*Journal de Théorie des Nombres*
*de Bordeaux* **19** (2007), 101–124

# On wild ramification in quaternion extensions

par G. Griffith ELDER et Jeffrey J. HOOPER

Résumé. Cet article fournit un catalogue complet des nombres de ramification qui se produisent dans la filtration de ramification des extensions totalement ramifiées des corps de nombres dyadiques qui contiennent $\sqrt{-1}$, et dont le groupe Galois est isomorphe au groupe des quaternions (avec quelques résultats partiels dans le cas plus général). Ce catalogue dépend d'un *rafinement* de la filtration de ramification. Cette filtration était definie dans [2] comme associée au sous-corps biquadratique. En outre, nous montrons que les contre-exemples de type quaternion aux conclusions du théorème de Hasse-Arf sont extrêmement rares et ne peuvent se produire que seulement dans le cas où la filtration raffinée de ramification est extrême dans deux directions distinctes.

Abstract. This paper provides a complete catalog of the break numbers that occur in the ramification filtration of fully and thus wildly ramified quaternion extensions of dyadic number fields which contain $\sqrt{-1}$ (along with some partial results for the more general case). This catalog depends upon the *refined ramification filtration*, which as defined in [2] is associated with the biquadratic subfield. Moreover we find that quaternion counter-examples to the conclusion of the Hasse-Arf Theorem are extremely rare and can occur only when the refined ramification filtration is, in two different ways, extreme.

## 1. Introduction

Quaternion extensions are often the smallest extensions to exhibit special properties and have played an important role in Galois module structure [8]. In the setting of the Hasse-Arf Theorem, they are used to illustrate the fact that upper ramification numbers in a non-abelian extension need not be integers [13, IV§3 Exercise 2]. To better understand the counter-examples to the conclusion of the Hasse-Arf Theorem and as a first step towards an explicit description of wildly ramified Galois module structure

Manuscrit reçu le 11 septembre 2005.
Elder was partially supported by NSF grant DMS-0201080, Hooper was partially supported by NSERC.

(*e.g.* [1, 3, 4, 5]), we catalog the ramification break numbers of totally ramified quaternion extensions of dyadic number fields.

**1.1. Notation.** Let $\mathbb{Q}_2$ be the field of dyadic numbers, and let $K/\mathbb{Q}_2$ be a finite extension with $T$ its maximal unramified subfield. Then $e_K = [K : T]$ is its degree of absolute ramification and $f_K = [T : \mathbb{Q}_2]$ is its degree of inertia. We will continue to use subscripts to denote field of reference. So $\pi_K$ is a prime element in $K$, $\mathfrak{O}_K$ the ring of integers, $\mathfrak{P}_K = \pi_K \mathfrak{O}_K$ its maximal ideal, and $v_K(\cdot)$ the valuation normalized so that $v_K(\pi_K^n) = n$ for $n \in \mathbb{Z}$. By abuse of notation, we identify the residue fields $\mathfrak{O}_K/\mathfrak{P}_K = \mathfrak{O}_T/\mathfrak{P}_T = \mathbb{F}_q$ with the finite field of $q = 2^{f_K}$ elements.

Let $N/K$ be a fully ramified quaternion extension with

$$G = \mathrm{Gal}(N/K) = \left\langle \sigma, \gamma \mid \sigma^2 = \gamma^2, \gamma^{-1}\sigma\gamma = \sigma^{-1} \right\rangle .$$

It is a quick exercise to check that these relations, $\sigma^2 = \gamma^2$ and $\gamma^{-1}\sigma\gamma = \sigma^{-1}$, yield $\sigma^4 = 1$. Recall the ramification filtration $G_i = \{s \in G : v_N((s-1)\pi_N) \geq i+1\}$ and that *break numbers* (or jump numbers) are those integers $b$ such that $G_b \supsetneq G_{b+1}$ [13, ChIV].

Since $\mathrm{Gal}(N/K)$ has a unique subgroup of order 2, namely $\langle \sigma^2 \rangle$, and since the quotient of consecutive ramification groups (in a fully ramified $p$-extension) is necessarily elementary abelian [13, IV §2 Prop 7 Cor 3], the ramification filtration for $N/K$ decomposes naturally into two filtrations: one for $M/K$ where $M = N^{\langle \sigma^2 \rangle}$, and one for $N/M$. Indeed the ramification break for $N/M$ is the largest ramification break for $N/K$ [13, IV §1 Prop 2]. The other break(s) for $N/K$ are those of $M/K$ [13, IV §1 Prop 3 Cor]. This suggests

**Question 1.** How does ramification above (*i.e.* in $N/M$) depend upon ramification below (*i.e.* in $M/K$)?

**1.2. On ramification in biquadratic extensions.** There are either one or two break numbers in the ramification filtration for the quotient group $\overline{G} = \mathrm{Gal}(M/K)$. In the one break case, the break satisfies $1 \leq b < 2e$ with $b$ odd. In the two break case, the breaks $b_1 < b_2$ satisfy $1 \leq b_1 < 2e$ with $b_1$ odd, and $b_1 < b_2 \leq 4e - b_1$ with $b_2 \equiv b_1 \bmod 4$ when $b_2 < 4e - b_1$. This follows by considering upper ramification numbers and the Herbrand Function [13, IV§3].

Let $b_3$ denote the break for $\mathrm{Gal}(N/M)$. Then from §1.1 we see that the ramification breaks for $G$ are either $b < b_3$ or $b_1 < b_2 < b_3$. To give a complete description of $b_3$ in the one break case, $b < b_3$, we will need information provided by the refined ramification filtration [2]. This is discussed in detail as part of §3, so for now we simply summarize the main results: (1) There is a refined second break number $r \in \mathbb{Z}$, which satisfies $b < r < b_3$. (2) Associated with this second refined break number is a

$(q-1)$st root of unity $\omega$ (actually an equivalence class, but for the moment it does no harm to confuse the equivalence class with its representative).

As a result, to any fully ramified quaternion extension of $N/K$ we can assign a ramification triple: either $(b, r, b_3)$ in the one break case or $(b_1, b_2, b_3)$ in the two break case. We are interested in cataloging these triples. There are three cases to consider. Indeed the set of fully ramified quaternion extensions of $K$ can be partitioned as $\mathcal{Q}_{1^*}^K \cup \mathcal{Q}_1^K \cup \mathcal{Q}_2^K$.

- If $M/K$ has one ramification break $b$, then there is a second refined break $r$ along with an associated root of unity $\omega$.
  - If $\omega^3 = 1$, we place $N$ in $\mathcal{Q}_{1^*}^K$.
  - If $\omega^3 \neq 1$, we place $N$ in $\mathcal{Q}_1^K$.
- If $M/K$ has two ramification breaks $b_1 < b_2$, then we place $N$ in $\mathcal{Q}_2^K$.

**1.3. Catalogs of triples: subsets of $\mathbb{Z}^3$.** In this section, based upon a choice of positive integer $e$, we define three sets of triples $\mathcal{R}_i^e \subset \mathbb{Z}^3$ with $i \in \{1, 1^*, 2\}$, whose elements will be denoted by $(s_1, s_2, s_3)$. In our descriptions of these sets, the values of a coordinate $s_j$ will, in each case, depend upon the values of preceding coordinates ($s_h$ for $h < j$). So we begin by describing the first coordinates. In all cases

$$s_1 \in S_1 = \{n \in \mathbb{Z} : 0 < n < 2e, n \equiv 1 \bmod 2\}.$$

To describe $s_2$, we must consider two basic cases: $i \in \{1^*, 1\}$ and $i = 2$. Let

$$m_i(s_1) = \begin{cases} \min\{2s_1, 4e - s_1\} & \text{for } i = 1^*, 1, \\ 4e - s_1 & \text{for } i = 2. \end{cases}$$

Then

$$s_2 \in S_2^i(s_1) = \{n \in \mathbb{Z} : s_1 < n \leq m_i(s_1), n \equiv s_1 \bmod 4 \text{ if } n < m_i(s_i)\}.$$

Observe that since $m_1(s_1) \leq m_2(s_1)$, $S_2^1(s_1) \subseteq S_2^2(s_1)$.

We now turn to the description of the third coordinate $s_3$. There are three cases: $i = 1, 1^*$ and 2. We should also point out that in each case, our description will break naturally into two parts. Borrowing terminology from Wyman [15], there is *stable ramification* when $s_3$ is uniquely determined by $s_1$ and $s_2$, and there is *unstable ramification* when it is not.

We begin by describing $s_3$ under unstable ramification. In each case, there are lower and upper bounds

$$L_i = \begin{cases} 7s_1 - 2s_2 & \text{for } i = 1^*, \\ 5s_1 & \text{for } i = 1, \\ 2s_1 + 3s_2 & \text{for } i = 2, \end{cases} \qquad U_i = \begin{cases} 8e - 3s_1 & \text{for } i = 1^*, 1, \\ 8e - 2s_1 - s_2 & \text{for } i = 2. \end{cases}$$

Notice that $L_{1^*} \leq L_1 \leq L_2$ and $U_2 \leq U_{1^*} = U_1$ (with equality everywhere, if we formally equate $s_1 = s_2$). When there is room between the lower and upper bounds, namely $L_i < U_i$, we have unstable ramification and

$$s_3 \in {}^u\!S_3^i(s_1, s_2) = \{n \in \mathbb{Z} : L_i \leq n \leq U_i, s_3 \equiv s_i \bmod 8 \text{ if } L_i < n < U_i\}.$$

Note that in the description of ${}^u\!S_3^i(s_1, s_2)$, "$s_3 \equiv s_i \bmod 8$" means $s_3 \equiv s_2 \bmod 8$ for $i = 2$ and $s_3 \equiv s_1 \bmod 8$ for $i = 1, 1^*$. Note furthermore that the condition $L_i < U_i$, means $5s_1 - s_2 < 4e$ for $i = 1^*$, $s_1 < e$ for $i = 1$ and $s_1 + s_2 < 2e$ for $i = 2$. Outside of this condition, when $L_i \geq U_i$, we have ${}^u\!S_3^i(s_1, s_2) = \emptyset$ and stable ramification:

$$s_3 = 4e + \begin{cases} s_i & \text{for } i = 1, 2, \\ 2s_1 - s_2 & \text{for } i = 1^*, \end{cases}$$

which, of course, defines a set ${}^s\!S_3^i(s_1, s_2)$ for each $i \in \{1, 1^*, 2\}$. Naturally, we set ${}^s\!S_3^i(s_1, s_2) = \emptyset$ for $L_i < U_i$, and thus in all cases $s_2 \in S_3^i(s_1, s_2)$ with partition $S_3^i(s_1, s_2) = {}^u\!S_3^i(s_1, s_2) \cup {}^s\!S_3^i(s_1, s_2)$.

