Can. J. Math., Vol. XXVI, No. 4, 1974, pp. 908–916

RAMIFICATION THEORY FOR VALUATIONS OF ARBITRARY RANK

MURRAY A. MARSHALL

Throughout, we consider a finite Galois extension $L|K$ of non-archimedian valued fields which are maximally complete [**2**, Chapter 2]. Let v denote the valuation on L and let L^* denote the group of non-zero elements of L. We may identify the value group $v(L^*)$ of L with a subgroup of D, where D denotes the minimal divisible ordered group containing $v(K^*)$. We denote the residue field of L by $\bar{L}$, and will always assume that the field extension $\bar{L}|\bar{K}$ is separable. The characteristic of $\bar{K}$ will invariably be denoted by p; much of what follows is trivial in case $p = 0$. Let G denote the Galois group of $L|K$ and let $\bar{G}$ denote the Galois group of $\bar{L}|\bar{K}$. The kernel of the natural homomorphism of G onto $\bar{G}$ is the ramification group.

$$G_0 = \left\{\sigma \in G | v\left(\frac{\sigma u}{u} - 1\right) > 0 \text{ for all } u \in \mathscr{U}\right\},$$

where $\mathscr{U}$ denotes the unit group of L. The fixed field R of G_0 is the maximal unramified extension of K in L [**2**, p. 68]; the extension $L|R$ is totally ramified. The higher ramification groups G_x, $x \in D$, $x \geqq 0$ are defined by

$$G_x = \left\{\sigma \in G_0 | v\left(\frac{\sigma a}{a} - 1\right) \geqslant x \text{ for all } a \in L^*\right\}.$$

By the uniqueness of the extension of v from K to L we have that $v(\sigma x) = v(x)$ for all $x \in L^*$, $\sigma \in G$. Using this, one may verify readily that the ramification groups G_x, $x \geqq 0$ are invariant subgroups of G. The ramification groups form a decreasing chain with $G_x = 1$ for x sufficiently large.

From Lemma 1 below it follows that for each ramification group $G_z \neq 1$ there is a largest $x \in D$ such that $G_x = G_z$. Such an x will be called a jump of the extension $L|K$. If $x \in D$, $x \geqq 0$, let $0 = x_0 \leqq x_1 \leqq \ldots\ldots \leqq x_k = x$ be a sequence of elements of D containing all jumps of $L|K$ which lie in the interval $[0, x]$. The quantity

$$\phi(x) = \sum_{s=1}^{k} \# G_{x_s}(x_s - x_{s-1})$$

is independent of the choice of sequence and thus defines a function $\phi : D^+ \rightarrow D^+$ called the Herbrand Function of $L|K$. The Herbrand Function is strictly increasing and piecewise linear (in the obvious sense), and is thus bijective. It will be convenient to extend this function to $D^+ \cup \{\infty\}$ by defining $\phi(\infty) = \infty$.

Received February 14, 1973 and in revised form, August 14, 1973.

We may define a new indexing of the ramification groups (called the upper numbering) by defining

$$G^x = G_{\phi^{-1}(x)} \qquad \text{for } x \in D^+.$$

We call an element $y \in D^+$ an upper jump if $G^y \supsetneq G^{y+\epsilon}$ for all $\epsilon > 0$, $\epsilon \in D$. (Thus the upper jumps are just the values $\phi(x)$ where x is a lower jump).

The principal results in the classical rank 1 discrete case are:

(a) (Herbrand) If E is a Galois subextension of $L|K$ then the natural homomorphism of $G_{L|K}$ onto $G_{E|K}$ carries $G_{L|K}{}^x$ onto $G_{E|K}{}^x$ for all $x \in D^+$.

(b) (Hasse-Arf) If $L|K$ is abelian then the upper jumps of $L|K$ all lie in $v(K^*)$.

