ANNALES DE L'INSTITUT FOURIER

GOVE GRIFFITH ELDER

Galois module structure of ideals in wildly ramified cyclic extensions of degree p^2

Annales de l'institut Fourier, tome 45, n° 3 (1995), p. 625-647

<http://www.numdam.org/item?id=AIF_1995__45_3_625_0>

© Annales de l'institut Fourier, 1995, tous droits réservés.

L'accès aux archives de la revue « Annales de l'institut Fourier » (http://annalif.ujf-grenoble.fr/) implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme
Numérisation de documents anciens mathématiques
http://www.numdam.org/

Ann. Inst. Fourier, Grenoble
45, 3 (1995), 625-647

GALOIS MODULE STRUCTURE OF IDEALS IN WILDLY RAMIFIED CYCLIC EXTENSIONS OF DEGREE p^2

by Gove GRIFFITH ELDER

1. Introduction.

Let L/K be a totally ramified cyclic extension of degree p^2 of local fields which are finite extensions of $\mathbb{Q}_p$, the field of p-adic numbers. Let $\mathfrak{O}_L$ be the ring of integers in L, and let $\mathfrak{P}_L$ be its unique maximal ideal. Then each fractional ideal, $\mathfrak{P}_L^n$ where n is a rational integer, is canonically a $\mathbb{Z}_p[G]$-module, where $G = \mathrm{Gal}(L/K)$ and $\mathbb{Z}_p$ is the ring of p-adic integers. By the Krull-Schmidt Theorem, $\mathfrak{P}_L^n$ decomposes uniquely into a direct sum of indecomposable $\mathbb{Z}_p[G]$- modules. What is this decomposition? In this paper, we give the $\mathbb{Z}_p[G]$-module decomposition of $\mathfrak{P}_L^n$ explicitly in terms of the following : the $4p+1$ indecomposable $\mathbb{Z}_p[G]$-modules classified by Heller and Reiner [5] Thm 34.32, the lower ramification numbers of L/K, the absolute ramification index of $K/\mathbb{Q}_p$, and n itself. It should be noted that a partial answer for $\mathfrak{O}_L$, the particular case $n \equiv 0 \bmod p^2$, was given by Rzedowski-Calderón, Villa- Salvador and Madan [16] Thm 2, under a rather severe restriction on the first ramification number. In this paper, we eliminate the need for the restriction required by [16], and generalize the result to include all fractional ideals.

In the second section we introduce the notation recalling, in particular, the $4p+1$ indecomposable $\mathbb{Z}_p[G]$- modules. Then in the third section, we state and prove our main result. The proof consists of four steps, the

Key words : Galois module structure – Wild ramification – Local number field – Integral representation – Finite representation type.
Math. classification : 11S15 – 20C32.

most important of which is the choice of a suitable explicit integral basis for $\mathfrak{P}_L^{n\,H}$ which is amenable to an analysis of the Galois action, where $\mathfrak{P}_L^{n\,H}$ denotes the submodule of $\mathfrak{P}_L^n$ fixed under the subgroup, H, of index p. In the final section, we end with some remarks.

The reader is referred to [16] for more background, to joint work with Madan [6] for a generalization of [16] to arbitrarily large cyclic extensions of p-power degree and to the papers of Miyata [15] and Vostokov [19] for a discussion of the $\mathfrak{O}_K[G]$-module structure of $\mathfrak{P}_L^n$. Note that in the papers of Miyata and Vostokov, the focus is on conditions under which $\mathfrak{P}_L^n$ is indecomposable as an $\mathfrak{O}_K[G]$-module; (it almost always is!). As we will see, $\mathfrak{P}_L^n$ is almost always decomposable as a $\mathbb{Z}_p[G]$-module.

It should also be mentioned that, motivated by the work of Leopoldt [10], J. Martinet [12] has introduced the concept of the associated order, $\mathcal{A} = \{x \in K[G] : x\mathfrak{O}_L \subseteq \mathfrak{O}_L\}$. What, then, is the structure of $\mathfrak{O}_L$ as an $\mathcal{A}$-module? This problem has been extensively studied, notably by Bergé [1], F. Bertrandias [2], J.-P. Bertrandias [3] and M.-J. Ferton [7].

Finally, the standard reference for the Galois module structure of the ring of integers in global number fields is Fröhlich's book [8].

2. Notation.

Let p be a rational prime and let K_2/K_0 be a cyclic, totally ramified extension of local fields of degree p^2, with $[K_0 : \mathbb{Q}_p] = e_0 f$, e_0 denoting the absolute ramification index. Let $G = \mathrm{Gal}(K_2/K_0)$ be generated by σ. Let K_1 be the fixed field of $H = \langle \sigma^p \rangle$. Let $\mathfrak{O}_i$ be the ring of integers of K_i, $\mathfrak{P}_i$ be the unique maximal ideal of $\mathfrak{O}_i$, and from now on, let $\mathfrak{P}_2^n$ be a particular fractional ideal. So n is a fixed rational integer. Let π_i be a prime element of K_i, v_i be the normalized valuation of K_i so that $v_i(\pi_i) = 1$, and let $\mathbb{F}_p$ be the field of p elements. Let T be the largest unramified extension of $\mathbb{Q}_p$ contained in K_0, so $[T : \mathbb{Q}_p] = f$, and let $\mathfrak{O}_T$ be its ring of integers.

Let b_1, b_2 be the lower ramification numbers of K_2/K_0, and for any rational integer, x, let $\mathfrak{P}_k^{\lambda_{j,k}(x)}$ be the largest power of $\mathfrak{P}_k$ to divide $\mathfrak{P}_j^x \mathfrak{D}_{K_j/K_k}$, where $\mathfrak{D}_{K_j/K_k}$ denotes the relative different. Let $\lfloor x \rfloor$ denote the floor function (*i.e.* the greatest integer function), and $\lceil x \rceil$, the ceiling function (*i.e.* the least integer function), where these two functions are

related by $\left\lfloor \frac{x-1}{p} \right\rfloor = \left\lceil \frac{x}{p} \right\rceil - 1$. It is easily seen using [18] pg 64, that

$$(1)\quad \lambda_{1,0}(x) = \left\lfloor \frac{x+(b_1+1)(p-1)}{p} \right\rfloor,\ \lambda_{2,1}(x) = \left\lfloor \frac{x+(b_2+1)(p-1)}{p} \right\rfloor,$$

$$\lambda_{2,0}(x) = \left\lfloor \frac{x+(b_1+1)(p^2-1)+(b_2-b_1)(p-1)}{p^2} \right\rfloor.$$

In fact if T_{K_j/K_k} denotes the relative trace from K_j to K_k, then as in a theorem of Yokoi [21] Thm 1,

(2)

$$T_{K_1/K_0}(\mathfrak{P}_1^x) = \mathfrak{P}_0^{\lambda_{1,0}(x)},\ T_{K_2/K_1}(\mathfrak{P}_2^x) = \mathfrak{P}_1^{\lambda_{2,1}(x)},\ T_{K_2/K_0}(\mathfrak{P}_2^x) = \mathfrak{P}_0^{\lambda_{2,0}(x)}.$$

At this point we should also note that the submodule of $\mathfrak{P}_2^n$ fixed under H is $\mathfrak{P}_1^{\left\lceil \frac{n}{p} \right\rceil}$, while the submodule fixed under G is $\mathfrak{P}_0^{\left\lceil \frac{n}{p^2} \right\rceil}$.

We recall the following notation for the $4p+1$ indecomposable $\mathbb{Z}_p[G]$-modules [5] Thm 34.32 :

$$(3)\quad \begin{gathered} Z,\ R_1,\ E,\ R_2,\ (R_2, Z; 1), \text{ and } (R_2, E; \lambda^i) \text{ for } i = 0, 1, \ldots, p-1, \\ (R_2, R_1; \lambda^i), \text{ and } (R_2, Z \oplus R_1; 1 \oplus \lambda^i) \text{ for } i = 0, 1, \ldots, p-2, \\ \text{and } (R_2, Z \oplus E; 1 \oplus \lambda^i) \text{ for } i = 1, \ldots, p-2. \end{gathered}$$

And for each of these modules we give explicit interpretations, following [16] pg 407-8 and [5] pg 175-6. In each case, σ acts via multiplication by x, and $\Phi_{p^i}(x)$ denotes the p^i-th cyclotomic polynomial.

(4)

$$Z = \frac{\mathbb{Z}_p[x]}{\langle (x-1) \rangle},\ R_2 = \frac{\mathbb{Z}_p[x]}{\langle \Phi_{p^2}(x) \rangle},\ (R_2, R_1; \lambda^i) = \frac{\frac{\mathbb{Z}_p[x]}{\langle (x^{p^2}-1) \rangle} \oplus \frac{\mathbb{Z}_p[x]}{\langle \Phi_p(x) \rangle}}{\langle (\Phi_{p^2}(x), (x-1)^i) \rangle},$$

$$R_1 = \frac{\mathbb{Z}_p[x]}{\langle \Phi_p(x) \rangle},$$

$$(R_2, Z \oplus R_1; 1 \oplus \lambda^i) = \frac{\frac{\mathbb{Z}_p[x]}{\langle (x^{p^2}-1) \rangle} \oplus \frac{\mathbb{Z}_p[x]}{\langle (x-1) \rangle} \oplus \frac{\mathbb{Z}_p[x]}{\langle \Phi_p(x) \rangle}}{\langle (\Phi_{p^2}(x), 1, (x-1)^i) \rangle},$$

$$E = \frac{\mathbb{Z}_p[x]}{\langle (x^p-1) \rangle},$$

$$(R_2, Z \oplus E; 1 \oplus \lambda^i) = \frac{\frac{\mathbb{Z}_p[x]}{\langle (x^{p^2}-1) \rangle} \oplus \frac{\mathbb{Z}_p[x]}{\langle (x-1) \rangle} \oplus \frac{\mathbb{Z}_p[x]}{\langle (x^p-1) \rangle}}{\langle (\Phi_{p^2}(x), 1, (x-1)^i) \rangle},$$

$$(R_2, Z; 1) = \frac{\dfrac{\mathbb{Z}_p[x]}{\langle (x^{p^2}-1)\rangle} \oplus \dfrac{\mathbb{Z}_p[x]}{\langle (x-1)\rangle}}{\langle (\Phi_{p^2}(x), 1)\rangle},$$

$$(R_2, E; \lambda^i) = \frac{\dfrac{\mathbb{Z}_p[x]}{\langle (x^{p^2}-1)\rangle} \oplus \dfrac{\mathbb{Z}_p[x]}{\langle (x^p-1)\rangle}}{\langle (\Phi_{p^2}(x), (x-1)^i)\rangle}.$$

Note that $(R_2, E; \lambda^0) \cong \mathbb{Z}_p[G]$. In Theorem 1, we determine which of these indecomposables appears in the $\mathbb{Z}_p[G]$- decomposition of $\mathfrak{P}_2^n$. Notice that the precise decomposition depends only on e_0, f, b_1, b_2 and n.

