PORTUGALIAE MATHEMATICA
Vol. 54 Fasc. 1 – 1997

ON THE MAIN INVARIANT OF AN ELEMENT OVER A LOCAL FIELD

N. Popescu and A. Zaharescu

Let K be a local field and let $\bar{K}$ be a fixed algebraic closure of it. In our previous work [6] is proved that to each element $a \in \bar{K}$ one can associate some numerical invariants relative to K. In the present paper we consider so called "main invariant" of a, defined in (1). In first section we get some remarks about this invariant. This invariant is related to so called "fundamental principle" of [6] and this principie is somewhat analogous to so called Krasner's lemma. This lemma is related to another numerical invariant, namely $\omega(a)$ defined in (2). Furthermore to the main invariant $\delta(a)$ it is assigned the subfield $K(a, \delta(a))$ of $K(a)$ (see Proposition 1.4). We observe that to $\omega(a)$ is "assigned" the subfield $K(a)$, and $K(a) = K(a, \delta(a))$ if and only if $\delta(a) = \omega(a)$. Moreover, Theorem 2.9 assert that always the extension $K(a)/K(a, \delta(a))$ is widly ramified! Finally, in Theorem 2.10 are related some invariants of a and b where (a, b) is a distinguished pair.

The results of this paper, will be utilised further to the study of extensions of a local field and specially to the study of closed subfields of $\boldsymbol{C}_p$ (the completion of the algebraic closure of p-adic numbers).

1 – Notations, definitions and general results

1. In this work by local field we shall mean a field K complete relative to a rank one and discrete valuation v (see [3], [4], [8], [9]). Let $\bar{K}$ be a fixed algebraic closure of K and denote also v the unique extension of v to $\bar{K}$. If $K \subseteq L \subseteq \bar{K}$ is an intermediate field, denote by: $G(L) = \{v(x);\ x \in L\}$. As usually $G(K)$ will be identified to the ordered group $\mathbb{Z}$ of rational integers and for any L, $G(L)$ will be viewed as a subgroup of the additive group $\mathbb{Q}$ of rational numbers. One has canonically: $G(K) = \mathbb{Z} \subseteq G(L) \subseteq G(\bar{K}) = \mathbb{Q}$. If L is an intermediate field,

Received: June 23, 1995; *Revised*: August 14, 1996.

denote $A(L) = \{x \in L, v(x) \geq 0\}$, the ring of integers of L, and $M(L) = \{x \in L, v(x) > 0\}$ the maximal ideal of $A(L)$. Let $R(L) = A(L)/M(L)$ the residue field of L. If $x \in A(L)$ denote x^* the image of x in $R(L)$.

Let L/K be a finite extension. Denote $e(L/K)$ the ramification index and by $f(L/K)$ the inertial degree of L. One has: $[L : K] = e(L/K) \cdot f(L/K)$.

2. If $a \in \bar{K}$, denote $\deg a = [K(a) : K]$ the *degree* of a. If $a \in \bar{K} \backslash K$ let us denote:

$$\delta(a) = \sup\Big\{v(a-c),\ c \in \bar{K},\ \deg c < \deg a\Big\}\ . \tag{1}$$

According to Krasner's principle ([3], pag. 66) it follows that $\delta(a)$ is finite whereas a is separable over K. Moreover according to ([2], Prop. 3.7 and Theorem 3.9) it follows that $\delta(a)$ is also finite even when a is not separable over K. It is easy to see that $\delta(a)$ is a rational number, and we call it the *main invariant* of a (with respect to K). According to ([6], Remark 3.3) relative to $\delta(a)$ it is true the following "*fundamental principle*": If $b \in \bar{K}$ is such that $v(b-a) > \delta(a)$, then $R(K(a)) \subseteq R(K(b))$ and $G(K(a)) \subseteq G(K(b))$. This principle is in consense with Krasner's principle ([3], pag. 66); it has weaker hypothesis and conclusions.

Remark 1.1. For any $a \in \bar{K} \backslash K$ one has:

1) If $x \in K$ then $\delta(a+x) = \delta(a)$.

2) $\delta(a^{-1}) = \delta(a) - 2v(a)$.

3) If $\delta \in \mathbb{Q}$ then (a, δ) is a minimal pair (see [2]) if and only if $\delta > \delta(a)$.

