Journal de Théorie des Nombres
de Bordeaux **17** (2005), 87–107

New ramification breaks and additive Galois structure

par NIGEL P. BYOTT et G. GRIFFITH ELDER

RÉSUMÉ. Quels invariants d'une p-extension galoisienne de corps local L/K (de corps résiduel de charactéristique p et groupe de Galois G) déterminent la structure des idéaux de L en tant que modules sur l'anneau de groupe $\mathbb{Z}_p[G]$, $\mathbb{Z}_p$ l'anneau des entiers p-adiques? Nous considérons cette question dans le cadre des extensions abéliennes élémentaires, bien que nous considérions aussi brièvement des extensions cycliques. Pour un groupe abélien élémentaire G, nous proposons et étudions un nouveau groupe (dans l'anneau de groupe $\mathbb{F}_q[G]$ où $\mathbb{F}_q$ est le corps résiduel) ainsi que ses filtrations de ramification.

ABSTRACT. Which invariants of a Galois p-extension of local number fields L/K (residue field of char p, and Galois group G) determine the structure of the ideals in L as modules over the group ring $\mathbb{Z}_p[G]$, $\mathbb{Z}_p$ the p-adic integers? We consider this question within the context of elementary abelian extensions, though we also briefly consider cyclic extensions. For elementary abelian groups G, we propose and study a new group (within the group ring $\mathbb{F}_q[G]$ where $\mathbb{F}_q$ is the residue field) and its resulting ramification filtrations.

1. Introduction

There is, at the present, a small collection of results [3, 4, 2, 5, 6] concerning the structure (the explicit decomposition) of the ring of integers, in a wildly ramified local number field extension L/K, as a module over the group ring $\mathbb{Z}_p[G]$. Here $G = \mathrm{Gal}(L/K)$, $\mathbb{Z}_p$ denotes the p-adic integers and K is a finite extension of the p-adic numbers, $\mathbb{Q}_p$.

Looking through this collection, one might notice the following: the ramification invariants of the extension are sufficient to determine this

We thank Andrew Gacek for suggesting Proposition 2.4, and the referee for many helpful suggestions including the short argument for Lemma 3.1. Elder was partially supported by NSF grant DMS-0201080.

$\mathbb{Z}_p[G]$-structure *only* when their number is maximal. Otherwise? In particular, what happens when there are not enough breaks in the Hilbert ramification filtration of G?

As observed in [2] where $G \cong C_2 \times C_2$, additional information is needed. But how should this information be understood? In this paper, we propose a *refined ramification filtration*[1] and find that the information required for [2] arises from breaks in this new filtration.

1.1. Notation. Recall that K is a finite extension of $\mathbb{Q}_p$, and let L be a finite, fully ramified, Galois p-extension of K. Let T denote the maximal unramified extension of $\mathbb{Q}_p$ contained in K. Thus $e_0 = [K : T]$ is the absolute ramification index of K while $f = [T : \mathbb{Q}_p]$ is its inertia degree. Use subscripts to denote the field of reference. So π_L denotes a prime element in L, $\mathfrak{O}_L$ its ring of integers, $\mathfrak{P}_L = \pi_L \mathfrak{O}_L$ the prime ideal of $\mathfrak{O}_L$ and v_L the valuation normalized so that $v_L(\pi_L) = 1$. Let $\mathbb{F}_p$ denote the finite field of p elements and $\mathbb{F}_q = \mathfrak{O}_T/\mathfrak{P}_T$ the finite field of $q = p^f$ elements. Let $\Phi_p(x) = (x^p - 1)/(x - 1)$ be the cyclotomic polynomial. Let $\mathbb{Z}_{(p)}$ denote the integers localized at p, and define *truncated exponentiation* by the polynomial,

$$(1 + x)^{[y]} = \sum_{i=0}^{p-1} \binom{y}{i} x^i \in \mathbb{Z}_{(p)}[x, y],$$

which results from a truncation of the binomial series.

By the *ramification invariants* of L/K, we mean the two integers, e_0 and f, along with the information provided by the ramification filtration of $G = \mathrm{Gal}(L/K)$: the list of the quotients G_i/G_{i+1} of the ramification groups $G_i = \{\sigma \in G : v_L((\sigma - 1)\pi_L) \geq i + 1\}$. Naturally, we are primarily interested in nontrivial quotients. These occur at a *break*, where $G_i \supsetneq G_{i+1}$. To distinguish the collection of such breaks $\{b_j : G_{b_j} \supsetneq G_{b_j+1}\}$, from other 'breaks' (to be defined later), we will refer to them as *Hilbert breaks*. It is easy to see, because G is a p-group, that there can be at most $\log_p |G|$ Hilbert breaks – when each nontrivial quotient has order p. This is what we mean by 'maximal number'.

1.2. Cyclic extensions. Each quotient G_i/G_{i+1} in a fully ramified p-extension L/K is elementary abelian [9]. Thus cyclic fully ramified p-extensions have a maximal number of ramification invariants. It was determined in [3] (in [6] respectively) that ramification invariants are sufficient to determine the $\mathbb{Z}_p[G]$-structure of the ring of integers in fully ramified C_{p^2}-extensions (in C_{2^3}-extensions). Does this generalize?

Question. Are ramification invariants sufficient for cyclic p-extensions?

[1] The refined ramification filtration is, at this point, relative to an element $\alpha \in L$ and is not (yet) guaranteed to be canonical.

Of course, we are far more interested in the following general

Question. Are ramification invariants sufficient for p-extensions with a maximal number of ramification invariants?

The first question, as it is phrased, is still open. Though based upon [5, 11], we can answer it with a qualified 'yes'. We explain this now.

Let L/K be an arbitrary fully ramified cyclic extension of degree p^n. Let σ generate its Galois group G, and let $b_1 < b_2 < \cdots < b_n$ denote its Hilbert breaks. The first Hilbert break satisfies $1 \leq b_1 \leq B_1$ where $B_1 = pe_0/(p-1)$. If we restrict b_1 to about one half of its possible values, namely $B_1/2 < b_1 \leq B_1$, then the $\mathbb{Z}_p[G]$-structure of the ring of integers of L is given in [5]. It is determined completely by ramification invariants.

Let K_1 denote the fixed field of σ^p. Note that $b_2 < b_3 < \cdots < b_n$ are the Hilbert breaks for L/K_1. If we restrict b_1 to $B_1/p \leq b_1$, so-called *stable ramification*, the other Hilbert breaks are determined by b_1. In fact, $b_i = b_1 + (p^{i-1}-1)B_1$ [11]. Under this condition b_2 satisfies $B_2/2 < b_2 \leq B_2$, where $B_2 = p^2e_0/(p-1)$ is the generic upper bound on b_2, and so the main result of [5] can be applied to the $\mathbb{Z}_p[\sigma^p]$-structure of the ring of integers of L. Since this structure is completely determined by ramification invariants and since $\langle \sigma^p \rangle$ is the maximal proper subgroup of G, we are justified in saying that the Galois structure of the integers in a cyclic stably ramified p-extension is 'almost' completely determined by the ramification invariants.

What about unstably ramified extensions? Wyman has shown that the ramification filtration in $\mathbb{Z}_p$-extensions eventually stabilizes [11]. Thus, among the infinitely many cyclic extensions of degree p^n that lie in a $\mathbb{Z}_p$-extension, only finitely many are not covered by the main result of [5]. So, in a sense, ramification invariants are 'generally sufficient' for cyclic p-extensions.

1.3. Elementary abelian extensions. On the other hand, extensions with $G \cong C_p^n$ may have from 1 to n Hilbert breaks. Indeed the situation, where there are not enough ramification invariants, is essentially an elementary abelian problem – one of the quotients G_i/G_{i+1} is not cyclic. As such, the deficiency of Hilbert's ramification filtration is a deficiency of elementary abelian Galois groups. We propose to repair it on the elementary abelian level.

It is worth mentioning that our proposal arises from an effort to generalize the main result of [2], concerning the Galois module structure of ideals for biquadratic extensions, to bicyclic extensions, $G \cong C_p \times C_p$. Curiously,

we were led to truncated exponentiation: of $\sigma \in G$ by $\omega \in \mathfrak{O}_T^*$,

$$\sigma^{[\omega]} = \sum_{i=0}^{p-1} \binom{\omega}{i} (\sigma - 1)^i.$$

This paper may be viewed as an attempt to understand this expression.

We begin by asking for an appropriate environment. There are two natural candidates: $\mathfrak{O}_T[G]$ and $\mathbb{F}_q[G]$. Weiss has shown that up to conjugation $\mathfrak{O}_T[G]$ contains only one finite p-group (namely G itself) [10]. As we want the 'appropriate environment' to generalize the Galois group (and thus be finite), we choose $\mathbb{F}_q[G]$.

Now truncated exponentiation $x^{[\omega]}$, of $x \in \mathbb{F}_q[G]$ by $\omega \in \mathbb{F}_q$, can be viewed as an $\mathbb{F}_q$-action on $\mathbb{F}_q[G]$, and Theorem 2.1 explains that this action is a consequence of certain natural properties. Define $G^{\mathcal{F}}$ to be the closure of G under this action. We suggest that a *refined ramification filtration* upon $G^{\mathcal{F}}$ should yield arithmetically interesting information. Indeed in §4, we show this to be the case for $G \cong C_2 \times C_2$.

Note that the idea of filtering something besides the Galois group to obtain invariants related to Galois module structure is not new. For example, see [1]. We have, however, chosen a minimal object. And though our refined filtration cannot, at this point, be considered canonical (it depends upon a choice of element $\alpha \in L$); given an α that is chosen 'well', Theorem 3.3 and its corollary say that $G^{\mathcal{F}}$ is as 'big as possible' – indicating that the group $G^{\mathcal{F}}$ is.

2. Elementary Abelian Groups under $\mathbb{F}_q$-action

Recall that $\mathbb{F}_q$ denotes the finite field with $q = p^f$ elements. Let $G = C_p^n$ be an elementary abelian group, and let $J = \langle \sigma - 1 : \sigma \in G \rangle$ be the Jacobson radical of the group ring $\mathbb{F}_q[G]$. So $1 + J$ denotes the group of 1-units in $\mathbb{F}_q[G]$. The finite field $\mathbb{F}_p$ possesses a natural action (via exponentiation) on the $1 + J$. If this is extended to an $\mathbb{F}_q$-action, what properties should the $\mathbb{F}_q$-action have?