In this paper we show that (a) is true in general if and only if the value group quotient $\bar{\Gamma} = v(L^*)/v(K^*)$ has cyclic p-component. We also show that (b) holds in this case. The proof techniques are simple modifications of those in [**1**, Chapter 11], and [**3**] respectively.

1. Preliminaries. We begin with some elementary results on jumps.

LEMMA 1. *For $\sigma \in G_0$, the set of values $\{v(\sigma a/a - 1)|a \in L^*\}$ has a minimum; further, this minimum is not achieved for $a \in \mathscr{U}$* (except in the trivial case $\sigma = 1$).

Proof. Choose elements $1 = a_1, a_2, \ldots, a_n$ in L^* such that $v(a_1), \ldots, v(a_n)$ represent the distinct cosets of $\bar{\Gamma}$, each exactly once. Thus $a_1, a_2, \ldots, a_n$ form a basis of $L|R$; each $a \in L^*$ can be written uniquely in the form $a = \sum_{i=1}^n c_i a_i$, where $c_i \in R$ and $v(a) = v(c_{i_0} a_{i_0}) < v(c_i a_i)$ for $i \neq i_0$. Also

$$\frac{\sigma a}{a} - 1 = \sum_{i=2}^{n} \frac{c_i a_i}{a} \left(\frac{\sigma a_i}{a_i} - 1\right).$$

Thus $v(\sigma a/a - 1) \geqq \min \{v(\sigma a_i/a_i - 1)|i = 2, 3, \ldots, n\}$. This inequality is strict when $a \in \mathscr{U}$, since then $i_0 = 1$.

In view of this result we see that for each $x \geqq 0$, $G_x = \{\sigma \in G_0|i(\sigma) \geqq x\}$ where $i(\sigma)$ is defined by

$$(1) \qquad i(\sigma) = \min \{v(\sigma a/a - 1)|a \in L^*\}.$$

Also the jumps of the extension $L|K$ are just the values $i(\sigma)$, $\sigma \in G_0$, $\sigma \neq 1$ (so they are actually in $v(L^*)$).

We will have cause to use the following refined form of Lemma 1.

LEMMA 2. *If $b_1, \ldots, b_s$ are elements of L^* such that $\overline{v(b_1)}, \ldots, \overline{v(b_s)}$ generate $\bar{\Gamma}$, then for each $\sigma \in G_0$,*

$$i(\sigma) = \min \left\{v\left(\frac{\sigma b_i}{b_i} - 1\right) \mid i = 1, \ldots, s\right\}.$$

Proof. If $b \in L^*$ then

$$b = \prod_{i=1}^{s} b_i^{v_i} \cdot c \cdot u$$

https://doi.org/10.4153/CJM-1974-085-9 Published online by Cambridge University Press

where $c \in R$, $u \in \mathscr{U}$. Thus

$$\frac{\sigma b}{b} = \prod_{i=1}^{s} \left(\frac{\sigma b_i}{b_i}\right)^{v_i} \cdot \frac{\sigma u}{u},$$

so the result is clear from Lemma 1.

If i is a jump of $L|K$, let $j = \min \{i(\sigma)|i(\sigma) > i\}$. We examine the quotients $\bar{G}_i = G_i/G_j$ as in [**2**, Chapter 3]. Let $\overline{\mathscr{U}}_i$ denote the quotient group $\mathscr{U}_i/\mathscr{U}_{i^+}$, where

$$\mathscr{U}_i = \{1 + x \in \mathscr{U}|v(x) \geqq i\}, \qquad \mathscr{U}_{i^+} = \{1 + x \in \mathscr{U}|v(x) > i\}.$$