4) A pair (a, b) of elements of $\bar{K}$ will be called *distinguished* (see [6]) if:

1) $\deg a < \deg b$;

2) $v(b-a) = \delta(b)$;

3) If $\deg c < \deg a$ then $v(a-c) < \delta(b)$.

Remark 1.2. Let (a, b) be a distinguished pair. Then one has

1) $(a, \delta(b))$ is a minimal pair.

2) $R(K(a)) \subseteq R(K(b))$ and $G(K(a)) \subseteq G(K(b))$.

This Remark follows by ([6], Theorems 3.1 and 3.2).

Let $\gamma \in \mathbb{Q}$. Denote by $e(\gamma/K)$ the smallest non-zero positive rational integer such that $e\gamma \in G(K)$.

If $a \in \bar{K} \backslash K$, then generally one has

$$v(a) \leq \delta(a) \leq \omega(a) \tag{2}$$

(where $\omega(a) = \sup\{v(a - a')$, a' runs over all conjugates of a over K and $a' \neq a$, if a is separable$\}$, and $\omega(a) = \infty$ if a is not separable).

Remark 1.3. If $K(a)/K$ is totally ramified and a is an uniformising element of $K(a)$ then $\delta(a) = v(a)$. The next result tries to generalize this remark.

Proposition 1.4. *Let $a \in \bar{K} \backslash K$. The following assertions are equivalent:*

1) $v(a) = \delta(a)$.

2) *$e(K(a)/K) = e(v(a)/K)$ and for a suitable $h \in K$ such that $v(h) = ev(a)$, ($e = e(v(a)/K)$), the element $(a^e/h)^*$ generates $R(K(a))$ over $R(K)$.*

Proof: **1**)⇒**2**) One has: $v(a - 0) = v(a) = \delta(a)$. Hence, $(0, a)$ is a distinguished pair and so $(0, v(a))$ is a minimal pair (Remark 1.2). Let w be the residual transcendental extension of v to $K(x)$ defined by the minimal pair $(0, v(a))$ (see [1]).

Then according to ([6], Theorem 3.2) it follows that $f(X)$, the minimal and monic polynomial of a over K, is the lifting in $K[X]$ of a suitable polynomial of $R(K)[Y]$. Namely, since the minimal polynomial of 0 is X, there results $v(a) = w(X)$. Let $e = e(v(a)/K)$ and $h \in K$ be such that $v(h) = e\,v(a)$. One has $w(f) = n\,v(a)$, where $n = \deg a$. Also one has $n = e\,m$, and $(f/h^m)^* = G$ is an irreducible polynomial of $R(K)[Y]$ of degree m (there $Y = (X^e/h)^*$). Then f is the lifting of G relative to w. Hence one has: $f = X^{me} + A_1 X^{(m-1)e} + ... + A_m + H = f_1 + H$, where $H \in K[X]$, $\deg H < m\,e = n$, $w(H) > m\,e\,v(a)$ and $(f_1/h^m)^* = G$. Now, since $f(a) = 0$ it follows $G((a^e/h)^*) = 0$ and so $[R(K(a)) : R(K)] \geq m$. But $n = e\,m$ and so $R(K)((a^e/h)^*) = R(K(a))$, as claimed.

2)⇒**1**) Let us assume $v(a) < \delta(a)$. Let $b \in \bar{K}$ be such that (b, a) is a distinguished pair. One has: $v(b) = v(a)$ and so $e(K(b)/K) \geq e(v(b)/K) = e(v(a)/K) = e(K(a)/K)$. Now since $v(a/b - 1) > 0$, it follows that for any $h \in K$ such that $v(h) = e\,v(a)$, one has: $(a^e/h)^* = (b^e/h)^*$. Thus, by hypothesis it follows: $f(K(b)/K) \geq f(K(a)/K)$, and so: $\deg b = e(K(b)/K)\,f(K(b)/K) \geq e(K(a)/K) \cdot f(K(a)/K) = \deg a$, a contradiction. Hence the inequality $v(a) < \delta(a)$ is impossible and so by (2) $v(a) = \delta(a)$, as claimed. ∎

One can show that for any wildly ramified extension L of the Q_p, the field of p-adic numbers, there exists an element $a \in L$ such that $L = Q_p(a)$ and that a is as in Proposition 1.4. This remark will be developed in a forthcoming paper.

