The valuation criterion for normal basis generators in unequal characteristic

B. de Smit, M. Florence, L. Thomas

March 18, 2010

1 Introduction

Let K be a field. Let L be a finite Galois extension of K, with Galois group G. An element $x \in L$ is called a *normal basis generator* of L over K, or simply a *normal* element of L over K, if the conjugates of x under G form a basis of L as a vector space over K. The normal basis theorem states that such an element exists.

Assume that K (resp. L) is a local field, i.e., that it is complete with respect to a discrete valuation $v_K \colon K^* \twoheadrightarrow \mathbb{Z}$ (resp. $v_L \colon L^* \twoheadrightarrow \mathbb{Z}$). We consider the following question, suggested by Byott and Elder [2].

Question. *Is there an element $d \in \mathbb{Z}$ so that every $x \in L$ with $v_L(x) = d$ is normal over K?*

Note that, if such an integer d exists, then all integers that are congruent to d modulo the ramification index $e_{L/K}$ satisfy the same property.

For example, when $K = \mathbb{Q}_2$ and $L = \mathbb{Q}_2(\sqrt{-1})$, then all elements of odd valuation in L are normal. However, for $L = \mathbb{Q}_2(\sqrt{2})$, the powers of $\sqrt{2}$ give elements of L of all possible valuations which are not normal, so the answer to the question is no.

If $x \in L$ is normal over K, then the Galois conjugates are linearly independent, so their sum, the trace $\mathrm{Tr}_{L/K}(x)$, is non-zero. It turns out that it is quite easy to give a valuation criterion, formulated in the next Proposition, for this weaker property of having a non-zero trace.
We denote the valuation of the different of L/K by $d_{L/K}$.

Proposition 1.1. *Let L/K be a finite separable extension of local fields, and let $d \in \mathbb{Z}$. Every element of L of valuation d has non-zero trace over K if and only if the following two properties hold.*

(1) *L/K is totally ramified.*

(2) $d \equiv -d_{L/K} - 1 \bmod [L : K]$.

The proof is given in Section 2.

In particular, Proposition 1.1 implies that the answer to the question is positive if and only if the following statement holds:

$$\mathrm{VC}(L/K): \quad \text{all } x \in L^* \text{ with } v_L(x) \equiv -d_{L/K} - 1 \bmod e_{L/K} \text{ are normal over } K.$$

We will call this statement the *valuation criterion* for normal basis generators of L over K.

Proposition 1.2. *Let L/K be a finite Galois extension of local fields. The valuation criterion* $\mathrm{VC}(L/K)$ *holds if and only if the following two conditions hold.*

(1) *L/K is totally ramified and $[L : K]$ is a power of the residue characteristic p.*

(2) *Every non-zero $K[G]$-submodule of L contains an element of valuation* 0.

The proof will be given in Section 3. It is based on a duality result for the set of valuations of elements of a sub-K-vector space of L.

Note that, if the residue field of K has characteristic zero, then proposition 1.2 can be restated as: $\mathrm{VC}(L/K)$ holds if and only if $L = K$.

Note also that, in condition (2), we may restrict to the minimal non-zero $K[G]$-submodules of L. The condition in (1) that $[L : K]$ is a power of p can be omitted — we will see in the proof that it is implied by condition (2). The condition that L/K should be totally ramified can not be omitted.

If K has characteristic $p > 0$ and condition (1) in Proposition 1.2 holds, then condition (2) also holds because every nonzero G-stable K-vector subspace of L then contains K; see [7, Ch. IX, Th. 2]. In the equal characteristic case Proposition 1.2 therefore tells us that condition (1) implies $\mathrm{VC}(L/K)$, which was shown already by Thomas [6] and by Elder [3].

In the unequal characteristic case, condition (1) of Proposition 1.2 is not sufficient for $\mathrm{VC}(L/K)$. For example, consider the extension $\mathbb{Q}_2(\sqrt{2}))/\mathbb{Q}_2$. More generally, elements in extensions of K that are strictly contained in L are never normal elements of L, so one sees that the condition $p \nmid -d_{L/K} - 1$ is necessary for $\mathrm{VC}(L/K)$ to hold. For cyclic extensions of degree p this condition is also sufficient; cf. [2]. However, we will see in Example 4.1 that this condition is not sufficient for cyclic extensions of degree p^2.