In summary, we have defined three sets, $\mathcal{R}_{1^*}^e, \mathcal{R}_1^e, \mathcal{R}_2^e$:

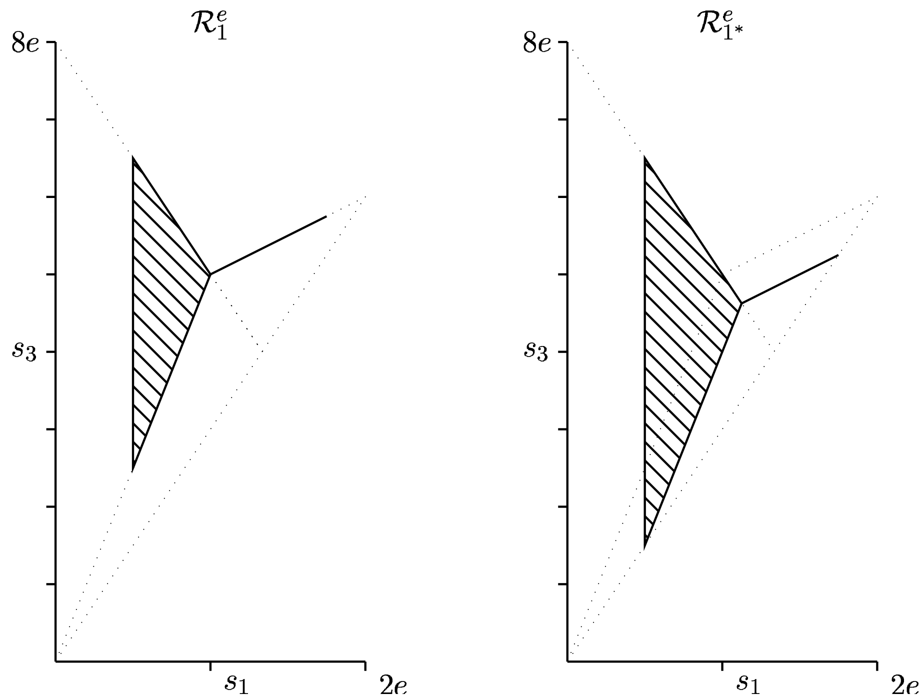
$$\mathcal{R}_i^e = \left\{(s_1, s_2, s_3) \in \mathbb{Z}^3 : s_1 \in S_1, s_2 \in S_i(s_1), s_3 \in S_3^i(s_1, s_2)\right\}.$$

Our interest in these sets is largely due to our interest in counter-examples to the conclusion of Hasse-Arf. By a result of Fontaine [7, Prop 4.5], we know that such counter-examples can occur only in the one break case. So we focus now on $\mathcal{R}_{1^*}^e, \mathcal{R}_1^e$. We are principally interested in the relationship between $s_1$ and $s_3$, which as we might suspect from §1.2 corresponds to the two (usual) ramification breaks in a quaternion extension. To provide a two dimensional visual aid, we slice now each of $\mathcal{R}_1^e, \mathcal{R}_{1^*}^e$ by the hyperplane $s_2 - s_1 = e/2$, and project each slice to the $(s_1, s_3)$-plane (with axes scaled 1–2). The result (sketched below) includes a line segment (representing stable ramification) along with a triangular region (representing unstable ramification). To aid comparison, we have included certain dotted segments of the lines $s_3 = 3s_1$, $s_3 = 5s_1$, $s_3 = s_1 + 4e$ and $s_3 = 8e - 3s_1$ in both sketches. Note that since the upper bound for $s_2$, namely $\min\{2s_1, 4e - s_1\}$ depends upon whether or not $s_1 \leq 4e/3$, the hyperplane $s_2 - s_1 = e/2$ intersects $\mathcal{R}_1, \mathcal{R}_1^*$ only for $e/2 \leq s_1 \leq 7e/4$.

**1.4. Statement of main results.** Given a base field $K$, there is a map that sends each fully ramified quaternion extension $N/K$ to its ramification triple, either $(b_1, b_2, b_3)$ or $(b, r, b_3) \in \mathbb{Z}^3$ depending upon the filtration in its biquadratic subfield $M/K$. A catalog of such ramification triples should be considered complete if

(1) the range of this map is given an explicit description, and
(2) the map is also shown to be onto this range.

Using this definition, the catalog of ramification triples that we give below is complete for fields $K$ that contain the 4th roots of unity, namely $\sqrt{-1} \in K$.




To state our results, we recall, from §1.2, the partition of the set fully ramified quaternion extensions of $K$ into three sets: $\mathcal{Q}_{1^*}^K, \mathcal{Q}_1^K, \mathcal{Q}_2^K$. We also recall, from §1.3, the three ranges (subsets of $\mathbb{Z}^3$): $\mathcal{R}_{1^*}^e, \mathcal{R}_1^e, \mathcal{R}_2^e$.

**Theorem 1.1.** *If $\sqrt{-1} \in K$ and $N/K$ is a fully ramified quaternion extension, so $N \in \mathcal{Q}_i^K$ for some $i \in \{1, 1^*, 2\}$. Then its ramification triple, either $(b, r, b_3)$ or $(b_1, b_2, b_3)$, lies in $\mathcal{R}_i^{e_K}$, where $e_K$ denotes the absolute ramification of $K$.*

*Moreover, given $K/\mathbb{Q}_2$ with $\sqrt{-1} \in K$ and any triple $(s_1, s_2, s_3) \in \mathcal{R}_i^{e_K}$ where $i \in \{1, 1^*, 2\}$, there is a fully ramified quaternion extension $N/K$ with $N \in \mathcal{Q}_i^K$ whose ramification triple is $(s_1, s_2, s_3)$.*

**Theorem 1.2.** *If $\sqrt{-1} \notin K$ and $N/K$ is a fully ramified quaternion extension with $N \in \mathcal{Q}_1^K \cup \mathcal{Q}_2^K$ and a stable ramification triple, either $(b, r, b_3)$ with $b > e_K$ or $(b_1, b_2, b_3)$ with $b_1 + b_2 > 2e_K$, then its ramification triple lies in $\mathcal{R}_i^{e_K}$, where $e_K$ denotes the absolute ramification of $K$.*

Notice, when $\sqrt{-1} \notin K$, that our results are not complete[1]. Theorem 1.2 does not address condition (2). It also does not address condition (1) in the following situations: (i) Case 1*, (ii) the unstable situation $b \leq e_K$ in Case 1, (iii) the unstable situation $b_1 + b_2 \leq 2e_K$ in Case 2.

**1.5. Hasse-Arf.** The Hasse-Arf Theorem states that upper ramification numbers in abelian extensions are integers. Our results confirm a result of Fontaine, which says that in quaternion extensions upper ramification numbers generally are integers.

**Theorem 1.3** ([7, Prop 4.5]). *Upper ramification numbers of fully ramified quaternion extensions of dyadic number fields are integers, except when there is only one break $b$ for $M/K$ and $b_3 = 3b$.*

Note that the upper ramification numbers in a quaternion extension are integers precisely when $b_3 \equiv b_2$ (or $b$) mod 4 [13, IV§3]. Using Theorem 1.1 and the descriptions for $\mathcal{R}_i^e$ in §1.3, we see that if $\sqrt{-1} \in K$ the exceptional situation $b_3 = 3b$ *can occur* only when both the second refined break is *maximal*: $r = \min\{4e_K - b, 2b\}$, and its associated root of unity $\omega$ is *minimal*: $\omega^3 = 1$. If there is stable ramification, so $r = 4e_K - b$, the exceptional situation $b_3 = 3b$ *must occur*.

## 2. Embeddability and quadratic defects

In 1936 E. Witt characterized the biquadratic extensions $M = K(\sqrt{u}, \sqrt{v})$ that embed in a quaternion extension [14]. When $K$ is a finite extension of $\mathbb{Q}_2$, his condition is equivalent to the Hilbert symbol equality: $(-u, -v) = (-1, -1)$, which is equivalent to the product formula $(-1, u)(-1, v)(u, v) = 1$.

If the product formula holds then, replacing $u$ or $v$ with $uv$ if necessary and using Hilbert symbol properties, we may assume without loss of generality that $(u, v) = 1$ and $(uv, -1) = 1$. As a result, when $M$ embeds in a quaternion extension, we may assume that there are two elements $\eta \in K(\sqrt{u})$ and $\tau \in K(\sqrt{uv})$ whose norms satisfy $N_{K(\sqrt{u})/K}(\eta) = v$ and $N_{K(\sqrt{uv})/K}(\tau) = -1$.

An observation of H. Reichardt then characterizes the quaternion extensions $N/K$ that contain $M$: for if we let $\alpha_k \in M$ be defined by

$$\alpha_k = k \cdot \sqrt{uv} \cdot \eta \cdot \begin{cases} 1 & i = \sqrt{-1} \in K \\ \tau & i = \sqrt{-1} \notin K \end{cases}$$

[1] Assumptions on the roots of unity in the base field are common in ramification theory. For example, the ramification break number $b$ of a ramified $C_p$-extension $L/K$ of local number fields with residue characteristic $p$, satisfies $1 \leq b \leq pe_K/(p-1)$ with the additional condition that $\gcd(b, p) = 1$ for $b < pe_K/(p-1)$. But the case $b = pe_K/(p-1)$ is possible only when $K$ contains a $p$th root of unity [6, III§2 Prop 2.3]. As a further example, note that [15, Thm 32] concerning $C_{p^2}$-extensions is proven under the assumption that the base field contains the $p$th roots of unity.

where $k \in K^*$ and $N = M(\sqrt{\alpha_k})$, then $N/K$ is a quaternion extension [12]. Moreover it is generic in the sense that any quaternion extension of $K$ containing $M$ can be expressed as $M(\sqrt{\alpha_k})$ for some $k \in K$. Jensen and Yui provide a nice source for these results. Indeed Witt's condition [10, Lem I.1.1] can be translated to the Hilbert symbol condition using [10, Lem I.1.6], and Reichardt's observation appears as [10, Lem I.1.2].

**2.1. Quadratic extensions and quadratic defect.** Let $F$ denote a finite extension of $\mathbb{Q}_2$, and let $T_F$ be its maximal unramified subfield. As is well-known, a vector space basis for $F^*/(F^*)^2$ over $\mathbb{F}_2$ is given by $\{1 + a\pi_F^{2n-1} : a \in \mathfrak{O}_{T_F}/2\mathfrak{O}_{T_F}, 1 \leq n \leq e_F\}$ along with $\pi_F$ and $1 + 4\lambda$ for some $\lambda \in \mathfrak{O}_{T_F}$ with $x^2 + x + \lambda$ irreducible over $T_F$, [9, Ch15]. It is easy to check that $F(\sqrt{1 + 4\lambda})/F$ is unramified. This means that there are essentially two types of ramified quadratic extensions: those that arise from the square root of a prime, $F(\sqrt{\pi_F})$, and those that arise from the square root of a one-unit, $F(\sqrt{u})$ with $u = 1 + \beta$ and $0 < v_F(\beta) < 2e_F$ odd. Define the defect in $F$ of a prime element to be $\mathrm{def}_F(\pi_F) = 0$ and of a unit to be $\mathrm{def}_F(u) = \max\{v_F(k^2u - 1) : k \in F\}$ [11, §63A]. If $u = 1 + \beta$ as above, $\mathrm{def}_M(1 + \beta) = v_F(\beta)$. It is straightforward now to verify that the ramification number of $F(\sqrt{\kappa})/F$ (for $\kappa \in F^* \setminus (F^*)^2$) is tied to the defect of $\kappa$ by $b = 2e_F - \mathrm{def}_F(\kappa)$. (All this is generalized to include odd primes $p$ in [15, §4].)

Recall Question 1. Given a quaternion extension $N/K$, we are interested in determining $b_3$, the ramification break for the quadratic extension $N/M$, which is tied to the quadratic defect of $\alpha_k$ in $M$ by

$$b_3 = 8e_K - \mathrm{def}_M(\alpha_k).$$

Indeed we will determine $b_3$ by determining $\mathrm{def}_M(\alpha_k)$. Recall that $\alpha_k$ is a product: either $k \cdot \sqrt{uv} \cdot \eta$ or $k \cdot \sqrt{uv} \cdot \eta \cdot \tau$ depending upon whether $\sqrt{-1} \in K$ or not. It is easy to see that $\mathrm{def}_M(A \cdot B) \geq \min\{\mathrm{def}_M(A), \mathrm{def}_M(B)\}$ for $A, B \in M$, and that we can be certain of equality only when $\mathrm{def}_M(A) \neq \mathrm{def}_M(B)$. The technical work in this paper addresses two issues: (1) The terms in $\alpha_k$ lie in proper subfields of $M$. As a result, the defect in $M$ of each term is not immediately obvious from its expression. (2) Moreover, once the defect of each term has been determined, there are often at least two terms with the same defect.

