A VALUATION CRITERION FOR NORMAL BASIS GENERATORS IN LOCAL FIELDS OF CHARACTERISTIC $p$

G. GRIFFITH ELDER

Abstract. Let $K$ be a complete local field of characteristic $p$ with perfect residue field. Let $L/K$ be a finite, fully ramified, Galois $p$-extension. If $\pi_L \in L$ is a prime element, and $p'(x)$ is the derivative of $\pi_L$’s minimal polynomial over $K$, then the relative different $D_{L/K}$ is generated by $p'(\pi_L) \in L$. Let $v_L$ be the normalized valuation normalized with $v_L(L) = \mathbb{Z}$. We show that any element $\rho \in L$ with $v_L(\rho) \equiv -v_L(p'(\pi_L)) - 1 \mod [L : K]$ generates a normal basis, $K[\text{Gal}(L/K)] \cdot \rho = L$. This criterion is tight: Given any integer $i$ such that $i \not\equiv -v_L(p'(\pi_L)) - 1 \mod [L : K]$, there is a $\rho_i \in L$ with $v_L(\rho_i) = i$ such that $K[\text{Gal}(L/K)] \cdot \rho_i \not\subseteq L$.

The Normal Basis Theorem states that in a finite Galois extension $L/K$ with $G = \text{Gal}(L/K)$, there is an element $\rho \in L$, called a normal basis generator, whose conjugates $\{\sigma \rho : \sigma \in G\}$ provide a basis for $L$ over $K$. In the setting of local field extensions, the most important property of an element is its valuation, and so $[2]$ asked whether there is a valuation criterion: Is there a valuation (an integer certificate) that guarantees that any element bearing this valuation is a normal basis generator?

Let $K$ be a complete local field with a perfect residue field of characteristic $p$. So the characteristic of $K$ is 0 or $p$. It is not too hard to see that as a necessary condition, if a valuation criterion exists for a finite Galois extension $L/K$, then $L/K$ must be fully ramified and have order a power of $p$. But are these necessary conditions also sufficient? In this paper we give an affirmative answer to this question in the case where $K$ has characteristic $p$.

For $K$ of characteristic 0 and regular (so $K$ does not contain the $p$th roots of unity), a valuation criterion for fully ramified elementary abelian $p$-extensions is given in [2]. For $K$ of characteristic $p$, a valuation criterion for fully ramified abelian $p$-extensions is given in [3]. In both cases, the valuation criterion is described in terms of the largest ramification break number associated with $L/K$. The main contribution of this paper is a restatement of that criterion in terms of the exponent of the relative different (see remark following proposition). The relative different satisfies $D_{L/K} = (p'(\pi_L))$ with $\pi_L$ a prime element of $L$ and $p(x)$ the minimal polynomial of $\pi_L$ over $K$ [4]. In both cases, the valuation criterion is described in terms of the exponent of the relative different (see remark following proposition). The relative different satisfies $D_{L/K} = (p'(\pi_L))$ with $\pi_L$ a prime element of $L$ and $p(x)$ the minimal polynomial of $\pi_L$ over $K$ [4].

This means that we can state our main result as follows:

Theorem 0.1. Let $K$ be a complete local field of characteristic $p$ with perfect residue field. Let $L/K$ be a finite, Galois extension with $G = \text{Gal}(L/K)$, and let $v_L$ be the valuation normalized so that $v_L(L) = \mathbb{Z}$. If $L/K$ is fully ramified and $[L : K] = p^n$ for some integer $n$, there is a valuation criterion: Let $\pi_L \in L$ be a

Date: February 12, 2008.
1991 Mathematics Subject Classification. 11S15.
prime element and let \( p(x) \) be its minimal polynomial over \( K \). Then any element \( \rho \in L \) with \( v_L(\rho) \equiv -v_L(p'(\pi_L)) \equiv 1 \mod [L : K] \) generates a normal basis for \( L/K \). So \( L = K[G] \cdot \rho \).

Moreover the assumption that \( L/K \) is a fully ramified \( p \)-extension is necessary and the criterion under that assumption is tight: Outside of the assumption, given any \( i \in \mathbb{Z} \), or under the assumption, given any \( i \not\equiv -v_L(p'(\pi_L)) \equiv 1 \mod [L : K] \), there is a \( \rho_i \in L \) with \( v_L(\rho_i) = i \) such that \( L \supseteq K[G] \cdot \rho_i \).

