Canad. Math. Bull. Vol. **45** (2), 2002 pp. 168–179

Biquadratic Extensions with One Break

Nigel P. Byott and G. Griffith Elder

Abstract. We explicitly describe, in terms of indecomposable $\mathbb{Z}_2[G]$-modules, the Galois module structure of ideals in totally ramified biquadratic extensions of local number fields with only one break in their ramification filtration. This paper completes work begun in [Elder: Canad. J. Math. (5) **50**(1998), 1007–1047].

1 Introduction

The Galois module structure of ambiguous ideals in biquadratic extensions of global number fields was studied in [Eld98]. In this paper, we examine the one situation that [Eld98] left unresolved: The structure of ideals in totally ramified biquadratic extensions of local number fields with only one ramification break. So that we can be more precise, we introduce some notation.

Let K be a finite extension of the 2-adic numbers $\mathbb{Q}_2$ and N be a totally ramified biquadratic extension of K with Galois group G generated by σ and γ. Let $G = G_{-1} \supseteq G_0 \supseteq G_1 \supseteq \cdots$ denote the ramification filtration of G (with lower numbering). In general, the filtration of a biquadratic extension may contain one or two breaks. We focus here on the one break situation where $G = \cdots = G_b \supsetneq G_{b+1} = G_{b+2} = \cdots = \{e\}$, for some odd integer b satisfying $0 < b < 2e_0$. See [Ser79]. Using subscripts to denote the field of reference, we let $\mathfrak{O}_N$ denote the ring of integers of N, $\mathfrak{P}_N$ its unique prime ideal and $\mathfrak{P}_N^i$ (for some integer i) a generic ideal. We also let $\mathbb{Z}_2$ denote the ring of 2-adic integers.

The main result of this paper is Theorem 3.2, where assuming exactly one ramification break, we explicitly decompose each ideal $\mathfrak{P}_N^i$ into indecomposable $\mathbb{Z}_2[G]$-modules.

As explained in [Eld98], the $\mathbb{Z}[G]$-module structure of an ambiguous ideal in a biquadratic extension of global number fields is completely determined by its 2-adic completion. This is the result of a special property of $G = C_2 \times C_2$, namely that the conclusion of the Krull-Schmidt Theorem holds for $\mathbb{Z}[G]$. Consequently, Theorem 3.2 together with the results of [Eld98] provide an explicit description, as a sum of indecomposable $\mathbb{Z}[G]$-modules, of any ambiguous ideal in a biquadratic extension of global number fields.

As we will need further notation, we introduce it now. Let π_N denote a prime element in N and v_N denote its valuation, then $v_N(\pi_N) = 1$ and $\mathfrak{P}_N = \pi_N\mathfrak{O}_N$. Besides N and K, we will need to refer to T, the maximal unramified extension of $\mathbb{Q}_2$

Received by the editors July 20, 2000.
The first author was partially supported by EPSRC grant GR/M91037 and by UCR grant MG2000-03, The University of Nebraska at Omaha.
AMS subject classification: Primary: 11S15; secondary: 20C11.

contained in K. Clearly $e_0 := [K : T]$ is the absolute ramification index of K, while $f := [T : \mathbb{Q}_2]$ is its degree of inertia.

1.1 Motivation of Method

In [Eld98] the Galois module structure of an ideal, $\mathfrak{P}_N^i$, was determined by constructing a basis over $\mathfrak{O}_T$ upon which the Galois action could be explicitly followed. The essential ingredient in this construction was the determination of the valuation of an expression of the form, $(\gamma - 1)\alpha + (\sigma - 1)\theta$, for certain elements $\alpha, \theta \in N$ with $v_N(\alpha) \neq v_N(\theta)$ although $v_N(\alpha) \equiv v_N(\theta) \bmod 4$. It was found that this pair of conditions on α, θ could be satisfied only when there were two breaks in the ramification filtration. When there was only one break in this filtration of G, necessarily $v_N(\alpha) = v_N(\theta)$. This presented an obstacle which could not be overcome, except in a few isolated cases—see [Eld98, Theorem 3.5].

In this paper, we return to this issue. Note that since $v_N(\alpha) = v_N(\theta)$, there must be a $2^f - 1$ root of unity, ω, and a principal unit, $1+\Gamma \in \mathfrak{O}_N$, such that $\theta = \omega(1+\Gamma)\alpha$. We will determine both ω and $1 + \Gamma$ in determining the Galois module structure of ideals. Doing so however, requires a characterization of biquadratic extensions with only one break number.

2 Characterization of Extensions and a Galois Relationship

As one might expect, any restriction on the ramification in a biquadratic extension will restrict the type of square roots that can be used to generate the extension. Indeed if N/K is to have only one break, at b, in its ramification filtration; then the ramification break of each quadratic subfield must also occur at b. Since a quadratic extension with break number b is generated by the square root of a unit with quadratic defect $2e_0 - b$, we may assume that $N = K(x, y)$, where $x^2 = 1 + \beta$, $y^2 = 1 + \beta^* \in K$, and $v_K(\beta) = v_K(\beta^*) = 2e_0 - b$. Since the extension, $K(xy)/K$, must also have b as its break number, $\beta^*/\beta \equiv \omega^{-2} \bmod \pi_K$ for some nontrivial $2^f - 1$ root of unity, ω^{-2}. (Note that any $2^f - 1$ root of unity may be expressed as a square.)