**2.2. Three technical lemmas.** If $E/F$ is a ramified quadratic extension and $\kappa \in F$, then $\mathrm{def}_E(\kappa) > \mathrm{def}_F(\kappa)$. To describe this increase in valuation carefully, we need to define the following continuous increasing function.

$$g_{F,b}(x) = \min\{2x + b, x + 2e_F\} = \begin{cases} 2x + b & \text{for } x \leq 2e_F - b, \\ x + 2e_F & \text{for } x > 2e_F - b. \end{cases}$$

**Lemma 2.1.** *Let $E/F$ be a ramified quadratic extension with break number $b$ odd. If $\kappa \in F^* \setminus (E^*)^2$, then*

$$\mathrm{def}_E(\kappa) \geq g_{F,b}(\mathrm{def}_F(\kappa))$$

*with equality when $\mathrm{def}_F(\kappa) \neq 2e_F - b$. As a result, given a threshold value $\delta \geq 0$ with $\mathrm{def}_F(\kappa) \geq \delta$, then $\mathrm{def}_E(\kappa) \geq g_{F,b}(\delta) \geq b$.*

*Proof.* Since $\kappa \notin (E^*)^2$, $E(\sqrt{\kappa})/F$ is a biquadratic extension. The break number of $F(\sqrt{\kappa})/F$ is $2e_F - \mathrm{def}_F(\kappa)$. Passing to the upper numbering for the filtration of $E(\sqrt{\kappa})/F$ [13, ChIV§3], we see that the break number for $E(\sqrt{\kappa})/E$ is

$$\begin{array}{ll} 4e_F - 2\mathrm{def}_F(\kappa) - b & \text{for } 2e_F - \mathrm{def}_F(\kappa) > b\,; \\ 2e_F - \mathrm{def}_F(\kappa) & \text{for } 2e_F - \mathrm{def}_F(\kappa) < b\,; \\ \leq b & \text{for } 2e_F - \mathrm{def}_F(\kappa) = b\,. \end{array}$$

As a result,

$$\mathrm{def}_E(\kappa) = \begin{cases} 2\mathrm{def}_F(\kappa) + b & \text{for } 2e_F - \mathrm{def}_F(\kappa) > b\,; \\ 2e_F + \mathrm{def}_F(\kappa) & \text{for } 2e_F - \mathrm{def}_F(\kappa) < b\,; \\ \geq 4e_F - b & \text{for } 2e_F - \mathrm{def}_F(\kappa) = b\,. \end{cases}$$

The result follows. □

Given two elements of known defect, can one be described in terms of another?

**Lemma 2.2.** *Given $\beta \in F$ with $v_F(\beta) = 2e_F - b$ and $0 < b < 2e_F$ odd. If $\kappa \in 1 + \mathfrak{P}_F$ and $\mathrm{def}_F(\kappa) = 2e_F - a$ with $0 < a \leq b$, there is a $\mu \in \mathfrak{O}_F$ with $v_F(\mu) = (b-a)/2$ and a $\lambda \in \mathfrak{O}_{T_F}$, either $0$ or so that $z^2 + z = \lambda$ is irreducible over $T_F$, such that*

$$\kappa = (1 + \mu^2\beta)(1 + 4\lambda) \in (1 + \mathfrak{P}_F)/(1 + \mathfrak{P}_F)^2.$$

*Proof.* Clearly $\kappa = (1+\mu_0^2\beta)(1+\mu_1^2\beta)(1+\mu_2^2\beta)\cdots(1+4\lambda) \in (1+\mathfrak{P}_F)/(1+\mathfrak{P}_F)^2$ for some $\mu_i \in \mathfrak{O}_F$ with $(b-a)/2 = v_F(\mu_0) < v_F(\mu_1) < v_F(\mu_2) < \cdots$. Now use $(1+\mu_0^2\beta)(1+\mu_1^2\beta) \equiv 1 + (\mu_0+\mu_1)^2\beta \bmod \mu_1^2\beta\mathfrak{P}_F$ repeatedly. □

And finally, what is the defect of the norm of an element?

**Lemma 2.3.** *Let $E/F$ be a ramified quadratic extension with break number $b$ odd and let $N_{E/F}$ denote the norm. Given $\alpha_E \in E$ with $\mathrm{def}_E(\alpha_E) = a < \infty$ and $a \notin \{b, 2e_E\}$, then $\mathrm{def}_F(N_{E/F}(\alpha_E)) = \varphi(a)$ where $\varphi(x)$ is the Herbrand function*

$$\varphi(x) = \begin{cases} x & \text{for } x < b, \\ (x+b)/2 & \text{for } x \geq b. \end{cases}$$

*If $a = 2e_E$ then $\mathrm{def}_F(N_{E/F}(\alpha_E)) = \infty$. Since the kernel of $N_{E/F}$ contains elements of defect $b$, if $a = b$, we may also have $\mathrm{def}_F(N_{E/F}(\alpha_E)) = \infty$. If however $a = b$ and $\mathrm{def}_F(N_{E/F}(\alpha_E)) < \infty$, then $\mathrm{def}_F(N_{E/F}(\alpha_E)) = b$.*

*Moreover, given $\alpha_F \in F$ with $v_F(\alpha_F - 1) = c > b$, then there is a $\alpha_E \in E$ with $v_E(\alpha_E - 1) = 2c - b$ such that $N_{E/F}(\alpha_E) = \alpha_F$.*

*Proof.* All this follows from [13, V§3]. □

## 3. One break biquadratic extensions

Let $M/K$ be a fully ramified biquadratic extension which has only one ramification break, at $b$. In this case the ramification numbers for each of the three subfields must be the same. Using Lemma 2.2, there must be a $\beta \in K$ with $v_K(\beta) = 2e_K - b$; a nontrivial $2^{f_K} - 1 = (q-1)$st root of unity $\omega \in \mathfrak{O}_T$; a $\mu \in K$ where either $\mu = 0$ or $v_K(\mu) = m$ with $0 < m < b/2$; and a $\lambda \in K$ where either $\lambda = 0$ or $\lambda$ is a $(q-1)$st root of unity with $z^2 + z = \lambda$ irreducible over $T$; such that $M = K(x, y)$ where

$$x^2 = 1 + \beta,$$
$$y^2 = \left(1 + (\omega + \mu)^2 \beta\right)(1 + 4\lambda).$$

Without loss of generality, we let $\sqrt{u} = x$ and $\sqrt{v} = y$, and for the remainder of this section set $L = K(x)$. Note that because $N_{L/K}(x - 1) = -\beta$ and $v_K(\beta) = 2e_K - b$, we must have $v_L(x - 1) = 2e_K - b$. We let $\overline{G} = \mathrm{Gal}(M/K) = \langle \sigma, \gamma \rangle$ where the generators act by $\sigma x = x$ and $\gamma y = y$. (It should cause no confusion that we use $\sigma, \gamma$ to denote both the generators of the quaternion group $G$ and its $C_2 \times C_2$ quotient group $\overline{G}$.)

Before we turn to the refined ramification filtration, notice that the extension $M/L$ is quadratic with break $b$. As a result, there should be a unit $U \in M$ of defect $\mathrm{def}_M(U) = 4e_K - b$ such that $M = L(U)$. Motivated by an identity in $\mathbb{Q}(A, X)$,

$$(1) \quad (1 + A(X-1))^2 = (1 + A^2 B)\left(1 + 2(A - A^2)(X-1)\frac{1}{1 + A^2 B}\right),$$

where $B = X^2 - 1$, we choose $Y \in M$ so that

$$(2) \qquad yY = 1 + (\omega + \mu)(x - 1) \in L.$$

Now using (1) with $X = x$, $B = \beta$, and $A = \omega + \mu$, we find that

$$(3) \quad Y^2 = \left(1 + 2((\omega+\mu) - (\omega+\mu)^2)(x-1)\frac{1}{1 + (\omega+\mu)^2\beta}\right)(1 + 4\lambda)^{-1}.$$

As a result, by applying the norm $N_{M/L}(Y - 1) = 1 - Y^2$ where $v_L(1 - Y^2) = 4e_K - b$. Thus $v_M(Y - 1) = 4e_K - b$. So $Y$ is our desired unit, and $M = L(Y)$ with $\sigma Y = -Y$.

**3.1. The second refined break and its associated root of unity.** When there is only one ramification break, all Galois action "looks" the same from the perspective of the usual ramification filtration. Thus the necessity of a *refined ramification filtration*, which helps us "see" a difference. As an aid to the reader, we replicate some of the material from [2], restricting to $p = 2$, so that many of the details are simpler.

Let $J = (\sigma - 1, \gamma - 1)$ be the Jacobson radical of $\mathbb{F}_q[\overline{G}]$. Define an $\mathbb{F}_q$-'action' on the one-units $1 + J$ by the map

$$(a, 1 + x) \in \mathbb{F}_q \times (1 + J) \longrightarrow x^{[a]} := 1 + ax \in 1 + J.$$

This makes $1 + J$ a near space over $\mathbb{F}_q$ with all the properties of a vector space, except that scalar multiplication does not necessarily distribute: It is possible to find $x, y \in J$ and $a \in \mathbb{F}_q$ so that $((1 + x)(1 + y))^{[a]}(1 + x)^{[-a]}$ $(1+y)^{[-a]} = 1+(a^2+a)xy \neq 1$. We do not have a proper action. To achieve one and create a vector space, we deviate slightly from [2] and define

$$\overline{G}^{\mathcal{F}} := (1 + J)/(1 + J^2).$$

It is straightforward to check that this vector space over $\mathbb{F}_q$ has basis $\{\sigma, \gamma\}$.

To define a ramification filtration for $\overline{G}^{\mathcal{F}}$, choose any element $\rho \in M$ with valuation $v_M(\rho) = b$, and define, for $s \in \overline{G}^{\mathcal{F}}$, $w_\rho(s) = \max\{v_M((\tilde{x} - 1)\rho) : \tilde{x} \in \mathfrak{O}_T[\overline{G}], x = \tilde{x} + 2\mathfrak{O}_T[\overline{G}], x \in \mathbb{F}_q[\overline{G}], s = x(1 + J^2)\}$, and the refined ramification groups by

$$\overline{G}_i^{\mathcal{F}} = \{s \in \overline{G}^{\mathcal{F}} : w_\rho(s) - v_M(\rho) \geq i\}.$$

For example, we will use $\rho = 2/(Y - 1)$. If we replace $y^2$ with $(\omega^{-1}y)^2 = (\omega^{-2} + \beta)(1 + \mu^2\beta) \bmod \mu^2\beta\mathfrak{P}_K$, then we have notation (including $\sigma, \gamma$ as generators of the Galois group) exactly as in [2, §4.1]. As a result, we can apply [2, Prop4.2] and find that

$$v_M((\gamma\sigma^{[\omega]} - 1)\rho) = v_M(\rho) + r$$

where $r = \min\{4e_K - b, b + 4m, 2b\}$. Thus there are two breaks in the refined filtration: namely $b < r$ with $\overline{G}_b^{\mathcal{F}} \supsetneq \overline{G}_{b+1}^{\mathcal{F}}$ and $\overline{G}_r^{\mathcal{F}} \supsetneq \overline{G}_{r+1}^{\mathcal{F}}$, where the *second refined break* satisfies $r \leq \min\{2b, 4e_k - b\}$ and away from this upper bound satisfies $r \equiv b \bmod 4$. These breaks are independent of our choices: of $\rho$ and of the generators for $\overline{G}$.

Additionally, the second refined break $r$ is associated with a root of unity, namely $\omega$, which does depends upon our choice of generators for $\overline{G}$. Replace $\gamma$ by $\gamma\sigma$ and we have an alternative root of unity $\equiv \omega + 1 \bmod 2$. Indeed these are the only two roots of unity that arise from a change of generators for $\mathrm{Gal}(M/K)$. This suggests an equivalence relation on nontrivial $(q - 1)$st roots of unity: $\omega \sim \omega'$ if and only if $\omega \equiv \omega'$ or $\omega' + 1 \bmod 2$. If we identify these nontrivial $(q - 1)$st roots of unity with their images in $\mathbb{F}_q \setminus \mathbb{F}_2$, then the equivalence classes of this relation can be identified with the $q/2-1$ nontrivial additive cosets of $\mathbb{F}_q/\mathbb{F}_2$. Thus the second refined break $r$ is actually associated with an equivalence class of two $(q-1)$st roots of unity. We are going to be interested in whether the elements of a particular equivalence class satisfy a condition: whether they both are nontrivial cube roots of unity. So it is worth pointing out that $\omega^2+\omega+1=0 \bmod 2$ if and only if $(\omega+1)^2+(\omega+1)+1 \equiv 0 \bmod 2$. As a result, in the statements of our results we can refer to "$r$ and its associated root of unity $\omega$" (equating each equivalence class with a representative). The condition $\omega^3=1$ is well-defined.

**Remark 1.** In the two break case, this refined ramification filtration produces the usual two ramification break numbers.

### 3.2. The determination of $\mathrm{def}_M(\alpha_k)$.

We begin with a lemma.