3. The main result.

THEOREM 1. — *Using the notation introduced above :*

$$\mathfrak{P}_2^n \cong Z^{a\cdot f} \oplus R_1^{b\cdot f} \oplus E^{c\cdot f} \oplus \sum_{i=0}^{p-2} \left(R_2, Z \oplus R_1; 1 \oplus \lambda^i\right)^{d_i \cdot f} \oplus \sum_{i=0}^{p-1} \left(R_2, E; \lambda^i\right)^{g_i \cdot f}$$

$$\oplus \sum_{i=1}^{p-2} \left(R_2, R_1; \lambda^i\right)^{h_i \cdot f} \oplus R_2^{k\cdot f} \text{ as } \mathbb{Z}_p[G]\text{-modules,}$$

where

$$r = \max\left\{0, \left\lfloor \frac{p^2(\lambda_{2,0}(n) - e_0) - n}{pb_1} \right\rfloor\right\},$$

$$s = \max\left\{0, (p-1) + \left\lceil \frac{\lambda_{2,1}(n) - pe_0 - p\left\lceil \dfrac{n}{p^2} \right\rceil + p}{b_1} \right\rceil\right\},$$

$$s_j = \max\left\{0, (p-1+j) + \left\lceil \frac{\lambda_{2,1}(n) - pe_0 - p\left\lceil \dfrac{n + jpb_1}{p^2} \right\rceil}{b_1} \right\rceil\right\}$$

for $j = 0, 1, \ldots, r$, *and*

$$a = \max\left\{0, \lambda_{2,0}(n) - \left\lceil \frac{n}{p^2} \right\rceil - e_0\right\};$$

$$b = \sum_{j=0,\ s_j > p-1}^{r} \left(\left\lceil \frac{n-(p-j-1)pb_1}{p^2} \right\rceil - \left\lceil \frac{n-(p-j)pb_1}{p^2} \right\rceil \right)$$

$$+ \sum_{j=0,\ p-1 \geq s_j > p-2}^{r} \min\left\{ \left\lceil \frac{\lambda_{2,1}(n) - (s_j - j)b_1}{p} \right\rceil - e_0, \left\lceil \frac{n-(p-j-1)pb_1}{p^2} \right\rceil \right\}$$

$$- \left\lceil \frac{n-(p-j)pb_1}{p^2} \right\rceil;$$

$$c = \left\lceil \frac{\lambda_{2,1}(n)}{p} \right\rceil - \lambda_{1,0}\left(\left\lceil \frac{n}{p} \right\rceil \right);$$

$$d_i = \begin{cases} 0 & \text{for } i < r, \\ e_0 - \lambda_{2,0}(n) + \left\lceil \dfrac{n+(r+1)pb_1}{p^2} \right\rceil & \text{for } i = r, \\ \left\lceil \dfrac{n+(i+1)pb_1}{p^2} \right\rceil - \left\lceil \dfrac{n+ipb_1}{p^2} \right\rceil & \text{for } r < i; \end{cases}$$

$$g_i = \begin{cases} 0 & \text{for } i < s, \\ e_0 + \left\lceil \dfrac{n}{p^2} \right\rceil - b_1 - \left\lceil \dfrac{\lambda_{2,1}(n) - (s+1)b_1}{p} \right\rceil & \text{for } i = s, \\ \left\lceil \dfrac{\lambda_{2,1}(n) - (i)b_1}{p} \right\rceil - \left\lceil \dfrac{\lambda_{2,1}(n) - (i+1)b_1}{p} \right\rceil & \text{for } s < i; \end{cases}$$

$$h_i = \sum_{j=0,\ s_j - 1 = i}^{r-1} \max\left\{0, \left(\left\lceil \frac{n-(p-j-1)pb_1}{p^2} \right\rceil \right.\right.$$

$$\left.\left. - \left\lceil \frac{\lambda_{2,1}(n) - (s_j - j)b_1}{p} \right\rceil + e_0 \right)\right\}$$

$$+ \sum_{j=0,\ s_j = i}^{r} \min\left\{ \left\lceil \frac{\lambda_{2,1}(n) - (s_j - j)b_1}{p} \right\rceil \right.$$

$$\left. - e_0, \left\lceil \frac{n-(p-j-1)pb_1}{p^2} \right\rceil \right\} - \left\lceil \frac{n-(p-j)pb_1}{p^2} \right\rceil;$$

$$k = \left\lceil \frac{\lambda_{2,1}(n)}{p} \right\rceil - \lambda_{1,0}\left(\left\lceil \frac{n}{p} \right\rceil \right) + b.$$

Remark. — Byott has studied $\mathfrak{O}_k[G]$-isomorphisms among fractional ideals in [4]. Note that one can use this theorem to determine the existence of $\mathbb{Z}_p[G]$ - isomorphisms between any two given fractional ideals in totally ramified cyclic extensions of degree p^2. Remark : There are certain conditions under which the statement of the theorem becomes more manageable. Of course there are other conditions under which the statement is quite unmanageable. In what follows we discuss three different situations : 1) If $\lambda_{2,0}(n) \leq e_0 + \left\lceil \frac{n}{p^2} \right\rceil$ then the expression in Theorem 1 becomes quite simple : $r = s = 0$, $b = 0$ and $h_i = 0$ for all i. Note that this condition occurs when the ramification numbers are relatively small, which is quite unexpected. Generally it is not when the ramification numbers are small but when they are large that things are well behaved, see Wyman's discussion of stable ramification [20], and also [6]. 2) If b_1 is too small with respect to p, the expression becomes somewhat sporadic. For instance, when $b_1 = 1$, $n \equiv 1 \bmod p^2$ and $p \geq 3$, then $b_2 = 1 + p(up - v)$ for some integer u, and $v \in \{0, 1, \ldots p-1\}$, $a = b = 0$, $c = u(p-1) - v$, $d_i = 0$ for all i, $g_0 = e_0 - u(p-1) + v$ for $v = 0$, $g_0 = e_0 - u(p-1) + v - 1$ for $v \neq 0$, $g_i = 0$ for $i \neq v \neq 0$, $g_v = 1$ for $v \neq 0$, $h_i = 0$ for all i and $k = u(p-1) - v$. Notice that in this case, f copies of $(R_2, E; \lambda^i)$ appear for different values of i depending on v. 3) If, on the other hand, b_1 is large enough with respect to p, the expression behaves smoothly as we vary b_2. The invariants, r, s, s_i, do not take on wildly different values. In fact it is easily seen that if we choose b_1 large enough, r, s and s_i all take on roughly the same value. One can also see that in this case, all the g_i for $i > s$ and all the d_i for $i > r$ have approximately the same value, $\lfloor b_1/p \rfloor \approx \lceil b_1/p \rceil$.

Proof of Theorem 1. — The theorem is proven in four steps. But first, we observe that there is one particular pair of ramification numbers which warrants special consideration. This pair occurs when p divides the first ramification number, b_1. It is well-known, [20], that $p \mid b_1$ implies K_0 contains the p-th roots of unity, $b_1 = \dfrac{pe_0}{p-1}$ and $b_2 = \dfrac{p^2 e_0}{p-1}$. In this case, the reader may check that the following members of $\mathbb{Q}_p[G]$ map $\mathfrak{P}_2^n$ into itself : $\dfrac{1}{p^2} T_{K_2/K_0}$, $\dfrac{1}{p} T_{K_2/K_1} - \dfrac{1}{p^2} T_{K_2/K_0}$ and $1 - \dfrac{1}{p} T_{K_2/K_1}$. Therefore,

$$\mathfrak{P}_2^n \cong Z^{e_0 f} \oplus R_1^{e_0 f} \oplus R_2^{e_0 f} \text{ as } \mathbb{Z}_p[G]\text{-modules.} \tag{5}$$

From now on, we shall exclude this special case from our consideration, and assume that b_1 and, hence, b_2 is relatively prime to p.

Step 1. In this step we construct a special basis for $\mathfrak{P}_1^{\lceil \frac{n}{p} \rceil}$ over $\mathfrak{O}_T$ which is amenable to the investigation of its Galois module structure. Our first lemma is well known, we state and prove it for the sake of completeness.

LEMMA 1. — $v_1\left((\sigma-1)^i\pi_1^{b_1}\right) = (i+1)b_1$ *for* $i = 0, 1, 2, \ldots, p-1$, *and* $v_1\left((\sigma-1)^{p-1}\pi_1^{b_1}\right) = v_1\left((1+\sigma+\sigma^2+\cdots+\sigma^{p-1})\pi_1^{b_1}\right) = pb_1$.

Note. — In a paper of MacKenzie and Whaples [11], it was shown that cyclic extensions of degree p with $(b_1, p) = 1$ are generated by a root, Λ, of an Artin-Schreier equation, $x^p - x - \lambda = 0$, with $v_0(\lambda) = -b_1$. Clearly, $v_1(\Lambda) = -b_1$. Therefore, Λ^{-1} can be used as a canonical replacement for the element $\pi_1^{b_1}$ in the statement of this lemma.

