A VALUATION CRITERION FOR NORMAL BASES IN ELEMENTARY ABELIAN EXTENSIONS

NIGEL P. BYOTT AND G. GRIFFITH ELDER

Abstract. Let \( p \) be a prime number and let \( K \) be a finite extension of the field \( \mathbb{Q}_p \) of \( p \)-adic numbers. Let \( N \) be a fully ramified, elementary abelian extension of \( K \). Under a mild hypothesis on the extension \( N/K \), we show that every element of \( N \) with valuation congruent mod \([N : K]\) to the largest lower ramification number of \( N/K \) generates a normal basis for \( N \) over \( K \).

1. Introduction

The Normal Basis Theorem states that in a finite Galois extension \( N/K \) there are elements \( \alpha \in N \) whose conjugates \( \{\sigma \alpha : \sigma \in \text{Gal}(N/K)\} \) provide a vector space basis for \( N \) over \( K \). If \( K \) is a finite extension of the field \( \mathbb{Q}_p \) of \( p \)-adic numbers, the valuation \( v_N(\alpha) \) of an element \( \alpha \) of \( N \) is an important property. We therefore ask whether anything can be said about the valuation of normal basis generators in this case. We will prove

**Theorem 1.** Let \( K \) be a finite extension of the \( p \)-adic numbers, let \( N/K \) be a fully ramified, elementary abelian \( p \)-extension, and let \( b_{\text{max}} \) denote the largest lower ramification number. If the upper ramification numbers of \( N/K \) are relatively prime to \( p \), then every element \( \alpha \in N \) with valuation \( v_N(\alpha) \equiv b_{\text{max}} \) mod \([N : K]\) generates a normal field basis. Moreover, no other equivalence class has this property: given any integer \( v \) with \( v \not\equiv b_{\text{max}} \) mod \([N : K]\), there is an element \( \rho_v \in N \) with \( v_N(\rho_v) = v \) which does not generate a normal basis.

This result arose out of work on the Galois module structure of ideals in extensions of \( p \)-adic fields. For such extensions, it has been found that the usual ramification invariants are, in general, insufficient to determine Galois module structure, and thus that there is a need for a refined ramification filtration \([\text{BE}02, \text{BE}05, \text{BE}]\). This refined filtration is defined for elementary abelian \( p \)-extensions and requires elements that generate normal field bases. Such elements are provided by Theorem 1. Recent work \([\text{EL}]\) suggests that what is known for \( p \)-adic fields should also hold in the analogous situation in characteristic \( p \), where \( K \) is a finite extension of \( \mathbb{F}_p(X) \). Here \( \mathbb{F}_p \) denotes the finite field with \( p \) elements, and \( X \) is an indeterminate. We therefore make the

**Conjecture.** Theorem 1 holds when \( K \) is a finite extension of \( \mathbb{F}_p(X) \) as well.

\footnotesize

*Date:* September 26, 2006.

1991 Mathematics Subject Classification. 11S15, 13B05.

Key words and phrases. Normal Basis Theorem; Ramification Theory.

Elder was partially supported by NSF grant DMS-0201080.
2. Preliminary Results

Let $K$ be a finite extension of the field $\mathbb{Q}_p$ of $p$-adic numbers, and let $N/K$ be a fully ramified, elementary abelian $p$-extension with $G = \text{Gal}(N/K) \cong C_p^n$. Use subscripts to denote field of reference. So $\pi_N$ denotes a prime element in $N$, $v_N$ denotes the valuation normalized so that $v_N(\pi_N) = 1$, and $e_K$ denotes the absolute ramification index. Let $\text{Tr}_{N/K}$ denote the trace from $N$ down to $K$. For each integer $i \geq -1$, let $G_i = \{\sigma \in G : v_N(\sigma - 1)\pi_N) \geq i + 1\}$ be the $i$th ramification group [Ser79, IV, §1]. Then $G_{-1} = G_0 = G_1 = G$, and the integers $b_i$ such that $G_b \supseteq G_{b+1}$ are the lower ramification break (or jump) numbers. The collection of such numbers, $b_1 < \cdots < b_m$, is the set of lower breaks. They satisfy $b_1 \equiv \cdots \equiv b_m \mod p$ [Ser79, IV, §2, Prop. 11], where if $b_m \equiv 0 \mod p$ then the extension $N/K$ is cyclic [Ser79, IV, §2, Ex. 3]. Let $g_i = |G_i|$. Then the upper ramification break numbers $u_1 < \cdots < u_m$ are given by $u_1 = b_1 g_{b_1}/p^n = b_1$ and $u_i = (b_1 g_{b_1} + (b_2 - b_1) g_{b_2} + \cdots + (b_i - b_{i-1}) g_{b_i})/p^n$ for $i \geq 2$ [Ser79, IV, §3].