**Lemma 3.1.** *Let $M/K$ be a fully ramified biquadratic extension with one ramification break, at $b$. Then for all $k \in K$, $\mathrm{def}_M(k) \geq 3b$. In particular, $\mathrm{def}_M(\pi_K)=3b$. And if $k \in 1+\mathfrak{P}_K$ with $0<\mathrm{def}_K(k)<2e_K-b$, then $\mathrm{def}_M(k)=3b+4\mathrm{def}_K(k)$. So $3b<\mathrm{def}_M(k)<8e_K-b$ with $\mathrm{def}_M(k) \equiv -b \bmod 8$. Otherwise if $k \in 1+\mathfrak{P}_K$ with $2e_K-b \leq \mathrm{def}_K(k)$ then $\mathrm{def}_M(k) \geq 8e_K-b$.*

*Proof.* Apply Lemma 2.1 twice, once to $M/L$ and once to $L/K$ (where $L$ is one of the intermediate quadratic subfields). Note that for $0<\mathrm{def}_K(k)<2e_K-b$, $\mathrm{def}_K(k) \equiv b \bmod 2$, therefore $3b+4\mathrm{def}_K(k) \equiv 7b \bmod 8$. □

Now we assume that $M=K(x,y)$ embeds in a quaternion extension, that $x=\sqrt{u}, y=\sqrt{v}$, and adopting notation as in §2, we determine $\mathrm{def}_M(\alpha_k)$. Our analysis decomposes: Case 1 in §3.3 when $\omega^3 \neq 1$. and Case 1* in §3.4 when $\omega^3=1$. We begin with the easier case.

### 3.3. Case 1: Assume $\omega^3 \neq 1$.

Under this assumption there is both stable and unstable ramification. We begin with stable situation.

#### 3.3.1. *Stable ramification:* $b>e_K$.

We *do not* assume $\sqrt{-1} \in K$. It follows immediately from the following lemma that if $b>e_K$ then $b_3=4e_K+b$, the value given in the catalog in Section 1.3.

**Lemma 3.2.** *If $b>e_K$ and $\omega^3 \neq 1$, then $\mathrm{def}_M(\alpha_k)=4e_K-b$.*

*Proof.* Because of the possibility that $i=\sqrt{-1} \notin K$, we have $\alpha_k=kxy\eta\tau$. It suffices therefore to check that $\mathrm{def}_M(k \cdot yY\eta \cdot \tau)>4e_K-b$ and that $\mathrm{def}_M(xY)=4e_K-b$.

We prove the first statement, $\mathrm{def}_M(k \cdot yY\eta \cdot \tau)>4e_K-b$, by showing $\mathrm{def}_M(k)>4e_K-b$, $\mathrm{def}_M(yY\eta)>4e_K-b$ and $\mathrm{def}_M(\tau)>4e_K-b$. Using Lemma 3.1 and $b>e_K$, we have $\mathrm{def}_M(k) \geq 3b>4e_K-b$. The other two inequalities will follow from Lemma 2.1 if we can show $\mathrm{def}_L(yY\eta) > 2e_K - b$ and $\mathrm{def}_{K(xy)}(\tau) > 2e_K - b$, respectively. Recall that $L = K(x)$. We begin with $\mathrm{def}_L(yY\eta)$: Note that by (2), $yY \in L$ and by assuming $x = \sqrt{u}$, $\eta \in L$ as well. Now check, using $b > e_K$, that $N_{L/K}(1+\omega(x-1)) \equiv 1+\omega^2\beta \bmod \beta\mathfrak{P}_K$. Using Lemma 2.3, we see that $\eta \equiv 1+\omega(x-1) \bmod (x-1)\mathfrak{P}_L$. Hence using (2) we see that $\mathrm{def}_L(yY\eta) > 2e_K - b$. Finally consider $\mathrm{def}_{K(xy)}(\tau)$: Since $\mathrm{def}_K(-1) \geq e_K$ and $e_K < b$, we can use Lemma 2.3 and the fact that the Herbrand function $\varphi$ is increasing to see that $\mathrm{def}_{K(xy)}(\tau) \geq e_K > 2e_K - b$.

We prove the second statement, $\mathrm{def}_M(xY) = 4e_K - b$. Notice that $\mathrm{def}_M(Y) = v_M(Y-1) = 4e_K - b$ and that Lemma 2.1 gives $\mathrm{def}_M(x) = 4e_K - b$. This makes $\mathrm{def}_M(xY)$ difficult to determine, but also means that there is a unit $a \in \mathfrak{O}_K$ such that $x = 1 + a(Y-1)$ in $\mathcal{M} := (1+\mathfrak{P}_M)/[(1+\mathfrak{P}_M)^2(1+(Y-1)\mathfrak{P}_M)]$. We will have the desired conclusion if we can show $a \not\equiv 1 \bmod \mathfrak{P}_K$. Since $v_L(2) = 2e_K$ is even, there is a $\kappa \in L$ such that $\kappa^2 \equiv 2(\omega-\omega^2) \bmod 2\mathfrak{P}_L$. Using (1), we expand $(1+(1/\kappa)(Y-1))^2 = A\cdot B \bmod (Y-1)\mathfrak{P}_M$ where $A = 1+(Y^2-1)/\kappa^2 \in L$ and $B = 1+2(1/\kappa - 1/\kappa^2)(Y-1)$. This means that $A = B$ in $\mathcal{M}$. Since $(Y^2-1)/\kappa^2 \equiv (x-1) \bmod (x-1)\mathfrak{P}_L$, we see that $A = x\cdot C$ where $\mathrm{def}_L(C) > 2e_K - b$ and thus by Lemma 2.1, $\mathrm{def}_M(C) > 4e_K - b$. So $A = x$ in $\mathcal{M}$, and thus $x = B$ in $\mathcal{M}$. Notice that $B \equiv 1 - 2(Y-1)/\kappa^2 \equiv 1 + (\omega-\omega^2)^{-1}(Y-1) \bmod (Y-1)\mathfrak{P}_M$. This means that $x = 1+(\omega^2+\omega)^{-1}(Y-1)$ in $\mathcal{M}$. And because $\omega^3 \neq 1$, $(\omega^2+\omega)^{-1} \not\equiv 1 \bmod \mathfrak{P}_K$. □

**3.3.2.** ***Two preliminary results:*** For the remaining cases, we need two additional technical results. Define the following:

For $b < e_K$, (for use in §3.3.3)

$$\mathcal{L} = \frac{1+\mathfrak{P}_L}{(1+\mathfrak{P}_K)(1+\mathfrak{P}_L)^2(1+(\beta/2)(x-1)\mathfrak{P}_L)},$$
$$\mathcal{M} = \frac{1+\mathfrak{P}_M}{(1+\mathfrak{P}_K)(1+\mathfrak{P}_M)^2(1+(\beta/2)(Y-1)\mathfrak{P}_M)}.$$

For all $b$, (for use in §3.4)

$$\mathcal{L}^* = \frac{1+\mathfrak{P}_L}{(1+\mathfrak{P}_K)(1+\mathfrak{P}_L)^2(1+\beta\mathfrak{P}_L)},$$
$$\mathcal{M}^* = \frac{1+\mathfrak{P}_M}{(1+\mathfrak{P}_K)(1+\mathfrak{P}_M)^2(1+(x-1)(Y-1)\mathfrak{P}_M)}.$$

It is easy to see that, under $b < e_K$, the natural maps, $\mathcal{L}^* \to \mathcal{L}$ and $\mathcal{M}^* \to \mathcal{M}$, are surjective. Moreover, we can define defects with respect to these groups in the natural way. For example, for $\mu \in 1+\mathfrak{P}_M$, $\mathrm{def}_{\mathcal{M}^*}(\mu) = \max\{v_M(m-1) : m = \mu \in \mathcal{M}^*\}$. Note: We will regularly abuse notation by identifying a coset with one of its coset representatives.

**Lemma 3.3.** *The inclusions* $1+(\beta/2)(x-1)\mathfrak{P}_L \subseteq (1+\mathfrak{P}_M)^2(1+(\beta/2)(Y-1)\mathfrak{P}_M)$ *for* $b<e_K$, $1+\beta\mathfrak{P}_L \subseteq (1+\mathfrak{P}_M)^2(1+(x-1)(Y-1)\mathfrak{P}_M)$ *yield the following natural, well-defined maps:* $\mathcal{L}\to\mathcal{M}$ *defined for* $b<e_K$ *and* $\mathcal{L}^*\to\mathcal{M}^*$ *defined for all* $b$.

*Proof.* Use Lemma 2.1 to determine the two inclusions. □

**Lemma 3.4.** *For* $i=\sqrt{-1}\in K$, *the coset equality holds for all* $b$:

$Y=(1+i(\omega+\omega^2+\mu+\mu^2)(x-1))\cdot(1+(\omega+\omega^2)(x-1)(Y-1))\in\mathcal{M}^*.$

*Moreover for* $b<e_K$, $Y=(1+i(\omega+\omega^2+\mu+\mu^2)(x-1))\in\mathcal{M}$. *For* $b>e_K$, $Y=(1+(\omega+\omega^2+\mu+\mu^2)(x-1))\cdot(1+(\omega+\omega^2)(x-1)(Y-1))\in\mathcal{M}^*$.

*Proof.* Expand $(1+(Y-1)/(i-1))^2=1-(1+i)(Y-1)+i(Y-1)^2/2=1-(1+2i)(Y-1)+i(Y^2-1)/2\equiv Y+i(Y^2-1)/2 \bmod (x-1)(Y-1)\mathfrak{P}_M$, noting that $v_M(2(Y-1))>v_M((x-1)(Y-1))$. Factor $Y+i(Y^2-1)/2=A\cdot B$ with

$$A=\left(1+i\frac{Y^2-1}{2}\right)\in L,\qquad B=\left(1+(Y-1)\frac{1}{1+i\frac{Y^2-1}{2}}\right)\in M.$$

Each of $A$ and $B$ has a copy of $i(Y^2-1)/2$ that needs to be replaced. From (3) we have the approximation $(Y^2-1)/2\equiv(\omega+\omega^2+\mu+\mu^2)(x-1)-2\lambda \bmod \beta\mathfrak{P}_L$. So $A\equiv(1+i(\omega+\omega^2+\mu+\mu^2)(x-1))\cdot(1-2i\lambda) \bmod \beta\mathfrak{P}_L$. Because $b>e_K$ means $v_L((i-1)(x-1))>v_L(\beta)$, we can drop the first "$i$" in this expression when $b>e_K$. Thus we find that as elements of $\mathcal{L}^*$, and using Lemma 3.3, also as elements of $\mathcal{M}^*$,

$$A=\begin{cases}1+(\omega+\omega^2+\mu+\mu^2)(x-1) & \text{for } b>e_K,\\ 1+i(\omega+\omega^2+\mu+\mu^2)(x-1) & \text{for } b\le e_K.\end{cases}$$

We also have $i(Y^2-1)/2\equiv(\omega+\omega^2)(x-1) \bmod (x-1)\mathfrak{P}_L$, which yields $B\equiv Y\cdot(1+(\omega+\omega^2)(x-1)(Y-1)) \bmod (x-1)(Y-1)\mathfrak{P}_M$. So as elements of $\mathcal{M}^*$, we also have $B=Y\cdot(1+(\omega+\omega^2)(x-1)(Y-1))$. And by putting everything together, we get the result. □

**3.3.3.** ***Unstable ramification:*** $b\le e_K$. Assume that $i=\sqrt{-1}\in K$. Then $e_K$ must be even. But since $b$ is odd, this means that we are really assuming $b<e_K$.

In the following lemma we prove that if $i\in K$, $b<e_K$ and $\omega^3\ne1$, then $\mathrm{def}_{\mathcal{M}}(\alpha_1)=8e_K-5b$. Recall the definition of $\mathcal{M}$. Because $8e_K-5b=v_M((\beta/2)(Y-1))$, this means that there is a $k_0\in K$ such that $\mathrm{def}_M(\alpha_{k_0})=8e_K-5b$. Using Lemma 3.1 and in particular congruence considerations, we see that $\mathrm{def}_M(k)\ne 8e_K-5b$ for $k\in K^*$. As a result, $3b\le\mathrm{def}_M(\alpha_k)\le 8e_K-5b$, and $\mathrm{def}_M(\alpha_k)\equiv -b \bmod 8$ when $3b<\mathrm{def}_M(\alpha_k)<8e_K-5b$. The values for $b_3$ listed in the catalog in §1.3 follow immediately. Moreover, each of these values for $\mathrm{def}_M(\alpha_k)$ is realized.

**Lemma 3.5.** *If* $i \in K$, $b < e_K$ *and* $\omega^3 \neq 1$, *then* $\mathrm{def}_{\mathcal{M}}(xy\eta) = 8e_K - 5b$.