Proof. — Let $y_0 = 1$, $y_1 = \pi_1$, $y_2 = \pi_1\sigma(\pi_1)$, ..., $y_n = \pi_1\sigma(\pi_1)\cdots\sigma^{n-1}(\pi_1)$, as in Sen [17]. Clearly, $v_1(y_i) = i$, and $p \mid i$ implies $y_i \in K_0$. The $\{y_i\}_{i=0}^{pe_0-1}$ form a basis for $\mathfrak{O}_1$ over $\mathfrak{O}_T$. Now,

$$v_1\left((\sigma-1)y_i\right) = \begin{cases} i+b_1 & \text{if } p \nmid i \\ \infty & \text{if } p \mid i. \end{cases} \tag{6}$$

Of course $v_1\left(\pi_1^{b_1}\right) = b_1$ and $p \nmid b_1$. Assume now that for $1 \le i \le p-1$, $v_1\left((\sigma-1)^{i-1}\pi_1^{b_1}\right) = ib_1$, then clearly $p \nmid ib_1$, and $(\sigma-1)^{i-1}\pi_1^{b_1} = uy_{ib_1} + w$, for some unit, u, of $\mathfrak{O}_0$, and some element, w, of $\mathfrak{O}_1$ with strictly higher valuation than ib_1. Using (6), $v_1\left((\sigma-1)^i\pi_1^{b_1}\right) = v_1\left((\sigma-1)y_{ib_1}\right) = (i+1)b_1$. By (1) and (2), $v_0\left(T_{K_1/K_0}(\pi_1^{b_1})\right) = \left\lfloor \dfrac{b_1 + (b_1+1)(p-1)}{p} \right\rfloor = b_1$, and so $v_1\left(\Phi_p(\sigma)\pi_1^{b_1}\right) = pb_1$. □

LEMMA 2 (*A special* $\mathfrak{O}_T$*-basis for* $\mathfrak{P}_1^{\lceil \frac{n}{p} \rceil}$). — *Let* $t_m = \left\lceil \dfrac{n - p^2m}{pb_1} \right\rceil - 2$, *then*

$$\mathfrak{P}_1^{\lceil \frac{n}{p} \rceil} = \sum_{m=\lceil \frac{n}{p^2} \rceil - b_1}^{\lceil \frac{n-pb_1}{p^2} \rceil - 1} \mathfrak{O}_T\Phi_p(\sigma)\pi_1^{b_1}\pi_0^m + \sum_{m=\lceil \frac{n-pb_1}{p^2} \rceil}^{e_0 + \lceil \frac{n}{p^2} \rceil - b_1 - 1} \sum_{i=0}^{p-1} \mathfrak{O}_T(\sigma-1)^i\pi_1^{b_1}\pi_0^m$$

$$+ \sum_{m=\lceil \frac{n}{p^2} \rceil - b_1}^{\lceil \frac{n-pb_1}{p^2} \rceil - 1} \left(\sum_{i=t_m+1}^{p-2} \mathfrak{O}_T(\sigma-1)^i\pi_1^{b_1}\pi_0^m + \sum_{i=0}^{t_m} \mathfrak{O}_T(\sigma-1)^i p\pi_1^{b_1}\pi_0^m \right).$$

Proof. — As a first step, define the following sets :

$A_m = \left\{v_1((\sigma-1)^i\pi_1^{b_1}\pi_0^m\right\}_{i=0}^{p-1}$ for all $m \in \mathbb{Z}$, where $\mathbb{Z}$ is the integers. It is an easy exercise to check that the sets A_m are mutually disjoint, and that $\bigcup_{m\in\mathbb{Z}} A_m = \mathbb{Z}$. By choosing elements, $(\sigma-1)^i\pi_1^{b_1}\pi_0^m$ with $\left\lceil \frac{n}{p} \right\rceil \leq (i+1)b_1 + pm \leq pe_0 + \left\lceil \frac{n}{p} \right\rceil - 1$, we arrive at a basis for $\mathfrak{O}_1$ over $\mathfrak{O}_T$. For $\left\lceil \frac{n}{p^2} \right\rceil - b_1 \leq m \leq \left\lceil \frac{n-pb_1}{p^2} \right\rceil - 1$, we then may replace $(\sigma-1)^{p-1}\pi_1^{b_1}\pi_0^m$ by $\Phi_p(\sigma)\pi_1^{b_1}\pi_0^m$, using Lemma 1. Then clearly each $(\sigma-1)^i\pi_1^{b_1}\pi_0^m$ where $e_0 + \left\lceil \frac{n}{p^2} \right\rceil - b_1 \leq m \leq e_0 + \left\lceil \frac{n-pb_1}{p^2} \right\rceil - 1$ and $(i+1)b_1 + pm \leq pe_0 - 1$ can be replaced by $(\sigma-1)^i p\pi_1^{b_1}\pi_0^m$ where $\left\lceil \frac{n}{p^2} \right\rceil - b_1 \leq m \leq \left\lceil \frac{n-pb_1}{p^2} \right\rceil - 1$. The condition, $(i+1)b_1 + p(e_0+m) \leq pe_0 + \left\lceil \frac{n}{p} \right\rceil - 1$, is then equivalent to $i \leq \left\lceil \frac{n-p^2m}{pb_1} \right\rceil - 2$. □

Let

$$(7)\quad \alpha_m = \Phi_p(\sigma)\pi_1^{b_1}\pi_0^m \text{ for } m = \left\lceil \frac{n}{p^2} \right\rceil - b_1, \ldots, \left\lceil \frac{n-pb_1}{p^2} \right\rceil - 1,$$

$$(8)\quad \beta_m = \begin{cases} p\pi_1^{b_1}\pi_0^m - \Phi_p(\sigma)\pi_1^{b_1}\pi_0^m, \\ \qquad\qquad \text{for } m = \left\lceil \frac{n}{p^2} \right\rceil - b_1, \ldots, \left\lceil \frac{n+pb_1}{p^2} \right\rceil - b_1 - 1 \\ -(\sigma-1)^{t_m+1}\pi_1^{b_1}\pi_0^m, \\ \qquad\qquad \text{for } m = \left\lceil \frac{n+pb_1}{p^2} \right\rceil - b_1, \ldots, \left\lceil \frac{n-pb_1}{p^2} \right\rceil - 1, \end{cases}$$

$$(9)\quad \gamma_m = \pi_1^{b_1}\pi_0^m \text{ for } m = \left\lceil \frac{n-pb_1}{p^2} \right\rceil, \ldots, e_0 + \left\lceil \frac{n}{p^2} \right\rceil - b_1 - 1.$$

LEMMA 3. — *For any integer* m,

$$\mathbb{Z}_p\Phi_p(\sigma)\pi_1^{b_1}\pi_0^m = \mathbb{Z}_p\alpha_m \cong Z \text{ as } \mathbb{Z}_p[G]\text{-modules.}$$

$$\sum_{i=0}^{p-1} \mathbb{Z}_p(\sigma-1)^i\pi_1^{b_1}\pi_0^m = \mathbb{Z}_p[G]\gamma_m \cong E \text{ as } \mathbb{Z}_p[G]\text{- modules.}$$

Proof. — Clear. □

We now know that the first two summands in the statement of Lemma 2 correspond to Z's and E's. As one might expect, knowing [16] Thm 1, the final summand should somehow correspond to a collection of R_1's.

LEMMA 4. — *Let* $t_m = \left\lceil \frac{n-p^2m}{pb_1} \right\rceil - 2$. *Then for* $m = \left\lceil \frac{n}{p^2} \right\rceil - b_1, \ldots, \left\lceil \frac{n+pb_1}{p^2} \right\rceil - b_1 - 1$,

$$\mathbb{Z}_p\left(p\pi_1^{b_1}\pi_0^m - \Phi_p(\sigma)\pi_1^{b_1}\pi_0^m\right) + \sum_{i=1}^{p-2} \mathbb{Z}_p(\sigma-1)^i p\pi_1^{b_1}\pi_0^m$$
$$= \mathbb{Z}_p[G]\beta_m \cong R_1 \text{ as } \mathbb{Z}_p[G]\text{- modules,}$$

and for $m = \left\lceil \frac{n+pb_1}{p^2} \right\rceil - b_1, \ldots, \left\lceil \frac{n-pb_1}{p^2} \right\rceil - 1$,

$$\sum_{i=t_m+1}^{p-2} \mathbb{Z}_p(\sigma-1)^i\pi_1^{b_1}\pi_0^m + \mathbb{Z}_p\left(p\pi_1^{b_1}\pi_0^m - \Phi_p(\sigma)\pi_1^{b_1}\pi_0^m\right) + \sum_{i=1}^{t_m} \mathbb{Z}_p(\sigma-1)^i p\pi_1^{b_1}\pi_0^m$$
$$= \mathbb{Z}_p[G]\beta_m \cong R_1 \text{ as } \mathbb{Z}_p[G]\text{- modules.}$$

Proof. — Clearly, these are $\mathbb{Z}_p$-torsion free modules which are annihilated by $\Phi_p(\sigma)$. What remains to be shown is that they are closed under the group action : given a basis element α, that $(\sigma-1)\alpha$ is expressible as a linear combination of basis elements. Clearly, the only difficulty lies in showing this for $\alpha = (\sigma-1)^{p-2}\pi_1^{b_1}\pi_0^m$. But by a lemma of Hasse [9] pg. 76, $\Phi_p(\sigma) = \sum_{i=0}^{p-1} \binom{p}{i+1}(\sigma-1)^i$. So, $(\sigma-1)\alpha = (\sigma-1)^{p-1}\pi_1^{b_1}\pi_0^m =$
$$-\sum_{i=t_m+1}^{p-2} \binom{p}{i+1}(\sigma-1)^i\pi_1^{b_1}\pi_0^m - \left(p\pi_1^{b_1}\pi_0^m - \Phi_p(\sigma)\pi_1^{b_1}\pi_0^m\right) - \sum_{i=1}^{t_m} \frac{\binom{p}{i+1}}{p}(\sigma-1)^i p\pi_1^{b_1}\pi_0^m.$$ □

Using these lemmas, $\left\lceil \frac{\left\lceil \frac{n}{p} \right\rceil}{p} \right\rceil = \left\lceil \frac{n}{p^2} \right\rceil$ and $\lambda_{1,0}\left(\left\lceil \frac{n}{p} \right\rceil\right) - \left\lceil \frac{n}{p^2} \right\rceil = \left\lceil \frac{n-pb_1}{p^2} \right\rceil - \left\lceil \frac{n}{p^2} \right\rceil + b_1$, we obtain the following generalization of [16] Thm 1.

