Can. J. Math. Vol. **50** (5), 1998 pp. 1007–1047.

GALOIS MODULE STRUCTURE OF AMBIGUOUS IDEALS IN BIQUADRATIC EXTENSIONS

G. GRIFFITH ELDER

ABSTRACT. Let N/K be a biquadratic extension of algebraic number fields, and $G = \mathrm{Gal}(N/K)$. Under a weak restriction on the ramification filtration associated with each prime of K above 2, we explicitly describe the $\mathbb{Z}[G]$-module structure of each ambiguous ideal of N. We find under this restriction that in the representation of each ambiguous ideal as a $\mathbb{Z}[G]$-module, the exponent (or multiplicity) of each indecomposable module is determined by the invariants of ramification, alone.

For a given group, G, define S_G to be the set of indecomposable $\mathbb{Z}[G]$-modules, M, such that there is an extension, N/K, for which $G \cong \mathrm{Gal}(N/K)$, and M is a $\mathbb{Z}[G]$-module summand of an ambiguous ideal of N. Can S_G ever be infinite? In this paper we answer this question of Chinburg in the affirmative.

1. **Introduction.** Suppose that K is a finite extension of the rational numbers, $\mathbb{Q}$, while N is some finite Galois extension of K. It is well-known that the ring of integers of N, $\mathfrak{O}_N$, is a free module over the ring of rational integers, $\mathbb{Z}$. Since the Galois group, $G = \mathrm{Gal}(N/K)$, acts on the ring of integers; $\mathfrak{O}_N$ may be viewed, canonically, as a module over the group ring, $\mathbb{Z}[G]$. Is the ring of integers, $\mathfrak{O}_N$, free over the group ring, $\mathbb{Z}[G]$?

In 1932, E. Noether determined that in order for $\mathfrak{O}_N$ to be free over $\mathbb{Z}[G]$, the extension, N/K, must be at most tamely ramified [18]. In the 1970's, a lot of work was done in determining necessary and sufficient conditions for the ring of integers, $\mathfrak{O}_N$, to be free over $\mathbb{Z}[G]$ when the extension N/K is tame. This culminated in M. J. Taylor's proof of Fröhlich's Conjecture. Fröhlich's book is an excellent reference for this topic [9].

If the extension, N/K, is not tamely ramified but in fact has some wild ramification, we can not expect $\mathfrak{O}_N$ to be free over $\mathbb{Z}[G]$. What can we expect? This is the question that we seek to address in this paper.

Any effort to address the question of $\mathbb{Z}[G]$-module structure of $\mathfrak{O}_N$ in wildly ramified extensions must contend with two basic obstacles:

(1) The Krull-Schmidt Theorem generally does not hold. Consequently, while a given $\mathbb{Z}[G]$-module will decompose into a direct sum of indecomposable $\mathbb{Z}[G]$-modules, the decomposition will not necessarily be unique.

(2) The number of indecomposable $\mathbb{Z}[G]$-modules is usually infinite, for a nice survey see Dieterich [3].

Received by the editors April 21, 1997.

I would like to express my appreciation to Ted Chinburg, Roger Wiegand and Steve Wilson for helpful suggestions, and especially to Jacques Queyrut and Université de Bordeaux for support during the summer of 1995 while part of this paper was being completed.

AMS subject classification: Primary: 11R33; secondary: 11S15, 20C32.

Key words and phrases: Galois module structure, Wild ramification.

https://doi.org/10.4153/CJM-1998-050-4 Published online by Cambridge University Press

There are two ways that one may retrieve the Krull-Schmidt Theorem. On the one hand, one might consider the analogous question for local number field extensions, N/K (where the Krull-Schmidt Theorem does hold). Alternatively, one may restrict oneself to those Galois groups, G, and their group rings, $\mathbb{Z}[G]$ for which the Krull-Schmidt Theorem happens to hold.

In the work of Rzedowski-Caldéron, *et al.* [19] and previous work of the author with Madan [6], the first approach was adopted. Based upon this work, in particular [8], it is clear that explicit expressions for the Galois module structure of the ring of integers in wildly ramified extensions of local fields can be quite complicated.

In this paper we adopt an alternate approach. We restrict our attention to the class of biquadratic number field extensions, because the Krull-Schmidt Theorem holds for $\mathbb{Z}[C_2\times C_2]$-modules. Fortunately, not only does the Krull-Schmidt Theorem hold, but the infinitely many inequivalent, indecomposable $\mathbb{Z}[C_2\times C_2]$-modules have been classified by Nazarova [16] with complete proofs in [17].

The approach which we employ in this paper enables us to explicitly determine the $\mathbb{Z}[G]$-module structure of $\mathfrak{O}_N$ (as well as any other ambiguous ideal) in terms of indecomposable $\mathbb{Z}[G]$-modules which are indexed at the end of the paper. In particular, we determine this structure for the wide class of biquadratic extensions N/K which arise as the composite of two arithmetically disjoint quadratic extensions, see Maus [14]. This is enough, for us to answer a question posed by Chinburg.

QUESTION 1.1 (CHINBURG). For a given group, G, define S_G to be the set of indecomposable $\mathbb{Z}[G]$-modules, M, such that there is an extension, N/K, for which $G\cong \mathrm{Gal}(N/K)$, and M is a $\mathbb{Z}[G]$-module summand of an ambiguous ideal of N. Can S_G be infinite?

In this paper, we explicitly construct a family of extensions whose Galois module structure of the ring of integers we determine. As a consequence, we are able to answer this question in the affirmative. See Section 3.41.

Although we are able to apply the methods of this paper to determine the $\mathbb{Z}[G]$-module structure of $\mathfrak{O}_N$ for a wide class of biquadratic number fields, we are unable to apply the methods of this paper to all biquadratic extensions. In Section 3.42 we examine this in greater detail. In Section 5 we show that our results are tight by providing a family of extensions (not covered by our Theorems) to which our approach can not be applied.

1.1. *Organization of Paper* The paper it organized as follows: Note that as some of the proofs are rather technical, they have been collected in Section 3.43.

https://doi.org/10.4153/CJM-1998-050-4 Published online by Cambridge University Press

1.2. *Related topics.* We would be remiss, if we did not include a brief discussion of other material related to the main topic of this paper. The main results of this paper are local, and so in this section we are concerned with the question, "the Galois module structure of the ring of integers in wildly ramified local extensions." Let N/L be a wildly ramified Galois extension of local number fields, with $[L : \mathbb{Q}_p]$ finite, $\mathbb{Q}_p$ denoting the field of p-adic numbers. Let $G = \mathrm{Gal}(N/L)$. Use subscripts to denote the field of reference, so that $\mathfrak{O}_L$ is the ring of integers of L, while $\mathfrak{O}_N$ is the ring of integers of N.

Here are two approaches to this question:

(1) For K any subfield of L, one can ask for the $\mathfrak{O}_K[G]$-module structure of $\mathfrak{O}_N$. In this paper we are interested in the the situation where $K = \mathbb{Q}_p$ and $p = 2$. Actually, although we are principally interested in the situation, $K = \mathbb{Q}_2$; our approach answers the question for $K = T$, the maximal unramified extension of $\mathbb{Q}_2$, which by restriction determines the answer to the question for all K's unramified extension over $\mathbb{Q}_2$, and in particular $K = \mathbb{Q}_2$. At the other extreme, Miyata [15] and Vostokov [22] have examined the situation when $K = L$. There, they find that when G is a p-group (N/L fully ramified), $\mathfrak{O}_N$ is usually indecomposable as a $\mathfrak{O}_L[G]$-module. We find, on the other hand, that $\mathfrak{O}_N$ usually decomposes as a $\mathbb{Z}_p[G]$-module.

(2) Another approach is motivated by the work of Leopoldt [12]. One may study the structure of $\mathfrak{O}_N$ as a module over the associated order, $\{x \in L[G] : x\mathfrak{O}_N \subseteq \mathfrak{O}_N\}$. Martel [13] has done this for biquadratic extensions of $\mathbb{Q}_2$. Burns [2] has studied this question more generally.

2. **Reduction: from global to local.** Let N/K be a biquadratic extension of number fields, with Galois group, $G = \mathrm{Gal}(N/K) \cong C_2 \times C_2$. Let $\mathfrak{O}_N$ denote the ring of integers of N. An ambiguous ideal, $\mathfrak{A}$, is a fractional ideal of $\mathfrak{O}_N$ with the property that $\sigma\mathfrak{A} = \mathfrak{A}$ for all $\sigma \in G$. In our examination of the $\mathbb{Z}[G]$-module structure of ambiguous ideals, we will require a result from representation theory: Namely, that the local structure completely determines the global structure. To precisely state and prove this result, we require a definition:

DEFINITION 2.1. If $\mathfrak{N}$ is a $\mathbb{Z}[G]$-module, let $\hat{\mathfrak{N}}$ denote the tensor product, $\mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathfrak{N}$. The $\mathbb{Z}_2[G]$ action on $\hat{\mathfrak{N}}$ is defined by the following: For $a\beta \in \mathbb{Z}_2[G]$ with $a \in \mathbb{Z}_2$, $\beta \in G$, and $b \otimes_{\mathbb{Z}} \alpha \in \mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathfrak{N}$, let $a\beta \cdot b \otimes_{\mathbb{Z}} \alpha = ab \otimes_{\mathbb{Z}} \beta\alpha$.

THEOREM 2.2 (LOCAL-GLOBAL). *Let $\mathfrak{N}$ and $\mathfrak{M}$ be $\mathbb{Z}[G]$-modules, with $G \cong C_2 \times C_2$.*

$$\textit{If } \hat{\mathfrak{N}} \cong \hat{\mathfrak{M}} \textit{ as } \mathbb{Z}_2[G]\textit{-modules}, \quad \textit{then } \mathfrak{N} \cong \mathfrak{M} \textit{ as } \mathbb{Z}[G]\textit{-modules}.$$

PROOF. If $\hat{\mathfrak{N}} \cong \hat{\mathfrak{M}}$ as $\mathbb{Z}_2[G]$-modules, then $\mathfrak{N}$ and $\mathfrak{M}$ belong to the same genus, see [5, p. 642]. Let $O = 1/4(\sigma+1)(\gamma+1)\mathbb{Z} + 1/4(\sigma-1)(\gamma+1)\mathbb{Z} + 1/4(\sigma+1)(\gamma-1)\mathbb{Z} + 1/4(\sigma-1)(\gamma-1)\mathbb{Z}$ denote the maximal order of $\mathbb{Q}[G]$. If furthermore, $O\mathfrak{N} \cong O\mathfrak{M}$ as O-modules (where $O\mathfrak{N} = O \otimes_{\mathbb{Z}[G]} \mathfrak{N}$) then $\mathfrak{N}$ and $\mathfrak{M}$ belong to the same restricted genus, see [11, p. 10]. Clearly, $O\mathfrak{N} \cong Z^a \oplus R_\sigma^b \oplus R_\gamma^c \oplus R_{\sigma\gamma}^d$ for some nonnegative integers a, b, c, d (for explanation of $\mathbb{Z}[G]$-module notation, see Section 4). Note that $\hat{O}\hat{\mathfrak{N}} \cong \hat{Z}^a \oplus \hat{R}_\sigma^b \oplus \hat{R}_\gamma^c \oplus \hat{R}_{\sigma\gamma}^d$ for the same nonnegative integers, a, b, c, d. Therefore, if $\hat{\mathfrak{N}}$ and $\hat{\mathfrak{M}}$ are in the same genus, the nonnegative integers a, b, c, d are determined, so that $\mathfrak{N}$ and $\mathfrak{M}$ must lie in the same restricted genus. Because the ring, $\mathbb{Z}[G]$, has direct sum cancellation [23, p. 458], there is only one isomorphism class per restricted genus [23, p. 443]. ∎

As a consequence of this theorem we turn our attention to examine the $\mathbb{Z}_2[G]$-module structure of $\mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathfrak{A}$.

Let $\mathfrak{p}_j$, $j = 1, \ldots, g$ be the list of distinct prime ideals of $\mathfrak{O}_K$ which lie over 2. Suppose that $\mathfrak{p}_j$ splits into g_j distinct prime ideals, $\mathfrak{P}_{(i,j)}$, in N, so that $\mathfrak{p}_j\mathfrak{O}_N = \Pi_{i=1}^{g_j}\mathfrak{P}_{(i,j)}^{e_j}$. Clearly, $g_j = 1, 2$ or 4. Reorganize the subscripts of the $\mathfrak{p}_j$'s, so that we have:

$$\begin{array}{lll}
\text{for } j = 1, \ldots, a & g_j = 1, & \\
\text{for } j = a+1, \ldots, b & g_j = 2, & \sigma\mathfrak{P}_{(1,j)} = \mathfrak{P}_{(1,j)} \\
\text{for } j = b+1, \ldots, c & g_j = 2, & \gamma\mathfrak{P}_{(1,j)} = \mathfrak{P}_{(1,j)} \\
\text{for } j = c+1, \ldots, d & g_j = 2, & \gamma\sigma\mathfrak{P}_{(1,j)} = \mathfrak{P}_{(1,j)} \\
\text{for } j = d+1, \ldots, g & g_j = 4, &
\end{array}$$

for some a, b, c, d with $0 \le a \le b \le c \le d \le g$. Adopt the convention that when $g_j = 4$, $\sigma\mathfrak{P}_{(1,j)} = \mathfrak{P}_{(2,j)}$, $\gamma\mathfrak{P}_{(1,j)} = \mathfrak{P}_{(3,j)}$, and $\gamma\sigma\mathfrak{P}_{(1,j)} = \mathfrak{P}_{(4,j)}$.

Let $N_{(i,j)}$ be the completion of N at the prime, $\mathfrak{P}_{(i,j)}$, let K_j be the completion of K at the prime, $\mathfrak{p}_j$, and let $\mathfrak{A}_{(i,j)}$ be the embedding of $\mathfrak{A}$ into $N_{(i,j)}$. If we identify $\mathfrak{P}(i,j)$ with the maximal ideal in $N_{(i,j)}$, then $\mathfrak{A}_{(i,j)} = \mathfrak{P}(i,j)^t$ for some $t \in \mathbb{Z}$.

THEOREM 2.3. *Adopting the notation above,*

$$\mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathfrak{A} \cong \oplus \sum_{j=1}^{g} \sum_{i=1}^{g_j} \mathfrak{A}_{(i,j)} \quad \textit{as } \mathbb{Z}_2\textit{-modules}.$$

PROOF. See, for instance, [10, Ch. III]. ∎

Note that for $j = d+1, \ldots, g$, $\mathfrak{A}_{(i,j)} \cong \mathbb{Z}_2$ as $\mathbb{Z}_2$-module while $\sigma\mathfrak{A}_{(1,j)} = \mathfrak{A}_{(2,j)}$, $\gamma\mathfrak{A}_{(1,j)} = \mathfrak{A}_{(3,j)}$, and $\gamma\sigma\mathfrak{A}_{(1,j)} = \mathfrak{A}_{(4,j)}$. Therefore $\mathfrak{A}_{(1,j)} + \mathfrak{A}_{(2,j)} + \mathfrak{A}_{(3,j)} + \mathfrak{A}_{(4,j)} \cong \hat{G}$ as $\mathbb{Z}_2[G]$-modules, where $\hat{G}$ denotes the group ring, $\mathbb{Z}_2[G]$. Similarly,

$$\begin{aligned}
\mathfrak{A}_{(1,j)} + \mathfrak{A}_{(2,j)} &\cong \mathbb{Z}_2[\langle\gamma\rangle] \otimes_{\mathbb{Z}} \mathfrak{A}_{(1,j)} \quad \text{for } j = a+1, \ldots, b,\\
\mathfrak{A}_{(1,j)} + \mathfrak{A}_{(2,j)} &\cong \mathbb{Z}_2[\langle\sigma\rangle] \otimes_{\mathbb{Z}} \mathfrak{A}_{(1,j)} \quad \text{for } j = b+1, \ldots, c,\\
\mathfrak{A}_{(1,j)} + \mathfrak{A}_{(2,j)} &\cong \mathbb{Z}_2[\langle\sigma\rangle] \otimes_{\mathbb{Z}} \mathfrak{A}_{(1,j)} \quad \text{for } j = c+1, \ldots, d;
\end{aligned}$$

where the action of $\mathbb{Z}_2[G]$ is the natural one: If $a\gamma^l\sigma^k \in \mathbb{Z}_2[G]$ for some $a \in \mathbb{Z}_2$ and $\alpha \otimes_{\mathbb{Z}} \beta \in \mathbb{Z}_2[\langle\gamma\rangle] \otimes_{\mathbb{Z}} \mathfrak{A}_{(1,j)}$ for $j = a+1, \ldots, b$, or $\alpha \otimes_{\mathbb{Z}} \beta \in \mathbb{Z}_2[\langle\sigma\rangle] \otimes_{\mathbb{Z}} \mathfrak{A}_{(1,j)}$ for $j = b+1, \ldots, d$; define the action of $\mathbb{Z}_2[G]$ by

$$a\gamma^l\sigma^k \cdot \alpha \otimes_{\mathbb{Z}} \beta = \begin{cases} a\gamma^l\alpha \otimes_{\mathbb{Z}} \sigma^k\beta & \text{for } j = a+1, \ldots, b,\\ a\sigma^k\alpha \otimes_{\mathbb{Z}} \gamma^l\beta & \text{for } j = b+1, \ldots, c,\\ a\sigma^{k-l}\alpha \otimes_{\mathbb{Z}} (\gamma\sigma)^l\beta & \text{for } j = c+1, \ldots, d. \end{cases}$$

Finally, for each j with $g_j = 1$, note that $\mathfrak{A}_{(1,j)}$ is closed under the action of the group, and therefore is already a $\mathbb{Z}_2[G]$-module. As a consequence, we have the following result:

THEOREM 2.4. *Adopting the notation from above,*

$$\begin{aligned}
\mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathfrak{A} \cong{}& \oplus \sum_{j=1}^{a} \mathfrak{A}_{(1,j)} \oplus \sum_{j=a+1}^{b} (\mathbb{Z}_2[\langle\gamma\rangle] \otimes_{\mathbb{Z}} \mathfrak{A}_{(1,j)})\\
&\oplus \sum_{j=b+1}^{c} (\mathbb{Z}_2[\langle\sigma\rangle] \otimes_{\mathbb{Z}} \mathfrak{A}_{(1,j)}) \oplus \sum_{j=c+1}^{d} (\mathbb{Z}_2[\langle\sigma\rangle] \otimes_{\mathbb{Z}} \mathfrak{A}_{(1,j)})\\
&\oplus \sum_{j=d+1}^{g} \hat{G} \quad \textit{as } \mathbb{Z}_2[G]\textit{-modules}.
\end{aligned}$$

Because of this theorem, we now turn our attention to the local question: What is the $\mathbb{Z}_2[G_j]$-module structure of $\mathfrak{A}_{(1,j)}$, where G_j is the Galois group, $\mathrm{Gal}(N_{(1,j)}/K_j)$. In other words, we need to know the Galois module structure of ideals in quadratic and biquadratic extensions of local number fields. This question is addressed in the remainder of this paper.

https://doi.org/10.4153/CJM-1998-050-4 Published online by Cambridge University Press

3. Quadratic and biquadratic local extensions.

3.1. *Notation.* There should be no confusion, if we now let K refer to a finite extension of the 2-adic numbers, $\mathbb{Q}_2$. Let e_0 denote the absolute ramification index, while f denotes the degree of inertia, then $[K:\mathbb{Q}_2]=e_0f$. Let N be a finite Galois extension of K, call the Galois group of N over K, $G=\mathrm{Gal}(N/K)$. Use subscripts to denote the field of reference so that $\mathfrak{O}_N$ refers to the ring of integers of N, $\mathfrak{P}_N$ denotes the maximal ideal of $\mathfrak{O}_N$, π_N a prime element in N and v_N the normalized valuation of N, so that $v_N(\pi_N)=1$. Let G_{-1}, $G_0, G_1, G_2\cdots$ denote the ramification filtration of G [21, Chapter IV]. So $G_{-1}=G$ while G_0 is the inertia subgroup of G. A break (ramification) number of N/K will always refer to a lower break (ramification) number, so that b is a break number if $G_b\neq G_{b+1}$. Let T denote the maximal unramified extension of $\mathbb{Q}_2$ contained in K. Clearly, $[T:\mathbb{Q}_2]=f$. Let $\lfloor x\rfloor$ denote the floor function (also called the greatest integer function), while $\lceil x\rceil$ denotes the ceiling function (the least integer function). Clearly, $\lfloor (x-1)/n\rfloor=\lceil x/n\rceil-1$ for any positive integer n.

3.2. *Quadratic extensions.* When N/K is a quadratic extension, the $\mathbb{Z}_2[G]$-module structure of $\mathfrak{P}_N^i$ is known. We reprove this result to introduce the approach which we will employ in the proofs of our later results.

THEOREM 3.1. *Let N/K be a quadratic extension of local number fields (ramified or unramified), where $[K:\mathbb{Q}_2]=e_0f$, e_0 denoting the absolute ramification index. Let b be the ramification number of N/K, let $G=\mathrm{Gal}(N/K)$ be generated by γ, and let*

$$a=\begin{cases}\lceil (i+b)/2\rceil-\lceil i/2\rceil & \text{if } b\neq -1,\\ 0 & \text{if } b=-1.\end{cases}$$

Then

$$\mathfrak{P}_N^i\cong \hat{Z}^{af}\oplus \hat{R}_\sigma^{af}\oplus \hat{E}_+^{(e_0-a)f}\quad \text{as } \mathbb{Z}_2[G]\text{-modules}.$$

PROOF. If N/K is unramified, one may easily verify that each fractional ideal has a normal integral basis.

Note that b is even means that $b=2e_0$, see [24]. Consequently, $(\gamma+1)/2$ is an idempotent element which takes $\mathfrak{P}_N^i$ into itself, yielding the desired result.

If b is odd, let $\alpha\in N$ have valuation, $v_N(\alpha)=b$. Let $\alpha_m=\pi_K^m\alpha$ so that $v_N(\alpha_m)=b+2m$. Because $v_N\big((\gamma+1)\alpha_m\big)=2b+2m$, the elements in the following two sets serve as a basis for $\mathfrak{P}_N^i$ over $\mathfrak{O}_T$:

$$\begin{aligned}(3.1)\qquad &\{\alpha_m,(\gamma+1)\alpha_m:\lceil (i-b)/2\rceil\le m\le e_0-b+\lceil i/2\rceil-1\},\\ &\{(\gamma+1)\alpha_m,2\alpha_m:\lceil i/2\rceil-b\le m\le\lceil (i-b)/2\rceil-1\}.\end{aligned}$$

From this basis the $\mathfrak{O}_T[G]$-structure is apparent which determines the $\mathbb{Z}_2[G]$-module structure.