If $a \in L^*$ and $\sigma \in G_i$, then $\sigma a/a \in \mathscr{U}_i$ and the class of $\sigma a/a$ in $\overline{\mathscr{U}}_i$ depends only on the class of $\mu = v(a)$ in $\bar{\Gamma}$ and the class of σ in $\bar{G}_i$. In this way we obtain a bilinear mapping $(\bar{\sigma}, \bar{\mu}) \rightarrow (\sigma a/a).\mathscr{U}_{i^+}$ of $\bar{G}_i \times \bar{\Gamma}$ into $\overline{\mathscr{U}}_i$. Since $v(\sigma a/a - 1) > i$ for all $a \in L^*$ implies $i(\sigma) \geqq j$, we see that the derived homomorphism

$$\bar{G}_i \rightarrow \operatorname{Hom}(\bar{\Gamma}, \overline{\mathscr{U}}_i)$$

is injective. Moreover, since

$$\overline{\mathscr{U}}_i \cong \begin{cases} \bar{L}^*, & \text{if } i = 0, \\ \bar{L}, & \text{if } i > 0 \end{cases}$$

the group $\bar{G}_i$ is

(a) abelian of order prime to p if $i = 0$,

(b) an elementary p-group if $i > 0$. Consequently,

(c) G_0 is solvable.

(d) If T denotes the fixed field of G_j where $j = \min \{i(\sigma)|i(\sigma) > 0\}$, then T is the maximal tamely ramified extension of K in L [**2**, Chapter 3, § 2].

Using customary terminology, the extension $L|T$ will be called wildly ramified.

2. The Herbrand relationship. Suppose E is a subextension of $L|K$. Denote by H the Galois group of $L|E$ and by H_x, $x \in D^+$, the ramification groups of $L|E$. Then it is clear that

$$H_x = H \cap G_x \qquad \text{for all } x \in D^+.$$

We now assume that the extension $E|K$ is also Galois, and study the more complicated relationship between the ramification groups G_x and $(G/H)_x$. To avoid a lot of essentially trivial reductions we shall assume throughout this section that $L|K$ is totally ramified. The reader may verify that Theorems 1 and 2 are true as stated in the general case. For $\sigma \in G$, let $\bar{\sigma}$ denote its coset in G/H, and let $\bar{\imath}(\bar{\sigma})$ denote the function as defined by (1), but with respect to the extension $E|K$. That is, $\bar{\imath}(\bar{\sigma}) = \min \{v(\sigma a/a - 1)|a \in E^*\}$

LEMMA 3. *For all* $\sigma \in G$, $\bar{\imath}(\bar{\sigma}) \leqq \sum_{\gamma \in H} i(\sigma\gamma)$.

https://doi.org/10.4153/CJM-1974-085-9 Published online by Cambridge University Press

Proof. Using the solvability of $G = G_0$ we may assume $\# H = l$ is prime. We also assume $\bar{\imath}(\bar{\sigma}) > i(\sigma\gamma)$ for all $\gamma \in H$, since otherwise the result is trivially true. Thus the quantity $v(\sigma\gamma b/b - 1)$ never achieves the minimum value $i(\sigma\gamma)$ for $b \in E^*$. Choose any $a \in L^*$ such that $v(a)$ generates $v(L^*)$ modulo $v(E^*)$. In view of Lemma 2 plus what has just been said, we have

(2) $\quad i(\sigma\gamma) = v(\sigma\gamma a/a - 1) \quad$ for all $\gamma \in H$.

Let

$$f(x) = \prod_{\gamma \in H} (x - \gamma a) = b_0 + b_1 x + \ldots + b_{l-1}x^{l-1} + x^l$$

be the minimum polynomial of a over E. Since $v(a)$ generates $v(L^*)$ modulo $v(E^*)$ and since $f(a) = 0$ we have

(3) $\quad lv(a) = v(a^l) = v(b_0) < v(b_i a^i), \qquad i = 1, 2, \ldots, l-1.$

Since $f^\sigma(x) = \prod_{\gamma \in H} (x - \sigma\gamma a) = \sigma b_0 + \sigma b_1 x + \ldots + \sigma b_{l-1}x^{l-1} + x^l$, we have

$$\prod_{\gamma \in H} (a - \sigma\gamma a) = f^\sigma(a) = f^\sigma(a) - f(a) = \sum_{i=0}^{l-1} (\sigma b_i - b_i)a^i,$$

or

(4) $$a^l \prod_{\gamma \in H} \left(1 - \frac{\sigma\gamma a}{a}\right) = \sum_{i=0}^{l-1} \left(\frac{\sigma b_i}{b_i} - 1\right) b_i a^i.$$