As a consequence of this discussion and since $K(\omega^{-2}y) = K(y)$, we assume, without loss of generality, that $N = K(x, y)$ for

$$x^2 = 1 + \beta,$$
$$y^2 = (\omega^2 + \beta)(1 + \tau), \tag{2.1}$$

where $\beta, \tau \in \mathfrak{P}_K$, $v_K(\beta) = 2e_0 - b$ and ω is a non-trivial $2^f - 1$ root of unity. Clearly τ might be zero. If $\tau \neq 0$, since we are only interested in the unit $1 + \tau$ up to a square factor, we may assume that $v_K(\tau) := 2e_0 - t$ where either t is odd and $0 < t < b$, or $t = 0$. Choose $\sigma, \gamma \in \mathrm{Gal}(N/K)$ so that

$$\sigma(y) = -y, \quad \sigma(x) = x, \quad \gamma(y) = y, \quad \gamma(x) = -x.$$

Let $L := K(x)$ and consider the quadratic extension N/L. Since N/L has ramification number b, there is a $\Delta \in L$ with valuation, $v_L(\Delta) = 4e_0 - b$, such that $N = L(Y)$

https://doi.org/10.4153/CMB-2002-020-3 Published online by Cambridge University Press

and

$$Y^2 = 1 + \Delta.$$

Since $L(y) = L(Y)$, there is an element $a_1 + a_2 x \in L$ $(a_1, a_2 \in K)$ such that

$$Y = (a_1 + a_2 x) \cdot y. \tag{2.2}$$

To better understand this relationship between Y and y, we seek a characterization of a_1 and a_2. Note that (2.2) leads to $1 + \Delta = (a_1 + a_2 x)^2(\omega^2 + \beta)(1 + \tau)$. Therefore,

(2.3)

$$\begin{aligned} 1 + \Delta = {} & (a_1 + a_2)^2\omega^2 + \big((a_1 + a_2)^2 + a_2^2\omega^2\big)\beta \\ & + (a_1 + a_2)^2\omega^2\tau + a_1 a_2 \omega^2 2(x-1) + a_2^2\beta^2 + \big((a_1 + a_2)^2 + a_2^2\omega^2\big)\beta\tau \\ & + a_1 a_2\big(2(x-1)\big)\beta + a_1 a_2 \omega^2\big(2(x-1)\big)\tau + a_1 a_2\big(2(x-1)\big)\tau\beta + a_2^2\beta^2\tau \end{aligned}$$

To clarify matters, we eliminate some terms,

$$1 \equiv (a_1 + a_2)^2\omega^2 \bmod \beta.$$

Therefore $(a_1 + a_2)\omega = 1 + c$ for some $c \in \mathfrak{P}_K$. Since $(1 + c)^2 \equiv 1 \bmod \beta$, we have $2c + c^2 \equiv 0 \bmod \beta$. To get the stronger congruence $2c + c^2 \equiv 0 \bmod \beta\pi_K$, we consider two cases. If $v_K(c) \geq e_0$, then $v_K(2c + c^2) = v_K\big(c(2 + c)\big) \geq v_K(c) + e_0 \geq 2e_0 > v_K(\beta)$. On the other hand, if $v_K(c) < e_0$, then $v_K(2c + c^2) = v_K\big(c(2 + c)\big) = 2v_K(c)$. Since $v_K(2c + c^2)$ is even and $v_K(\beta)$ is odd, $v_K(2c + c^2) > v_K(\beta)$. In any case, $1 \equiv (a_1 + a_2)^2\omega^2 \bmod \beta \cdot \pi_K$. Now reducing (2.3) modulo $\beta \cdot \pi_L$, we find $1 \equiv (a_1 + a_2)^2\omega^2 + \big((a_1 + a_2)^2 + a_2^2\omega^2\big)\beta \bmod \beta \cdot \pi_L$. Since each term lies in K, we may replace $\bmod \beta \cdot \pi_L$ with $\bmod \beta \cdot \pi_K$. Therefore,

$$\begin{aligned} 1 &= (a_1 + a_2)^2\omega^2 \bmod \pi_K\beta, \\ 0 &= (a_1 + a_2 + \omega a_2)^2\beta \bmod \pi_K\beta. \end{aligned} \tag{2.4}$$

These equations yield $a_1 + a_2 = \omega^{-1} \bmod \pi_K(x-1)$ and $a_1 + a_2 + \omega a_2 = 0 \bmod \pi_K$. Solving for a_1 and a_2, we find that there are elements $\kappa_1, \kappa_2 \in K$ with positive valuation such that $a_1 = \omega^{-1} + \omega^{-2} + \kappa_1$ and $a_2 = \omega^{-2} + \kappa_2$. Since $a_1 + a_2 = \omega^{-1} \bmod \pi_K(x-1)$, $\kappa_1 \equiv \kappa_2 \bmod \pi_K(x-1)$. Therefore

$$\begin{aligned} a_1 &= \omega^{-1} + \omega^{-2} + \kappa_1 \\ a_2 &= \omega^{-2} + \kappa_1 + u(x-1), \end{aligned} \tag{2.5}$$

for some $u \in L$ with $v_L(u) \geq 2$. Note, in particular, that a_1 and a_2 are units in K.

This is used to derive the following Galois relationship.