For an alternative proof, see [19, Theorem 1]. ∎

https://doi.org/10.4153/CJM-1998-050-4 Published online by Cambridge University Press

REMARK 3.2. When we outline our approach in Section 3.42, we will refer back to this proof as a prototype. Therefore, it is important to notice some things about the argument we use in the case when b is odd.

Because the extension N/K is wildly ramified, the Galois action (namely, the action of $\gamma+1$) shifts the valuation of α_m. This is important because as m varies, $v_N(\alpha_m)$ represents every odd integer, while $v_N\big((\gamma+1)\alpha_m\big)$ represents every even integer. Together the elements α_m and $(\gamma+1)\alpha_m$ whose valuations lie between i and $2e_0+i-1$ are listed in (3.1). Note that we successfully created (3.1) knowing only the following information about the quadratic extension: the absolute ramification index, e_0, the ramification number of N/K, b, and the integer i which corresponds to $\mathfrak{P}_N^i$, and that the elements of (3.1) satisfy the following two conditions:

1. The Galois relations among the members of (3.1) are very basic. In particular, the Galois action on any member of (3.1) takes it to a rather simple linear combination of members in (3.1) where the coefficients come from $\mathbb{Z}_2$.

2. The elements of (3.1) have valuations in one-to-one correspondence with the integers $\{i, i+1, \ldots, 2e_0+i-1\}$. Because N/T is a fully ramified extension, they provide a basis for $\mathfrak{P}_N^i$ over $\mathfrak{O}_T$.

Indeed, note that to determine the $\mathbb{Z}_2[G]$-module structure of an ideal we determined the $\mathfrak{O}_T[G]$-module structure. This is both the strength and the weakness of our approach.

3.3. *Partially ramified biquadratic extensions.* Let N/K be a biquadratic extension. Let $\mathrm{Gal}(N/K)$ be generated by σ and γ and let L denote the fixed field of σ, N^σ, while $M=N^\gamma$. Clearly, an extension is either fully ramified or it is not. If N/K is not fully ramified, then because unramified extensions are cyclic, there must be a unique unramified quadratic extension of K contained in N. Without loss of generality, let it be L. The extensions N/L and M/K are, therefore, fully ramified.

THEOREM 3.3. *If the extension, N/K, is partially ramified then there must be two breaks in the ramification filtration, and the first break number must be $b_1=-1$. Let b_2 denote the second lower ramification number, and assume that $\langle\sigma\rangle = G_0 = \cdots = G_{b_2}$. If $a=\lceil (i+b_2)/2\rceil - \lceil i/2\rceil$, then*

$$\mathfrak{P}_N^i \cong \hat{E}_+^{af} \oplus \hat{E}_-^{af} \oplus \hat{G}^{(e_0-a)f} \text{ as } \mathbb{Z}_2[G]\text{-modules}.$$

PROOF. Because N/K is in this case the compositum of a fully ramified quadratic extension of K (namely M) and an unramified quadratic extension of K (namely L); each fractional ideal of N, is the compositum of a fractional ideal of $\mathfrak{O}_M$ and the ring, $\mathfrak{O}_L$: $\mathfrak{P}_N^i = \mathfrak{O}_L\mathfrak{P}_M^i$. The ring of integers of an unramified quadratic extension has a normal integral basis, so $\mathfrak{O}_L = \mathfrak{O}_K[\gamma]\alpha$ (for some $\alpha\in\mathfrak{O}_L$), and so $\mathfrak{O}_N = \mathbb{Z}_2[\gamma]\alpha\cdot\mathfrak{P}_M^i$. Therefore $\mathfrak{O}_N^i = \mathbb{Z}_2[\gamma]\otimes_{\mathbb{Z}_2}\mathfrak{P}_M^i$, where the action of $\mathbb{Z}_2[G]$ is defined naturally. Clearly, the lower ramification number of M/K is b_2. Determining the $\mathbb{Z}_2[\sigma]$ structure of $\mathfrak{P}_M^i$ as in Theorem 3.1, and comparing the structure of $\mathbb{Z}_2[\gamma]\otimes_{\mathbb{Z}}\mathfrak{P}_M^i$ with the modules listed in Section 4, we derive our theorem. ∎

https://doi.org/10.4153/CJM-1998-050-4 Published online by Cambridge University Press

3.4. *Fully ramified biquadratic extensions.*

3.4.1. Results for fully ramified biquadratic extensions. Let N be a fully ramified biquadratic extension of K. Let $\mathrm{Gal}(N/K)$ be generated by σ and γ and let $L = N^{\sigma}$, $M = N^{\gamma}$. As a result of ramification theory, there is either one or two breaks in the ramification filtration of N/K.

CASE 1: ONE BREAK IN THE RAMIFICATION FILTRATION. Suppose that there is only one break in the ramification filtration of N/K. Let b denote the ramification number associated this break. Then the ramification groups of N/K are: $G = G_0 = \cdots = G_b$, and $\langle 1\rangle = G_{b+1} = \cdots$, and it is easily seen that b is the ramification number of each extension: L/K M/K, N/L, and N/M, [21, Chapter IV].

It is well known that the lower ramification number of a ramified extension, K/k, of degree 2 is $\leq 2e_k$ (where e_k is the absolute ramification index of $k/\mathbb{Q}_p$) and that the ramification number is odd unless it is equal to $2e_k$, see [24]. Since b is the ramification number of L/K, $b \leq 2e_0$. But b is also the ramification number of N/L. So since $b \leq 2e_0 < 4e_0$, b must be odd.

In every case, regardless of the ideal, $\mathfrak{P}_N^i$, or the ramification number, b; we are able to use the basic approach of the proof of Theorem 3.1 and capture the ideal, $\mathfrak{P}_N^i$, in a short exact sequence:

THEOREM 3.4. *Let N be any fully ramified biquadratic extension of K with $[K : \mathbb{Q}_2] = e_0 f$, e_0 denoting the absolute ramification index. Assume that there is one break in the ramification filtration of N/K. Let b denote the ramification number associated with this break, and let $\mu = \lceil (i+2b)/4\rceil - \lceil i/4\rceil$, while $\tau = \lceil (i-b)/4\rceil - \lceil (i-3b)/4\rceil$. Then the following short exact $\mathbb{Z}_2[G]$-sequence exits.*

$$0 \longrightarrow (\hat{Z} \oplus \hat{R}_{\sigma})^{\mu f} \oplus \hat{E}_+^{(e_0-\mu)f} \longrightarrow \mathfrak{P}_N^i \longrightarrow (\hat{R}_{\gamma} \oplus \hat{R}_{\sigma\gamma})^{\tau f} \oplus \hat{E}_-^{(e_0-\tau)f} \longrightarrow 0.$$

PROOF. See Section 3.43. ∎

However it is only for a special class of ideals in a restricted class of extension that we can use the approach of the proof of Theorem 3.1 to explicitly determine the Galois module structure of the ideal. The underlying reasons for this are explained in Section 3.42.

THEOREM 3.5 (CASE 1). *Let N be any fully ramified biquadratic extension of K with $[K : \mathbb{Q}_2] = e_0 f$, e_0 denoting the absolute ramification index. Assume that there is one break in the ramification filtration of N/K. Let b denote the ramification number associated with this break. If $b = 1$ and $i \equiv 0, 1, 2 \bmod 4$, or $b = 3$ and $i \equiv 2 \bmod 4$,*

Then

$$\begin{aligned} \mathfrak{P}_N^i &\cong \hat{C}^{(\lceil \frac{i-3b}{4}\rceil - \lceil \frac{i}{4}\rceil + b)f} \oplus \hat{D}^{(\lceil \frac{i-b}{4}\rceil - \lceil \frac{i-2b}{4}\rceil)f} \oplus \hat{G}^{(e_0 + \lceil \frac{i}{4}\rceil - \lceil \frac{i+3b}{4}\rceil)f} \quad \text{if } 3b < 4e_0,\\ &\cong \hat{C}^f \oplus \hat{D}^f \oplus \hat{M}^f \quad \text{if } 3b > 4e_0, \text{ as } \mathbb{Z}_2[G]\text{-modules.} \end{aligned}$$

Note that since $b \in \{1, 3\}$; $3b > 4e_0$ implies $b = 3$ and $e_0 = 2$.

https://doi.org/10.4153/CJM-1998-050-4 Published online by Cambridge University Press

PROOF. See Section 3.43. ∎

CASE 2: TWO BREAKS IN THE RAMIFICATION FILTRATION. Suppose that there are two breaks in the ramification filtration of N/K associated with the two lower ramification numbers, b_1, b_2 where $b_1 < b_2$. It is well known that $b_1 \equiv b_2 \bmod 2$, see [21, Chapter IV], and because N/K is not cyclic, that $b_1 < 2e_0$, see [21, Chapter IV, Exercise 3] or [24]. Therefore $b_1 \equiv b_2 \equiv 1 \bmod 2$. Now without loss of generality assume that $\langle\sigma\rangle = G_{b_2}$, so the ramification groups of N/K are: $G = G_0 = \cdots = G_{b_1}$, $\langle\sigma\rangle = G_{b_1+1} = \cdots = G_{b_2}$, and $\langle 1\rangle = G_{b_2+1} = \cdots$. If s denotes the ramification number of L/K while t denotes the ramification number of M/K, it is necessarily the case that $s < t$, and that $s = b_1$ while $t = (b_2 + b_1)/2$ (this is a consequence of Herbrand's Theorem, see [21, Chapter IV Section 3]). It is easily seen that the ramification number of N/M is $b_1 = s$, while ramification number of N/L is $b_2 = 2t - s$ (this is a basic property of lower ramification numbers).

Each extension N/K may be constructed in the following manner. Begin with L/K and M/K arithmetically disjoint, ramified quadratic extensions. This is to say that the ramification numbers s and t of L/K and M/K respectively, are distinct. See Maus [14]. Without loss of generality, let $s < t$. From this we may conclude that $N = LM$ is a fully ramified biquadratic extension of K which has two breaks in its ramification filtration, associated with two lower ramification numbers, b_1 and b_2, where $b_1 = s$ while $b_2 = 2t - s$.

Since $s < t \leq 2e_0$, s is necessarily odd. On the other hand, t may be odd or even:

Case 2-odd. The case when t is odd, $(b_1 \equiv b_2 \bmod 4)$,

Case 2-even. The case when $t = 2e_0$ is even, $(b_1 \not\equiv b_2 \bmod 4)$.

Although each case requires the same basic approach of the proof of Theorem 3.1, the technical details are substantially different, and as a consequence, the results themselves are also substantially different.

THEOREM 3.6 (CASE 2-ODD). *Let N be any fully ramified biquadratic extension of K where $[K : \mathbb{Q}_2] = e_0 f$, e_0 denoting the absolute ramification index. Assume that N is the composite of two arithmetically disjoint quadratic extensions of K, denoted by L and M. Let $s < t < 2e_0$ denote the respective ramification numbers of L/K and M/K. Let $\mathrm{Gal}(N/K) = \langle\sigma,\gamma\rangle$, where L is the fixed field of $\langle\sigma\rangle$. Then*

$$\mathfrak{P}_N^i \cong \hat{H}_{k-1}^{(\lceil\frac{i+2t-s}{4}\rceil - \lceil\frac{i+2s}{4}\rceil + k(\frac{t-s}{2}))f} \oplus \hat{H}_k^{(\lceil\frac{i-2t}{4}\rceil - \lceil\frac{i-2t-s}{4}\rceil - k(\frac{t-s}{2}))f}$$
$$\oplus \begin{cases} \hat{G}^{(\lceil\frac{i}{4}\rceil - \lceil\frac{i+2t+s}{4}\rceil + e_0)f} \oplus \hat{C}^{(\lceil\frac{i+s}{4}\rceil - \lceil\frac{i}{4}\rceil)f} \oplus \hat{D}^{(\lceil\frac{i+2t+s}{4}\rceil - \lceil\frac{i+2t}{4}\rceil)f} & \text{if } 2t+s < 4e_0 \\ \hat{M}^{(\lceil\frac{i+2t+s}{4}\rceil - \lceil\frac{i}{4}\rceil - e_0)f} \oplus \hat{C}^{(\lceil\frac{i+s}{4}\rceil - \lceil\frac{i+2t+s}{4}\rceil + e_0)f} \oplus \hat{D}^{(\lceil\frac{i}{4}\rceil + e_0 - \lceil\frac{i+2t}{4}\rceil)f} & \text{if } 2t+s > 4e_0 \end{cases}$$

as $\mathbb{Z}_2[G]$-modules, where k is defined below.

Let $r \in \{0,1,2,3\}$ such that $r \equiv -i - 2 \bmod 4$, then $k = \lfloor (s+r)/(2t-2s) \rfloor$.

PROOF. See Section 3.43. ∎

Based upon the result of Theorem 3.6, we answer Chinburg's Question in the affirmative with Corollary 3.8.

DEFINITION 3.7. Let S_G^2 be the set of all indecomposable $\mathbb{Z}_2[G]$-modules, M, which are realized as direct summands of ideals, $\mathfrak{P}_N^i$, in local number field extensions, N/K, $[K:\mathbb{Q}_2]<\infty$, with $\mathrm{Gal}(N/K)\cong G$.

COROLLARY 3.8. *$S^2_{C_2\times C_2}$ is infinite, and so $S_{C_2\times C_2}$ is infinite.*

PROOF. This is a consequence of Theorem 3.6, Proposition 4.3 and the following family of biquadratic extensions. For $e=2n+1$, let $\sqrt[e]{2}$ be a root of $x^e-2=0$. Then $K_e=\mathbb{Q}_2(\sqrt[e]{2})$ is a fully ramified extension of $\mathbb{Q}_2$ with absolute ramification index, $e_0=e$. Let $\alpha=1+\sqrt[e]{2}$, then the quadratic defect of α is 1. The quadratic defect of $\beta=1+(\sqrt[e]{2})^3$ is 3. Let A be a root of $x^2-\alpha=0$ while B is a root of $x^2-\beta=0$. Following Wyman [24], $K_e(A)/K$ is a fully ramified quadratic extension with ramification number $2e-1$, $K_e(B)/K$ is a fully ramified quadratic extension with ramification number $2e-3$. Consequently, $N_e=K_e(A,B)/K_e$ is a fully ramified biquadratic extension with break numbers $b_1=2e-3$ and $b_2=2e+1$. As a result of Theorem 3.6, one copy of H_{n-1} appears in the decomposition of $\mathfrak{O}_{N_e}$.

Clearly, as there is no constraint on n, the corollary is verified. ∎

THEOREM 3.9 (CASE 2-EVEN). *Let N be fully ramified biquadratic extension of K where $[K:\mathbb{Q}_2]=e_0f$, e_0 denoting the absolute ramification index. Assume that N is the composite of two arithmetically disjoint quadratic extensions of K, denoted by L and M. Let s denote the ramification number of L/K, while $2e_0$ is the ramification number of M/K. Let $\mathrm{Gal}(N/K)=\langle\sigma,\gamma\rangle$, and assume that L is the fixed field of $\langle\sigma\rangle$. Then*

$$\begin{aligned}\mathfrak{P}_N^i \cong{}& (\hat{Z}\oplus\hat{R}_\sigma)^{(\lceil\frac{i-s-2}{4}\rceil-\lceil\frac{i-2s-2}{4}\rceil)f}\oplus(\hat{R}_\gamma\oplus\hat{R}_{\sigma\gamma})^{(\lceil\frac{i+s-2}{4}\rceil-\lceil\frac{i-2}{4}\rceil)f}\\ &\oplus\hat{I}_{k-1}^{af}\oplus\hat{L}_{k-1}^{bf}\oplus\hat{J}_l^{cf}\oplus\hat{K}_{l-1}^{df}\\ &\textit{as } \mathbb{Z}_2[G]\textit{-modules, where } a, b, c, d, k \textit{ and } l \textit{ are defined below}.\end{aligned}$$

Let $r\in\{0,1,2,3\}$ such that $r\equiv -i \bmod 4$, then let $k'=\big\lceil(s+r+1)/\big(4(2e_0-s)\big)\big\rceil$. If $\lceil(i+s-2)/4\rceil+k'(2e_0-s)=2e_0+\lceil(i+2s-2)/4\rceil$ and $\lceil(i-s-2)/4\rceil+(k'-1)(2e_0-s)-1=\lceil(i-2)/4\rceil$, then let $l=k=k'-1$; otherwise let $k=k'$ and if $\lceil(i-s-2)/4\rceil+k(2e_0-s)>e_0+\lceil(i-2s-2)/4\rceil$ or $\lceil(i+s-2)/4\rceil+k(2e_0-s)>e_0+\lceil(i-2)/4\rceil$ let $l=k-1$, otherwise let $l=k$.

For $l=k-1$

$$\begin{aligned}a&=\left\lceil\frac{i-2}{4}\right\rceil-\left\lceil\frac{i-s-2}{4}\right\rceil-(k-1)(2e_0-s),\\ b&=\left\lceil\frac{i+2s-2}{4}\right\rceil-\left\lceil\frac{i+s-2}{4}\right\rceil-(k-1)(2e_0-s),\\ c&=\left\lceil\frac{i+s-2}{4}\right\rceil-\left\lceil\frac{i-2}{4}\right\rceil+k(2e_0-s)-e_0,\\ d&=\left\lceil\frac{i-s-2}{4}\right\rceil-\left\lceil\frac{i-2s-2}{4}\right\rceil+k(2e_0-s)-e_0.\end{aligned}$$

https://doi.org/10.4153/CJM-1998-050-4 Published online by Cambridge University Press

For $l = k$

$$a = \left\lceil \frac{i+s-2}{4} \right\rceil - \left\lceil \frac{i+2s-2}{4} \right\rceil + k(2e_0 - s),$$
$$b = \left\lceil \frac{i-s-2}{4} \right\rceil - \left\lceil \frac{i-2}{4} \right\rceil + k(2e_0 - s),$$
$$c = \left\lceil \frac{i-2s-2}{4} \right\rceil - \left\lceil \frac{i-s-2}{4} \right\rceil - k(2e_0 - s) + e_0,$$
$$d = \left\lceil \frac{i-2}{4} \right\rceil - \left\lceil \frac{i+s-2}{4} \right\rceil - k(2e_0 - s) + e_0.$$

PROOF. See Section 3.43. ∎

3.4.2. Outline and evaluation of the method. Our method is a generalization of the method employed in a rudimentary form to prove Theorem 3.1 (see Remark 3.2). In our attempt to generalize the proof of Theorem 3.1, we will attempt to construct a set of elements, $\{\mu_j\}$, satisfying the following two conditions:

CONDITION 1. The members of the Galois group should take each element, μ_{j_0}, to some linear combination of μ_j's with coefficients in $\mathbb{Z}_2$.

CONDITION 2. It should be possible to index the elements by their valuation, so that $v_N(\mu_j) = j$ for $j = i, \ldots, 4e_0 + i - 1$.

We will attempt to construct the set, $\{\mu_j\}$, satisfying Conditions 1 and 2, knowing only the following information about the fully ramified biquadratic extension, N/K: The absolute ramification index of K, e_0, the ramification filtration of the extension N/K, and the integer i corresponding to the ideal, $\mathfrak{P}_N^i$.

Generalizing the proof of Theorem 3.1, by achieving both conditions simultaneously is difficult, especially while requiring so little information about the extension. Ideally, in following the proof of Theorem 3.1 (where we found integers, $v_N(\alpha)$ and $v_N\big((\gamma+1)\alpha\big)$ to have have opposite parity, *i.e.* to be distinct modulo 2), we would like to find an element $\alpha \in N$, with the analogous property, that the integers $v_N(\alpha)$, $v_N\big((\sigma+1)\alpha\big)$, $v_N\big((\gamma+1)\alpha\big)$ and $v_N\big((\gamma+1)(\sigma+1)\alpha\big)$ are all distinct modulo 4. If this were possible, we could immediately construct a set $\{\mu_j\}$ satisfying both conditions; follow the proof of Theorem 3.1 letting $\alpha_m = \alpha\pi_K^m$, *etc*. The principal difficulty with which we must contend is that this is not possible; because regardless of the choice of α, the integers $v_N\big((\sigma+1)\alpha\big)$, $v_N\big((\gamma+1)\alpha\big)$ and $v_N\big((\gamma+1)(\sigma+1)\alpha\big)$ are always even.

Fortunately, we are able to circumvent this obstacle somewhat. Using some basic results from ramification theory (namely Lemmas 3.12, 3.13 and 3.14), we can select four elements α, $(\sigma+1)\alpha$, ρ, $(\gamma+1)(\sigma+1)\alpha$ which have distinct valuations modulo 4. We can even make this selection with some control over the difference between $(\gamma+1)\alpha$ and ρ (see Lemmas 3.15, 3.17, 3.22). When there are two breaks in the ramification filtration, we are able to exert complete control, hence Theorem 3.6 and Theorem 3.9. When there is only one break in the ramification filtration, we are not. As a result, our results for one break are comparatively weak, Theorem 3.4 and Theorem 3.5.

We should explain that our results for fully ramified biquadratic extensions with one break number are weak, because it is not possible to generalize the proof of Theorem 3.1 for these extensions without knowing more information about the particular biquadratic extension involved.

If based only upon e_0, the ramification filtration and i we could generalize the proof of Theorem 3.1, then for all extensions N/K with absolute ramification index, e_0, and one break number b, it would necessarily be the case that $\mathfrak{P}_N^i \cong \mathfrak{O}_T \otimes_{\mathbb{Z}_2} M$ as $\mathfrak{O}_T[G]$-modules for some $\mathbb{Z}_2[G]$-module, M; the action of $\mathfrak{O}_T[G]$ being defined naturally: If $a \in \mathfrak{O}_T$ and $\sigma \in G$, while $b \otimes \beta \in \mathfrak{O}_T \otimes_{\mathbb{Z}_2} M$, then $a\sigma \cdot b \otimes \beta = ab \otimes \sigma\beta$, see [5, Section 30B].

