
Volume 305 · Number 1, November 1, 2006 · ISSN 0021-8693
ELSEVIER
JOURNAL OF
ALGEBRA
Editor-in-Chief
Michel Broué
Editor of the section on Computational Algebra
Gerhard Hiss
Founding Editor
G. Higman, 1964–1984
Editor-in-Chief
W. Feit, 1985–2000
Editorial Board
Luchezar L. Avramov
Eva Bayer-Fluckiger
Corrado de Concini
William Crawley-Boevey
Steven Dale Cutkosky
Kent R. Fuller
Dihua Jiang
Masaki Kashiwara
E.I. Khukhro
Kazuhiko Kurano
Gus I. Lehrer
Martin Liebeck
Peter Littelmann
Susan Montgomery
Laurent Moret-Bailly
Jan Saxl
Leonard L. Scott, Jr.
Vera Serganova
Aner Shalev
Ronald Solomon
J.T. Stafford
Gernot Stroth
Michel Van den Bergh
Efim Zelmanov
Section on Computational Algebra
Jon Carlson
Henri Cohen
John Cremona
Patrick Dehornoy
Harm Derksen
Meinolf Geck
Gerhard Hiss
Derek Holt
William M. Kantor
Reinhard Laubenbacher
Gunter Malle
Eamonn O'Brien
Bruno Salvy
Jean-Yves Thibon

Available online at www.sciencedirect.com
ScienceDirect
Journal of Algebra 305 (2006) 603–613
JOURNAL OF Algebra
www.elsevier.com/locate/jalgebra

A formula for Tignol's constant

Munish Kumar, Sudesh K. Khanduja *

Department of Mathematics, Panjab University, Chandigarh 160014, India

Received 25 September 2005
Available online 17 February 2006
Communicated by Eva Bayer-Fluckiger

Abstract

Let (K, v) be a Henselian valued field and (L, w) be a finite separable extension of (K, v). In 2004, it was proved that the set $A_{L/K}$ defined by $A_{L/K} = \{v(\mathrm{Tr}_{L/K}(\alpha)) - w(\alpha) \mid \alpha \in L, \alpha \neq 0\}$ has a minimum element if and only if $[L : K] = ef$ where e, f are the ramification index and the residual degree of w/v, i.e., $(L, w)/(K, v)$ is defectless. The constant $\min A_{L/K}$ was first introduced by Tignol and is referred to as Tignol's constant. In 2005, K. Ota and Khanduja gave a formula for $\min A_{L/K}$ when $(L, w)/(K, v)$ is an extension of local fields. In this paper, we give this formula when (L, w) is any finite separable defectless extension of a Henselian valued field of arbitrary rank and thereby generalize some well-known results of Dedekind regarding "different" of extensions of algebraic number fields and ramification of prime ideals.

Keywords: Valued fields; Non-Archimedean valued fields

1. Introduction

Throughout this paper, v is a Henselian valuation of arbitrary rank of a field K and $\tilde{v}$ is the unique prolongation of v to a fixed algebraic closure $\tilde{K}$ of K. Let $(L, w) \subseteq (\tilde{K}, \tilde{v})$ be a finite extension of (K, v). The extension $(L, w)/(K, v)$ (or briefly L/K) is called defectless if $[L : K] = ef$ where e and f are the index of ramification and the residual

* Corresponding author.
E-mail addresses: msingla79@yahoo.com (M. Kumar), skhand@pu.ac.in (S.K. Khanduja).

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2006.01.016

degree of w/v. Since (K, v) is Henselian, for any α in L and σ in $\mathrm{Gal}(\tilde{K}/K)$, $\tilde{v} \circ \sigma(\alpha) = \tilde{v}(\alpha)$ and consequently $v(\mathrm{Tr}_{L/K}(\alpha)) \geqslant w(\alpha)$; here and elsewhere Tr stands for the trace map. In 1990, Tignol proved that if $(L, w)/(K, v)$ is a finite separable defectless extension of degree equal to the characteristic of the residue field of v, then the set $A_{L/K}$ defined by

$$A_{L/K} = \{v(\mathrm{Tr}_{L/K}(\alpha)) - w(\alpha) \mid \alpha \in L,\ \alpha \neq 0\}$$