Proposition 2.1 *There are elements $\alpha \in N$ and $\kappa, \beta' \in K$ with $v_N(\alpha) = b$ and $v_K(\beta') = 2e_0 - b$ such that*

$$\rho := \Big[(\gamma + 1) + (\omega^{-1} + \kappa)(\sigma + 1) + \beta'\frac{1}{2}(\gamma - 1)(\sigma - 1)\Big]\alpha$$

has valuation $v_N(\rho) = 3b$. Let $s = v_K(\kappa)$. If $2t > b$ and $2b - t < 2e_0$ then $s = (b - t)/2$. Otherwise, $s > e_0 - b/2$.

https://doi.org/10.4153/CMB-2002-020-3 Published online by Cambridge University Press

Proof Since $\gamma(Y) \neq Y$ there is a $\delta \neq 1$ in L such that $\gamma(Y)/Y = \delta$. From (2.2) we find that

$$\delta = \frac{a_1 - a_2 x}{a_1 + a_2 x} = 1 + 2d_0 + 2d_1 x,$$

where $d_0 = a_2^2(1+\beta)/\big(a_1^2 - a_2^2(1+\beta)\big) \in \mathfrak{O}_K$ and $d_1 = -a_1 a_2/\big(a_1^2 - a_2^2(1+\beta)\big) \in \mathfrak{O}_K$. Recall that since Y and y are units, $a_1 + a_2 x$ must be a unit. So its norm, namely $a_1^2 - a_2^2(1+\beta)$, is a unit.

Let $\alpha = (x-1)(Y-1)$, so $v_N(\alpha) = 8e_0 - 3b$. Then

$$(\gamma - 1)\alpha = 2x - 2(d_0 + d_1 + d_1\beta)Y - 2(1 + d_0 + d_1)xY,$$
$$(\sigma - 1)\alpha = 2Y - 2xY,$$
$$1/2 \cdot (\gamma - 1)(\sigma - 1)\alpha = 2(d_0 + d_1 + d_1\beta)Y + 2(1 + d_0 + d_1)xY.$$

Letting $A = 1 - (1 + 2d_0 + 2d_1 + d_1\beta)^{-1}$ and $A' = d_0 + d_1 + d_1\beta$, we find that

$$(2.6) \qquad (\gamma - 1)\alpha + (1 - A)A'(\sigma - 1)\alpha + (A/2)(\gamma - 1)(\sigma - 1)\alpha = 2x - 2xY.$$

Note that $v_N\big((\sigma - 1)\alpha\big) = 8e_0 - 2b$. So $(\sigma - 1)\alpha$ may be expressed in terms of an element fixed by γ having valuation $8e_0 - 2b$ and an element in N of higher valuation. As a consequence, $v_N\big((\gamma - 1)(\sigma - 1)\alpha\big) > 8e_0 - b$. Meanwhile $v_N\big(2x(1 - Y)\big) = 8e_0 - b$.

Let $\rho_0 = [(2x - 2xY) - (d_0 + d_1)/(1 + 2d_0 + 2d_1 + d_1\beta)(\gamma - 1)(\sigma - 1)\alpha]\pi_K^b/4$. Since d_0 and d_1 are integers in K, $v_N(\rho_0) = 3b$. Redefine α to be $\alpha := \alpha \cdot \pi_K^b/4$ and replace $2x - 2xY$ using (2.6). All this results in the expression, $\rho_0 = [(\gamma - 1) + \Omega(\sigma - 1) + (\beta'/2)(\gamma - 1)(\sigma - 1)]\alpha$, with

$$\Omega = \frac{d_0 + d_1 + \beta d_1}{1 + 2d_0 + 2d_1 + \beta d_1} \qquad \beta' = \frac{d_1}{1 + 2d_0 + 2d_1 + d_1\beta} \cdot \beta.$$

Add $2(1 + \Omega)\alpha$ to both sides of this equation. Let $\rho := \rho_0 + 2(1 + \Omega)\alpha$. Since $v_N(2\alpha) = 4e_0 + b > 3b$, $v_N(\rho) = 3b$. Therefore

$$(2.7) \qquad \rho = \Big[(\gamma + 1) + \Omega(\sigma + 1) + \beta' \frac{1}{2}(\gamma - 1)(\sigma - 1)\Big]\alpha$$

where $v_K(\alpha) = b$ and $v_N(\rho) = 3b$.

Using (2.5) we find that d_0 and d_1 are units, so that $v_K(\beta') = v_K(\beta) = 2e_0 - b$. To characterize Ω, note that $\Omega \equiv d_0 + d_1 \equiv (\delta - 1)/2 \equiv -a_2/(a_1 + a_2) \bmod (x - 1)$. Meanwhile from (2.5), $-a_2/(a_1 + a_2) \equiv -(\omega^{-2} + \kappa_1)\omega \bmod (x - 1)$. So

$$\Omega = \omega^{-1} + \kappa,$$

for some $\kappa \in \mathfrak{P}_K$ with $\kappa \equiv \omega\kappa_1 \bmod (x - 1)$.