Let $(\omega, 1 + x) \in 1 + J$, denote the effect of $\omega \in \mathbb{F}_q$ acting upon $1 + x$ for $x \in J$. At a minimum we should ask that

(1) $(1, 1 + x) = 1 + x$, for all $x \in J$, and

(2) $(\omega_1 + \omega_2, 1 + x) = (\omega_1, 1 + x) \cdot (\omega_2, 1 + x)$ for all $\omega_1, \omega_2 \in \mathbb{F}_q, x \in J$.

These properties determine the action of $\mathbb{F}_p$ and the fact that $(0, 1 + x) = (p, 1+x) = (1, 1+x)^p = 1$. But for $f > 1$, they are not sufficient to uniquely determine an $\mathbb{F}_q$-action. We must include further properties.

Observe that for $x \in J$, $x^p = 0$. To see this express $x \in J$ as a linear combination of terms $(\sigma_1 - 1)^{a_1} \cdots (\sigma_n - 1)^{a_n}$ for $\sigma_1, \ldots, \sigma_n$ generators of G and $a_i \geq 1$ for at least one i. Now note that for $\omega \in \mathbb{F}_p$, $(\omega, 1 + x) =$

$\sum_{i=0}^{p-1} \binom{\omega}{i} x^i$ is a polynomial in x with coefficients dependent only upon ω. This should hold for all $\omega \in \mathbb{F}_q$. And so we ask that there are functions $f_i : \mathbb{F}_q \longrightarrow \mathbb{F}_q$ such that

$$(\omega, 1+x) = 1 + \sum_{i=1}^{p-1} f_i(\omega) x^i \quad \text{for all } \omega \in \mathbb{F}_q, x \in J. \tag{3}$$

Turn to the situation considered in §1.3. Given two nontrivial elements $\sigma_1, \sigma_2 \in G_i \setminus G_{i+1}$, we have $v_L((\sigma_1 - 1)\pi_L) = v_L((\sigma_2 - 1)\pi_L) = i + 1$. Since L/T is fully ramified, there is a unit $\tilde{\omega} \in \mathfrak{O}_T$ such that $(\sigma_1 - 1)\pi_L \equiv \tilde{\omega}(\sigma_2 - 1)\pi_L \bmod \pi_L^{i+2}$. So $\sigma_1 \pi_L \equiv [1 + \tilde{\omega}(\sigma_2 - 1)]\pi_L \bmod \pi_L^{i+2}$. We can approximate the *effect* of one group element by the *effect* of an expression involving another. Motivated by this and the fact that $\mathfrak{O}_T / p\mathfrak{O}_T = \mathbb{F}_q$, we ask that $f_1(\omega) = \omega$. In other words,

$$(\omega, 1+x) \equiv 1 + \omega x \bmod x^2, \quad \text{for } \omega \in \mathbb{F}_q, x \in J. \tag{4}$$

Finally, we require

$$(\omega_1, (\omega_2, 1+x)) = (\omega_2, (\omega_1, 1+x)) \quad \text{for } \omega_1, \omega_2 \in \mathbb{F}_q, x \in J, \tag{5}$$

Theorem 2.1. *There is only one $\mathbb{F}_q$-action on $1+J$ that satisfies properties* (1) through (5). *It is provided by truncated exponentiation: $(\omega, 1+x) \to (1+x)^{[\omega]}$ for $\omega \in \mathbb{F}_q$, $x \in J$. Moreover $\left((1+x)^{[\omega_1]}\right)^{[\omega_2]} = (1+x)^{[\omega_1 \omega_2]}$ for $\omega_i \in \mathbb{F}_q$ and $x \in J$.*

Proof. First we check that $(1+x)^{[\omega]}$ satisfies the properties: (1), (3), (4) are trivial, while (2), (5) rely upon the fact that $x^p = 0$ for $x \in J$. In the polynomial ring $\mathbb{Q}[x, y, z]/(x^p)$, we have $(1+x)^{[y]} \cdot (1+x)^{[z]} = (1+x)^y \cdot (1+x)^z = (1+x)^{y+z} = (1+x)^{[y+z]}$, and $\left((1+x)^{[y]}\right)^{[z]} = ((1+x)^y)^z = (1+x)^{yz} = (1+x)^{[yz]}$. Thus $(1+x)^{[y]} \cdot (1+x)^{[z]} = (1+x)^{[y+z]}$, and $\left((1+x)^{[y]}\right)^{[z]} = (1+x)^{[yz]}$ in $\mathbb{Z}_{(p)}[x, y, z]/(x^p)$. Reduce modulo p. The resulting polynomial identities in $\mathbb{F}_p[x, y, z]/(x^p)$ yield (2) and (5) respectively.

We use induction to prove that truncated exponentiation is the *only* such $\mathbb{F}_q$-action. Note $f_1(\omega) = \binom{\omega}{1}$. Suppose $f_i(\omega) = \binom{\omega}{i}$ for all i such that $1 \leq i < k \leq p-1$, and consider $f_k(\omega)$. Since $\left((1+x)^{[y]}\right)^{[z]} \equiv \left((1+x)^{[z]}\right)^{[y]} \bmod x^{k+1}$ in $\mathbb{Z}_{(p)}[x, y, z]/(x^p)$, $\sum_{j=0}^{k} \binom{\omega_2}{j} \left[\sum_{i=1}^{k} \binom{\omega_1}{i} x^i\right]^j \equiv \sum_{j=0}^{k} \binom{\omega_1}{j} \left[\sum_{i=1}^{k} \binom{\omega_2}{i} x^i\right]^j \bmod x^{k+1}$ for $\omega_i \in \mathbb{F}_p$, $x \in J$. Compare this to the similar expression from property (5), $\sum_{j=0}^{k} f_j(\omega_2) \left[\sum_{i=1}^{k} f_i(\omega_1) x^i\right]^j \equiv \sum_{j=0}^{k} f_j(\omega_1) \left[\sum_{i=1}^{k} f_i(\omega_2) x^i\right]^j \bmod x^{k+1}$. Subtract, note that $f_i(\omega) = \binom{\omega}{i}$

for all $1 \leq i < k$, and look at the coefficient of x^k. Thus $(\omega_1 - \omega_1^k)f_k(\omega_2) - (\omega_2 - \omega_2^k)f_k(\omega_1) = (\omega_1 - \omega_1^k)\binom{\omega_2}{k} - (\omega_2 - \omega_2^k)\binom{\omega_1}{k}$. Set $\omega_1 = r$, a primitive root of $\mathbb{F}_p$ (order of r is $p-1$). By properties (1) and (2), $f_k(r) = \binom{r}{k}$. So $(r - r^k)f_k(\omega_2) = (r - r^k)\binom{\omega_2}{k}$. Since $1 < k \leq p-1$, $r - r^k \neq 0$. So $f_k(\omega_2) = \binom{\omega_2}{k}$. □

We are interested in G, a subgroup of $1 + J$, which is closed under $\mathbb{F}_p$ but not under $\mathbb{F}_q$. Thus we are led to the following

Definition. Let $G^{\mathcal{F}}$ be the least subgroup with $G \subseteq G^{\mathcal{F}} \subseteq 1 + J$ that is closed under $\mathbb{F}_q$.

2.1. Near Spaces. A *near space* is a group upon which $\mathbb{F}_q$ operates, satisfying all the properties of a vector space *except* the distributive property [8]. Since $J^p \neq \{0\}$ if $G \neq C_p$ (even though $x^p = 0$ for $x \in J$), distribution does not generally hold and $G^{\mathcal{F}}$ is a near space. For example consider $p = 2$. If $\omega \in \mathbb{F}_{2^f} \setminus \mathbb{F}_2$, $x, y \in J$ and $xy \neq 0$, then $((1+x)(1+y))^{[\omega]} = 1 + \omega(x + y + xy) \neq 1 + \omega(x + y) + \omega^2 xy = (1 + x)^{[\omega]} \cdot (1 + y)^{[\omega]}$. Indeed distribution holds only for $G \cong C_p$ or $\mathbb{F}_p = \mathbb{F}_q$. So we will focus on $G^{\mathcal{F}}$ under $|G| > p$ and $\mathbb{F}_p \subsetneq \mathbb{F}_q$. A *near basis* will be a minimal generating set over $\mathbb{F}_q$.

Define the *ω-commutator*, $[a, b]_\omega = (ab)^{[\omega]}a^{[-\omega]}b^{[-\omega]}$ for $a, b \in G^{\mathcal{F}}$ and $\omega \in \mathbb{F}_q$. We could equally well call this the ω-distributor: If $[a, b]_\omega \neq 1$, the $\mathbb{F}_q$-action does not distribute. However when $\omega = 1$ this expression resembles the usual commutator of group theory. Following [8], we define an *ideal* $\mathcal{I}$ of $G^{\mathcal{F}}$ to be any subgroup of $G^{\mathcal{F}}$ that is closed under the $\mathbb{F}_q$-action with $[g, i]_\omega \in \mathcal{I}$ for $g \in G^{\mathcal{F}}$, $i \in \mathcal{I}$ and $\omega \in \mathbb{F}_q$.

Define a commutator of ideals, A and B, to be the ideal generated by the commutators $[A, B] = \big([a, b]_\omega : a \in A, b \in B, \omega \in \mathbb{F}_q\big)$. Let the *derived series* of $G^{\mathcal{F}}$ be defined by $\mathcal{A}_0 = G^{\mathcal{F}}$ and $\mathcal{A}_{n+1} := [\mathcal{A}_n, \mathcal{A}_n]$. Note $\mathcal{A}_n/\mathcal{A}_{n+1}$ is a vector space. So if $\ell(G^{\mathcal{F}})$ is the length of the derived series, the minimal integer ℓ such that $\mathcal{A}_\ell = \{1\}$ or ∞, then $\ell(G^{\mathcal{F}})$ measures the lack of the distributivity.

2.2. A bound on the length of the derived series. Let $G \cong C_p^n$. In this section we bound $\ell(G^{\mathcal{F}}) < \infty$. Indeed, for a fixed n, it is almost always the case that $\ell(G^{\mathcal{F}}) = 2$. First we need a lemma.