has a minimum element; moreover he gave a formula to calculate $\min A_{L/K}$ in this case (see [8, Proposition 2.5], [9, Lemma 1.1]). The constant $\min A_{L/K}$ is referred to as Tignol's constant. It is also known that for a finite separable extension, Tignol's constant is zero if and only if the extension is tamely ramified (see [2]). In 2004, Khanduja and Singh [3] extended the result of Tignol besides proving its converse by showing that a finite extension (L, w) of a Henselian valued field (K, v) is defectless if and only if $A_{L/K}$ has a minimum element. They also proved that if $K \subseteq M \subseteq L$ is a tower of finite separable defectless extensions then

$$\min A_{L/K} = \min A_{L/M} + \min A_{M/K} \tag{1}$$

(see [3, Theorem 2.5]). This gives rise to the following natural question:

Question. *Can we find a simple formula for* $\min A_{L/K}$*, where* (L, w) *is any finite separable defectless extension of* (K, v)*?*

In 2005, Khanduja and Ota [4] gave a formula for Tignol's constant when (L, w) is a finite extension of a local field (K, v), i.e., K is a finite extension of the field Q_p of p-adic numbers or of $F_p((t))$. Indeed they proved that $\min A_{L/K} = \frac{d}{[L:K]} - 1 + \frac{1}{e}$, where e is the ramification index and P_K^d the discriminant of $(L, w)/(K, v)$, P_K being the maximal ideal of the valuation ring of v. In this paper, we give a formula for Tignol's constant when the base field is a Henselian valued field (K, v) of arbitrary rank; this formula yields "Dedekind's Theorem" regarding ramification of prime ideals in algebraic number fields and will be stated after introducing some notations.

In what follows, for a finite extension L of K contained in $\tilde{K}$, the valuation on L will be the restriction of $\tilde{v}$ and G_L, R_L, $\bar{L}$ will stand respectively for the value group, valuation ring and the residue field of this valuation. For any ξ in the valuation ring of $\tilde{v}$, $\bar{\xi}$ will denote its $\tilde{v}$-residue, i.e., the image of ξ under the canonical homomorphism from the valuation ring of $\tilde{v}$ onto its residue field. Also $e(L/K)$ will denote the ramification index, i.e., the index of the value group G_K of v in G_L. As in [1, 18.3], it can be easily seen that elements of the set

$$S_{L/K} = \{\lambda \in G_L \mid 0 \leqslant \lambda < \gamma \text{ for all positive } \gamma \text{ in } G_K\} \tag{2}$$

lie in different cosets of G_L/G_K and hence $S_{L/K}$ has at most $e(L/K)$ elements. The maximum element of $S_{L/K}$ will be denoted by $\lambda_{L/K}$. We shall denote by $C_{L/K}$ the codifferent of L/K (with respect to v) defined by

$$C_{L/K} = \{\alpha \in L \mid \mathrm{Tr}_{L/K}(\alpha R_L) \subseteq R_K\}.$$

For proving the main result of this paper, it will be proved that the fractional ideal $C_{L/K}$ is principal. This result is also of independent interest. Note that in case v is a discrete valuation, then $C_{L/K}^{-1}$ is the usual different of the extension L/K (cf. [7, p. 50]).

With the above notations, we prove

Theorem 1.1. *Let v be a Henselian valuation of arbitrary rank of a field K and $\tilde{v}$ be the unique prolongation of v to the fixed algebraic closure $\tilde{K}$ of K. Let L be a finite separable defectless extension of K, then the R_L-module $C_{L/K}$ is generated by a single element and*

$$\min A_{L/K} = -\min_{\alpha \in C_{L/K}} \{\tilde{v}(\alpha)\} - \lambda_{L/K}.$$

The corollary stated below is an immediate consequence of Theorem 1.1.

Corollary 1.2. *Let v be a Henselian discrete valuation of a field K having value group $\mathbb{Z}$. Let L/K be a finite separable defectless extension with ramification index e and codifferent P_L^{-D}, P_L being the maximal ideal of the valuation ring R_L. Then*

$$\min A_{L/K} = \frac{D}{e} - \frac{e-1}{e}.$$

Keeping in mind that $\min A_{L/K} \geqslant 0$ and the result that $\min A_{L/K} = 0$ if and only if the extension L/K is tamely ramified proved in [2], the above corollary yields at once the following well-known results of Dedekind (cf. [6, Theorem 4.8, Proposition 6.2], [7, Chapter III, Propositions 10, 13, Theorem 1]).