Now we show that when $2t > b$ and $2b - t < 2e_0$, $v_K(\kappa) = (b - t)/2$. Otherwise $v_K(\kappa) > e_0 - b/2$. First recall from (2.5) that $u(x - 1) = a_2 - \omega^{-2} - \kappa_1 \in K$. Therefore $v_L\big(u(x - 1)\big)$ is even, and as a result, $v_L(u)$ is odd.

https://doi.org/10.4153/CMB-2002-020-3 Published online by Cambridge University Press

Consider $2t > b$ (*i.e.* $v_L(\tau) < v_L(\Delta)$) and reduce (2.3) modulo $\tau \cdot \pi_L$. Since $2t > b > 0$, $2(x-1) \equiv 0 \bmod \tau \cdot \pi_L$. So $1 \equiv (a_1+a_2)^2\omega^2 + \big((a_1+a_2)^2 + a_2^2\omega^2\big)\beta + (a_1+a_2)^2\omega^2\tau + a_2^2\beta^2 \bmod \tau \cdot \pi_L$. Using (2.5), $(a_1+a_2)^2 \equiv \omega^{-2} + u^2\beta \bmod \tau \cdot \pi_L$, while $a_2^2 = \omega^{-4} + k_1^2 + u^2\beta \bmod \tau \cdot \pi_L$. Substitution leads to

$$(2.8)\quad 0 \equiv (\omega^2u^2 + \omega^2\kappa_1^2)\beta + \tau + \big((1+\omega^2)u^2 + \omega^{-4} + \kappa_1^2\big)\beta^2 + u^2\beta^3 \bmod \tau \cdot \pi_L.$$

If $v_L(\tau) < v_L(\beta^2)$ (in other words $2b-t < 2e_0$), then $v_L\big((\omega^2u^2+\omega^2\kappa_1^2)\beta\big)$ must equal $v_L(\tau)$. In other words, $v_L(\chi^2\beta) = v_L(\tau)$ with $\chi = \omega(u+\kappa_1)$. Consequently $v_L(\chi) = \big(v_L(\tau) - v_L(\beta)\big)/2 = b - t$. Since $t > 0$, t is odd. Of course b is odd. Therefore $v_L(\chi) = b - t$ is even. Since $v_L(\kappa_1)$ is even while $v_L(u)$ is odd and $\chi = \omega(u+\kappa_1)$ has even valuation, $v_L(\omega\kappa_1) = v_L(\chi)$. Therefore $v_K(\omega\kappa_1) = (b-t)/2$. Since $2b-t < 2e_0$, $v_L(\omega\kappa_1) < v_L(x-1)$. So since $\kappa \equiv \omega\kappa_1 \bmod (x-1)$, $v_K(\kappa) = (b-t)/2$. Alternatively, if $v_L(\tau) > v_L(\beta^2)$ (in other words $2b - t > 2e_0$), an examination of (2.8) leads to $v_L\big((\omega^2u^2 + \omega^2\kappa_1^2)\beta\big) \geq v_L(\beta^2)$. As a result, $v_L(\chi^2) \geq v_L(\beta)$. Since $v_L(u)$ and $v_L(\kappa_1)$ have opposite parity $v_L(\kappa_1) \geq v_L(\beta)/2$. Therefore $\kappa \equiv \omega\kappa_1 \equiv 0 \bmod (x-1)$ and so $v_L(\kappa) \geq 2e_0 - b$. Since $v_K(\kappa)$ is an integer, $v_K(\kappa) > e_0 - b/2$.

Consider $b > 2t$ (*i.e.* $v_L(\tau) > v_L(\Delta)$) and reduce (2.3) modulo Δ. Clearly $1 \equiv (a_1+a_2)^2\omega^2 + \big((a_1+a_2)^2 + a_2^2\omega^2\big)\beta + a_2^2\beta^2 \bmod \Delta$. Again use (2.5) to replace a_1 and a_2. This results in

$$(2.9)\qquad 0 \equiv (\omega^2u^2 + \omega^2\kappa_1^2)\beta + \big((1+\omega^2)u^2 + \omega^{-4} + \kappa_1^2\big)\beta^2 + u^2\beta^3 \bmod \Delta.$$

If $v_L(\beta^2) < v_L(\Delta)$, then $v_L\big((\omega^2u^2 + \omega^2\kappa_1^2)\beta\big) \geq v_L(\beta^2)$. By following the discussion in the previous paragraph $v_K(\kappa) > e_0 - b/2$. So assume instead that $v_L(\beta^2) \geq v_L(\Delta)$. In this case (2.9) leads to $0 = \chi^2\beta \bmod \Delta$. So $v_L(\chi^2) \geq v_L(\Delta/\beta) = b$, and $v_L(\chi) \geq b/2$. Since $v_L(u)$ is odd while $v_L(\kappa_1)$ is even, $v_L(\kappa_1) = v_L(\chi) \geq b/2$. If $v_L(\kappa_1) > 2e_0 - b$ then as before $v_K(\kappa) > e_0 - b/2$. So assume $v_L(\kappa_1) < 2e_0 - b$. But then since $\kappa \equiv \omega\kappa_1 \bmod (x-1)$, $v_K(\kappa) = v_K(\kappa_1) > b/4$. Therefore $v_N\big(\kappa(\sigma+1)\alpha\big) > 3b$, and so ρ has the same valuation as $\rho - \kappa(\sigma+1)\alpha$. Replace one by the other. This results in a revised expression in (2.7), one with $\Omega = \omega^{-1}$. But then $\kappa = 0$ while clearly $v_K(0) > e_0 - b/2$. ■

3 Structure of Ideals

In this section we determine the Galois module structure of each ideal $\mathfrak{P}_N^i$, using the same technique as in [Eld98]. Thus we first find elements μ_k of N, for $k \in \mathbb{Z}$ such that $v_N(\mu_k) = k$. Clearly $\mu_i, \mu_{i+1}, \dots, \mu_{i+4e_0-1}$ will be a basis for $\mathfrak{P}_N^i$ over $\mathfrak{O}_T$. We then adjust this basis to obtain a new basis, whose elements will not necessarily have distinct valuations, but on which the action of the Galois group is easier to follow.