Recall that $\mathbb{Z}_{(p)}$ denotes the localization of $\mathbb{Z}$ at p. Consider the commutator, $[1 + X, 1 + Y]_W = \big((1 + X)(1 + Y)\big)^{[W]}(1 + X)^{[-W]}(1 + Y)^{[-W]} \in \mathbb{Z}_{(p)}[X, Y, W]$. We shall relate this to the polynomial

$$Q(X, Y) := \frac{(X + Y + XY)^p - X^p - Y^p - X^pY^p}{p} \in \mathbb{Z}[X, Y].$$

Lemma 2.2. *In the quotient ring* $\mathcal{R} := \mathbb{Z}_{(p)}[X,Y,W]/(X^p, Y^p)$ *we have the congruence* $[1+X, 1+Y]_W \equiv 1 + (W^p - W)Q(X,Y) \pmod{p\mathcal{R}}$.

Proof. Set $T = X + Y + XY \in \mathcal{R}$. As $X^p = Y^p = 0$, we have $T^{2p-1} = 0$, while $T^p = pQ(X,Y) \in p\mathcal{R}$. The usual binomial expansions result in $(1+X)^W = \sum_{i=0}^{p-1} \binom{W}{i} X^i$, $(1+Y)^W = \sum_{i=0}^{p-1} \binom{W}{i} Y^i$ and $(1+T)^W = \sum_{i=0}^{2p-2} \binom{W}{i} T^i$. These expressions are all in $\mathcal{R}$ since for $0 \le i \le p-1$, $\binom{W}{i} \in \mathbb{Z}_{(p)}[W]$, $\binom{W}{p+i} \in p^{-1}\mathbb{Z}_{(p)}[W]$ and $T^{p+i} = pQ(X,Y)T^i$. Thus $(1+X)^{[W]}(1+Y)^{[W]} = (1+X)^W(1+Y)^W = (1+T)^W$.

To analyse the expression for $(1+T)^W$ further, note that we have the congruences $p\binom{W}{p} \equiv W - W^p \pmod{p\mathbb{Z}_{(p)}[W]}$ and $p\binom{W}{p+i} \equiv p\binom{W}{p}\binom{W}{i} \pmod{p\mathbb{Z}_{(p)}[W]}$ for $0 \le i \le p-1$. Hence

$$\begin{aligned}(1+T)^W &\equiv \left(1 + \binom{W}{1} + \ldots + \binom{W}{p-1} T^{p-1}\right)\left(1 + p\binom{W}{p} Q(X,Y)\right) \\ &\equiv (1+T)^{[W]}\,(1 + (W - W^p)Q(X,Y)) \pmod{p\mathcal{R}}.\end{aligned}$$

Therefore $(1+X)^{[W]}(1+Y)^{[W]} \equiv (1+T)^{[W]}(1 + (W - W^p)Q(X,Y)) \pmod{p\mathcal{R}}$. Since $Q(X,Y)^2 = 0$,

$$(1 + (W - W^p)Q(X,Y))(1 + (W^p - W)Q(X,Y)) = 1.$$

The result now follows since $(1+X)^{[W]}(1+X)^{[-W]} = (1+X)^W(1+X)^{-W} = 1$ and $(1+Y)^{[W]}(1+Y)^{[-W]} = (1+Y)^W(1+Y)^{-W} = 1$. □

Corollary 2.3. *For any* $x, y \in J$ *and* $\omega \in \mathbb{F}_q$ *we have* $[1+x, 1+y]_\omega = 1 + (\omega^p - \omega)Q(x,y)$. *In particular* $\mathcal{A}_1 \subseteq 1 + J^p$.

Proof. Since $x^p = 0$ and $y^p = 0$, there is a ring homomorphism $\mathcal{R} \longrightarrow G^{\mathcal{F}}$ given by reduction mod p followed by the specialization $X = x$, $Y = y$, $W = \omega$. The identity in the lemma then yields the first assertion. The second assertion follows since $G^{\mathcal{F}} \subseteq 1 + J$, and $\mathcal{A}_1$ is generated by elements of the form $[1+x, 1+y]_\omega$. □

Let $\lceil x \rceil$ denote the least integer function (the ceiling function).

Proposition 2.4. *If* $G \cong C_p^n$ *and* $\mathbb{F}_p \subsetneq \mathbb{F}_q$, *then*

$$\ell(G^{\mathcal{F}}) \le \lceil \log_p(n(p-1)+1) \rceil.$$

Proof. Using the pigeon hole principle, $J^{n(p-1)+1} = \{0\}$. Note $G^{\mathcal{F}} = \mathcal{A}_0 \subseteq 1 + J$. Using Corollary 2.3, $[1 + J^n, 1 + J^n] \subseteq 1 + J^{pn}$. Thus $[1 + J^{p^{k-1}}, 1 + J^{p^{k-1}}] \subseteq 1 + J^{p^k}$. So $\mathcal{A}_k \subseteq 1 + J^{p^k}$. □

Corollary 2.5. *Let* $G \cong C_p^n$. *If* $\mathbb{F}_p \subsetneq \mathbb{F}_q$ *and* $p \ge n-1$, *then* $\ell(G^{\mathcal{F}}) = 2$.

It is natural to ask the following

Question. Is the bound given by Proposition 2.4 tight?

For $p = 2$, $Q(x, y) = xy$ is a monomial. Indeed it is a simple calculation to check

$$[1 + x, 1 + y]_\omega = 1 + (\omega - \omega^2)xy. \tag{6}$$

And so we are able to answer the question in this particular case.

Proposition 2.6. *Let $G \cong C_2^n$ and $\mathbb{F}_2 \subsetneq \mathbb{F}_q$, then $G^{\mathcal{F}} = 1 + J$ and $\ell(G^{\mathcal{F}}) = \lceil \log_2(n + 1) \rceil$.*

Proof. First we prove that $G^{\mathcal{F}} = 1 + J$. To do so, it is helpful to note that we can express any element of $1 + J$ as a product of elements of the form $1 + \omega_* X^{(m)}$, where $\omega_* \in \mathbb{F}_q$ and $X^{(m)} = (\sigma_1 - 1) \dots (\sigma_m - 1)$ for $\langle \sigma_1, \dots, \sigma_m \rangle$ a subgroup of G with degree p^m. To prove that $1 + J \subseteq G^{\mathcal{F}}$ it suffices to prove that each $1 + \omega_* X^{(m)} \in G^{\mathcal{F}}$. This follows by induction using (6). Note that $[1 + x, 1 + y]_\omega^{[\omega_*/(\omega - \omega^2)]} = 1 + \omega_* xy$.

Again using (6), it is easy to show that $[1 + J^{2^k}, 1 + J^{2^k}] \subseteq 1 + J^{2^{k+1}}$. To prove $1 + J^{2^{k+1}} \subseteq [1 + J^{2^k}, 1 + J^{2^k}]$, we again note that any element of $1 + J^{2^{k+1}}$ can be decomposed into a product of elements of the form $1 + \omega_* X^{(m)}$, where $m \geq 2^{k+1}$. One can break $X^{(m)}$ into the product of two monomials of degree $\geq 2^k$. Using (6), we can prove that $1 + \omega_* X^{(m)} \in [1 + J^{2^k}, 1 + J^{2^k}]$. Thus $A_k = 1 + J^{2^k}$. □

2.3. A basis for $(C_p^2)^{\mathcal{F}}$. In this section, we restrict our attention to one particular elementary abelian group, $G \cong C_p^2$ with generators σ, γ, and give a complete description of $G^{\mathcal{F}}$. Assume $\mathbb{F}_p \subsetneq \mathbb{F}_q$. Using Proposition 2.4, $\ell(G^{\mathcal{F}}) \leq 2$. Thus $\mathcal{A}_1$ is a vector space. Our first result establishes the existence of $p - 1$ elements of $\mathcal{A}_1$ that are linearly independent over $\mathbb{F}_q$.

Lemma 2.7. *Choose $\omega \in \mathbb{F}_q \setminus \mathbb{F}_p$ and set $\psi_i := [\sigma, \gamma^i]_\omega$. Then $\{\psi_i : 1 \leq i \leq p - 1\}$ is a basis for the $\mathbb{F}_q$-vector space $(1 + J^p)/(1 + J^{p+1})$. Moreover, for $1 \leq j \leq p - 1$,*

$$\Psi_j := \prod_{i=1}^{p-1} \psi_i^{-j(-i)^{j-1}} \equiv 1 + (\omega^p - \omega)(\sigma - 1)^j (\gamma - 1)^{p-j} \bmod 1 + J^{p+1}.$$

Proof. Clearly $(1 + J^p)/(1 + J^{p+1})$ is a vector space. Let $x = \sigma - 1$ and $y = \gamma - 1$ then $\{1 + x^j y^{p-j} : 1 \leq j \leq p - 1\}$ is an $\mathbb{F}_q$-basis. Note that for $1 \leq k \leq p - 1$, $\binom{p}{k} p^{-1} \in \mathbb{Z}$. Furthermore

$$\binom{p}{k} p^{-1} \equiv (-1)^{p-k} k^{-1} \bmod p. \tag{7}$$

Since $\gamma^i = (1 + y)^i \equiv 1 + iy \pmod{y^2}$, using Corollary 2.3 and (7) we find that $\psi_i \equiv 1 + (\omega^p - \omega) \sum_{k=1}^{p-1} (-i)^{p-k} k^{-1} \cdot x^k y^{p-k} \pmod{1 + J^{p+1}}$. Because

the product of any two elements in J^p is zero,

$$\begin{aligned}\Psi_j &= \prod_{i=1}^{p-1} \psi_i^{-j(-i)^{j-1}} \\ &\equiv 1 + (\omega^p - \omega) \sum_{i=1}^{p-1} -j(-i)^{j-1} \cdot \sum_{k=1}^{p-1} (-i)^{p-k} k^{-1} \cdot x^k y^{p-k} \\ &\equiv 1 + (\omega^p - \omega) \sum_{k=1}^{p-1} C_{j,k} x^k y^{p-k} \pmod{1 + J^{p+1}},\end{aligned}$$

where $C_{j,k} = \sum_{i=1}^{p-1} -j(-i)^{j-1} \cdot (-i)^{p-k} k^{-1} \equiv -jk^{-1} \cdot \sum_{s=1}^{p-1} (r^s)^{p-k+j-1} \bmod p$ for r a primitive root. Thus if $j = k$, $C_{j,k} \equiv 1 \bmod p$. Otherwise $C_{j,k} \equiv 0 \bmod p$. □

To prove that the ψ_i span $\mathcal{A}_1$ we need the following

Lemma 2.8. *Choose $\omega \in \mathbb{F}_q \setminus \mathbb{F}_p$ and define Ψ_j as in Lemma 2.7. Then*

$$\left[\sigma^{[\omega_1]}, \gamma^{[\omega_2]}\right]_\omega = \prod_{j=1}^{p-1} \Psi_j^{\left[\frac{(-1)^{j-1}}{j} \omega_1^j \omega_2^{p-j}\right]}$$

Proof. Specializing the polynomial ring $\mathbb{Z}_{(p)}[z, z_1, z_2, x, y]/(x^p, y^p)$ modulo p by setting $x = \sigma - 1$, $y = \gamma - 1$, $z = \omega$ and $z_i = \omega_i$ (for $i = 1, 2$), we obtain a ring into which $\mathbb{F}_p[\omega, \omega_1, \omega_2][G]$ has an obvious injection. Our proof will rely upon Corollary 2.3 and the verification of an identity (resulting from expression above) in the polynomial ring, $\mathbb{Z}_{(p)}[z, z_1, z_2, x, y]/(x^p, y^p)$.