Corollary 1.3. *Let (K, v), R_L, e and P_L be as in Corollary* 1.2 *and $\mathfrak{D}$ be the different of the extension L/K (with respect to v). Then the following hold*:

(i) *P_L^{e-1} divides $\mathfrak{D}$.*
(ii) *L/K is tamely ramified if and only if the exact power of P_L dividing $\mathfrak{D}$ is $e-1$.*
(iii) *L/K is unramified if and only if P_L does not divide $\mathfrak{D}$.*

2. Some preliminary results

We retain the notations of the preceding section. For α belonging to the algebraic closure $\tilde{K}$ of K, we shall write $\tilde{v}(\alpha)$ as $v(\alpha)$.

Lemma 2.1. *If $K \subseteq M \subseteq L$ is a tower of finite extensions of (K, v), then the following hold*:

(a) $\lambda_{L/M} + \lambda_{M/K} = \lambda_{L/K}$.
(b) *If L/K is a separable extension, then $C_{L/M}C_{M/K} \subseteq C_{L/K}$; further if $C_{M/K}$ is a principal ideal, then $C_{L/M}C_{M/K} = C_{L/K}$.*

Proof. Let l_0 and m_0 be elements of L and M, respectively, such that $v(l_0) = \lambda_{L/M}$ and $v(m_0) = \lambda_{M/K}$. First we show that

$$\lambda_{L/M} + \lambda_{M/K} \leqslant \lambda_{L/K}. \tag{3}$$

Suppose to the contrary that $\lambda_{L/K} < \lambda_{L/M} + \lambda_{M/K}$, so there exists $t \in K$ such that $0 < v(t) \leqslant v(l_0) + v(m_0)$, i.e., $v(t) - v(m_0) \leqslant v(l_0)$. As $v(m_0) = \lambda_{M/K}$, $v(t) - v(m_0)$ must be positive. Thus we see that t/m_0 is an element of M with positive valuation which is at most $\lambda_{L/M}$. This is impossible in view of the definition of $\lambda_{L/M}$. Hence (3) is proved.

To prove that equality holds in (3), let γ be any positive element of the value group G_M. By definition of $\lambda_{M/K}$, there exists $\delta \in G_K$ with $0 < \delta \leqslant \lambda_{M/K} + \gamma$. Since $\delta > \lambda_{L/K}$ by definition of $\lambda_{L/K}$, it follows that $\gamma > \lambda_{L/K} - \lambda_{M/K}$. This inequality holds for all $\gamma \in G_M$ with $\gamma > 0$, hence $\lambda_{L/M} \geqslant \lambda_{L/K} - \lambda_{M/K}$, which proves assertion (a) of the lemma.

To verify $C_{L/M}C_{M/K} \subseteq C_{L/K}$, note that for any α belonging to $C_{L/M}$ and a in $C_{M/K}$, we have $\mathrm{Tr}_{L/K}(a\alpha R_L) = \mathrm{Tr}_{M/K}(a\,\mathrm{Tr}_{L/M}(\alpha R_L)) \subseteq \mathrm{Tr}_{M/K}(aR_M) \subseteq R_K$ and hence the result. Suppose now that $C_{M/K}$ is a principal ideal generated by b. The chain of equivalences

$$\begin{aligned}\beta \in C_{L/K} \quad &\Leftrightarrow \quad \mathrm{Tr}_{L/K}(\beta R_L) \subseteq R_K \quad \Leftrightarrow \quad \mathrm{Tr}_{M/K}\big(\mathrm{Tr}_{L/M}(\beta R_L)R_M\big) \subseteq R_K \\ &\Leftrightarrow \quad \mathrm{Tr}_{L/M}(\beta R_L) \subseteq C_{M/K} = bR_M \quad \Leftrightarrow \quad b^{-1}\beta \in C_{L/M}\end{aligned}$$

proves that $C_{L/K} = C_{L/M}C_{M/K}$. □

Lemma 2.2. *Let $K \subseteq M \subseteq L$ be a tower of finite separable defectless extensions of (K, v). If Theorem* 1.1 *holds for the extensions L/M and M/K, then it holds for L/K.*

Proof. By the hypothesis, $C_{L/M}$ and $C_{M/K}$ are principal ideals and

$$\min A_{L/M} = -\min_{\alpha \in C_{L/M}}\big\{v(\alpha)\big\} - \lambda_{L/M}, \qquad \min A_{M/K} = -\min_{\alpha \in C_{M/K}}\big\{v(\alpha)\big\} - \lambda_{M/K}.$$