THEOREM 2. — *Let $\eta_1, \dots, \eta_f$ be a basis of $\mathfrak{O}_T$ over $\mathbb{Z}_p$, and let $\alpha_{m,j} = \alpha_m \cdot \eta_j$, $\beta_{m,j} = \beta_m \cdot \eta_j$ and $\gamma_{m,j} = \gamma_m \cdot \eta_j$, then*

$$\mathfrak{P}_1^{\left\lceil \frac{n}{p} \right\rceil} = \sum_{m=\left\lceil \frac{n}{p^2} \right\rceil - b_1}^{\left\lceil \frac{n-pb_1}{p^2} \right\rceil - 1} \mathfrak{O}_T[G]\alpha_m + \sum_{m=\left\lceil \frac{n}{p^2} \right\rceil - b_1}^{\left\lceil \frac{n-pb_1}{p^2} \right\rceil - 1} \mathfrak{O}_T[G]\beta_m + \sum_{m=\left\lceil \frac{n-pb_1}{p^2} \right\rceil}^{e_0 + \left\lceil \frac{n}{p^2} \right\rceil - b_1 - 1} \mathfrak{O}_T[G]\gamma_m$$

$$= \sum_{j=1}^{f} \left(\sum_{m=\left\lceil \frac{n}{p^2} \right\rceil - b_1}^{\left\lceil \frac{n-pb_1}{p^2} \right\rceil - 1} \mathbb{Z}_p[G]\alpha_{m,j} + \sum_{m=\left\lceil \frac{n}{p^2} \right\rceil - b_1}^{\left\lceil \frac{n-pb_1}{p^2} \right\rceil - 1} \mathbb{Z}_p[G]\beta_{m,j} + \sum_{m=\left\lceil \frac{n-pb_1}{p^2} \right\rceil}^{e_0 + \left\lceil \frac{n}{p^2} \right\rceil - b_1 - 1} \mathbb{Z}_p[G]\gamma_{m,j} \right)$$

$$\cong Z^{\left(\lambda_{1,0}\left(\left\lceil \frac{n}{p} \right\rceil\right) - \left\lceil \frac{n}{p^2} \right\rceil\right)f} \oplus R_1^{\left(\lambda_{1,0}\left(\left\lceil \frac{n}{p} \right\rceil\right) - \left\lceil \frac{n}{p^2} \right\rceil\right)f} \oplus E^{\left(e_0 - \lambda_{1,0}\left(\left\lceil \frac{n}{p} \right\rceil\right) + \left\lceil \frac{n}{p^2} \right\rceil\right)f}$$

as $\mathbb{Z}_p[G]$- modules.

So in general,

$\mathfrak{P}_1^t \cong Z^{\left(\lambda_{1,0}(t) - \left\lceil \frac{t}{p} \right\rceil\right)f} \oplus R_1^{\left(\lambda_{1,0}(t) - \left\lceil \frac{t}{p} \right\rceil\right)f} \oplus E^{\left(e_0 - \lambda_{1,0}(t) + \left\lceil \frac{t}{p} \right\rceil\right)f}$ *as $\mathbb{Z}_p[G]$-modules.*

COROLLARY 1. — *For any integer, x, let $r(x) = x - p\left\lfloor \frac{x-1}{p} \right\rfloor$ be the remainder in $\{1, 2, \dots, p\}$ of x divided by p. Let $\varphi(\mathfrak{P}_1^x) = \left\lfloor \frac{r(x) - r(b_1+1)}{p} \right\rfloor + 1$, then*

$$\mathfrak{P}_1^s \cong \mathfrak{P}_1^t \text{ as } \mathbb{Z}_p[G]\text{- modules, if and only if } \varphi(\mathfrak{P}_1^s) = \varphi(\mathfrak{P}_1^t).$$

Note that $\varphi(\mathfrak{P}_1^x)$ takes values in $\{0, 1\}$, that $\varphi(\mathfrak{D}_{K_1/K_0}^{-1}) = \varphi(\mathfrak{O}_1) = 1$, in fact that $\varphi(\mathfrak{P}_1^t) = 1$ for all t if $p \mid b_1$, but that if $(p, b_1) = 1$ then $\varphi(\mathfrak{P}_1) = \cdots = \varphi(\mathfrak{P}_1^{r(b_1+1)-1}) = 0$.

Proof. — Clearly $\mathfrak{P}_1^s \cong \mathfrak{P}_1^t$ as $\mathbb{Z}_p[G]$-modules if and only if $\lambda_{1,0}(s) - \left\lceil \frac{s}{p} \right\rceil = \lambda_{1,0}(t) - \left\lceil \frac{t}{p} \right\rceil$ which is equivalent to $\left\lfloor \frac{s + (b_1+1)(p-1)}{p} \right\rfloor - \left\lceil \frac{s}{p} \right\rceil =$

$\left\lfloor \frac{t+(b_1+1)(p-1)}{p} \right\rfloor - \left\lceil \frac{t}{p} \right\rceil$. This, it is easily seen, is equivalent to

$$\left\lfloor \frac{r(s)-r(b_1+1)}{p} \right\rfloor = \left\lfloor \frac{r(t)-r(b_1+1)}{p} \right\rfloor. \qquad \square$$

Step 2. In this step we provide elements of $\mathfrak{P}_1^{\lambda_{2,1}(n)}$ which generate $\mathfrak{P}_1^{\lambda_{2,1}(n)}/p\mathfrak{P}_1^{\left\lceil \frac{n}{p} \right\rceil}$ over $\mathfrak{O}_T/p\mathfrak{O}_T[G]$. First, we list the valuations of a basis for $\mathfrak{P}_1^{\left\lceil \frac{n}{p} \right\rceil}$ over $\mathfrak{O}_T$. For $m = \left\lceil \frac{n}{p^2} \right\rceil - b_1, \ldots, \left\lceil \frac{n-pb_1}{p^2} \right\rceil - 1$,

$$v_1(\alpha_m) = pb_1 + pm; \tag{10}$$

$$v_1((\sigma-1)^i\beta_m) = (i+t_m+2)b_1 + pm \text{ where } i = 0, \ldots, p-t_m-3,$$

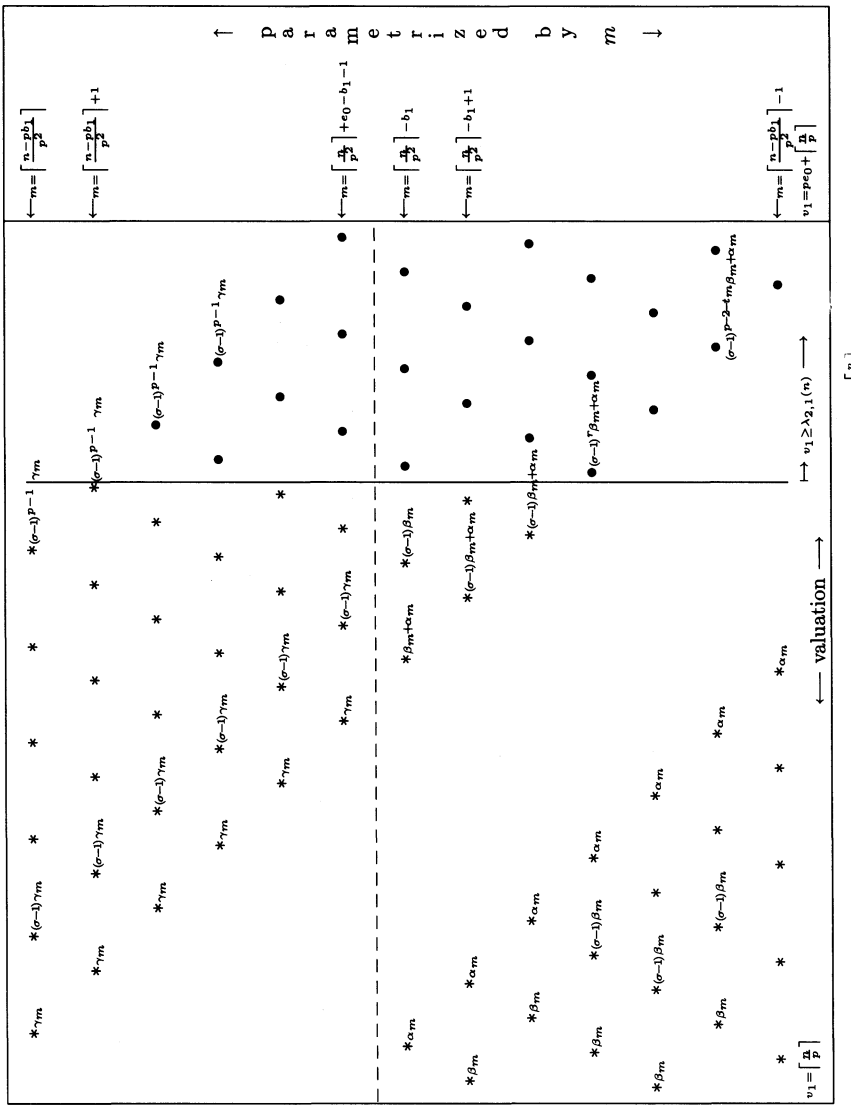
$$v_1((\sigma-1)^{p-t_m-2}\beta_m + \alpha_m) = b_1 + pe_0 + pm, \tag{11}$$

and $v_1((\sigma-1)^i\beta_m) = (i-(p-t_m-3))b_1 + pe_0 + pm$ where $i = p-t_m-1, \ldots, p-2$.