By condition (2) in Proposition 1.2, we can easily identify the Kummer extensions for which the valuation criterion holds. Recall that L/K is a *Kummer extension* if there is a number m so that K contains a primitive root of unity of order m, and $\mathrm{Gal}(L/K)$ is abelian of exponent m. Then the characteristic of K does not divide m, and by Kummer theory we have $L = K(\sqrt[m]{W})$ for $W = L^{*m} \cap K^*$. If, in addition, we have $v_K(W) \subset m\mathbb{Z}$, then L is obtained by adjoining m-th roots of units of the valuation ring of K, and we say that L is a *unit root Kummer extension* of K. For example, $\mathbb{Q}_2(\sqrt{-1})$ is a unit root Kummer extension of $\mathbb{Q}_2$, whereas $\mathbb{Q}_2(\sqrt{2})$ is not.

Theorem 1.3. *Let L/K be a totally ramified Kummer extension of local fields whose degree is a power of the residue characteristic p. Then* $\mathrm{VC}(L/K)$ *holds if and only if L is a unit root Kummer extension of K.*

In Section 4 we give the proof, and we show how the general abelian case can be reduced to the Kummer case. Precisely, we will show the following theorem.

Theorem 1.4. *Let L/K be a totally ramified abelian extension of local fields whose degree is a power of the residue characteristic $p > 0$. Let m be the exponent of* $\mathrm{Gal}(L/K)$*, and let $r \mid m$ be the number of m-th roots of unity inside K. If $p = 2$ and $8 \mid m$, assume that $r \neq 2$. Then* $\mathrm{VC}(L/K)$ *holds if and only if every cyclic subextension F/E of L/K of degree r is a unit root Kummer extension.*

If $r = 1$ in Theorem 1.4, then the condition in the theorem is trivially satisfied, so that the valuation criterion holds. In particular, if K does not contain a primitive pth root of unity, then the valuation criterion holds for every abelian p-extension L of K.

When $p = 2$, the additional hypothesis is due to the fact that $(\mathbb{Z}/2^k\mathbb{Z})^*$ is not cyclic for $k \geq 3$. If $K = \mathbb{Q}_2(\sqrt{-2})$ and $L = \mathbb{Q}_2(\mu_{32})$, then we have $m = 8$ and $p = r = 2$. Theorem 1.4 implies that $\mathrm{VC}(F/E)$ holds for all extensions $E \subset F$ with $K \subset E \subset F \subset L$ of degree at most 4. We will see in Example 3.3 that $\mathrm{VC}(L/K)$ does not hold. Thus, we cannot omit the condition when $p = 2$ in Theorem 1.4.

2 The valuation criterion for having non-zero trace

The purpose of this section is to prove Proposition 1.1.

As before, K denotes a local field and $v_K\colon\ K^* \twoheadrightarrow \mathbb{Z}$ is the normalized valuation. Inside K we consider the valuation ring $\mathcal{O}_K = \{x \in K^*\colon\ v_K(x) \geq 0\} \cup \{0\}$, its maximal ideal $\mathfrak{p}_K$ and its unit group $\mathcal{O}_K^* = \{x \in K^*\colon\ v_K(x) = 0\}$. The valuation $v_L(\mathfrak{a})$ of a fractional ideal $\mathfrak{a}$ is the valuation of any of its generators, so $v_K(\mathfrak{p}_K^i) = i$ for all $i \in \mathbb{Z}$.

Suppose now that L is a finite separable field extension of K. Then L has the structure of a local field as well. We denote by $\mathrm{Tr}_{L/K}$ the trace map from L to K. Two integers are naturally attached to the extension L/K. The first one is its ramification index $e_{L/K}$, given by the equality $v_L(K^*) = e_{L/K}\mathbb{Z}$. The second one is $d_{L/K}$, the valuation of the different of L over K, which is characterized by the property that

$$i \geq -d_{L/K} \iff \mathrm{Tr}_{L/K}(\mathfrak{p}_L^i) \subset \mathcal{O}_K$$

for all $i \in \mathbb{Z}$; cf. [7, Ch. III]. Using this it is easy to identify the traces of ideals: for every $i \in \mathbb{Z}$ we have

$$\mathrm{Tr}_{L/K}(\mathfrak{p}_L^{-d_{L/K}+i}) = \mathfrak{p}_K^{\left\lfloor \frac{i}{e_{L/K}} \right\rfloor}, \tag{2.1}$$

where $\lfloor x \rfloor$ denotes the largest integer n with $n \leq x$.

