, a_r\}$ and $B = \{b_1, b_2, \dots, b_s\}$ be sets of decreasing, nonnegative integers. Furthermore, assume that A and B are disjoint. Define $\mathcal{R}_{A:B}$ or alternatively, $\mathcal{R}_{a_1,\dots,a_r:b_1,\dots,b_s}$ to be a particular extension of $\mathcal{R}_{a_1} \oplus \cdots \oplus \mathcal{R}_{a_r}$ by $\mathcal{R}_{b_1} \oplus \cdots \oplus \mathcal{R}_{b_s}$. Namely:

$$\mathcal{R}_{A:B} = \mathcal{R}_{a_1,\dots,a_r:b_1,\dots,b_s} := \frac{\mathcal{E}_{a_1} \oplus \cdots \oplus \mathcal{E}_{a_r} \oplus \mathcal{R}_{b_1} \oplus \cdots \oplus \mathcal{R}_{b_s}}{\mathcal{M}}$$

where $\mathcal{M}$ is the submodule generated by the following r elements: each of the r elements has the form $\alpha_i + \beta_i$ $i = 1, \dots, r$, where $\alpha_i = (0, \dots, 0, \Phi_{p^{a_i}}(x), 0, \dots, 0) \in \mathcal{E}_{a_1} \oplus \cdots \oplus \mathcal{E}_{a_i} \oplus \cdots \oplus \mathcal{E}_{a_r}$ and $\beta_i = (\beta_i(1), \beta_i(2), \dots, \beta_i(s)) \in \mathcal{R}_{b_1} \oplus \cdots \oplus \mathcal{R}_{b_s}$ where

$$\beta_i(j) := \begin{cases} (x-1)^{\phi\left(p^{b_j}\right)-1} & \text{if } a_i > b_j \\ 0 & \text{otherwise.} \end{cases}$$

A.2. A subclass of module. In this subsection we define a function, $\mathcal{R}_n(i)$, from the integers to a subset of modules listed above. Following §4.3.1 we let $\mathfrak{b} = pe_0 - (p-1)b_1$ and express i p-adically as

$$i = c_0 + c_1 p + c_2 p^2 + \cdots + c_{m-1} p^{m-1} + C p^m, \tag{A.1}$$

where $c_k \in \{0, \mathfrak{b}\}$, and $C \not\equiv 0, b_1 \bmod p$ unless $m = n-1$ in which case there is no restriction on C. Now partition the set $\{n, n-1, \dots, n-1-m\}$ into two sets: $A = \{n\} \cup \{n-1-i : 0 \le i \le m-1, a_i = 0\}$, $B = \{n-1-m\} \cup \{n-1-i : 0 \le i \le m-1, a_i \ne 0\}$. List the elements of A and B in decreasing order. Define

$$\mathcal{R}_n(i) := \mathcal{R}_{A:B}.$$

A.3. Dictionary: our notation and others. In this section we explicitly list the 15 modules required to describe $\mathfrak{O}_3$ and when possible relate our notation to the notation used in [11].

First we note that $\mathcal{R}_0$ is the trivial module called $\mathcal{Z}$ in [11], and that $\mathcal{R}_{1:0} = \mathcal{E}_1$. So $\mathcal{R}_0, \mathcal{R}_1, \mathcal{R}_{1:0}$ are the three indecomposable modules associated to the cyclic group of order p.

Furthermore, translating our notation into the notation used in [11], we note that $\mathcal{R}_{2:1,0} = (\mathcal{R}_2, \mathcal{Z} \oplus \mathcal{R}_1; 1 \oplus \lambda^{p-2})$, $\mathcal{R}_{2,1:0} = (\mathcal{R}_2, \mathcal{E}_1; \lambda^{p-1})$, $\mathcal{R}_{2:1} = (\mathcal{R}_2, \mathcal{R}_1; \lambda^{p-2})$. So $\mathcal{R}_i$ $i = 0, 1, 2$, along with $\mathcal{R}_{1:0}$, $\mathcal{R}_{2:1,0}$, $\mathcal{R}_{2,1:0}$ and $\mathcal{R}_{2:1}$ are the seven modules used in Theorem 2.2 to express $\mathfrak{O}_2$.