To expedite matters, we begin with [Eld98, Lemmma 3.15] and the discussion following the lemma. Note that the only condition on α_m in [Eld98, Lemmma 3.15] is in terms of valuation, $v_N(\alpha_m) = b + 4m$. Any element with the same valuation can be used. So we let $\alpha_m := \alpha \cdot \pi_K^m$ with α from Proposition 2.2. Using all other elements as in [Eld98, Lemma 3.15] (in particular the element $\rho_m \in N$ produced in the proof of that lemma), we may create bases for $\mathfrak{P}_N^i$ over $\mathfrak{O}_T$. For example, under

$3b < 4e_0$ the elements listed in [Eld98, (3.2)–(3.5)] all have distinct valuations and so serve as a basis for $\mathfrak{P}_N^i$ over $\mathfrak{O}_T$. Note that we may replace any element in this basis with another element of the same valuation (and still have a basis). And so we replace each ρ_m in [Eld98, (3.4)] with $\rho \cdot \pi_K^m$ (where ρ is from Proposition 2.2). It should not cause any confusion if each such $\rho \cdot \pi_K^m$ is now referred to as ρ_m. Note however that we have not replaced any of the ρ_m in [Eld98, (3.2), (3.3), (3.5)], and so for each of these ρ_m we have $\rho_m - (\gamma + 1)\alpha_m$ contained in the fixed field of σ. Following [Eld98, Remark 3.16] we can replace each ρ_m in [Eld98, (3.2), (3.3), (3.5)] with $(\gamma + 1)\alpha_m$ and still have a basis over $\mathfrak{O}_T$ (although one which no longer has distinct valuations). Consequently the elements listed in [Eld98, (3.6)–(3.9)] provide an $\mathfrak{O}_T$-basis for $\mathfrak{P}_N^i$ when $3b < 4e_0$. Similarly, when $3b < 4e_0$, we can conclude that the elements in [Eld98, (3.10)–(3.13)] provide a basis. In both cases, the elements α_m arose as $\alpha \cdot \pi_K^m$ with α from Proposition 2.2, while the ρ_m (that appear) are $\rho \cdot \pi_K^m$ with ρ from Proposition 2.2.

For the convenience of the reader, we include a slight revision of these lists. Each element of [Eld98, (3.9)] is divided by 2 and is listed in (3.1) below. These elements are followed in sequence by the elements in [Eld98, (3.6)–(3.8)]. Meanwhile we have divided the elements in [Eld98, (3.12), (3.13)] by 2 and listed them as (3.5) and (3.6) below. They are followed by the elements listed in [Eld98, (3.10), (3.11)]. Let $\lceil x \rceil$ denote the ceiling function (least integer greater than or equal to x).

Case $3b < 4e_0$

(3.1) $$1/2(\gamma+1)(\sigma+1)\alpha_m,\ \alpha_m,\ (\sigma+1)\alpha_m,\ (\gamma+1)\alpha_m,$$
$$\text{for } e_0 + \left\lceil \frac{i}{4} \right\rceil - b \le m \le e_0 + \left\lceil \frac{i-3b}{4} \right\rceil - 1.$$

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

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

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

Case $3b > 4e_0$

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

https://doi.org/10.4153/CMB-2002-020-3 Published online by Cambridge University Press

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

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

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

The following lemma enables us to clarify the Galois action upon the elements listed in (3.4) and (3.8).

Lemma 3.1 *Let ω, κ and β' be defined as in the previous section. Then*

$$\eta := \frac{(\omega^{-1}-1+\kappa)(\omega^{-1}+1+\kappa-\beta')}{(\omega^{-1}+\kappa-\beta')(\omega^{-1}+\kappa)} \equiv (1-\omega^2) \bmod \pi_K.$$

Furthermore

$$a := v_K\big(\eta-(1-\omega^2)\big) = \begin{cases} b-t & \text{if } 2t>b \text{ and } 2b-t<2e_0,\\ 2e_0-b & \text{otherwise}\end{cases}.$$

Proof One may check that

$$\eta = (1-\omega^2) + \frac{\omega^2}{\big(1+\omega(\kappa-\beta')\big)(1+\omega\kappa)}\cdot B$$

where $B=(1-\omega)\beta'-2\omega\kappa+\omega^2\kappa^2-\omega^2\kappa\beta'$. If $v_K(\kappa^2)<v_K(\beta')$ (equivalently, $2s<2e_0-b$), then $v_K(B)=v_K(-2\omega\kappa+\omega^2\kappa^2)$ and $v_K(\kappa)=(b-t)/2<e_0$. Therefore $v_K(-2\omega\kappa+\omega^2\kappa^2)=v_K(\omega^2\kappa^2)=2s$. If $v_K(\kappa^2)>v_K(\beta')$ or $2s>2e_0-b$ then $v_K(2\omega\kappa)=e_0+s>2e_0-b/2>2e_0-b$. So $v_K(B)=v_K\big((1-\omega)\beta'\big)=2e_0-b$. ∎

For m such that $\lceil(i-3b)/4\rceil\le m\le\lceil(i-2b)/4\rceil-1$ (in other words, those m listed in (3.4) and (3.8)), we redefine α_{m+a} in terms of α_m. Let

$$\alpha_{m+a} := \big(\eta-(1-\omega^2)\big)\,\alpha_m,$$

since the elements have the same valuation. Furthermore if $m+a\le\lceil(i-2b)/4\rceil-1$, let $\rho_{m+a} := \big(\eta-(1-\omega^2)\big)\,\rho_m$.