Also by (3)

(5) $\quad v(\sigma b_0 - b_0) \geqq \bar{\imath}(\bar{\sigma}) + l\, v(a)$

$\quad v((\sigma b_i - b_i)a^i) > \bar{\imath}(\bar{\sigma}) + l\, v(a), \; i = 1, 2, \ldots, l-1.$

Combining (2), (4), and (5) yields

$$\sum_{\gamma \in H} i(\sigma\gamma) + lv(a) \geqslant \bar{\imath}(\bar{\sigma}) + l\, v(a),$$

so the lemma is proved.

LEMMA 4. *If the p-component of $\bar{\Gamma}$ is cyclic, then*

$$\sum_{\gamma \in H} i(\sigma\gamma) = \bar{\imath}(\bar{\sigma}), \quad \sigma \in G$$

holds for all Galois subextensions E of $L|K$, and conversely.

Proof. First assume $\bar{\Gamma}$ has cyclic p-component. As in Lemma 3, we may assume $\# H = l$ is prime. Let T denote the maximal tame extension of K in L. Then $E \cap T$ is the maximal tame extension of K in E. $v(L^*)/v(T^*)$ is cyclic by assumption. If $l = p$, then $E \cap T = T$ so $v(L^*)/v(E \cap T^*)$ is cyclic. This is true in any case, since $l \neq p$ implies

$$v(L^*)/v(E \cap T^*) \cong v(L^*)/v(E^*) \times v(L^*)/v(T^*).$$

https://doi.org/10.4153/CJM-1974-085-9 Published online by Cambridge University Press

Let $a \in L^*$ be such that $v(a)$ generates $v(L^*)$ modulo $v(E \cap T^*)$. If σ fixes $E \cap T$, then by Lemma 2, $i(\sigma\gamma) = v(\sigma\gamma a/a - 1)$ for all $\gamma \in H$. Reexamining the proof of Lemma 3 we see that $v(b_0) = lv(a)$ so $v(b_0)$ generates $v(E^*)$ modulo $v(E \cap T^*)$. Again applying Lemma 2, we have equality in (5) in the case $i = 0$. On the other hand, if $\bar{\sigma}$ does not fix $E \cap T$, then $\bar{\imath}(\bar{\sigma}) = 0 = i(\sigma\gamma)$ for all $\gamma \in H$. Thus the result is true in any case.

To prove the converse let T be the maximal tame extension of K in L, and let $p^n = [L : T]$. We prove a stronger result : namely we prove that if the formula holds for all extensions $L|E_i|K$, $i = 1, 2, \ldots, n-1$, where $K \subset T = E_0 \subset E_1 \subset \ldots \subset E_n = L$ is some special sequence of Galois subfields such that $[E_i : T] = p^i$, then $v(L^*)/v(T^*)$ is cyclic. When $n = 1$, the assumption is vacuous, but the result is obvious. In general, we choose $E = E_1$. By assumption, the formula holds for $L|E_i|K$, $i = 1, \ldots, n-1$, and hence certainly for $L|E_i|E$, $i = 2, \ldots, n-1$. Thus, by induction, $v(L^*)/v(E^*)$ is cyclic. Choose $a \in L^*$ such that $v(a)$ generates $v(L^*)$ modulo $v(E^*)$, and choose any $\sigma \in G$ fixing T but not E (i.e. $0 < \bar{\imath}(\bar{\sigma}) < \infty$). For $\gamma \in H$, $v(\sigma\gamma x/x - 1)$ is never the minimal value $i(\sigma\gamma)$ when $x \in E^*$, for this would imply $\bar{\imath}(\bar{\sigma}) = i(\sigma\gamma)$, contradicting $\bar{\imath}(\bar{\sigma}) = \sum_{\gamma \in H} i(\sigma\gamma)$. Thus, by Lemma 2, $i(\sigma\gamma) = v(\sigma\gamma a/a - 1)$ for all $\gamma \in H$. Using the terminology of Lemma 3, we see that the condition $\bar{\imath}(\bar{\sigma}) = \sum_{\gamma \in H} i(\sigma\gamma)$ forces $\bar{\imath}(\bar{\sigma}) = v(\sigma b_0/b_0 - 1)$. Clearly this implies that $v(b_0) = v(N_{L|E}(a)) = p^{n-1}v(a)$ generates $v(E^*)$ modulo $v(T^*)$. In particular $p^{n-1} v(a) \notin v(T^*)$, so the order of $\overline{v(a)}$ in $v(L^*)/v(T^*)$ must be p^n.