Consider the right-hand-side of the identity. Recall the expression for Ψ_j in Lemma 2.7. Note that since $\Psi_j \in 1 + J^p$, $(\Psi_j - 1)(\Psi_k - 1) = 0$. So $\prod_{j=1}^{p-1} \Psi_j^{\left[(-1)^{j-1} j^{-1} \omega_1^j \omega_2^{p-j}\right]} = 1 + \sum_{j=1}^{p-1} (-1)^{j-1} j^{-1} \omega_1^j \omega_2^{p-j} (\Psi_j - 1) = 1 - \sum_{j=1}^{p-1} \sum_{i=1}^{p-1} i^{j-1} \omega_1^j \omega_2^{p-j} (\psi_i - 1)$. Now identify ψ_i with $[1 + x, (1 + y)^i]_z$. Set $(1 + y)^i = 1 + y_i \in \mathbb{Z}_{(p)}[y]/(y^p)$. Since $y_i = y \cdot Y$ for some $Y \in \mathbb{Z}_{(p)}[y]/(y^p)$, we find that $y_i^p = y^p \cdot Y^p = 0$. Thus using Lemma 2.2, $[1+x, 1+y_i]_z \equiv 1 - \binom{z}{p} ((1 + x)(1 + y_i) - 1)^p = 1 - \binom{z}{p} \left((1 + x)(1 + y)^i - 1\right)^p \bmod p$. The right-hand-side of the identity to be proven is mapped to $1 + \binom{z}{p} \sum_{j=1}^{p-1} \sum_{i=1}^{p-1} i^{j-1} z_1^j z_2^{p-j} \left((1 + x)(1 + y)^i - 1\right)^p \bmod p$. It is worth mentioning that this expression differs from 1 by a linear combination of monomials $x^r y^s$ with $r, s < p$ and $r + s \geq p$.

Now consider the left-hand-side of the identity. Set $(1+x)^{[z_1]} = 1+x'$ and $(1+y)^{[z_2]} = 1+y'$. As was the case with y_i, $(x')^p = (y')^p = 0$. So using Lemma 2.2, $\left[(1+x)^{[z_1]}, (1+y)^{[z_2]}\right]_z \equiv 1 - \binom{z}{p}\left((1+x)^{[z_1]}(1+y)^{[z_2]} - 1\right)^p \pmod{p}$.

Taking into account the p in the denominator of $\binom{z}{p}$, the lemma is verified if we can show in $\mathbb{Z}_{(p)}[z, z_1, z_2, x, y]/(x^p, y^p)$ that

(8)
$$\left((1+x)^{[z_1]}(1+y)^{[z_2]} - 1\right)^p \equiv \sum_{i=1}^{p-1} c_i \left((1+x)(1+y)^i - 1\right)^p \pmod{p^2}$$

where

(9)
$$c_i = -\sum_{j=1}^{p-1} i^{j-1} z_1^j z_2^{p-j}.$$

Expand the pth powers in (8), use (7) to replace $\binom{p}{k}$. Now compare coefficients of $x^r y^s$ on both sides, where $r, s < p$ and $r+s \geq p$. Our identity, which was reduced to (8), is now further reduced to determining whether $\binom{z_1 p}{r}\binom{z_2 p}{s} + \sum_{k=1}^{p-1} k^{-1} p \binom{z_1 k}{r}\binom{z_2 k}{s} \equiv \sum_{i=1}^{p-1} c_i \left(\binom{p}{r}\binom{ip}{s} + \sum_{k=1}^{p-1} k^{-1} p \binom{k}{r}\binom{ik}{s}\right)$ (mod p^2) for all pairs (r, s), or whether

(10)
$$\sum_{k=1}^{p-1} k^{-1} \binom{z_1 k}{r}\binom{z_2 k}{s} \equiv \sum_{i=1}^{p-1} c_i \left(\sum_{k=1}^{p-1} k^{-1} \binom{k}{r}\binom{ik}{s}\right) \pmod{p}.$$

We verify this condition now, an identity in $\mathbb{F}_p[z_1, z_2]$ with the c_i as in (9), for all relevant pairs (r, s) . Recall that for an indeterminate X and an integer $r \geq 1$ we have $\binom{X}{r} = \frac{1}{r!}\sum_{u=1}^{r}(-1)^{r-u}\begin{bmatrix} r \\ u \end{bmatrix} X^u$, for some coefficients $\begin{bmatrix} r \\ u \end{bmatrix} \in \mathbb{Z}$ (Stirling numbers of the first kind [7, p249].) The left-hand side of (10) becomes

(11)
$$\frac{1}{r!s!}\sum_{k=1}^{p-1}\sum_{u=1}^{r}\sum_{v=1}^{s}(-1)^{r-u+s-v}\begin{bmatrix} r \\ u \end{bmatrix}\begin{bmatrix} s \\ v \end{bmatrix} k^{-1}(z_1 k)^u (z_2 k)^v$$
$$\equiv \frac{(-1)^{r+s-p+1}}{r!s!}\sum_{u+v=p}\begin{bmatrix} r \\ u \end{bmatrix}\begin{bmatrix} s \\ v \end{bmatrix} z_1^u z_2^v \pmod{p}.$$

Replacing the c_i using (9), the right-hand side of (10) becomes

$$(12)\qquad \frac{1}{r!s!}\sum_{i=1}^{p-1}\sum_{k=1}^{p-1}\sum_{u=1}^{r}\sum_{v=1}^{s}(-1)^{r-u+s-v}c_i\begin{bmatrix}r\\u\end{bmatrix}\begin{bmatrix}s\\v\end{bmatrix}i^v k^{u+v-1}$$

$$\equiv \frac{(-1)^{r+s-p+1}}{r!s!}\sum_{i=1}^{p-1}\sum_{u+v=p} c_i\begin{bmatrix}r\\u\end{bmatrix}\begin{bmatrix}s\\v\end{bmatrix}i^v$$

$$\equiv \frac{(-1)^{r+s-p}}{r!s!}\sum_{i=1}^{p-1}\sum_{u+v=p}\begin{bmatrix}r\\u\end{bmatrix}\begin{bmatrix}s\\v\end{bmatrix}\sum_{j=1}^{p-1} i^{v+j-1}z_1^j z_2^{p-j}$$

$$\equiv \frac{(-1)^{r+s-p+1}}{r!s!}\sum_{u+v=p}\begin{bmatrix}r\\u\end{bmatrix}\begin{bmatrix}s\\v\end{bmatrix}z_1^u z_2^v \pmod p.$$

Note that (11) and (12) agree. □

This leads to the main result of the section.

Theorem 2.9. *Let $G = \langle\sigma,\gamma\rangle \cong C_p^2$. Suppose $\mathbb{F}_p \subsetneq \mathbb{F}_q$ and choose $\omega \in \mathbb{F}_q \setminus \mathbb{F}_p$. Then $\mathcal{A}_1$ is a vector space over $\mathbb{F}_q$ with basis $\{[\sigma,\gamma^i]_\omega : i = 1,\dots,p-1\}$. Indeed,*

$$G^{\mathcal{F}} = \left\{\sigma^{[\omega_{-1}]}\cdot\gamma^{[\omega_0]}\cdot\prod_{i=1}^{p-1}[\sigma,\gamma^i]_\omega^{[\omega_i]} : \omega_i \in \mathbb{F}_q\right\}$$

Proof. Set $A = \left\{\sigma^{[\omega_{-1}]}\cdot\gamma^{[\omega_0]}\cdot\prod_{j=1}^{p-1}\psi_j^{[\omega_j]} : \omega_j \in \mathbb{F}_q\right\}$. This is clearly a subgroup. It is easy to see, since $\psi_j = [\sigma,\gamma^j]_\omega \in G^{\mathcal{F}}$, that $A \subseteq G^{\mathcal{F}}$. To show that $G^{\mathcal{F}} \subseteq A$, we need only show that A is closed under $\mathbb{F}_q$. Note $\prod_{j=1}^{p-1}\psi_j^{[\omega_j]} \in 1 + J^p$. The result will follow from Lemma 2.8 and the fact that for $a \in J$ and $b \in J^p$, $\big((1+a)(1+b)\big)^{[\omega]} = (1+a)^{[\omega]}(1+b)^{[\omega]}$ while $(1+b)^{[\omega]} = 1+\omega b$. First observe that $J^{2p-1} = \{0\}$. So $b^2 = a^{p-1}b = 0$. Thus $(1+b)^{[\omega]} = 1+\omega b$. Now expand $\big((1+a)(1+b)\big)^{[\omega]} = \sum_{i=0}^{p-1}\binom{\omega}{i}(a+b(1+a))^i = \sum_{i=0}^{p-1}\binom{\omega}{i}a^i + \left(\sum_{i=1}^{p-1}\binom{\omega}{i}i(a^{i-1}+a^i)\right)b$ carefully using $\binom{\omega}{i+1}(i+1)+\binom{\omega}{i}i = \omega\binom{\omega}{i}$. □

Remark. For a given value of p, Theorem 2.9 can be verified computationally. In fact this is how it was discovered, using MAPLE.

