Can. J. Math. Vol. **49** (4), 1997 pp. 722–735.

GALOIS MODULE STRUCTURE OF THE INTEGERS IN WILDLY RAMIFIED $C_p \times C_p$ EXTENSIONS

G. GRIFFITH ELDER AND MANOHAR L. MADAN

ABSTRACT. Let L/K be a finite Galois extension of local fields which are finite extensions of $\mathbb{Q}_p$, the field of p-adic numbers. Let $\mathrm{Gal}(L/K) = G$, and $\mathfrak{O}_L$ and $\mathbb{Z}_p$ be the rings of integers in L and $\mathbb{Q}_p$, respectively. And let $\mathfrak{P}_L$ denote the maximal ideal of $\mathfrak{O}_L$. We determine, explicitly in terms of specific indecomposable $\mathbb{Z}_p[G]$-modules, the $\mathbb{Z}_p[G]$-module structure of $\mathfrak{O}_L$ and $\mathfrak{P}_L$, for L, a composite of two arithmetically disjoint, ramified cyclic extensions of K, one of which is only weakly ramified in the sense of Erez [6].

1. Introduction

Let L/K be a finite Galois extension of number fields with Galois group, G. If $\mathfrak{O}_L$, $\mathfrak{O}_K$ denote their rings of integers and $\mathbb{Z}$ denotes the ring of rational integers, one may ask for the structure of $\mathfrak{O}_L$ as an $\mathfrak{O}_K[G]$-module, or as a $\mathbb{Z}[G]$-module. In either case, unfortunately, the Krull-Schmidt Theorem fails to hold, *i.e.* $\mathfrak{O}_L$ is not necessarily uniquely expressible as a direct sum of indecomposable modules. However, in the special case when K is the field of rationals, G is abelian and $[L : K]$ is relatively prime to the discriminant of L, Hilbert proved in 1897 that there is an element $\alpha \in \mathfrak{O}_L$ whose conjugates form a $\mathbb{Z}$-basis of $\mathfrak{O}_L$, *i.e.* $\mathfrak{O}_L$ is free as a $\mathbb{Z}[G]$-module. (By the Normal Basis Theorem for fields, a field basis of this type always exists.) The existence of a normal integral basis is subject to arithmetic constraints. We refer the reader to Fröhlich's book, [7], for results concerning the existence of such a basis.

The Krull-Schmidt Theorem is valid if L/K is a finite Galois extension of local fields, *i.e.* finite extensions of $\mathbb{Q}_p$, the field of p-adic numbers. As a consequence of a theorem of E. Noether [12], when the extension, L/K, is at most tamely ramified, $\mathfrak{O}_L \cong \mathbb{Z}_p[G]^{n_0}$ as $\mathbb{Z}_p[G]$-modules, where $[K : \mathbb{Q}_p] = n_0$ and $\mathbb{Z}_p$ denotes the ring of p-adic integers and $G = \mathrm{Gal}(L/K)$. If however, the extension is wildly ramified, very little is known. We refer the reader to Miyata [11] and Vostokov [18] for some results concerning the $\mathfrak{O}_K[G]$-module structure of $\mathfrak{O}_L$, and to other papers of the authors for some situations where the $\mathbb{Z}_p[G]$-module structure of $\mathfrak{O}_L$ is known. In particular, we cite the paper of the second author with Rzedowski-Calderón and Villa-Salvador [13]; it was in [13] that this type of question was first asked. We also draw particular attention to [4] where this type of question is answered for elementary abelian, weakly ramified extensions of arbitrarily large degree.

In this paper, we explicitly determine the $\mathbb{Z}_p[G]$-module structure of $\mathfrak{O}_L$ when L is a totally ramified elementary abelian extension of K with degree p^2 and has two breaks

Received by the editors May 21, 1996.
AMS subject classification: Primary: 11S15; secondary: 20C32.
Key words and phrases: Galois module structure—integral representation.

https://doi.org/10.4153/CJM-1997-035-2 Published online by Cambridge University Press

in its ramification filtration, the first break occurring with ramification number one. Equivalently, this means considering the family of extensions, L/K, which arise as the composite of two arithmetically disjoint, ramified cyclic extensions of degree p, one of which is only weakly ramified [6] (*i.e.* One of the two cyclic extensions has ramification number equal to one).

We note that it is an easy exercise to determine the explicit $\mathbb{Z}_p[G]$-module structure of $\mathfrak{O}_L$ in the case where L is the composite of an unramified cyclic extension of degree p, L_u, and a ramified cyclic extension of degree p, L_w. Simply use the fact that in this situation $\mathfrak{O}_L = \mathfrak{O}_u \cdot \mathfrak{O}_w$, where $\mathfrak{O}_u$ and $\mathfrak{O}_w$ are the rings of integers in L_u and L_w, respectively, and $\mathfrak{O}_u$ has a normal integral basis. See the example in Section 8 for further details.

Once one has considered partially ramified elementary abelian extensions it is natural to consider fully ramified extensions. However to keep complications to a minimum, it is perhaps natural to consider extensions which are the composite of two fields, one of which is now only weakly ramified. This is what we do. Ullom [17] determined that although the ring of integers in a weakly ramified extension does not have a normal integral basis, the maximal ideal does.

As our following main result shows, one finds a very interesting and complicated $\mathbb{Z}_p[G]$-module structure in the situation that we consider.

THEOREM 1. *Let L/K be a totally ramified elementary abelian extension of local number fields, with $[L : K] = p^2$ and $G = \mathrm{Gal}(L/K) = \langle \sigma, \gamma \rangle$ where the ramification group $G_{b_2} = \langle \sigma \rangle$. Let $[K : \mathbb{Q}_p] = e_0 f$, e_0 denoting the absolute ramification index. Furthermore, let L/K have two distinct lower ramification numbers, b_1 and b_2, with n and r, nonnegative integers where $r \in \{0, 1, \ldots, p-1\}$ so that $b_2 = b_1 + p(np - r)$.*

If $b_1 = 1$ and $r \neq 1$, then

$$\begin{aligned}\mathfrak{O}_L \cong{}& E^{(n(p-1)-r)f} \oplus (R_1 \otimes E, E; \lambda^r)^f \oplus (R_1 \otimes E, E; 1)^{(e_0 - n(p-1)+r-2)f} \\ &\oplus (R_1 \otimes E, Z \oplus R_1; 1 \oplus 1)^f \oplus (R_1 \otimes E)^{(n(p-1)-r)f}.\end{aligned}$$

If $b_1 = 1$ and $r = 1$, then

$$\mathfrak{O}_L \cong \begin{cases} E^{(e_0-1)f} \oplus Z^f \oplus R_1^f \oplus (R_1 \otimes E)^{e_0 f} & \text{for } p = 2, \\ E^{(e_0-1)f} \oplus Z^f \oplus (R_1 \otimes E, R_1; \lambda)^f \oplus (R_1 \otimes E)^{(e_0-1)f} & \text{for } p \neq 2; \end{cases}$$

as $\mathbb{Z}_p[G]$-modules. The $\mathbb{Z}_p[G]$-modules are described below.

Here are explicit descriptions of the indecomposable $\mathbb{Z}_p[G]$-modules. In each case σ acts via multiplication by x, while γ acts via multiplication by y. Let $\Phi_p(x) = (x^p - 1)/(x - 1)$ be the cyclotomic polynomial.

$$Z = \frac{\mathbb{Z}_p[x, y]}{\langle x - 1, y - 1 \rangle}, \quad R_1 = \frac{\mathbb{Z}_p[x, y]}{\langle x - 1, \Phi_p(y) \rangle}, \quad E = \frac{\mathbb{Z}_p[x, y]}{\langle x - 1, y^p - 1 \rangle},$$

$$(R_1 \otimes E, E; \lambda^i) = \frac{\frac{\mathbb{Z}_p[x,y]}{\langle x^p - 1, y^p - 1 \rangle} \oplus \frac{\mathbb{Z}_p[x,y]}{\langle x - 1, y^p - 1 \rangle}}{\Big\langle \big(\Phi_p(x), (y-1)^i\big) \Big\rangle},$$

https://doi.org/10.4153/CJM-1997-035-2 Published online by Cambridge University Press

$$R_1 \otimes E = \frac{\mathbb{Z}_p[x,y]}{\langle \Phi_p(x), y^p - 1\rangle}, \quad (R_1 \otimes E, R_1; \lambda) = \frac{\frac{\mathbb{Z}_p[x,y]}{\langle x^p-1, y^p-1\rangle} \oplus \frac{\mathbb{Z}_p[x,y]}{\langle x-1, \Phi_p(y)\rangle}}{\Big\langle \big(\Phi_p(x), y-1\big)\Big\rangle},$$

$$(R_1 \otimes E, Z \oplus R_1; 1 \oplus 1) = \frac{\frac{\mathbb{Z}_p[x,y]}{\langle x^p-1, y^p-1\rangle} \oplus \frac{\mathbb{Z}_p[x,y]}{\langle x-1, y-1\rangle} \oplus \frac{\mathbb{Z}_p[x,y]}{\langle x-1, \Phi_p(y)\rangle}}{\Big\langle \big(\Phi_p(x), 1, 1\big)\Big\rangle}.$$

Note that $(R_1 \otimes E, E; \lambda^0) \cong \mathbb{Z}_p[G]$. For the convenience of the reader, we provide a table recording certain other properties of these modules.