Proof of Proposition 1.1. For any $d \in \mathbb{Z}$ let us consider the map

$$\varphi\colon\ \mathfrak{p}_L^d/\mathfrak{p}_L^{d+1} \longrightarrow \mathrm{Tr}_{L/K}(\mathfrak{p}_L^d)/\mathrm{Tr}_{L/K}(\mathfrak{p}_L^{d+1}).$$

induced by the trace map. Denoting the residue field of K by k, and the degree of the residue field extension of L/K by $f = [L : K]/e_{L/K}$, we see that the domain of φ is an f-dimensional vector space over k. By (2.1) above, the codomain of f is a vector space over k which is of dimension 1 if $d \equiv -d_{L/K} - 1 \bmod [L : K]$ and of dimension 0 if $d \not\equiv -d_{L/K} - 1 \bmod [L : K]$. Since φ is a k-linear surjective map it follows that φ is an isomorphism if and only if both conditions (1) and (2) in the Proposition are satisfied.

We now distinguish two cases. If φ is an isomorphism, then for any element $x \in L^*$ with $v_L(x) = d$ we have $\mathrm{Tr}_{L/K}(x) \notin \mathrm{Tr}_{L/K}(\mathfrak{p}_L^{d+1})$, which implies that $\mathrm{Tr}_{L/K}(x) \neq 0$.

If, on the other hand, φ is not an isomorphism, then we can choose $x \in \mathfrak{p}_L^d$ so that ($x \bmod \mathfrak{p}_L^{d+1}$) is a non-zero element of the kernel of φ. We then have $\mathrm{Tr}_{L/K}(x) \in \mathrm{Tr}_{L/K}(\mathfrak{p}_L^{d+1})$, so that $\mathrm{Tr}_{L/K}(x) = \mathrm{Tr}_{L/K}(y)$ for some $y \in \mathfrak{p}_L^{d+1}$. But this implies that $x - y$ is an element of L of valuation d and trace 0. This completes the proof of Proposition 1.1. □

3 The set of valuations of elements in a linear subspace

In this section we prove Propostion 1.2. The key tools we develop for this, and for applications in the next section, are basic properties of the set of valuations of elements in subspaces of a field extension.

Let L/K be a finite separable totally ramified extension of local fields of degree n.

Let $v\colon\ L^* \to \mathbb{Z}/n\mathbb{Z}$ be given by $x \mapsto v_L(x) \bmod n$.

For any sub-K-vector space V of L we define the set $s(V)$ by

$$s(V) = \{v(x)\colon\ x \in V,\ x \neq 0\} \subset \mathbb{Z}/n\mathbb{Z}.$$

Since L is totally ramified over K, Proposition 1.1 implies that exactly one residue class modulo $e_{L/K}$ does not occur as the valuation of an element of the "trace zero" hyperplane. This is a general fact that holds for all sub-K-vector spaces of L.

Lemma 3.1. *For every sub-K-vector space V of L, we have $\#s(V) = \dim_K(V)$.*

Proof. Let S be a subset of V such that v maps S bijectively to $s(V)$. We will show that S is a basis of V over K.

Note that in a non-trivial K-linear combination of elements of S, all non-zero terms have valuations which are distinct modulo n. Thus, these valuations are distinct and their minimum is the valuation of the sum. In particular, this sum is not zero in L, and it follows that S is a linearly independent set over K.