For $m = \left\lceil \frac{n-pb_1}{p^2} \right\rceil, \ldots, e_0 + \left\lceil \frac{n}{p^2} \right\rceil - b_1 - 1$,

$$v_1((\sigma-1)^i\gamma_m) = (i+1)b_1 + pm \text{ where } i = 0, \ldots, p-1. \tag{12}$$

Next, we graph this basis in Figure I, plotting the valuation of each member of the basis against the parameter m. This diagram will prove insightful, turning some of the arguments that follow into easy exercises. Note that each horizontal row, determined by a fixed value of m, represents an $\mathfrak{O}_T[G]$- module, which is either a copy of $\mathfrak{O}_T \otimes_{\mathbb{Z}_p[G]} E$ (for each row above the dotted line) or a copy of $\mathfrak{O}_T \otimes_{\mathbb{Z}_p[G]} (Z \oplus R_1)$ (for each row below the dotted line). By placing a vertical line at the point where the valuation is $\lambda_{2,1}(n)$, we are able to visually discern which elements of our $\mathfrak{O}_T$-basis of $\mathfrak{P}_1^{\left\lceil \frac{n}{p} \right\rceil}$ lie in $\mathfrak{P}_1^{\lambda_{2,1}(n)}$, the image of $\mathfrak{P}_2^n$ under the trace. Let $\bullet$'s represent basis elements which lie in $\mathfrak{P}_1^{\lambda_{2,1}(n)}$ while $*$'s represent basis elements which do not lie in $\mathfrak{P}_1^{\lambda_{2,1}(n)}$. Let M be the collection of m's (rows) which have as a member, a basis element in $\mathfrak{P}_1^{\lambda_{2,1}(n)}$. Now for each $m \in M$, let ρ_m be the basis element in $\mathfrak{P}_1^{\lambda_{2,1}(n)}$ which has minimal valuation, and for each


valuation
$v_1 \geq \lambda_{2,1}(n)$
$v_1 = \lceil \frac{n}{p} \rceil$
$v_1 = pe_0 + \lceil \frac{n}{p} \rceil$
$m = \lceil \frac{n-pb_1}{p^2} \rceil - 1$
$m = \lceil \frac{n-pb_1}{p^2} \rceil + 1$
$m = \lceil \frac{n}{p^2} \rceil - b_1$
$m = \lceil \frac{n}{p^2} \rceil - b_1 + 1$
$m = \lceil \frac{n}{p^2} \rceil + e_0 - b_1 - 1$
$(\sigma-1)^{p-1}\gamma_m$
$(\sigma-1)^{p-1}\gamma_m$
$(\sigma-1)^{p-1}\gamma_m$
$(\sigma-1)^{p-1}\gamma_m$
$(\sigma-1)\gamma_m$
$(\sigma-1)\gamma_m$
$(\sigma-1)\gamma_m$
$(\sigma-1)\gamma_m$
$(\sigma-1)\gamma_m$
$(\sigma-1)\beta_m$
$(\sigma-1)\beta_m$
$(\sigma-1)\beta_m$
$(\sigma-1)\beta_m$
$(\sigma-1)\beta_m$
$(\sigma-1)\beta_m$
$(\sigma-1)\beta_m$
$(\sigma-1)\beta_m$
$(\sigma-1)\beta_m+\alpha_m$
$(\sigma-1)\beta_m+\alpha_m$
$(\sigma-1)\beta_m+\alpha_m$
$(\sigma-1)\beta_m+\alpha_m$
$(\sigma-1)^r\beta_m+\alpha_m$
$(\sigma-1)^{p-2-t}m\beta_m+\alpha_m$
γ_m
γ_m
γ_m
γ_m
γ_m
γ_m
γ_m
α_m
α_m
$\alpha

$m \notin M$, let $\rho_m = 0$. It is then easily seen that $\{\rho_m | m \in M\}$ generates $\mathfrak{P}_1^{\lambda_{2,1}(n)}/p\mathfrak{P}_1^{\left\lceil \frac{n}{p} \right\rceil}$ over $\mathfrak{O}_T/p\mathfrak{O}_T[G]$. And if we let $\rho_{m,j} = \rho_m \cdot \eta_j$ where the η_j's were defined in Theorem 2, then $\{\rho_{m,j} | m \in M, j = 1, \ldots, f\}$ generates $\mathfrak{P}_1^{\lambda_{2,1}(n)}/p\mathfrak{P}_1^{\left\lceil \frac{n}{p} \right\rceil}$ over $\mathbb{F}_p[G]$.

Our next lemma determines the ρ_m's for $m = \left\lceil \frac{n - pb_1}{p^2} \right\rceil, \ldots, e_0 + \left\lceil \frac{n}{p^2} \right\rceil - b_1 - 1$.

LEMMA 5.

Let $s = \max\left\{0, (p-1) + \left\lceil \frac{\lambda_{2,1}(n) - pe_0 - p\left\lceil \frac{n}{p^2} \right\rceil + p}{b_1} \right\rceil\right\}$. *Then :*

for $\left\lceil \frac{n - pb_1}{p^2} \right\rceil \leq m \leq \left\lceil \frac{\lambda_{2,1}(n) - pb_1}{p} \right\rceil - 1$, $v_1((\sigma-1)^{p-1}\gamma_m) < \lambda_{2,1}(n)$, $\rho_m = 0$;

for $\left\lceil \frac{\lambda_{2,1}(n) - pb_1}{p} \right\rceil \leq m \leq \left\lceil \frac{\lambda_{2,1}(n) - (p-1)b_1}{p} \right\rceil - 1$, $\rho_m = (\sigma-1)^{p-1}\gamma_m$;

for $\left\lceil \frac{\lambda_{2,1}(n) - (p-1)b_1}{p} \right\rceil \leq m \leq \left\lceil \frac{\lambda_{2,1}(n) - (p-2)b_1}{p} \right\rceil - 1$, $\rho_m = (\sigma-1)^{p-2}\gamma_m$;

$\vdots$

for $\left\lceil \frac{\lambda_{2,1}(n) - (s+2)b_1}{p} \right\rceil \leq m \leq \left\lceil \frac{\lambda_{2,1}(n) - (s+1)b_1}{p} \right\rceil - 1$, $\rho_m = (\sigma-1)^{s+1}\gamma_m$;

and for $\left\lceil \frac{\lambda_{2,1}(n) - (s+1)b_1}{p} \right\rceil \leq m \leq e_0 + \left\lceil \frac{n}{p^2} \right\rceil - b_1 - 1$, $\rho_m = (\sigma-1)^s\gamma_m$.

Proof. — This is an easy exercise using (12). □

In our next lemma we show that for each row below the dotted line, ρ_m lies strictly to the right of α_m.

LEMMA 6.

$v_1(\alpha_m) < \lambda_{2,1}(n)$ *for every* $m = \left\lceil \frac{n}{p^2} \right\rceil - b_1, \ldots, \left\lceil \frac{n - pb_1}{p^2} \right\rceil - 1$.

Proof. — By (10) $v_1(\alpha_m) = p(b_1 + m)$. All we need to show is that $\lambda_{2,1}(n) > p\left(b_1 + \left\lceil \frac{n - pb_1}{p^2} \right\rceil - 1\right)$. The proof breaks up into two cases : Case 1. If $b_1 \geq \frac{e_0}{p-1}$ then by [20, Cor 29, Thm 33], $b_2 = b_1 + pe_0$, and one can easily check that the inequality is satisfied. Case 2. If $b_1 < \frac{e_0}{p-1}$, consider the Kummer case where $\zeta_p \in K_0$, ζ_p denotes a primitive pth root of unity. By [20, Thm 32], $b_2 = \frac{p^2 e_0}{p-1} - pj + b_1$ for $b_1 \leq j \leq \Psi_{K_1/K_0}\left(\frac{e_0}{p-1}\right)$ where Ψ_{K_1/K_0} is defined in [18] pg 73. Using [18] and the fact that $b_1 \leq \frac{e_0}{p-1}$, it is easily shown that $\Psi_{K_1/K_0}\left(\frac{e_0}{p-1}\right) = p\left(\frac{e_0}{p-1} - b_1\right) + b_1$. And so clearly, $b_2 \geq \left(\frac{p^2 e_0}{p-1} - p\Psi_{K_1/K_0}\left(\frac{e_0}{p-1}\right) + b_1\right) = (p^2 - p + 1)b_1$. Now, it is an easy exercise to check that this inequality implies the desired inequality.

In the other case, where $\zeta_p \notin K_0$, $[K_0(\zeta_p) : K_0] = d$ for some $d \mid p-1$, and $K_2(\zeta_p)/K_0(\zeta_p)$ is a cyclic fully ramified extension of degree p^2 with lower ramification numbers, $b_2' = db_2$, $b_1' = db_1$ 20, Thm 15]. Clearly $b_2' \geq (p^2 - p + 1)b_1'$ implies $b_2 \geq (p^2 - p + 1)b_1$, from which we can, once again, deduce the desired inequality. □

As a result of Lemma 6, for each $m = \left\lceil \frac{n}{p^2} \right\rceil - b_1, \ldots, \left\lceil \frac{n - pb_1}{p^2} \right\rceil - 1$, $v_1(\rho_m) > v_1(\alpha_m)$. Therefore it must be that $\rho_m = (\sigma - 1)^{p-2-t_m}\beta_m + \alpha_m$; or $\rho_m = (\sigma - 1)^{i_m + p - 2 - t_m}\beta_m$ for some i_m, $1 \leq i_m \leq t_m$; or if $\lambda_{2,1}(n) > v_1\left((\sigma - 1)^{p-2}\beta_m\right)$, then $\rho_m = 0$. In order to determine which of these is the case, we group the m's together according to the value of t_m. These groupings will be useful in verifying subsequent lemmas.

$$
\begin{aligned}
&\text{For } \left\lceil \frac{n - p^2 b_1}{p^2} \right\rceil \leq m \leq \left\lceil \frac{n - (p-1)pb_1}{p^2} \right\rceil - 1,\ t_m = p - 2, \\
&\text{for } \left\lceil \frac{n - (p-1)pb_1}{p^2} \right\rceil \leq m \leq \left\lceil \frac{n - (p-2)pb_1}{p^2} \right\rceil - 1,\ t_m = p - 3, \\
&\text{for } \left\lceil \frac{n - (p-2)pb_1}{p^2} \right\rceil \leq m \leq \left\lceil \frac{n - (p-3)pb_1}{p^2} \right\rceil - 1,\ t_m = p - 4, \\
&\qquad\qquad \vdots \\
&\text{and for } \left\lceil \frac{n - 2pb_1}{p^2} \right\rceil \leq m \leq \left\lceil \frac{n - pb_1}{p^2} \right\rceil - 1,\ t_m = 0.
\end{aligned}
\tag{13}
$$

For $\left\lceil \frac{n}{p^2} \right\rceil - b_1 \leq m < \max\left\{ \left\lceil \frac{n}{p^2} \right\rceil - b_1, \lambda_{2,0}(n) - e_0 - b_1 \right\}$, the ρ_m's lie strictly to the right of $(\sigma-1)^{p-2-t_m}\beta_m+\alpha_m$, because $v_1\left((\sigma-1)^{p-2-t_m}\beta_m+\alpha_m\right) < \lambda_{2,1}$. We determine these ρ_m's in the following lemma.

LEMMA 7. — *Let* $r = \max\left\{0, \left\lfloor \frac{p^2(\lambda_{2,0}(n)-e_0)-n}{pb_1} \right\rfloor\right\}$, *and for* $j = 0, 1, \ldots, r$ *let* $s_j = \max\left\{0, (p-1+j) + \left\lceil \frac{\lambda_{2,1}(n) - pe_0 - p\left\lceil \frac{n+jpb_1}{p^2} \right\rceil}{b_1} \right\rceil\right\}$.