Adding the above two equations and using (1) together with Lemma 2.1, we see that $C_{L/K} = C_{L/M}C_{M/K}$ and

$$\min A_{L/K} = -\min_{\alpha \in C_{L/M}}\big\{v(\alpha)\big\} - \min_{\alpha \in C_{M/K}}\big\{v(\alpha)\big\} - \lambda_{L/K} = -\min_{\alpha \in C_{L/K}}\big\{v(\alpha)\big\} - \lambda_{L/K}$$

as desired.

Lemma 2.3. *Let L be a finite defectless separable extension of (K, v). If $l' \in L$ is such that $v(\mathrm{Tr}_{L/K}(l')) - v(l') = \min A_{L/K}$, then $l'/\mathrm{Tr}_{L/K}(l')$ belongs to $C_{L/K}$.*

Proof. Let r be any element of R_L. For verifying that $\mathrm{Tr}_{L/K}(l'r/\mathrm{Tr}_{L/K}(l'))$ belongs to R_K, note that

$$\begin{aligned} &v\big(\mathrm{Tr}_{L/K}(l'r)\big) - v\big(\mathrm{Tr}_{L/K}(l')\big) \\ &\quad = v\big(\mathrm{Tr}_{L/K}(l'r)\big) - v(l'r) - \big[v\big(\mathrm{Tr}_{L/K}(l')\big) - v(l')\big] + v(r) \geqslant 0. \qquad \square \end{aligned}$$

Lemma 2.4. *Let $K \subseteq M \subseteq L$ be a tower of finite separable defectless extensions. If Theorem 1.1 holds for the extensions L/K and L/M, then it holds for M/K.*

Proof. By hypothesis, $C_{L/K}$ and $C_{L/M}$ are principal R_L-ideals generated by α_0 and α_1 respectively (say), and

$$\min A_{L/K} = -v(\alpha_0) - \lambda_{L/K}, \qquad \min A_{L/M} = -v(\alpha_1) - \lambda_{L/M}.$$

On subtracting and using formula (1) together with Lemma 2.1(a), it follows from the last two equations that

$$\min A_{M/K} = v(\alpha_1) - v(\alpha_0) - \lambda_{M/K}. \tag{4}$$

Claim is that $C_{M/K}$ is a principal ideal, i.e., the set $\{v(m) \mid m \in C_{M/K}\}$ has a minimum element which will indeed be equal to $v(\alpha_0) - v(\alpha_1)$ by virtue of Lemma 2.1(b). This will prove the lemma in view of (4). We now verify the claim. By Lemma 2.1(b) $C_{L/M}C_{M/K} \subseteq C_{L/K}$ and hence on recalling that $C_{L/K}, C_{L/M}$ are generated by α_0, α_1 respectively, we have $C_{M/K} \subseteq (\alpha_0/\alpha_1)R_L$, i.e.,

$$v(m) \geqslant v(\alpha_0) - v(\alpha_1) \quad \text{for all } m \in C_{M/K}.$$

The above inequality and (4) imply that for each m in $C_{M/K}$, one has

$$\min A_{M/K} + v(m) \geqslant -\lambda_{M/K}. \tag{5}$$

On setting $\min A_{M/K} = v(\mathrm{Tr}_{M/K}(m')) - v(m')$, $m' \in M$, inequality (5) can be rewritten as

$$v(m') - v\big(\mathrm{Tr}_{M/K}(m')\big) - v(m) \leqslant \lambda_{M/K}, \quad m \in C_{M/K}. \tag{6}$$

Keeping in mind that $\lambda_{M/K}$ is the maximum element of the finite set $S_{M/K}$ defined by (2) and that $m'/\mathrm{Tr}_{M/K}(m')$ belongs to $C_{M/K}$ by Lemma 2.3, it now follows from (6) that the set $\{v(m) \mid m \in C_{M/K}\}$ has minimum element $v(m') - v(\mathrm{Tr}_{M/K}(m')) - \lambda$ for some λ in $S_{M/K}$. This proves the claim and completes the proof of the lemma. $\square$

Definition. Let $(L, w)/(K, v)$ be an extension of degree n. A basis $\alpha_1, \ldots, \alpha_n$ of L/K is called a valuation basis (with respect to w/v) if for each $\alpha = \Sigma a_i\alpha_i$ in L, $a_i \in K$, the equation $w(\alpha) = \min_i w(a_i\alpha_i)$ holds.