Now let W be the sub-K-vector space of V generated by S. Consider the finitely generated $\mathcal{O}_K$-submodules $W^0 = W \cap \mathcal{O}_L \subset V^0 = V \cap \mathcal{O}_L$ of $\mathcal{O}_L$. Using the fact that $v(W^0\backslash\{0\}) = v(V^0\backslash\{0\})$ one sees that $V^0 = W^0 + \mathfrak{p}_K V^0$. Nakayama's lemma then implies that $V^0 = W^0$. It follows that $V = KV^0 = KW^0 = W$. □

Recall that we have a non-degenerate symmetric K-bilinear form on L given by $(x, y) \mapsto \mathrm{Tr}_{L/K}(xy)$. For any sub-$K$-vector space V of L, the orthogonal space $V^\perp \subset L$ is isomorphic to the K-dual of L/V.

Lemma 3.2. *Let $\overline{d} = (-d_{L/K} - 1 \bmod n\mathbb{Z}) \in \mathbb{Z}/n\mathbb{Z}$. For every sub-$K$-vector space V of L the set $s(V^\perp)$ is the complement in $(\mathbb{Z}/n\mathbb{Z})$ of the set $\overline{d} - s(V)$.*

Proof. For non-zero $x \in V$ and $y \in V^\perp$ we have $\mathrm{Tr}_{L/K}(xy) = 0$, so that $v(x) + v(y) = v(xy) \neq \overline{d}$ by Proposition 1.1. It follows that $\overline{d} \notin s(V) + s(V^\perp)$, so that $s(V^\perp)$ is contained in the complement in $(\mathbb{Z}/n\mathbb{Z})$ of the set $d - s(V)$. One sees with Lemma 3.1 that these two sets have the same cardinality, the codimension over K of V in L, so they are equal. □

For example, taking $V = K$ the orthogonal space $V^\perp$ is the kernel of the trace, and $s(V^\perp) = (\mathbb{Z}/n\mathbb{Z})\backslash\{\overline{d}\}$.

Proof of Proposition 1.2. If L/K is not totally ramified, then Proposition 1.1 implies that $\mathrm{VC}(L/K)$ is false; we may thus assume that L/K is totally ramified of degree n.

Clearly, $\mathrm{VC}(L/K)$ holds if and only if no $K[G]$-submodule V strictly contained in L contains an element x with $v(x) = \overline{d}$, where $\overline{d} = (-d_{L/K} - 1 \bmod n\mathbb{Z}) \in \mathbb{Z}/n\mathbb{Z}$. This means that $\overline{d} \notin s(V)$ for all such V. By duality, the map $V \mapsto W = V^\perp$ gives a bijection from the set of $K[G]$-submodules V of L that are strictly contained in L to the set of non-zero $K[G]$-submodules W of L. By Lemma 3.2, we have $\overline{d} \notin s(V) \iff 0 \in s(V^\perp)$, so we deduce that $\mathrm{VC}(L/K)$ holds if and only if $0 \in s(W)$ for every non zero $K[G]$-submodule W of L. Thus we see that $\mathrm{VC}(L/K)$ is equivalent to condition (2).

It remains to show that condition (2) implies that $[L : K]$ is a power of the residue characteristic p. To see this, let L'/K be the maximal tamely ramified subextension of L over K. Then condition (2) also holds for L'/K. So, by what we proved already, $\mathrm{VC}(L'/K)$ holds. Since L'/K is tamely ramified, we have $d_{L'/K} = e_{L'/K} - 1$ [7, Ch. III, §6, Prop. 13]. Then $\mathrm{VC}(L'/K)$ implies that non-zero elements of K are normal basis generators for L' over K, so $L' = K$. □

Example 3.3. Let $K = \mathbb{Q}_2(\sqrt{-2})$ and for n a power of 2 let ζ_n denote a root of unity of order n in a fixed algebraic closure of K. For $d = 2, 4, 8, 16, \ldots$ the field $L_d = \mathbb{Q}_2(\zeta_{4d})$ is cyclic of order d over K, and its Galois group G_d is generated by the automorphism $\sigma\colon\ \zeta_{4d} \mapsto \zeta_{4d}^3$.

To check whether condition (2) of Proposition 1.2 holds for the extension L_4/K, note that the minimal non-zero $K[G_4]$-submodules of L_4 are the kernels of the elements $f(\sigma)$ acting on L_4, where f ranges over the irreducible factors $X-1$, $X+1$ and X^2+1 of $X^4-1 \in K[X]$. Thus, the minimal $K[G_4]$-submodules of L_4 are K and $\ker \mathrm{Tr}_{L_2/K}$, and $\ker \mathrm{Tr}_{L_4/L_2}$. These contain the units: $1, \zeta_4$ and ζ_{16}. So, by Proposition 1.2, $\mathrm{VC}(L_4/K)$ holds.