We also state here the result for the $\mathbb{Z}_p[G]$-module structure of $\mathfrak{P}_L$, the unique maximal ideal of $\mathfrak{O}_L$.

THEOREM 2. *Under the conditions of the previous theorem. If $b_1 = 1$,*

$$\mathfrak{P}_L \cong E^{(n(p-1)-r)f} \oplus (R_1 \otimes E, E; \lambda^r)^f \oplus (R_1 \otimes E, E; 1)^{(e_0-n(p-1)+r-1)f} \oplus (R_1 \otimes E)^{(n(p-1)-r)f}$$

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

The method of our proof, at times, involves investigating $\mathfrak{O}_T[G]$-module structure, where $\mathfrak{O}_T$ denotes the ring of integers in the field, T, which is the maximal unramified extension of $\mathbb{Q}_p$ contained in K. In particular, we create a basis over $\mathfrak{O}_T$ of elements with distinct valuations upon which we can track the Galois action. From the $\mathfrak{O}_T[G]$-module structure, the $\mathbb{Z}_p[G]$-module structure can be deduced.

In Section 2, we explain the assumption on the ramification filtration and the reason for the restriction of our attention to the two fractional ideals, $\mathfrak{O}_L$ and $\mathfrak{P}_L$.

In Section 3, we establish our notation. Then in Section 4 through Section 7 we prove our two theorems.

At the end, in Section 8, we give an application of Theorem 1. We explicitly determine the Galois module structure of the ring of integers in the maximal elementary abelian p-extension of an arbitrary ramified quadratic extension of $\mathbb{Q}_p$, when $p > 3$.

We believe that the methods of this paper and those used in [3], [4], [5], and [13] may be applied to prove structure theorems of this type for other classes of arithmetically distinguished extensions. However, the proof of a structure theorem in complete generality will, probably, require new techniques.

2. Motivation for the ramification assumption

In this section, we motivate the assumption, $b_1 = 1$ and also explain why we have restrict our attention to $\mathfrak{O}_L$ and $\mathfrak{P}_L$.

Let us focus our attention for the moment on $\mathfrak{O}_L$. Let K' be any intermediate extension of an elementary abelian extension, L/K, of degree p^2 (K'/K has degree p). Let $\mathfrak{O}_{K'}$ be the ring of integers in K', then the following canonical short exact sequence,

$$0 \longrightarrow \mathfrak{O}_{K'} \longrightarrow \mathfrak{O}_L \longrightarrow \mathfrak{O}_L/\mathfrak{O}_{K'} \longrightarrow 0,$$

can be used to determine the Galois module structure of $\mathfrak{O}_L$. (Indeed, an analogous sequence is provided in (2) which can be used to investigate the Galois module structure of other fractional ideals.) From [13, Theorem 1], the $\mathbb{Z}_p[G]$-structure of $\mathfrak{O}_{K'}$ is known. If

https://doi.org/10.4153/CJM-1997-035-2 Published online by Cambridge University Press

https://doi.org/10.4153/CJM-1997-035-2 Published online by Cambridge University Press

Column	I	II	III	IV	V	VI	VII
M/G	M^σ	M^γ	As $\mathbb{Z}_p[\sigma]$-module $M \cong Z^a \oplus R_1^b \oplus E^c$ $(a, b, c) =$	$T_{L/K_1}(M)$ as $\mathbb{Z}_p[\sigma]$ -module	M/M^G	$H^0(\sigma, M)$ as $\mathbb{F}[\gamma]$ -module	$H^0(G, M)$
Z	Z	Z	$(1, 0, 0)$	Z	0	$L(1)$	C_{p^2}
R_1	R_1	0	$(p-1, 0, 0)$	R_1	R_1	$L(p-1)$	0
E	E	Z	$(p, 0, 0)$	E	R_1	$L(p)$	C_p
$R_1 \otimes E$	0	R_1	$(0, p, 0)$	0	$R_1 \otimes E$	$L(0)$	0

$(R_1 \otimes E, E; \lambda^i)$
$0 \leq i \leq p-1$
	E	E
		if $i = 0$
		$Z \oplus R_1$
		if $i > 0$
			$(i, i, p-i)$	E
				if $i = 0$
				$Z \oplus R_1$
				if $i > 0$
					$(R_1 \otimes E, R_1; \lambda^i)$
					if $0 \leq i \leq p-2$
					$R_1 \oplus (R_1 \otimes E)$
					if $i = p-1$
						$L(i)$	0
							if $i = 0$
							C_p
							if $i > 0$

$(R_1 \otimes E, R_1; \lambda)$ $0 \leq i \leq p-2$	R_1	R_1	$(1, 2, p-2)$	R_1	$(R_1 \otimes E, R_1; \lambda)$	$L(1)$	0
$(R_1 \otimes E, Z \oplus R_1; 1 \oplus \lambda^i)$ $0 \leq i \leq p-2$	$Z \oplus R_1$	$Z \oplus R_1$	$(i+1, i+1, p-i-1)$	E	$(R_1 \otimes E, R_1; \lambda^i)$	$L(i+1)$	C_p

Properties of certain $\mathbb{Z}_p[C_p \times C_p]$-modules the $\mathbb{Z}_p[G]$-module structure of $\mathfrak{O}_L/\mathfrak{O}_{K'}$ could be determined, then we could investigate the structure of $\mathfrak{O}_L$ by describing the $\mathbb{Z}_p[G]$- module, $\mathrm{Ext}^1_{\mathbb{Z}_p[G]}(\mathfrak{O}_L/\mathfrak{O}_{K'}, \mathfrak{O}_{K'})$.

Unfortunately, in general, the structure of the $\mathbb{Z}_p[G]$-module, $\mathfrak{O}_L/\mathfrak{O}_{K'}$, can be unlimited in potential complexity. If $\mathrm{Gal}(L/K') = \langle\sigma\rangle$, where $\mathrm{Gal}(L/K) = \langle\sigma,\gamma\rangle$, then since the relative trace, $T_{L/K'} = \Phi_p(\sigma)$, takes $\mathfrak{O}_L$ into $\mathfrak{O}_{K'}$, the $\mathbb{Z}_p[G]$-module, $\mathfrak{O}_L/\mathfrak{O}_{K'}$, can be reinterpreted as a $\mathbb{Z}_p[\zeta_p][\langle\gamma\rangle]$-module, where ζ_p is a primitive p-th root of unity. Jacobinski has shown that, for $p > 3$, there are infinitely many indecomposable $\mathbb{Z}_p[\zeta_p][\langle\gamma\rangle]$-modules [1, p. 691]. To avoid the difficulty that this result presents, in this paper we restrict ourselves to circumstances under which $\mathfrak{O}_L/\mathfrak{O}_{K'}$ is free as a $\mathbb{Z}_p[\zeta_p][\langle\gamma\rangle]$-module,

$$(1) \qquad \mathfrak{O}_L/\mathfrak{O}_{K'} \cong \mathbb{Z}_p[\zeta_p][\langle\gamma\rangle]^{n_0}.$$

(We furthermore restrict ourselves to those ideals for which the analogous result holds.)

As the following lemma indicates, in order for (1) to hold, it is necessary that there be a subfield, K'', of L/K distinct from K' such that the extension L/K'' has ramification number equal to one.

LEMMA 1. *Unless there is an intermediate extension, K'', such that the ramification number of L/K'' is 1, it is not possible that*

$$\mathfrak{O}_L/\mathfrak{O}_{K'} \cong \mathbb{Z}_p[\zeta_p][\langle\gamma\rangle]^{n_0} \quad \textit{as } \mathbb{Z}_p[G]\textit{-modules},$$

where $\langle\gamma\rangle = \mathrm{Gal}(L/K'')$, K' is distinct from K'' and $\langle\sigma\rangle = \mathrm{Gal}(L/K')$.