**Proof.** Recall the definition of the ramification groups \( G_i \) [4, IV]. We begin by assuming that \( G = G_1 \), which is equivalent to the assumption that \( L/K \) is a fully ramified extension of degree \( p^n \) for some \( n \). Let \( d = v_L(p'(\pi_L)) \) and let \( \rho \in L \) with \( v_L(\rho) \equiv -d - 1 \mod p^n \). Express \( \rho \) in terms of the field basis \( B = \{ \pi_L/p'(\pi_L) : i = 0, \ldots, p^n - 2 \} \) for \( L/K \). It is a result of Euler that

\[
\text{Tr}_G \frac{\pi_i^j}{p'(\pi_L)} = \begin{cases} 
0 & \text{for } 0 \leq i \leq p^n - 2 \\
1 & \text{for } i = p^n - 1
\end{cases}
\]

[4] III §6 Lemma 2. Since \( v_L(\rho) \equiv v_L(\pi_L^{p^n-1}/p'(\pi_L)) \mod p^n \), the coefficient of \( \pi_L^{p^n-1}/p'(\pi_L) \) in the expression for \( \rho \) must be nonzero. Therefore \( \text{Tr}_G \rho \not= 0 \). Moreover, we can replace \( B \) by the alternate basis \( \{ \rho, \pi_L/p'(\pi_L) : i = 0, \ldots, p^n - 2 \} \), and get

\[
L = K \cdot \rho + \sum_{i=0}^{p^n - 2} K \cdot \frac{\pi_i^j}{p'(\pi_L)}.
\]

The Normal Basis Theorem, stated in terms of Tate cohomology, says that \( \tilde{\text{H}}^{-1}(G, L) = 0 \) [4, VIII §1 & X §1 Proposition 1]. This means that any element \( \eta \in L \) with \( \text{Tr}_G \eta = 0 \) satisfies \( \eta \in \mathcal{I}_G \cdot L \), where \( \mathcal{I}_G = (\sigma - 1 : \sigma \in G) \) is the augmentation ideal of the group ring \( K[G] \). Therefore \( L = K \cdot \rho + \mathcal{I}_G \cdot L \), but also

\[
L = K[G] \cdot \rho + \mathcal{I}_G \cdot L.
\]

Now notice that because \( G \) is a \( p \)-group and \( K \) has characteristic \( p \), \( \mathcal{I}_G \) is also the Jacobson radical of \( K[G] \). Thus, by Nakayama’s Lemma, \( L = K[G] \cdot \rho \).

We have proven the criterion. The elements \( \pi_L^{p^n-1}/p'(\pi_L) \) for \( i \not= p^n - 1 \) show that the criterion is sharp. (All of this argument applies equally well in characteristic 0, except for one step: In characteristic 0, the augmentation ideal \( \mathcal{I}_G \) is not the Jacobson radical of \( K[G] \).)

Now we address \( G \supseteq G_1 \). Let \( L' = L^{G_1} \) and \( L'' = L^{G_0} \). So \( L''/K \) is unramified and \( L'/L'' \) is fully but tamely ramified. Replace \( K \) and \( G \), in our earlier argument with \( L' \) and \( G_1 \) respectively. So \( d \) is defined in terms of the relative different of the fully ramified \( p \)-part of the extension, \( \mathfrak{p}_L' = \mathfrak{D}_{L'/L} \) and \( p^n = [L : L'] \). From earlier work, given any integer \( i \not= -d - 1 \mod p^n \) there is a \( \rho \in L \) with \( v_L(\rho) = i \) such that \( \text{Tr}_{G_1} \rho = 0 \). So \( K[G] \rho \not\subseteq L \).

To consider the case \( i \equiv -d - 1 \mod p^n \), notice that the trace \( \text{Tr}_{G_1} \) maps fractional ideals of \( \mathfrak{D}_L \), the ring of integers of \( L \), to fractional ideals of \( \mathfrak{D}_{L''} \). Indeed, using basis \( B \) from above, \( \text{Tr}_{G_1} \mathfrak{P}_L = \mathfrak{P}_L^{p^n-d} \cdot \mathfrak{P}_L^{k-1} \). Moreover \( \text{Tr}_{G_1} \mathfrak{P}_L^{k-1} \subseteq \mathfrak{P}_L^{k-1} \), because of [4] III §3 Proposition 7]. Observe that this means that given any element \( \tau \in L' \) with \( v_L(\tau) = k - 1 \), there is a \( \rho_\tau \in L \) with \( v_L(\rho_\tau) = kp^n - d - 1 \) such that \( \text{Tr}_{G_1} \rho_\tau = \tau \).