Let us try the same for L_8/K. The polynomial $X^8 - 1$ factors over K into irreducible polynomials as follows:

$$X^8 - 1 = (X - 1)(X + 1)(X^2 + 1)(X^2 + \sqrt{-2}X - 1)(X^2 - \sqrt{-2}X + 1),$$

so in addition to the minimal submodules we found inside L_4, which we know contain units, we need to consider two sub-$K[G_8]$-modules of K-dimension 2 inside $\ker \mathrm{Tr}_{L_8/L_4}$.

Now ζ_{32} is contained in $\ker_{L_8/L_4}$, so let us put $x = \sigma^2(\zeta_{32}) - \sqrt{-2}\sigma(\zeta_{32}) - \zeta_{32}$. Then the sub-$K$-vector space V of L generated by x and $\sigma(x)$ is a minimal $K[G]$-submodule of L. One now checks with a computation that $v_{L_8}(x) = 10$ and $v_{L_8}(\sigma(x) - x) = 14$, so that $\{2, 6\} \subset s(V) \subset (\mathbb{Z}/8\mathbb{Z})$. With Lemma 3.1 we see that $s(V) = \{2, 6\}$, and it follows from Proposition 1.2 that $\mathrm{VC}(L_8/K)$ does not hold. From the proof above we see that an element of L of valuation $-d_{L_8/K} - 1$ can be found inside the $K[G_8]$-submodule $V^\perp$ of L_8.

We conclude this section with some easy consequences of Propostion 1.2.

Corollary 3.4. *If $K \subset L \subset M$ are finite extensions of local fields with M and L both Galois over K, then* $\mathrm{VC}(M/K)$ *implies* $\mathrm{VC}(L/K)$.

Note that, in the setting of this corollary, a normal element for M over K is not necessarily normal over L; see [1] for an easy example, and [4, 5]. We do not know whether the implication $\mathrm{VC}(M/K) \implies \mathrm{VC}(M/L)$ always holds, even for abelian extensions. However, it does hold in a particular setting of Kummer extensions — see Lemma 4.3.

Lemma 3.5. *Let L/K be a totally ramified Galois extension of local fields whose degree n is a power of the residue characteristic $p > 0$. For every finite tamely ramified extension $\widetilde{K}/K$ we have*

$$\mathrm{VC}(\widetilde{K}L/\widetilde{K}) \implies \mathrm{VC}(L/K).$$

Proof. Put $\widetilde{L} = \tilde{K}L$. Note first that $[\widetilde{L} : \widetilde{K}] = [L : K]$, because the tame part of L/K is trivial. Let V be a K-submodule of L. Put $\widetilde{V} = \widetilde{K}V$; it is a $\widetilde{K}$-submodule of $\widetilde{L}$. Note that we have the obvious inclusion

$$e_{\widetilde{K}/K} s(V) \subset s(\widetilde{V}).$$

Since $e_{\widetilde{K}/K}$ is coprime to p and therefore to n, and since $s(V)$ and $s(\widetilde{V})$ are both of cardinality $\dim_K(V)$ (Lemma 3.1), it follows that this inclusion is in fact an equality. Thus, V contains a unit of L (i.e., 0 belongs to $s(V)$) if and only if $\widetilde{V}$ contains a unit of $\widetilde{L}$ (i.e., 0 belongs to $s(\widetilde{V})$). Assume now that $\mathrm{VC}(\widetilde{L}/\widetilde{K})$ holds. Then Proposition 1.2 implies that the space $\widetilde{V}$ contains a unit, so that V contains a unit too. The K-submodule V of L being arbitrary, again by Proposition 1.2 it follows that $\mathrm{VC}(L/K)$ holds. □

4 Applications to abelian extensions

In this section we consider only abelian extensions L/K. We will show that Theorems 1.3 and 1.4 hold by using Proposition 1.2.