*Proof.* Recall that because $i \in K$ we have $\alpha_k = kxy\eta$. Since $v_M((\beta/2)(Y-1)) = 8e_K - 5b$, it is clear that our goal should be to find a unit $u \in M$ such that $xy\eta = 1 + u(\beta/2)(Y-1)$ as elements in $\mathcal{M}$. But since it is easier to work in $L$, we first find an equivalent expression in $\mathcal{L}$ for $x \cdot yY \cdot \eta \in L$. Then we use Lemma 3.4 to replace $Y$.

Note that because $b < e_K$, $v_K(\beta/2) = v_L((x-1)/(i-1) > 0$. Now for $X \in \mathfrak{O}_K$, expand $(1+(X/(i-1))(x-1))^2 = 1+iX^2\beta/2-[iX^2+X(1+i)](x-1)$, using $x^2 = 1+\beta$. Factor out $1+iX^2\beta/2 \in 1+\mathfrak{P}_K$. The result

$$(4) \qquad 1+\frac{X^2(x-1)-(1+i)(X+X^2)(x-1)}{1+iX^2\beta/2} \in (1+\mathfrak{P}_K)(1+\mathfrak{P}_L)^2.$$

If we substitute $X=1$ in (4) and notice that $v_L(2(1+i)(x-1)) > v_L(\beta)$ and $v_L((i+1)(\beta/2)(x-1)) > v_L(\beta)$, we see that $1+(x-1)/(1+\beta/2) \in (1+\mathfrak{P}_K)(1+\mathfrak{P}_L)^2(1+\beta\mathfrak{P}_L)$. Therefore

$$(5) \qquad x = 1+(\beta/2)(x-1)\frac{1}{1+\beta/2} \ \text{ in } \ \mathcal{L}^*.$$

and since $v_L(\beta) > v_L((\beta/2)(x-1))$, we have $x = 1+(\beta/2)(x-1) \in \mathcal{L}$.

Now substitute $X = \omega+\mu$ in (4). Simplify, again using $v_L(2(1+i)(x-1)) > v_L(\beta) = v_L((x-1)^2) > v_L((\beta/2)(x-1))$. This results in the identity $(1+(\omega+\mu)(x-1))\cdot(1-i(\omega+\mu+\omega^2+\mu^2)(x-1))\cdot(1+\omega^4(\beta/2)(x-1)) = 1$ in $\mathcal{L}$. Recall (2), namely $yY = 1+(\omega+\mu)(x-1)$. Therefore since $x = 1+(\beta/2)(x-1) \in \mathcal{L}$,

$$xyY = (1-i(\omega+\mu+\omega^2+\mu^2)(x-1))\cdot(1+(1+\omega^4)(\beta/2)(x-1)) \in \mathcal{L}.$$

Now check, using $b < e_K$ and thus $\beta/2 \in \mathfrak{P}_K$, that $(1+(\omega+\mu)^2(\beta/2)(x-1))^{\sigma+1} \equiv 1+(\omega+\mu)^2\beta \bmod \beta\mathfrak{P}_K$. As a result, using Lemma 2.3 and $v_K(\beta) = 2e_k - b > b$, there is a $\eta^* \in 1+(\beta/2)(x-1)\mathfrak{P}_L$ such that $[(1+(\omega+\mu)^2(\beta/2)(x-1))\eta^*]^{\sigma+1} = (1+(\omega+\mu)^2\beta)(1+4\lambda)$. Therefore $\eta = 1+(\omega+\mu)^2(\beta/2)(x-1) = 1+\omega^2(\beta/2)(x-1) \in \mathcal{L}$. So

$$xyY\eta = (1-i(\omega+\mu+\omega^2+\mu^2)(x-1))\cdot(1+(1+\omega^2+\omega^4)(\beta/2)(x-1)) \in \mathcal{L}.$$

Now using Lemma 3.4, we have

$$xy\eta = (1+(1+\omega^2+\omega^4)(\beta/2)(x-1)) \in \mathcal{M}.$$

Note that $1+(1+\omega^2+\omega^4)(\beta/2)(x-1) \in L$ and because $\omega$ is not a third root of unity, by Lemma 2.1 we see that $\mathrm{def}_M(1+(1+\omega^2+\omega^4)(\beta/2)(x-1)) = 8e_K - 5b$. □

**3.4. Case $1^*$: Assume $\omega^3 = 1$.** Throughout this section we assume that $i = \sqrt{-1} \in K$. Because of $1 + \omega + \omega^2 = 0$, we will require descriptions of $\alpha_k = kxy\eta$ up to terms that have valuation strictly greater than $8e_K - 3b$. In other words, we will need to identify $\alpha_k$ in $\mathcal{M}^*$. This bound of $8e_K - 3b = v_M((x-1)(Y-1))$ is significantly larger than the bounds required in §3.3.1 and §3.3.3: namely, $b + 4e_K$ in the stable case and $8e_K - 5b$ in the unstable case. And this results in additional technicalities.

The material in §3.3.3 is a good source of motivation. Indeed, it suggests that we proceed in two steps: First, identify an equivalent expression in $\mathcal{L}^*$ for $x \cdot yY \cdot \eta \in L$. Most of our technical difficulties are associated with the expression for $\eta$. Second, use Lemma 3.4 to replace $Y$. There will be three cases: (1) $b \le e_K$, (2) $e_K < b < e_K + m$ and (3) $e_K + m \le b$, each associated with a different expression for $\eta$. But in order to keep the parallels to §3.3.1 and §3.3.3 evident, we present the material in two sections: $b > e_K$, which is mostly stable ramification, and $b \le e_K$, which is most of unstable ramification.

**3.4.1. *Mostly stable ramification:* $b > e_K$.** Using Lemma 3.7 below, we determine $\mathrm{def}_{\mathcal{M}^*}(xy\eta) \le v_M((x-1)(Y-1))$. This means that there is a $k_0 \in K$ such that $\mathrm{def}_M(k_0xy\eta) = \mathrm{def}_{\mathcal{M}^*}(xy\eta)$. For $b > e_K + m$, $\mathrm{def}_M(k_0xy\eta) = \min\{4e_K - b + 4m, 8e_K - 3b\}$. Since $b > e_K + m$ can be rewritten as $3b > 4e_K - b + 4m$, by Lemma 3.1 we have $\mathrm{def}_M(k) \ge 3b > \mathrm{def}_M(k_0xy\eta)$ for all $k \in K^*$. This means that $\mathrm{def}_M(kxy\eta) = \min\{4e_K - b + 4m, 8e_K - 3b\}$ for all $k \in K$. For $e_K < b < e_K + m$, we find using Lemma 3.1 that by considering congruences $\mathrm{def}_M(k) \ne \mathrm{def}_M(\alpha_{k_0}) = \min\{8e_K - 5b + 8m, 8e_K - 3b\}$ for all $k \in K^*$. As a result, for $k \in K^*$, $3b \le \mathrm{def}_M(\alpha_k) \le \min\{8e_K - 5b + 8m, 8e_K - 3b\}$ and $\mathrm{def}_M(\alpha_k) \equiv -b \pmod 8$ away from the two extreme values. Moreover, each of these possible values for $\mathrm{def}_M(\alpha_k)$ is realized.

We start with a result that describes $\eta$.

**Lemma 3.6.** *If $i = \sqrt{-1} \in K$, there is an $\eta^* \in L$ that satisfies*

$$\mathrm{def}_L(\eta^*) = \begin{cases} 2m + 2e_K - b & \text{for } m + e_K < b, \\ 4m + 4e_K - 3b & \text{for } m + e_K \ge b, \end{cases}$$

*and the coset identity $\eta = (1 + \omega(x-1)) \cdot \eta^*$ in $\mathcal{L}^*$. Furthermore, when $b = e_K + m$, $\mathrm{def}_L(\pi_K\eta^*) = \mathrm{def}_L(\eta^*) = b$, despite $\mathrm{def}_L(\pi_K) = b$.*

*Proof.* Recall that we have assumed that there is a $\eta \in L$ with norm $N_{L/K}(\eta) = \eta^{\sigma+1} = (1+(\omega+\mu)^2\beta)(1+4\lambda) \equiv 1+(\omega^2+\mu^2)\beta \bmod (\mu^2\beta\mathfrak{P}_K, 4)$. For $\mu \ne 0$ the congruence follows from $m < b/2 < e_K$. We are interested in an explicit description for $\eta \bmod \beta\mathfrak{P}_L$. So choose $\nu_0 \in K$ with

$$v_K(\nu_0) = \begin{cases} 4e_K - 2b & \text{for } b \geq 4e_K/3, \\ 2e_K - (b+1)/2 & \text{for } b < 4e_K/3. \end{cases}$$

And observe that from Lemma 2.3, if $a \in 1 + \nu_0\mathfrak{P}_K$ lies in the image of the norm map $N_{L/K}$, its preimage may be assumed to lie in $1 + \beta\mathfrak{P}_L$.

Note that $(1 + i\omega(x-1))^{\sigma+1} = 1 + \omega^2\beta - 2i\omega$. Choose a $(q-1)$st root of unity $\omega'$ so that $(\omega')^2 = \omega$. Then $(1 + \omega'(i-1))^2 = 1 - 2i\omega + 2\omega'(i-1)$ with $v_K(2(i-1)) = 3e_K/2$. By checking cases, we see that $v_K(2(i-1)) > v_K(\nu_0)$ and that $v_K(4) > v_K(2\beta) > v_K(\beta^2) \geq v_K(\nu_0)$. Therefore

$$[\eta \cdot (1 + i\omega(x-1)) \cdot C]^{\sigma+1} \equiv 1 + \mu^2\beta \bmod (\mu^2\beta\pi_K, \nu_0\pi_K),$$

where $C = (1 + \omega'(i-1)) \cdot (1 + \omega^2\beta) \in 1 + \mathfrak{P}_K$.

Now observe that if $a' \in 1 + \mu^2\beta\mathfrak{O}_K$ lies in the image of the norm map $N_{L/K}$ with $\mathrm{def}_K(a') = v_K(\mu^2\beta)$, we may use Lemma 2.3 to choose its preimage $A$ to lie in $1 + B\mathfrak{O}_K$ with defect

$$\mathrm{def}_L(A) = v_L(B) = \begin{cases} 2m + 2e_K - b & \text{for } m + e_K < b, \\ 4m + 4e_K - 3b & \text{for } m + e_K \geq b. \end{cases}$$

As a result, $\eta \cdot (1 + i\omega(x-1)) \cdot C \equiv \eta^* \bmod (B\pi_L, \beta\pi_K)$ with $\mathrm{def}_L(\eta^*) = v_L(B)$. Since $v_L((i-1)(x-1)) > v_L(\beta)$, we can drop the "$i$" from $1 + i\omega(x-1)$ and the first part of the result follows.