For $\sigma \in G$, let

$$i_\sigma = \max\{i(\sigma\gamma) \mid \gamma \in H\} = \max\{x \mid \sigma H \cap G_x \neq \phi\}.$$

Let $\tilde{\phi}$ denote the Herbrand Function as previously defined, but with respect to the extension $L|E$.

LEMMA 5. $\sum_{\gamma \in H} i(\sigma\gamma) = \tilde{\phi}(i_\sigma)$.

Proof. Let $0 = x_0 \leqq x_1 \leqq x_2 \leqq \ldots \leqq x_k = i_\sigma$ be any set of elements of D containing all the jumps of $L|K$ (and hence of $L|E$) in the interval $[0, i_\sigma]$. Let δ be the Kronecker Symbol:

$$\delta(x, S) = \begin{cases} 0, & \text{if } x \notin S. \\ 1, & \text{if } x \in S. \end{cases}$$

Then

$$\sum_{\gamma \in H} i(\sigma\gamma) = \sum_{\gamma \in H} \sum_{v=1}^{k} \delta(\sigma\gamma, G_{x_v})(x_v - x_{v-1})$$
$$= \sum_{v=1}^{k} \sum_{\gamma \in H} \delta(\sigma\gamma, G_{x_v})(x_v - x_{v-1}) = \sum_{v=1}^{k} \#(\sigma H \cap G_{x_v})(x_v - x_{v-1}).$$

However, if $\sigma H \cap G_x \neq \phi$, say $\sigma\gamma_0 \in \sigma H \cap G_x$, then $\sigma\gamma \to \gamma_0^{-1}\gamma$ defines a

$1-1$ correspondence between the elements of $\sigma H \cap G_x$ and the elements of $G_x \cap H = H_x$; thus the result.

If E is any Galois subextension of $L|K$, let H denote the Galois group of $L|E$ and let $\phi, \tilde{\phi}, \bar{\phi}$ denote the Herbrand Functions for $L|K$, $L|E$, and $E|K$. With these notations we have the following result.

THEOREM 1. *For all* $x \in D^+$,
(i) $G_x H/H \supset (G/H)_{\tilde{\phi}(x)}$,
(ii) $\phi(x) \geqq \bar{\phi}(\tilde{\phi}(x))$,
(iii) $G^x H/H \supset (G/H)^x$.

Proof. (i) By Lemmas 3 and 5, if $\sigma \in G$, then $\bar{\imath}(\bar{\sigma}) \leqq \tilde{\phi}(i_\sigma)$. Hence $\bar{\sigma} \in (G/H)_{\tilde{\phi}(x)} \Leftrightarrow \bar{\imath}(\bar{\sigma}) \geqq \tilde{\phi}(x) \Rightarrow \tilde{\phi}(i_\sigma) \geqq \tilde{\phi}(x) \Leftrightarrow i_\sigma \geqq x \Leftrightarrow \bar{\sigma} \in G_x H/H$.