PROPOSITION 3.10. *If $\{\mu_j\}$ is a subset of N which satisfies Conditions 1 and 2, then $\mathfrak{P}_N^i \cong \mathfrak{O}_T \otimes_{\mathbb{Z}_2} M$ as $\mathfrak{O}_T[G]$-modules for some $\mathbb{Z}_2[G]$-module, M.*

PROOF. Suppose that we have a set of elements $\{\mu_j\}$, satisfying Conditions 1 and 2. If the μ_j satisfy the Condition 1, then for a given j_0, each member of the Galois group takes μ_{j_0} to some linear combination of μ_j's with coefficients in $\mathbb{Z}_2$. If this is possible, then $M = \sum \mathbb{Z}_2\mu_j$ is closed under the action of the group, so that M is a $\mathbb{Z}_2[G]$-module. If furthermore, Condition 2 is satisfied, and we find that $v_N(\mu_j) = j$ for $j = i, \ldots, 4e_0 + i - 1$; then this set of μ_j's also serves as a basis for $\mathfrak{P}_N^i$ over $\mathfrak{O}_T$, so that $\mathfrak{P}_N^i = \sum \mathfrak{O}_T\mu_j = \mathfrak{O}_T \cdot M$. Therefore $\mathfrak{P}_N^i \cong \mathfrak{O}_T \otimes_{\mathbb{Z}_2} M$ as $\mathfrak{O}_T[G]$-modules. ∎

In Section 5, we exhibit a family of fully ramified biquadratic extensions N_b/K_b with one break in their ramification filtration (at b), along with ideals $\mathfrak{P}_{N_b}^i$, such that $\mathfrak{P}_{N_b}^i \not\cong \mathfrak{O}_T \otimes_{\mathbb{Z}_2} M$ as $\mathfrak{O}_T[G]$-modules for any $\mathbb{Z}_2[G]$-module, M. Thereby we show that one can not generalize the proof of Theorem 3.1 in the case where N/K is fully ramified with one break in its ramification filtration, except in the cases that we have already successfully done so, namely when $b = 1$ and $i \not\equiv 3 \bmod 4$, or when $b = 3$ and $i \equiv 2 \bmod 4$.

REMARK 3.11. If N/K is a fully ramified biquadratic extension with one break in the ramification filtration, because of the discussion above we should expect that Galois relationships among any basis for $\mathfrak{P}_N^i$ over $\mathfrak{O}_T$ to involve elements of $\mathfrak{O}_T - \mathbb{Z}_2$. Note that N/K has only one break in the ramification filtration exactly when N^σ, N^γ, and $N^{\sigma\gamma}$ are all generated by the square root of elements of K with the same quadratic defect. If we have three elements: α, β and $\alpha\beta \in K$ which all have the same quadratic defect, then without loss of generality we can assume that $\alpha - 1 = u \cdot (\beta - 1)$ for some u a unit in $\mathfrak{O}_T$. So in the case where N/K is a fully ramified biquadratic extension with one break in the ramification filtration, it would seem that this unit, u, should play a significant role in the Galois relationships among the members of any basis for $\mathfrak{P}_N^i$ over $\mathfrak{O}_T$.

3.4.3. Proofs for fully ramified biquadratic extensions. In this section we collect the technical proofs.

PRELIMINARY RESULTS. In this subsection we collect a few basic results from ramification theory. Serre's book is a good reference, [21].

LEMMA 3.12. *Let k be a finite extension of $\mathbb{Q}_2$. Let K/k be a cyclic ramified extension of degree 2, with $\langle\sigma\rangle = \mathrm{Gal}(K/k)$. Let v_K denote the normalized valuation of K, and b, the ramification number of K/k. Then for $\alpha \in K$ if $v_K(\alpha)$ is odd, then $v_K\big((\sigma-1)(\alpha)\big) = v_K(\alpha) + b$.*

PROOF. Let π denote a prime element in K, so that $v_K(\pi) = 1$. Clearly, $v_K\big((\sigma-1)\pi\big) = 1 + b$. If $\alpha \in K$ has odd valuation, express α uniquely as $\alpha = m + n\pi$, where $m, n \in k$. Since $v_K(m)$ is even while $v_K(n\pi) = v_K(n) + 1$ is odd, we find that, since $v_K(\alpha)$ is odd, $v_K(\alpha) = v_K(n\pi) < v_K(m)$. Therefore, $v_K\big((\sigma-1)(m+n\pi)\big) = v_K\big(n(\sigma-1)\pi\big) = v_K(n)+1+b = v_K(\alpha) + b$. ∎

LEMMA 3.13. *Let k be a finite extension of $\mathbb{Q}_2$. Let K/k be a cyclic ramified extension of degree 2, with $\langle\sigma\rangle = \mathrm{Gal}(K/k)$. Let v_k, v_K denote the normalized valuations of k and K, respectively. Let b denote the ramification number of K/k. Then for each $\mu \in k$ with $v_k(\mu) = n$, there exists a $\rho \in K$ with $v_K(\rho) = 2n - b$ such that $(\sigma + 1)\rho = \mu$.*

PROOF. From [21, p. 83] we have $\mathfrak{P}_K^m = \mathfrak{P}_k^{\lfloor (m+b+1)/2 \rfloor}$ which gives the result. ∎

LEMMA 3.14. *Let k be a finite extension of $\mathbb{Q}_2$. Let K/k be a cyclic ramified extension of degree 2, with $\langle\sigma\rangle = \mathrm{Gal}(K/k)$. Let v_K denote the normalized valuation of K, and b, the ramification number of K/k. Assume that b is odd If $\tau \in K$ be an element with even valuation, such that $(\sigma+1)\tau = 0$, then there is an element α with $v_K(\alpha) = v_K(\tau) - b$ such that $(\sigma-1)\alpha = \tau$.*

PROOF. Since $H^{-1}(\langle\sigma\rangle, K) = 0$ there is an element α such that $(\sigma-1)\alpha = \tau$. Clearly we may change α by an element of k without effecting the property that $(\sigma-1)\alpha = \tau$. So we may assume that $v_K(\alpha)$ is odd. This with Lemma 3.12 proves the result. ∎

CASE 1: ONE BREAK IN THE RAMIFICATION FILTRATION. Let b denote the ramification number of N/K.

LEMMA 3.15. *Let α_m be any element of N with $v_N(\alpha_m) = b+4m$. Then $v_N\big((\sigma+1)\alpha_m\big) = 2b + 4m$, $v_N\big((\gamma+1)(\sigma+1)\alpha_m\big) = 4b + 4m$, and there are elements $\rho_m, \theta_m \in N$ with $v_N(\rho_m) = 3b + 4m$, $v_N(\theta_m) = b + 4m$ such that $\rho_m - (\gamma+1)\alpha_m = (\sigma+1)\theta_m$.*

$$v_N(\alpha_m) = b + 4m, \quad v_N\big((\sigma+1)\alpha_m\big) = 2b + 4m,$$
$$v_N(\rho_m) = 3b + 4m, \quad v_N\big((\gamma+1)(\sigma+1)\alpha_m\big) = 4b + 4m.$$

PROOF. Clearly, $v_N\big((\sigma+1)\alpha_m\big) = \min\big\{v_N\big((\sigma-1)\alpha_m\big), v_N((2\alpha_m)\big\} = v_N\big((\sigma-1)\alpha_m\big)$, since $b < 4e_0$. Since $v_N(\alpha_m)$ is odd, by Lemma 3.12, $v_N\big((\sigma-1)\alpha_m\big) = 2b + 4m$. Similarly, $v_N\big((\gamma+1)\alpha_m\big) = 2b + 4m$. Since $v_L\big((\sigma+1)\alpha_m\big)$ is odd, by Lemma 3.12, $v_N\big((\gamma+1)(\sigma+1)\alpha_m\big) = 4b + 4m$.

By Lemma 3.13, there is an element, $\rho_m^* \in N$ with $v_N(\rho_m^*) = 3b + 4m$, and $(\sigma+1)\rho_m^* = (\sigma+1)(\gamma+1)\alpha_m$. Clearly, $\rho_m^* - (\gamma+1)\alpha_m$ is killed by $(\sigma+1)$, so by Lemma 3.14 there is an element $\theta_m \in N$ such that $\rho_m^* - (\gamma+1)\alpha_m = (\sigma-1)\theta_m$ and $v_N(\theta_m) = b + 4m$.

Now $b < 2e_0$, therefore $v_N(\rho_m^*) = 3b + 4m < 4e_0 + b + 4m = v_N(2\theta_m)$. So if we let $\rho_m = \rho_m^* + 2\theta_m$, then $v_N(\rho_m) = 3b + 4m$, and $\rho_m - (\gamma+1)\alpha_m = (\sigma+1)\theta_m$. Note that ρ_m and $(\gamma+1)\alpha$ differ by an element in L. ∎

Since b is odd, $\{\overline{b+4m}, \overline{2b+4m}, \overline{3b+4m}, \overline{4b+4m}\} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ where $\overline{x}$ denotes the residue modulo 4. Therefore we may use α_m, $(\sigma+1)\alpha_m$, ρ_m and $(\gamma+1)(\sigma+1)\alpha_m$ to construct a basis for $\mathfrak{P}_N^i$ over $\mathfrak{O}_T$. Clearly, $3b < 4e_0$ or $3b > 4e_0$. If $3b < 4e_0$, then the following sequence is increasing $\cdots < v_N(\alpha_m) < v_N\big((\sigma+1)\alpha_m\big) < v_N(\rho_m) < v_N\big((\gamma+1)(\sigma+1)\alpha_m\big) < v_N(2\alpha_m) < v_N(2(\sigma+1)\alpha_m) < v_N(2\rho_m) < \cdots$, while if $3b > 4e_0$, then there is an alternative increasing sequence $\cdots < v_N\big((\sigma+1)\alpha_m\big) < v_N(\rho_m) < v_N(2\alpha_m) < v_N\big((\gamma+1)(\sigma+1)\alpha_m\big) < v_N\big(2(\sigma+1)\alpha_m\big) < v_N(2\rho_m) < v_N(4\alpha_m) < \cdots$.

Note that for example when $3b < 4e_0$, if $v_N(\alpha_m) \le i < v_N\big((\sigma+1)\alpha_m\big)$, then $v_N(2\alpha_m) \le 4e_0 + i < v_N(2(\sigma+1)\alpha_m)$. Based upon observations such as this, we choose those elements whose valuation, v_N, lies in the set $\{i, i+1, \ldots, 4e_0 + i - 1\}$. They make up an $\mathfrak{O}_T$-basis for $\mathfrak{P}_N^i$.

There are two cases to consider, either $3b < 4e_0$ or $3b > 4e_0$. In either case, there are four possible orderings to consider. First we consider the case, $3b < 4e_0$.

CASE 1, $3b < 4e_0$.

(3.2)
$$\alpha_m,\ (\sigma+1)\alpha_m,\ \rho_m,\ (\gamma+1)(\sigma+1)\alpha_m, \quad \text{for } \left\lceil \frac{i-b}{4} \right\rceil \le m \le e_0 + \left\lceil \frac{i}{4} \right\rceil - b - 1.$$
(3.3)
$$(\sigma+1)\alpha_m,\ \rho_m,\ (\gamma+1)(\sigma+1)\alpha_m,\ 2\alpha_m, \quad \text{for } \left\lceil \frac{i-2b}{4} \right\rceil \le m \le \left\lceil \frac{i-b}{4} \right\rceil - 1.$$
(3.4)
$$\rho_m,\ (\gamma+1)(\sigma+1)\alpha_m,\ 2\alpha_m,\ 2(\sigma+1)\alpha_m, \quad \text{for } \left\lceil \frac{i-3b}{4} \right\rceil \le m \le \left\lceil \frac{i-2b}{4} \right\rceil - 1.$$
(3.5)
$$(\gamma+1)(\sigma+1)\alpha_m,\ 2\alpha_m,\ 2(\sigma+1)\alpha_m,\ 2\rho_m, \quad \text{for } \left\lceil \frac{i}{4} \right\rceil - b \le m \le \left\lceil \frac{i-3b}{4} \right\rceil - 1.$$

We know that $v_N\big((\sigma+1)\theta_m\big) = v_N\big((\sigma+1)\alpha_m\big)$, where of course $(\sigma+1)\theta_m = \rho_m - (\gamma+1)\alpha_m$.

REMARK 3.16. Clearly $\mathfrak{P}_N^i = \mathfrak{P}_L^{\lceil i/2 \rceil} + X$ where X is spanned by the elements of type α and ρ. Since we may alter any $\mathfrak{O}_T$-basis element of X by an element in $\mathfrak{P}_L^{\lceil i/2 \rceil}$, and still have an $\mathfrak{O}_T$-basis for $\mathfrak{P}_N^i$, when the difference between ρ and $(\gamma+1)\alpha$ lies in $\mathfrak{P}_L^{\lceil i/2 \rceil}$, we may replace ρ by $(\gamma+1)\alpha$.

Therefore in (3.2), because $(\sigma+1)\theta_m \in \mathfrak{P}_L^{\lceil i/2 \rceil}$, we replace ρ_m with $(\gamma+1)\alpha_m$, while in (3.3) and (3.5), because $2(\sigma+1)\theta_m \in \mathfrak{P}_L^{\lceil i/2 \rceil}$ so we replace $2\rho_m$ with $2(\gamma+1)\alpha_m$. Only in (3.4) is $(\sigma+1)\theta_m \notin \mathfrak{P}_L^{\lceil i/2 \rceil}$, and so in this particular case, we leave ρ_m in our basis.

CASE 1, $3b < 4e_0$ (REVISED).

(3.6)
$$\alpha_m,\ (\sigma+1)\alpha_m,\ (\gamma+1)\alpha_m,\ (\gamma+1)(\sigma+1)\alpha_m, \quad \text{for } \left\lceil\frac{i-b}{4}\right\rceil \le m \le e_0 + \left\lceil\frac{i}{4}\right\rceil - b - 1.$$
(3.7)
$$(\sigma+1)\alpha_m,\ (\gamma+1)\alpha_m,\ (\gamma+1)(\sigma+1)\alpha_m,\ 2\alpha_m, \quad \text{for } \left\lceil\frac{i-2b}{4}\right\rceil \le m \le \left\lceil\frac{i-b}{4}\right\rceil - 1.$$
(3.8)
$$\rho_m,\ (\gamma+1)(\sigma+1)\alpha_m,\ 2\alpha_m,\ 2(\sigma+1)\alpha_m, \quad \text{for } \left\lceil\frac{i-3b}{4}\right\rceil \le m \le \left\lceil\frac{i-2b}{4}\right\rceil - 1.$$
(3.9)
$$(\gamma+1)(\sigma+1)\alpha_m,\ 2\alpha_m,\ 2(\sigma+1)\alpha_m,\ 2(\gamma+1)\alpha_m, \quad \text{for } \left\lceil\frac{i}{4}\right\rceil - b \le m \le \left\lceil\frac{i-3b}{4}\right\rceil - 1.$$

CASE 1, $3b > 4e_0$ (ALREADY REVISED). In this other case, we have gone ahead and replaced ρ_m with $(\gamma+1)\alpha_m$ whenever we can. In (3.10), $(\sigma+1)\theta_m \in \mathfrak{P}_L^{\lceil i/2\rceil}$, so we have replaced ρ_m with $(\gamma+1)\alpha_m$, while in (3.12) and (3.13), $2(\sigma+1)\theta_m \in \mathfrak{P}_L^{\lceil i/2\rceil}$, so we have replaced $2\rho_m$ with $2(\gamma+1)\alpha_m$. Only in (3.11), have we left ρ_m alone.

$$(3.10)\qquad (\sigma+1)\alpha_m,\ (\gamma+1)\alpha_m,\ 2\alpha_m,\ (\gamma+1)(\sigma+1)\alpha_m, \quad \text{for } \left\lceil\frac{i-2b}{4}\right\rceil \le m \le e_0 + \left\lceil\frac{i}{4}\right\rceil - b - 1$$

$$(3.11)\qquad \rho_m,\ 2\alpha_m,\ (\gamma+1)(\sigma+1)\alpha_m,\ 2(\sigma+1)\alpha_m, \quad \text{for } \left\lceil\frac{i-3b}{4}\right\rceil \le m \le \left\lceil\frac{i-2b}{4}\right\rceil - 1$$

$$(3.12)\qquad 2\alpha_m,\ (\gamma+1)(\sigma+1)\alpha_m,\ 2(\sigma+1)\alpha_m,\ 2(\gamma+1)\alpha_m, \quad \text{for } \left\lceil\frac{i-b}{4}\right\rceil - e_0 \le m \le \left\lceil\frac{i-3b}{4}\right\rceil - 1$$

$$(3.13)\qquad (\gamma+1)(\sigma+1)\alpha_m,\ 2(\sigma+1)\alpha_m,\ 2(\gamma+1)\alpha_m,\ 4\alpha_m, \quad \text{for } \left\lceil\frac{i}{4}\right\rceil - b \le m \le \left\lceil\frac{i-b}{4}\right\rceil - e_0 - 1.$$

Based upon the $\mathfrak{O}_T$-basis described in (3.6) through (3.13), we prove Theorem 3.4.

PROOF (THEOREM 3.4). Clearly $0 \longrightarrow \mathfrak{P}_L^{\lceil i/2\rceil} \longrightarrow \mathfrak{P}_N^i \longrightarrow \mathfrak{P}_N^i/\mathfrak{P}_L^{\lceil i/2\rceil} \longrightarrow 0$ is a short exact sequence. We need only determine the $\mathbb{Z}_2[G]$-module structure of the $\mathfrak{P}_L^{\lceil i/2\rceil}$ and $\mathfrak{P}_N^i/\mathfrak{P}_L^{\lceil i/2\rceil}$, and the structure of $\mathfrak{P}_L^{\lceil i/2\rceil}$ is already determined by Theorem 3.1. The structure of $\mathfrak{P}_N^i/\mathfrak{P}_L^{\lceil i/2\rceil}$ results from a careful examination of (3.6)–(3.13), and an understanding of the Galois action upon the ρ_m which appear in the basis of $\mathfrak{P}_N^i/\mathfrak{P}_L^{\lceil i/2\rceil}$. In each case (3.8) or (3.11), $\overline{\rho_m}$ and $\overline{2\alpha_m}$ contribute as $\mathfrak{O}_T$-basis elements of $\mathfrak{P}_N^i/\mathfrak{P}_L^{\lceil i/2\rceil}$. Note that $\overline{(\sigma+1)\rho_m} = \overline{0}$, and $\overline{(\gamma+1)\rho_m} = \overline{0}$, while $\overline{(\sigma+1)(2\alpha_m+\rho_m)} = \overline{0}$, and $\overline{(\gamma-1)(2\alpha_m+\rho_m)} = \overline{0}$. Therefore $\mathfrak{O}_T\overline{\rho_m}$ is isomorphic to f copies of the $\mathbb{Z}_2[G]$-module, $\hat{R}_{\sigma\gamma}$, while $\mathfrak{O}_T\overline{(2\alpha_m+\rho_m)}$ is isomorphic to f copies of the $\mathbb{Z}_2$-module, $\hat{R}_\gamma$. ∎

However our stated aim is to determine the $\mathbb{Z}_2[G]$-module structure of $\mathfrak{P}_N^i$ itself, not to merely capture it in a short exact sequence. The ρ_m's in (3.8) and (3.11) present an essential obstruction which we are unable to overcome (see Section 3.4.2). But if $\lceil (i-3b)/4\rceil = \lceil (i-2b)/4\rceil$, the cases (3.8) and (3.11) do not occur. And $\lceil (i-3b)/4\rceil = \lceil (i-2b)/4\rceil$, if and only if $b = 1$ and $i \equiv 0,1,2 \bmod 4$, or $b = 3$ and $i \equiv 2 \bmod 4$. Under these circumstances, we may say that for each m the four elements listed in (3.6), (3.7), (3.9), (3.10), (3.12), (3.13) collectively give rise to $\mathfrak{O}_T[G]$-summands of $\mathfrak{P}_N^i$. In Section 4, we have listed certain $\mathbb{Z}_2[G]$-modules which appear in the course of this paper. Clearly, each m in (3.6) gives rise to f copies of the group ring, $\hat{G}$. Each m in (3.9) and (3.12) give rise to f copies of $\hat{C}$; each m in (3.7) and (3.10) provide f copies of $\hat{D}$, while each m in (3.13) contributes f copies of the maximal order, $\hat{M} \cong \hat{Z} \oplus \hat{R}_\sigma \oplus \hat{R}_\gamma \oplus \hat{R}_{\sigma\gamma}$. This is collected in Theorem 3.5.

CASE 2: TWO BREAKS IN THE RAMIFICATION FILTRATION. Let s, $2t - s$ be the lower ramification numbers of N/K. In particular, note that $2t - s$ is the ramification number of N/L. In the following situation, we assume that t is odd.

CASE 2-ODD.

LEMMA 3.17. *Let α_m be any element of N with $v_N(\alpha_m) = 2t - s + 4m$. Then $v_N\big((\sigma+1)\alpha_m\big) = 4t - 2s + 4m$, $v_N\big((\gamma+1)(\sigma+1)\alpha_m\big) = 4t + 4m$. If t is odd, then there are elements $\rho_m, \theta_m \in N$ with $v_N(\rho_m) = 2t + s + 4m$, $v_N(\theta_m) = s + 4m$ such that $\rho_m - (\gamma+1)\alpha_m = (\sigma+1)\theta_m$.*

$$v_N(\alpha_m) = 2t - s + 4m, \quad v_N\big((\sigma+1)\alpha_m\big) = 4t - 2s + 4m,$$
$$v_N(\rho_m) = 2t + s + 4m, \quad v_N\big((\gamma+1)(\sigma+1)\alpha_m\big) = 4t + 4m.$$

PROOF. Because $2t - s + 4m$ is odd, $v_N\big((\sigma+1)\alpha_m\big)$ which is equal to $\min\big\{v_N\big((\sigma-1)\alpha_m\big), v_N(2\alpha_m)\big\}$ is equal to $v_N\big((\sigma-1)\alpha_m\big)$, since $2t - s < 4e_0$. By Lemma 3.12, $v_N\big((\sigma-1)\alpha_m\big) = 4t - 2s + 4m$. Therefore $v_N\big((\sigma+1)\alpha_m\big) = 4t - 2s + 4m$. Similarly, $v_N\big((\gamma+1)\alpha_m\big) = v_N\big((\gamma-1)\alpha_m\big) = 2t + 4m$. Furthermore, since $v_L\big((\sigma+1)\alpha_m\big) = 2t - s + 2m$ is odd, $v_L\big((\gamma+1)(\sigma+1)\alpha_m\big) = 2t + 2m$, so that by Lemma 3.12, $v_N\big((\gamma+1)(\sigma+1)\alpha_m\big) = 4t + 4m$.