PROOF. Clearly, $\mathbb{Z}_p[\zeta_p][\langle\gamma\rangle] \cong \mathbb{Z}_p[\langle\gamma\rangle]^{p-1}$ as $\mathbb{Z}_p[\langle\gamma\rangle]$-modules and so the cohomology group $H^0(\langle\gamma\rangle, \mathbb{Z}_p[\zeta_p][\langle\gamma\rangle]^{n_0}) = 0$. However, if the ramification number of L/K'' is greater than 1, then π'', a prime element of K'', gives a nonzero element of $H^0(\langle\gamma\rangle, \mathfrak{O}_L/\mathfrak{O}_{K'})$. ■

In order for an intermediate extension, K'', to exist with the ramification number of L/K'' equal to one, it is necessary that the first lower ramification number of L/K be one.

Before we go on, we turn our attention to the question of determining the $\mathbb{Z}_p[G]$-module structure of other fractional ideals. We remark that since $1 \in \mathfrak{O}_L$ also lies in $\mathfrak{O}_{K'}$, there is the following canonical isomorphism:

$$\mathfrak{O}_L/\mathfrak{O}_{K'} \cong \mathfrak{P}_L/\mathfrak{P}_{K'} \text{ as } \mathbb{Z}_p[G]\text{-modules}.$$

Now let $\mathfrak{P}_L^i$ be any fractional ideal. Clearly the canonical short exact sequence exists, which can be used to determine the Galois module structure of $\mathfrak{P}_L^i$,

$$(2) \qquad 0 \longrightarrow \mathfrak{P}_{K'}^{\lceil i/p\rceil} \longrightarrow \mathfrak{P}_L^i \longrightarrow \mathfrak{P}_L^i/\mathfrak{P}_{K'}^{\lceil i/p\rceil} \longrightarrow 0,$$

where $\lceil x\rceil$ denoting the least integer function, and $\mathfrak{P}_{K'}^{\lceil i/p\rceil}$ is the largest fractional ideal in K' contained in $\mathfrak{P}_L^i$. Obviously $\mathfrak{O}_L \cong \pi_K^t\mathfrak{O}_L$ and $\mathfrak{P}_L \cong \pi_K^t\mathfrak{P}_L$ as $\mathbb{Z}_p[G]$-modules. As a result, the only fractional ideals of L which we have not considered are those

https://doi.org/10.4153/CJM-1997-035-2 Published online by Cambridge University Press

fractional ideals, $\mathfrak{P}_L^i$, for which i is not congruent to 0 or 1 modulo p^2. As the following lemma shows unless $i \equiv 0, 1 \bmod p^2$, it is never the case that $\mathfrak{P}_L^i / \mathfrak{P}_{K'}^{\lceil i/p \rceil}$ is free as a $\mathbb{Z}_p[\zeta_p][\langle\gamma\rangle]$-module.

LEMMA 2. *Unless $i \equiv 0, 1 \bmod p^2$, it is not possible that*

$$\mathfrak{P}_L^i / \mathfrak{P}_{K'}^{\lceil i/p \rceil} \cong \mathbb{Z}_p[\zeta_p][\langle\gamma\rangle]^{n_0} \quad \textit{as } \mathbb{Z}_p[G]\textit{-modules},$$

PROOF. Following the proof of Lemma 1, one sees that $\pi''^{\lceil i/p \rceil}$, where π'' is a prime element of K'', is a nonzero element of $H^0(\langle\gamma\rangle, \mathfrak{P}_L^i / \mathfrak{P}_{K'}^{\lceil i/p \rceil})$ whenever $i \not\equiv 0, 1 \bmod p^2$. ■

As a consequence of these lemmas we restrict our attention to the two ideals, $\mathfrak{O}_L$ and $\mathfrak{P}_L$, and furthermore assume the first ramification number of L/K to be one.

3. **Notation** We standardize our notation. Assume that L/K has two distinct ramification numbers, $b_1 = 1$ and b_2, where necessarily $b_2 = 1 + p(t-1)$ for some t greater than 1. Let K_1 be the fixed field of the ramification group $G_{b_2} = \langle\sigma\rangle$, and let K_2 be any intermediate extension distinct from K_1 with $\mathrm{Gal}(L/K_2) = \langle\gamma\rangle$. Then the ramification number of L/K_2 equals the ramification number of K_1/K which is 1. The ramification number of L/K_1 is b_2 and the ramification number of K_2/K is t. Now, there exist unique $n \in \mathbb{Z}$ and $r \in \{0, 1, \ldots, p-1\}$, such that $b_2 = 1 + p(np - r)$. Clearly, $t - 1 = np - r$.

Let T be the maximal unramified extension of $\mathbb{Q}_p$ contained in K. Let $\mathfrak{O}_L$, $\mathfrak{O}_1$, $\mathfrak{O}_2$, $\mathfrak{O}_K$, $\mathfrak{O}_T$ be the ring of integers in L, K_1, K_2, K, and T respectively. Let $\mathfrak{P}_L$, $\mathfrak{P}_1$, $\mathfrak{P}_2$, $\mathfrak{P}_K$, $\mathfrak{P}_T$ be their unique maximal ideals, π_L, π_1, π_2, π_K, π_T prime elements and v_L, v_1, v_2, v_K, v_T the additive valuations of these respective fields such that $v_L(\pi_L) = v_1(\pi_1) = v_2(\pi_2) = v_K(\pi_K) = v_T(\pi_T) = 1$.

We let $\lambda(i)$ be the largest power of $\mathfrak{P}_K$ to divide $\mathfrak{P}_L^i \mathfrak{D}_{L/K}$, where $\mathfrak{D}_{L/K}$ is the relative different. Similarly we let $\lambda_2(i)$ be the largest power of $\mathfrak{P}_K$ to divide $\mathfrak{P}_{K_2}^i \mathfrak{D}_{K_2/K}$, letting $\lambda_2(0)$ be simply λ_2. Since L/K_2, and K_1/K have the same ramification number we can let $\lambda_1(i)$ denote both the largest power of $\mathfrak{P}_K$ to divide $\mathfrak{P}_{K_1}^i \mathfrak{D}_{K_1/K}$ and the largest power of $\mathfrak{P}_{K_2}$ to divide $\mathfrak{P}_L^i \mathfrak{D}_{L/K_2}$. We finally let $\lambda_2'(i)$ be the largest power of $\mathfrak{P}_{K_1}$ to divide $\mathfrak{P}_L^i \mathfrak{D}_{L/K_1}$.

It can be easily shown using [15, p. 64 Proposition 4] and $b_1 = 1$, that

$$\lambda(i) = \left\lfloor \frac{i + (2)(p^2-1) + (b_2-1)(p-1)}{p^2} \right\rfloor, \lambda_2(i) = \left\lfloor \frac{i + (t+1)(p-1)}{p} \right\rfloor,$$

$$\lambda_1(i) = \left\lfloor \frac{i + (2)(p-1)}{p} \right\rfloor, \quad \lambda_2'(i) = \left\lfloor \frac{i + \big(2 + p(t-1)\big)(p-1)}{p} \right\rfloor, \tag{3}$$

where $\lfloor x \rfloor$ denotes the greatest integer less than or equal to x. Note that $\lambda_2'(0) = \lambda_2'(1) = (np-r)(p-1) + 1$, and that

$$\left\lceil \frac{\lambda_2'(0)}{p} \right\rceil = n(p-1) - r + 1.$$

https://doi.org/10.4153/CJM-1997-035-2 Published online by Cambridge University Press

As a result of ramification theory [15], if $T_{L/K}$ denotes the relative trace from L to K, and $T_{L/K_1}, T_{L/K_2}, T_{K_1/K}, T_{K_2/K}$ are defined similarly,

$$\text{(4)}\qquad \begin{gathered} T_{L/K}(\mathfrak{P}_L^i) = \mathfrak{P}_K^{\lambda(i)}, \quad T_{L/K_1}(\mathfrak{P}_L^i) = \mathfrak{P}_1^{\lambda_2'(i)}, \quad T_{L/K_2}(\mathfrak{P}_L^i) = \mathfrak{P}_2^{\lambda_1(i)}, \\ T_{K_1/K}(\mathfrak{P}_1^i) = \mathfrak{P}_K^{\lambda_1(i)}, \quad T_{K_2/K}(\mathfrak{P}_2^i) = \mathfrak{P}_K^{\lambda_2(i)}. \end{gathered}$$

4. **The structure of $\mathfrak{O}_L/\mathfrak{O}_1$** Now we establish the fact that $b_1 = 1$ is sufficient for $\mathfrak{O}_L/\mathfrak{O}_1$ to be a free $\mathbb{Z}_p[\zeta_p][\langle\gamma\rangle]$-module. (Note that $\mathfrak{P}_L/\mathfrak{P}_1 \cong \mathfrak{O}_L/\mathfrak{O}_1$. We will not make further reference to $\mathfrak{P}_L/\mathfrak{P}_1$ in this section.)