Proof of Theorem 1.3. Suppose that $G = \mathrm{Gal}(L/K)$ is of exponent m, and that K contains a primitive mth root of unity. Put $n = \#G$. By Kummer theory there exists a K-basis R of L such that $\{r^m : \ r \in R\}$ is a full set of coset representatives of $K^* \cap L^{*m}$ modulo K^{*m}. Thus, L/K is a unit root Kummer extension if and only if $m \mid v_K(r^m)$ for all $r \in R$.

The K-algebra $K[G]$ is totally split, and L is free of rank 1 over $K[G]$, so L is the direct sum of its n distinct minimal non-zero $K[G]$-submodules, and they all have dimension 1 over K. These submodules are therefore the modules Kr with $r \in R$.

By Proposition 1.2, we know that $\mathrm{VC}(L/K)$ holds if and only if all minimal non-zero $K[G]$-submodules of L contain an element of $\mathcal{O}_L^*$. The result now follows by noting that

$$Kr \cap \mathcal{O}_L^* \neq \emptyset \iff n \mid v_L(r) \iff nm \mid v_L(r^m) \iff m \mid v_K(r^m).$$

□

Example 4.1. Suppose that K contains μ_{p^2}, that $u \in \mathcal{O}_K^*$ is not a p-th power and that $\pi \in K^*$ satisfies $v_K(\pi) = 1$. Then $u\pi^p$ is not a p-th power in K, so $L = K(\sqrt[p^2]{u\pi^p})$ is a cyclic extension of degree p^2. It is a Kummer extension, and by Theorem 1.4 it does not satisfy $\mathrm{VC}(L/K)$. However, the intermediate field $M = K(\sqrt[p]{u})$ satisfies both $\mathrm{VC}(M/K)$ and $\mathrm{VC}(L/M)$. Note that $-1 - d_{L/K} \equiv -1 - d_{L/M} \not\equiv 0 \bmod p$.

In order to prove Theorem 1.4 we first present two auxilliary results.

Lemma 4.2. *If L/K is an abelian extension, and K has characteristic 0, then $\mathrm{VC}(L/K)$ holds if and only if $\mathrm{VC}(E/K)$ holds for all intermediate fields $K \subset E \subset L$ for which E is cyclic over K.*

Proof. Let V be a minimal non-zero $K[G]$-submodule of L. Since the group ring $K[G]$ is a product of fields, the image F of $K[G]$ in $\mathrm{End}_K(V)$ is a field. Let H be the kernel of the canonical map $G \to F^*$, and let $E = L^H$. Then $V \subset E$, and $G/H = \mathrm{Gal}(E/K)$ is cyclic because it embeds into F^*. We have just shown that every minimal non-zero $K[G]$-submodule of L is contained inside a field E with $K \subset E \subset L$ and E/K cyclic. The lemma now follows from Proposition 1.2. □

Lemma 4.3. *Let M/K be a Galois extension of local fields and let L be a subfield of M which is normal over K. If M/L is abelian of exponent r and K contains a root of unity of order r then*

$$\mathrm{VC}(M/K) \implies \mathrm{VC}(M/L).$$

Proof. Suppose that $x \in M$ is normal over K. We will show that x is also normal over L. We write $G = \mathrm{Gal}(M/K)$ and $H = \mathrm{Gal}(M/L)$. Then we know that x has trivial annihilator in the ring $K[G]$, so it also has trivial annihilator in $K[H]$. The latter is a totally split K-algebra. Since $L[H]$ is a totally split L-algebra with the same number of components, each of its nonzero ideals contains a nonzero element of $K[H]$. Thus, x also has a trivial annihilator in $L[H]$, and x is normal over L.

If we assume that $\mathrm{VC}(M/K)$ holds, then for some $d \in \mathbb{Z}$ all $x \in M^*$ of valuation d are normal over K. We just showed that all these x are then normal for M/L too. With Proposition 1.1 this implies that $d \equiv -d_{M/L} - 1 \bmod [M : L]$, and it follows that $\mathrm{VC}(M/L)$ holds. □

The core of our argument lies in the proof of the following two lemmas.