3. Ramification Filtrations

Elementary abelian groups G can be viewed as vector spaces over $\mathbb{F}_p$. From this perspective, the fact that $\dim_{\mathbb{F}_p} G$ may exceed the number of Hilbert breaks is a deficiency. In this section we define a family of *refined ramification filtrations* of $G^{\mathcal{F}}$ and prove that these refined filtrations lack

the deficiency of the Hilbert filtration: $\dim_{\mathbb{F}_q} G^{\mathcal{F}}$ equals the number of *refined breaks.*

3.1. Refined Ramification Filtration. To define a ramification filtration of $G^{\mathcal{F}}$ we need $G^{\mathcal{F}} \subseteq \mathbb{F}_q[G]$ to act in a well-defined manner upon elements of L. Naturally, the action should be through $\mathfrak{O}_T[G]$. We also need a well-defined notion of valuation. Consider the following example: Suppose $\alpha \neq 0$. Choose $x = 1 \in \mathbb{F}_q[G]$, and for $k \geq 1$, $y_k = 1 + p^k$, $y_\infty = 1$ elements of $\mathfrak{O}_T[G]$. View elements of $\mathbb{F}_q[G]$ as cosets of $p\mathfrak{O}_T[G]$ in $\mathfrak{O}_T[G]$. Then $y_k + p\mathfrak{O}_T[G] = x$ for all k, and $v_L((y_1 - 1)\alpha) < \cdots < v_L((y_k - 1)\alpha) < \cdots < v_L((y_\infty - 1)\alpha) = \infty$. Since one would reasonably expect $(x-1)\alpha$ to have infinite 'valuation', we are led to the following definition: For $\alpha \in L$ and $x \in G^{\mathcal{F}}$ define

$$w_\alpha(x) = \sup\{v_L((y-1)\alpha) : y \in \mathfrak{O}_T[G],\ y + p\mathfrak{O}_T[G] = x\} \tag{13}$$

where sup denotes the supremum. Note that $w_\alpha(x) = \infty$ for $\alpha \in L$ and $x = 1$, also for $\alpha \in K$ and $x \in G^{\mathcal{F}}$.

Definition. A *refined ramification filtration* of $G^{\mathcal{F}}$ is defined for $\alpha \in L$ by $G_i^{\mathcal{F},\alpha} = \{x \in G^{\mathcal{F}} : w_\alpha(x) \geq v_L(\alpha) + i\}$,

The purpose of these filtrations is to provide interesting arithmetic information. If $\alpha \in K$, then $w_\alpha(x) = \infty$ for all $x \in G^{\mathcal{F}}$. So $G^{\mathcal{F}} = G_\infty^{\mathcal{F},\alpha}$ and the filtration is decidedly uninteresting. To avoid this problem, we will restrict ourselves to α from

$$\mathcal{N} = \{\alpha \in L : \forall x \in G^{\mathcal{F}} \setminus \{1\}, w_\alpha(x) < \infty\}.$$

To prove $\mathcal{N} \neq \emptyset$, we consider another class of element. By the Normal Basis Theorem there are elements $\alpha \in L$ that generate a normal basis for L over K. Collect these elements together as

$$\mathcal{N}_b = \left\{\alpha \in L : \sum_{\sigma \in G} K \cdot \sigma\alpha = L\right\}.$$

Note the following

Lemma 3.1. $\emptyset \neq \mathcal{N}_b \subseteq \mathcal{N}$

Proof. By the Normal Basis Theorem, $\emptyset \neq \mathcal{N}_b$. Now observe the following basic property of $\mathfrak{O}_T$-lattices: Given any $\mathfrak{O}_T$-lattice $\mathcal{U} \subset L$ there is a bound $B_{\mathcal{U}}$ such that for $u \in \mathcal{U}$,

$$u \notin p\mathcal{U} \implies v_L(u) \leq B_{\mathcal{U}}.$$

Without restriction we may suppose that $\mathcal{U}$ is a full-dimensional lattice. Then there exist $a < b \in \mathbb{Z}$ with $p^a\mathfrak{O}_L \subset \mathcal{U} \subset p^b\mathfrak{O}_L$ and so $\mathcal{U} \setminus p\mathcal{U} \subset p^b\mathfrak{O}_L \setminus p^{a+1}\mathfrak{O}_L$. Let $B_{\mathcal{U}} = (a+1)v_L(p)$.

Now let $\alpha \in \mathcal{N}_b$. Note that $\mathfrak{O}_T[G]\alpha$ is an $\mathfrak{O}_T$-lattice. Let $y \in \mathfrak{O}_T[G]$ with $y + p\mathfrak{O}_T[G] = x$. Then $y \not\equiv 1 \bmod p$, $(y-1)\alpha \notin p\mathfrak{O}_T[G]\alpha$, and so $v_L((y-1)\alpha) \leq B_{\mathfrak{O}_T[G]\alpha}$. Therefore $w_\alpha(x) \leq B_{\mathfrak{O}_T[G]\alpha} < \infty$. □

Lemma 3.2. *For $\alpha \in \mathcal{N}$, $G_i^{\mathcal{F},\alpha}$ is an ideal of $G^{\mathcal{F}}$.*

Proof. Throughout x_j will denote an element of $G_i^{\mathcal{F},\alpha}$, and $y_j \in \mathfrak{O}_T[G]$ with $y_j + p\mathfrak{O}_T[G] = x_j$ and $v_L((y_j-1)\alpha) \geq v_L(\alpha) + i$. Let $\bar{\omega} \in \mathbb{F}_q$ and $\omega \in \mathfrak{O}_T$ with $\omega + p\mathfrak{O}_T = \bar{\omega}$. First we check that the sets are closed under multiplication. Note that $y_1 \cdot y_2 + p\mathfrak{O}_T[G] = x_1 \cdot x_2$ and $y_1y_2 - 1 = y_1(y_2-1) + (y_1-1)$. Since $v_L(y_1(y_2-1)\alpha) \geq v_L(\alpha) + i$ and $v_L((y_1-1)\alpha) \geq v_L(\alpha) + i$, we find that $v_L((y_1y_2-1)\alpha) \geq v_L(\alpha) + i$. Let $\tilde{J}$ denote the preimage of J under $\mathfrak{O}_T[G] \to \mathbb{F}_q[G]$. To check that the sets are closed under $\mathbb{F}_q$, note that $y_1^{[\omega]} + p\mathfrak{O}_T[G] = x_1^{[\bar{\omega}]}$ and $v_L((y_1^{[\omega]}-1)\alpha) = v_L(\omega(y_1-1)\alpha) \geq v_L(\alpha) + i$. Observe that since L/K is a fully ramified p-extension, $v_L((y-1)\mu) \geq v_L(\mu)$ for all $y \in \tilde{J}$, $\mu \in L$. Finally we check that given $x^* \in G^{\mathcal{F}}$, $[x^*, x_1]_{\bar{\omega}} \in G_i^{\mathcal{F},\alpha}$. Let $y^* \in \mathfrak{O}_T[G]$ with $y^* + p\mathfrak{O}_T[G] = x^*$. Note y^*-1, $y_1-1 \in \tilde{J}$ and $[y^*, y_1]_\omega + p\mathfrak{O}_T[G] = [x^*, x_1]_{\bar{\omega}}$. Use Lemma 2.2. Since $Q(X,Y)$ is a polynomial divisible by Y, $Q(y^*-1, y_1-1) \in \tilde{J}(y_1-1)$. Therefore $v_L(([y^*, y_1]_{\bar{\omega}} - 1)\alpha) \geq v_L((y_1-1)\alpha) \geq v_L(\alpha) + i$. □

Refined ramification filtrations have breaks, where $G_i^{\mathcal{F},\alpha} \supsetneq G_{i+1}^{\mathcal{F},\alpha}$. We will refer to these integers as *refined breaks.* Moreover *refined ramification invariants* will refer to e_0, f and the quotients $G_i^{\mathcal{F},\alpha}/G_{i+1}^{\mathcal{F},\alpha}$. Our main result is the following

Theorem 3.3. *For $\alpha \in \mathcal{N}$, refined ramification filtrations possess $\dim_{\mathbb{F}_q} G^{\mathcal{F}}$ breaks.*

Proof. Each element $1 \neq x \in G^{\mathcal{F}}$, is associated with an integer $w_\alpha(x) < \infty$. As a result, there is an integer T such that $G_t^{\mathcal{F},\alpha} = \{1\}$ for $t \geq T$. Let Q_i be a set of distinct coset representatives of $G_i^{\mathcal{F},\alpha}/G_{i+1}^{\mathcal{F},\alpha}$, and set $q_i = |Q_i|$. The result will follow if we can prove that for all integers $i \geq 1$

$$q_i \in \{1, q\}.$$

Suppose that $q_i \neq 1$. First we prove $q_i \geq q$. Since $q_i > 1$, choose $x \in G_i^{\mathcal{F}}$ with $x \notin G_{i+1}^{\mathcal{F}}$. By Lemma 3.2, $x^{[\bar{\omega}]} \in G_i^{\mathcal{F},\alpha}$ for each $\bar{\omega} \in \mathbb{F}_q$. We need only prove that if $\bar{\omega}_1 \neq \bar{\omega}_2 \in \mathbb{F}_q$ then $x^{[\bar{\omega}_1]} \not\equiv x^{[\bar{\omega}_2]} \bmod G_{i+1}^{\mathcal{F},\alpha}$. But this is equivalent to $x^{[\bar{\omega}]} \notin G_{i+1}^{\mathcal{F},\alpha}$ for all $\bar{\omega} \neq 0$. And this is obvious, since if $x^{[\bar{\omega}]} \in G_{i+1}^{\mathcal{F},\alpha}$ for $\bar{\omega} \neq 0$, then $x = (x^{[\bar{\omega}]})^{[\bar{\omega}^{-1}]} \in G_{i+1}^{\mathcal{F},\alpha}$.

Now we prove $q_i \leq q$. Pick any two nontrivial coset representatives $x_1, x_2 \in Q_i$. We need to prove that $x_2 \equiv x_1^{[\bar{\omega}]} \bmod G_{i+1}^{\mathcal{F},\alpha}$ for some $\bar{\omega} \in \mathbb{F}_q$. Choose $y_j \in \mathfrak{O}_T[G]$ such that $v_L((y_j-1)\alpha) = v_L(\alpha)+i$ and $y_j + p\mathfrak{O}_T[G] = x_j$

for $j = 1, 2$. Since $v_L((y_1 - 1)\alpha) = v_L((y_2 - 1)\alpha)$, there is a $\omega \in \mathfrak{O}_T^\times$ such that $v_L((y_2 - 1)\alpha - \omega(y_1 - 1)\alpha) > v_L(\alpha) + i$. Therefore $v_L((y_2 - y_1^{[\omega]})\alpha) > v_L(\alpha) + i$ since $i \geq 1$. Since x_2 in a unit in $\mathbb{F}_q[G]$, y_2 is a unit in $\mathfrak{O}_T[G]$. Therefore $y_2^{-1} \in \mathfrak{O}_T[G]$ and $v_L((y_2^{-1}y_1^{[\omega]} - 1)\alpha) \geq v_L(\alpha) + i + 1$. Thus $w_\alpha(x_2^{-1}x_1^{[\bar{\omega}]}) \geq v_L(\alpha) + i + 1$ and so $x_2^{-1}x_1^{[\bar{\omega}]} \in G_{i+1}^{\mathcal{F},\alpha}$. □

This leads to the following generalization of [9, IV §1 Prop 7].