Now by the Normal Basis Theorem, the set

$$\mathcal{NB} = \left\{ \rho \in N : \sum_{\sigma \in G} K \cdot \sigma \rho = N \right\}$$

does normal basis generators is nonempty. We desire integers $v \in \mathbb{Z}$ such that $\{\rho \in N : v_N(\rho) = v\} \subset \mathcal{NB}$. And so we are concerned by the following

**Example 1.** Suppose $K$ contains a $p$th root of unity $\zeta$, and let $N = K(x)$ with $x^p - \pi_K = 0$. Let $\sigma$ generate $\text{Gal}(N/K)$. Observe that $(\sigma - 1)x^i = 0$ and $\text{Tr}_{N/K} x^i = 0$ for $p \nmid i$. So for each $i \in \mathbb{Z}$, we have $v_N(x^i) = i$ and $x^i \notin \mathcal{NB}$. Here $N/K$ has one ramification break $b = pe_K/(p-1)$, which is divisible by $p$. [Ser79, IV, §2, Ex. 4].

**Remark.** Fortunately, these extensions provide the only obstacle. The restriction in Theorem 1 to elementary abelian extensions with upper ramification numbers relatively prime to $p$ is a restriction to those extensions that do not contain a cyclic subfield such as in Example 1 [Ser79, IV, §3 Prop. 14].

To prove Theorem 1 we need two results.

**Lemma 2.** Let $N/K$ be as above with $b_m \equiv 0 \mod p$, and let $t_G = \sum_{i=1}^{m} b_i \cdot |G_{b_i} \setminus G_{b_{i+1}}|$. If $\rho \in N$ with $v_N(\rho) \equiv b_m \mod p^n$, then $v_N(\text{Tr}_{N/K}\rho) = v_N(\rho) + t_G$. Conversely, given $\alpha \in K$ there is a $\rho \in N$ with $v_N(\rho) = v_N(\alpha) - t_G \equiv b_m \mod p^n$ such that $\text{Tr}_{N/K}(\rho) = \alpha$.

**Proof.** Use induction. Consider $n = 1$ when $\text{Gal}(N/K) = \langle \sigma \rangle$ is cyclic of degree $p$. There is only one break $b$, which satisfies $b < pe_K/(p-1)$. Let $\rho \in N$ with $v_N(\rho) \equiv b \mod p$. We have $\text{Tr}_{N/K}\rho \equiv (\sigma - 1)^{p-1}\rho \mod pp$. Since $(p-1)b < pe_K$, $v_N(\text{Tr}_{N/K}\rho) = v_N(\rho) + (p-1)b$. And given $\alpha \in K$, use [Ser79] V, §3, Lem. 4 to find $\rho \in N$ with $v_N(\rho) = v_N(\alpha) - (p-1)b$ and $\text{Tr}_{N/K}\rho = \alpha$.

Assume now that the result is true for $n$, and consider $N/K$ to be a fully ramified abelian extension of degree $p^{n+1}$. Recall $g_i = |G_i|$. Let $H$ be a subgroup of $G$ of index $p$ with $G_{b_2} \subseteq H$. Let $L = N^H$ and note that $N/L$ satisfies our induction hypothesis. Moreover the ramification filtration of $H$ is given by $H_i = G_i \cap H$ [Ser79, IV, §1]. So $|H_i| = g_i$ for $i > b_1$. Therefore $t_H = b_m(g_{b_m-1}) + b_{m-1}(g_{b_{m-1}-1}) + \cdots + b_1(p^n - g_2)$. Given $\rho \in N$ with $v_N(\rho) \equiv b_m \mod p^{n+1}$, by induction $v_N(\text{Tr}_{N/L}\rho) = v_N(\rho) + t_H$. By the Hasse-Arf Theorem, $p^{n+1} \mid g_b(b_i - b_{i-1})$ for $1 \leq
\[ i \leq m. \text{ Thus } t_H \equiv -b_m + p^n b_1 \mod p^{n+1} \text{ and } v_L(\text{Tr}_{N/L}\rho) \equiv b_1 \mod p. \]

Using [Ser79 IV, §1, Prop. 3 Cor.], \( b_1 \) is the Hilbert break for the \( C_p \)-extension \( L/K \). Applying the case \( n = 1 \), we find \( v_L(\text{Tr}_{N/K}\rho) = v_N(\rho) + t_H + p^n(p - 1)b_1 = v_N(\rho) + t_G \). The converse statement follows similarly, using \( t_H + p^n(p - 1)b_1 = t_G \).

\[ \square \]

The following generalizes a technical relationship used in the proof of Lemma 2.