By Lemma 3.13,there is an element $\rho_m^* \in N$ with $v_N(\rho_m^*) = 2t + s + 4m$ such that $(\sigma+1)(\rho_m^*) = (\gamma+1)(\sigma+1)\alpha_m$. Therefore $\rho_m^* - (\gamma+1)\alpha_m$ is killed by $(\sigma+1)$, and so by Lemma 3.14 $\rho_m^* - (\gamma+1)\alpha_m = (\sigma-1)\theta_m$, for some $\theta_m \in N$ where $v_N(\theta_m) = s + 4m$. Now we use the fact that t is odd and so $t < 2e_0$. Let $\rho_m = \rho_m^* + 2\theta_m$, then $v_N(\rho_m) = v_N(\rho_m^*)$ and we have $\rho_m - (\gamma+1)\alpha_m = (\sigma+1)\theta_m$. Note that ρ_m and $(\gamma+1)\alpha$ differ by an element in L. ∎

Since s is odd, $\{\overline{2t-s}, \overline{4t-2s}, \overline{2t+s}, \overline{4t}\} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ where $\bar{x}$ denotes the residue modulo 4. Consequently, we may use α_m, $(\sigma+1)\alpha_m$, ρ_m and $(\gamma+1)(\sigma+1)\alpha_m$ as we did in Case 1 to construct a basis for $\mathfrak{P}_N^i$ over $\mathfrak{O}_T$. Choose those elements whose valuation, v_N, lies in the set $\{i, i+1, \ldots, 4e_0 + i - 1\}$.

Before we list the $\mathfrak{O}_T$-basis for $\mathfrak{O}_N$, notice a complication which did not appear in Case 1. If $3s < 2t$, then $v_N(\rho_m) < v_N\big((\sigma+1)\alpha_m\big)$, while if $3s > 2t$, then $v_N(\rho_m) > v_N\big((\sigma+1)\alpha_m\big)$. Note $3s \neq 2t$, since s is odd. (By contrast, in Case 1 it was always the case that $v_N(\rho_m) > v_N\big((\sigma+1)\alpha_m\big)$.) Meanwhile, there is another condition, depending on whether $2t+s < 4e_0$ or $2t+s > 4e_0$. (This condition is reminiscent of the condition $3b < 4e_0$ or $3b > 4e_0$, from Case 1.) This condition affects the ordering of the valuations of $(\gamma+1)(\sigma+1)\alpha_m$ and $2\alpha_m$. Taking these two conditions into account we have the following four orderings of the valuations: If $3s < 2t$ and $2t+s < 4e_0$, then the following sequence is increasing $\cdots < v_N(\alpha_m) < v_N(\rho_m) < v_N\big((\sigma+1)\alpha_m\big) < v_N\big((\gamma+1)(\sigma+1)\alpha_m\big) < v_N(2\alpha_m) < v_N(2\rho_m) < v_N\big(2(\sigma+1)\alpha_m\big) < \cdots$; if $3s < 2t$ and $2t+s > 4e_0$, then the following sequence is increasing $\cdots < v_N(\rho_m) < v_N\big((\sigma+1)\alpha_m\big) < v_N(2\alpha_m) < v_N\big((\gamma+1)(\sigma+1)\alpha_m\big) < v_N(2\rho_m) < v_N\big(2(\sigma+1)\alpha_m\big) < v_N(4\alpha_m) < \cdots$; if $3s > 2t$ and $2t+s < 4e_0$, then the following sequence is increasing $\cdots < v_N(\alpha_m) < v_N\big((\sigma+1)\alpha_m\big) < v_N(\rho_m) < v_N\big((\gamma+1)(\sigma+1)\alpha_m\big) < v_N(2\alpha_m) < v_N\big(2(\sigma+1)\alpha_m\big) < v_N(2\rho_m) < \cdots$; while if $3s > 2t$ and $2t+s > 4e_0$, then the following sequence is increasing $\cdots < v_N\big((\sigma+1)\alpha_m\big) < v_N(\rho_m) < v_N(2\alpha_m) < v_N\big((\gamma+1)(\sigma+1)\alpha_m\big) < v_N\big(2(\sigma+1)\alpha_m\big) < v_N(2\rho_m) < v_N(4\alpha_m) < \cdots$. Now as we did in Case 1, we choose those elements whose valuation, v_N, lies in the set $\{i, i+1, \ldots, 4e_0+i-1\}$. They make up an $\mathfrak{O}_T$-basis for $\mathfrak{P}_N^i$.

CASE 2-ODD, $3s < 2t$, $2t+s < 4e_0$.

(3.14)
$$\alpha_m,\ \rho_m, (\sigma+1)\alpha_m,\ (\gamma+1)(\sigma+1)\alpha_m, \quad \text{for } \left\lceil \frac{i-2t+s}{4} \right\rceil \le m \le e_0 + \left\lceil \frac{i}{4} \right\rceil - t - 1$$

(3.15)
$$\rho_m,\ (\sigma+1)\alpha_m, (\gamma+1)(\sigma+1)\alpha_m, 2\alpha_m, \quad \text{for } \left\lceil \frac{i-2t-s}{4} \right\rceil \le m \le \left\lceil \frac{i-2t+s}{4} \right\rceil - 1$$

(3.16)
$$(\sigma+1)\alpha_m,\ (\gamma+1)(\sigma+1)\alpha_m,\ 2\alpha_m,\ 2\rho_m, \quad \text{for } \left\lceil \frac{i+2s}{4} \right\rceil - t \le m \le \left\lceil \frac{i-2t-s}{4} \right\rceil - 1;$$

(3.17)
$$(\gamma+1)(\sigma+1)\alpha_m,\ 2\alpha_m,\ 2\rho_m,\ 2(\sigma+1)\alpha_m, \quad \text{for } \left\lceil \frac{i}{4} \right\rceil - t \le m \le \left\lceil \frac{i+2s}{4} \right\rceil - t - 1$$

CASE 2-ODD, $3s < 2t$, $2t+s > 4e_0$. :

(3.18)
$$\rho_m,\ (\sigma+1)\alpha_m,\ 2\alpha_m,\ (\gamma+1)(\sigma+1)\alpha_m, \quad \text{for } \left\lceil \frac{i-2t-s}{4} \right\rceil \le m \le e_0 + \left\lceil \frac{i}{4} \right\rceil - t - 1$$

(3.19)
$$(\sigma+1)\alpha_m,\ 2\alpha_m,\ (\gamma+1)(\sigma+1)\alpha_m,\ 2\rho_m, \quad \text{for } \left\lceil \frac{i+2s}{4} \right\rceil - t \le m \le \left\lceil \frac{i-2t-s}{4} \right\rceil - 1;$$

https://doi.org/10.4153/CJM-1998-050-4 Published online by Cambridge University Press

(3.20)
$$2\alpha_m,\ (\gamma+1)(\sigma+1)\alpha_m,\ 2\rho_m,\ 2(\sigma+1)\alpha_m,\quad \text{for } \left\lceil\frac{i-2t+s}{4}\right\rceil - e_0 \le m \le \left\lceil\frac{i+2s}{4}\right\rceil - t - 1,$$

(3.21)
$$(\gamma+1)(\sigma+1)\alpha_m,\ 2\rho_m,\ 2(\sigma+1)\alpha_m,\ 4\alpha_m,\quad \text{for } \left\lceil\frac{i}{4}\right\rceil - t \le m \le \left\lceil\frac{i-2t+s}{4}\right\rceil - e_0 - 1$$

CASE 2-ODD, $3s > 2t$, $2t+s < 4e_0$.

(3.22)
$$\alpha_m,\ (\sigma+1)\alpha_m,\ \rho_m,\ (\gamma+1)(\sigma+1)\alpha_m,\quad \text{for } \left\lceil\frac{i-2t+s}{4}\right\rceil \le m \le e_0 + \left\lceil\frac{i}{4}\right\rceil - t - 1;$$

(3.23)
$$(\sigma+1)\alpha_m,\ \rho_m,\ (\gamma+1)(\sigma+1)\alpha_m,\ 2\alpha_m,\quad \text{for } \left\lceil\frac{i+2s}{4}\right\rceil - t \le m \le \left\lceil\frac{i-2t+s}{4}\right\rceil - 1$$

(3.24)
$$\rho_m,\ (\gamma+1)(\sigma+1)\alpha_m,\ 2\alpha_m,\ 2(\sigma+1)\alpha_m,\quad \text{for } \left\lceil\frac{i-2t-s}{4}\right\rceil \le m \le \left\lceil\frac{i+2s}{4}\right\rceil - t - 1;$$

(3.25)
$$(\gamma+1)(\sigma+1)\alpha_m,\ 2\alpha_m,\ 2(\sigma+1)\alpha_m,\ 2\rho_m,\quad \text{for } \left\lceil\frac{i}{4}\right\rceil - t \le m \le \left\lceil\frac{i-2t-s}{4}\right\rceil - 1$$

CASE 2-ODD, $3s > 2t$, $2t+s > 4e_0$.

(3.26)
$$(\sigma+1)\alpha_m,\ \rho_m,\ 2\alpha_m,\ (\gamma+1)(\sigma+1)\alpha_m,\quad \text{for } \left\lceil\frac{i+2s}{4}\right\rceil - t \le m \le e_0 + \left\lceil\frac{i}{4}\right\rceil - t - 1$$

(3.27)
$$\rho_m,\ 2\alpha_m,\ (\gamma+1)(\sigma+1)\alpha_m,\ 2(\sigma+1)\alpha_m,\quad \text{for } \left\lceil\frac{i-2t-s}{4}\right\rceil \le m \le \left\lceil\frac{i+2s}{4}\right\rceil - t - 1;$$

(3.28)
$$2\alpha_m,\ (\gamma+1)(\sigma+1)\alpha_m,\ 2(\sigma+1)\alpha_m,\ 2\rho_m,\quad \text{for } \left\lceil\frac{i-2t+s}{4}\right\rceil - e_0 \le m \le \left\lceil\frac{i-2t-s}{4}\right\rceil - 1$$

(3.29)
$$(\gamma+1)(\sigma+1)\alpha_m,\ 2(\sigma+1)\alpha_m,\ 2\rho_m,\ 4\alpha_m,\quad \text{for } \left\lceil\frac{i}{4}\right\rceil - t \le m \le \left\lceil\frac{i-2t+s}{4}\right\rceil - e_0 - 1;$$

CASE 2-ODD, REVISITED. As we did in Case 1, whenever we can using Remark 3.16, we replace ρ_m with $(\gamma+1)\alpha_m$. Note that because $3s < 2t$, $v_N(\alpha_m) \le v_N((\sigma+1)\theta_m \le v_N(\rho_m)$, therefore, in (3.30), (3.33), (3.34), (3.37), (3.38), we go ahead and replace ρ_m by $(\gamma+1)\alpha_m$. Also $v_N\big((\gamma+1)(\sigma+1)\alpha_m\big) \le v_N\big(2(\sigma+1)\theta_m\big)$ since $t < 2e_0$, therefore, in (3.39), we replace $2\rho_m$ by $2(\gamma+1)\alpha_m$. Finally, we split (3.15) into two cases, (3.31) and (3.32) depending on whether or not $(\sigma+1)\theta_m \in$ or $\notin \mathfrak{P}_L^{\lceil i/2\rceil}$. In (3.31), we replace ρ_m by $(\gamma+1)\alpha_m$. Similarly, (3.18) is now split into two cases, (3.35) and (3.36), where in (3.35) we replace ρ_m with $(\gamma+1)\alpha_m$.

CASE 2-ODD, $3s < 2t$, $2t + s < 4e_0$.

$$\alpha_m,\ (\gamma+1)\alpha_m,\ (\sigma+1)\alpha_m,\ (\gamma+1)(\sigma+1)\alpha_m,\quad \text{for } \left\lceil \frac{i-2t+s}{4} \right\rceil \le m \le e_0 + \left\lceil \frac{i}{4} \right\rceil - t - 1 \tag{3.30}$$

$$(\gamma+1)\alpha_m,\ (\sigma+1)\alpha_m,\ (\gamma+1)(\sigma+1)\alpha_m,\ 2\alpha_m,\quad \text{for } \left\lceil \frac{i-2t}{4} \right\rceil \le m \le \left\lceil \frac{i-2t+s}{4} \right\rceil - 1 \tag{3.31}$$

$$\rho_m,\ (\sigma+1)\alpha_m,\ (\gamma+1)(\sigma+1)\alpha_m,\ 2\alpha_m,\quad \text{for } \left\lceil \frac{i-2t-s}{4} \right\rceil \le m \le \left\lceil \frac{i-2t}{4} \right\rceil - 1 \tag{3.32}$$

$$(\sigma+1)\alpha_m,\ (\gamma+1)(\sigma+1)\alpha_m,\ 2\alpha_m,\ 2(\gamma+1)\alpha_m,\quad \text{for } \left\lceil \frac{i+2s}{4} \right\rceil - t \le m \le \left\lceil \frac{i-2t-s}{4} \right\rceil - 1; \tag{3.33}$$

$$(\gamma+1)(\sigma+1)\alpha_m,\ 2\alpha_m,\ 2(\gamma+1)\alpha_m,\ 2(\sigma+1)\alpha_m,\quad \text{for } \left\lceil \frac{i}{4} \right\rceil - t \le m \le \left\lceil \frac{i+2s}{4} \right\rceil - t - 1 \tag{3.34}$$

CASE 2-ODD, $3s < 2t$, $2t + s > 4e_0$.

$$(\gamma+1)\alpha_m,\ (\sigma+1)\alpha_m,\ 2\alpha_m,\ (\gamma+1)(\sigma+1)\alpha_m,\quad \text{for } \left\lceil \frac{i-2t}{4} \right\rceil \le m \le e_0 + \left\lceil \frac{i}{4} \right\rceil - t - 1 \tag{3.35}$$

$$\rho_m,\ (\sigma+1)\alpha_m,\ 2\alpha_m,\ (\gamma+1)(\sigma+1)\alpha_m,\quad \text{for } \left\lceil \frac{i-2t-s}{4} \right\rceil \le m \le \left\lceil \frac{i-2t}{4} \right\rceil - 1 \tag{3.36}$$

$$(\sigma+1)\alpha_m,\ 2\alpha_m,\ (\gamma+1)(\sigma+1)\alpha_m,\ 2(\gamma+1)\alpha_m,\quad \text{for } \left\lceil \frac{i+2s}{4} \right\rceil - t \le m \le \left\lceil \frac{i-2t-s}{4} \right\rceil - 1; \tag{3.37}$$

$$2\alpha_m,\ (\gamma+1)(\sigma+1)\alpha_m,\ 2(\gamma+1)\alpha_m,\ 2(\sigma+1)\alpha_m,\quad \text{for } \left\lceil \frac{i-2t+s}{4} \right\rceil - e_0 \le m \le \left\lceil \frac{i+2s}{4} \right\rceil - t - 1, \tag{3.38}$$

$$(\gamma+1)(\sigma+1)\alpha_m,\ 2(\gamma+1)\alpha_m,\ 2(\sigma+1)\alpha_m,\ 4\alpha_m,\quad \text{for } \left\lceil \frac{i}{4} \right\rceil - t \le m \le \left\lceil \frac{i-2t+s}{4} \right\rceil - e_0 - 1 \tag{3.39}$$

https://doi.org/10.4153/CJM-1998-050-4 Published online by Cambridge University Press

The only place where ρ_m still remains, is (3.32) and (3.36). In these cases note that $\rho_m = (\gamma+1)\alpha_m + (\sigma+1)\theta_m$ where $v_N(\theta_m) = s+4m = (2t-s)+4\big(m-(t-s)/2\big)$. Note that when we initially chose the α_m, we chose them based on their valuation alone. In fact any element with the same valuation would do, so we make another stipulation. Once, we have selected the α_m for each m, for $\lceil (i-2t-s)/4\rceil \le m \le \lceil (i-2t)/4\rceil - 1$, and have determined the θ_m's, choose α_m for $\lceil (i+s)/4\rceil - t \le m \le \lceil (i+2s)/4\rceil - t - 1$, to be $\theta_{m+(t-s)/2}$. As a consequence, we can list the following $\mathfrak{O}_T$-basis for $\mathfrak{P}_N^i$, from which we determine the $\mathbb{Z}_2[G]$-module structure immediately.

CASE 2-ODD, $3s < 2t$, $2t+s < 4e_0$, (FINAL REVISION).

$$\begin{aligned}(3.40)\qquad &\alpha_m,\ (\gamma+1)\alpha_m,\ (\sigma+1)\alpha_m,\ (\gamma+1)(\sigma+1)\alpha_m,\\ &\qquad\text{for } \left\lceil\frac{i-2t+s}{4}\right\rceil \le m \le e_0 + \left\lceil\frac{i}{4}\right\rceil - t - 1\end{aligned}$$

$$\begin{aligned}(3.41)\qquad &(\gamma+1)\alpha_m,\ (\sigma+1)\alpha_m,\ (\gamma+1)(\sigma+1)\alpha_m,\ 2\alpha_m,\\ &\qquad\text{for } \left\lceil\frac{i-2t}{4}\right\rceil \le m \le \left\lceil\frac{i-2t+s}{4}\right\rceil - 1\end{aligned}$$

$$\begin{aligned}&(\gamma+1)\alpha_m + (\sigma+1)\alpha_n,\ (\sigma+1)\alpha_m,\ (\gamma+1)(\sigma+1)\alpha_m,\ 2\alpha_m,\\ (3.42)\qquad &(\gamma+1)(\sigma+1)\alpha_n,\ 2\alpha_n,\ 2(\gamma+1)\alpha_n,\ 2(\sigma+1)\alpha_n,\\ &\qquad\text{for } \left\lceil\frac{i-2t-s}{4}\right\rceil \le m \le \left\lceil\frac{i-2t}{4}\right\rceil - 1 \text{ where } n = m-(t-s)/2\end{aligned}$$

$$\begin{aligned}(3.43)\qquad &(\sigma+1)\alpha_m,\ (\gamma+1)(\sigma+1)\alpha_m,\ 2\alpha_m,\ 2(\gamma+1)\alpha_m,\\ &\qquad\text{for } \left\lceil\frac{i+2s}{4}\right\rceil - t \le m \le \left\lceil\frac{i-2t-s}{4}\right\rceil - 1;\end{aligned}$$

$$\begin{aligned}(3.44)\qquad &(\gamma+1)(\sigma+1)\alpha_m,\ 2\alpha_m,\ 2(\gamma+1)\alpha_m,\ 2(\sigma+1)\alpha_m,\\ &\qquad\text{for } \left\lceil\frac{i}{4}\right\rceil - t \le m \le \left\lceil\frac{i+s}{4}\right\rceil - t - 1\end{aligned}$$

CASE 2-ODD, $3s < 2t$, $2t+s > 4e_0$, (FINAL REVISION).

$$\begin{aligned}(3.45)\qquad &(\gamma+1)\alpha_m,\ (\sigma+1)\alpha_m,\ 2\alpha_m,\ (\gamma+1)(\sigma+1)\alpha_m,\\ &\qquad\text{for } \left\lceil\frac{i-2t}{4}\right\rceil \le m \le e_0 + \left\lceil\frac{i}{4}\right\rceil - t - 1\end{aligned}$$

$$\begin{aligned}&(\gamma+1)\alpha_m + (\sigma+1)\alpha_n,\ (\sigma+1)\alpha_m,\ 2\alpha_m,\ (\gamma+1)(\sigma+1)\alpha_m,\\ (3.46)\qquad &2\alpha_n,\ (\gamma+1)(\sigma+1)\alpha_n,\ 2(\gamma+1)\alpha_n,\ 2(\sigma+1)\alpha_n,\\ &\qquad\text{for } \left\lceil\frac{i-2t-s}{4}\right\rceil \le m \le \left\lceil\frac{i-2t}{4}\right\rceil - 1 \text{ where } n = m-(t-s)/2\end{aligned}$$

https://doi.org/10.4153/CJM-1998-050-4 Published online by Cambridge University Press

(3.47) $$(\sigma+1)\alpha_m,\ 2\alpha_m,\ (\gamma+1)(\sigma+1)\alpha_m,\ 2(\gamma+1)\alpha_m,$$
$$\text{for } \left\lceil\frac{i+2s}{4}\right\rceil - t \le m \le \left\lceil\frac{i-2t-s}{4}\right\rceil - 1;$$

(3.48) $$2\alpha_m,\ (\gamma+1)(\sigma+1)\alpha_m,\ 2(\gamma+1)\alpha_m,\ 2(\sigma+1)\alpha_m,$$
$$\text{for } \left\lceil\frac{i-2t+s}{4}\right\rceil - e_0 \le m \le \left\lceil\frac{i+s}{4}\right\rceil - t - 1,$$

(3.49) $$(\gamma+1)(\sigma+1)\alpha_m,\ 2(\gamma+1)\alpha_m,\ 2(\sigma+1)\alpha_m,\ 4\alpha_m,$$
$$\text{for } \left\lceil\frac{i}{4}\right\rceil - t \le m \le \left\lceil\frac{i-2t+s}{4}\right\rceil - e_0 - 1$$

Clearly, each m in (3.40) yields f copies of the group ring, $\hat{G}$. One may check that each m in (3.44) and (3.48) yields f copies of $\hat{C}$; each m in (3.41) and (3.45) yields f copies of $\hat{D}$; each m in (3.42) and (3.46) yields f copies of $\hat{H}_0$; each m in (3.43) and (3.47) yields f copies of $\hat{E}_+ \oplus \hat{E}_- = \hat{H}_{-1}$; while each m in (3.49) yields f copies of the maximal ideal, $\hat{M} \cong \hat{Z} \oplus \hat{R}_\sigma \oplus \hat{R}_\gamma \oplus \hat{R}_{\sigma\gamma}$. All this is collected into Theorem 3.6.