Lemma 2.5. *Let $L = K(\theta)$ be a separable extension of degree n of (K, v) with $f(x)$ as the minimal polynomial of θ over K. The following hold*:

(a) *If $R_L = R_K[\theta]$, then $C_{L/K} = \frac{1}{f'(\theta)} R_L$.*
(b) *If $1, \theta, \ldots, \theta^{n-1}$ is a valuation basis of L/K (with respect to v), then*

$$\min A_{L/K} = v\big(f'(\theta)\big) - (n-1)v(\theta).$$

Proof. We prove only assertion (b) of the lemma as the first assertion is already known (see [7, Corollary 2, p. 56], [6, Theorem 4.6]). By hypothesis $1, \theta, \ldots, \theta^{n-1}$ is a valuation basis of L/K, hence so is $\frac{1}{f'(\theta)}, \frac{\theta}{f'(\theta)}, \ldots, \frac{\theta^{n-1}}{f'(\theta)}$. Let η be a non-zero element of L. Write $\eta = \sum a_i\theta^i / f'(\theta)$, $a_i \in K$. Then by what we have said above

$$v(\eta) = \min_i \left\{ v(a_i) + v\left(\frac{\theta^i}{f'(\theta)}\right) \right\}.$$

Also by the triangle law

$$v\big(\mathrm{Tr}_{L/K}(\eta)\big) \geqslant \min_i \left\{ v(a_i) + v\left(\mathrm{Tr}_{L/K}\left(\frac{\theta^i}{f'(\theta)}\right)\right) \right\}.$$

Therefore

$$v\big(\mathrm{Tr}_{L/K}(\eta)\big) - v(\eta) \geqslant \min_i \left\{ v\left(\mathrm{Tr}_{L/K}\left(\frac{\theta^i}{f'(\theta)}\right)\right) - v\left(\frac{\theta^i}{f'(\theta)}\right) \right\}. \tag{7}$$

By an elementary result of field theory (see [5, Chapter VI, Proposition 5.5], [7, Chapter 3, Lemma 2]), we have

$$\mathrm{Tr}_{L/K}\left(\frac{\theta^{n-1}}{f'(\theta)}\right) = 1, \qquad \mathrm{Tr}_{L/K}\left(\frac{\theta^i}{f'(\theta)}\right) = 0 \quad \text{for } 0 \leqslant i \leqslant n-2.$$

So the minimum on the right-hand side of (7) is $v(f'(\theta)) - (n-1)v(\theta)$. This proves the required result. □

Lemma 2.6. *Theorem* 1.1 *holds when L is any defectless separable extension of (K, v) of prime degree.*

Proof. Let q denote the degree of the extension L/K and $\bar{K} \subseteq \bar{L}$ stand for the residue fields as introduced in the first section. We split the proof into two cases:

Case I. $\bar{K} \neq \bar{L}$. Since L/K is defectless, there exists $\theta \in L$ such that $v(\theta) = 0$ and the v-residue of θ does not belong to the residue field of v. So the v-residue of θ is algebraic of degree q over the residue field $\bar{K}$ of v. Therefore for any element $\xi = \sum_{i=0}^{q-1} a_i\theta^i$ belonging to L, $v(\xi) = \min_i\{v(a_i)\}$, for otherwise $v(\xi) > \min_i\{v(a_i)\} = v(a_j)$ which would imply

$\sum_{i=0}^{q-1}(\overline{a_i/a_j})\bar{\theta}^i = \bar{0}$ and consequently $\bar{\theta}$ would satisfy a non-zero polynomial of degree less than q over $\bar{K}$, contrary to our assumption. Thus $1, \theta, \ldots, \theta^{q-1}$ is a valuation basis of L/K and $R_L = R_K[\theta]$. On applying Lemma 2.5, we see that $C_{L/K}$ is a principal ideal and that the desired equality holds in the present case.

Case II. $G_L \neq G_K$. Let $S_{L/K}$ denote the set defined by (2). This case is split into two subcases.