LEMMA 3.
$$\frac{\mathfrak{O}_L/\mathfrak{O}_1}{(\sigma-1)\mathfrak{O}_L/\mathfrak{O}_1} \cong \mathbb{F}_p[\langle\gamma\rangle]^{n_0}$$
as an $\mathbb{F}_p[\langle\gamma\rangle]$-module, where $\mathbb{F}_p$ is the field of p elements.

PROOF. Since $\mathfrak{O}_L/\mathfrak{O}_1$ is a $\mathbb{Z}_p[\zeta_p][\langle\gamma\rangle]$-module, $\frac{\mathfrak{O}_L/\mathfrak{O}_1}{(\sigma-1)\mathfrak{O}_L/\mathfrak{O}_1}$ is an $\mathbb{F}_p[\langle\gamma\rangle]$-module, where the indecomposable $\mathbb{F}_p[\langle\gamma\rangle]$-modules are $L(i) = \frac{\mathbb{F}_p[x]}{(x-1)^i}$ for $i = 1, 2, \ldots, p$ and γ acts via multiplication by x. Note that $L(p) \cong \mathbb{F}_p[\langle\gamma\rangle]$. So there are nonnegative integers $\{a_i\}_{i=1}^p$, such that
$$\frac{\mathfrak{O}_L/\mathfrak{O}_1}{(\sigma-1)\mathfrak{O}_L/\mathfrak{O}_1} \cong \oplus\sum_{i=1}^{p} L(i)^{a_i}$$
as $\mathbb{F}_p[\langle\gamma\rangle]$-modules. Now $\frac{\mathfrak{O}_L/\mathfrak{O}_1}{(\sigma-1)\mathfrak{O}_L/\mathfrak{O}_1} \cong \frac{\mathfrak{O}_L}{(\sigma-1)\mathfrak{O}_L+\mathfrak{O}_1}$ and so,
$$(\gamma-1)^{p-1}\left(\frac{\mathfrak{O}_L}{(\sigma-1)\mathfrak{O}_L+\mathfrak{O}_1}\right) = (\gamma-1)^{p-1}L(p)^{a_p}.$$

Since $(\gamma-1)^{p-1} \equiv 1+\gamma+\cdots+\gamma^{p-1} \bmod p$, and $\dim_{\mathbb{F}_p}\bigl((\gamma-1)^{p-1}L(p)\bigr) = 1$, we find that,
$$a_p = \dim_{\mathbb{F}_p}\left((1+\gamma+\cdots+\gamma^{p-1})\frac{\mathfrak{O}_L}{(\sigma-1)\mathfrak{O}_L+\mathfrak{O}_1}\right).$$
By (3) and (4), $(1+\gamma+\cdots+\gamma^{p-1})\mathfrak{O}_L = \mathfrak{P}_2^{\lambda_1} = \mathfrak{P}_2$. Therefore we calculate:

$$\text{(5)}\qquad a_p = \dim_{\mathbb{F}_p}\left(\frac{\mathfrak{P}_2+(\sigma-1)\mathfrak{O}_L+\mathfrak{O}_1}{(\sigma-1)\mathfrak{O}_L+\mathfrak{O}_1}\right) = \dim_{\mathbb{F}_p}\left(\frac{\mathfrak{P}_2}{\mathfrak{P}_2\cap\bigl((\sigma-1)\mathfrak{O}_L+\mathfrak{O}_1\bigr)}\right).$$

In order to calculate this dimension, we simplify its denominator:

If $\alpha \in \mathfrak{O}_L, \beta \in \mathfrak{O}_1$ and $\tau \in \mathfrak{P}_2$ such that $(\sigma-1)\alpha+\beta = \tau$, then $p\beta = (1+\sigma+\cdots+\sigma^{p-1})\tau$ and so $\beta \in \mathfrak{O}_K$. Since $v_L((\sigma-1)\alpha) \geq 1+b_2 > 0$ and $v_L(\tau) \geq p > 0$, it follows that $v_L(\beta) > 0$. Therefore $\beta \in \mathfrak{P}_K$, and we find that $\mathfrak{P}_2\cap\bigl((\sigma-1)\mathfrak{O}_L+\mathfrak{O}_1) = \bigl(\mathfrak{P}_2\cap(\sigma-1)\mathfrak{O}_L\bigr)+\mathfrak{P}_K$. Now if $\alpha \in \mathfrak{O}_L$, $\tau \in \mathfrak{P}_2$ such that $(\sigma-1)\alpha = \tau$, then $(1+\sigma+\cdots+\sigma^{p-1})\tau = 0$. Since $v_L\bigl((\sigma-1)\alpha\bigr) \geq 1+b_2$, $\tau \in \mathfrak{P}_2\cap\mathfrak{P}_L^{1+b_2} = \mathfrak{P}_2^{\lceil\frac{1+b_2}{p}\rceil}$. Let $y_0 = 1$, $y_1 = \pi_2$, $y_2 = \sigma\pi_2\cdot\pi_2$, $y_2 = \sigma^2\pi_2\cdot\sigma\pi_2\cdot\pi_2, \cdots$ as in Sen [14]; so that $v_2\bigl((\sigma-1)y_i\bigr) = i+t$ for $(i,p) = 1$,

https://doi.org/10.4153/CJM-1997-035-2 Published online by Cambridge University Press

$(\sigma - 1)y_{pi} = 0$. Using these y_i's as a basis for $\mathfrak{P}_2^{\lceil \frac{1+b_2}{p} \rceil - t}$ over $\mathfrak{O}_T$, it is easy to see (as in [9, Prop 4]) that the part of $\mathfrak{P}_2^{\lceil \frac{1+b_2}{p} \rceil}$ killed by the trace $(1 + \sigma + \cdots + \sigma^{p-1})$ is $(\sigma - 1)\mathfrak{P}_2^{\lceil \frac{1+b_2}{p} \rceil - t}$. Therefore $\tau \in (\sigma - 1)\mathfrak{P}_2^{\lceil \frac{1+b_2}{p} \rceil - t}$. Since $\lceil \frac{1+b_2}{p} \rceil - t = 0$, $\tau \in (\sigma - 1)\mathfrak{O}_2$. The extension K_2/K is fully ramified, therefore $(\sigma - 1)\mathfrak{O}_2 = (\sigma - 1)\mathfrak{P}_2$. So, $(\sigma - 1)\alpha \in (\sigma - 1)\mathfrak{P}_2$ and we find that

$$\mathfrak{P}_2 \cap \big((\sigma - 1)\mathfrak{O}_L + \mathfrak{O}_1\big) = \big(\mathfrak{P}_2 \cap (\sigma - 1)\mathfrak{O}_L\big) + \mathfrak{P}_K = (\sigma - 1)\mathfrak{P}_2 + \mathfrak{P}_K.$$

As a result, (5) can be rewritten as,

$$a_p = \dim_{\mathbb{F}_p}\left(\frac{\mathfrak{P}_2}{(\sigma - 1)\mathfrak{P}_2 + \mathfrak{P}_K}\right).$$

For $\tau \in \mathfrak{P}_2$, $(1 + \sigma + \cdots + \sigma^{p-1})\tau \equiv p\tau\big(\mathrm{mod}(\sigma - 1)\mathfrak{P}_2\big)$, therefore $p\mathfrak{P}_2 \subseteq (\sigma - 1)\mathfrak{P}_2 + \mathfrak{P}_K$. Let

$$0 \longrightarrow \frac{(\sigma - 1)\mathfrak{P}_2 + \mathfrak{P}_K}{p\mathfrak{P}_2} \longrightarrow \frac{\mathfrak{P}_2}{p\mathfrak{P}_2} \longrightarrow \frac{\mathfrak{P}_2}{(\sigma - 1)\mathfrak{P}_2 + \mathfrak{P}_K} \longrightarrow 0 \tag{6}$$

be the canonical short $\mathbb{F}_p$-exact sequence. Clearly, $\dim_{\mathbb{F}_p}(\frac{\mathfrak{P}_2}{p\mathfrak{P}_2}) = pe_0$. To calculate $\dim_{\mathbb{F}_p}(\frac{\mathfrak{P}_2}{(\sigma-1)\mathfrak{P}_2 + \mathfrak{P}_K})$, using (6), we will first calculate, $\dim_{\mathbb{F}_p}(\frac{(\sigma-1)\mathfrak{P}_2 + \mathfrak{P}_K}{p\mathfrak{P}_2})$. Using the proof of [13, Theorem 1] we find that

$$\mathfrak{P}_2 \cong Z^{(\lambda_2(1)-1)f} \oplus R_1^{(\lambda_2(1)-1)f} \oplus E^{n_0-(\lambda_2(1)-1)f} \quad \text{as } \mathbb{Z}_p[\langle\sigma\rangle]\text{-modules.}$$