(ii) Since the functions ϕ, $\bar{\phi} \circ \tilde{\phi}$ are piecewise linear on D^+, and $\phi(0) = 0 = \bar{\phi}(\tilde{\phi}(0))$, it is enough to show that the left-hand derivatives satisfy $\phi_l'(x) \geqq (\bar{\phi} \circ \tilde{\phi})_l'(x)$ for all $x \in D^+$:

$$(\bar{\phi} \circ \tilde{\phi})_l'(x) = \bar{\phi}_l'(\tilde{\phi}(x)) \cdot \tilde{\phi}_l'(x) = \#(G/H)_{\tilde{\phi}(x)} \cdot \#H_x \leqq \#(G_xH/H) \cdot \#H_x = \#(G_x/G_x \cap H) \cdot \#(G_x \cap H) = \#G_x = \phi_l'(x).$$

(iii) Let $x = \phi(y)$. Then $x \geqq \bar{\phi}(\tilde{\phi}(y))$ by (ii); hence

$$G^xH/H = G_yH/H \supset (G/H)_{\tilde{\phi}(y)} \supset (G/H)_{\bar{\phi}^{-1}(x)} = (G/H)^x.$$

THEOREM 2. *For a given Galois subextension E of $L|K$, the following conditions are equivalent:*
(i) $G_xH/H = (G/H)_{\tilde{\phi}(x)}$ *holds for all* $x \in D^+$,
(ii) $\phi = \bar{\phi} \circ \tilde{\phi}$,
(iii) $G^xH/H = (G/H)^x$ *holds for all* $x \in D^+$.
Further, these conditions hold for all Galois subextensions E of $L|K$ if and only if $\bar{\Gamma}$ has cyclic p-component.

Proof. (i) $\Leftrightarrow$ (ii). We have $G_xH/H \supset (G/H)_{\tilde{\phi}(x)}$ by Theorem 1. Thus $G_xH/H = (G/H)_{\tilde{\phi}(x)} \Leftrightarrow \#(G_xH/H) = \#(G/H)_{\tilde{\phi}(x)} \Leftrightarrow \phi_l'(x) = (\bar{\phi} \circ \tilde{\phi})_l'(x)$ as we see from the proof of Theorem 1.

(i), (ii) $\Leftrightarrow$ (iii). The result is immediate on examination of the proof of Theorem 1, (iii).

Finally, if we examine the proof of Theorem 1(i), we see that $G_xH/H = (G/H)_{\tilde{\phi}(x)}$ for all $x \in D^+ \Leftrightarrow \bar{\imath}(\bar{\sigma}) = \tilde{\phi}(i_\sigma)$ for all $\sigma \in G \Leftrightarrow \bar{\imath}(\bar{\sigma}) = \sum_{\gamma \in H} i(\sigma\gamma)$ for $\sigma \in G$. Hence the last assertion follows from Lemma 4.

3. The abelian case. The proof of the Hasse-Arf Theorem given below is a simple generalization of the proof given in [**3**] for the rank 1 discrete case.

THEOREM 3. *Assume $L|K$ is abelian and that the p-component of $\bar{\Gamma}$ is cyclic. Then the upper jumps of $L|K$ all lie in $v(K^*)$.*

Reduction of proof. Let x be an upper jump of $L|K$. By replacing L by a subfield if necessary, we may assume that x is the largest upper jump of $L|K$. Choose cyclic extensions $L_1, \ldots, L_s$ of K in L such that $[L_i : K]$ is a prime power for each i and such that L is the compositum of these subfields. Let $G(i)$ denote the Galois group of L_i over K. By Theorem 2, the natural surjective homomorphism $G \to G(i)$ carries G^y onto $G(i)^y$ for all $y \in D^+$. Hence the natural injection $G \to G(1) \times \ldots \times G(s)$ carries G^y into $G(1)^y \times \ldots \times G(s)^y$. In particular, $G^x \neq 1$ so there exists i_0 such that $G(i_0)^x \neq 1$. On the other hand, $G^{x+\epsilon} = 1$ for all $\epsilon > 0$, so $G(i_0)^{x+\epsilon} = 1$ for $\epsilon > 0$. Thus x is an upper jump of $L_{i_0}|K$. Now suppose $[L_{i_0} : K] = l^n$. If $l \neq p$, then $x = 0 \in v(K^*)$. Thus we have reduced the proof to the case where $L|K$ is wildly ramified and cyclic.