**Lemma 3.** Let \( N/K \) be a fully ramified, noncyclic, elementary abelian extension with group \( G \cong C_p^n \). Let \( H \) be a subgroup of \( G \) of index \( p \), and let \( L = N^H \). If \( b_m \) is the largest lower break of \( N/K \), \( b \) the only break of \( N/L \), and \( \rho \) any element of \( N \) with \( v_N(\rho) \equiv b_m \mod p^n \), then \( v_L(\text{Tr}_{N/L}\rho) \equiv b \mod p \).

**Proof.** In the proof of Lemma 2, \( H \supseteq G_{b_2} \) so that \( G_{b_1}H/H \subseteq G_{b_1+1}H/H \) following [Ser79 IV, §1, Prop. 3, Cor.], and the break for \( G/H \) was \( b_1 \). Here we have no such luxury and we have to involve the upper numbers in our considerations, although the argument is really no different. Note that there is a \( k \) such that \( G^{u_k+1}H/H \not\subseteq G^{u_k}H/H \). Thus \( u_k \) is the upper ramification number of \( G/H \). Since there is only one break in the filtration of \( G/H \), the lower and upper numbers for \( G/H \) are the same, \( b = u_k \).

The ramification filtration for \( H \) is given by taking intersections: \( H_j = G_j \cap H \). Note that \( |G_{b_i} : G_{b_i} \cap H| = p \) for \( i \leq k \) and \( G_{b_i} \subseteq H \) for \( i > k \). Let \( h_j = |H_j| \). Then \( h_j = g_j/p \) for \( j \leq b_k \), and \( h_j = g_j \) for \( j > b_k \). Now let \( v_N(\rho) = b_m + p^n t \).

Following the proof of Lemma 2 and using the Hasse-Arf Theorem,

\[
v_N(\text{Tr}_{N/L}\rho) = b_m + p^n t + b_m(h_{b_m} - 1) + b_{m-1}(h_{b_{m-1}} - h_{b_m}) + \cdots + b_1(h_1 - h_{b_2}) = p^n t + (b_m - b_{m-1})h_{b_m} + (b_{m-1} - b_{m-2})h_{b_{m-1}} + \cdots + (b_2 - b_1)h_{b_2} + b_1h_1 \equiv (b_k - b_{k-1})h_{b_k} + \cdots + (b_2 - b_1)h_{b_2} + b_1h_1 \equiv p^n u_k/p \equiv p^{n-1} b \mod p^n
\]

Therefore \( v_L(\text{Tr}_{N/L}\rho) \equiv b \mod p \).

\[ \square \]

3. Main Result

**Proof of Theorem 1.** There are two statements to prove. We begin with the first:

We assume the upper breaks satisfy \( p \nmid u_i \), and prove that for \( \rho \in N \)

\[ v_N(\rho) \equiv b_m \mod p^n \implies \rho \in N^B. \]

The argument breaks up into two cases: the Kummer case where \( \zeta \in K \) and the non-Kummer case where \( \zeta \notin K \). Here \( \zeta \) is a nontrivial \( p \)th root of unity.

We begin with the Kummer case, and start with \( n = 1 \). Let \( \sigma \) generate the Galois group, and denote the one ramification number by \( b \). Since in this case \( b \) is also the upper number, \( p \nmid b \). Therefore \( \{v_N((\sigma - 1)^j \rho) : 0 \leq i < p \} \) is a complete set of residues modulo \( p \). And since \( N/K \) is fully ramified, \( \rho \) generates a normal basis.

Now let \( n \geq 2 \) and note that \( N = K(x_1, x_2, \ldots, x_n) \) with each \( x_i^p \in K \). It suffices to show that \( K[G] \rho \) contains each element \( y = x_1^{j_1} x_2^{j_2} \cdots x_n^{j_n} \) with \( 0 \leq j_i \leq p - 1 \).

For \( y = 1 \) this is clear, since \( \text{Tr}_{N/K}(\rho) \in K \).

For any other \( y \), we can change the ramification number of \( L/K \). By Lemma 3, \( v_L(\text{Tr}_{N/L}(\rho)) \equiv b \mod p \).

Since \( b \) is an upper number of the ramification filtration of \( G, p \nmid b \).

Now apply the \( n = 1 \) argument, using \( \text{Tr}_{N/L}(\rho) \) in \( L/K \). Thus \( y \in K[G] \rho \).

We now turn to the non-Kummer case with \( \zeta \notin K \). Let \( E = K(\zeta) \), let \( E/K \) have ramification index \( e_{E/K} \), and let \( F = N(\zeta) \). Then \( F/E \) is a fully ramified Kummer extension of degree \( p^m \).