So there are elements $\{\alpha_i, \beta_i, \tau_i\}$ in $\mathfrak{P}_2$ such that

$$\mathfrak{P}_2 = \sum_{i=1}^{(\lambda_2(1)-1)f} \mathbb{Z}_p\alpha_i + \sum_{i=1}^{(\lambda_2(1)-1)f} \frac{\mathbb{Z}_p[\sigma]}{\Phi_p(\sigma)}\beta_i + \sum_{i=1}^{(e_0-\lambda_2(1)+1)f} \mathbb{Z}_p[\sigma]\tau_i \tag{7}$$

And from this explicit basis it is easy to explicitly determine $\mathfrak{P}_K$ and $(\sigma - 1)\mathfrak{P}_2$, and find that

$$\dim_{\mathbb{F}_p}\left(\frac{(\sigma - 1)\mathfrak{P}_2 + \mathfrak{P}_K}{p\mathfrak{P}_2}\right) = (p - 1)e_0 f. \tag{8}$$

Using (6) ,(7), we find that

$$a_p = \dim_{\mathbb{F}_p}\left(\frac{\mathfrak{P}_2}{(\sigma - 1)\mathfrak{P}_2 + \mathfrak{P}_K}\right) = e_0 f.$$

By counting dimensions, we find that $a_i = 0$ for $i \neq p$. ■

LEMMA 4. *$\mathbb{Z}_p[\zeta_p][\langle\gamma\rangle]$ is a local ring with unique maximal ideal:*

$$N = (\zeta_p - 1)\mathbb{Z}_p[\zeta_p][\langle\gamma\rangle] + (\gamma - 1)\mathbb{Z}_p[\zeta_p][\langle\gamma\rangle].$$

https://doi.org/10.4153/CJM-1997-035-2 Published online by Cambridge University Press

PROOF. This is a simple exercise following [8, Theorem 1.7, p. 76]. ■

PROPOSITION 1. *Let L/K be a totally ramified Galois extension of local fields, with* $\mathrm{Gal}(L/K) \cong C_p \times C_p$, *where L/K satisfies the condition, $b_1 = 1$. Then*

$$\mathfrak{O}_L/\mathfrak{O}_1 \cong \mathbb{Z}_p[\zeta_p][\langle\gamma\rangle]^{e_0} \quad \textit{as } \mathbb{Z}_p[G]\textit{-modules}.$$

PROOF. This is the standard argument employing Nakayama's Lemma, using Lemmas 3, 4. We omit the details. ■

We now note that as $\mathbb{Z}_p[G]$-modules

$$\mathbb{Z}_p[\zeta_p][\langle\gamma\rangle] \cong \frac{\mathbb{Z}_p[G]}{\langle\Phi_p(\sigma)\rangle} \cong R_1 \otimes E.$$

5. **The structure of $\mathfrak{O}_1$ and $\mathfrak{P}_1$** Although the Galois module structure of $\mathfrak{O}_1$ and $\mathfrak{P}_1$ may be easily determined as in [13], we determine it through an explicit basis as in [5].

As in [5], because $v_1\big((\gamma-1)^i\pi_1\pi_K^m\big) = (i+1) + pm$, it is easily shown that

$$\{(\gamma-1)^i\pi_1\pi_K^m\}_{i=0,1,\ldots,p-1;m=0,1\ldots,e_0-1} \tag{9}$$

provides a $\mathfrak{O}_T$-basis for $\mathfrak{P}_1$. Clearly, $\{(\gamma-1)^i\pi_1\pi_K^m\}_{i=0,\ldots,p-1}$, for each value of m, is an $\mathfrak{O}_T[G]$-module summand of $\mathfrak{P}_1$, where

$$\mathfrak{O}_T\pi_1\pi_K^m + \mathfrak{O}_T(\gamma-1)\pi_1\pi_K^m + \cdots + \mathfrak{O}_T(\gamma-1)^{p-1}\pi_1\pi_K^m \cong \mathfrak{O}_T[\langle\gamma\rangle],$$

as $\mathfrak{O}_T[G]$-modules. Therefore as is proven in Ullom [17]

$$\mathfrak{P}_1 \cong \mathfrak{O}_T[\langle\gamma\rangle]^{e_0} \quad \text{as } \mathfrak{O}_T[G]\text{-modules.}$$

Similarly,

$$\begin{aligned}\{(\gamma-1)^i\pi_1\pi_K^m\}_{i=0,1,\ldots,p-1;m=0,1,\ldots,e_0-2} &\cup \{(\gamma-1)^i p\pi_1\pi_K^{-1}\}_{i=0,1,\ldots p-2}\\ &\cup \{(1+\gamma+\cdots+\gamma^{p-1})\pi_1\pi_K^{-1}\}\end{aligned} \tag{10}$$

provides a $\mathfrak{O}_T$-basis for $\mathfrak{O}_1$. One may check, as in [5, Lem 4], that the $\mathfrak{O}_T$-submodule of $\mathfrak{O}_1$ given by the $p-1$ elements:

$$\{p\pi_1\pi_K^{-1} - (1+\gamma+\cdots+\gamma^{p-1})\pi_1\pi_K^{-1}\} \cup \{(\gamma-1)^i p\pi_1\pi_K^{-1}\}_{i=1,\ldots,p-2}$$

is closed under the action of γ. The only difficulty lies in expressing $(\gamma-1)\cdot(\gamma-1)^{p-1}p\pi_1\pi_K^{-1}$ in terms of the other elements. Simply use the equation $x^p = \sum_{i=0}^p \binom{p}{i}(x-1)^i$ to find that $x^p - 1 = \sum_{i=1}^p \binom{p}{i}(x-1)^i$. Therefore $(x^{p-1}+\cdots+x+1) = \sum_{i=0}^p \binom{p}{i+1}(x-1)^i$, and $(\gamma-1)^{p-1}\pi_1\pi_K^m = -\big(p\pi_1\pi_K^{-1} - (1+\gamma+\cdots+\gamma^{p-1})\pi_1\pi_K^{-1}\big) - \sum_{i=0}^p \frac{\binom{p}{i+1}}{p}(\gamma-1)^i p\pi_1\pi_K^{-1}$. Since these $p-1$ elements, in addition, are clearly annihilated by $(1+\gamma+\cdots+\gamma^{p-1})$,

https://doi.org/10.4153/CJM-1997-035-2 Published online by Cambridge University Press

they form an $\mathfrak{O}_T[G]$-module summand of $\mathfrak{O}_1$ isomorphic to $\mathfrak{O}_T[\zeta_p]$ where γ acts via multiplication by ζ_p, a p-th root of unity. As a result,

$$\mathfrak{O}_1 \cong \mathfrak{O}_T \oplus \mathfrak{O}_T[\zeta_p] \oplus \mathfrak{O}_T[\langle\gamma\rangle]^{e_0-1} \quad \text{as } \mathfrak{O}_T[G]\text{-modules.}$$

Note the $\mathfrak{O}_1$ is almost free as an $\mathfrak{O}_T[\langle\gamma\rangle]$-module which loosely put, corresponds to the fact that the extension, K_1/K, is barely wild.