Now assume $L|K$ is wildly ramified cyclic and let $p^n = [L : K]$, $G = \langle \sigma \rangle$. If $\tau \in G$, $m \in Z$, then $i(\tau) \leqq i(\tau^m)$ with equality if and only if $p \nmid m$. Thus the jumps of $L|K$ are precisely the values $i_0 < i_i < \ldots < i_{n-1}$ where $i_k = i(\sigma^{p^k})$. The upper jumps are the values

$$\phi(i_k) = p^n i_0 + p^{n-1}(i_1 - i_0) + \ldots + p^{n-k}(i_k - i_{k-1}),\qquad k = 0, 1, 2, \ldots, n-1.$$

Thus, the conclusion of the Hasse-Arf Theorem in this case is equivalent to the statement

$$(6)\qquad p^{n-k}(i_k - i_{k-1}) \in v(K^*),\qquad k = 1, 2, \ldots, n-1.$$

We can rephrase this in yet another way: If $\mu \in v(L^*)$, let $\bar{\mu}$ denote the coset of μ in $\bar{\Gamma}$, and define $o(\mu) = s$ where p^s is the index of the cyclic subgroup $\langle \bar{\mu} \rangle$ in $\bar{\Gamma}$. Since $\bar{\Gamma}$ is cyclic, this also measures the p-divisibility of $\bar{\mu}$. Then (6) is equivalent to the statement

$$(7)\qquad o(i_k - i_{k-1}) \geqq k,\qquad k = 1, 2, \ldots, n-1.$$

If $\mu \in v(L^*)$, we define $\sigma^\mu = \sigma^{p^{o(\mu)}}$. An element $x \in L^*$ will be called *Special* (for σ) if

$$v(\sigma x/x - 1) = i(\sigma^{v(x)}).$$

LEMMA 6. *For each $\mu \in v(L^*)$, there is a special element $x \in L^*$ satisfying $v(x) = \mu$.*

Proof. If $o(\mu) = n$, then $\mu \in v(K^*)$. In this case any $x \in K^*$ for which $v(x) = \mu$ will serve. Now suppose $o(\mu) = s < n$. Then $\mu = p^s\alpha + \beta$ where $\alpha \in v(L^*)$, $\beta \in v(K^*)$. Moreover $o(\alpha) = 0$, so $\bar{\alpha}$ generates $\bar{\Gamma}$. Choose any $a \in L^*$ such that $v(a) = \alpha$, and any $b \in K^*$ such that $v(b) = \beta$. If we define

$$x = b \prod_{i=0}^{p^s-1} \sigma^i a,$$

then clearly $v(x) = \mu$. Moreover $\sigma x/x = \sigma^{p^s}a/a$, so the result is clear by Lemma 2.

LEMMA 7. *Every element $x \in L^*$ can be written as a finite sum of special elements whose values are distinct modulo $v(K^*)$.*

Proof. Using Lemma 6, we can form a basis of $L|K$ by choosing special elements of L^* whose value classes in $\bar{\Gamma}$ are distinct. Since the product of a special element with an element of K^* is again special, the result is obvious.