Now consider the case $b = e_K + m$ when $\mathrm{def}_L(\eta^*) = b$. This means that $v_K(2/(\mu\beta)) = 0$ and so there is a $(q-1)$st root of unity $\omega_*$ such that $2/(\mu\beta) \equiv \omega_* \bmod \mathfrak{P}_K$. The condition $b = e_K + m$ also means that $v_L(\mu(x-1)) = v_K(\mu^2\beta) = b$. So without loss of generality we may assume that there is a $(q-1)$st root of unity $a$ such that $\eta^* \equiv 1 + a\mu(x-1) \bmod \mu(x-1)\mathfrak{P}_K$. In fact, we must have $(1 + a\mu(x-1))^{\sigma+1} \equiv 1 + \mu^2\beta \bmod \mu^2\beta\mathfrak{P}_K$, which means that the equation $a^2 + a\omega_* \equiv 1 \bmod \mathfrak{P}_K$ must be solvable for $a$. As a result, it is clear that $a + \omega_* \not\equiv 0 \bmod \mathfrak{P}_K$. Now note that given any $\pi_K \in K$, $\beta/\pi_K \in (1 + \mathfrak{P}_K)(K^*)^2$. Using Lemma 2.1, we see that $\mathrm{def}_L(\beta/\pi_K) > b$, though $\mathrm{def}_L(\beta) = \mathrm{def}_L(\pi_K) = b$. We can be more explicit: Because $(x-1)^2 = \beta \cdot (1 - 2(x-1)/\beta))$, we have $\beta = (1 - 2(x-1)/\beta)$ in $L^*/(L^*)^2$ and since $-2/\beta \equiv \omega^*\mu \bmod \mu\mathfrak{P}_K$, thus $\pi_K = \beta = (1 + \omega_*\mu(x-1))$ in $L^*/((L^*)^2(1 + \mathfrak{P}_L^{b+1}))$. Since $a + \omega_* \not\equiv 0 \bmod \mathfrak{P}_K$, this means $\mathrm{def}_L(\pi_K\eta^*) = \mathrm{def}_L(\eta^*) = b$. □

**Lemma 3.7.** *If $i \in K$, $b > e_K$ and $\omega^3 = 1$, then*

$$\mathrm{def}_{\mathcal{M}^*}(xy\eta) = \begin{cases} \min\{4e_K - b + 4m, 8e_K - 3b\} & \text{for } m + e_K < b, \\ \min\{8e_K - 5b + 8m, 8e_K - 3b\} & \text{for } m + e_K \geq b. \end{cases}$$

*Proof.* Recall from (2) that $yY = 1+(\omega+\mu)(x-1)$. Use Lemma 3.6 to find that $x\cdot yY\cdot\eta = x\cdot(1+(\omega+\mu)(x-1))\cdot(1+\omega(x-1))\cdot\eta^*$ in $\mathcal{L}^*$. Expand the product $(1+(\omega+\mu)(x-1))\cdot(1+\omega(x-1)) \equiv (1+\mu(x-1))\cdot(1+\omega^2\beta) \bmod \beta\mathfrak{P}_L$. So $x\cdot yY\cdot\eta = x\cdot(1+\mu(x-1))\cdot\eta^*$ in $\mathcal{L}^*$. Since $\omega+\omega^2 \equiv 1 \bmod 2$, Lemma 3.4 yields $Y = (1+(1+\mu+\mu^2)(x-1))\cdot(1+(x-1)(Y-1))$ in $\mathcal{M}^*$. Thus $xy\eta = x\cdot(1+\mu(x-1))\cdot\eta^*\cdot(1+(1+\mu+\mu^2)(x-1))\cdot(1+(x-1)(Y-1))$ in $\mathcal{M}^*$. In general, for $a, a' \in \mathfrak{O}_K$, we have $(1+a(x-1))(1+a'(x-1)) \equiv 1+(a+a')(x-1)$ in $\mathcal{M}^*$. Applying this here, we see that $xy\eta = \eta^*\cdot(1+\mu^2(x-1))\cdot(1+(x-1)(Y-1))$ in $\mathcal{M}^*$. Since $\mathrm{def}_L(\eta^*) < v_L(\mu^2(x-1))$, we have $\mathrm{def}_L(\eta^*(1+\mu^2(x-1))) = \mathrm{def}_L(\eta^*)$. We need to use Lemma 2.1 to determine $\mathrm{def}_M(\eta^*)$. First note that $\mathrm{def}_L(\eta^*) < 4e_K - b$. For $m + e_K < b$ this follows from the fact that $m < e_K$ (otherwise $m \geq e_K$ and $b > m + e_K \geq 2e_K$, yielding a contradiction). For $m+e_K \geq b$ this follows from $m < b/2$. Then because $\mathrm{def}_L(\eta^*) < 4e_K - b$, we have $\mathrm{def}_M(\eta^*) = 2\mathrm{def}_L(\eta^*) + b$. It is easy to check, using the fact that $b$ is odd, that $\mathrm{def}_M(\eta^*) \neq v_L((x-1)(Y-1))$. And so we have determined that such that $\mathrm{def}_M(xy\eta) = \min\{\mathrm{def}_M(\eta^*), v_M((x-1)(Y-1))\}$. Thus, unless $b = e_K + m$, we can use Lemma 3.1 to find that $\mathrm{def}_M(xy\eta) \neq \mathrm{def}_M(k)$ for all $k \in K$ and the result follows. When $b = e_K + m$, since $\mathrm{def}_M(\eta^*) = \mathrm{def}_M(\pi_K)$, we need to be careful. But by Lemma 3.6 $\mathrm{def}_L(\pi_K\eta^*) = \mathrm{def}_L(\eta^*)$ and thus $\mathrm{def}_M(\pi_K\eta^*) = \mathrm{def}_M(\eta^*)$. So also in this case $\mathrm{def}_M(kxy\eta) = \mathrm{def}_M(xy\eta)$ for all $k \in K$. □

**3.4.2.** ***Most of unstable ramification: assume $b \leq e_K$.*** From Lemma 3.9 below, we find that $\mathrm{def}_{\mathcal{M}^*}(xy\eta) = \min\{8e_K - 5b + 8m, 8e_K - 3b\} \leq v_M((x-1)(Y-1))$. As a result there is a $k_0 \in K$ such that $\mathrm{def}_M(k_0xy\eta) = \min\{8e_K - 5b + 8m, 8e_K - 3b\}$. Using Lemma 3.1 we find that for $k \in K^*$ $3b \leq \mathrm{def}_M(kxy\eta) \leq \min\{8e_K - 5b + 8m, 8e_K - 3b\}$ and $\mathrm{def}_M(\alpha_k) \equiv -b \pmod 8$ except at the two extreme values. Moreover, each of these possible values for $\mathrm{def}_M(\alpha_k)$ is realized.

Again we start with a lemma that describes $\eta$.

**Lemma 3.8.** *If $i = \sqrt{-1} \in K$, $b < e_K$ and $\omega^3 = 1$ there is in $\mathcal{L}^*$ the following coset identity*

$$\eta = \left(1 + \left[\omega^2 + \mu^2 + \frac{\omega(\beta/2)^2 + \omega^2(\beta/2)^3}{1+(\beta/2)^3}\right]\cdot(\beta/2)(x-1)\right)\cdot E$$

*for some $E \in 1 + \mu^2(\beta/2)(x-1)\mathfrak{P}_L$.*

*Proof.* Note that since $b < e_K$ we have $\mathbb{X} := \beta/2 \in \mathfrak{P}_K$. We are interested in an expression for $\eta \bmod (\mu^2\mathbb{X}(x-1)\pi_L, \beta\pi_L)$. Now note that because $b < e_K$, any element in $1 + \mu^2\beta\mathfrak{P}_K$ has a preimage under the norm $N_{L/K}$ that lies in $1 + \mu^2\mathbb{X}(x-1)\mathfrak{P}_L$, and any element of $1 + \mathfrak{P}_K^{2e_K-(b-1)/2}$ has a preimage in $1 + \beta\mathfrak{P}_L$ [13, V§3]. So we study the image $N_{L/K}\eta = \eta^{\sigma+1}$ mod $(\mu^2\beta\pi_K, \pi_K^{2e_K-\frac{b-1}{2}})$.

To compute this image, observe that for $M \in \mathfrak{O}_K$, $(1-M\mathbb{X}(x-1))^{\sigma+1} = 1+(M-M^2\mathbb{X}^2)\beta$. Now set

$$M = \omega^2 + \mu^2 + \frac{\omega\mathbb{X}^2 + \omega^2\mathbb{X}^3}{1+\mathbb{X}^3}.$$

Since $v_K(2) = e_K > b > 2m = v_K(\mu^2)$ we can expand $M^2$ mod 2 and find that

$$(1-M\mathbb{X}(x-1))^{\sigma+1} \equiv 1 + \left[\omega^2 + \mu^2 + \frac{\omega^2\mathbb{X}^3 + \omega\mathbb{X}^5}{1+\mathbb{X}^6}\right]\beta \bmod \mu^2\beta\mathfrak{P}_K.$$

Since $v_K(\beta^2) > 2e_K - (b-1)/2$, we have $(1-M\mathbb{X}(x-1))^{\sigma+1} \equiv (1+(\omega^2+\mu^2)\beta)\cdot T$ with

$$T = 1 + \frac{\omega^2\mathbb{X}^3 + \omega\mathbb{X}^5}{1+\mathbb{X}^6}\beta \bmod (\mu^2\beta\pi_K, \pi_K^{2e_K-\frac{b-1}{2}}).$$

Choose $\omega'$ to be a $(q-1)$st root of unity such that $(\omega')^2 = \omega$ and observe that since $2\mathbb{X} = \beta$,

$$\left(1 + \omega'(i-1)\frac{\omega^2\mathbb{X}^2 + \mathbb{X}^3}{1+\mathbb{X}^3}\right)^2 \equiv T \bmod 2(i-1)\mathbb{X}^2\mathfrak{O}_K.$$

Since $e_K > b$ we have $v_K(2(i-1)\mathbb{X}^2) \geq 2e_K - (b-1)/2$. So when $T \not\equiv 1 \bmod (\mu^2\beta\pi_K, \pi_K^{2e_K-\frac{b-1}{2}})$, it lies in $(1+\mathfrak{P}_K)^2$. Thus $\eta \in (1-M\mathbb{X}(x-1))(1+\mathfrak{P}_K)^2(1+\mu^2\mathbb{X}(x-1)\mathfrak{P}_L)(1+\beta\mathfrak{P}_L)$ and the result is proven. $\square$

**Lemma 3.9.** *If $i \in K$, $b < e_K$ and $\omega^3 = 1$ then*

$$\mathrm{def}_{\mathcal{M}^*}(xy\eta) = \min\{8e_K - 5b + 8m, 8e_K - 3b\}.$$

*Proof.* We follow the proof of Lemma 3.5. In fact the first three paragraphs (up through (5)) of that proof hold here verbatim. So we begin at the point where we substitute $X = \omega + \mu$ into (4), but examine the result in $\mathcal{L}^*$ (instead of $\mathcal{L}$). Again as in the proof of Lemma 3.8, we set $\mathbb{X} = \beta/2 \in \mathfrak{P}_K$. Using the fact that $v_L(2(x-1)) > v_L(\beta)$, $v_L((1+i)(x-1)\mathbb{X}) > v_L(\beta)$ and since $\omega^3 = 1$, $\omega + \omega^2 \equiv 1 \bmod 2$, we find that

$$1 = 1 + (\omega^2+\mu^2)(x-1)\frac{1}{1+(\omega^2+\mu^2)\mathbb{X}} + (1+i)(1+\mu+\mu^2)(x-1)$$

is coset identity in $\mathcal{L}^*$. Note that for $a_1, a_2 \in (x-1)\mathfrak{O}_L$ we have $(1+a_1)(1+a_2) = 1 + a_1 + a_2$ as cosets in $\mathcal{L}^*$. This means that the coset identity factors: $1 = A\cdot B\cdot C$ where $A = 1+(\omega^2+\mu^2)(x-1)/(1+(\omega^2+\mu^2)\mathbb{X})$, $B = 1+(1+\mu+\mu^2)(x-1)$ and $C = 1+i(1+\mu+\mu^2)(x-1)$. Notice that

$$\frac{1}{1+(\omega^2+\mu^2)\mathbb{X}} \equiv 1 - \frac{\omega^2\mathbb{X}}{1+\omega^2\mathbb{X}} - \mu^2\mathbb{X} \bmod \mu^2\mathbb{X}\mathfrak{P}_L.$$

This means that we can factor $A$, in $\mathcal{L}^*$, further as

$$A = (1 + (\omega^2 + \mu^2)(x-1))\left(1 + \frac{\omega\mathbb{X}}{1+\omega^2\mathbb{X}}(x-1)\right)E$$

where $E \in 1 + \mu^2\mathbb{X}(x-1)\mathfrak{P}_L$. Now recall (2) and multiply both sides of $1 = A \cdot B \cdot C$ by $yY = 1 + (\omega + \mu)(x-1)$. Recall (5) and multiply both sides by $x$. The result is $xyY = C \cdot (1 + \Theta_1\mathbb{X}(x-1)) \cdot E$ where

$$\Theta_1 = \frac{1}{1+\mathbb{X}} + \frac{\omega}{1+\omega^2\mathbb{X}} + \mu^2.$$

Using Lemma 3.8, we multiply both sides by $\eta$. This results in $xyY\eta = C \cdot \big(1 + (\mu^2 + \Theta_2)\mathbb{X}(x-1)\big) \cdot E'$, an equivalence of cosets in $\mathcal{L}^*$, where $E' \in 1 + \mu^2\mathbb{X}(x-1)\mathfrak{P}_L$ and

$$\Theta_2 = \omega^2 + \frac{\omega\mathbb{X}^2 + \omega^2\mathbb{X}^3}{1+\mathbb{X}^3} + \frac{1}{1+\mathbb{X}} + \frac{\omega}{1+\omega^2\mathbb{X}} \equiv 0 \bmod 2.$$

To see that $\Theta_2 \equiv 0 \bmod 2$, multiply both sides by the unit $(1 + \mathbb{X}^3) \equiv (1+\mathbb{X})(1+\omega\mathbb{X})(1+\omega^2\mathbb{X}) \bmod 2$.