Corollary 3.4. *Given a refined ramification filtration (depending upon $\alpha \in \mathcal{N}$), one can choose a near-basis for $G^{\mathcal{F}}$ in one–to–one correspondence with the values of the refined breaks. Moreover each nontrivial quotient of refined ramification groups is canonically isomorphic to the corresponding quotient of unit groups. For refined break number b, the isomorphism $\phi : G_b^{\mathcal{F},\alpha}/G_{b+1}^{\mathcal{F},\alpha} \longrightarrow U_b/U_{b+1}$ is defined by $\phi(x) = y\alpha/\alpha$ where $y \in \mathfrak{O}_T[G]$ with $y + p\mathfrak{O}_T[G] = x$ such that for all $y' \in \mathfrak{O}_T[G]$ with $y' + p\mathfrak{O}_T[G] = x$, $v_L((y - 1)\alpha) \geq v_L((y' - 1)\alpha)$.*

3.2. On the values of refined breaks. Let $\mathcal{R}_\alpha$ denote the set of refined breaks from the refined ramification filtration that depends upon $\alpha \in \mathcal{N}$. Let $\mathcal{H}$ denote the set of Hilbert breaks. To be justified in the use of the term 'refined', we would like $\mathcal{H} \subseteq \mathcal{R}_\alpha$. But this requires a restriction on α. As a first step, we restrict to $\alpha \in \mathcal{N}_b$. Note that the group ring $K[G]$ acts faithfully on L. So $\alpha_1, \alpha_2 \in \mathcal{N}_b$ if and only if there is a unit $u \in K[G]^*$ such that $\alpha_2 = u\alpha_1$. Note also that the elements of $\mathcal{N}_b$ are quite natural for Galois structure.

Now consider the following

Example. Let L/K be a fully ramified C_p-extension with Hilbert break $h < pe_0/(p - 1)$, and Galois group $G = \langle\sigma\rangle$. Pick any element $\alpha \in L$ with $v_L(\alpha) = h$. Since $\gcd(p, h) = 1$ and $v_L((\sigma - 1)^i\alpha) = (i + 1)h$ for $0 \leq i \leq p - 1$, we find $\alpha \in \mathcal{N}_b$. Let $x_j = \Phi_p(\sigma) + p^j$ for $j \geq 2$. Since $\chi(x_j) \neq 0$ for each character χ, it follows that $x_j \in K[G]^*$. Thus $x_j\alpha \in \mathcal{N}_b$. In the situation that we are considering $G^{\mathcal{F}} = \{\sigma^{[\omega]} : \omega \in \mathbb{F}_q\}$. There is one Hilbert break and one refined break. Note that $v_L((\sigma - 1)x_j\alpha) = v_L(p^j) + 2h$ and $v_L(x_j\alpha) = ph$. Since $\gcd(h, p) = 1$, $w_{x_j\alpha}(\sigma) = v_L(p^j) + 2h$. So $\mathcal{R}_{x_j\alpha} = \{jpe_0 - (p - 2)h\}$, while $\mathcal{H} = \{h\}$. So $\mathcal{H} \not\subset \mathcal{R}_{x_j\alpha}$.

To find $\mathcal{H} \subset \mathcal{R}_\alpha$ we need to restrict α to a proper subset of $\mathcal{N}_b$. What should that be? Consider the fact that $p \mid v_L(x_j\alpha)$ in this example. Since elements in K have valuation divisible by p, perhaps this is the problem. Let

$$\mathcal{N}_c = \{\alpha \in \mathcal{N}_b : p \nmid v_L(\alpha)\}.$$

Proposition 3.5. *For noncyclic, elementary abelian extensions, if $\alpha \in \mathcal{N}_c$ then $\mathcal{H} \subset \mathcal{R}_\alpha$.*

Proof. Note $G \subseteq G^{\mathcal{F}}$. Let $\alpha \in \mathcal{N}_c$. Note that $v_L((\sigma-1)\alpha) - v_L(\alpha) < v_L(p)$ for $\sigma \in G$. Therefore $w_\alpha(\sigma) = v_L((\sigma-1)\alpha)$. □

This proposition however, does not say whether the refined breaks in $\mathcal{R}_\alpha \setminus \mathcal{H}$ are canonical. It does not answer the following question: For $\alpha_1, \alpha_2 \in \mathcal{N}_c$, is $\mathcal{R}_{\alpha_1} = \mathcal{R}_{\alpha_2}$? There is an equivalence relation on $\mathcal{N}_c$. Define $\alpha_1 \sim \alpha_2$ if there is a $u \in \pi_K^{\mathbb{Z}} \cdot \mathfrak{O}_K[G]^\times$ such that $\alpha_1 = u\alpha_2$.

Lemma 3.6. *If $\alpha_1 \sim \alpha_2$, then $\mathcal{R}_{\alpha_1} = \mathcal{R}_{\alpha_2}$.*

Proof. This is clear since $u \in \mathfrak{O}_K[G]^\times$ fixes valuations. □

Based upon Lemma 3.6, we might answer the question above by choosing an equivalence class of $\sim$. However as the following example illustrates, $\sim$ is not the weakest equivalence relation that yields the conclusion of Lemma 3.6.

Example. Suppose that $\mathfrak{O}_L$ were free over its associated order A on the normal basis α. Then $\mathcal{R}_\alpha = \mathcal{R}_{\alpha'}$ whenever $\alpha' = u\alpha$ with $u \in 1+\mathfrak{P}_K A \subset A^*$.

We close by repeating the question.

Question. We need a canonical subset $\mathcal{N}_? \subset \mathcal{N}_c$, such that $\alpha_1, \alpha_2 \in \mathcal{N}_?$ implies $\mathcal{R}_{\alpha_1} = \mathcal{R}_{\alpha_2}$. What should $\mathcal{N}_?$ be?

4. Biquadratic Extensions

Let $p = 2$ and consider L/K a fully ramified biquadratic extension. The structure of each ideal $\mathfrak{P}_L^i$ in L as a $\mathfrak{O}_T[G]$-module (and by restriction of coefficients also as a $\mathbb{Z}_2[G]$-module) was studied in [4, 2]. It was found that ramification invariants are sufficient to determine the Galois structure of each ideal when there are two Hilbert breaks [4]. But if there is only one Hilbert break, additional information is required [2]. The main result of this section is that *all* the information required to determine the Galois structure of ideals in biquadratic extensions is contained in the refined ramification filtration.

As noted in the proof of Proposition 2.6, $G^{\mathcal{F}} = 1 + J$ for $p = 2$ and $\mathbb{F}_2 \subsetneq \mathbb{F}_q$. So for $G = \langle \sigma, \gamma \rangle \cong C_2 \times C_2$, we have $G^{\mathcal{F}} = \langle \sigma, \gamma, 1+(\sigma-1)(\gamma-1) \rangle$. This is, of course, also a consequence of Theorem 2.9. For $\alpha \in \mathcal{N}$, there will be three refined breaks in the filtration of $G^{\mathcal{F}}$. To determine what those breaks might be, we need to begin with a listing of the possible Hilbert breaks. There are three cases to consider: (1) one Hilbert break h, (2) two congruent Hilbert breaks $h_1 < h_2$ with $h_1 \equiv h_2 \bmod 4$, and (3) two incongruent Hilbert breaks $h_1 < h_2$ with $h_1 \not\equiv h_2 \bmod 4$.

4.1. Case (1) : One Hilbert break extensions. Let L/K be a fully ramified biquadratic extension with one Hilbert break, h. As noted in [2], h is odd, $1 \leq h < 2e_0$, the residue class degree f of $K/\mathbb{Q}_2$ must exceed 1, and L must be expressible as $L = K(x, y)$ for

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

with $\beta, \tau \in K$, ω a nontrivial $2^f - 1$ root of unity, $v_K(\beta) = 2e_0 - h$, and $v_K(\tau) = 2e_0 - t$ for some $0 \leq t < h$ (if $t \neq 0$ then t must be odd). Let $G = \mathrm{Gal}(L/K) = \langle \sigma, \gamma \rangle$ where $\sigma(x) = x$ and $\gamma(y) = y$. As we will want to refer directly to results in [2], it is important to point out that our notation differs in two ways. Here we call the Hilbert break h (instead of b). The ω^{-1} of this paper is ω in [2, (2.1)]. (So in [2], $y^2 = (\omega^2 + \beta)(1 + \tau)$.) Otherwise the notation is the same.

4.2. Cases (2) & (3) : Two Hilbert break extensions. Let L/K be a fully ramified biquadratic extension with two Hilbert breaks, $h_1 < h_2$, and let $G = G_{h_1} = \langle \sigma, \gamma \rangle$ where $G_{h_2} = \langle \sigma \rangle$. Then $s = h_1$ and $t = (h_2 + h_1)/2$ are the two *upper ramification numbers* of L/K [9, IV §3]. Since upper ramification groups behave well upon passing to quotients, s will be the Hilbert break of L^σ/K where L^σ is the fixed field of $\langle \sigma \rangle$, and t will be the Hilbert break of L^γ/K. Let $L^\sigma = K(x)$ and $L^\gamma = K(y)$ where $x^2, y^2 \in K$. Since $1 \leq s < t \leq 2e_0$, s is odd. So we may assume that $x^2 = 1 + \beta$ for some $\beta \in K$ with $v_K(\beta) = 2e_0 - s$. Either $t < 2e_0$ and odd, or $t = 2e_0$. If t odd then $y^2 = 1 + \tau$ for some $\tau \in K$ with $v_K(\tau) = 2e_0 - t$. If $t = 2e_0$, then $y^2 = \pi_K$ for some prime element π_K. In any case, the Hilbert breaks of L/K where $L = K(x, y)$ are $h_1 = s$ and $h_2 = 2t - s$. Case (2), where $h_1 \equiv h_2 \bmod 4$, occurs when t is odd. Case (3), where $h_1 \not\equiv h_2 \bmod 4$, occurs when $t = 2e_0$.