REMARK 3.18. Note that Theorem 3.6 is stated without respect to the condition $3s < 2t$. Certainly, if $k=0$, then $3s < 2t$, however if $3s < 2t$ then $k=0$ or $k=1$. To be sure that the statement of the Theorem is consistent with the the basis expressed in (3.60) through (3.69), above observe the following: If $3s < 2t$ while $k=1$, then $\lceil (i+2t-s)/4\rceil - \lceil (i+2s)/4\rceil = 0$, so $\hat{H}_{-1}$ does not appear in $\mathfrak{P}_N^i$. Clearly, $\lceil (i-2)/4\rceil - \lceil (i-2t-s)/4\rceil - (t-s)/2 = 0$, so $\hat{H}_1$ doesn't really appear in the statement of the Theorem. While $\lceil (i+2t-s)/4\rceil + (t-s)/2 - \lceil (i+2s)/4\rceil = \lceil (i-2t)/4\rceil - \lceil (i-2t-s)/4\rceil$.

CASE 2-ODD, $3s > 2t$. Note that in this case, $v_N(\alpha_m) \le v_N((\sigma+1)\theta_m \le v_N\big((\sigma+1)\alpha_m\big)$, and so in (3.50), (3.54), (3.58) based upon Remark 3.16, we have gone ahead and replaced ρ_m by $(\gamma+1)\alpha_m$. Also $v_N\big((\gamma+1)(\sigma+1)\alpha_m\big) \le v_N\big(2(\sigma+1)\theta_m\big)$, therefore, in (3.59), we have replaced $2\rho_m$ by $2(\gamma+1)\alpha_m$. Now $\lceil (i-2t)/4\rceil \ge \lceil \big(i-2t-2(t-s)\big)/4\rceil = \lceil (i+2s)/4\rceil - t$, and if $m \ge \lceil (i-2t)/4\rceil$, then $2t+4m \ge i$ and consequently, $(\sigma+1)\theta_m \in \mathfrak{P}_L^{\lceil i/2\rceil}$. So we can break (3.23), (3.26) up into two parts depending on whether or not $(\sigma+1)\theta_m \in$ or $\notin \mathfrak{P}_L^{\lceil i/2\rceil}$ yielding (3.51) and (3.52), and (3.55) and (3.56).

CASE 2-ODD, $3s > 2t$, $2t+s < 4e_0$.

(3.50) $$\alpha_m,\ (\sigma+1)\alpha_m,\ (\gamma+1)\alpha_m,\ (\gamma+1)(\sigma+1)\alpha_m,$$
$$\text{for } \left\lceil\frac{i-2t+s}{4}\right\rceil \le m \le e_0 + \left\lceil\frac{i}{4}\right\rceil - t - 1;$$

(3.51) $$(\sigma+1)\alpha_m,\ (\gamma+1)\alpha_m,\ (\gamma+1)(\sigma+1)\alpha_m,\ 2\alpha_m,$$
$$\text{for } \left\lceil\frac{i-2t}{4}\right\rceil \le m \le \left\lceil\frac{i-2t+s}{4}\right\rceil - 1$$

https://doi.org/10.4153/CJM-1998-050-4 Published online by Cambridge University Press

$$(\sigma+1)\alpha_m,\ \rho_m,\ (\gamma+1)(\sigma+1)\alpha_m,\ 2\alpha_m, \quad \text{for } \left\lceil\frac{i+2s}{4}\right\rceil - t \le m \le \left\lceil\frac{i-2t}{4}\right\rceil - 1 \tag{3.52}$$

$$\rho_m,\ (\gamma+1)(\sigma+1)\alpha_m,\ 2\alpha_m,\ 2(\sigma+1)\alpha_m, \quad \text{for } \left\lceil\frac{i-2t-s}{4}\right\rceil \le m \le \left\lceil\frac{i+2s}{4}\right\rceil - t - 1; \tag{3.53}$$

$$(\gamma+1)(\sigma+1)\alpha_m,\ 2\alpha_m,\ 2(\sigma+1)\alpha_m,\ 2(\gamma+1)\alpha_m, \quad \text{for } \left\lceil\frac{i}{4}\right\rceil - t \le m \le \left\lceil\frac{i-2t-s}{4}\right\rceil - 1 \tag{3.54}$$

CASE 2-ODD, $3s > 2t$, $2t + s > 4e_0$.

$$(\sigma+1)\alpha_m,\ (\gamma+1)\alpha_m,\ 2\alpha_m,\ (\gamma+1)(\sigma+1)\alpha_m, \quad \text{for } \left\lceil\frac{i-2t}{4}\right\rceil \le m \le e_0 + \left\lceil\frac{i}{4}\right\rceil - t - 1 \tag{3.55}$$

$$(\sigma+1)\alpha_m,\ \rho_m,\ 2\alpha_m,\ (\gamma+1)(\sigma+1)\alpha_m, \quad \text{for } \left\lceil\frac{i+2s}{4}\right\rceil - t \le m \le \left\lceil\frac{i-2t}{4}\right\rceil - 1 \tag{3.56}$$

$$\rho_m,\ 2\alpha_m,\ (\gamma+1)(\sigma+1)\alpha_m,\ 2(\sigma+1)\alpha_m, \quad \text{for } \left\lceil\frac{i-2t-s}{4}\right\rceil \le m \le \left\lceil\frac{i+2s}{4}\right\rceil - t - 1; \tag{3.57}$$

$$2\alpha_m,\ (\gamma+1)(\sigma+1)\alpha_m,\ 2(\sigma+1)\alpha_m,\ 2(\gamma+1)\alpha_m, \quad \text{for } \left\lceil\frac{i-2t+s}{4}\right\rceil - e_0 \le m \le \left\lceil\frac{i-2t-s}{4}\right\rceil - 1 \tag{3.58}$$

$$(\gamma+1)(\sigma+1)\alpha_m,\ 2(\sigma+1)\alpha_m,\ 2(\gamma+1)\alpha_m,\ 4\alpha_m, \quad \text{for } \left\lceil\frac{i}{4}\right\rceil - t \le m \le \left\lceil\frac{i-2t+s}{4}\right\rceil - e_0 - 1; \tag{3.59}$$

Before we proceed, we need to collect certain observations:

LEMMA 3.19. *Let $r \in \{0,1,2,3\}$ with $r \equiv -i-2 \bmod 4$, and let $k = \lfloor (s+r)/(2t-2s) \rfloor$. Then k is the least integer such that $\lceil (i+2s)/4 \rceil - t - k(t-s)/2 < \lceil (i-2t-s)/4 \rceil$.*

PROOF. Since s is odd, $r \equiv -i-2 \equiv -i-2s \bmod 4$, so $i+2s = 4n-r$ for some integer n. The inequality reduces to $-t-k(t-s)/2 \le \lceil (-3s-r-2t)/4 \rceil - 1$. This is equivalent to $-t-k(t-s)/2 \le \lceil (-3s-r-2t-1)/4 \rceil$, or $-t-k(t-s)/2 \le (-3s-r-2t-1)/4$ which is equivalent to $k(t-s)/2 \ge (3s+r-2t+1)/4$. This is equivalent to $k \ge (3s+r-2t+1)/(2t-2s)$, and also to $k \ge \lceil (3s+r-2t+1)/(2t-2s) \rceil = \lceil (3s+r-2t)/(2t-2s) \rceil + 1 = \lceil (s+r)/(2t-2s) \rceil$. ∎

LEMMA 3.20. *Since s,t are odd, $\lceil (i-2t-s)/4 \rceil - \lceil (i-2t)/4 \rceil + \lceil (i+2s)/4 \rceil = \lceil (i+s)/4 \rceil$. Therefore $\lceil (i-2t)/4 \rceil - \lceil (i+2s)/4 \rceil + t \le e_0 - \lceil (i-2t+s)/4 \rceil + \lceil (i-2t-s)/4 \rceil$. Also $\lceil (i-2t)/4 \rceil - \lceil (i+2s)/4 \rceil \le \lceil (i-2t-s)/4 \rceil + \lceil i/4 \rceil$.*

PROOF. Let $i = 4a + b$, $b = 0, 1, 2, 3$; $t = 2c + 1$; $s = 4e + f$, $f = 1$ or 3. The equality in the lemma is true if and only if $\lceil (b-2-f)/4\rceil - \lceil (b-2)/4\rceil + \lceil (b+2f)/4\rceil = \lceil (b+f)/4\rceil$, which one can easily verify is true, by checking all possibilities for f and b. The first inequality in this lemma reduces to $\lceil (i + 2t + s)/4\rceil - \lceil (i + s)/4\rceil \leq e_0$, which is easily verified using $t < 2e_0$. Replace i, t and s in the second inequality and it reduces to $\lceil (b-2)/4\rceil - \lceil (b + 2f)/4\rceil - e \leq \lceil (b-2-f)/4\rceil$, which one can verify by checking all possibilities for f and b. ∎

As we did when $3s < 2t$, we are going to choose the α_m listed in (3.53), (3.54), (3.57) and (3.58) again. First note that $\lceil (i-2t)/4\rceil - (t-s)/2 = \lceil (i + 2s)/4\rceil - t$. Therefore if m is listed in (3.52) with $\lceil (i + 2s)/4\rceil - t \leq m \leq \lceil (i-2t)/4\rceil - 1$, then $m - (t-s)/2 \leq \lceil (i + 2s)/4\rceil - t - 1$, and listed in (3.53). Let

$$f(m, i) = m - i(t-s)/2.$$

Begin with an m listed in (3.52) or (3.56), redefine $\alpha_{f(m,1)}$ to be θ_m. Now $\alpha_{f(m,1)}$ is listed in (3.53) or (3.57) respectively. So long as $m - i(t-s)/2 \geq \lceil (i-2t-s)/4\rceil$, recursively define $\alpha_{f(m,i+1)} = \theta_{f(m,i)}$. Define k as in Lemma 3.19, then depending on m, the last $\alpha_{f(m,r)}$ to be redefined is either $\alpha_{f(m,k+1)}$ or $\alpha_{f(m,k+2)}$. In either case the last element to be redefined is listed in (3.54) or (3.58) respectively, because as one can check using Lemma 3.20, the number of m's in (3.52) and (3.56) are respectively fewer than the number of m's in (3.54) and (3.58). Then, as one may verify, the following elements do constitute a $\mathfrak{O}_T$-basis for $\mathfrak{P}^i_N$.

CASE 2-ODD, $3s > 2t$, $2t + s < 4e_0$, (FINAL REVISION).

$$\alpha_m,\ (\sigma+1)\alpha_m,\ (\gamma+1)\alpha_m,\ (\gamma+1)(\sigma+1)\alpha_m, \quad \text{for } \left\lceil \frac{i-2t+s}{4}\right\rceil \leq m \leq e_0 + \left\lceil \frac{i}{4}\right\rceil - t - 1; \tag{3.60}$$

$$(\sigma+1)\alpha_m,\ (\gamma+1)\alpha_m,\ (\gamma+1)(\sigma+1)\alpha_m,\ 2\alpha_m, \quad \text{for } \left\lceil \frac{i-2t}{4}\right\rceil \leq m \leq \left\lceil \frac{i-2t+s}{4}\right\rceil - 1 \tag{3.61}$$

$$\begin{gathered}
(\sigma+1)\alpha_m,\ (\gamma+1)\alpha_m + (\sigma+1)\alpha_{f(m,1)},\ (\gamma+1)(\sigma+1)\alpha_m,\ 2\alpha_m,\\
(\gamma+1)\alpha_{f(m,1)} + (\sigma+1)\alpha_{f(m,2)},\\
(\gamma+1)(\sigma+1)\alpha_{f(m,1)},\ 2\alpha_{f(m,1)},\ 2(\sigma+1)\alpha_{f(m,1)},\\
\vdots\\
(\gamma+1)\alpha_{f(m,k+1)} + (\sigma+1)\alpha_{f(m,k+2)},\\
(\gamma+1)(\sigma+1)\alpha_{f(m,k+1)},\ 2\alpha_{f(m,k+1)},\ 2(\sigma+1)\alpha_{f(m,k+1)},\\
(\gamma+1)(\sigma+1)\alpha_{f(m,k+2)},\ 2\alpha_{f(m,k+2)},\ 2(\sigma+1)\alpha_{f(m,k+2)},\ 2(\gamma+1)\alpha_{f(m,k+2)},\\
\text{for } \left\lceil \frac{i-2t-s}{4}\right\rceil + k\left(\frac{t-s}{2}\right) \leq m \leq \left\lceil \frac{i-2t}{4}\right\rceil - 1\\
(\sigma+1)\alpha_m,\ (\gamma+1)\alpha_m + (\sigma+1)\alpha_{f(m,1)},\ (\gamma+1)(\sigma+1)\alpha_m,\ 2\alpha_m,
\end{gathered} \tag{3.62}$$

https://doi.org/10.4153/CJM-1998-050-4 Published online by Cambridge University Press

$$
\begin{gathered}
(\gamma+1)\alpha_{f(m,1)}+(\sigma+1)\alpha_{f(m,2)},\\
(\gamma+1)(\sigma+1)\alpha_{f(m,1)},\ 2\alpha_{f(m,1)},\ 2(\sigma+1)\alpha_{f(m,1)},\\
\vdots\\
(\gamma+1)\alpha_{f(m,k)}+(\sigma+1)\alpha_{f(m,k+1)},\\
(\gamma+1)(\sigma+1)\alpha_{f(m,k)},\ 2\alpha_{f(m,k)},\ 2(\sigma+1)\alpha_{f(m,k)},\\
(\gamma+1)(\sigma+1)\alpha_{f(m,k+1)},\ 2\alpha_{f(m,k+1)},\ 2(\sigma+1)\alpha_{f(m,k+1)},\ 2(\gamma+1)\alpha_{f(m,k+1)},\\
\text{for } \left\lceil\frac{i+2s}{4}\right\rceil-t\le m\le\left\lceil\frac{i-2t-s}{4}\right\rceil+k\left(\frac{t-s}{2}\right)-1
\end{gathered}\tag{3.63}
$$

$$
\begin{gathered}
(\gamma+1)(\sigma+1)\alpha_m,\ 2\alpha_m,\ 2(\sigma+1)\alpha_m,\ 2(\gamma+1)\alpha_m,\\
\text{for } \left\lceil\frac{i}{4}\right\rceil-t\le m\le\left\lceil\frac{i+s}{4}\right\rceil-t-1
\end{gathered}\tag{3.64}
$$

CASE 2-ODD, $3s>2t$, $2t+s>4e_0$, (FINAL REVISION).

$$
\begin{gathered}
(\sigma+1)\alpha_m,\ (\gamma+1)\alpha_m,\ 2\alpha_m,\ (\gamma+1)(\sigma+1)\alpha_m,\\
\text{for } \left\lceil\frac{i-2t}{4}\right\rceil\le m\le e_0+\left\lceil\frac{i}{4}\right\rceil-t-1
\end{gathered}\tag{3.65}
$$

$$
\begin{gathered}
(\sigma+1)\alpha_m,\ (\gamma+1)\alpha_m+(\sigma+1)\alpha_{f(m,1)},\ 2\alpha_m,\ (\gamma+1)(\sigma+1)\alpha_m,\\
(\gamma+1)\alpha_{f(m,1)}+(\sigma+1)\alpha_{f(m,2)},\\
2\alpha_{f(m,1)},\ (\gamma+1)(\sigma+1)\alpha_{f(m,1)},\ 2(\sigma+1)\alpha_{f(m,1)},\\
\vdots\\
(\gamma+1)\alpha_{f(m,k+1)}+(\sigma+1)\alpha_{f(m,k+2)},\\
2\alpha_{f(m,k+1)},\ (\gamma+1)(\sigma+1)\alpha_{f(m,k+1)},\ 2(\sigma+1)\alpha_{f(m,k+1)},\\
2\alpha_{f(m,k+2)},\ (\gamma+1)(\sigma+1)\alpha_{f(m,k+2)},\ 2(\sigma+1)\alpha_{f(m,k+2)},\ 2(\gamma+1)\alpha_{f(m,k+2)},\\
\text{for } \left\lceil\frac{i-2t-s}{4}\right\rceil+k\left(\frac{t-s}{2}\right)\le\left\lceil\frac{i-2t}{4}\right\rceil-1
\end{gathered}\tag{3.66}
$$

$$
\begin{gathered}
(\sigma+1)\alpha_m,\ (\gamma+1)\alpha_m+(\sigma+1)\alpha_{f(m,1)},\ 2\alpha_m,\ (\gamma+1)(\sigma+1)\alpha_m,\\
(\gamma+1)\alpha_{f(m,1)}+(\sigma+1)\alpha_{f(m,2)},\\
2\alpha_{f(m,1)},\ (\gamma+1)(\sigma+1)\alpha_{f(m,1)},\ 2(\sigma+1)\alpha_{f(m,1)},\\
\vdots\\
(\gamma+1)\alpha_{f(m,k)}+(\sigma+1)\alpha_{f(m,k+1)},\\
2\alpha_{f(m,k)},\ (\gamma+1)(\sigma+1)\alpha_{f(m,k)},\ 2(\sigma+1)\alpha_{f(m,k)},\\
2\alpha_{f(m,k+1)},\ (\gamma+1)(\sigma+1)\alpha_{f(m,k+1)},\ 2(\sigma+1)\alpha_{f(m,k+1)},\ 2(\gamma+1)\alpha_{f(m,k+1)},\\
\text{for } \left\lceil\frac{i+2s}{4}\right\rceil-t\le m\le\left\lceil\frac{i-2t-s}{4}\right\rceil+k\left(\frac{t-s}{2}\right)-1
\end{gathered}\tag{3.67}
$$

$$
\begin{gathered}
2\alpha_m,\ (\gamma+1)(\sigma+1)\alpha_m,\ 2(\sigma+1)\alpha_m,\ 2(\gamma+1)\alpha_m,\\
\text{for } \left\lceil\frac{i-2t+s}{4}\right\rceil-e_0\le m\le\left\lceil\frac{i+s}{4}\right\rceil-t-1
\end{gathered}\tag{3.68}
$$

https://doi.org/10.4153/CJM-1998-050-4 Published online by Cambridge University Press

(3.69) $$(\gamma+1)(\sigma+1)\alpha_m,\ 2(\sigma+1)\alpha_m,\ 2(\gamma+1)\alpha_m,\ 4\alpha_m,$$
$$\text{for } \left\lceil\frac{i}{4}\right\rceil - t \le m \le \left\lceil\frac{i-2t+s}{4}\right\rceil - e_0 - 1;$$

Clearly, each m in (3.60) yields f copies of the group ring, $\hat{G}$. One may check that each m in (3.64) and (3.68) yields f copies of $\hat{C}$; each m in (3.61) and (3.65) yields f copies of $\hat{D}$; each m in (3.63) and (3.67) yields f copies of $\hat{H}_{k-1}$; each m in (3.62) and (3.66) yields f copies of $\hat{H}_k$; while each m in (3.69) yields f copies of the maximal ideal, $\hat{M} \cong \hat{Z} \oplus \hat{R}_\sigma \oplus \hat{R}_\gamma \oplus \hat{R}_{\sigma\gamma}$. All this is consistent with the statement of Theorem 3.6.

CASE 2-EVEN. Since t, the ramification number of M/K, is $2e_0$, $M = K(\sqrt{\pi})$, where $\sqrt{\pi}$ is a square root of a prime element of K. Since s the ramification number of L/K is odd; $L = K(\sqrt{u})$, where $\sqrt{u}$ is a square root of unit, $u \in K$, with quadratic defect, $2e_0 - s$ [24].

REMARK 3.21. Because $t = 2e_0$ is even, if we attempt to repeat the process which we used successfully in the proof of Lemma 3.17, we would find that $v_N(\rho_m^*) = 2t + s + 4m = 4e_0 + s = v_N(2\theta_m)$. This makes the valuation of $\rho_m = \rho_m^* + 2\theta_m$ difficult to determine, preventing us from simply replacing ρ_m^* by ρ_m as we did in the proof of Lemma 3.17. But this is not the only obstacle which prevents us from handling the two cases similarly. In Lemma 3.17, because t is odd, $v_N(\alpha_m) \ne v_N(\theta_m)$, while, $v_N(\alpha_m) \equiv v_N(\theta_m) \bmod 4$. Therefore, θ_m could be considered to be another α_n for some other $n \ne m$. However, if t is even, then $v_N(\alpha_m) \not\equiv v_N(\theta_m) \bmod 4$, and so we may not consider θ_m as another α_n. These two differences prevent us from handling Case 2-odd and Case 2-even in the same way.

Fortunately, we may handle the case when t is even, with the following lemma.

LEMMA 3.22. *Let τ_m be any element of K with $v_K(\tau_m) = m$. Then there exist elements α_m and ρ_m such that $(\sigma-1)\alpha_m = (\gamma-1)\rho_m = \sqrt{u}\cdot\sqrt{\pi}\cdot\tau_m$. Furthermore, $2(\gamma+1)\alpha_m = (\sigma+1)(\gamma+1)\alpha_m$, $2(\sigma+1)\rho_m = (\sigma+1)(\gamma+1)\rho_m$, $(\gamma-1)\rho_m = (\sigma+1)\alpha_m - 2\alpha_m$, and*

$$v_N(\alpha_m) = 2 + s + 4m - 4e_0, \quad v_N(\rho_m) = 2 + 4m - s$$
$$v_N\big((\sigma+1)\rho_m\big) = 2 - 2s + 4e_0 + 4m, \quad v_N\big((\gamma+1)\alpha_m\big) = 2 + 2s + 4m - 4e_0.$$

PROOF. Since σ fixes L while γ fixes M we see that $\sigma+1$ and $\gamma+1$ both kill $\sqrt{u}\cdot\sqrt{\pi}\cdot\tau_m \in N$, where clearly $v_N(\sqrt{u}\cdot\sqrt{\pi}\cdot\tau_m) = 2 + 4m$. Therefore, by Lemma 3.14, there are elements α_m, $\rho_m \in N$ with the desired properties. The other statements are consequences of $(\sigma-1)\alpha_m = (\gamma-1)\rho_m = \sqrt{u}\cdot\sqrt{\pi}\cdot\tau_m$. ∎

Now $\{\overline{2+s}, \overline{2+2s}, \overline{2-s}, \overline{2}\} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ where $\overline{x}$ denotes the residue modulo 4. We may therefore use α_m, $(\gamma+1)\alpha_m$, ρ_m and $(\sigma+1)\alpha_m$ to construct a basis for $\mathfrak{P}_N^i$ over $\mathfrak{O}_T$. If $3s < 4e_0$, then the following sequence is increasing $\cdots < v_N(\alpha_m) < v_N\big((\gamma+1)\alpha_m\big) < v_N(\rho_m) < v_N\big((\sigma+1)\alpha_m\big) < v_N(2\alpha_m) < v_N(2(\gamma+1)\alpha_m) < v_N(2\rho_m) < \cdots$, while if $3s > 4e_0$, then the following alternative sequence is increasing $\cdots < v_N(\alpha_m) < v_N(\rho_m) < v_N\big((\gamma+1)\alpha_m\big) < v_N\big((\sigma+1)\alpha_m\big) < v_N(2\alpha_m) < v_N(2\rho_m) < v_N\big(2(\gamma+1)\alpha_m\big) < \cdots$. Choose those elements whose valuation, v_N, lies in the set $\{i, i+1, \ldots, 4e_0+i-1\}$.