Then if

$$\tau_{m,k} = \begin{cases} (\sigma-1)^k\beta_m & k \leq p-2 \\ 0 & k \geq p-1. \end{cases}$$

For $j = 0, \ldots, r-1$ *when*

$$\left\lceil \frac{n-(p-j)pb_1}{p^2} \right\rceil \leq m \leq \min\left\{ \left\lceil \frac{\lambda_{2,1}(n)-(s_j-j)b_1}{p} \right\rceil - e_0, \left\lceil \frac{n-(p-j-1)pb_1}{p^2} \right\rceil \right\} - 1, \quad \rho_m = \tau_{m,s_j},$$

while when

$$\left\lceil \frac{\lambda_{2,1}(n)-(s_j-j)b_1}{p} \right\rceil - e_0 \leq m \leq \left\lceil \frac{n-(p-j-1)pb_1}{p^2} \right\rceil - 1,$$

$\rho_m = \tau_{m,s_j-1}$.

For $\left\lceil \frac{n-(p-r)pb_1}{p^2} \right\rceil \leq m \leq \lambda_{2,0}(n) - e_0 - b_1 - 1$, $\rho_m = \tau_{m,s_r}$.

Proof. — It is an easy calculation to show that for each $j = 0, \ldots, r$, s_i is the smallest power of $\sigma-1$ such that $v_1\left((\sigma-1)^{s_i}\rho_m\right) \geq \lambda_{2,1}(n)$ where $m = \left\lceil \frac{n-(p-j)pb_1}{p^2} \right\rceil$. It is also easy to check that for each $j = 0, \ldots, r$, if for $m = \left\lceil \frac{n-(p-j-1)pb_1}{p^2} \right\rceil - 1$, $v_1\left((\sigma-1)^t\rho_m\right) \geq \lambda_{2,1}(n)$, then for $m = \left\lceil \frac{n-(p-j)pb_1}{p^2} \right\rceil$, $v_1\left((\sigma-1)^{t+1}\rho_m\right) \geq \lambda_{2,1}(n)$. Therefore for each span of m's, $\left\lceil \frac{n-(p-j)pb_1}{p^2} \right\rceil \leq m \leq \left\lceil \frac{n-(p-j-1)pb_1}{p^2} \right\rceil - 1$, $\rho_m = \tau_{m,s_j}$ or $\rho_m = \tau_{m,s_j-1}$, and if $\left\lceil \frac{n-(p-r)pb_1}{p^2} \right\rceil < \lambda_{2,0}(n) - e_0 - b_1 - 1$,

then $s_r = r+1$. It is then, easy to check that $\lambda_{2,0}(n) = b_1 + \left\lceil \dfrac{\lambda_{2,1}(n) - b_1}{p} \right\rceil$. The lemma quickly follows. □

We now determine the rest of the ρ_m.

LEMMA 8. — *Let* $r = \max\left\{0, \left\lfloor \dfrac{p^2(\lambda_{2,0}(n) - e_0) - n}{pb_1} \right\rfloor\right\}$.

Then for

$$\max\left\{\left\lceil \frac{n}{p^2} \right\rceil - b_1, \lambda_{2,0}(n) - e_0 - b_1\right\} \leq m \leq \left\lceil \frac{n - (p-r-1)pb_1}{p^2} \right\rceil - 1,$$

$\rho_m = (\sigma - 1)^r \beta_m + \alpha_m$;

for $$\left\lceil \frac{n - (p-r-1)pb_1}{p^2} \right\rceil \leq m \leq \left\lceil \frac{n - (p-r-2)pb_1}{p^2} \right\rceil - 1,$$

$$\rho_m = (\sigma - 1)^{r+1} \beta_m + \alpha_m;$$

$$\vdots$$

and for $\left\lceil \dfrac{n - 2pb_1}{p^2} \right\rceil \leq m \leq \left\lceil \dfrac{n - pb_1}{p^2} \right\rceil - 1$, $\rho_m = (\sigma - 1)^{p-2} \beta_m + \alpha_m$.

Proof. — This is an easy exercise using (11) and (13). □

Step 3. In this step we construct generators of $\mathfrak{P}_2^n / \mathfrak{P}_1^{\left\lceil \frac{n}{p} \right\rceil}$ over $\mathbb{Z}_p[G]$. These generators are constructed to be compatible with the generators of $\mathfrak{P}_1^{\lambda_{2,1}(n)} / p\mathfrak{P}_1^{\left\lceil \frac{n}{p} \right\rceil}$ over $\mathbb{F}_p[G]$ given by the $\{\rho_{m,j} \mid m \in M, j = 1, \ldots f\}$ in the previous step. In the next two lemmas, we construct an explicit basis for $\mathfrak{P}_2^n$ over $\mathfrak{O}_T$ in an analogous fashion to the construction in Lemma 2.

LEMMA 9. — *Let* μ_t *for* $t = \left\lceil \dfrac{n}{p} \right\rceil, \ldots, pe_0 + \left\lceil \dfrac{n}{p} \right\rceil - 1$ *be the element listed in* (10), (11) *and* (12) *such that* $v_1(\mu_t) = t$. *Then there are elements,* $\{\nu_{ap+b_2}\}_{a \in \mathbb{Z}} \in K_2$, *with* $v_2(\nu_{ap+b_2}) = ap + b_2$ *such that they have the following property :*

$$T_{K_2/K_1}(\nu_{ap+b_2}) = p^{\left\lfloor \frac{b_2+a}{pe_0} \right\rfloor} \mu_{b_2+a-\left\lfloor \frac{b_2+a}{pe_0} \right\rfloor pe_0}.$$

And for $i = 0, 1, 2, \ldots, p-1$, $v_2\left((\sigma^p - 1)^i \nu_{ap+b_2}\right) = ap + (i+1)b_2$.

Proof. — From (1) and (2), $T_{K_2/K_1}(\mathfrak{P}_2^{ap+b_2}) = T_{K_2/K_1}(\mathfrak{P}_2^{ap+b_2-1}) = \cdots = T_{K_2/K_1}(\mathfrak{P}_2^{ap+b_2-(p-1)}) = \mathfrak{P}_1^{a+b_2}$. Therefore, for any a there exists an element $\nu_{ap+b_2} \in \mathfrak{P}_2^{ap+b_2}/\mathfrak{P}_2^{ap+b_2+1}$ with the aforementioned property. It is easy to show as in Lemma 1 that for $i = 0, 1, \ldots, p-1$, $v_2\left((\sigma^p - 1)^i \nu_{ap+b_2}\right) = ap + (i+1)b_2$. □

Clearly the elements $\left\{(\sigma^p - 1)^i \nu_{ap+b_2}\right\}$ for $i = 0, 1, \ldots, p-1$ and $a \in \mathbb{Z}$ have distinct valuations. As in Lemma 2, we may therefore select from this collection only those elements such that $0 \leq v_2\left((\sigma^p - 1)^i \nu_{ap+b_2}\right) \leq p^2 e_0 - 1$, and from them form an $\mathfrak{O}_T$-basis of $\mathfrak{O}_2$. Using these elements, we construct a basis for $\mathfrak{P}_2^n$ over $\mathfrak{O}_T$ as in Lemma 2.

LEMMA 10 . — *Let* $t_a = \left\lceil \frac{n - pa}{b_2} \right\rceil - 2$. *Then*

$$\mathfrak{P}_2^n = \sum_{a=n-b_2}^{n+\left\lceil \frac{-b_2}{p} \right\rceil - 1} \mathfrak{O}_T \Phi_{p^2}(\sigma) \nu_{ap+b_2} + \sum_{a=n+\left\lceil \frac{-b_2}{p} \right\rceil}^{pe_0+n-b_2-1} \sum_{i=0}^{p-1} \mathfrak{O}_T (\sigma^p - 1)^i \nu_{ap+b_2}$$

$$+ \sum_{a=n-b_2}^{n+\left\lceil \frac{-b_2}{p} \right\rceil - 1} \left(\sum_{i=t_a+1}^{p-2} \mathfrak{O}_T (\sigma^p - 1)^i \nu_{ap+b_2} + \sum_{i=0}^{t_a} \mathfrak{O}_T (\sigma^p - 1)^i p \nu_{ap+b_2} \right).$$

Proof. — Similar to Lemma 2.

We now change the basis of Lemma 10, making it more suitable for our needs. Using the fact that every element of (10), (11) and (12) which lies in $\mathfrak{P}_1^{\lambda_{2,1}(n)}$ has the form $(\sigma - 1)^i \rho_m$ for some $m \in M$ and some $i \geq 0$, we see that for any ν_{ap+b_2} with $a < pe_0 + \left\lceil \frac{n}{p} \right\rceil - b_2$, $T_{K_2/K_1}(\nu_{ap+b_2}) = (\sigma - 1)^i \rho_m$ for some $m \in M$ and $i \geq 0$. If $T_{K_2/K_1}(\nu_{ap+b_2}) = (\sigma - 1)^i \rho_m$ for $i > 0$, then there is another a' such that $T_{K_2/K_1}(\nu_{a'p+b_2}) = \rho_m$, and we may replace ν_{ap+b_2} by $\nu_{ap+b_2} - (\sigma - 1)^{i_a} \nu_{a'p+b_2}$. We do this for all $a < pe_0 + \left\lceil \frac{n}{p} \right\rceil - b_2$. For every other $\mathfrak{O}_T$-basis element, τ, given by Lemma 10, we replace τ by $\tau - \frac{1}{p} T_{K_2/K_1}(\tau)$. In this manner we end up with a collection of elements in $\mathfrak{P}_2^n$ with the following two properties : 1) The nonzero elements of this collection form an $\mathfrak{O}_T$-basis for $\mathfrak{P}_2^n/\mathfrak{P}_1^{\left\lceil \frac{n}{p} \right\rceil}$. 2) This $\mathfrak{O}_T$-basis for $\mathfrak{P}_2^n/\mathfrak{P}_1^{\left\lceil \frac{n}{p} \right\rceil}$ breaks up into two disjoint sets; the first set, which may be parametrized

by $m \in M$, lies in one to one correspondance under the trace map with the nonzero ρ_m, while the second set is annihilated by the trace, T_{K_2/K_1}.