4. Let $a \in \bar{K}$ be separable over K. If δ is a real number, let us denote $\mathcal{H}(a,\delta)$ the subgroup of $\mathrm{Gal}(\bar{K}/K) = G$ consisting by all elements σ such that $v(a-\sigma(a)) > \delta$. Denote $K(a,\delta) = \mathrm{Fix}(\mathcal{H}(a,\delta))$. Since for any $\sigma \in G$ such that $\sigma(a) = a$ one has $\sigma \in \mathcal{H}(a,\delta)$, then $K(a,\delta) \subseteq K(a)$. $K(a,\delta)$ will be called the subfield of $K(a)$ *associated to* δ. Particularly $K(a)$ is associated to ∞. If $\delta_1 < \delta_2$, then $K(a,\delta_1) \subseteq K(a,\delta_2)$.

Proposition 1.5. *Let a, b be separable over K. Assume that $v(a-b) > \delta(a)$. Then $K(a,\delta(a)) \subseteq K(b,\delta(b))$.*

Proof: To prove that inclusion, will be enough to show that $\mathcal{H}(a,\delta(a)) \supseteq \mathcal{H}(b,\delta(b))$. Indeed the relation $v(a-b) > \delta(a)$, show that $\deg a \leq \deg b$. Then $\delta(a) \leq \delta(b)$, since if c is such that $\deg c < \deg a$ and $v(a-c) = \delta(a)$, then necessarily $v(b-c) = \delta(a)$. But then if $\sigma \in \mathcal{H}(b,\delta(b))$, then $v(b-\sigma(b)) > \delta(b)$ and so $v(a-\sigma(a)) = v(a-b+b-\sigma(b)+\sigma(b)-\sigma(a)) > \delta(a)$. Hence $\sigma \in \mathcal{H}(a,\delta(a))$, as claimed. ∎

Remark 1.6. Let a be separable over K and δ a real number. Denote $\mathcal{M}(a,\delta) = \{\sigma(a),\ \sigma \in \mathcal{H}(a,\delta)\}$ and let $m(a,\delta)$ be the cardinality of $\mathcal{M}(a,\delta)$. Then one has: $m(a,\delta) = [K(a) : K(a,\delta)]$ and elements of $\mathcal{M}(a,\delta)$ are exactly the conjugates of a over $K(a,\delta)$.

5. Proposition 1.7. *Let $a, b \in \bar{K}$ be both separable over K. Assume that (a,b) is a distinguished pair. Let f be the monic minimal polynomial of a over K and let $\gamma = v(f(b))$. Then $\gamma \in G(K(a)) + Z\,\delta(b)$.*

Proof: Let $M = \mathcal{M}(a,\delta(b))$. One has: $\gamma = v(f(b)) = \sum_{a' \in M} v(b-a') + \sum_{a'' \notin M} v(b-a'') = m\,\delta(b) + e$, where $m = m(a,\delta(b))$ and $e = \sum_{a''\notin M} v(b-a'')$. The proof will be finished if we show $e \in G(K(a))$. For that let f' be the derivative of f and let w be the r.t. extension of v to $K(X)$ defined by the minimal pair $(a,\delta(b))$ (see Remark 1.2). According to ([1], Theorem 2.1) one has: $w(f'(X)) = v(f'(a)) \in G(K(a))$. On the other hand we can write: $f'(a) = \prod_{a' \in M\setminus\{a\}}(a-a') \cdot \prod_{a''\notin M}(a-a'')$. Now we remark that if $a'' \notin M$, then $v(b-a'') \leq \delta(b)$ and so $v(a-a'') = v(a-b+b-a'') = v(b-a'')$. Therefore we can write: $v(f'(a)) = \sum_{a'\in M\setminus\{a\}} v(a-a') + e$. The proof will be finished if we show that $\sum_{a'\in M\setminus\{a\}} v(a-a') \in G(K(a))$. For that let g be the monic minimal polynomial of a over $K(a,\delta(b))$. Over $\bar{K}$ we can write: $g(X) = \prod_{a'\in M}(X-a')$, and $g'(a) = \prod_{a'\in M\setminus\{a\}}(a-a'')$. Now since g has the coefficients in $K(a)$, we see that $v(g'(a)) = \sum_{a'\in M\setminus\{a\}} v(a-a') \in G(K(a))$, as claimed. ∎

By the last result one obtains:

Remark 1.8. The hypothesis and notations are as in Proposition 1.7. If $\delta = \delta(b) \in G(K(b))$ then m is relatively prime to q, the order of the factor group: $G(K(b))/G(K(a))$.