4.3. Refined filtration for Cases (1) and (2). Let $h_{\max}$ denote the largest Hilbert break of L/K, and let

$$\mathcal{N}_{\max} = \{\alpha \in L : v_L(\alpha) \equiv h_{\max} \bmod 4\}.$$

We will find if there is one Hilbert break or two congruent Hilbert breaks that $\mathcal{N}_{\max} \subset \mathcal{N}_c$ and that the set of refined breaks $\mathcal{R}_\alpha$ is independent of choice of $\alpha \in \mathcal{N}_{\max}$. So in these two cases $\mathcal{N}_{\max}$ gives an answer to the question of §3.2.

Proposition 4.1. *For fully ramified biquadratic extensions with one Hilbert break or two congruent Hilbert breaks, $\mathcal{N}_{\max} \subset \mathcal{N}_c$.*

Proof. Since $h_{\max}$ is odd, we only need to check that $\mathcal{N}_{\max} \subset \mathcal{N}_b$. Let $h_1 \leq h_2$ denote the Hilbert breaks. So if there is one Hilbert break, $h_1 = h_2 = h$. Let $\alpha \in L$ be any element with $v_L(\alpha) = h_2 + 4m$, $m \in \mathbb{Z}$. Then

$v_L((\sigma+1)\alpha) = 2h_2+4m$, $v_L((\gamma-1)(\sigma+1)\alpha) = 2h_1+2h_2+4m$. Following [4, Lemma 3.15, 3.17], we find $\rho \in L$ such that $v_L(\rho) = 2h_1 + h_2 + 4m$ and $\rho = (\gamma-1)\alpha + (\sigma-1)\theta$ for some $\theta \in L$ with $v_L(\theta) = h_1 + 4m$. Since h_1, h_2 are odd, $h_2, 2h_2, 2h_1+2h_2, 2h_1+h_2$ yield the residues modulo 4. So $L = K\alpha + K(\sigma+1)\alpha + K(\gamma-1)(\sigma+1)\alpha + K\rho \subseteq K[G]\alpha + K\rho$. We want to prove that $\rho \in K[G]\alpha$. For the one Hilbert break case, this follows immediately from [2, Prop 2.1]. We will however treat both cases simultaneously.

Since $\theta \in L$ we find that $\theta = a\alpha + b(\sigma+1)\alpha + c(\gamma-1)(\sigma+1)\alpha + d\rho$ for some $a, b, c, d \in K$. Note that $v_L(\theta) \leq v_L(d\rho)$. So $v_L(d) \geq -h_1 - h_2$. It is important to observe here that since $h_1 + h_2 < 4e_0$ (in the two cases which we are considering) we have $d \neq 1/2$. Substitute in for θ. So $\rho = (\gamma-1)\alpha + (\sigma-1)[a\alpha + d\rho]$. Thus $[1-d(\sigma-1)]\rho = [(\gamma-1)+a(\sigma-1)]\alpha$. We need to prove that $1-d(\sigma-1) \in K[G]^\times$. But this follows since $((1+d)-d\sigma)((1+d)+d\sigma) = (1+d)^2 - d^2$, and $d \neq -1/2$. □

Proposition 4.2 (One Hilbert Break). *Assume the notation of §4.1. Since $f > 1$, there are three refined breaks. For $\alpha \in \mathcal{N}_{\max}$, the refined breaks are $r_1 = h$, $r_2 = \min\{4e_0 - h, 3h - 2t, 2h\}$ and $r_3 = 3h$. Moreover $G^{\mathcal{F}}_{r_2}/G^{\mathcal{F}}_{r_2+1} = \langle \gamma\sigma^{[\bar{\omega}]} \rangle$, where $\bar{\omega}$ is the image of ω in $\mathbb{F}_q$.*

Proof. Clearly, since $h < 2e_0 < 4e_0$ and $v_L(\alpha)$ is odd, $w_\alpha(\gamma) = v_L(\alpha) + h$. Since $f > 1$, $1+(\sigma-1)(\gamma-1) \in G^{\mathcal{F}}$. We claim that $w_\alpha(1+(\sigma-1)(\gamma-1)) = v_L(\alpha) + 3h$. It is easy to check that $v_L((\gamma+1)\alpha) = v_L(\alpha) + h$. Since $v_{K(y)}((\gamma+1)\alpha)$ is odd, $v_L((\sigma-1)(\gamma+1)\alpha) = v_L(\alpha)+3h$. To prove our claim we need to understand $v_L(((\sigma-1)(\gamma+1)+2f(\sigma,\gamma))\alpha)$ for $f(\sigma,\gamma) \in \mathfrak{O}_T[G]$. Since h is odd, $3h \neq 4e_0$. If $3h < 4e_0$, this valuation is $v_L(\alpha)+3h$ regardless of $f(\sigma,\gamma)$. So consider $4e_0 < 3h$. We may write $f(\sigma,\gamma) = u+j$ where either $u = 0$ or $u \in \mathfrak{O}_T^\times$, and j is in the ideal generated by $2, \sigma-1, \gamma-1$. If $u \in \mathfrak{O}_T^\times$ then $v_L(((\sigma-1)(\gamma+1)+2f(\sigma,\gamma))\alpha) = v_L(\alpha) + 4e_0$. On the other hand, if $u = 0$ then since $h < 2e_0$, $v_L(2j\alpha) \geq 4e_0 + h + v_L(\alpha) > 3h + v_L(\alpha)$. So $v_L(((\sigma-1)(\gamma+1)+2f(\sigma,\gamma))\alpha) = v_L(\alpha)+3h$. Thus $w_\alpha(1+(\sigma-1)(\gamma-1)) = v_L(\alpha) + 3h$.

To determine another refined break we quote directly from [2], keeping in mind the two notational differences mentioned in §4.1. First we restrict our attention to the particular $\alpha \in L$ defined in the proof of [2, Prop 2.1]. Note that it satisfies $v_L(\alpha) = h$. Use [2, Prop 2.1] to find that $v_L((\gamma+1+\omega(\sigma+1))\alpha) = v_L(\alpha) + \min\{4e_0-h, 3h-2t, 2h\}$. Since $\min\{4e_0-h, 3h-2t, 2h\} < 4e_0 = v_L(2)$, we find that $v_L((\gamma\sigma^{[\omega]}-1)\alpha) = v_L((\gamma-\sigma^{[-\omega]})\alpha) = v_L((\gamma-1+\omega(\sigma-1))\alpha) = v_L(\alpha)+\min\{4e_0-h, 3h-2t, 2h\}$. Now we extend this to all $\alpha' \in L$ with $v_L(\alpha') \equiv h \bmod 4$. Let L^σ denote the fixed field of σ. Then α' can be expressed as $\alpha' = m\alpha+n$ for some $m, n \in L^\sigma$ with $v_L(\alpha') = v_L(m\alpha) < v_L(n)$. Note that $(\gamma\sigma^{[\omega]}-1)\alpha' = m(\gamma\sigma^{[\omega]}-1)\alpha +$

$(\gamma-1)m\cdot\gamma\sigma^{[\omega]}\alpha+(\gamma-1)n$ where $v_L((\gamma-1)m\cdot\gamma\sigma^{[\omega]}\alpha)>v_L(\alpha)+2h$ and $v_L((\gamma-1)n)\geq v_L(n)+2h$. Therefore $v_L((\gamma\sigma^{[\omega]}-1)\alpha')=\min\{4e_0-h, 3h-2t, 2h\}+v_L(\alpha')$. Thus $w_{\alpha'}(\gamma\sigma^{[\bar{\omega}]})=v_L(\alpha')+\min\{4e_0-h, 3h-2t, 2h\}$. □

Proposition 4.3 (Two Congruent Hilbert Breaks). *Let L/K be a fully ramified biquadratic extension with two Hilbert breaks, $h_1<h_2$ and $h_1\equiv h_2 \bmod 4$. Regardless of $\alpha\in\mathcal{N}_{\max}$, the first two breaks are $r_1=h_1$, $r_2=h_2$, and if $f>1$ there is a third refined break $r_3=h_2+2h_1$.*

Proof. Adopt the notation of §4.2. So $\langle\sigma,\gamma\rangle=G=G_{h_1}$, and $\langle\sigma\rangle=G=G_{h_2}$. Since $h_2<4e_0$ and $v_L(\alpha)$ is odd, $w_\alpha(\gamma)=v_L(\alpha)+h_1$ and $w_\alpha(\sigma)=v_L(\alpha)+h_2$. If $f=1$ there are only these two refined breaks. If $f>1$, then $1+(\sigma-1)(\gamma-1)\in G^{\mathcal{F}}$. It is easy to check, since $(\sigma+1)\alpha\in L^\sigma$, that $v_L((\gamma-1)(\sigma+1)\alpha)=v_L(\alpha)+h_2+2h_1$. Now follow the argument in Prop 4.2 to determine that $w_\alpha(1+(\sigma-1)(\gamma-1))=v_L(\alpha)+h_2+2h_1$. □

4.4. On refined filtrations in Case (3). We turn to the case of two incongruent Hilbert Breaks. Using [4, Lem 3.22], one finds that there are elements $\alpha\in L$ with $v_L(\alpha)=h_{\max}$ and $(\sigma-1)(\gamma+1)\alpha=0$. So $\mathcal{N}_{\max}\not\subset\mathcal{N}_b$. And as the following example illustrates, neither will $\mathcal{N}_{\max}\cap\mathcal{N}_b$ serve as the 'canonical' set of §3.2.