Of the remaining eight modules, $\mathcal{R}_3$ requires no translation. Meanwhile four modules can be expressed using notation similar to [11] (See also [2, Thm 34.32]):

$$\begin{aligned}
\mathcal{R}_{3:2} &= (\mathcal{R}_3, \mathcal{R}_2; \lambda^{p^2-p-1}),\\
\mathcal{R}_{3,1:2,0} &= (\mathcal{R}_3, \mathcal{R}_2 \oplus \mathcal{E}_1; \lambda^{p^2-p-1} \oplus \lambda^{p-1}),\\
\mathcal{R}_{3:2,1} &= (\mathcal{R}_3, \mathcal{R}_2 \oplus \mathcal{R}_1; \lambda^{p^2-p-1} \oplus \lambda^{p-2}),\\
\mathcal{R}_{3:2,1,0} &= (\mathcal{R}_3, \mathcal{R}_2 \oplus \mathcal{R}_1 \oplus \mathcal{Z}; \lambda^{p^2-p-1} \oplus \lambda^{p-2} \oplus 1).
\end{aligned}$$

The remaining three modules, $\mathcal{R}_{3,2,1:0}$ $\mathcal{R}_{3,2:1,0}$, $\mathcal{R}_{3,2:1}$, are quite different and would require an expansion of the notation in [11]. They are extensions of modules which are themselves an extension. They should be understood as generalizations of $\mathcal{R}_{2,1:0} = (\mathcal{R}_2, \mathcal{E}_1; \lambda^{p-1})$.

References

[1] F. Bertrandias, *Sur les extensions cycliques de degré p^n d'un corps local.* Acta Arith. **34** (1979), no. 4, 361–377.

[2] C. W. Curtis, I. Reiner, *Methods of Representation Theory*, vol. 1. Wiley-Interscience, New York, 1990.

[3] G. G. Elder, *Galois module structure of integers in wildly ramified cyclic extensions of degree p^2.* Ann. Inst. Fourier **45** (1995), 625–647, *errata ibid.* **48** (1998), 609–610.

[4] G. G. Elder, *Galois module structure of ideals in wildly ramified biquadratic extensions.* Can. J. Math. **50** (1998), 1007–1047.

[5] G. G. Elder, M. L. Madan, *Galois module structure of integers in wildly ramified cyclic extensions.* J. Number Theory **47** (1994), 138–174.

[6] A. Heller, I. Reiner, *Representations of cyclic groups in rings of integers* I. Ann. of Math. (2) **76** (1962), 73–92.

[7] E. Maus, *Existenz p-adischer zahlkorper zu vorgegebenem verzweigungsverhalten.* Ph.D. thesis, Univ. Hamburg, 1965.

[8] H. Miki, *On the ramification numbers of cyclic p-extensions over local fiels.* J. Reine Angew. Math. **328** (1981), 99–115.

[9] Y. Miyata, *On the module structure in a cyclic extensions over a p-adic number field.* Nagoya Math. J. **73** (1979), 61–68.

[10] E. Noether, *Normalbasis bei Körpern ohne höhere Verzweigung.* J. Reine Angew. Math. **167** (1932), 147–152.

[11] M. Rzedowski-Calderón, G. Villa-Salvador, M. L. Madan, *Galois module structure of rings of integers.* Math. Z. **204** (1990), 401–424.

[12] J-P. Serre, *Local fields.* Springer-Verlag, Berlin/Heidelberg/New York, 1979.

[13] S. Ullom, *Integral Normal Bases in Galois Extensions of Local Fields.* Nagoya Math. J. **39** (1970), 141–148.

[14] S. V. Vostokov, *Ideals of an Abelian p-extension of a local field as Galois modules.* Zap. Naučn. Sem. Leningrad. Otdel. Mat. Inst. Steklov. (LOMI) **57** (1976), 64–84.

[15] B. Wyman, *Wildly ramified gamma extensions.* Amer. J. Math. **91** (1969), 135–152.

[16] H Yokoi, *On the ring of integers in an algebraic number field as a representation module of galois group.* Nagoya Math. J. **16** (1960), 83–90.

G. Griffith Elder
Department of Mathematics
University of Nebraska at Omaha
Omaha, Nebraska 68182-0243, U. S. A.
E-mail : elder@unomaha.edu