Proof: Let us assume $\delta \in G(K(b))$. According to ([1], Theorem 2.1) and ([6], Theorem 3.2) one has: $G(K(b)) = G(K(a)) + Z\,\gamma$. Hence $\delta = \mu + c\,\gamma$, $\mu \in G(K(a))$, $c \in \mathbb{Z}$. But according to the proof of Proposition 1.5, one has: $\gamma = m\,\delta + e$, $e \in G(K(a))$. Hence $\delta = c\,m\,\delta + \mu'$, $\mu' \in G(K(a))$, and so $(1 - c\,m)\,\delta \in G(K(a))$. Then $1 - c\,m = d\,q$, $d \in \mathbb{Z}$, i.e. m is relatively prime to q, as claimed.

By this remark there results that if m is not relatively prime to q, then we can not find $a \in K(b)$ such that (a, b) is a distinguished pair. However this is always possible if the residue field of K has zero characteristic since in this case the extension $\bar{K}/K$ is separable.

2 – Ramification conjugates of an element

1. In this section L/K will be a finite separable extension such that the residue extension $R(L)/R(K)$ is also separable. According to the classical theory of local fields (see [9], Theorems 3.2.10 and 3.4.7) the extension L/K will be refined as:

$$K \subseteq T(L) \subseteq V(L) \subseteq L$$

where $T(L)/K$ and $V(L)/K$ are respectively the maximal unramified extension and the maximal tamely ramified extension of L/K.

Let $G = \mathrm{Gal}(\bar{K}/K)$. Denote

$$\mathcal{T}(L) = \Big\{\sigma \in G /\ v(\sigma(x) - x) > 0,\ \forall\, x \in A(L)\Big\}\ .$$

Remark 2.1. $\mathcal{T}(L) = \{\sigma \in G/\ \sigma(x) = x, \forall\, x \in T(L)\}$.

Proof: Let $x \in T(L)$ be such that $A(T(L)) = A(K)[x]$, and $R(L) = R(K)[x^*]$ ([9], Theorem 3.2.6). Let $\sigma \in \mathcal{T}(L)$. Since $v(\sigma(x) - x) > 0$ then $\bar{\sigma}(x^*) = x^*$, where $\bar{\sigma}$ is the canonical image of σ in $\mathrm{Gal}(R(\bar{K})/R(K))$. Hence $\sigma(x) = x$. Conversely, let $\sigma \in G$ be trivial on $T(L)$. Let $y \in A(L)$. If $v(y) > 0$, then $v(\sigma(y) - y) \geq v(y) > 0$. If $v(y) = 0$, let $x \in T(L)$ be such that $v(y - x) > 0$. Then $v(\sigma(y) - y) = v(\sigma(y) - x + x - y) > 0$. Hence $\sigma \in \mathcal{T}(L)$, as claimed. ∎

Corollary 2.2. *The quotient set $G/\mathcal{T}(L)$ has exactly $[T(L):K]$ elements.*

The proof follows by Remark 2.1 and ([9], Proposition 3.5.1). The Corollary 2.2 is not true if $R(L)$ is not separable over $R(K)$:

Example 2.3: Let p a prime number, F_p the field with p elements, $k = F_p(X)$ and $K = k((t))$. Consider the polynomial $f(Y) = Y^p + t\,Y + X \in K[Y]$. Since $\bar{f}(Y) = Y^p + X$ is an Eisenstein polynomial, then $f(Y)$ is also irreducible. Let $a \in \bar{K}$ be such that $f(a) = 0$. $K(a)/K$ is a separable extension and it is easy to see that $\mathcal{T}(K(a)) = G$.

2. Let us denote:

$$\mathcal{V}(L) = \Big\{\sigma \in G/\ v(\sigma(x) - x) > v(x),\ \ \forall\, x \in A(L)\Big\}\ .$$

Obviously one has $\mathcal{V}(L) \subseteq \mathcal{I}(L)$.

Remark 2.4. $\mathcal{V}(L) = \{\sigma \in G/\ v(\sigma(x) - x) > v(x)$ for all $x \in L^*\}$.