Example. Recall the notation of §4.2: $L=K(x,y)$ where $x^2=1+\beta\in K$, $v_K(\beta)=2e_0-s$ is odd, $1<s<2e_0$, and $y^2=\pi_K$. Assume that $f>1$, so $1+(\sigma-1)(\gamma-1)\in G^{\mathcal{F}}$. The two Hilbert breaks of L/K are $h_1=s$, $h_2=4e_0-s$. As in [4, Lem 3.22], there are $\alpha,\rho\in L$ such that $(\sigma-1)\alpha=(\gamma-1)\rho=xy$. Note that $v_L(\alpha)\equiv -s \bmod 4$ and $v_L(\rho)\equiv s \bmod 4$. Clearly $(\gamma+1)\alpha\in K$ and $0\neq(\sigma+1)\rho\in K$. So $\mathcal{E}=(\gamma+1)\alpha/(\sigma+1)\rho\in K$. First we show that if $k\in K$ with $k\notin\{0,1,\mathcal{E}\}$, then $\alpha-k\rho\in\mathcal{N}_b$. Let $A=\alpha-k\rho$. We need to prove that if $(r+s\sigma+t\gamma+u\sigma\gamma)A=0$ for some $r,s,t,u\in K$, then $r+s\sigma+t\gamma+u\sigma\gamma=0$. Apply $(\gamma+1)(\sigma-1)$ to both sides. Thus $-k(r+t-s-u)(\gamma+1)(\sigma-1)\rho=0$. Since $(\gamma-1)(\sigma+1)\rho=0$ and $(\sigma\gamma-1)\rho\neq 0$, we find $r+t-s-u=0$. Now apply $(\gamma-1)(\sigma+1)$ instead. This results in $r+s-t-u=0$. Thus $r=u$ and $s=t$. We have reduced the equation to $(r+s\sigma)(1+\sigma\gamma)A=0$. Apply $(\sigma-1)$ to this new equation. The result is $(1-k)(r-s)(1+\sigma\gamma)(\sigma-1)\rho=0$. Since $k\neq 1$ and $(\sigma+1)(\gamma-1)\rho=0$, we find that $r=s$. The original equation, $(r+s\sigma+t\gamma+u\sigma\gamma)A=0$, is now $r(1+\sigma)(1+\gamma)A=0$. But this is the same as $r[2(\gamma+1)\alpha-2k(\sigma+1)\rho]=0$. Since $k\neq(\gamma+1)\alpha/(\sigma+1)\rho$, $r=0$. Now if we furthermore assume $v_L(\alpha)<v_L(k\rho)$, then

$$\alpha-k\rho\in\mathcal{N}_{\max}\cap\mathcal{N}_b.$$

If we further restrict k, namely assume $e_0 \nmid v_K(k)$, then we can easily prove that

$$w_{\alpha+k\rho}(1+(\sigma-1)(\gamma-1)) = 4v_K(k) + 8e_0 - s.$$

Note that $(\sigma+1)(\gamma+1)A - 2(\gamma+1)A = 2(\gamma+1)k\rho - 2(\sigma+1)k\rho$. So $v_L((\sigma+1)(\gamma+1)A - 2(\gamma+1)A) = v_L(2(\gamma+1)k\rho) \equiv 2s \bmod 4$. We need to examine $v_L((\sigma+1)(\gamma+1)A - 2(\gamma+1)A + 2f(\sigma,\gamma))$ for $f(\sigma,\gamma) \in \mathfrak{O}_T[G]$. Express $f(\sigma,\gamma) = r + s(\sigma+1) + t(\gamma+1) + u(\sigma+1)(\gamma+1)$ for $r, s, t, u \in \mathfrak{O}_T$. Since $v_L(rA) \equiv -s \bmod 4$ and $v_L(t(\gamma+1)A) \equiv v_L(u(\sigma+1)(\gamma+1)A) \equiv 0 \bmod 4$, the only way to increase valuation is if $v_L(2s(\sigma+1)A = v_L(2(\gamma+1)k\rho)$, or $v_K(k) = v_K(s)$. But since $s \in \mathfrak{O}_T$, $e_0 \mid v_K(s)$.

Remark (Two Incongruent Hilbert Breaks). As a result of the example (and until a 'canonical' $\mathcal{N}_?$ is determined), we can only determine the first two refined breaks of fully ramified biquadratic extensions with two Hilbert breaks, $h_1 < h_2$, and $h_1 \not\equiv h_2 \bmod 4$. If $\alpha \in \mathcal{N}_c$, the first two refined breaks are $r_1 = h_1$, $r_2 = h_2$. If $f > 1$ there is a third refined break. Its value depends upon choice of $\alpha \in L$.

4.5. Galois structure in biquadratic extensions. Fortunately, for biquadratic extensions the first two refined breaks are sufficient for additive Galois structure.

Theorem 4.4. *The Galois module structure of the ring of integers in a biquadratic extension is determined by refined ramification invariants.*

Proof. Compare the information in Propositions 4.2, 4.3 and the Remark with the requirements of [4, Thm 3.6, 3.9] and [2, Thm 3.2]. □

4.6. Twists. Recall the question and example of [2, §4].

Question. Let V be a continuous Galois representation of $\bar{G} = \mathrm{Gal}(\bar{K}/K)$, k be the kernel of V and let L be the fixed field of k. Associated with V there is an integral representation (indeed a whole sequence of them) given by the valuation ring $\mathfrak{O}_L$ (or by the sequence of ideals $\mathfrak{P}_L^i$ – the Galois structure of ideals). Suppose now that we twist V to obtain a new representation V' with kernel k' fixing L', and that $\bar{G}/k \cong \bar{G}/k'$. *How are these two associated integral representations of the (abstract) finite group $\bar{G}/k$ and $\bar{G}/k'$ related?*

The following example suggests that when the twist is "weak" the integral representations, the Galois structure of ideals, associated to V and V' will be isomorphic.

Example. Let $L_1 = K(x,y)$ be a biquadratic extension of K with $x^2 = 1+\beta$, $y^2 = \omega^{-2} + \beta$ where $v_K(\beta) = 2e_0 - h$, $1 \le h < 2e_0$ is odd, and ω is a nontrivial $2^f - 1$ root of unity. Therefore L_1/K has one Hilbert break, h. Let $K(z)$ be a quadratic extension with $z^2 = 1+\tau$, $v_K(\tau) = 2e_0 - t$ and

$0 \leq t < 2e_0$ (if $t \neq 0$ then t is odd). Let χ_y, χ_{xy}, χ_z be quadratic characters of $\mathrm{Gal}(\bar{K}/K)$ with fixed fields $K(y)$, $K(xy)$ and $K(z)$ respectively. Let V_1 be the 2-dimensional representation of $\bar{G} = \mathrm{Gal}(\bar{K}/K)$ with character $\chi_y + \chi_{xy}$, kernel k_1 and fixed field L_1. Note that the kernel k_z of $V_z = V_1 \otimes \chi_z$ has fixed field $L_z = K(x, yz)$.

To be sure that $\bar{G}/k_1 \cong \bar{G}/k_z$, assume that $K(y)/K$ and $K(z)/K$ have distinct Hilbert breaks, $h \neq t$. Using Proposition 4.2, and as in §4.1, making repeated reference to [2, Thm 3.2], observe the following: If the twist is 'weak', the ramification number associated to the twist is small (namely $t < h/2$ or $t < 2h - 2e_0$), then the Hilbert breaks, the refined breaks and the Galois structure of ideals are preserved by the twist (L_1 and L_z look the same). However, if we strengthen the twist (so $h/2 < t < h$ and $2h - 2e_0 < t < h$) then 'things begin to break down': The refined breaks and the Galois structure of ideals in L_z no longer agree with that in L_1, although the Hilbert breaks are preserved. And finally if we strengthen the twist even further (so $h < t$), 'everything breaks down': there will be two Hilbert breaks in L_z but only one in L_1. And so the refined breaks and Galois structure of ideals will also disagree.

Observation. *Apparently*, twists effect the Galois structure of ideals through their effect on ramification filtrations (Hilbert and refined).

5. Questions

As mentioned in §1.3, this paper can be viewed as an attempt to understand truncated exponentiation. This led to $G^{\mathcal{F}}$ and its filtrations. One would like to see $G^{\mathcal{F}}$ generalized. However there are difficulties with extending the definition of $G^{\mathcal{F}}$ to other abelian groups. There seem to be prohibitive difficulties involved in extending the definition to nonabelian p-groups. Could it be that $G^{\mathcal{F}}$ is defined *only* in the context of elementary abelian groups?

A number of other questions remain. Is the bound provided by Proposition 2.4 tight? What is $\dim_{\mathbb{F}_q} G^{\mathcal{F}}$ in general? However the most pressing question remains the one asked in §3.2: How should we choose $\alpha \in L$ so that the refined ramification filtration is canonical? Naturally, we propose to address the question by placing appropriate restrictions on α. But a canonical filtration should provide interesting arithmetic information, and so no answer will be complete until we understand the deeper question: How and to what extent do refined ramification filtrations determine additive Galois structure?

References

[1] M. V. BONDARKO, *Links between associated additive Galois modules and computation of H^1 for local formal group modules.* J. Number Theory **101** (2003), 74–104.

[2] N. P. BYOTT, G. G. ELDER, *Biquadratic extensions with one break.* Can. Math. Bull. **45** (2002), 168–179.
[3] G. G. ELDER, *Galois module structure of integers in wildly ramified cyclic extensions of degree p^2.* Ann. Inst. Fourier (Grenoble) **45** (1995), 625–647; errata ibid. **48** (1998), 609–610.
[4] G. G. ELDER, *Galois module structure of ambiguous ideals in biquadratic extensions.* Can. J. Math. **50** (1998), 1007–1047.
[5] G. G. ELDER, *On the Galois structure of the integers in cyclic extensions of local number fields.* J. Théor. Nombres Bordeaux. **14** (2002), 113–149.
[6] G. G. ELDER, *The Galois module structure of ambiguous ideals in cyclic extensions of degree* 8. To appear in the Proceedings of the International Algebraic Conference dedicated to the memory of Z. I. Borevich, Sept 17–23, 2002.
[7] R. L. GRAHAM, D. E. KNUTH, O. PATASHNIK, *Concrete Mathematics: A Foundation for Computer Science.* Addison Wesley, Reading MA 1989.
[8] J. V. KUZMIN, *Representations of finite groups by automorphisms of nilpotent near spaces and by automorphisms of nilpotent groups.* Sibirsk. Mat. Ž. **13** (1972), 107–117.
[9] J-P. SERRE, *Local Fields.* Springer-Verlag, New York, 1979.
[10] A. WEISS, *Rigidity of p-adic p-torsion.* Ann. of Math. (2) **127** (1988), 317–332.
[11] B. WYMAN, *Wildly ramified gamma extensions.* Amer. J. Math. **91** (1969), 135–152.

Nigel P. BYOTT
Department of Mathematical Sciences
University of Exeter
Exeter EX4 4QE
United Kingdom
E-mail : N.P.Byott@ex.ac.uk

G. Griffith ELDER
Department of Mathematics
University of Nebraska at Omaha
Omaha, NE 68182-0243 U.S.A.
E-mail : elder@unomaha.edu