CASE 2-EVEN, $3s < 4e_0$. The following elements comprise an $\mathfrak{O}_T$-basis of $\mathfrak{P}_N^i$.

$$\alpha_m, (\gamma+1)\alpha_m,\ \rho_m,\quad (\sigma+1)\alpha_m \quad \text{for } e_0+\left\lceil\frac{i-s-2}{4}\right\rceil \le m \le e_0+\left\lceil\frac{i-2}{4}\right\rceil-1 \tag{3.70}$$

$$(\gamma+1)\alpha_m,\ \rho_m,\ (\sigma+1)\alpha_m,\ 2\alpha_m \quad \text{for } e_0+\left\lceil\frac{i-2s-2}{4}\right\rceil \le m \le e_0+\left\lceil\frac{i-s-2}{4}\right\rceil-1 \tag{3.71}$$

$$\rho_m,\ (\sigma+1)\alpha_m,\ 2\alpha_m,\ 2(\gamma+1)\alpha_m \quad \text{for } \left\lceil\frac{i+s-2}{4}\right\rceil \le m \le e_0+\left\lceil\frac{i-2s-2}{4}\right\rceil-1 \tag{3.72}$$

$$(\sigma+1)\alpha_m,\ 2\alpha_m,\ 2(\gamma+1)\alpha_m,\ 2\rho_m \quad \text{for } \left\lceil\frac{i-2}{4}\right\rceil \le m \le \left\lceil\frac{i+s-2}{4}\right\rceil-1 \tag{3.73}$$

CASE 2-EVEN, $3s > 4e_0$.

$$\frac{1}{2}(\sigma+1)\alpha_m,\ \alpha_m,\ \rho_m,\ (\gamma+1)\alpha_m \quad \text{for } e_0+\left\lceil\frac{i-2}{4}\right\rceil \le m \le 2e_0+\left\lceil\frac{i-2s-2}{4}\right\rceil-1 \tag{3.74}$$

$$\alpha_m,\ \rho_m,\ (\gamma+1)\alpha_m,\ (\sigma+1)\alpha_m \quad \text{for } e_0+\left\lceil\frac{i-s-2}{4}\right\rceil \le m \le e_0+\left\lceil\frac{i-2}{4}\right\rceil-1 \tag{3.75}$$

$$\rho_m,\ (\gamma+1)\alpha_m,\ (\sigma+1)\alpha_m,\ 2\alpha_m \quad \text{for } \left\lceil\frac{i+s-2}{4}\right\rceil \le m \le e_0+\left\lceil\frac{i-s-2}{4}\right\rceil-1 \tag{3.76}$$

$$(\gamma+1)\alpha_m,\ (\sigma+1)\alpha_m,\ 2\alpha_m,\ 2\rho_m \quad \text{for } e_0+\left\lceil\frac{i-2s-2}{4}\right\rceil \le m \le \left\lceil\frac{i+s-2}{4}\right\rceil-1 \tag{3.77}$$

REVISION OF THE BASIS. It is sometimes the case that ρ_m ($2\rho_m$) appears in our $\mathfrak{O}_T$-basis of $\mathfrak{P}_N^i$, while $\big((\sigma+1)/2\big)\rho_m \in \mathfrak{P}_N^i$ ($(\sigma+1)\rho_m \in \mathfrak{P}_N^i$). Based upon Remark 3.16, when this happens we may replace ρ_m by $\beta_m = \rho_m - \big((\sigma+1)/2\big)\rho_m$ ($2\rho_m$ by $2\beta_m = 2\rho_m - (\sigma+1)\rho_m$) and still have a basis. As one may easily check, $(\sigma+1)\beta_m = 0$ and $(\gamma-1)\beta_m = (\gamma-1)\rho_m = (\sigma+1)\alpha_m - 2\alpha_m$. Since the Galois action on β_m is more easily described than the Galois action on ρ_m, we replace ρ_m by β_m whenever possible.

CASE 2-EVEN, $3s < 4e_0$. In this case, because $4e_0 > 3s$ one may easily check that, since $m \ge e_0 + \lceil (i-s-2)/4 \rceil$, $v_N\Big(\big((\sigma+1)/2\big)\rho_m\Big) \ge i + (4e_0 - 3s) \ge i$, for each ρ_m in (3.70). Therefore we replace each ρ_m in (3.70) by β_m. One can also easily see that each $2\rho_m$ in (3.73) may be replaced by $2\beta_m$. However in (3.71) and (3.72) we do not always have $v_N\Big(\big((\sigma+1)/2\big)\rho_m\Big) \ge i$. Consequently, for clarity's sake, we now break

CASE 2-EVEN, $3s < 4e_0$. Into three cases depending upon whether $s < e_0$, $s = e_0$ or $s > e_0$.

CASE 2, $s < e_0$. In this case, since $m \geq e_0 + \lceil (i-2s-2)/4 \rceil$, $v_N\Big(\big((\sigma+1)/2\big)\rho_m\Big) \geq i + 4(e_0 - s) \geq i$, we may replace every ρ_m in (3.71) by a β_m. However not every ρ_m in (3.72) may be replaced, and so we separate (3.72) into two cases depending on whether or not $v_N\Big(\big((\sigma+1)/2\big)\rho_m\Big) \geq i$.

The following elements comprise an $\mathfrak{O}_T$-basis of $\mathfrak{P}_N^i$:

$$\alpha_m,\ (\gamma+1)\alpha_m,\ \beta_m,\ (\sigma+1)\alpha_m \quad \text{for } e_0 + \left\lceil \frac{i-s-2}{4} \right\rceil \leq m \leq e_0 + \left\lceil \frac{i-2}{4} \right\rceil - 1 \tag{3.78}$$

$$(\gamma+1)\alpha_m,\ \beta_m,\ (\sigma+1)\alpha_m,\ 2\alpha_m \quad \text{for } e_0 + \left\lceil \frac{i-2s-2}{4} \right\rceil \leq m \leq e_0 + \left\lceil \frac{i-s-2}{4} \right\rceil - 1 \tag{3.79}$$

$$\beta_m,\ (\sigma+1)\alpha_m,\ 2\alpha_m,\ 2(\gamma+1)\alpha_m \quad \text{for } \left\lceil \frac{i+2s-2}{4} \right\rceil \leq m \leq e_0 + \left\lceil \frac{i-2s-2}{4} \right\rceil - 1 \tag{3.80}$$

$$\rho_m,\ (\sigma+1)\alpha_m,\ 2\alpha_m,\ 2(\gamma+1)\alpha_m \quad \text{for } \left\lceil \frac{i+s-2}{4} \right\rceil \leq m \leq \left\lceil \frac{i+2s-2}{4} \right\rceil - 1 \tag{3.81}$$

$$(\sigma+1)\alpha_m,\ 2\alpha_m,\ 2(\gamma+1)\alpha_m,\ 2\beta_m \quad \text{for } \left\lceil \frac{i-2}{4} \right\rceil \leq m \leq \left\lceil \frac{i+s-2}{4} \right\rceil - 1 \tag{3.82}$$

Now for each m from $\lceil (i+s-2)/4 \rceil + (e_0 - s)$ up to $e_0 + \lceil (i-2s-2)/4 \rceil$ recursively redefine the τ_m's employed in Lemma 3.22. Once τ_m has been defined, define $\tau_{m+(e_0-s)}$ to be $1/2\Big(\big((\sigma+1)(\gamma+1)\rho_m\big)/\big((\sigma+1)(\gamma+1)\alpha_m\big)\Big) \cdot \tau_m$. Note that $v_K\bigg(1/2\Big(\big((\sigma+1)(\gamma+1)\rho_m\big)/\big((\sigma+1)(\gamma+1)\alpha_m\big)\Big)\bigg) = e_0 - s$. Then we may assume without loss of generality that $\alpha_{m+(e_0-s)} = 1/2\Big(\big((\sigma+1)(\gamma+1)\rho_m\big)/\big((\sigma+1)(\gamma+1)\alpha_m\big)\Big) \cdot \alpha_m$. Therefore $(\sigma+1)\rho_m = 2(\gamma+1)\alpha_{m+(e_0-s)}$.

Then for each m in (3.80) we can replace the four elements: β_m, $(\sigma+1)\alpha_m$, $2\alpha_m$, $2(\gamma+1)\alpha_m$; by $(\sigma+1)\alpha_m$, $\gamma(\sigma+1)\alpha_m$ and β_m, $(\sigma+1)\alpha_m - 2\alpha_m$. We can also replace the four elements in (3.81): ρ_m, $(\sigma+1)\alpha_m$, $2\alpha_m$, $2(\gamma+1)\alpha_m$; by $(\sigma+1)\alpha_m$, $\gamma(\sigma+1)\alpha_m$ and ρ_m, $(\sigma+1)\alpha_m - 2\alpha_m$. For $\lceil (i+s-2)/4 \rceil \leq m \leq \lceil (i+2s-2)/4 \rceil - 1$, we group the four elements: $(\sigma+1)\alpha_{m+(e_0-s)}$, $\gamma(\sigma+1)\alpha_{m+(e_0-s)}$, ρ_m, $(\sigma+1)\alpha_m - 2\alpha_m$, together. This leaves the elements $(\sigma+1)\alpha_m$, $\gamma(\sigma+1)\alpha_m$ for $\lceil (i+s-2)/4 \rceil \leq m \leq \lceil (i+s-2)/4 \rceil + (e_0 - s)$, and β_m, $(\sigma+1)\alpha_m - 2\alpha_m$ for $\lceil (i+2s-2)/4 \rceil \leq m \leq e_0 + \lceil (i-2s-2)/4 \rceil - 1$. All this is collected in the revised basis:

CASE 2, $s < e_0$ (REVISED). The following elements comprise an $\mathfrak{O}_T$-basis of $\mathfrak{P}_N^i$:

$$\alpha_m,\ (\gamma+1)\alpha_m,\ \beta_m,\ (\sigma+1)\alpha_m \quad \text{for } e_0 + \left\lceil \frac{i-s-2}{4} \right\rceil \leq m \leq e_0 + \left\lceil \frac{i-2}{4} \right\rceil - 1 \tag{3.83}$$

https://doi.org/10.4153/CJM-1998-050-4 Published online by Cambridge University Press

$$(\gamma+1)\alpha_m,\ \beta_m,\ (\sigma+1)\alpha_m,\ 2\alpha_m \quad \text{for } e_0+\left\lceil\frac{i-2s-2}{4}\right\rceil \le m \le e_0+\left\lceil\frac{i-s-2}{4}\right\rceil-1 \tag{3.84}$$

$$\beta_m,\ (\sigma+1)\alpha_m-2\alpha_m, \quad \text{for } \left\lceil\frac{i+2s-2}{4}\right\rceil \le m \le e_0+\left\lceil\frac{i-2s-2}{4}\right\rceil-1 \tag{3.85}$$

$$(\sigma+1)\alpha_{m+(e_0-s)},\ \gamma(\sigma+1)\alpha_{m+(e_0-s)},\ \rho_m,\ (\sigma+1)\alpha_m-2\alpha_m, \quad \text{for } \left\lceil\frac{i+s-2}{4}\right\rceil \le m \le \left\lceil\frac{i+2s-2}{4}\right\rceil-1 \tag{3.86}$$

$$(\sigma+1)\alpha_m,\ \gamma(\sigma+1)\alpha_m, \quad \text{for } \left\lceil\frac{i+s-2}{4}\right\rceil \le m \le \left\lceil\frac{i+s-2}{4}\right\rceil+(e_0-s)-1 \tag{3.87}$$

$$(\sigma+1)\alpha_m,\ 2\alpha_m,\ 2(\gamma+1)\alpha_m,\ 2\beta_m \quad \text{for } \left\lceil\frac{i-2}{4}\right\rceil \le m \le \left\lceil\frac{i+s-2}{4}\right\rceil-1 \tag{3.88}$$

One may easily check at this point that each m in (3.83) yields f copies of $\hat{B}$, each m in (3.84) yields f copies of $\hat{Z}\oplus\hat{R}_\sigma\oplus\hat{E}_-$, each m in (3.85) yields f copies of $\hat{E}_-$, each m in (3.86) yields f copies of $\hat{A}$, each m in (3.87) yields f copies of $\hat{E}_+$, while each m in (3.88) yields f copies of $\hat{E}_+\oplus R_\gamma\oplus R_{\sigma\gamma}$. This has been collected into the statement of Theorem 3.9.

REMARK 3.23. Note that the condition $8e_0 > 5s$ is not equivalent to $k'=1$. If $8e_0 > 5s$, nor is the natural condition $3s < 4e_0$ identical with the condition stated in Theorem 3.9 for $l = m-1$. This complication is similar to the complication dealt with in Remark 3.18. As one may check, when a discrepancy arises the exponents given in the theorem for the modules involved are zero, while the modules do not actually appear in our description here. For instance, when $8e_0 > 5s$ and $k'=2$, then $a=b=0$ while I_0, L_0, are listed with zero occurrence.

CASE 2-EVEN, $s = e_0$. If however, $s=e_0$, then we may not replace any ρ_m in (3.72) by a β_m, while all ρ_m's in (3.71) may be replaced. We are therefore principally concerned with the $\mathbb{Z}_2[G]$-structure arising from the four elements listed in (3.71). As in the case $s<e_0$, for each m in $\lceil(i+s-2)/4\rceil \le m \le e_0+\lceil(i-2s-2)/4\rceil-1$, let $\tau'_m = 1/2\Big(\big((\sigma+1)(\gamma+1)\rho_m\big)/\big((\sigma+1)(\gamma+1)\alpha_m\big)\Big)\cdot\tau_m$. Then define $\alpha'_m = 1/2\Big(\big((\sigma+1)(\gamma+1)\rho_m\big)/\big((\sigma+1)(\gamma+1)\alpha_m\big)\Big)\cdot\alpha_m$. Therefore $(\sigma+1)\rho_m = 2(\gamma+1)\alpha'_m$. Now replace $(\sigma+1)\alpha_m$ and $2(\gamma+1)\alpha_m$ with $(\sigma+1)\alpha'_m$ and $2(\gamma+1)\alpha'_m$. By Remark 3.16, we may replace $2\alpha_m$ with $(\sigma+1)\alpha_m-2\alpha_m$. Observe that we now have copies of $(\sigma+1)\alpha'_m$, $\gamma(\sigma+1)\alpha'_m$, ρ_m, $(\sigma+1)\alpha_m-2\alpha_m$ in (3.71) which give rise to $\hat{A}$'s. Otherwise everything else is the same as when $s<e_0$, and the theorem results.

CASE 2-EVEN, $3e_0 < 3s < 4e_0$. In this case, we may not replace any ρ_m in (3.72) by a β_m, while certain ρ_m's in (3.71) may be replaced. We separate (3.71) into two cases.

https://doi.org/10.4153/CJM-1998-050-4 Published online by Cambridge University Press

The following elements comprise an $\mathfrak{O}_T$-basis of $\mathfrak{P}_N^i$:

$$\alpha_m,\ (\gamma+1)\alpha_m,\ \beta_m,\ (\sigma+1)\alpha_m \quad \text{for } e_0+\left\lceil\frac{i-s-2}{4}\right\rceil \le m \le e_0+\left\lceil\frac{i-2}{4}\right\rceil-1 \tag{3.89}$$

$$(\gamma+1)\alpha_m,\ \beta_m,\ (\sigma+1)\alpha_m,\ 2\alpha_m \quad \text{for } \left\lceil\frac{i+2s-2}{4}\right\rceil \le m \le e_0+\left\lceil\frac{i-s-2}{4}\right\rceil-1 \tag{3.90}$$

$$(\gamma+1)\alpha_m,\ \rho_m,\ (\sigma+1)\alpha_m,\ 2\alpha_m \quad \text{for } e_0+\left\lceil\frac{i-2s-2}{4}\right\rceil \le m \le \left\lceil\frac{i+2s-2}{4}\right\rceil-1 \tag{3.91}$$

$$\rho_m,\ (\sigma+1)\alpha_m,\ 2\alpha_m,\ 2(\gamma+1)\alpha_m \quad \text{for } \left\lceil\frac{i+s-2}{4}\right\rceil \le m \le e_0+\left\lceil\frac{i-2s-2}{4}\right\rceil-1 \tag{3.92}$$

$$(\sigma+1)\alpha_m,\ 2\alpha_m,\ 2(\gamma+1)\alpha_m,\ 2\beta_m \quad \text{for } \left\lceil\frac{i-2}{4}\right\rceil \le m \le \left\lceil\frac{i+s-2}{4}\right\rceil-1 \tag{3.93}$$

In this case, we begin by assuming that the α_m, ρ_m have been defined for $e_0 + \lceil(i-2s-2)/4\rceil \le m \le \lceil(i+2s-2)/4\rceil - 1$. Then as when $s < e_0$, define $\tau_{m-(s-e_0)} = 1/2\Big(\big((\sigma+1)(\gamma+1)\rho_m\big)/\big((\sigma+1)(\gamma+1)\alpha_m\big)\Big)\cdot\tau_m$. Then we may assume without loss of generality that $\alpha_{m-(s-e_0)} = 1/2\Big(\big((\sigma+1)(\gamma+1)\rho_m\big)/\big((\sigma+1)(\gamma+1)\alpha_m\big)\Big)\cdot\alpha_m$. Therefore $(\sigma+1)\rho_m = 2(\gamma+1)\alpha_{m-(s-e_0)}$.

Because $3s < 4e_0$, $\lceil(i+s-2)/4\rceil - (s-e_0) \ge \lceil(i-2)/4\rceil$, and so the following elements comprise an $\mathfrak{O}_T$-basis of $\mathfrak{P}_N^i$:

$$\alpha_m,\ (\gamma+1)\alpha_m,\ \beta_m,\ (\sigma+1)\alpha_m \quad \text{for } e_0+\left\lceil\frac{i-s-2}{4}\right\rceil \le m \le e_0+\left\lceil\frac{i-2}{4}\right\rceil-1 \tag{3.94}$$

$$(\gamma+1)\alpha_m,\ \beta_m,\ (\sigma+1)\alpha_m,\ 2\alpha_m \quad \text{for } \left\lceil\frac{i+2s-2}{4}\right\rceil \le m \le e_0+\left\lceil\frac{i-s-2}{4}\right\rceil-1 \tag{3.95}$$

$$(\gamma+1)\alpha_m,\ (\sigma+1)\alpha_m, \quad \text{for } e_0+\left\lceil\frac{i-2s-2}{4}\right\rceil \le m \le \left\lceil\frac{i+2s-2}{4}\right\rceil-1 \tag{3.96}$$

$$(\sigma+1)\alpha_{m-(s-e_0)},\ 2(\gamma+1)\alpha_{m-(s-e_0)},\ \rho_m,\ (\sigma+1)\alpha_m-2\alpha_m \quad \text{for } \left\lceil\frac{i+s-2}{4}\right\rceil \le m \le \left\lceil\frac{i+2s-2}{4}\right\rceil-1 \tag{3.97}$$

$$(\sigma+1)\alpha_m,\ 2(\gamma+1)\alpha_m, \quad \text{for } \left\lceil\frac{i-2}{4}\right\rceil \le m \le \left\lceil\frac{i+s-2}{4}\right\rceil-(s-e_0)-1 \tag{3.98}$$

$$2\alpha_m-2\beta_m-(\sigma+1)\alpha_m,\ 2\beta_m-(\sigma+1)\alpha_m \quad \text{for } \left\lceil\frac{i-2}{4}\right\rceil \le m \le \left\lceil\frac{i+s-2}{4}\right\rceil-1 \tag{3.99}$$

https://doi.org/10.4153/CJM-1998-050-4 Published online by Cambridge University Press

One may easily check that each m in (3.94) yields f copies of $\hat{B}$, while each m in (3.95) yields f copies of $\hat{Z} \oplus \hat{R}_\sigma \oplus \hat{E}_-$, each m in (3.96) yields f copies of $\hat{Z} \oplus \hat{R}_\sigma$, each m in (3.97) yields f copies of $\hat{A}$, each m in (3.98) yields f copies of $\hat{E}_+$, while each m in (3.99) yields f copies of $\hat{R}_\gamma \oplus \hat{R}_{\sigma\gamma}$. Because of Remark 3.23, this is consistent with Theorem 3.9.

CASE 2-EVEN, $3s > 4e_0$. In this case, one may easily check that for each $2\rho_m$ in (3.77), $v_N\big((\sigma+1)\rho_m\big) \geq i$, therefore we replace $2\rho_m$ by $2\beta_m$. One also easily sees that we may replace every ρ_m in (3.74) by a β_m, and that we may not replace any ρ_m in (3.76). Not every ρ_m in (3.75) may be replaced. Therefore we separate (3.75) into two cases depending on whether or not $v_N\Big(\big((\sigma+1)/2\big)\rho_m\Big) \geq i$.