Lemma 4.4. *Let L/K be a totally ramified abelian extension of local fields of mixed characteristic $(0, p)$, whose degree is a power of p. Let μ_p be the group of pth roots of unity in an algebraic closure of K. If $\mu_p \not\subset K$ and $L(\mu_p)/K(\mu_p)$ is a Kummer extension then $\mathrm{VC}(L(\mu_p)/K(\mu_p))$ holds.*

Proof. Put $\widetilde{K} = K(\mu_p)$, $\widetilde{L} = L(\mu_p)$ and $G = \mathrm{Gal}(L/K) = \mathrm{Gal}(\widetilde{L}/\widetilde{K})$. Let m be the exponent of G. Note first that $\widetilde{K}[G]$ is a totally split $\widetilde{K}$-algebra, so $\widetilde{L}$ is the direct sum of its minimal non-zero submodules, which are exactly the eigenspaces

$$E_\chi = \{x \in L\colon\ gx = \chi(g)x \text{ for all } g \in G\},$$

where χ ranges over $\mathrm{Hom}(G, \widetilde{K}^*)$. We will consider the sets $s(E_\chi)$, where s is as in Section 3 for the extension $\widetilde{L}/\widetilde{K}$. Since E_χ is 1-dimensional over $\widetilde{K}$, these are one element sets.

By our assumptions, there is an element $\sigma \in \mathrm{Gal}(\widetilde{L}/K)$ that acts non-trivially on μ_p, so it acts on $\mu_m \subset \widetilde{K}^*$ by raising elements to the power c for some $c \in \mathbb{Z}$, which is not 1 modulo p.

Now on the one hand $s(\sigma(E_\chi)) = s(E_\chi)$, because σ preserves the valuation. On the other hand, we have $x^c \in E_{\chi^c} = \sigma(E_\chi)$ for all $x \in E_\chi$, so $s(\sigma(E_\chi)) \supset cs(E_\chi)$. Since $c-1$ is coprime to $[\widetilde{L} : \widetilde{K}]$ and $s(E_\chi)$ is a set consisting of a single element, this implies that $s(E_\chi) = \{0\}$. By Proposition 1.2, it then follows that $\mathrm{VC}(\widetilde{L}/\widetilde{K})$ holds. □

Lemma 4.5. *Let L/K be a totally ramified cyclic extension of local fields of mixed characteristic $(0,p)$ whose degree n is a power of p. Let $r \mid n$ be the number of n-th roots of unity in K^*. Assume that $p \mid r$, and if $p = 2$ and $8 \mid n$ assume that $r \neq 2$. For the chain of fields $K \subset L_r \subset L_p \subset L$ where $[L : L_p] = p$ and $[L : L_r] = r$ we then have*

$$\mathrm{VC}(L/L_r) \text{ and } \mathrm{VC}(L_p/K) \implies \mathrm{VC}(L/K).$$

Proof. If σ is a generator of $G = \mathrm{Gal}(L/K)$, then the minimal non-zero $K[G]$-submodules of L are the spaces $V_f = \{x \in L\colon\ f(\sigma)\cdot x = 0\}$, where f ranges over the monic irreducible factors of $X^n - 1$ in $K[X]$. Let μ_n be the group of n-th roots of unity in some algebraic closure of K. Every $z \in \mu_n$ either has order less than n, so that it is a zero of $X^{n/p} - 1$, or it has order n and then $z^{n/r}$ is a root of unity of order r in K. Thus we see that

$$X^n - 1 = (X^{n/p} - 1) \prod_{\substack{\zeta \in K^* \\ \#\langle\zeta\rangle = r}} (X^{n/r} - \zeta).$$

We claim that the polynomials $X^{n/r} - \zeta$ are all irreducible in $K[X]$. In order to see this, note first that $\mathrm{Gal}(K(\mu_n)/K) \subset \mathrm{Aut}(\mu_n) = (\mathbb{Z}/n\mathbb{Z})^*$. Let H be the kernel of the map $(\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/r\mathbb{Z})^*$. Then $\mathrm{Gal}(K(\mu_n)/K)$ is a subgroup of H, not contained in the kernel of the map $(\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/pr\mathbb{Z})^*$. Under the assumption we made, H is the only such group, so that $\mathrm{Gal}(K(\mu_n)/K) = H$ and $K(\mu_n)$ has degree $n/r = \#H$ over K. This shows the claim.