We will be interested in those $\mathfrak{O}_T$-basis elements which lie in the image of the trace map,

$$T_{L/K_1}(\mathfrak{O}_L) = T_{L/K_1}(\mathfrak{P}_L) = \mathfrak{P}_1^{\lambda_2'} = \mathfrak{P}_1^{(np-r)(p-1)+1}.$$

To begin with, we note that the case $r = 1$ occurs precisely when the ramification number, t, of K_2/K is equal to $pe_0/(p-1)$, so $b_2 = p^2e_0/(p-1) - (p-1)$ and $\lambda_2'(0) = pe_0 - p + 2$. If $p = 2$, then $\lambda_2'(0) = 2e_0$, so $(1+\sigma)\mathfrak{O}_L = 2\mathfrak{O}_1$, and $(1+\sigma)/2$ is an idempotent element giving $\mathfrak{O}_L \cong \mathfrak{O}_1 \oplus \mathfrak{O}_T[\zeta_p][\langle\gamma\rangle]^{e_0}$ as $\mathfrak{O}_T[G]$-modules. The $\mathbb{Z}_p[G]$-module structure of $\mathfrak{O}_L$ is then determined by restriction of coefficients. We will henceforth assume that whenever $r = 1$ we have $p \neq 2$.

Since $\lambda_2'(0) < pe_0$, there are always elements in (10) which lie in the image of the trace map. In fact if $r \neq 1$, then for each $m = 0, 1, \ldots, n(p-1)-r-1$, $v_1\big((\gamma-1)^i\pi_1\pi_K^m\big) < \lambda_2'(0)$ for all i. When $m = n(p-1)-r$, then $v_1\big((\gamma-1)^i\pi_1\pi_K^m\big) < \lambda_2'(0)$ for $i = 0, 1, \ldots, r-1$, while $v_1\big((\gamma-1)^i\pi_1\pi_K^m\big) \geq \lambda_2'(0)$ for $i = r, \ldots, p-1$. Finally, for $m = n(p-1)-r+1, \ldots, e_0-2$, $v_1\big((\gamma-1)^i\pi_1\pi_K^m\big) \geq \lambda_2'(0)$ for all i. And since $r \neq 1$, the ramification number, t, of K_2/K is relatively prime to p and strictly less than $pe_0/(p-1)$. So $np - r + 1 < pe_0/(p-1)$ and therefore, $\lambda_2'(0) \leq v_1(p\pi_1\pi_K^{-1})$.

If $r = 1$, then for $m = 0, \ldots, e_0 - 2$, $v_1\big((\gamma-1)^i\pi_1\pi_K^m\big) \geq \lambda_2'(0)$ for all i, and $v_1(p\pi_1\pi_K^{-1}) < \lambda_2'(0) \leq v_1\big((\gamma-1)p\pi_1\pi_K^{-1}\big)$.

For each m, we define ρ_m as follows: If $r = 1$, then let

$$\rho_m := \begin{cases} 0 & m = 0, 1, \ldots, e_0 - 2 \\ (\gamma-1)p\pi_1\pi_K^{-1} & m = e_0 - 1 \end{cases} \tag{11}$$

(Note that ρ_{e_0-1} lies in the $\mathfrak{O}_T[\langle\gamma\rangle]$-summand, $\mathfrak{O}_T[\zeta_p]$. Clearly $p\pi_1\pi_K^{-1} - (1 + \gamma + \cdots + \gamma^{p-1})\pi_1\pi_K^{-1}$ generates $\mathfrak{O}_T[\zeta_p]$, and ρ_{e_0-1} is $\gamma - 1$ applied once to this generator.)

If $r \neq 1$, then let

$$\rho_m := \begin{cases} 0 & m = 0, \ldots, n(p-1) - r - 1 \\ (\gamma-1)^r\pi_1\pi_K^{n(p-1)-r} & m = n(p-1) - r \\ \pi_1\pi_K^m & m = n(p-1) - r + 1, \ldots, e_0 - 2 \\ p\pi_1\pi_K^{-1} & m = e_0 - 1 \end{cases} \tag{12}$$

(Note that $\rho_{n(p-1)-r}$ lies in a free $\mathfrak{O}_T[\langle\gamma\rangle]$-summand, and that $\rho_{n(p-1)-r}$ is $\gamma - 1$ applied r times to the generator of this module. Furthermore, ρ_m for each $m = n(p-1) - r + 1, \ldots, e_0 - 2$ is the generator of the free $\mathfrak{O}_T[\langle\gamma\rangle]$-summand to which it belongs. Finally, observe that $\rho_{e_0-1} = \big((1+\gamma+\cdots+\gamma^{p-1})\pi_1\pi_K^{-1}\big) + \big(p\pi_1\pi_K^{-1} - (1+\gamma+\cdots+\gamma^{p-1})\pi_1\pi_K^{-1}\big)$.

https://doi.org/10.4153/CJM-1997-035-2 Published online by Cambridge University Press

As a result, ρ_{e_0-1} is the sum of the generators of the two summands, $\mathfrak{O}_T$ and $\mathfrak{O}_T[\zeta]$. We will use these observations in Section 7.)

Finally, we observe that any $\mathfrak{O}_T$-basis element which lies non-trivially in $\mathfrak{P}_1^{\lambda_2'(0)}/p\mathfrak{O}_1$ may be expressed as $(\gamma-1)^i\rho_m$ for some i and some m. Let $M := \{m \mid 0 \le m \le e_0-1, \rho_m \neq 0\}$, then the ρ_m, $m \in M$, provide a $\mathfrak{O}_T/p\mathfrak{O}_T[\langle\gamma\rangle]$-basis for $\mathfrak{P}_1^{\lambda_2'(0)}/p\mathfrak{O}_1$.

If $\eta_1, \eta_2, \ldots, \eta_f$ is a basis for $\mathfrak{O}_T$ over $\mathbb{Z}_p$, then $\rho_m \cdot \eta_j$, $m \in M\, j = 1, \ldots, f$, provides a $\mathbb{F}_p[\langle\gamma\rangle]$-basis for $\mathfrak{P}_1^{\lambda_2'(0)}/p\mathfrak{O}_1$. We will use this observation in the next section.

On the other hand, when handling the Galois module structure of $\mathfrak{P}_L$, one can easily check that $\lambda_2'(1) < pe_0 - 1$ always. Therefore there are always elements of the basis in (9) whose valuation is greater than or equal to $\lambda_2'(1)$. In fact, define $\rho_m = 0$ for each $m = 0, 1, \ldots, n(p-1) - r - 1$, $\rho_{n(p-1)-r} = (\gamma-1)^r\pi_1\pi_K^{n(p-1)-r}$, and $\rho_m = \pi_1\pi_K^m$ for each $m = n(p-1) - r + 1, \ldots, e_0 - 1$. Furthermore, analogous observations concerning how the ρ_m may be expressed in terms of $\mathfrak{O}_T[\langle\gamma\rangle]$-basis elements, and how the ρ_m, $m \notin M$, provide a $\mathfrak{O}_T/p\mathfrak{O}_T[\langle\gamma\rangle]$-basis for $\mathfrak{P}_1^{\lambda_2'(1)}/p\mathfrak{P}_1$ can be made.

6. **A refinement of the structure of $\mathfrak{O}_L/\mathfrak{O}_1$ and $\mathfrak{P}_L/\mathfrak{P}_1$** Let $\eta_1, \eta_2, \ldots, \eta_f$ be the basis for $\mathfrak{O}_T$ over $\mathbb{Z}_p$ chosen in the previous section. In this section we construct a $\mathbb{Z}_p[G]$-basis for $\mathfrak{O}_L/\mathfrak{O}_1$ which is compatible with the $\mathbb{F}_p[G]$-module basis of $\mathfrak{P}_1^{\lambda_2'(0)}/p\mathfrak{O}_1$ given by $\{\rho_m \cdot \eta_j \mid \rho_m \neq 0, j = 1, \ldots, f\}$. In everything that we do, from now on, there is an analogous result for $\mathfrak{P}_L$ or $\mathfrak{P}_L^{\lambda_2'(1)}/p\mathfrak{P}_1$. For ease of exposition we will not include those details pertaining to $\mathfrak{P}_L$, but focus all of our attention on $\mathfrak{O}_L$.