Now for a particular value of m, consider the Galois action on the basis elements:

$$\rho_m, 2\alpha_m, (\gamma+1)(\sigma+1)\alpha_m, 2(\sigma+1)\alpha_m.$$

First, note that we still have a basis if these are replaced by

$$\rho_m, \rho_m - 2\alpha_m, (\gamma-1)(\sigma+1)\alpha_m, (\gamma+1)(\sigma+1)\alpha_m.$$

Since $\nu_N(\rho_m) < \nu_N(2\alpha_m) < \nu_N(2\beta'\alpha_m)$, we may also replace ρ_m by $\rho_m - 2\beta'\alpha_m$. Therefore we instead examine the Galois action on the alternative elements:

$$\rho_m - 2\beta'\alpha_m, \rho_m - 2\alpha_m, (\gamma-1)(\sigma+1)\alpha_m, (\gamma+1)(\sigma+1)\alpha_m.$$

The action on $(\gamma-1)(\sigma+1)\alpha_m, (\gamma+1)(\sigma+1)\alpha_m$ is clear. Meanwhile it is easy to check that

$$(\gamma-1)(\rho_m - 2\beta'\alpha_m) = (\gamma-1)(\sigma+1)[\omega^{-1}+\kappa-\beta']\alpha_m$$
$$(\gamma+1)(\rho_m - 2\alpha_m) = (\gamma+1)(\sigma+1)[\omega^{-1}+\kappa]\alpha_m$$

The effect of σ is more complicated: $(\sigma+1)(\rho_m - 2\beta'\alpha_m) = (\gamma+1)(\sigma+1)\cdot[\omega^{-1}+1+\kappa-\beta']\alpha_m - (\gamma-1)(\sigma+1)[\omega^{-1}+\kappa-\beta']\alpha_m$ while $(\sigma+1)(\rho_m-2\alpha_m) = (\gamma+1)(\sigma+1)[\omega^{-1}+\kappa]\alpha_m - (\gamma-1)(\sigma+1)[\omega^{-1}-1+\kappa]\alpha_m$. As a result, we use the fact that $\sigma\gamma+1 = (\sigma+1)(\gamma+1) - (\sigma+1) - (\gamma-1)$ and $\sigma\gamma-1 = (\sigma+1)(\gamma-1) + (\sigma+1) - (\gamma+1)$ to easily determine the much simpler effect of $\sigma\gamma$:

$$(\sigma\gamma+1)(\rho_m - 2\beta'\alpha_m) = (\gamma+1)(\sigma+1)[\omega^{-1}+1+\kappa-\beta']\alpha_m$$
$$(\sigma\gamma-1)(\rho_m - 2\alpha_m) = (\gamma-1)(\sigma+1)[\omega^{-1}-1+\kappa]\alpha_m.$$

As we are working with a basis over $\mathfrak{O}_T$, we may multiply basis elements by units in $\mathfrak{O}_T$. As a result, we use the alternative basis elements:

$$y_m^+ := \frac{\omega^{-1}-1+\kappa}{\omega^{-1}+\kappa-\beta'}(\rho_m - 2\beta'\alpha_m), \quad y_m^- := \rho_m - 2\alpha_m,$$
$$x_m^+ := (\gamma+1)(\sigma+1)[\omega^{-1}+\kappa]\alpha_m, \quad x_m^- := (\gamma-1)(\sigma+1)[\omega^{-1}-1+\kappa]\alpha.$$

Since $\alpha_{m+a} = [\eta - (1-\omega^2)]\alpha_m$, $x_{m+a}^+ = [\eta-(1-\omega^2)]x_m^+$, and so $\eta x_m^+ = (1-\omega^2)x_m^+ + x_{m+a}^+$. Therefore

$$(3.9) \qquad \begin{gathered}(\gamma-1)y_m^+ = x_m^- \quad (\gamma+1)y_m^- = x_m^+\\ (\sigma\gamma+1)y_m^+ = (1-\omega^2)x_m^+ + x_{m+a}^+ \quad (\sigma\gamma-1)y_m^- = x_m^-.\end{gathered}$$

Now consider the situation where $m+a \geq \lceil (i-2b)/4\rceil$. If $m+a < e_0 + \lceil (i-3b)\rceil$ then it is clear that $(\gamma+1)\alpha_{m+a}$ is an element in our basis, appearing in (3.1)–(3.3) or (3.5)–(3.7). If $m+a \geq e_0 + \lceil (i-3b)\rceil$ then $(\gamma+1)\alpha_{m+a} \in 2\mathfrak{P}_N^i$. In either case, we may replace y_m^+ by $\bar{y}_m^+ := y_m^+ - (\gamma+1)[\omega^{-1}+\kappa]\alpha_{m+a}$ and still have a basis. Note that

$(\gamma - 1)$ has the same effect upon $\bar{y}_m^+$ as on y_m^+, but that the effect of $(\sigma\gamma + 1)$ is much simpler:

$$(\sigma\gamma + 1)\bar{y}_m^+ = (1 - \omega^2)x_m^+.$$

Replace each such y_m^+ with $\bar{y}_m^+$. Therefore without loss of generality, we may replace the elements listed in (3.4) and (3.8) by

$$y_m^+, y_m^-, x_m^+, x_m^-$$

and assume that the Galois action is defined by (3.9) except that

$$(3.10) \qquad (\sigma\gamma + 1)y_m^+ = \begin{cases} (1 - \omega^2)x_m^+ + x_{m+a}^+ & \text{if } m + a < \lceil (i - 2b)/4 \rceil \\ (1 - \omega^2)x_m^+ & \text{otherwise} \end{cases}.$$