Suppose now that f is an irreducible factor of $X^n - 1$. If f is a factor of $X^{n/p} - 1$ then V_f is a $K[G]$-submodule of L_p. Otherwise, $f = X^{n/r} - \zeta$ for some $\zeta \in K^*$ of order r, and V_f is an eigenspace for the action of $G_r = \langle\sigma^{n/r}\rangle = \mathrm{Gal}(L/L_r)$ on L, so it is an $L_r[G_r]$-submodule of L. Thus, every minimal $K[G]$-submodule of L is a $K[G]$-submodule of L_p or it is an $L_r[G_r]$-submodule of L. Our statement now follows with Proposition 1.2. □

We can now prove our main theorem.

Proof of Theorem 1.4. Let us first assume that VC(L/K) holds, and suppose that we have intermediate fields $K \subset E \subset F \subset L$ with F/E cyclic of degree r. Then VC(F/K) holds by Corollary 3.4 and VC(F/E) holds by Lemma 4.3. With Theorem 1.3, we then see that F/E is a unit root Kummer extension.

To show the other implication, we assume that F/E is a unit root Kummer extension for all E, F as above, which by Theorem 1.3 implies that VC(F/E) holds too. We also assume that we are not in the case where $p = r = 2$ and $8 \mid m$. We will prove that VC(L/K) holds, and by Lemma 4.2 it suffices to do this under the additional hypothesis that L/K is cyclic. So we assume that L/K is cyclic of degree n. We now consider two cases: $r = 1$ and $r > 1$.

If $r > 1$ then we proceed with induction on n/r, where $n = [L : K]$. If $n/r = 1$, then we may take E/F to be L/K, and we are done. If $n/r > 1$, then consider $K \subset L \subset L_r \subset L_p \subset L$ as in Lemma 4.5. By the induction hypothesis we then see that VC(L_p/K) holds. Taking F/E to be L/L_r we see that VC(L/L_r) holds. Thus, Lemma 4.5 completes the proof in the case that $r > 1$.

Now suppose that $r = 1$. Put $\widetilde{K} = K(\mu_p)$ and $\widetilde{L} = L(\mu_p)$. We claim that VC($\widetilde{F}/\widetilde{E}$) holds whenever $\widetilde{K} \subset \widetilde{E} \subset \widetilde{F} \subset \widetilde{L}$ and $\widetilde{F}/\widetilde{E}$ is a Kummer extension. By Galois theory, $\widetilde{E}$ and $\widetilde{F}$ are of the form $\widetilde{E} = E(\mu_p)$ and $\widetilde{F} = F(\mu_p)$ for certain intermediate fields $K \subset E \subset F \subset L$. We then have $\mu_p \not\subset E$, because L/K has only a trivial tame part, so by Lemma 4.4 we see that VC($\widetilde{E}/\widetilde{F}$) holds, as claimed. By using the already proven case $r > 1$ of Theorem 1.4, it follows that VC($\widetilde{L}/\widetilde{K}$) holds. By Lemma 3.5 this implies that VC(L/K) holds. □

References

[1] D. Blessenohl, K. Johnsen, *Eine Verschärfung des Satzes von der Normalbasis*, Journal of Algebra, **103** (1986), 141-159.

[2] N. P. Byott, G.G. Elder, *A valuation criterion for normal bases in elementary abelian extensions*, Bull. London Math. Soc., **39** (5) (2007), 705-708.

[3] G.G. Elder, *A valuation criterion for normal basis generators in local fields of characteristic p*, Arch. Math., **94** (2010), 43-47.

[4] C.C. Faith, *Extensions of normal bases and completely basic fields*, Transactions of the American Mathematical Society, **85** (1957), 406 - 427.

[5] D. Hachenberger, *Finite fields, Normal bases and completely free elements*, Kluwer Academic Publishers, 1997.

[6] L.Thomas, *A valuation criterion for normal basis generators in equal positive characteristics*, Journal of Algebra, preprint 2008.

[7] J.-P. Serre, *Corps locaux*, fourth edition, Hermann, Paris, 1968.