LEMMA 5. *Let $M = \{m \mid \rho_m \neq 0\}$, then for each ρ_m, $m \in M$ listed in (11) and (12) there is a $\nu_m \in \mathfrak{O}_L$ such that $T_{L/K_1}(\nu_m) = \rho_m$. In fact $\{\nu_m \cdot \eta_j \mid m \in M, j = 1, \ldots, f\}$ can be supplemented with elements $\{\nu_m \cdot \eta_j \mid m \in \{0, 1, \ldots, e_0 - 1\} - M, j = 1, \ldots, f\}$ where $T_{L/K_1}(\nu_m) = 0$ when $m \notin M$, so that $\{\nu_m \cdot \eta_j \mid m \in \{0, 1, \ldots, e_0 - 1\}, j = 1, \ldots, f\}$ is a $\mathbb{Z}_p[G]$-module basis of $\mathfrak{O}_L/\mathfrak{O}_1$.*

PROOF. From (3) it is easily seen that $T_{L/K_1}(\mathfrak{P}_L^{ap+b_2}) = T_{L/K_1}(\mathfrak{P}_L^{ap+b_2-1}) = \cdots = T_{L/K_1}(\mathfrak{P}_L^{ap+b_2-(p-1)}) = \mathfrak{P}_1^{a+b_2}$. Therefore, for any element, μ, of $\mathfrak{O}_1$ with valuation $a + b_2$ there exists an element $\nu_{ap+b_2} \in \mathfrak{P}_L^{ap+b_2}/\mathfrak{P}_L^{ap+b_2+1}$ so that $T_{L/K_1}(\nu_{ap+b_2}) = \mu$. As a result there are elements $\nu_m \in \mathfrak{O}_L$ so that $T_{L/K_1}(\nu_m) = \rho_m$.

Soon we will use Nakayama's Lemma applied to the $\mathbb{Z}_p[\zeta][\langle\gamma\rangle]$-module, $\mathfrak{O}_L/\mathfrak{O}_1$. Note that if $\mathcal{M}$ is the unique maximal ideal of $\mathbb{Z}_p[\zeta][\langle\gamma\rangle]$ (Lemma 4), then $(\mathfrak{O}_L/p\mathfrak{O}_1)/\mathcal{M}(\mathfrak{O}_L/p\mathfrak{O}_1) \cong \mathfrak{O}_L/\big((\sigma-1)\mathfrak{O}_L + (\gamma-1)\mathfrak{O}_L + \mathfrak{O}_1\big) = \mathcal{V}$.

Now using the fact observed earlier that $\{\rho_m \cdot \eta_j \mid m \in M, j = 1, \ldots, f\}$ is an $\mathbb{F}_p[\langle\gamma\rangle]$-basis of $\mathfrak{P}_1^{\lambda_2'(0)}/p\mathfrak{O}_1$ we show that the $\nu_m \cdot \eta_j$, $m \in M$ are linearly independent in $\mathcal{V}$. Suppose that $\sum a_{m,j}\nu_m \cdot \eta_j = (\sigma-1)\alpha + (\gamma-1)\beta + \tau$ for some $a_{m,j} \in \mathbb{Z}_p$, $\alpha, \beta \in \mathfrak{O}_L$ and $\tau \in \mathfrak{O}_1$. Then act via the trace, T_{L/K_1}, and find that $\sum a_{m,j}\rho_m \cdot \eta_j = (\gamma-1)T_{L/K_1}(\beta) + p\tau$. Clearly $T_{L/K_1}(\beta)$ can be expressed as $\sum b_{m,j}(\gamma)\rho_m \cdot \eta_j$ for $b_{m,j}(\gamma) \in \mathbb{Z}_p[\langle\gamma\rangle]$. Therefore $\sum(a_{m,j} - (\gamma-1)b_{m,j}(\gamma))\rho_m \cdot \eta_j \in p\mathfrak{O}_1$. Since the $\rho_m \cdot \eta_j$ are a $\mathbb{F}_p[\langle\gamma\rangle]$-basis this forces the $a_{m,j}$ to be zero.

https://doi.org/10.4153/CJM-1997-035-2 Published online by Cambridge University Press

Now that we have shown that the $\nu_m \cdot \eta_j$ are a linearly independent set in the $\mathbb{F}_p$-vector space, V, where by Proposition 1 we know this vector space to have dimension $e_0 f$ over $\mathbb{F}_p$, let $\nu_m \cdot \eta_j = \nu_{m,j}$ for $m \in M$, $j = 1, \ldots, f$, and supplement these elements with elements in $\mathfrak{O}_L$, calling them $\{\nu_{m,j} \mid m \in \{0, 1, \ldots, e_0 - 1\} - M; j = 1, \ldots, f\}$, so that we have a basis of V.

Now consider a $\nu_{m_0,j_0} \in \mathfrak{O}_L$ where $m_0 \notin M$. Since the $\rho_m \cdot \eta_j$ provide a $\mathbb{F}_p[\langle\gamma\rangle]$-basis of $\mathfrak{P}_1^{\lambda_2'(0)}/p\mathfrak{O}_1$, $T_{L/K_1}(\nu_{m_0,j_0}) = \sum b_{m,j}(\gamma)\rho_m \cdot \eta_j + p\tau$ for $b_{m,j}(\gamma) \in \mathbb{Z}_p[\langle\gamma\rangle]$ and $\tau \in \mathfrak{O}_1$. As a result we may change our basis for V replacing ν_{m_0,j_0} by $\nu_{m_0,j_0} - \sum b_{m,j}(\gamma)\nu_{m,j} - \tau$. In this way the $T_{L/K_1}(\nu_{m,j}) = 0$ for $m \notin M$.

Then as a result of Lemma 4 and Nakayama's Lemma, the $\{\nu_{m,j} \mid m = 0, 1, \ldots, e_0 - 1; j = 1, \ldots, f\}$ provide a $\mathbb{Z}_p[G]$-module basis for $\mathfrak{O}_L/\mathfrak{O}_1$. ■

7. **The Galois module structure of $\mathfrak{O}_L$ and $\mathfrak{P}_L$** In the following proof we make liberal use of the arguments in [1, Section 8A, Section 34B and Section 34C]. We note that those same arguments have been used in [2] to classify a family of $\mathbb{Z}_p[G]$-modules which include the indecomposable $\mathbb{Z}_p[G]$-modules that appear in the statements of Theorem 1 and Theorem 2.

Let $\nu_{m,j}$ be the $\mathbb{Z}_p[G]$-module basis of $\mathfrak{O}_L/\mathfrak{O}_1$ given in Lemma 5. Let $\rho_{m,j} = \rho_m \cdot \eta_j$ also. Then

$$\mathfrak{O}_L/\mathfrak{O}_1 = \sum_{m=0}^{e_0-1}\sum_{j=1}^{f} \mathbb{Z}_p[G]\nu_{m,j} \overset{\eta}{\cong} (R_1 \otimes E)^{e_0 f}. \tag{13}$$

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 $\sum_{m=0}^{e_0-1}$ and $\sum_{j=1}^{f}$. Let ι be the inclusion map from $\mathfrak{O}_1$ into $\mathfrak{O}_L$, and let π be the projection map from $\mathfrak{O}_L$ onto $\mathfrak{O}_L/\mathfrak{O}_1$. We have the following $\mathbb{Z}_p[G]$-exact short sequence,

$$0 \longrightarrow \mathfrak{O}_1 \xrightarrow{\iota} \mathfrak{O}_L \xrightarrow{\eta\circ\pi} (R_1 \otimes E)^{e_0 f} \longrightarrow 0, \tag{14}$$

which gives rise to a long exact sequence [1, Theorem 8.6] and determines an element ξ in $\mathrm{Ext}^1_{\mathbb{Z}_p[G]}\big((R_1 \otimes E)^{e_0 f}, \mathfrak{O}_1\big)$ [1, p. 175–176] in the following way: Let $\{z_{m,f}\}$ be indeterminants with $\sum_m \sum_j \mathbb{Z}_p[G]z_{m,j}$ a free $\mathbb{Z}_p[G]$-module and let $y_{m,j} = \Phi_p(\sigma)z_{m,j}$. Let $\varphi \in \mathrm{Hom}_{\mathbb{Z}_p[G]}(\sum_m \sum_j \mathbb{Z}_p[G]z_{m,j}, \mathfrak{O}_L)$ be induced by $\varphi(z_{m,j}) = \nu_{m,j}$ which in turn induces $\mu \in \mathrm{Hom}_{\mathbb{Z}_p[G]}(\sum_m \sum_j \mathbb{Z}_p[G]y_{m,j}, \mathfrak{O}_1)$ such that $\mu(y_{m,j}) = \rho_{m,j}$. We have the following $\mathbb{Z}_p[G]$ commutative diagram,

$$\begin{tikzcd}
0 \arrow[r] & \sum_m \sum_j \mathbb{Z}_p[G]y_{m,j} \arrow[r] \arrow[d, "\mu"'] & \sum_m \sum_j \mathbb{Z}_p[G]z_{m,j} \arrow[r] \arrow[d, "\varphi"'] & (R_1 \otimes E)^{e_0 f} \arrow[r] \arrow[d, "="'] & 0 \\
0 \arrow[r] & \mathfrak{O}_1 \arrow[r, "\iota"] & \mathfrak{O}_L \arrow[r, "\eta\circ\pi"] & (R_1 \otimes E)^{e_0 f} \arrow[r] & 0.
\end{tikzcd}$$

Since $\sum_m \sum_j \mathbb{Z}_p[G]z_{m,j}$ is projective [1, p 174], $\xi \in \mathrm{Ext}^1_{\mathbb{Z}_p[G]}\big((R_1 \otimes E)^{e_0 f}, \mathfrak{O}_1\big)$, corresponds with and is completely is completely determined by

$$\bar{\mu} \in \frac{\mathrm{Hom}_{\mathbb{Z}_p[G]}(\sum_m \sum_j \mathbb{Z}_p[G]y_{m,j}, \mathfrak{O}_1)}{p\,\mathrm{Hom}_{\mathbb{Z}_p[G]}(\sum_m \sum_j \mathbb{Z}_p[G]y_{m,j}, \mathfrak{O}_1)},$$

https://doi.org/10.4153/CJM-1997-035-2 Published online by Cambridge University Press

which is completely determined by a "diagonal" matrix A with the $\rho_{m,j}$ appearing along the "diagonal".