Case II (a). $S_{L/K} \neq \{0\}$. Recall that $S_{L/K}$ is a finite set, we can chose $\theta \in L$ such that $v(\theta)$ is the least positive element of $S_{L/K}$. Now q (a prime number) is the least positive integer such that $qv(\theta) \in G_K$, so whenever a, b are any non-zero elements of K, then

$$v(a\theta^i) \neq v(b\theta^j), \quad 0 \leqslant i \neq j \leqslant q-1.$$

Therefore it follows from the strong triangle law that for any $\xi = \sum_{i=0}^{q-1} a_i\theta^i$ in L, we have $v(\xi) = \min_i v(a_i\theta^i)$; this proves that $1, \theta, \ldots, \theta^{q-1}$ is a valuation basis of L/K. Keeping in mind that $(q-1)v(\theta)$ is the largest element of $S_{L/K}$, it can be easily checked that $R_L = R_K[\theta]$. Applying Lemma 2.5, we see that Theorem 1.1 holds in the present situation.

Case II (b). $S_{L/K} = \{0\}$. Let I be a well-ordered set such that $\{C_i,\ i \in I\}$ is the chain of all convex subgroups of G_L with $C_i \subset C_j$ for $i < j$. Let j be the least index such that $C_j \cap G_K \neq C_j$. Note that C_j/C_{j-1} is of rank one and hence is order isomorphic to a subgroup of the group $\mathbb{R}$ of real numbers under addition (cf. [10, p. 45]). Also $C_j/(C_j \cap G_K)$ being isomorphic to a non-trivial subgroup of G_L/G_K is of order q. Consequently $(C_j \cap G_K)/C_{j-1}$ is a subgroup of index q of C_j/C_{j-1}. Choose an element θ of L with $v(\theta) \in C_j \backslash (C_j \cap G_K)$ such that $v(\theta) + C_{j-1}$ is the least positive element of C_j/C_{j-1} in case C_j/C_{j-1} is a cyclic group. In case it is not cyclic, this group as well as $(C_j \cap G_K)/C_{j-1}$ will be order isomorphic to dense subgroups of $(\mathbb{R}, +)$ (cf. [1, 4.1]); consequently in this situation

$$v(\theta) = \sup\bigl\{v(a) \mid a \in K,\ v(a) \in C_j \cap G_K,\ v(a) < v(\theta)\bigr\}. \tag{8}$$

Keeping in mind that $v(\theta)$ belongs to $C_j \setminus (C_j \cap G_K)$ and arguing as in Case II(a), we see that $1, \theta, \ldots, \theta^{q-1}$ is a valuation basis of L/K. In view of Lemma 2.5(b), the theorem is proved in the present situation, once we prove that

$$C_{L/K} = \frac{\theta^{q-1}}{f'(\theta)} R_L \tag{9}$$

where $f(x) = x^q - b_1x^{q-1} - \cdots - b_q$ is the minimal polynomial of θ over K. We first prove that

$$\frac{\theta^{q-1}}{f'(\theta)} R_L \subseteq C_{L/K}. \tag{10}$$

Let $\eta = \sum_{i=0}^{q-1} a_i\theta^i$, $a_i \in K$, be any element of R_L. It is required to be shown that

$$v\left(\mathrm{Tr}_{L/K}\left(\eta\frac{\theta^{q-1}}{f'(\theta)}\right)\right) \geqslant 0. \tag{11}$$

By an elementary result of field theory (see [5, Chapter VI, Proposition 5.5]), we have

$$\mathrm{Tr}_{L/K}\left(\frac{\theta^{q-1}}{f'(\theta)}\right) = 1, \qquad \mathrm{Tr}_{L/K}\left(\frac{\theta^{i}}{f'(\theta)}\right) = 0 \quad \text{for } 0 \leqslant i \leqslant q-2. \tag{12}$$

Using (12) repeatedly, a simple calculation shows that

$$\mathrm{Tr}_{L/K}\left(\eta\frac{\theta^{q-1}}{f'(\theta)}\right) = a_0 + a_1t_1 + \cdots + a_{q-1}t_{q-1}, \tag{13}$$

where

$$t_1 = b_1, \qquad t_i = b_1t_{i-1} + b_2t_{i-2} + \cdots + b_{i-1}t_1 + b_i, \quad 1 \leqslant i \leqslant q-1. \tag{14}$$