The following elements comprise an $\mathfrak{O}_T$-basis of $\mathfrak{P}_N^i$:

$$\frac{1}{2}(\sigma+1)\alpha_m,\ \alpha_m,\ \beta_m,\ (\gamma+1)\alpha_m \quad \text{for } e_0 + \left\lceil \frac{i-2}{4} \right\rceil \leq m \leq 2e_0 + \left\lceil \frac{i-2s-2}{4} \right\rceil - 1 \tag{3.100}$$

$$\alpha_m,\ \beta_m,\ (\gamma+1)\alpha_m,\ (\sigma+1)\alpha_m \quad \text{for } \left\lceil \frac{i+2s-2}{4} \right\rceil \leq m \leq e_0 + \left\lceil \frac{i-2}{4} \right\rceil - 1 \tag{3.101}$$

$$\alpha_m,\ \rho_m,\ (\gamma+1)\alpha_m,\ (\sigma+1)\alpha_m \quad \text{for } e_0 + \left\lceil \frac{i-s-2}{4} \right\rceil \leq m \leq \left\lceil \frac{i+2s-2}{4} \right\rceil - 1 \tag{3.102}$$

$$\rho_m,\ (\gamma+1)\alpha_m,\ (\sigma+1)\alpha_m,\ 2\alpha_m \quad \text{for } \left\lceil \frac{i+s-2}{4} \right\rceil \leq m \leq e_0 + \left\lceil \frac{i-s-2}{4} \right\rceil - 1 \tag{3.103}$$

$$(\gamma+1)\alpha_m,\ (\sigma+1)\alpha_m,\ 2\alpha_m,\ 2\beta_m \quad \text{for } e_0 + \left\lceil \frac{i-2s-2}{4} \right\rceil \leq m \leq \left\lceil \frac{i+s-2}{4} \right\rceil - 1 \tag{3.104}$$

CASE 2-EVEN, $6s > 8e_0 > 5s$. In this case, $e_0 + \lceil (i-s-2)/4 \rceil + (2e_0 - s) \geq e_0 + \lceil (i-2)/4 \rceil$, and $\lceil (i+s-2)/4 \rceil + (2e_0 - s) \geq \lceil (i+2s-2)/4 \rceil$, while $\lceil (i+2s-2)/4 \rceil + (2e_0 - s) = 2e_0 + \lceil (i-2s-2)/4 \rceil$. We now redefine the elements α_m and β_m for $\lceil (i+s-2)/4 \rceil + (2e_0 - s) \leq m \leq 2e_0 + \lceil (i-2s-2)/4 \rceil - 1$. Given any m such that $\lceil (i+s-2)/4 \rceil \leq m \leq \lceil (i+2s-2)/4 \rceil - 1$, define $\tau_{m+(2e_0-s)} = \Big(\big((\sigma+1)(\gamma+1)\rho_m\big) / \big((\sigma+1)(\gamma+1)\alpha_m\big)\Big) \cdot \tau_m$, so that $(\sigma+1)\rho_m = (\gamma+1)\alpha_{m+(2e_0-s)}$.

As a consequence we have the following $\mathfrak{O}_T$-basis for $\mathfrak{P}_N^i$.

$$\begin{gathered} \alpha_m,\ \rho_m,\ (\gamma+1)\alpha_m,\ (\sigma+1)\alpha_m \\ 1/2(\sigma+1)\alpha_{m+(2e_0-s)},\ \alpha_{m+(2e_0-s)},\ \beta_{m+(2e_0-s)},\ (\gamma+1)\alpha_{m+(2e_0-s)} \\ \text{where } (\sigma+1)\rho_m = (\gamma+1)\alpha_{m+(2e_0-s)}, \\ \text{for } e_0 + \left\lceil \frac{i-s-2}{4} \right\rceil \leq m \leq \left\lceil \frac{i+2s-2}{4} \right\rceil - 1 \end{gathered} \tag{3.105}$$

$$\rho_m,\ (\gamma+1)\alpha_m,\ (\sigma+1)\alpha_m,\ 2\alpha_m, \tag{3.106}$$

https://doi.org/10.4153/CJM-1998-050-4 Published online by Cambridge University Press

$$1/2(\sigma+1)\alpha_{m+(2e_0-s)},\ \alpha_{m+(2e_0-s)},\ \beta_{m+(2e_0-s)},\ (\gamma+1)\alpha_{m+(2e_0-s)}$$
$$\text{where } (\sigma+1)\rho_m=(\gamma+1)\alpha_{m+(2e_0-s)},$$
$$\text{for } e_0+\left\lceil\frac{i-2}{4}\right\rceil-(2e_0-s)\le m\le e_0+\left\lceil\frac{i-s-2}{4}\right\rceil-1$$

$$\rho_m,\ (\gamma+1)\alpha_m,\ (\sigma+1)\alpha_m,\ 2\alpha_m \tag{3.107}$$
$$\alpha_{m+(2e_0-s)},\ \beta_{m+(2e_0-s)},\ (\gamma+1)\alpha_{m+(2e_0-s)},\ (\sigma+1)\alpha_{m+(2e_0-s)}$$
$$\text{where } (\sigma+1)\rho_m=(\gamma+1)\alpha_{m+(2e_0-s)},$$
$$\text{for } \left\lceil\frac{i+s-2}{4}\right\rceil\le m\le e_0+\left\lceil\frac{i-2}{4}\right\rceil-(2e_0-s)-1$$

$$\alpha_m,\ \beta_m,\ (\gamma+1)\alpha_m,\ (\sigma+1)\alpha_m \tag{3.108}$$
$$\text{for } \left\lceil\frac{i+2s-2}{4}\right\rceil\le m\le\left\lceil\frac{i+s-2}{4}\right\rceil+(2e_0-s)-1$$

$$(\gamma+1)\alpha_m,\ (\sigma+1)\alpha_m,\ 2\alpha_m,\ 2\beta_m \tag{3.109}$$
$$\text{for } e_0+\left\lceil\frac{i-2s-2}{4}\right\rceil\le m\le\left\lceil\frac{i+s-2}{4}\right\rceil-1$$

One may easily check that each m in (3.105) yields f copies of $\hat{W}\oplus\hat{R}_\gamma\oplus\hat{R}_{\sigma\gamma}$, while each m in (3.106) yields f copies of $\hat{A}\oplus\hat{M}$, each m in (3.107) yields f copies of $\hat{Y}\oplus\hat{Z}\oplus\hat{R}_\sigma$, each m in (3.108) yields f copies of $\hat{B}$, while each m in (3.109) yields f copies of $\hat{M}$. Because of Remark 3.23, this is consistent with Theorem 3.9.

CASE 2-EVEN, $5s>8e_0$. Because. as we observed earlier, $\lceil(i+2s-2)/4\rceil+(2e_0-s)=2e_0+\lceil(i-2s-2)/4\rceil$, the numbers of m's in (3.101) and (3.100) is exactly $2e_0-s$. Because $2e_0-s$ can be quite small, even as small as $2e_0-s=1$, we may have to recursively define the τ_m's many times from $m=\lceil(i+s-2)/4\rceil$ till we end up in (3.101) or (3.100). There is one complication: Although the number of m's in (3.100), (3.101) and (3.103) are approximately the same, they are not the same. The number of m's in (3.103) can be less than the number of m's in (3.100) by one, the same, or more than the number of m's in (3.100) by one.

LEMMA 3.24. *Let k be the smallest integer such that $\lceil(i+s-2)/4\rceil+k(2e_0-s)>\lceil(i+2s-2)/4\rceil$, then if $r\in\{0,1,2,3\}$ so that $r\equiv -i \bmod 4$, we have $k=\lceil(s+r+1)/4(2e_0-s)\rceil$.*

PROOF. Since s is odd, $-i\equiv-(i+2s-2)\bmod 4$. And so this lemma is easily verified, as in Lemma 3.19. ∎

Beginning with $m=\lceil(i+s-2)/4\rceil$ redefine $\tau_{m+(2e_0-s)}$ to be

$$\Big(\big((\sigma+1)(\gamma+1)\rho_m\big)/\big((\sigma+1)(\gamma+1)\alpha_m\big)\Big)\cdot\tau_m,$$

so that $(\sigma+1)\rho_m=(\gamma+1)\alpha_{m+(2e_0-s)}$. Continue until all the α_m's and ρ_m's for $\lceil(i+s-2)/4\rceil+(2e_0-s)\ge 2e_0+\lceil(i-2s-2)/4\rceil$ have been redefined. Based upon Lemma 3.24 and the preceding comments, one may verify the statement of Theorem 3.9.

4. **Index of modules.** In this section we provide explicit descriptions in terms for generators and relations of the $\mathbb{Z}[G]$-modules that appear in this paper.

In Nazarova's Classification, [16], the $\mathbb{Z}[G]$-modules are represented as pairs of matrices. Note that the proofs for the results of [16] are explained in greater detail in [17]. In Section 4.2 we translate our notation to verify the indecomposability of the our modules.

4.1. *The modules expressed in terms of generators and relations.* For each $\mathbb{Z}[G]$-module, $\mathfrak{N}$, let $\hat{\mathfrak{N}}$ denote the $\mathbb{Z}_2[G]$-module, $\mathbb{Z}_2 \otimes_{\mathbb{Z}} \mathfrak{N}$. The $\mathbb{Z}_2[G]$ action on $\hat{\mathfrak{N}}$ is the natural one, explicitly stated in Definition 2.1. For practical purposes, each $\mathbb{Z}[G]$-module becomes a $\mathbb{Z}_2[G]$-module when you replace each occurrence of a $\mathbb{Z}$ in our description with a $\mathbb{Z}_2$.

In each description of the representation as a module, the action of $\sigma \in G$ is given by multiplication by x, while $\gamma \in G$ acts via multiplication by y.

First we introduce notation for the four modules whose rank over $\mathbb{Z}$ is one.

$$Z = \frac{\mathbb{Z}[x,y]}{\langle x-1, y-1\rangle}, \quad R_\sigma = \frac{\mathbb{Z}[x,y]}{\langle x-1, y+1\rangle},$$
$$R_\gamma = \frac{\mathbb{Z}[x,y]}{\langle x+1, y-1\rangle}, \quad R_{\sigma\gamma} = \frac{\mathbb{Z}[x,y]}{\langle x+1, y+1\rangle}.$$

Clearly, Z is the module with trivial group action, while for instance both σ and γ act on $R_{\sigma\gamma}$ via multiplication by -1. Notice that $Z \oplus R_\sigma \oplus R_\gamma \oplus R_{\sigma\gamma} \cong M$, the maximal order of $\mathbb{Z}[G]$.

Next we introduce two modules whose rank over $\mathbb{Z}$ is two.

$$E_+ = \frac{\mathbb{Z}[x,y]}{\langle x-1, y^2-1\rangle}, \quad E_- = \frac{\mathbb{Z}[x,y]}{\langle x+1, y^2-1\rangle}.$$

Notice that both of these modules are free over $\mathbb{Z}[\gamma]$, while σ acts trivially upon E_+ and through multiplication by -1 on E_-.

REMARK 4.1. Since σ acts trivially upon Z, R_σ and E_+, these $\mathbb{Z}[G]$-modules may be considered $\mathbb{Z}[\langle\gamma\rangle]$-modules, which explains the notation in Theorem 3.1.

One module of rank 4 over $\mathbb{Z}$ distinguishes itself by being the group ring:

$$G = \frac{\mathbb{Z}[x,y]}{\langle x^2-1, y^2-1\rangle} \cong \mathbb{Z}[G].$$

Besides the group ring, we require four other modules of rank 4 over $\mathbb{Z}$, two of these are elements of infinite families, the other two are listed here:

$$C = \frac{\frac{\mathbb{Z}[x,y]}{\langle x^2-1, y^2-1\rangle} \oplus \frac{\mathbb{Z}[x,y]}{\langle x-1, y-1\rangle} \oplus \frac{\mathbb{Z}[x,y]}{\langle x-1, y+1\rangle}}{\langle (x+1, 1, 1)\rangle},$$
$$D = \frac{\frac{\mathbb{Z}[x,y]}{\langle x^2-1, y-1\rangle} \oplus \frac{\mathbb{Z}[x,y]}{\langle x^2-1, y+1\rangle} \oplus \frac{\mathbb{Z}[x,y]}{\langle x-1, y^2-1\rangle}}{\langle (x+1, 0, y+1), (0, x+1, y-1)\rangle}.$$

https://doi.org/10.4153/CJM-1998-050-4 Published online by Cambridge University Press

Finally to complete the list of indecomposable $\mathbb{Z}[G]$-modules which we require, we construct five different infinite families of $\mathbb{Z}[G]$-modules: $\{H_j\}$, $\{I_j\}$, $\{J_j\}$, $\{K_j\}$, $\{L_j\}$.

REMARK 4.2. In the next section, we show that the H_j decompose. Because these modules arise naturally in the proof of Theorem 3.6, they are included along with these other families of indecomposable modules.

THE INFINITE FAMILY OF H_j'S. We construct the H_j's $j \geq 1$, where the $\mathbb{Z}$-rank of H_j is $4j + 8$. To define H_j, we introduce $\Omega(H)_j$ and its submodule, $\Lambda(H)_j$. Each H_j is then defined to be the quotient of $\Omega(H)_j$ by $\Lambda(H)_j$. Let

$$\begin{aligned}\Omega(H)_j = &\left(\frac{\mathbb{Z}[x,y]}{\langle x^2-1, y^2-1\rangle} \oplus \frac{\mathbb{Z}[x,y]}{\langle x^2-1, y^2-1\rangle} \oplus \frac{\mathbb{Z}[x,y]}{\langle x-1, y^2-1\rangle}\right)c \\ &+ \sum_{i=1}^{j}\left(\frac{\mathbb{Z}[x,y]}{\langle x^2-1, y^2-1\rangle} \oplus \frac{\mathbb{Z}[x,y]}{\langle x^2-1, y^2-1\rangle}\right. \\ &\left.\oplus \frac{\mathbb{Z}[x,y]}{\langle x-1, y-1\rangle} \oplus \frac{\mathbb{Z}[x,y]}{\langle x-1, y+1\rangle}\right)b_i \\ &+ \left(\frac{\mathbb{Z}[x,y]}{\langle x^2-1, y^2-1\rangle} \oplus \frac{\mathbb{Z}[x,y]}{\langle x-1, y-1\rangle} \oplus \frac{\mathbb{Z}[x,y]}{\langle x-1, y+1\rangle}\right)b_0.\end{aligned}$$

Let $\Lambda(H)_j$ be the submodule of $\Omega(H)_j$ generated by the following elements:

$$\begin{gathered}(x+1, 0, y+1)c + (0,0,1,1)b_j, \quad (y-1,0,0)c + (0,0,0,1)b_j, \\ (0, x+1, y-1)c + (0,0,1,1)b_j, \quad (0, y+1, 0)c + (0,0,1,0)b_j, \quad \text{and} \\ (x+1,0,1,0)b_i + (0,0,1,1)b_{i-1}, \quad (y-1,0,0,0)b_i + (0,0,0,1)b_{i-1}, \\ (0, x+1, 0, 1)b_i + (0,0,1,1)b_{i-1}, \quad (0, y+1, 0, 0)b_i + (0,0,1,0)b_{i-1}, \\ \text{for each } i = j, j-1, j-2, \ldots, 3, 2, \quad \text{and} \\ (x+1, 0, 1, 0)b_1 + (0,1,1)b_0, \quad (y-1,0,0,0)b_1 + (0,0,1)b_0, \\ (0, x+1, 0, 1)b_1 + (0,1,1)b_0, \quad (0, y+1, 0, 0)b_1 + (0,1,0)b_0, \\ \text{and finally } (x+1,1,1)b_0.\end{gathered}$$

Then, we define

$$H_j = \frac{\Omega(H)_j}{\Lambda(H)_j}.$$

Consistent with this definition is the next module which has $\mathbb{Z}$-rank eight.

$$H_0 = \frac{\frac{\mathbb{Z}[x,y]}{\langle x^2-1,y^2-1\rangle} \oplus \frac{\mathbb{Z}[x,y]}{\langle x^2-1,y^2-1\rangle} \oplus \frac{\mathbb{Z}[x,y]}{\langle x-1,y^2-1\rangle} \oplus \frac{\mathbb{Z}[x,y]}{\langle x^2-1,y^2-1\rangle} \oplus \frac{\mathbb{Z}[x,y]}{\langle x-1,y-1\rangle} \oplus \frac{\mathbb{Z}[x,y]}{\langle x-1,y+1\rangle}}{\langle (x+1,0,y+1,0,1,1),(y-1,0,0,0,0,1),(0,x+1,y-1,0,1,1),(0,y-1,0,0,1,0),(0,0,0,x+1,1,1)\rangle}.$$

Finally to simplify the statements in our theorems, define $H_{-1} = E_+ \oplus E_-$.

THE INFINITE FAMILY OF I_j'S. We construct the I_j's $j \geq 1$, where the $\mathbb{Z}$-rank of I_j is $4j+4$. Let

$$\Omega(I)_j = \sum_{i=0}^{j}\Big(\frac{\mathbb{Z}[x,y]}{\langle x^2-1, y^2-1\rangle} \oplus \frac{\mathbb{Z}[x,y]}{\langle x^2-1, y^2-1\rangle} \oplus \frac{\mathbb{Z}[x,y]}{\langle x-1, y-1\rangle} \oplus \frac{\mathbb{Z}[x,y]}{\langle x-1, y+1\rangle}\Big) b_i$$

Let $\Lambda(I)_j$ be the submodule of $\Omega(I)_j$ generated by the following elements:

$$(x+1,0,-1,-1)b_i, \quad (y+1,0,-1,0)b_i, \quad (0,y-1,0,-1)b_i,$$
$$(0,x+1,1,1)b_i + (0,0,1,0)b_{i-1}, \quad \text{for each } i = j, j-1, j-2, \ldots, 3, 2, 1, \quad \text{and}$$
$$(x+1,0,-1,-1)b_0, \quad (y+1,0,-1,0)b_0, (0,x+1,1,1)b_0, \quad (0,y-1,0,-1)b_0,$$

Then, we define

$$I_j = \frac{\Omega(I)_j}{\Lambda(I)_j}.$$

Consistent with this formulation is the rank 4 module,

$$I_0 \cong B = \frac{\frac{\mathbb{Z}[x,y]}{\langle x^2-1,y^2-1\rangle} \oplus \frac{\mathbb{Z}[x,y]}{\langle x^2-1,y^2-1\rangle} \oplus \frac{\mathbb{Z}[x,y]}{\langle x-1,y-1\rangle} \oplus \frac{\mathbb{Z}[x,y]}{\langle x-1,y+1\rangle}}{\langle (x+1,0,1,-1), (0,x+1,1,-1), (y-1,0,0,1), (0,y+1,1,0)\rangle}.$$

The next three families are extensions of I_j.

THE INFINITE FAMILY OF J_j'S. We construct the J_j's, $j \geq 1$, where the $\mathbb{Z}$-rank of J_j is $4j+2$. Let

$$\Omega(J)_j = \sum_{i=1}^{j}\Big(\frac{\mathbb{Z}[x,y]}{\langle x^2-1, y^2-1\rangle} \oplus \frac{\mathbb{Z}[x,y]}{\langle x^2-1, y^2-1\rangle} \oplus \frac{\mathbb{Z}[x,y]}{\langle x-1, y-1\rangle} \oplus \frac{\mathbb{Z}[x,y]}{\langle x-1, y+1\rangle}\Big) b_i + \Big(\frac{\mathbb{Z}[x,y]}{\langle x-1, y^2-1\rangle}\Big) b_0.$$

Let $\Lambda(J)_j$ be the submodule of $\Omega(J)_j$ generated by the following elements:

$$(x+1,0,-1,-1)b_i, \quad (y+1,0,-1,0)b_i, \quad (0,y-1,0,-1)b_i,$$
$$(0,x+1,1,1)b_i + (0,0,1,0)b_{i-1}, \quad \text{for each } i = j, j-1, j-2, \ldots, 3, 2, \quad \text{and}$$
$$(x+1,0,-1,-1)b_1, \quad (y+1,0,-1,0)b_1, \quad (0,y-1,0,-1)b_1,$$
$$(0,x+1,1,1)b_1 + (y+1)b_0.$$

Then, we define

$$J_j = \frac{\Omega(J)_j}{\Lambda(J)_j}.$$

Consistent with this definition is the rank 6 module,

$$J_1 \cong W = \frac{\frac{\mathbb{Z}[x,y]}{\langle x^2-1,y^2-1\rangle} \oplus \frac{\mathbb{Z}[x,y]}{\langle x^2-1,y^2-1\rangle} \oplus \frac{\mathbb{Z}[x,y]}{\langle x-1,y-1\rangle} \oplus \frac{\mathbb{Z}[x,y]}{\langle x-1,y+1\rangle} \oplus \frac{\mathbb{Z}[x,y]}{\langle x-1,y^2-1\rangle}}{\langle (x+1,0,1,-1,y+1), (0,x+1,1,-1,0), (y-1,0,0,1,0), (0,y+1,1,0,0)\rangle},$$

as well as the rank 2 module, $J_0 \cong E_+$.

THE INFINITE FAMILY OF K_j'S. We construct the K_j's $j \geq 1$, where the $\mathbb{Z}$-rank of K_j is $4j + 6$. Let

$$\Omega(K)_j = \left(\frac{\mathbb{Z}[x,y]}{\langle x^2-1, y^2-1\rangle}\right)c + \sum_{i=0}^{j}\left(\frac{\mathbb{Z}[x,y]}{\langle x^2-1, y^2-1\rangle} \oplus \frac{\mathbb{Z}[x,y]}{\langle x^2-1, y^2-1\rangle} \oplus \frac{\mathbb{Z}[x,y]}{\langle x-1, y-1\rangle} \oplus \frac{\mathbb{Z}[x,y]}{\langle x-1, y+1\rangle}\right)b_i.$$

Let $\Lambda(K)_j$ be the submodule of $\Omega(K)_j$ generated by the following elements:

$$\begin{gathered}
(x+1)c + (0,0,1,0)b_j \quad \text{and} \\
(x+1,0,-1,-1)b_i, \quad (y+1,0,-1,0)b_i, \quad (0,y-1,0,-1)b_i, \\
(0,x+1,1,1)b_i + (0,0,1,0)b_{i-1}, \quad \text{for each } i = j, j-1, j-2, \ldots, 3, 2, 1, \quad \text{and} \\
(x+1,0,-1,-1)b_0, \quad (y+1,0,-1,0)b_0, (0,x+1,1,1)b_0, \quad (0,y-1,0,-1)b_0, \\
K_j = \frac{\Omega(K)_j}{\Lambda(K)_j}.
\end{gathered}$$

Consistent with this definition is the following rank 6 module:

$$K_0 \cong Y = \frac{\frac{\mathbb{Z}[x,y]}{\langle x^2-1,y^2-1\rangle} \oplus \frac{\mathbb{Z}[x,y]}{\langle x^2-1,y^2-1\rangle} \oplus \frac{\mathbb{Z}[x,y]}{\langle x^2-1,y^2-1\rangle} \oplus \frac{\mathbb{Z}[x,y]}{\langle x-1,y-1\rangle} \oplus \frac{\mathbb{Z}[x,y]}{\langle x-1,y+1\rangle}}{\langle (x+1,0,0,1,0),(0,x+1,0,1,-1),(0,0,x+1,1,-1),(0,y-1,0,0,1),(0,0,y+1,1,0)\rangle},$$

as well as the rank 2 module, $K_{-1} \cong E_-$.