Let

$$(3.11) \qquad n := \left\lfloor \frac{\lfloor \frac{i-2b-1}{4} \rfloor + \lfloor \frac{3b-i}{4} \rfloor}{a} \right\rfloor,$$

$\lfloor x \rfloor$ denoting the floor or greatest integer function. One can easily verify that $\lfloor b/(4a) \rfloor - 1 \leq n \leq \lfloor b/(4a) \rfloor$, moreover n is the maximal integer such that $\lceil (i - 3b)/4 \rceil + na < \lceil (i - 2b)/4 \rceil$.

Therefore the basis elements listed in (3.4) and (3.8) result in a direct sum of $\mathfrak{O}_T[G]$-modules with bases such as:

$$(3.12) \qquad \begin{array}{c} y_{m+ka}^+, y_{m+ka}^-, x_{m+ka}^+, x_{m+ka}^- \\ \vdots \\ y_{m+2a}^+, y_{m+2a}^-, x_{m+2a}^+, x_{m+2a}^- \\ y_{m+a}^+, y_{m+a}^-, x_{m+a}^+, x_{m+a}^- \\ y_m^+, y_m^-, x_m^+, x_m^- \end{array}$$

Either $k = n$ or $k = n - 1$. Note that $(\sigma\gamma + 1)y_{m+ka}^+ = (1 - \omega^2)x_{m+ka}^+$.

Let us now examine the module that results from these basis elements. If we list the x_i^+ first then the x_i^-, followed by the y_i^+ and then the y_i^-; the Galois action is described by the following $4k \times 4k$ matrices over $\mathfrak{O}_T$:

$$\gamma \to \begin{vmatrix} E & 0 & 0 & E \\ 0 & -E & E & 0 \\ 0 & 0 & E & 0 \\ 0 & 0 & 0 & -E \end{vmatrix} \qquad \sigma\gamma \to \begin{vmatrix} E & 0 & M & 0 \\ 0 & -E & 0 & E \\ 0 & 0 & -E & 0 \\ 0 & 0 & 0 & E \end{vmatrix}$$

where E denotes a $k \times k$ identity matrix and M is the matrix in Jordan canonical form associated with the minimal polynomial $\big(x - (1 - \omega^2)\big)^k$. In other words, M is an $k \times k$ matrix with $1 - \omega^2$ on the diagonal and 1 just above the diagonal.

Upon restriction of scalars the Galois action appears essentially the same. Let $p(x)$ be the irreducible polynomial with $1-\omega^2$ as a root, and let d be the degree of $p(x)$. Then in this case E denotes a $kd \times kd$ identity matrix, while M denotes the $kd \times kd$ matrix over $\mathbb{Z}_2$ in Jordan canonical form with minimal polynomial $p(x)^k$. We denote this module by

$$\hat{\mathfrak{J}}_{k-1}\big(p(x)\big) \tag{3.13}$$

This module is part of a family of indecomposable modules identified in [Naz61, p. 1306] in the paragraph beginning "Let $n = d$". It is also listed among the modules classified in Lemma 1 of [Naz67, p. 1310] where a proof of its indecomposability is given. We have chosen our notation to be consistent with notation in [Eld98]. This module belongs in the same family as another module that also appears in the decomposition of ideals. Replacing $p(x)$ by $x-1$ we find that $\hat{\mathfrak{J}}_{k-1}(x-1) = \hat{\mathfrak{J}}_{k-1}$, the module listed on [Eld98, p. 1040].

We now list certain other $\mathbb{Z}_2[G]$-modules that we will require for our main result. Our notation is that used in [Eld98, Section 4]. Let $\hat{\mathfrak{G}} = \mathbb{Z}_2[G]$. Note this module occurs for each m in (3.2). Let $\hat{\mathfrak{Z}}$ denote the rank one module fixed by the group action, while for each $x \in G$ let $\hat{\mathfrak{R}}_x$ be the rank one module on which only x acts trivially upon (all other nontrivial group elements should act via multiplication by -1). Then the maximal order, $\hat{\mathfrak{Z}} \oplus \hat{\mathfrak{R}}_\sigma \oplus \hat{\mathfrak{R}}_\gamma \oplus \hat{\mathfrak{R}}_{\sigma\gamma}$, occurs for each m in (3.6).

Let $\hat{\mathfrak{C}}$ and $\hat{\mathfrak{D}}$ be rank 4 modules with Galois action described by the pairs of matrices below:

$$\hat{\mathfrak{C}}\colon \gamma \to \begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{vmatrix} \quad \sigma \to \begin{vmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{vmatrix}$$

$$\hat{\mathfrak{D}}\colon \gamma \to \begin{vmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{vmatrix} \quad \sigma \to \begin{vmatrix} 1 & 0 & 1 & -1 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{vmatrix}$$

Note that $\hat{\mathfrak{C}}$ occurs for each m in (3.1) and (3.6), while $\hat{\mathfrak{D}}$ occurs for each m in (3.3) and (3.7). All this is collected in the following Theorem:

Theorem 3.2 *Let ω, b, t be as in (2.1), $p(x)$ be the minimal polynomial of $1-\omega^2$ over $\mathbb{Z}_2$ and $d = \deg p(x)$. If $2t > b$ and $2b - t < 2e_0$, let $a = b - t$. Otherwise, let $a = 2e_0 - b$. Let*

$$n := \left\lfloor \frac{\lfloor \frac{i-2b-1}{4} \rfloor + \lfloor \frac{3b-i}{4} \rfloor}{a} \right\rfloor.$$

The $\mathbb{Z}_2[G]$-module structure of $\mathfrak{P}_N^i$ then, is as follows:

$$\mathfrak{P}_N^i \cong \mathfrak{X} \oplus \mathfrak{Y},$$

where

$$\mathcal{X} = \begin{cases} \hat{\mathcal{G}}^{(e_0+\lceil\frac{i-4b}{4}\rceil-\lceil\frac{i-b}{4}\rceil)f} \oplus \hat{\mathcal{D}}^{(\lceil\frac{i-b}{4}\rceil-\lceil\frac{i-2b}{4}\rceil)f} \oplus \\ \qquad \hat{\mathcal{C}}^{(\lceil\frac{i-3b}{4}\rceil-\lceil\frac{i-4b}{4}\rceil)f} & \text{if } b < 4e_0/3 \\ \hat{\mathcal{D}}^{(e_0+\lceil\frac{i-4b}{4}\rceil-\lceil\frac{i-2b}{4}\rceil)f} \oplus \hat{\mathcal{C}}^{(\lceil\frac{i-3b}{4}\rceil-\lceil\frac{i-b}{4}\rceil)f} \\ \qquad (\hat{\mathcal{Z}} \oplus \hat{\mathcal{R}}_\sigma \oplus \hat{\mathcal{R}}_\gamma \oplus \hat{\mathcal{R}}_{\sigma\gamma})^{(\lceil\frac{i-b}{4}\rceil-e_0-\lceil\frac{i-4b}{4}\rceil)f} & \text{otherwise} \end{cases}$$

while

$$\mathcal{Y} = \hat{\mathcal{I}}_{n-1}\big(p(x)\big)^{(\lceil\frac{i-3b}{4}\rceil-\lceil\frac{i-2b}{4}\rceil+(n+1)a)\frac{f}{d}} \oplus \hat{\mathcal{I}}_n\big(p(x)\big)^{(\lceil\frac{i-2b}{4}\rceil-\lceil\frac{i-3b}{4}\rceil-na)\frac{f}{d}}$$

Note that $\lceil x \rceil$ denotes the ceiling or least integer function.

4 Example: Quadratic Twist

Consider the class of biquadratic extensions with $\tau = 0$ (where τ is as in (2.1)). These are extensions $N_1 := K(x, y)$ with $x^2 = 1 + \beta$ and $y^2 = \omega^2 + \beta$ for some nontrivial $2^f - 1$ root of unity ω, and some $\beta \in K$ with $v_K(\beta) = 2e_0 - b$, b odd and $0 < b < 2e_0$. To compare such an extension with one for which $\tau \neq 0$ we introduce the quadratic extension $K(z)/K$ associated with the unit $z^2 = 1 + \tau$. So that $K(z)/K$ is truly a quadratic extension, we must have $v_K(\tau) = 2e_0 - t$ with $0 \leq t < 2e_0$.

Clearly N_1 and $N_2 := K(x, yz)$, both biquadratic extensions, sit in the larger field $K(x, y, z)$. To ensure that they both have exactly one break in their Galois filtration, we must assume $0 < t < b$.

Now use Theorem 3.2 to compare the Galois structure of ideals in N_1 and in N_2, and one notices something remarkable. The Galois structure of each ideal in N_2 is precisely the same as the Galois structure of the corresponding ideal in N_1 if $t < b/2$ or $2b - t > 2e_0$. Thus, if the ramification number t of $K(z)/K$ is sufficiently small (relative to b), each ideal of N_2 has the same Galois module structure as the corresponding ideal of N_1, whereas for larger values of t this is not the case. We would like to thank the referee for pointing out that we may view N_2 as the quadratic twist of N_1 associated with the extension $K(z)/K$, and for suggesting the following more general question:

Question 4.1 Given a representation V of $\mathrm{Gal}(\bar{K}/K)$ with fixed field N_1, and a one-dimensional character χ of $\mathrm{Gal}(\bar{K}/K)$, such that the twist $V \otimes \chi$ of V by χ has isomorphic image to V, how is the Galois module structure of ideals in the fixed field N_2 of $V \otimes \chi$ related to that of ideals in N_1? In particular, if χ is, in some appropriate sense, "not too highly ramified" (relative to V), will the ideals of N_1 and N_2 have "the same" Galois module structure?

References

[Eld98] G. G. Elder, *Galois module structure of ideals in wildly ramified biquadratic extensions*. Canad. J. Math. (5) **50**(1998), 1007–1047.

[Naz61] L. A. Nazarova, *Integral representations of Klein's four-group*. Soviet Math. Dokl. **2**(1961), 1304–1307.
[Naz67] ———, *Representation of a Tetrad*. Math. USSR-Izv. (6) **1**(1967), 1305–1321.
[Ser79] J-P. Serre, *Local fields*. Springer-Verlag, New York, 1979.

School of Mathematical Sciences
University of Exeter
Exeter EX4 4QE
United Kingdom
e-mail: N.P.Byott@exeter.ac.uk

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

https://doi.org/10.4153/CMB-2002-020-3 Published online by Cambridge University Press