Proof: If $x \in A(L)$ and $\sigma \in \mathcal{V}(L)$ then $v(\sigma(x) - x) > v(x) \geq 0$ and so $v(\frac{\sigma(x)}{x} - 1) > 0$ or equivalently $(\frac{\sigma(x)}{x})^* = 1$. Let $\sigma \in \mathcal{V}(L)$ and $x \in L^*$. Then $x = x_1/x_2$, $x_1, x_2 \in A(L)$, and $(\frac{\sigma(x_1)}{x_1})^* = (\frac{\sigma(x_2)}{x_2})^* = 1$. Hence $v(\frac{\sigma(x_1)\,x_2}{x_1\,\sigma(x_2)} - 1) > 0$ or equivalently $v(\sigma(x) - x) > v(x)$, as claimed.

Let π be an uniformising element of L/K. For any $\sigma \in \mathcal{T}(L)$, let us denote $u_\sigma = \frac{\sigma(\pi)}{\pi}$. The element u_σ^* is independent of π. Denote:

$$\psi\colon\ \mathcal{T}(L) \to R(\bar{K})\,, \qquad \psi(\sigma) = u_\sigma^*\ .$$

Remark 2.5.

a) $\psi(\sigma) = 1$ if and only if $\sigma \in \mathcal{V}(L)$.

b) If $\tau \in \mathcal{V}(L)$ and $\sigma \in \mathcal{T}(L)$, then $\psi(\sigma\,\tau) = \psi(\tau)$.

Proof: **a**) According to the proof of the Remark 2.4 one has $\psi(\sigma) = 1$ whereas $\sigma \in \mathcal{V}(L)$.

Conversely, let $\sigma \in \mathcal{T}(L)$ be such that $\psi(\sigma) = 1$. Then $\sigma \in \mathcal{V}(L)$. Indeed, one has $u_\sigma^* = (\frac{\sigma(\pi)}{\pi})^* = 1$ or equivalently $v(\sigma(\pi) - \pi) > v(\pi)$. Since π is an uniformising element of L one has $L = T(L)(\pi)$. Let $x \in L$. One has: $x = f(\pi)$, where $f \in T(L)[X]$, and $q = \deg f < [L : T(L)] = \deg_{T(L)} \pi$. Let $c_1, ..., c_q$ be all the roots of f in $\bar{K}$. We can write:

$$\frac{\sigma(x)}{x} = \frac{f(\sigma(\pi))}{f(\pi)} = \prod_{i=1}^{y}\left(1 + \frac{\sigma(\pi) - \pi}{\pi - c_i}\right)\ .$$

Since $(0,\pi)$ is a distinguished pair (with respect to the field $T(K)$) (see Remark 1.3), then $v(\pi - c_i) \leq v(\pi)$ for all $1 \leq i \leq q$. Therefore one has $(\frac{\sigma(x)}{x})^* = 1$, and so $v(\sigma(x) - x) > v(x)$. Thus $\sigma \in \mathcal{V}(L)$ (see Remark 2.4), as claimed.

b) One has: $u_{\sigma\tau} = \frac{\sigma\,\tau(\pi)}{\pi}$. Since $\tau \in \mathcal{V}(L)$ one has $v(\tau(\pi) - \pi) > v(\pi)$, and so $v(\sigma\,\tau(\pi) - \sigma(\pi)) > v(\pi)$, or equivalently $u^*_{\sigma\tau} = u^*_\sigma$. Hence $\psi(\sigma\,\tau) = \psi(\sigma)$ as claimed. ∎

For a subgroup H of G denote $\mathrm{Fix}(H) = \{x \in \bar{K} / \sigma(x) = x,\, \forall\, \sigma \subset H\}$.

Proposition 2.6. *One has* $\mathrm{Fix}(\mathcal{V}(L)) = V(L)$ *and the factor set* $\mathcal{T}(L)/\mathcal{V}(L)$ *has exactly* $d = [V(L) : T(L)]$ *elements.*

Proof: First we notice that $V(L) \subseteq \mathrm{Fix}(\mathcal{V}(L))$. Indeed, since $V(L)/T(L)$ is both totally and tamely ramified extension, according to ([9], Proposition 3.4.3) one has: $V(L) = T(L)(b)$ where $b = \sqrt[d]{x}$, and x is a suitable uniformising element of $T(L)$. Moreover for any $\sigma \in G$ one has: $v(\sigma(b) - b) = v(b)$. If $\sigma \in \mathcal{V}(L)$ then $v(\sigma(b) - b) > v(b)$ and so necessary $\sigma(b) = b$. Since $\mathcal{V}(L) \subseteq \mathcal{T}(L)$, then $V(L) \subseteq \mathrm{Fix}(\mathcal{V}(L))$, as claimed.