To use this observation notice that because \( L'/L'' \) is tamely ramified, there is a prime element of \( L'' \), namely \( \pi_{L''} \), such that \( L' = L''(\sqrt[p^n]{\pi_{L''}}) \) with \( p \not\in [4, II \S 3.5.
Proposition]. So for \( k \neq 1 \mod e \), let \( \tau = \sqrt[p]{r_{L/F}}^{k-1} \). Since \( \text{Tr}_{G_0/G_1} \sqrt[p]{r_{L/F}}^{k-1} = 0 \), \( \text{Tr}_{G_0}\rho = 0 \) and \( K[G]\rho \subset L \). For \( k \equiv 1 \mod e \), let \( \tau = \sigma_{K}^{(k-1)/e} \) and let \( \sigma \) be any non-trivial element in \( G/G_1 \). Then \( (\sigma - 1)\sigma_{K}^{k-1} = 0 \). Thus \( (\sigma - 1)\text{Tr}_{G_1}\rho = 0 \) and \( K[G]\rho \subset L \).

Now we connect the valuation criterion of this paper with that of \[2\], \[5\].

**Proposition 0.2.** Let \( K \) be a complete local field (characteristic 0 or \( p \)) with perfect residue field of characteristic \( p \). Let \( L/K \) be a finite, fully ramified, Galois \( p \)-extension. Let \( \pi_L \in L \) be a prime element and let \( p(x) \) be its minimal polynomial over \( K \). Then

\[
\nu_L(p'(\pi_L)) + 1 \equiv p^n u_m - b_m \mod [L : K]
\]

where \( b_m, u_m \) are the largest ramification break numbers in lower and upper numbering respectively.

**Remark 1.** When \( L/K \) is abelian \( u_m \in \mathbb{Z} \) by the Hasse-Arf Theorem and so we get the valuation criterion of \[2\], \[5\], namely \( \nu_L(\rho) \equiv b_m \mod p^n \).

**Proof.** Let \( d = \nu_L(p'(\pi_L)) \) and recall that \( \mathcal{O}_{L/K} = (p'(\pi_L)) \). Let \( G = G_1 \) and \( [L : K] = p^n \). Recall the ramification filtration \( G = G_1 \supset G_2 \supset \cdots \) where \( G_i = \{ \sigma \in G : \nu_L((\sigma - 1)\pi_L) \geq i + 1 \} \) \[3\] IV §1. The break numbers (in lower numbering) are those integers \( i \) such that \( G_i \supset G_{i+1} \). Let \( b_1 < b_2 < \cdots < b_m \) be the list of break numbers with \( b_m \) being the maximal break (again in lower numbering). Let \( g_i = |G_{b_i}| \), the number of elements in \( G_{b_i} \). Then by \[3\] IV §1 Proposition 4,

\[
d = (1 + b_1)(g_1 - 1) + \sum_{i=2}^{m} (b_i - b_{i-1})(g_i - 1) = (1 + b_1)g_1 - b_m - 1 + \sum_{i=2}^{m} (b_i - b_{i-1})g_i.
\]

Moreover, we can convert the lower numbering to upper numbering using the Herbrand function \( \varphi \) \[4\] IV §3. Be careful to notice a small difference in notation: We use \( g_i = |G_{b_i}| \) whereas \[4\] IV §3 uses \( g_{b_i} = |G_{b_i}| \). The largest break number in upper numbering is therefore

\[
u_m = \varphi(b_m) = \frac{1}{p^n} \left( b_1 g_1 + \sum_{i=2}^{m} (b_i - b_{i-1})g_i \right).
\]

Thus \( d + 1 = g_1 - b_m + p^n u_m \), where \( g_1 = p^n \).

We end the paper with a natural

**Question 1.** Does the statement of the Theorem (modified appropriately to address \[2\] Example 1) also hold in characteristic zero?

**References**

[1] B. de Smit and L. Thomas, ‘Local Galois module structure in positive characteristic and continued fractions’, *Arch. Math. (Basel)* 88 (2007), no. 3, 207–219.

[2] N. P. Byott and G. G. Elder, ‘A valuation criterion for normal bases in elementary abelian extensions’, *Bull. Lond. Math. Soc.* 39 (2007), no. 5, 705–708.

[3] I. B. Fesenko and S. V. Vostokov, ‘Local fields and their extensions’, (American Mathematical Society, Providence RI, 2002).

[4] J.-P. Serre, ‘Local fields’, (Springer-Verlag, New York, 1979).

[5] L. Thomas, ‘A valuation criterion for normal basis generators in equal positive characteristic’, preprint: August 9, 2007.
E-mail address: elder@unomaha.edu

Department of Mathematics, University of Nebraska at Omaha, Omaha, NE 68182-0243 U.S.A.