LEMMA 8. *If $0 < j < n - 1$ implies $o(i_j - i_{j-1}) \geqq j$, then the values $\mu + i(\sigma^\mu)$, $o(\mu) < n - 1$ are all distinct. They are also distinct from i_{n-2}.*

Proof. Suppose $\mu + i(\sigma^\mu) = \lambda + i(\sigma^\lambda)$. If $o(\mu) = o(\lambda)$, then $\sigma^\mu = \sigma^\lambda$ and therefore $\mu = \lambda$. Otherwise we see that $o(\mu - \lambda) = \min\{o(\mu), o(\lambda)\}$. But from the assumption, one also has $o(i(\sigma^\lambda) - i(\sigma^\mu)) > \min\{o(\mu), o(\lambda)\}$, so that $\mu - \lambda \neq i(\sigma^\lambda) - i(\sigma^\mu)$. As long as $o(\mu) < n - 1$ we have $o(i_{n-2} - i(\sigma^\mu)) > o(\mu)$ and therefore $i_{n-2} \neq \mu + i(\sigma^\mu)$.

Proof of Theorem 3. If $L|K$ is the extension of least degree for which the assertion fails, then by the proof reduction we may assume that $L|K$ is wildly ramified cyclic, and that the failure occurs at the largest jump only. Thus we have $o(i_k - i_{k-1}) \geqq k$, $k = 1, 2, \ldots, n - 2$, but $o(i_{n-1} - i_{n-2}) < n - 1$. Further, if E denotes the subfield of L fixed by σ^p, then by the minimality of n, the assertion is true for $L|E$, so $o(i_{n-1} - i_{n-2}) \geqq n - 2$. Thus $o(i_{n-1} - i_{n-2}) = n - 2$. Put $s = i_{n-2} - i_{n-1}$ and apply Lemma 6 to choose $z \in L^*$ special for σ^p such that $v(z) = s$. Thus $v(\sigma^p - 1)z) = s + i(\sigma^{ps}) = s + i_{n-1} = i_{n-2}$. Let $x = (\sigma^{p-1} + \sigma^{p-2} + \ldots + 1)z$. The operator $A = \sigma^{p-1} + \sigma^{p-2} + \ldots + 1$ is congruent to $(\sigma - 1)^{p-1}$ modulo p. Thus:

(8) $\quad v(x) = v(A(z)) > v(z) = s,$

(9) $\quad v((\sigma - 1)x) = v((\sigma^p - 1)z) = i_{n-2}.$

Expand x as in Lemma 7, $x = \sum_\mu x_\mu$, $v(x_\mu) = \mu$. Then set $y = \sum_\mu y_\mu$ where $y = (\sigma - 1)x$, $y_\mu = (\sigma - 1)x_\mu$. Break this expansion into two parts:

(10) $\quad y = \sum_{0(\mu)<n-1} y_\mu + \sum_{0(\mu)\geqslant n-1} y_\mu.$

By Lemma 8, the $v(y_\mu)$ occurring in the first sum are all distinct and $v(y) = i_{n-2}$ is also distinct from these. As for the second sum, notice that if μ occurs in it, one has $v(y_\mu) \geqq v(x_\mu) + i_{n-1}$ since $o(\mu) \geqq n - 1$. Since the values $v(x_\mu) = \mu$ lie in distinct cosets by choice, $v(x_\mu) \geqq v(x)$. Finally, by (8), $v(x) > s$. Hence $v(y_\mu) > s + i_{n-1} = i_{n-2}$ for terms in the second sum. Hence, if we write (10) in the form

$$y - \sum_{0(\mu)\geqslant n-1} y_\mu = \sum_{0(\mu)<n-1} y_\mu$$

and compare values, we obtain a contradiction.

https://doi.org/10.4153/CJM-1974-085-9 Published online by Cambridge University Press

References

1. E. Artin and J. Tate, *Class field theory* (Benjamin, New York, 1967).

2. O. F. G. Schilling, *The theory of valuations*, Math. Surveys No. *4* (Amer. Math. Soc., Providence, 1950).

3. S. Sen, *On automorphisms of local fields*, Ann. of Math. *90* (1969), 33–46.

University of Saskatchewan,
Saskatoon, Saskatchewan