Recall that $\eta = \sum_{i=0}^{q-1} a_i\theta^i$ belongs to R_L and $1, \theta, \ldots, \theta^{q-1}$ is a valuation basis of L/K; consequently $v(a_i) + iv(\theta) \geqslant 0$ for $0 \leqslant i \leqslant q-1$. Therefore in view of (13), the desired inequality (11) is proved once it is shown that

$$v(t_i) \geqslant iv(\theta), \quad 1 \leqslant i \leqslant q-1. \tag{15}$$

We prove (15) by induction on i. As $f(x) = x^q - b_1x^{q-1} - \cdots - b_q$ is the minimal polynomial of θ over K, it follows that

$$v(b_i) \geqslant iv(\theta), \quad i \geqslant 1. \tag{16}$$

In particular $v(t_1) = v(b_1) \geqslant v(\theta)$ which gives (15) for $i = 1$. Assume that (15) holds for all i with $1 \leqslant i \leqslant k \leqslant q-2$. By virtue of (14), we have

$$v(t_{k+1}) \geqslant \min_{1\leqslant i\leqslant k}\left\{v(b_it_{k+1-i}), v(b_{k+1})\right\}.$$

Now using induction hypothesis and (16), it follows that $v(t_{k+1}) \geqslant (k+1)v(\theta)$, which proves (15) for $i = k+1$. Thus the proof of (11) and hence that of (10) is complete.

For obtaining (9), it remains to be shown that

$$C_{L/K} \subseteq \frac{\theta^{q-1}}{f'(\theta)}R_L. \tag{17}$$

Take an element $\xi = \sum_{i=0}^{q-1} a_i\frac{\theta^i}{f'(\theta)}$ belonging to $C_{L/K}$, $a_i \in K$. To prove (17), it is required to be verified that $v(\xi f'(\theta)) \geqslant (q-1)v(\theta)$, which is the same as saying that

$$v(a_i) + iv(\theta) \geqslant (q-1)v(\theta), \quad 0 \leqslant i \leqslant q-1. \tag{18}$$

Recall that by the choice of θ, $v(\theta) + C_{j-1}$ is the least positive element of C_j/C_{j-1} in case C_j/C_{j-1} is a cyclic group and so $v(\theta)$ is the supremum of C_{j-1} in this case; also $v(\theta)$ satisfies (8) in the other case. Let a run over those elements of K for which $v(a) \in C_{j-1}$ when the group C_j/C_{j-1} is cyclic and $v(a) \in C_j \cap G_K$, $v(a) < v(\theta)$ in the other case. So (18) is proved once it is shown that for each such $v(a)$, we have

$$v(a_i) \geqslant (q-1-i)v(a), \quad 0 \leqslant i \leqslant q-1. \tag{19}$$

To verify the above inequality, let a be an element of K with $v(a)$ as above. Note that θ/a belongs to R_L. Keeping in mind that $\xi = \sum_{i=0}^{q-1} a_i \frac{\theta^i}{f'(\theta)}$ is an element of $C_{L/K}$, it follows that

$$\mathrm{Tr}_{L/K}\big(\xi(\theta/a)^k\big) \in R_K, \quad 0 \leqslant k \leqslant q-1. \tag{20}$$

Taking $k = 0$ in (20) and using (12), we obtain $v(a_{q-1}) \geqslant 0$. Again using (20) for $k = 1$ and (12), it can be easily seen that $v(a_{q-2} + a_{q-1}b_1) \geqslant v(a)$, which together with the fact $v(a_{q-1}) \geqslant 0$ and $v(b_1) \geqslant v(\theta) > v(a)$ implies that $v(a_{q-2}) \geqslant v(a)$. Thus (19) is verified for $i = q-1, q-2$. Now using (20) for $k = 2$ and arguing as above, we shall obtain $v(a_{q-3}) \geqslant 2v(a)$. Proceeding like this, (19) and hence (18) is proved. This proves (17) and completes the proof of (9). □

Lemma 2.7. *Theorem* 1.1 *holds if we have the extra hypothesis that the extension L/K is unramified.*

Proof. As L/K is unramified, $\bar{L}/\bar{K}$ is a separable extension of degree $[L : K] = n$. So there exists an element θ in L such that $v(\theta) = 0$ and $\bar{L} = \bar{K}(\bar{\theta})$. Proceeding as in the proof of Case I of Lemma 2.6, it can be easily seen that $1, \theta, \ldots, \theta^{n-1}$ is a valuation basis of L/K, $R_L = R_K[\theta]$ and the desired assertion follows from Lemma 2.5. □

Lemma 2.8. *Let N be a finite Galois extension of K. Then Theorem* 1.1 *holds for the maximal tame extension of (K, v) contained in N.*

Proof. Let K^T, K^V be the inertia field and ramification field of N/K (with respect to v). By ramification theory, K^V is the maximal tame extension of (K, v) contained in N, K^T/K is an unramified extension and K^V/K^T is an abelian extension.