THE INFINITE FAMILY OF L_j'S. We construct the L_j's $j \geq 1$, where the $\mathbb{Z}$-rank of L_j is $4j + 4$. Let

$$\begin{aligned}
\Omega(L)_j = \left(\frac{\mathbb{Z}[x,y]}{\langle x^2-1, y^2-1\rangle}\right)c + \left(\frac{\mathbb{Z}[x,y]}{\langle x-1, y^2-1\rangle}\right)b_0 \\
+ \sum_{i=1}^{j}\left(\frac{\mathbb{Z}[x,y]}{\langle x^2-1, y^2-1\rangle} \oplus \frac{\mathbb{Z}[x,y]}{\langle x^2-1, y^2-1\rangle}\right. \\
\left. \oplus \frac{\mathbb{Z}[x,y]}{\langle x-1, y-1\rangle} \oplus \frac{\mathbb{Z}[x,y]}{\langle x-1, y+1\rangle}\right)b_i
\end{aligned}$$

Let $\Lambda(L)_j$ be the submodule of $\Omega(L)_j$ generated by the following elements:

$$\begin{gathered}
(x+1)c + (0,0,1,0)b_j \quad \text{and} \\
(x+1,0,-1,-1)b_i, \quad (y+1,0,-1,0)b_i, \quad (0,y-1,0,-1)b_i, \\
(0,x+1,1,1)b_i + (0,0,1,0)b_{i-1}, \quad \text{for each } i = j, j-1, j-2, \ldots, 3, 2, \quad \text{and} \\
(x+1,0,-1,-1)b_1, \quad (y+1,0,-1,0)b_1, \quad (0,y-1,0,-1)b_1, \\
(0,x+1,1,1)b_1 + (y+1)b_0,
\end{gathered}$$

Then, we define

$$L_j = \frac{\Omega(L)_j}{\Lambda(L)_j}.$$

Consistent with this formulation is the following rank 4 module:

$$L_0 \cong A = \frac{\frac{\mathbb{Z}[x,y]}{\langle x^2-1,y^2-1\rangle} \oplus \frac{\mathbb{Z}[x,y]}{\langle x-1,y^2-1\rangle}}{\big\langle (x+1,y+1)\big\rangle}.$$

4.2. *Nazarova's notation and the indecomposability of the modules.* To be consistent with the notation in Nazarova's paper [16], we describe each infinite family of modules in terms of a matrix for the action of γ, and another matrix for the action of $\sigma\gamma$.

For each module, Nazarova [16] supplements the kernel of $\sigma\gamma - \gamma$ to obtain a basis for the entire module. Then the matrices representing the action of γ and $\sigma\gamma$ have the form:

$$\gamma = \left(\begin{array}{c||c} A_{11} & A_{12} \\ \hline 0 & A_{22} \end{array}\right) \qquad \sigma\gamma = \left(\begin{array}{c||c} A_{11} & B_{12} \\ \hline 0 & -A_{22} \end{array}\right).$$

Using what is known about representations of the cyclic group of order two, Nazarova decomposes A_{11} and A_{22} into indecomposable boxes. Let I denote the identity matrix and E be a matrix with copies of the regular representation of $\mathbb{Z}[\gamma]$ along the diagonal. One may easily verify that the matrices have the following form.

$$\gamma = \left(\begin{array}{c|c|c||c|c|c} I & 0 & 0 & 0 & A_{15} & A_{16} \\ \hline 0 & -I & 0 & A_{24} & 0 & A_{26} \\ \hline 0 & 0 & E & A_{34} & A_{35} & 0 \\ \hline\hline 0 & 0 & 0 & I & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & -I & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & E \end{array}\right)$$

$$\sigma\gamma = \left(\begin{array}{c|c|c||c|c|c} I & 0 & 0 & B_{14} & 0 & B_{16} \\ \hline 0 & -I & 0 & 0 & B_{25} & B_{26} \\ \hline 0 & 0 & E & B_{34} & B_{35} & 0 \\ \hline\hline 0 & 0 & 0 & -I & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & I & 0 \\ \hline 0 & 0 & 0 & 0 & 0 & -E \end{array}\right)$$

In what follows we provide a translation into Nazarova's Classification. Let M denote a square matrix with ones on the diagonal and just above the diagonal, zeroes everywhere else. Let N denote a matrix with two rows and zeroes everywhere except for the first column which contains ones. Let N^t be the transpose of N.

Each module $\mathcal{I}_j$ $j \geq 1$ which is given in Section 4.1 corresponds to a pair of matrices with $B_{14} = M$ and $B_{25} = A_{15} = A_{24} = I$ rank $j+1$, and where A_{16}, A_{26} A_{31}, A_{32} B_{16}, B_{26} B_{31}, B_{32} do not appear. Each module $\mathcal{J}_j$ $j \geq 1$ corresponds to a pair of matrices with $B_{14} = M$ and $B_{25} = A_{15} = A_{24} = I$ rank j, $B_{31} = N$, $B_{32} = A_{31} = A_{32} = 0$, and where A_{16}, A_{26} B_{16}, B_{26} do not appear. Each module $\mathcal{K}_j$ $j \geq 1$ corresponds to a pair of matrices with $B_{14} = M$ and $B_{25} = A_{15} = A_{24} = I$ rank $j+1$, $B_{16} = N^t$, $B_{26} = A_{16} = A_{26} = 0$, and where A_{31}, A_{32} B_{31}, B_{32} do not appear. Each module $\mathcal{L}_j$ $j \geq 1$ corresponds to a pair of matrices with $B_{14} = M$ and $B_{25} = A_{15} = A_{24} = I$ rank j, $B_{16} = N^t$, $B_{26} = A_{16} = A_{26} = 0$, and $B_{31} = N$, $B_{32} = A_{31} = A_{32} = 0$.

The I_j are listed in [16, p. 1306 middle of page], and in [17, p. 1310, Lemma 1'] as J^{4n} for $n = j + 1$. The J_j, K_j, L_j are listed near the bottom of the page in [16, p. 1307], and respectively as $J^{4n}(e)$ for $n = j$, $J^{4n}(f)$ for $n = j+1$, $J^{4n}(e, f)$ for $n = j$, in [17, p. 1312, Corollary]. They are all proven to be indecomposable in [17, Section 5]. One may check following [17, p. 1316, Lemma 5] that the H_j decompose. We include an brief proof for the benefit of the reader.

PROPOSITION 4.3. *The modules H_j decompose in the following manner,*

$$H_j \cong \begin{cases} L_{j/2} \oplus I_{j/2} & \text{if } j \text{ is even,} \\ J_{(j+1)/2} \oplus K_{(j-1)/2} & \text{if } j \text{ is odd.} \end{cases}$$

PROOF. Take the basis for H_k given in (3.66) and replace it with the following two sets:

$$\begin{gathered} (\sigma+1)\alpha_m, \quad (\gamma+1)(\sigma+1)\alpha_m \\ (\gamma-1)(\sigma+1)\alpha_{f(m,1)} + 2(\sigma+1)\alpha_{f(m,2)}, \quad (\gamma+1)(\sigma+1)\alpha_{f(m,2)}, \\ (\gamma-1)\alpha_{f(m,1)} + (\sigma+1)\alpha_{f(m,2)}, \quad (\gamma+1)\alpha_m + (\sigma-1)\alpha_{f(m,1)} \\ (\gamma-1)(\sigma+1)\alpha_{f(m,3)} + 2(\sigma+1)\alpha_{f(m,4)}, \quad (\gamma+1)(\sigma+1)\alpha_{f(m,4)}, \\ (\gamma-1)\alpha_{f(m,3)} + (\sigma+1)\alpha_{f(m,4)}, \quad (\gamma+1)\alpha_{f(m,2)} + (\sigma-1)\alpha_{f(m,3)} \\ \vdots \end{gathered} \tag{4.1}$$

and

$$\begin{gathered} (\gamma-1)(\sigma+1)\alpha_m + 2(\sigma+1)\alpha_{f(m,1)}, \quad (\gamma+1)(\sigma+1)\alpha_{f(m,1)}, \\ (\gamma-1)\alpha_m + (\sigma+1)\alpha_{f(m,1)}, \quad (\sigma-1)\alpha_m \\ (\gamma-1)(\sigma+1)\alpha_{f(m,2)} + 2(\sigma+1)\alpha_{f(m,3)}, \quad (\gamma+1)(\sigma+1)\alpha_{f(m,3)}, \\ (\gamma-1)\alpha_{f(m,2)} + (\sigma+1)\alpha_{f(m,3)}, \quad (\gamma+1)\alpha_{f(m,1)} + (\sigma-1)\alpha_{f(m,2)} \\ (\gamma-1)(\sigma+1)\alpha_{f(m,4)} + 2(\sigma+1)\alpha_{f(m,5)}, \quad (\gamma+1)(\sigma+1)\alpha_{f(m,5)}, \\ (\gamma-1)\alpha_{f(m,4)} + (\sigma+1)\alpha_{f(m,5)}, \quad (\gamma+1)\alpha_{f(m,3)} + (\sigma-1)\alpha_{f(m,4)} \\ \vdots \end{gathered} \tag{4.2}$$

Note that in each set the i in the $f(m, i)$ is incremented by 2 each time. How each set ends depends upon whether k is even or odd. Hence the result. ∎

5. **Examples.** In this section we provide the family of biquadratic extensions alluded to in Section 3.4.2. The existence of fully ramified bicyclic extensions, N/K, with the property that $\mathfrak{P}_N^i$ is not expressible as $\mathfrak{O}_T \otimes_{\mathbb{Z}_p[G]} M$ as $\mathfrak{O}_T[G]$-modules for any $\mathbb{Z}_p[G]$-module M, was first observed in a paper of Burns and Bley for $p = 3$ [1, Section 6].

Let $N = \mathbb{Q}_2(i, \sqrt[4]{12})$ and $\mathrm{Gal}(N/\mathbb{Q}_2) = \langle \sigma, \gamma \mid \sigma^4 = \gamma^2 = 1, \gamma\sigma\gamma = \sigma^3 \rangle$, where $\sigma(\sqrt[4]{12}) = i\sqrt[4]{12}$, σ fixes i, and γ is complex conjugation. One may check that $\pi =$

https://doi.org/10.4153/CJM-1998-050-4 Published online by Cambridge University Press

$1/2(\sqrt{3} + i\sqrt[4]{12} + 1)$ is a prime element in N. We used the computer package Pari to find this element. (The package was written by C. Batut, D. Bernardi, H. Cohen and M. Olivier, see [4].)

Let $K = \mathbb{Q}_2(\sqrt{-3}) = \mathbb{Q}_2(\zeta_3)$. Then one may easily verify that N/K is a fully ramified biquadratic extension with one break in its ramification filtration. The lower ramification number associated with this break is $b = 1$. Also note that in this case, $e_0 = 1$, $f = 2$, $T = K$, and $G = \mathrm{Gal}(N/K) = \langle \sigma^2, \sigma\gamma \rangle$.

We are interested in determining the $\mathbb{Z}_2[G]$-module structure of $\mathfrak{P}_N^3$, as this is not covered by Theorem 3.5. We begin by selecting a basis for $\mathfrak{P}_N^3$ over $\mathfrak{O}_T$. Clearly, $v_N\big(1/2(\sqrt{3}+i\sqrt[4]{12}+1)(1+\sqrt{3})\big) = 3$, $v_N(2) = 4$, $v_N(\sqrt{3}+i\sqrt[4]{12}+1) = 5$, $v_N\big(2(1+\sqrt{3})\big) = 6$. So

$$1/2(\sqrt{3} + i\sqrt[4]{12} + 1)(1 + \sqrt{3}), 2, \sqrt{3} + i\sqrt[4]{12} + 1, 2(1 + \sqrt{3}))$$

is an $\mathfrak{O}_T$-basis for $\mathfrak{P}_N^3$. We may alter this basis to get:

$$w_1 = 2, w_2 = 2\sqrt{3}, w_3 = i\sqrt[4]{12} + (\sqrt{3} + 1), w_4 = 1/2(i\sqrt[4]{12})(1 + \sqrt{3}) + \sqrt{3}$$

Clearly, the Galois action upon this basis is:

$$\sigma^2 \longrightarrow \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \quad \sigma\gamma \longrightarrow \begin{bmatrix} 1 & 0 & \frac{3-\sqrt{-3}}{6} & \frac{-\sqrt{-3}}{3} \\ 0 & -1 & \frac{-3+\sqrt{-3}}{6} & \frac{-3-\sqrt{-3}}{6} \\ 0 & 0 & -\frac{\sqrt{-3}}{3} & \frac{2\sqrt{-3}}{3} \\ 0 & 0 & \frac{-2\sqrt{-3}}{3} & \frac{-\sqrt{-3}}{3} \end{bmatrix}$$

Now if we make the following change of basis $w_1' = w_1$, $w_2' = -(1 + \sqrt{-3})/2w_2$, $w_3' = w_3 - (1 - \sqrt{-3})w_4/2$, $w_4' = w_4 - (1 - \sqrt{-3})w_3/2$, we find that

$$\sigma^2 \longrightarrow \begin{bmatrix} 1 & 0 & 1 & \zeta_3 \\ 0 & 1 & -1 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \quad \sigma\gamma \longrightarrow \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

If it were possible to express this $\mathfrak{O}_T[G]$-representation using matrices with $\mathbb{Z}_2$-coefficients, then it would be the case that this representation is isomorphic to

$$\sigma^2 \longrightarrow \begin{bmatrix} 1 & 0 & 1 & \zeta_3^2 \\ 0 & 1 & -1 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \quad \sigma\gamma \longrightarrow \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

In other words, the Frobenius element acts upon the pair of matrices associated with the action of σ^2 and $\sigma\gamma$, taking them to an $\mathfrak{O}_T[G]$-isomorphic pair. Let v_1, v_2, v_3, v_4 denote the basis of the first representation while w_1, w_2, w_3, w_4 denote the basis of the second representation. Since v_1 is the basis element killed by $(\sigma^2 - 1)$ and $(\sigma\gamma - 1)$, any isomorphism between these two modules must send v_1 to w_1. Similarly v_2 must be sent

https://doi.org/10.4153/CJM-1998-050-4 Published online by Cambridge University Press

to w_2. Certainly v_3 must be sent to $w_3 + aw_1 + bw_2$, from this one easily sees that v_3 must be sent to w_3. Finally, v_4 must be sent to $w_4 + aw_1 + bw_2 + cw_3$. By comparing $\sigma\gamma(v_4)$ with $\sigma\gamma(w_4 + aw_1 + bw_2 + cw_3)$, we see that $b = c = 0$. By comparing $\sigma^2(v_4)$ with $\sigma^2(w_4 + aw_1)$, we find that a must be $(\zeta_3^2 - \zeta_3)/2$ which is not an integer. So these two modules are not isomorphic over $\mathfrak{O}_T[G]$.

We now generalize this example. Let b be any odd positive integer. Let N and K be as before, and let $N_b = N(\sqrt[b]{2})$ while $K_b = K(\sqrt[b]{2})$, then since $\mathbb{Q}_2(\sqrt[b]{2})/\mathbb{Q}_2$ is tame, N_b/K_b is a fully ramified biquadratic extension with one break in its ramification filtration. The lower ramification number associated with this break is b. Clearly $v_{N_b}\big(1/2(\sqrt{3}+i\sqrt[4]{12}+1)\big) = b$, $v_{N_b}(1+\sqrt{3}) = 2b$, $v_{N_b}\big(1/2(\sqrt{3}+i\sqrt[4]{12}+1)(1+\sqrt{3})\big) = 3b$, while $v_{N_b}(\sqrt[b]{2^j}) = 4j$. By choosing elements with valuation, v_{N_b}, equal to $i, i+1, i+2, \dots 4b+i-1$ we will have a basis for $\mathfrak{P}_{N_b}^i$ over $\mathfrak{O}_T$. So

$$\begin{aligned}\mathfrak{P}_{N_b}^i = \sum_{j=0}^{b-1}(\sqrt[b]{2^j})\bigg(&\mathfrak{O}_T\frac{1}{2^{\lfloor\frac{4j-i}{4b}\rfloor}} + \mathfrak{O}_T\frac{1/2(\sqrt{3}+i\sqrt[4]{12}+1)}{2^{\lfloor\frac{4j+b-i}{4b}\rfloor}} + \mathfrak{O}_T\frac{1+\sqrt{3}}{2^{\lfloor\frac{4j+2b-i}{4b}\rfloor}}\\ &+ \mathfrak{O}_T\frac{1/2(\sqrt{3}+i\sqrt[4]{12}+1)(1+\sqrt{3})}{2^{\lfloor\frac{4j+3b-i}{4b}\rfloor}}\bigg).\end{aligned}$$

From this explicit description, we determine that

$$\begin{aligned}\mathfrak{P}_{N_b}^i \cong (\mathfrak{O}_N)^{\lceil\frac{b+i}{4}\rceil-\lceil\frac{i}{4}\rceil} \oplus (\mathfrak{P}_N)^{b+\lceil\frac{i}{4}\rceil-\lceil\frac{3b+i}{4}\rceil} \oplus (\mathfrak{P}_N^2)^{\lceil\frac{3b+i}{4}\rceil-\lceil\frac{2b+i}{4}\rceil}\\ \oplus (\mathfrak{P}_N^3)^{\lceil\frac{2b+i}{4}\rceil-\lceil\frac{b+i}{4}\rceil} \quad \text{as } \mathfrak{O}_T[G]\text{-modules.}\end{aligned}$$

Clearly the only time that $\mathfrak{P}_N^3$ does not appear is when $\lceil\frac{2b+i}{4}\rceil - \lceil\frac{b+i}{4}\rceil = 0$, which only happens when $b = 3$, $i \equiv 2 \bmod 4$ or when $b = 1$ and $i \equiv 0, 1, 2 \bmod 4$.

6**. Conclusion.** This research began in an attempt to determine the $\mathbb{Z}_p[\mathrm{Gal}(N/K)]$-module structure of the ring of integers of N, a fully ramified bicyclic extension of K, a finite extension of $\mathbb{Q}_p$, the field of p-adic numbers. The goal was to generalize the results of [7] by determining the structure without restriction on the ramification filtration.

Because of the complexities involved with the infinite families of modules and the problems presented by the computer generated examples of Burns and Bley [1] (as well as the examples of Section 5), it seemed prudent to restrict to biquadratic extensions and concentrate on a complete analysis. Fortunately, this restriction allowed us to present our results in global terms.

We mention the following questions concerning ambiguous ideals in biquadratic extensions which may be addressed based upon the explicit descriptions in Theorems 3.5, 3.6 and 3.9:

1. Cohomology of ambiguous ideals.
2. Galois isomorphisms among ambiguous ideals.
3. Duality relationships among the modules in an ambiguous ideal.

We note that the original question, the $\mathbb{Z}_p[G]$-module structure of the ring of integers in fully ramified bicyclic extensions, remains an open and very interesting question. Is it reasonable to expect that a resolution of this original question will result in structure theorems analogous to those in this paper, however with significantly more complicated expression?

Finally, as mentioned in Remark 3.11, a structure theorem for the ring of integers in local, fully ramified biquadratic extension with only one break in its ramification filtration will require more than just a knowledge of the ramification invariants of the extension. It remains an interesting and open problem to determine the nature of this additional, necessary information and the sort of structure of the ring of integers that will result as a consequence.

REFERENCES

1. W. Bley and D. Burns, *Über Arithmetische Assoziierte Ordnungen*. J. Number Theory (2) **58**(1996), 361–387.

2. D. Burns, *Factorisability and wildly ramified Galois extensions*. Ann. Inst. Fourier (Grenoble) **41**(1991), 393–430.

3. E. Dieterich, *Representation types of group rings over complete discrete valuation rings*. In: Integral representations and applications, Olberwolfach, 1980, Lecture Notes in Math., Springer, Berlin, New York, 1981, 369–389.

4. H. Cohen, *A course in computational algebraic number theory*. Springer-Verlag. Graduate Texts in Math. **138**, Berlin, Heidelberg, 1993.

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 (2) **47**(1994), 138–174.

7. ———, *Galois module structure of integers in wildly ramified $C_p \times C_p$ extensions*. Canad. J. Math. (4) **49**(1997), 722–735.

8. 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; errata ibid. (2) **48**(1998), 609–610.

9. A. Fröhlich, *Galois Module Structure of Algebraic Integers*. In: Ergebnisse der Mathematik und ihrer Grenzgebiete **3**, Folge, Bd. 1, Springer-Verlag, Berlin, Heidelberg, New York, 1983.

10. A. Fröhlich and M. J. Taylor, *Algebraic Number Theory*. Camb. Stu. Adv. Math. **27**, Cambridge Univ. Press, 1991.

11. H. Jakobinski, *Genera and Decompositions of Lattices over Orders*. Acta. Math. **121**(1968), 1–29.

12. H. W. Leopoldt, *Über die Hauptordnung der ganzen Elemente eines abelschen Zahlkörpers*. J. Reine Angew. Math. **201**(1959), 119–149.

13. B. Martel, *Sur l'anneau des entiers d'une extension biquadratique d'un corps* 2*-adique*. C. R. Acad. Sci. Paris **278**(1974), 117–120.

14. E. Maus, *Arithmetisch disjunkte Körper*. J. Reine Angew. Math. **226**(1967), 184–203.

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. L. A. Nazarova, *Integral representations of Klein's four-group*. Soviet Math. Dokl. **2**(1961), 1304–1307; English Translation.

17. ———, *Representation of a Tetrad*, Math. USSR-Izv. (6) **1**(1967), 1305–1321; English Translation.

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

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

20. S. Sen, *On automorphisms of local fields*. Ann. of Math. (2) **90**(1969), 33–46.

21. J-P. Serre, *Local fields*. Graduate Texts in Math. **67**, Springer-Verlag, Berlin, Heidelberg, New York, 1979.

22. 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.

23. R. Wiegand, *Cancellation over Commutative Rings of Dimension One and Two*. J. Algebra. (2) **88**(1984), 438–459.

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

Department of Mathematics
University of Nebraska at Omaha
Omaha, Nebraska 68132
U.S.A.
e-mail: elder@unomaha.edu