In summary, we have proven that there is an $E' \in 1 + \mu^2\mathbb{X}(x-1)\mathfrak{P}_L$ such that $xyY\eta = (1 + i(1+\mu+\mu^2)(x-1)) \cdot \big(1 + \mu^2\mathbb{X}(x-1)\big) \cdot E' \in \mathcal{L}^*$. Now use Lemma 3.4 to see that we have the coset identity

$$xy\eta = \big(1 + \mu^2\mathbb{X}(x-1)\big) \cdot (1 + (x-1)(Y-1)) \cdot E' \in \mathcal{M}^*.$$

Finally, by Lemma 2.1, since $m < b/2$ we have $\mathrm{def}_M((1+\mu^2\mathbb{X}(x-1)) \cdot E') = 8m + 8e_K - 5b$. Hence there is a $k_0 \in K$ such that $\mathrm{def}_M(k_0xy\eta) = \min\{8m + 8e_K - 5b, 8e_K - 3b\}$. Note that since $b$ is odd, $8m + 8e_K - 5b \neq 8e_K - 3b$. The result now follows from Lemma 3.1. □

## 4. Case 2: two break biquadratic extensions

Let $M = K(\sqrt{u}, \sqrt{v})$ as in §2 and assume that $M$ embeds in a quaternion extension. We are interested in determining $\mathrm{def}_M(\alpha_k)$. Since the ramification filtration of $\mathrm{Gal}(M/K)$ is asymmetric with respect to the group action, we have three cases to consider:

(1) $G_{b_2}$ **fixes** $K(\sqrt{u})$**.** In this case, $b_1$ is the break number of $K(\sqrt{u})/K$, $b_2$ is the break of $M/K(\sqrt{u})$, $(b_1+b_2)/2$ is the break of $K(\sqrt{uv})/K$, and $b_1$ is the break of $M/K(\sqrt{uv})$.

(2) $G_{b_2}$ **fixes** $K(\sqrt{uv})$**.** In this case, $(b_1+b_2)/2$ is the break of $K(\sqrt{u})/K$, $b_1$ is the break of $M/K(\sqrt{u})$ and $K(\sqrt{uv})/K$, and $b_2$ is the break of $M/K(\sqrt{uv})$.

(3) $G_{b_2}$ **fixes** $K(\sqrt{v})$**.** In this case, $(b_1+b_2)/2$ is the break of $K(\sqrt{u})/K$, $b_1$ is the break of $M/K(\sqrt{u})$, $(b_1+b_2)/2$ is the break of $K(\sqrt{uv})/K$, and $b_1$ is the break number of $M/K(\sqrt{uv})$.

**4.1. Stable ramification.** We begin by considering the case in which ramification is stable. We *do not* assume $\sqrt{-1} \in K$. Because of the following lemma, we conclude that if $b_1 + b_2 > 2e_K$ then the third break number $b_3$ must be $4e_K + b_2$, which is precisely the value given in the catalog in Section 1.3.

**Lemma 4.1.** *Suppose that* $b_1 + b_2 > 2e_K$. *Then* $def_M(\alpha_k) = 4e_K - b_2$.

*Proof.* Because of the possibility that $\sqrt{-1} \notin K$ we have $\alpha_k = k\sqrt{uv}\eta\tau$. The proof breaks naturally into three steps. First we prove that $\mathrm{def}_M(k) > 4e_K - b_2$ for all $k \in K$. We then show that $\mathrm{def}_M(\tau) > 4e_K - b_2$, and finally prove that in each of the three cases $\mathrm{def}_M(\sqrt{uv}\eta) = 4e_K - b_2$. The result will then follow immediately.

We begin by considering $\mathrm{def}_M(k)$. Choose $L$ to be the fixed field of $G_{b_2}$, so that the break of $L/K$ is $b_1$. By Lemma 2.1 we have $\mathrm{def}_L(k) \geq b_1$. The break of $M/L$ is $b_2$ and $b_1 > 2e_K - b_2$, and so by Lemma 2.1, $\mathrm{def}_M(k) > 4e_K - b_2$.

For the second step, we need to consider $\mathrm{def}_M(\tau)$. Recall that $\tau \in K(\sqrt{uv})$, $N_{K(\sqrt{uv})/K}(\tau) = -1$ and note that $\mathrm{def}_K(-1) \geq e_K$. In Cases (1) and (3), since $e_K < (b_1 + b_2)/2$ using [13, V§3] we see that $\mathrm{def}_{K(\sqrt{uv})}(\tau) \geq e_K$. Because $e_K > 2e_K - (b_1 + b_2)/2 > 2e_K - b_1$, Lemma 2.1 with respect to $M/K(\sqrt{uv})$ yields $\mathrm{def}_M(\tau) > 4e_K - b_1 > 4e_K - b_2$. Now consider Case (2): either $b_1 > e_K$ or $b_1 \leq e_K$. In the first situation, using [13, V§3] we see that $\mathrm{def}_{K(\sqrt{uv})}(\tau) \geq e_K$. But since $b_2 > b_1 > e_K$, $\mathrm{def}_{K(\sqrt{uv})}(\tau) > 2e_K - b_2$. In the second situation, using [13, V§3] we see that $\mathrm{def}_{K(\sqrt{uv})}(\tau) \geq 2e_K - b_1 > 2e_K - b_2$. Using Lemma 2.1 with respect to $M/K(\sqrt{uv})$ yields $\mathrm{def}_M(\tau) > 4e_K - b_2$. This completes the second part of the proof.

Finally, we proceed to prove $\mathrm{def}_M(\sqrt{uv}\eta) = 4e_K - b_2$. This time we will need to treat the three cases separately.

Suppose first that we are in case (3). Since $\mathrm{def}_K(v) = 2e_K - b_1$ to use [13, V§3], we need to consider the two possibilities $2e_K - b_1 < (b_1 + b_2)/2$ and $2e_K - b_1 \geq (b_1 + b_2)/2$ separately. In both situations however we see that $\mathrm{def}_{K(\sqrt{u})}(\eta) > 2e_K - (b_1 + b_2)/2$, so that using Lemma 2.1 yields $\mathrm{def}_M(\eta) > 4e_K - b_2$. Note that $\mathrm{def}_{K(\sqrt{uv})}(\sqrt{uv}) = 2e_K - (b_1 + b_2)/2$, which implies that $\mathrm{def}_M(\sqrt{uv}) = 4e_K - b_2$. Hence we have $\mathrm{def}_M(\sqrt{uv}\eta) = 4e_K - b_2$.

Case (2) is similarly easy. Note that in this case $\mathrm{def}_{K(\sqrt{uv})}(\sqrt{uv}) = 2e_K - b_1 > 2e_K - b_2$, and so again by Lemma 2.1, $\mathrm{def}_M(\sqrt{uv}) > 4e_K - b_2$. Since $\mathrm{def}_K(v) = 2e_K - (b_1 + b_2)/2$ and $2e_K - (b_1 + b_2)/2 < (b_1 + b_2)/2$, which is the break of $K(\sqrt{u})/K$, we see that $\mathrm{def}_{K(\sqrt{u})}(\eta) = 2e_K - (b_1 + b_2)/2$. Hence by Lemma 2.1 $\mathrm{def}_M(\eta) = 4e_K - b_2$ and so we have $\mathrm{def}_M(\sqrt{uv}\eta) = 4e_K - b_2$.

In Case (1), $\mathrm{def}_K(v) = 2e_K - (b_1 + b_2)/2$, and there are two cases to consider depending upon whether $2e_K - (b_1 + b_2)/2 > b_1$ or $2e_K - (b_1 + b_2)/2 \leq b_1$. In both cases, without loss of generality we find that

$\mathrm{def}_{K(\sqrt{u})}(\eta) > 2e_K - b_2$. Therefore $\mathrm{def}_M(\eta) > 4e_K - b_2$. On the other hand, $\mathrm{def}_{K(\sqrt{uv})}(\sqrt{uv}) = 2e_K - (b_1 + b_2)/2$, which means that $\mathrm{def}_M(\sqrt{uv}) = 4e_K - b_2$. Combining these yields $\mathrm{def}_M(\sqrt{uv}\eta) = 4e_K - b_2$. □

**4.2. Unstable ramification.** We assume here that $\sqrt{-1} \in K$. Because of the following lemma, if $b_1+b_2 < 2e_K$ then the third break number $b_3$ must be $2b_1+3b_2$, $8e_K-2b_1-b_2$, or else must satisfy $2b_1+3b_2 < b_3 < 8e_K-2b_1-b_2$ with $b_3 \equiv b_2 \bmod 8$. These are precisely the values listed in the catalog in Section 1.3.

**Lemma 4.2.** *Suppose that $M/K$ has two breaks which satisfy $b_1+b_2 < 2e_K$. Then the value of $\mathrm{def}_M(\alpha_k)$ must be $b_2 + 2b_1$, $8e_K - 3b_2 - 2b_1$ or else satisfy $b_2 + 2b_1 < \mathrm{def}_M(\alpha_k) < 8e_K - 3b_2 - 2b_1$ with $\mathrm{def}_M(\alpha_k) \equiv -b_2 \bmod 8$. Moreover, each of these possible values for $\mathrm{def}_M(\alpha_k)$ is realized.*

*Proof.* Because $\sqrt{-1} \in K$ and since $M/K$ embeds in a quaternion extension, we have the Hilbert symbol equations $(u, v) = (u, uv) = (uv, v) = 1$. This symmetry, among $u$, $v$, and $uv$, allows us to assume without loss of generality that $K(\sqrt{u})$ is the fixed field of $G_{b_2}$. Now we turn to an examination of $\alpha_k = k\sqrt{uv}\eta$.

To proceed with the proof, we separate $\alpha_k$ into two parts, $k\sqrt{uv}$ and $\eta$. Our first step is to explicitly determine the possibilities for $\mathrm{def}_M(k\sqrt{uv})$ from $\mathrm{def}_{K(\sqrt{uv})}(k\sqrt{uv})$. This will use the classification of all possible second ramification numbers in a cyclic degree 4 extension from [15]. Once that has been completed, we will show that $\mathrm{def}_M(k\sqrt{uv}) < \mathrm{def}_M(\eta)$. Since this implies that $\mathrm{def}_M(\alpha_k) = \mathrm{def}_M(k\sqrt{uv})$, the result will follow.

**Step 1.** Since $\sqrt{-1} \in K$, $K(\sqrt[4]{uv})/K$ is cyclic of degree 4. Given $k \in K$ either $K(\sqrt{k}, \sqrt[4]{uv})/K$ is cyclic of degree 4 or $\mathrm{Gal}(K(\sqrt{k}, \sqrt[4]{uv})/K) \cong C_2 \times C_4$. In either case, the subextension $K(\sqrt{k}\sqrt[4]{uv})/K$ will be cyclic of degree 4. Again using the assumption that $\sqrt{-1} \in K$, it is easy to check that any cyclic extension of degree 4 containing $K(\sqrt{uv})$ is expressible as $K(\sqrt{k}\sqrt[4]{uv})/K$ for some $k \in K$.

Let $t = (b_2 + b_1)/2$. Then $t$ is the break number of $K(\sqrt{uv})/K$. Since $t < e_K$, we find using [15, Thm 32] that the second break number of $K(\sqrt{k}\sqrt[4]{uv})/K$ must be one of $b_2 = 3t$, $4e_K - t$ or $b_2 = t + 4m$ with $3t < b + 4m < 4e_K - t$, and moreover that all these possible values for $b_2$ actually occur. Therefore $\mathrm{def}_{K(\sqrt{uv})}(k\sqrt{uv})$ must be one of the values $t$, $4e_K - 3t$ or $t < \mathrm{def}_{K(\sqrt{uv})}(k\sqrt{uv}) < 4e_K - 3t$ with $\mathrm{def}_{K(\sqrt{uv})}(k\sqrt{uv}) \equiv -t \bmod 4$. Since in every one of these cases $\mathrm{def}_{K(\sqrt{uv})}(k\sqrt{uv}) < 4e_K - b_1$, we may use Lemma 2.1 to determine that the possible values of $\mathrm{def}_M(k\sqrt{uv})$ are $b_2 + 2b_1$, $8e_K - 3b_2 - 2b_1$ or $b_2 + 2b_1 < \mathrm{def}_M(k\sqrt{uv}) < 8e_K - 3b_2 - 2b_1$ with $\mathrm{def}_M(k\sqrt{uv}) \equiv -b_2 \bmod 8$.