Now we shall prove that the quotient set $\mathcal{T}(L)/\mathcal{V}(L)$ has exactly d elements. Let π be an uniformising element of L/K and let $e = e(L/K)$. Let $x, y \in T(L)$ be such that $v(\pi)^e = v(x)$ and $v(\frac{\pi^e}{x} - y) > 0$. For any $\sigma \in \mathcal{T}(L)$ one has: $v(\frac{\sigma(\pi)^e}{x} - \frac{\pi^e}{x}) > 0$. Hence one has $v(u^e_\sigma - 1) > 0$ and so $(u^e_\sigma)^* = \psi(\sigma)^e = 1$. Since $e = dp^s$, and $(d,p) = 1$, then by $\psi(\sigma)^e = 1$ it follows $\psi(\sigma)^d = 1$. Thus according to Remark 2.5 it follows that the set $\mathcal{T}(L)/\mathcal{V}(L)$ has at most d elements. Now since $V(L)/T(L)$ is a separable extension, $\mathcal{T}(L)/\mathcal{V}(L)$ has at least d elements. Finally, this set has exactly d elements, and the equality $\mathrm{Fix}(\mathcal{V}(L)) = V(L)$ follows since L/K is a separable extension.

Corollary 2.7. *Let* π *be an uniformising element of* L/K *and let* $e = e(L/K)$. *Then* $\mathcal{V}(L) = \mathcal{H}(\pi, 1/e)$.

Proof: According to Remark 2.4 one has: $\mathcal{V}(L) \subseteq \mathcal{H}(\pi, 1/e)$, since $v(\pi) = 1/e$. The converse inclusion follows by the proof of Remark 2.5. ∎

Remark 2.8. The Corollary 2.7 give us the possibility to define the subfields of ramification of L/K. Indeed, for any $\delta \geq 1/e$ let us define $V_\delta(L) = \mathrm{Fix}(M(\pi,\delta))$. One has $V_{1/e}(L) = V(L)$. The subfields $V_\delta(L)$ are independent of the uniformising element π.

3. Let $a \in \bar{K}$ be separable over K and let $M = \{a = a_1, ..., a_n\}$, $n = \deg a$, be the set of all conjugates of a over K. For any real number δ, let us denote by $M(a, \delta) = \{a' \mid a' \in M(a) \text{ such that } v(a - a') > \delta\}$. Let us denote $m(a, \delta)$ the cardinality of $M(a, \delta)$. One has the following result:

Theorem 2.9. *Let $a \in \bar{K}$ be separable over K. Assume that $R(K(a))$ is also separable over $R(K)$. Denote by p the characteristic of $R(K)$. Then for any $\delta > \delta(a)$ one has:*

$$m(a, \delta) = \begin{cases} p^s, \quad s \geq 0 & \text{if } p > 0, \\ 1 & \text{if } p = 0 \;. \end{cases}$$

Proof: According to Proposition 2.6 it will be enough to show that $\mathcal{H}(a, \delta) \subseteq \mathcal{V}(K(a))$, or equivalently (see Remark 2.4), that for any $\sigma \in \mathcal{H}(a, \delta)$ one has: $v(\sigma(x) - x) > v(x)$ for any $x \in L^*$. This is done as in the proof of Remark 2.5 where instead of π one put a. ∎

4. For any $c \in \bar{K} \backslash K$, separable over K, let us denote:

$$\Delta(c) = \inf(v(c - c')) \,, \qquad c' \in M(c) \;.$$

Let (a, b) a distinguished pair such that a and b are separable over K. At this point we try to relate $\Delta(a)$, $\Delta(b)$, $\delta(b)$ and $\omega(b)$. Precisely one has the following result.

In what follows K is a local field of characteristic zero.