Applying Herbrand’s Theorem [Ser79 IV, §3, Lem. 5] to
the quotient $G = \text{Gal}(N/K)$ of $\text{Gal}(F/K)$, we find that the maximal ramification
break of $F/E$ is $e_{E/K}b_m \not\equiv 0 \mod p$. The above discussion for the Kummer case
therefore applies to $F/E$. Suppose now for a contradiction that $p \in N$ with $v_N(\rho) = b_m \mod p^n$, and
that $K[G]\rho$ is a proper subspace of $N$. Then by extending scalars
(noticing that $E$ and $N$ are linearly disjoint as their degrees are coprime) we have
that $E[G]\rho$ is a proper subspace of $F$. Moreover $v_F(\rho) \equiv e_{E/K}b_m \mod p^n$. This
contradicts the result already shown for the Kummer extension $F/K$, completing
the proof of the first statement of the theorem.

Consider the second statement: Given any integer $v$ with $v \not\equiv b_m \mod p^n$ there
is a $\rho_v \in N$ with $v_N(\rho_v) = v$ such that $\text{Tr}_{N/K}\rho_v = 0$ and thus $\rho_v \notin N\mathcal{B}$. To
prove this statement note that given $v \in \mathbb{Z}$, there is an $0 \leq a_v < p^n$ such that
$v \equiv a_v b_m \mod p^n$, since $p \nmid b_m$. If $a_v \neq 1$ we will construct an element $\rho_v \in N$ with
$v_N(\rho_v) = v$ and $\text{Tr}_{N/K}\rho_v = 0$. To begin, observe that there is a integer $k$ such that
$0 \leq k \leq n - 1$, $a_v \equiv 1 \mod p^k$ and $a_v \not\equiv 1 \mod p^{k+1}$. Recall $g_i = |G_i|$. Since the
ramification groups are $p$-groups with $g_{i+1} \leq g_i$, there is a Hilbert break $b_i$ such
that $g_{b_i+1} < p^{k+1} \leq g_{b_i}$. For $i = k, k+1$ choose $H_i$ with $|H_i| = p^i$ and $G_{b_i+1} \subset
H_k \subset H_{k+1} \subset G_{b_i}$. Recall from Lemma 2 the expression for $t_{G_i}$, and note that
t_{H_k} = b_m(g_{b_m-1}+b_{m-1}(g_{b_m-1}-g_{m})+\cdots+b_s(p^k-g_{b_{s+1}})) \equiv -b_m+b_m p^k \mod p^n$. Let
$L = N^{H_k}$. Since $a_v \not\equiv 1 \mod p^{k+1}$, $a_v \equiv 1 + rp^k \mod p^{k+1}$ for some $1 \leq r \leq p - 1$.
Using the fact that $b_s \equiv b_m \mod p, a_v b_m + t_{H_k} \equiv (r+1)b_m p^k \mod p^{k+1}$. Since
$p^k | v_N(\alpha)$ for $\alpha \in L$, we can choose $\alpha \in L$ with $v_N(\alpha) = v + t_{H_k} \equiv rp^k b_s$. So
$v_L(\alpha) \equiv b_s \mod p$. Let $\sigma \in G$ so that $\sigma H_k$ generates $H_{k+1}/H_k$. Therefore
$v_N((\sigma - 1)^*\alpha) = v + t_{H_k}$. Now using Lemma 2, we choose $\rho_v \in N$ such that
$v_N(\rho_v) = v$ and $\text{Tr}_{N/L}\rho_v = (\sigma - 1)^*\alpha$. Since $(1 + \sigma + \cdots + \sigma^{p-1})\text{Tr}_{N/L}\rho_v = 0$, we have $\text{Tr}_{N/K}\rho_v = 0$.

**Corollary 4.** Let $N/K$ be a fully ramified, elementary abelian extension of degree $p^n$ with $n > 1$ and one ramification break, at $b$. If $\rho \in N$ with $v_N(\rho) \equiv b \mod p^n$, then $\rho \in N\mathcal{B}$.

**References**

[BE] N. P. Byott and G. G. Elder, *On the necessity of new ramification breaks*, In preparation.

[BE02] N. P. Byott and G. G. Elder, *Biquadratic extensions with one break*, Can. Math. Bull. 45
(2002), no. 2, 168–179.

[BE05] N. P. Byott and G. G. Elder, *New ramification breaks and additive Galois structure*, J.
Théor. Nombres Bordeaux 17 (2005), no. 1, 87–107.

[Eld] G. G. Elder, *One-dimensional elementary-abelian extensions of local fields*, arXiv.org:math/0511174 (2005-11-15).

[Ser79] J.-P. Serre, *Local fields*, Springer-Verlag, New York, 1979.

Nigel P. Byott, School of Engineering, Computer Science and Mathematics, University of Exeter, Exeter EX4 4QE, United Kingdom
E-mail address: 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 address: elder@vt.edu
Current address: Department of Mathematics, Virginia Tech, Blacksburg VA 24061-0123