For ease of notation, we relable the $\mathfrak{O}_T$-basis of $\mathfrak{P}_2^n/\mathfrak{P}_1^{\lceil \frac{n}{p} \rceil}$ given in the previous paragraph. Each member of the first set, ν_{ap+b_2}, where $T_{K_2/K_1}(\nu_{ap+b_2}) = \rho_m$ for a nonzero ρ_m, we denote by ν_m where $m \in M$ and $T_{K_2/K_1}(\nu_m) = \rho_m$. Each member of the second set, which is killed by the trace, is denoted by ν_m for some $m \in \{0, 1, \ldots, e_0 p(p-1)\} - M$. Let $\eta_1, \eta_2, \ldots, \eta_f$ be the basis for $\mathfrak{O}_T$ over $\mathbb{Z}_p$ given in Theorem 2. Then $\nu_{m,j} = \eta_j \cdot \nu_m$ for $m \in M$ and $j = 1, \ldots f$ is a $\mathbb{Z}_p$-basis for $\mathfrak{P}_2^n/\mathfrak{P}_1^{\lceil \frac{n}{p} \rceil}$.

In the following lemma, we show that the elements $\nu_{m,j} = \eta_j \cdot \nu_m$ for $m \in M$ and $j = 1, \ldots f$ can be extended to a $\mathbb{Z}_p[G]$-module basis of $\mathfrak{P}_2^n/\mathfrak{P}_1^{\lceil \frac{n}{p} \rceil}$.

LEMMA 11. — *Let* $\nu_1, \nu_2, \ldots, \nu_s, \nu_{s+1}, \ldots, \nu_{e_0 f(p^2-p)}$ *be elements of* $\mathfrak{P}_2^n$ *which form a* $\mathbb{Z}_p$*-basis for* $\mathfrak{P}_2^n/\mathfrak{P}_1^{\lceil \frac{n}{p} \rceil}$ *and have the following properties :*

$T_{K_2/K_1}(\nu_1), T_{K_2/K_1}(\nu_2), \ldots, T_{K_2/K_1}(\nu_s)$ *form an* $\mathbb{F}_p[G]$*-basis of* $\mathfrak{P}_1^{\lambda_{2,1}(n)}/p\mathfrak{P}_1^{\lceil \frac{n}{p} \rceil}$ *and*

$T_{K_2/K_1}(\nu_i) = 0$ *for* $i = s+1, \ldots, e_0 f(p^2-p)$.

Then $\nu_1, \nu_2, \ldots, \nu_s$ *can be extended to a* $\mathbb{Z}_p[G]$*-basis of* $\mathfrak{P}_2^n/\mathfrak{P}_1^{\lceil \frac{n}{p} \rceil}$.

Proof. — Clearly, $\mathfrak{P}_2^n/\mathfrak{P}_1^{\lceil \frac{n}{p} \rceil}$ is a $\mathbb{Z}_p$-torsion free module which is annihilated by $T_{K_2/K_1} = \Phi_{p^2}(\sigma)$. As such, $\mathfrak{P}_2^n/\mathfrak{P}_1^{\lceil \frac{n}{p} \rceil}$ is a module over the principle ideal domain, $\mathbb{Z}_p[\zeta_{p^2}] \cong \dfrac{\mathbb{Z}_p[G]}{\Phi_{p^2}(\sigma)} = R_2$. It is well known then, that $\mathfrak{P}_2^n/\mathfrak{P}_1^{\lceil \frac{n}{p} \rceil}$ is free as an R_2-module. By checking ranks, clearly $\mathfrak{P}_2^n/\mathfrak{P}_1^{\lceil \frac{n}{p} \rceil} \cong R_2^{e_0 f}$ as $\mathbb{Z}_p[G]$- modules. Let $x_1, x_2, \ldots, x_{e_0 f}$ be elements of $\mathfrak{P}_2^n$ which form a $\mathbb{Z}_p[G]$-basis of $\mathfrak{P}_2^n/\mathfrak{P}_1^{\lceil \frac{n}{p} \rceil}$. So for each j, $\mathbb{Z}_p[G]x_j \cong R_2$, and $\mathfrak{P}_2^n/\mathfrak{P}_1^{\lceil \frac{n}{p} \rceil} = \sum_{j=1}^{e_0 f} \mathbb{Z}_p[G]x_j \cong R_2^{e_0 f}$. Then because the x_j form a $\mathbb{Z}_p[G]$-basis of $\mathfrak{P}_2^n/\mathfrak{P}_1^{\lceil \frac{n}{p} \rceil}$, for each $i = 1, 2, \ldots, s$, $\nu_i = \sum_{j=1}^{e_0 f} f_{i,j}(\sigma)x_j + A_i$ for some $f_{i,j}(\sigma) \in \mathbb{Z}_p[G]$ and some $A_i \in \mathfrak{P}_1^{\lceil \frac{n}{p} \rceil}$. Because the ν_i form a $\mathbb{Z}_p$-basis of

$\mathfrak{P}_2^n/\mathfrak{P}_1^{\lceil \frac{n}{p} \rceil}$, for each $j = 1, 2, \ldots e_0 f$, $x_j = \sum_{k=1}^{s} a_{j,k}\nu_k + \sum_{k=s+1}^{e_0 f(p^2-p)} a_{j,k}\nu_k + B_j$ for some $a_{j,k} \in \mathbb{Z}_p$ and $B_j \in \mathfrak{P}_1^{\lceil \frac{n}{p} \rceil}$. We can act via the trace on both of these expressions to find that :

$$T_{K_2/K_1}\nu_i \equiv \sum_{j=1}^{e_0 f} f_{i,j}(\sigma) T_{K_2/K_1} x_j + p\mathfrak{P}_1^{\lceil \frac{n}{p} \rceil},$$

$$T_{K_2/K_1} x_j \equiv \sum_{k=1}^{s} a_{j,k} T_{K_2/K_1}\nu_k + p\mathfrak{P}_1^{\lceil \frac{n}{p} \rceil}.$$

And so for each $i = 1, 2, \ldots, s$,

$$T_{K_2/K_1}\nu_i \equiv \sum_{j=1}^{e_0 f} f_{i,j}(\sigma) \sum_{k=1}^{s} a_{j,k} T_{K_2/K_1}\nu_k + p\mathfrak{P}_1^{\lceil \frac{n}{p} \rceil}.$$

Since the $T_{K_2/K_1}\nu_i$ form a $\mathbb{F}_p[G]$-basis of $\dfrac{T_{K_2/K_1}(\mathfrak{P}_2^n)}{p\mathfrak{P}_1^{\lceil \frac{n}{p} \rceil}} = \mathfrak{P}_1^{\lambda_{2,1}(n)}/p\mathfrak{P}_1^{\lceil \frac{n}{p} \rceil}$, we find that in $\mathbb{F}_p[G/H]$,

$$1 = \sum_{j=1}^{e_0 f} \overline{f_{i,j}(\sigma) a_{j,i}}, \text{ and } 0 = \sum_{j=1}^{e_0 f} \overline{f_{i,j}(\sigma) a_{j,k}}, \text{ for } k \neq i,$$

where $H = \langle \sigma^p \rangle$. In particular, we have found that for each ν_i there is a j_i such that in fact $f_{i,j_i}(\sigma) a_{j_i,i}$ is a unit in $\mathbb{Z}_p[G]$. Consider $i = 1$. Because $f_{1,j_1}(\sigma)$ is a unit in $\mathbb{Z}_p[G]$, we may change the $\mathbb{Z}_p[G]$-basis of $\mathfrak{P}_2^n/\mathfrak{P}_1^{\lceil \frac{n}{p} \rceil}$, replacing x_{j_1} by $f_{1,j_1}(\sigma)x_{j_1} + \sum_{j \neq j_1} f_{1,j}(\sigma)x_j + A_1 = \nu_1$. Now consider $i = 2$. There is a j_2 such that $f_{2,j_2}(\sigma)$ is a unit in $\mathbb{Z}_p[G]$. If $j_1 = j_2$ and $f_{2,j}$ is not a unit for any $j \neq j_2$, then $T_{K_2/K_1}(\nu_2) = f_{2,j_2}(\sigma) T_{K_2/K_1}(\nu_1) + \sum_{j \neq j_2} f_{2,j}(\sigma)x_j + A_2$, and

$$\overline{T_{K_2/K_1}(\nu_2)} \equiv \overline{f_{2,j_2}(\sigma) T_{K_2/K_1}(\nu_1)}, \text{ in } \frac{\mathfrak{P}_1^{\lambda_{2,1}}}{p\mathfrak{P}_1^{\lceil \frac{n}{p} \rceil} + (\sigma - 1)\mathfrak{P}_1^{\lambda_{2,1}(n)}},$$

which contradicts the fact that the ν_i are in one to one correspondance under T_{K_2/K_1} with a $\mathbb{F}_p[G/H]$- basis of $\mathfrak{P}_1^{\lambda_{2,1}(n)}/p\mathfrak{P}_1^{\lceil \frac{n}{p} \rceil}$. Therefore we may assume that $j_2 \neq j_1$ and replace x_{j_2} by $f_{2,j_2}(\sigma)x_{j_2} + \sum_{j \neq j_2} f_{2,j}(\sigma)x_j + A_2 = \nu_2$.

Clearly we can continue this process until we have replaced s elements of our $\mathbb{Z}_p[G]$-basis of $\mathfrak{P}_2^n/\mathfrak{P}_1^{\lceil \frac{n}{p} \rceil}$ by $\nu_1, \nu_2, \ldots, \nu_s$. This proves the lemma. □

As a result of this lemma, we may conclude that there is a $\mathbb{Z}_p[G]$-basis of $\mathfrak{P}_2^n/\mathfrak{P}_1^{\lceil \frac{n}{p} \rceil}$ consisting of elements $\nu_{m,j}$ for $m = -b_1, \ldots, e_0 - b_1 - 1$, $j = 1, \ldots, f$, such that

$$T_{K_2/K_1}(\nu_{m,j}) = \rho_m \cdot \eta_j \overset{\text{defn}}{=} \rho_{m,j}, \tag{14}$$

the nonzero $\rho_{m,j}$ constituting an $\mathbb{F}_p[G]$- basis of $T_{K_2/K_1}(\mathfrak{P}_2^n)/p\mathfrak{P}_1^{\lceil \frac{n}{p} \rceil}$.