So there exists a tower of field extensions

$$K^T \subset K_1 \subset \cdots \subset K_s = K^V$$

such that each extension K_i/K_{i-1} is of prime degree. The lemma now follows immediately from Lemmas 2.2, 2.6 and 2.7. □

3. Proof of Theorem 1.1

Let $p \geqslant 0$ denote the characteristic of the residue field of v. Let N be a finite Galois extension of K containing L and K^V be the ramification field of N/K with respect to v. Then N/K^V is a p-extension if $p > 0$ and $N = K^V$, otherwise. Since tameness is preserved under composition [1, 20.15], LK^V/L is a tame and hence defectless extension. Therefore LK^V/K is a defectless extension. In view of Lemma 2.4, Theorem 1.1 is proved for the extension L/K as soon as it is shown that it holds for the defectless extensions LK^V/K and LK^V/L.

We first verify the validity of the theorem for LK^V/K. Consider the groups

$$H_0 = \operatorname{Gal}(N/K^V), \quad H = \operatorname{Gal}(N/LK^V).$$

Since H_0 is a p-group, there exists a descending chain of subgroups

$$H_0 \supset H_1 \supset \cdots \supset H_t = H \supset H_{t+1} \supset \cdots \supset \{e\}$$

such that each H_i is normal subgroup of H_{i-1} of index p. If K_i denotes the fixed field of H_i, then

$$K^V = K_0 \subset K_1 \subset \cdots \subset K_t = LK^V$$

is a tower of extensions of degree p each. By Lemma 2.6, Theorem 1.1 holds for K_i/K_{i-1}, $1 \leqslant i \leqslant t$, and consequently for LK^V/K^V in view of Lemma 2.2. It is valid for K^V/K by Lemma 2.8 and thus is valid for LK^V/K.

It only remains to show that the theorem holds for LK^V/L. Let M be the maximal tame extension of L contained in N. As LK^V/L is tame, M contains LK^V. By Lemma 2.8, the theorem holds for M/L. So in view of Lemma 2.4, it is enough to verify the validity of the theorem for M/LK^V. Since N/LK^V is a Galois p-extension with subextension M/LK^V, arguing as in the above paragraph and applying Lemmas 2.6, 2.2, it can be seen that the theorem holds for the extension M/LK^V. This completes the proof.

Acknowledgment

This paper was written while the authors were visiting Harish-Chandra Research Institute, Allahabad, India. They are highly grateful to Professor I.B.S. Passi for numerous helpful suggestions and the institute for hospitality. The financial support by National Board for Higher Mathematics, Mumbai is gratefully acknowledged.

References

[1] O. Endler, Valuation Theory, Springer-Verlag, 1972.
[2] S.K. Khanduja, A characterization of finite tame extensions, Bull. London Math. Soc. 32 (2000) 551–554.

[3] S.K. Khanduja, A.P. Singh, On a theorem of Tignol for defectless extensions and its converse, J. Algebra 288 (2005) 400–408.
[4] S.K. Khanduja, K. Ota, A formula relating the discriminant of finite extension of local fields and Tignol's constant, submitted for publication.
[5] S. Lang, Algebra, third ed., Addison–Wesley, 1993.
[6] W. Narkiewicz, Elementary and Analytic Theory of Algebraic Numbers, second ed., Springer-Verlag, Polish Scientific Publishers, 1990.
[7] J.-P. Serre, Local Fields, Grad Texts in Math., vol. 67, Springer-Verlag, 1979.
[8] J.-P. Tignol, Algèbres à division et extensions de corps sauvagement ramifiées de degré premier, J. Reine Angew. Math. 404 (1990) 1–38.
[9] J.-P. Tignol, Classification of wild cyclic field extensions and division algebras of prime degree over a Henselian field, in: Contemp. Math., vol. 131, 1992, pp. 491–508.
[10] O. Zariski, P. Samuel, Commutative Algebra, vol. II, Van Nostrand, 1960.