**Step 2.** Recall that we have chosen $\eta \in K(\sqrt{u})$ so that $N_{K(\sqrt{u})/K}(\eta) = v$. Since the break of $K(\sqrt{v})$ is $t = (b_2+b_1)/2$, the defect $\mathrm{def}_K(v) = 2e_K - t$. Moreover, since $t < e_K$, we have $b_1 < e_K$, and so $b_1 < 2e_K - t$. Since $b_1$ is the break number of $K(\sqrt{u})/K$, we use [13, V§3] to choose $\eta \in K(\sqrt{u})$ such that $\mathrm{def}_{K(\sqrt{u})}(\eta) = 4e_K - b_2 - 2b_1$, and since the break of $M/K(\sqrt{u})$ is $b_2$ we may use Lemma 2.1 to find that $\mathrm{def}_M(\eta) = 8e_K - b_2 - 4b_1$. To finish, it suffices to note that $8e_K - b_2 - 4b_1 > 8e_K - 3b_2 - 2b_1 \geq \mathrm{def}_M(k\sqrt{uv})$. $\square$

## 5. Proof of main results

*Proof of Theorem 1.1.* Given the computations in Sections 3 and 4, the first statement has already been established; we just need to prove the second. In fact, since $\sqrt{-1} \in K$ it is enough to prove, for each $i \in \{1, 1^*, 2\}$, that if $s_1 \leq s_2$ are the first two coordinates of a triple in $\mathcal{R}_i^e$ then there exist a pair of elements $u, v \in K^*$ such that $(u, v) = 1$ and the following:

(1) If $i = 2$, then $v_K(u-1) = 2e_K - s_1$ and $\mathrm{def}_K(v) = 2e_K - (s_2+s_1)/2$.
(2) If $i \in \{1, 1^*\}$, then $v_K(u-1) = v_K(v-1) = 2e_K - s_1$. Indeed $v - 1 = (\omega + \mu)^2(u-1)$ where

   (a) $\omega$ is a nontrivial $(q-1)$st root of unity, with $\omega^2 + \omega + 1 = 0$ if $i = 1^*$ and $\omega^3 \neq 1$ if $i = 1$, and
   (b) $\mu \in K$, with $v_K(\mu) = (s_2 - s_1)/4$ if $s_2 < \min\{2s_1, 4e_K - s_1\}$ and $v_K(\mu) > (s_2 - s_1)/4$ if $s_2 = \min\{2s_1, 4e_K - s_1\}$.

   (Recall the definition of the refined break $r$ from §3.1.)

Under these circumstances, the biquadratic extension $M = K(\sqrt{u}, \sqrt{v})$ will embed in a quaternion extension, which lies in $\mathcal{Q}_i^K$ and have the desired ramification pair $s_1 \leq s_2$. The third coordinate $s_3$ of the triple is then achieved by using Lemma 3.1 to choose the $k$ in $\alpha_k$ appropriately.

We begin with cases where any pair of elements $u, v$ with the desired defects must automatically satisfy $(u, v) = 1$. If $i \in \{2\}$ and $s_2 + 3s_1 < 4e_K$, then using Lemma 2.3 we see that if $u \in K^*$ and $v_K(u-1) = 2e_K - s_1$, then any $v \in K^*$ that satisfies $\mathrm{def}_K(v) = 2e_K - (s_2+s_1)/2$ will satisfy $(u, v) = 1$. Similarly for $i \in \{1, 1^*\}$ when $s_1 < e_K$ every pair of units $u, v \in 1 + \mathfrak{P}_K$ that satisfies $v_K(u-1) = v_K(v-1) = 2e_K - s_1$ will satisfy $(u, v) = 1$. In these cases every such biquadratic extension $K(\sqrt{u}, \sqrt{v})/K$ embeds.

Outside of these two cases, we are free to choose $u$ based upon defect alone, but must choose $v$ dependent upon $u$. Suppose $i \in \{2\}$ and $s_2 + 3s_1 \geq 4e_K$. Pick any element $u \in K^*$ such that $v_K(u-1) = 2e_K - s_1$. Pick any element $\nu \in K(\sqrt{u})$ with $v_{K(\sqrt{u})}(\nu - 1) = 2e_K - (s_2 + s_1)/2$. By Lemma 2.3 we have $N_{K(\sqrt{u})/K}(\nu) = v \in K^*$ where $v_K(v-1) = 2e_K - (s_2+s_1)/2$ and so by design, $(u, v) = 1$.

Consider now $i \in \{1, 1^*\}$ and $s_1 > e_K$. Pick $\omega$ according to whether $i = 1$ or $i = 1^*$. Choose $\beta \in K$ with $v_K(\beta) = 2e_K - s_1$. Let $x^2 = u = 1+\beta$. Then $L/K$ where $L = K(x)$ has ramification break number $s_1$. We consider the cases $s_1 < 3e_K/2$ and $s_1 \geq 3e_K/2$ separately.

If $e_K < s_1 < 3e_K/2$, then then one can show, as in the proof of Lemma 3.6, that the norm

$$N_{L/K}\big((1 + i\omega(x-1)) \cdot (1 + \omega'(i-1))\big) \equiv 1 + \omega^2\beta \bmod \mathfrak{P}_K^{s_1+1}$$

where $(\omega')^2 = \omega$. By Lemma 2.3, any element $\alpha \in 1 + \mathfrak{P}_K^{s_1+1}$ satisfies $(1 + \beta, \alpha) = 1$. As a result, $(1 + \beta, 1 + \omega^2\beta) = 1$. Again using Lemma 2.3 there is, for any relevant value of $m$, an element $A \in L$ such that $v_K(N_{L/K}(A) - 1) = 2e_K - s_1 + 2m$. Note $(1 + \beta, (1 + \omega^2\beta) \cdot N_{L/K}(A)) = 1$. Using Lemma 2.2, we find a $\mu \in K$ with $v_K(\mu) = m$ such that $1 + (\omega + \mu)^2\beta \equiv (1 + \omega^2\beta) \cdot N_{L/K}(A)$ (modulo squares in $K^*$). So for $v = 1 + (\omega + \mu)^2\beta$ we have $(u, v) = 1$.

Assume $s_1 \geq 3e_K/2$. We see explicitly that for $a \in \mathfrak{O}_T$,

$$N_{L/K}\left(1 + a\frac{2}{1-x}\right) = 1 - \frac{4}{\beta}(a + a^2).$$

Let $\lambda \in \mathfrak{O}_T$ such that $y + y^2 = \lambda$ is irreducible. Then $(1+\beta, 1-4\lambda/\beta) = -1$. This means that we have $(1+\beta, 1+\omega^2\beta) = 1$ or $(1+\beta, 1+\omega^2\beta-4\lambda/\beta) = 1$. If we express $1 + \omega^2\beta - 4\lambda/\beta$ as $(1 + (\omega + \mu_0)^2\beta) \bmod 4$ using Lemma 2.2 we find that $v_K(\mu_0) = m = s_1 - e_K$. Of course, $1 + \omega^2\beta = (1 + (\omega + \mu_0)^2\beta)$ with $v_K(\mu_0) = \infty > s_1 - e_K$. Let $v_0 = 1 + (\omega + \mu_0)^2\beta$. Then $(u, v_0) = 1$ and $v_K(\mu_0) = m \geq s_1 - e_K$. Since $s_1 + 4m > 4e_K - s_1$ we find that $K(\sqrt{u}, \sqrt{v_0})$ embeds and has refined ramification filtration $s_1 < s_2 = 4e_K - s_1 = \min\{2s_1, 4e_K - s_1\}$. All that remains is the situation where $s_2 < 4e_K - s_1 = \min\{2s_1, 4e_K - s_1\}$. In other words, for each $0 < m < e_K - s_1/2$, we must find $\mu \in K$ with $v_K(\mu) = m$ so that $v = 1 + (\omega + \mu)^2\beta$ satisfies $(u, v) = 1$. The second refined break of $K(\sqrt{u}, \sqrt{v})$ will then be $s_2 = s_1 + 4m < 4e_K - s_1 = \min\{2s_1, 4e_K - s_1\}$. We know that $s_1 \geq 3e_K/2 > 4e/3$. We have $2m < 2e_K - s_1$. Pick any $A \in L$ with $v_L(A) = 2m + 2e_K - s_1 < 4e_K - 2s_1 < s_1$. Then using Lemma 2.3, $v_K(N_{L/K}(A) - 1) = 2e_K - s_1 + 2m$. So $(u, v_0 \cdot N_{L/K}(A)) = 1$. And using Lemma 2.2, we can express $v_0 \cdot N_{L/K}(A)$ as $v \equiv 1 + (\omega + \mu)^2\beta \bmod 4$ (also modulo squares in $K^*$) where $\mu \in K$ with $v_K(\mu) = m$. □

*Proof of Theorem 1.2.* This follows immediately from §3.3.1 and §4.1. □

## References

[1] N. P. BYOTT, G. G. ELDER, *Biquadratic extensions with one break*. Canadian Math. Bull. **45** (2002) no. 2, 168–179.

[2] N. P. BYOTT, G. G. ELDER, *New ramification breaks and additive Galois structure*. J. Théor. Nombres Bordeaux **17** (2005) no. 1, 87–07, Les XXIIIémes Journées Arithmetiques (Graz, 2003).

[3] G. G. ELDER, *Galois module structure in wildly ramified cyclic extensions of degree* $p^2$. Ann. Inst. Fourier (Grenoble) **45** (1995) no. 3, 625–647. *errata ibid.* **48** (1998) no. 2, 609–610.

[4] G. G. ELDER, *Galois module structure of ambiguous ideals in biquadratic extensions*. Canad. J. Math. **50** (1998), no. 5, 1007–1047.

[5] G. G. ELDER, *The Galois structure of ambiguous ideals in cyclic extensions of degree 8*. Noncommutative algebra and geometry, 63–89, Lect. Notes Pure Appl. Math., 243, Chapman & Hall/CRC, Boca Raton, FL, 2006.

[6] I. B. FESENKO, S. V. VOSTOKOV, *Local fields and their extensions*. Trans. of Math. Monographs, **121**, 2nd Ed., American Mathematical Society, Providence, RI, 2002.

[7] J.-M. FONTAINE, *Groupes de ramification et représentations d'Artin*. Ann. Sci. École Norm. Sup. (4) **4** (1971), 337–392.

[8] A. FRÖHLICH, *Galois module structure of algebraic integers*. Ergebnisse der Mathematik und ihrer Grenzgebiete (3), **1**, Springer-Verlag, Berlin, 1983.

[9] H. HASSE, *Number theory*. Classics in Mathematics, Springer-Verlag, Berlin, 2002, Reprint of 1980 English ed. Edited with a preface by H. G. Zimmer.

[10] C. U. JENSEN, N. YUI, *Quaternion extensions*. Algebraic geometry and commutative algebra, Vol. I, Kinokuniya, Tokyo, 1988, pp. 155–182.

[11] O. T. O'MEARA, *Introduction to quadratic forms*. Springer-Verlag, New York, 1971.

[12] H. REICHARDT, *Über normalkörper mit quaternionengruppe*. Math. Z. **41** (1936), 218–221.

[13] J.-P. SERRE, *Local Fields*. Springer-Verlag, New York, 1979.

[14] E. WITT, *Konstruktion von galoisschen körpern der characteristik* $p$ *zu vorgegebener gruppe der ordnung* $p^f$. J. Reine Angew. Math. **174** (1936), 237–245.

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

G. Griffith ELDER
Department of Mathematics
Virginia Tech
Blacksburg, VA 24061-0123 U.S.A.
*E-mail* : elder@vt.edu

Jeffrey J. HOOPER
Department of Mathematics and Statistics
Acadia University
Wolfville, NS
B4P 2R6 Canada
*E-mail* : jeff.hooper@acadiau.ca