Step 4. The main result

In the following proof we make liberal use of the arguments in [5] §8A, §34B & §34C] . As in the proof of Lemma 11, $\mathfrak{P}_2^n/\mathfrak{P}_1^{\lceil \frac{n}{p} \rceil} \cong R_2^{e_0 f}$ as $\mathbb{Z}_p[G]$-modules. Let $\nu_{m,j}$ be the $\mathbb{Z}_p[G]$-module basis of $\mathfrak{P}_2^n/\mathfrak{P}_1^{\lceil \frac{n}{p} \rceil}$ given in (14). Then

$$\mathfrak{P}_2^n/\mathfrak{P}_1^{\lceil \frac{n}{p} \rceil} = \sum_{m=\lceil \frac{n}{p^2} \rceil - b_1}^{e_0 + \lceil \frac{n}{p^2} \rceil - b_1 - 1} \sum_{j=1}^{f} \mathbb{Z}_p[G]\nu_{m,j} \overset{\eta}{\cong} R_2^{e_0 f}. \tag{15}$$

From now on we will suppress the range of values that m and j take and simply refer to $\sum_m$ and $\sum_j$ instead of $\sum_{m=\lceil \frac{n}{p^2} \rceil - b_1}^{e_0 + \lceil \frac{n}{p^2} \rceil - b_1 - 1}$ and $\sum_{j=1}^{f}$. Let ι be the inclusion map and π, the projection map. We have the following $\mathbb{Z}_p[G]$-exact short sequence,

$$0 \to \mathfrak{P}_1^{\lceil \frac{n}{p} \rceil} \xrightarrow{\iota} \mathfrak{P}_2^n \xrightarrow{\eta \circ \pi} R_2^{e_0 f} \to 0, \tag{16}$$

which determines an element ξ in $Ext^1_{\mathbb{Z}_p[G]}\left(\mathfrak{P}_2^n/\mathfrak{P}_1^{\lceil \frac{n}{p} \rceil}, \mathfrak{P}_1^{\lceil \frac{n}{p} \rceil}\right)$. Let $\{z_{m,f}\}$ be indeterminates with $\sum_m \sum_j \mathbb{Z}_p[G]z_{m,j}$ a free $\mathbb{Z}_p[G]$-module and let $y_{m,j} = \Phi_{p^2}(\sigma)z_{m,j}$. Let $\gamma \in \mathrm{Hom}_{\mathbb{Z}_p[G]}\left(\sum_m \sum_j \mathbb{Z}_p[G]z_{m,j}, \mathfrak{P}_2^n\right)$ be induced by $\gamma(z_{m,j}) = \nu_{m,j}$ which in turn induces $\mu \in \mathrm{Hom}_{\mathbb{Z}_p[G]}\left(\sum_m \sum_j \mathbb{Z}_p[G]y_{m,j},\right.$

$\mathfrak{P}_1^{\lceil \frac{n}{p} \rceil}\Big)$ such that $\mu(y_{m,j}) = \rho_{m,j}$. We have the following $\mathbb{Z}_p[G]$ commutative diagram,

$$\begin{array}{ccccccccc} 0 \to & \sum_m \sum_j \mathbb{Z}_p[G] y_{m,j} & \to & \sum_m \sum_j \mathbb{Z}_p[G] z_{m,j} & \to & R_2^{e_0 f} & \to 0 \\ & \mu \downarrow & & \gamma \downarrow & & = \downarrow & \\ 0 \to & \mathfrak{P}_1^{\lceil \frac{n}{p} \rceil} & \xrightarrow{\iota} & \mathfrak{P}_2^n & \xrightarrow{\eta \circ \pi} & R_2^{e_0 f} & \to 0. \end{array}$$

As in [5] pg 174-6, §34C , the $\mathbb{Z}_p[G]$- module structure of $\mathfrak{P}_2^n$ is completely determined by

$$\overline{\mu} \in \frac{\mathrm{Hom}_{\mathbb{Z}_p[G]}\left(\sum_m \sum_j \mathbb{Z}_p[G] y_{m,j}, \mathfrak{P}_1^{\lceil \frac{n}{p} \rceil}\right)}{p\mathrm{Hom}_{\mathbb{Z}_p[G]}\left(\sum_m \sum_j \mathbb{Z}_p[G] y_{m,j}, \mathfrak{P}_1^{\lceil \frac{n}{p} \rceil}\right)},$$

which is completely determined by the matrix A mapping $\rho_{m,j}$ to its expression in terms of the basis elements of Theorem 2. Outside of the case where a column of A contains a $\rho_{m,j} = (\sigma - 1)^{p-2-t_m}\beta_{m,j} + \alpha_{m,j} \in R_1 \oplus Z$ (as in Lemma 8), it is easy to see that any row and column of this matrix which intersect at a nonzero $\rho_{m,j}$ are zero elsewhere. As a result, a copy of $(R_2, E; \lambda^i)$ if $\rho_{m,j} = (\sigma - 1)^i \gamma$ or $(R_2, R_1; \lambda^i)$ if $\rho_{m,j} = (\sigma - 1)^i \beta_m$ decomposes off of $\mathfrak{P}_2^n$. In the case where a column contains a $\rho_{m,j} = (\sigma - 1)^{p-2-t_m}\beta_{m,j} + \alpha_{m,j} \in R_1 \oplus Z$, it is easy to see that the column is zero outside of the two places where $(\sigma - 1)^{p-2-t_m}\beta_{m,j}$ and $\alpha_{m,j}$ appear, and that the two rows intersecting the column at $(\sigma - 1)^{p-2-t_m}\beta_{m,j}$ and $\alpha_{m,j}$ are zero elsewhere, and as a result a copy of $(R_2, Z \oplus R_1; 1 \oplus \lambda^{p-2-t_m})$ decomposes off of $\mathfrak{P}_2^n$.

Therefore using Lemmas 5, 7 and 8, one arrives at Theorem 1. □

4. Remarks.

One can generate cyclic extensions of degree p^2 with prescribed lower ramification numbers using the results of Maus [13], Miki [14] and Wyman [20]. In particular, as we did in Lemma 6, one can use [20] Thm 32.

We observe that using our main result and [16] Table 2, one can generalize [16] Thm 3, unconditionally determining the modular representation

given by $\mathfrak{P}_2^n/p\mathfrak{P}_2^n$. One can also use our main result to prove a global theorem, as was done in [16] Thm 5, generalizing a Theorem of Yokoi [21] Thm 3.

Finally we observe that only $3p$ of the possible $4p+1$ indecomposable modules given by Heller and Reiner [5] Thm 34.32, actually appear in the decomposition of the ring of integers of a local field. What are the intrinsic reasons for this? When G is a p-group, neither cyclic of order p nor cyclic of order p^2, there are infinitely many inequivalent indecomposable $\mathbb{Z}_p[G]$-modules [5] pg 690. Which of these can occur in a fractional ideal of a local number field extension, L/K, with $\mathrm{Gal}(L/K) \cong G$? The answer to these interesting questions, even under some weak arithmetic condition, should have a profound effect upon future results concerning the the $\mathbb{Z}_p[G]$- module structure of $\mathfrak{O}_L$.

BIBLIOGRAPHY

[1] A.-M. BERGÉ, Sur l'arithmétique d'une extension cyclique totalement ramifiée d'une corps local, C. R. Acad. Sc. Paris, 281 (1975), 67-70.

[2] F. BERTRANDIAS, Sur les extensions cycliques de degré p^n d'un corps local, Acta Arith., 34-4 (1979), 361-377.

[3] F. BERTRANDIAS, J.-P. BERTRANDIAS, M.-J. FERTON, Sur l'anneau des entiers d'une extension cyclique de degré premier d'un corps local, C. R. Acad. Sc. Paris, 274 (1972), 1388-1391.

[4] N. BYOTT, On Galois isomorphisms between ideals in extensions of local fields, Manuscripta Math., 73 (1991), 289- 311.

[5] C. W. CURTIS, and I. REINER, Methods of Representation Theory, Wiley, New York, 1981.

[6] G. G. ELDER, and M. L. MADAN, Galois module structure of integers in wildly ramified cyclic extensions, J. Number Theory, 47 #2 (1994), 138-174.

[7] M.-J. FERTON, Sur L'anneau des entiers de certaines extensions cycliques d'un corps local, Astérisque, 24-25 (1975), 21-28.

[8] A. FRÖHLICH, Galois Module Structure of Algebraic Integers, Ergebnisse der Mathematik und ihrer Grenzgebiete, 3 Folge, Bd. 1, Springer-Verlag, Berlin-Heidelberg-New York, 1983.

[9] H. HASSE, Bericht über neuere Untersuchungen und Probleme aus der Theorie der Algebraischen Zahlkörper, Physica-Verlag, Würzburg- Wien, 1970.

[10] H. W. LEOPOLDT, Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers, J. Reine Angew. Math., 201 (1959), 119-149.

[11] R. E. MACKENZIE, and G. WHAPLES, Artin-Schreier equations in characteristic zero, Am. J. of Math., 78 (1956), 473-485.

[12] J. MARTINET, Bases normales et constante de l'équation fonctionnelle des fonctions L d'Artin, Séminaire Bourbaki (1973/74) no. 450.

[13] E. MAUS, Existenz $\mathfrak{P}$-adischer Zahlkörper zu Vorgegebenem Verzweigungsverhalten, Dissertation, Hamburg, 1965.

[14] H. MIKI, On the ramification numbers of cyclic p-extensions over local fields, J. Reine Angew. Math., 328 (1981), 99-115.

[15] Y. MIYATA, On the module structure of a p- extension over a p-adic number field, Nagoya Math. J., 77, (1980), 13-23.

[16] M. RZEDOWSKI-CALDERÓN, G. D. VILLA- SALVADOR, M. L. MADAN, Galois module structure of rings of integers, Math. Z., 204 (1990), 401-424.

[17] S. SEN, On automorphisms of local fields, Ann. Math., (2) 90 (1969), 33-46.

[18] J-P. SERRE, Local fields, Graduate Texts Mathematics, Vol. 67. Springer- Verlag, Berlin-Heidelberg-New York 1979.

[19] S. V. VOSTOKOV, Ideals of an abelian p- extension of a local field as Galois modules, Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Akad. Nauk. SSSR, 57 (1976), 64-84.

[20] B. WYMAN, Wildly ramified gamma extensions, Am. J. Math., 91 (1969), 135-152.

[21] 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.

Manuscrit reçu le 21 avril 1994,
accepté le 5 décembre 1994.

Gove GRIFFITH ELDER,
Department of Mathematics
The University of Nebraska et Omaha
203 Durham Science Center
Omaha NE 68182-0243 (USA).