We now refer back to the "notes" following (11) and (12). Suppose that $r \neq 1$, then matrix A appears with only zeros in the first $\big(n(p-1)-r\big)f$ rows and columns. As a consequence, $(n(p-1)-r)f$ copies of $E \oplus (R_1 \otimes E)$ decompose off of $\mathfrak{O}_L$. Now by the remark associated with (12), $\mu(y_{n(p-1)-r,j}) = (\gamma-1)^r$ for each $j = 1, \ldots, f$. Therefore f copies of $(R_1 \otimes E, E; \lambda^r)$ decompose off.

For each $m = n(p-1) - r + 1, \ldots, e_0 - 2$ and each $j = 1, \ldots, f$, $\mu(y_{m,j}) = 1$; so $(R_1 \otimes E, E; 1)^{(n(p-1)-r-2)f}$ appears in the decomposition of $\mathfrak{O}_L$. Finally $\mu(y_{e_0-1,j}) = 1 \oplus 1 \in Z \oplus R_1$, so that $(R_1 \otimes E, Z \oplus R_1; 1 \oplus 1)^f$ decomposes off. This is the complete decomposition of $\mathfrak{O}_L$. One may easily check as in [2] that the modules are indecomposable.

Note that the case $r = 1$ is handled similarly; while the argument determining the $\mathbb{Z}_p[G]$-module structure of $\mathfrak{P}_L$ follows in an analogous manner. ■

8. A canonical example

In this section, we apply the main result of this paper in a canonical situation. Assuming that $p > 3$, we consider the Galois module structure of the ring of integers in the maximal elementary abelian p-extension, L, of a ramified quadratic extension, $K/\mathbb{Q}_p$. Clearly the p-th roots of unity are not present in K, and so by a result of Shafarevich [16], $\mathrm{Gal}(L/K)$ is the direct product of three copies of the cyclic group of p elements, $\mathrm{Gal}(L/K) \cong C_p \times C_p \times C_p$. Since there exists a ramified extension of degree p over K with ramification number equal to one, and another with ramification number equal to two [10], and since there exists an unramified extension of degree p over K [15], L must actually be the composite of these three extensions. We will denote these extensions by L_1, L_2 and L_u respectively, so that $L = L_u \cdot L_1 \cdot L_2$. Let L_w be the composite of L_1 and L_2. Clearly L_w/K satisfies the conditions of Theorem 1, with $f = 1$, $n = 1$, $r = p - 1$ and $e_0 = 2$. Therefore if $\mathfrak{O}_w$ denotes the ring of integers in L_w,

$$\mathfrak{O}_w \cong (R_1 \otimes E, Z \oplus R_1; 1 \oplus 1) \oplus (R_1 \otimes E, E; \lambda^{p-1}) \quad \text{as } \mathbb{Z}_p[\mathrm{Gal}(L_w/K)]\text{-modules.}$$

Let $\mathfrak{O}_u$, $\mathfrak{O}_K$, $\mathfrak{O}_L$ denote the ring of integers in L_u, K and L respectively. Using the fact that L_u/K is unramified, while L_w/K is fully ramified it is easy to show that $\mathfrak{O}_L = \mathfrak{O}_u\mathfrak{O}_w$. By a theorem of E. Noether [12], using the fact that L_u/K is unramified and therefore tame, we find that $\mathfrak{O}_u$ has a normal integral basis over $\mathfrak{O}_K$. Therefore, if $\mathrm{Gal}(L_u/K) = \langle\rho\rangle$, there is an $\alpha \in \mathfrak{O}_u$ such that $\alpha\mathfrak{O}_K + \rho(\alpha)\mathfrak{O}_K + \cdots + \rho^{p-1}(\alpha)\mathfrak{O}_K = \mathfrak{O}_u$. Therefore,

$$\begin{aligned}
\mathfrak{O}_L &= \mathfrak{O}_u\mathfrak{O}_w \\
&= \alpha\mathfrak{O}_w + \rho(\alpha)\mathfrak{O}_w + \cdots + \rho^{p-1}(\alpha)\mathfrak{O}_w \\
&\cong \mathbb{Z}_p[\langle\rho\rangle] \otimes_{\mathbb{Z}_p} \mathfrak{O}_w \\
&\cong \mathbb{Z}_p[\langle\rho\rangle] \otimes_{\mathbb{Z}_p} \big((R_1 \otimes E, Z \oplus R_1; 1 \oplus 1) \oplus (R_1 \otimes E, E; \lambda^{p-1})\big)
\end{aligned}$$

as $\mathbb{Z}_p[\mathrm{Gal}(L/K)]$-modules.

REFERENCES

1. C. W. Curtis and I. Reiner, *Methods of Representation Theory*, Wiley, New York, 1981.
2. G. G. Elder, *The Galois module structure of the integers in wildly ramified extensions*, Dissertation, The Ohio State University, 1993.
3. G. G. Elder and M. L. Madan, *Galois module structure of integers in wildly ramified cyclic extensions*, J. Number Theory (2) **47**(1994), 138–174.
4. ———, *Galois module structure of integers in weakly ramified extensions*, Arch. Math. **64**(1995), 117–120.
5. G. G. Elder, *Galois module structure of integers in wildly ramified cyclic extensions of degree* p^2, Ann. Inst. Fourier (Grenoble) (3) **45**(1995), 625–647.
6. B. Erez, *The Galois structure of the square root of the inverse different*, Math. Z. **208**(1991), 239–255.
7. 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.
8. A. Heller and I. Reiner, *Representations of cyclic groups in rings of integers I*, Ann. of Math. (2) **76**(1962), 73–92.
9. J-F. Jaulent, *Sur la l-structure Galoisienne des ideaux ambiges dans une extension metacyclique de degree nl sur le corps des rationnels*, Number theory, 1979–1980 and 1980–1981, Exp. **3**, 20, Publ. Math. Fac. Sci. Besancon, Univ. Franche-Comté, Besancon, 1981.
10. E. Maus, *Existenz $\mathfrak{P}$-adischer Zahlkörper zu Vorgegebenem Verzweigungsverhalten*, Dissertation, Hamburg, 1965.
11. Y. Miyata, *On the module structure of a p-extension over a p-adic number field,* Nagoya Math. J. **77**(1980), 13–23.
12. E. Noether, *Normalbasis bei Körpern ohne höhere Verzweigung*, J. Reine Angew. Math. **167**(1932), 147–152.
13. M. Rzedowski-Calderón, G. D. Villa-Salvador and M. L. Madan, *Galois module structure of rings of integers*, Math. Z. **204**(1990), 401–424.
14. S. Sen, *On automorphisms of local fields*, Ann. of Math. (2) **90**(1969), 33–46.
15. J-P. Serre, *Local fields*, Graduate Texts Math. **67**, Springer-Verlag, Berlin, Heidelberg, New York, 1979.
16. I. R. Shafarevich, *On p-extensions*, Izv. Akad. Nauk. SSSR Ser. Mat. **15**(1951), 17–46.
17. S. Ullom, *Integral normal bases in Galois extensions of local fields*, Nagoya Math. J. **39**(1970), 141–146.
18. 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.
19. 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.

The Department of Mathematics
The Ohio State University
231 W. 18th Avenue
Columbus, Ohio 43210
U.S.A.

The Department of Mathematics
The University of Nebraska at Omaha
Omaha, Nebraska 68182
U.S.A.

https://doi.org/10.4153/CJM-1997-035-2 Published online by Cambridge University Press