Theorem 2.10. *Let (a, b) be a distinguished pair. Assume that a, b are separable over K and that $R(K(b))/R(K)$ is a separable extension.*

Denote by p the characteristic of $R(K)$. Then:

1) $\Delta(b) \leq \delta(b) + \frac{v(n)}{n-1}$, *where $n = \deg_K b$.*

2) $\Delta(b) \geq \inf(\Delta(a), \delta(b))$. *If $\Delta(a) < \delta(b)$ then $\Delta(b) = \Delta(a)$.*

3) $\omega(b) \leq \delta(b) + \frac{v(e(K(b)/K))}{p-1}$ *if $p \neq 0$.*

$$\omega(b) = \delta(b) \quad \text{if } \; p = 0 \;.$$

Proof: **1**) Let f be the monic minimal polynomial of b over K. One has: $(n-1)\,\Delta(b) \leq v(f'(b))$. Now since $\deg f' < n$, then for any root c of f' one has: $v(b - c) \leq v(b - a) = \delta(b)$. Hence $v(f'(b)) \leq (n-1)\,\delta(b) + v(n)$, and so $\Delta(b) \leq \delta(b) + \frac{v(n)}{n-1}$, as claimed.

2) Let $b' \in M(b)$, $b' \neq b$ and let $a' \in M(a)$ be such that $v(b'-a') = \delta(b)$. Then:

$$v(b-b') = v\Big(b-a+a-a'+a'-b'\Big) \geq \inf\Big(\delta(b), v(a-a')\Big) \geq \inf\Big(\delta(b), \Delta(a)\Big) .$$

Now let us assume $\Delta(a) = v(a-a') < \delta(b)$. Let $b' \in M(b)$ be such that $v(b'-a') = \delta(b)$. Then $v(b-b') = v(b-a+a-a'+a'-b') = \Delta(a)$. Hence $\Delta(b) = \Delta(a)$, as claimed.

3) If $\omega(b) = \delta(b)$ the proof is over. Let us assume $\omega(b) > \delta(b)$ (that is happen only if $p \neq 0$). Let $b = b_1, ..., b_q$ be all elements b' of $M(b)$ such that $v(b-b') \geq \omega(b)$. It is clear that $q \geq 2$. Let us denote: $G(b, \omega(b)) = \{\sigma \in \mathrm{Gal}(\bar{K}/K),\ v(b-\sigma(b)) \geq \omega(b)\}$. Then, $G(b,\omega(b))$ is a subgroup of $\mathrm{Gal}(\bar{K}/K)$, and let $L = \mathrm{Fix}(G(b,\omega(b)))$. One has $L \subset K(b)$ and $b_1, ..., b_q$ are all the conjugates of b over L. Let $h(x) \in L(x)$ be the monic minimal polynomial of b over L. Let $c_1, ..., c_{q-1}$ be all the roots of $h'(x)$. Since $\deg c_i < \deg b$, $1 \leq i \leq q-1$, then, $v(b-c_i) \leq \delta(b)$. Hence one has:

$$v(h'(b)) = (q-1)\,\omega(b) = v\Big(q\prod_{i=1}^{q-1}(b-c_i)\Big) \leq v(q) + (q-1)\,\delta(b) ,$$

i.e.

$$\omega(b) \leq \delta(b) + \frac{v(q)}{q-1} . \tag{3}$$

Now, according to Theorem 2.9, the extension $K(b)/L$ is totally ramified, and q is of the form p^t for a suitable $t \geq 1$. Thus the above inequality implies:

$$\omega(b) \leq \delta(b) + \frac{v\Big(e(K(b))/K\Big)}{p-1}$$

as claimed.

Corollary 2.11. *Let $b \in \bar{K}$ be separable over K and such that the extension $K(b)/K$ is totally ramified and that b is an uniformising element of $K(b)$. Assume $p = \mathrm{char}(R(K)) > 0$. Then one has:*

$$\Delta(b) \geq v(b) ,$$

$$\omega(b) \leq v(b) + \frac{v\Big(e(K(b)/K)\Big)}{p-1} .$$

The proof follows since according to Proposition 1.4 $(0,b)$ is a distinguished pair and so $\delta(b)=v(b)$.

Corollary 2.12. *Denote p the characteristic of residue field of K. For any element $b\in\bar{K}$, there exists an element $c\in K$ such that:*

$$\Delta(b)\leq v(b-c)+\frac{p\,v(p)}{(p-1)^3}\qquad \textit{if}\ \ p\neq 0\ ,$$

$$\Delta(b)=v(b-c)\qquad \textit{if}\ \ p=0\ .$$

Proof: Let us assume $p\neq 0$. According to [6], there exists elements $b_0=b,b_1,...,b_s$ such that for all i, $1\leq i<s$, the pair (b_{i-1},b_i) is distinguished, and $b_s\in K$. Let us denote $n_i=\deg b_i$, and let p^{h_i} be the greatest power of p which appear in the decomposition of n_i, $0\leq i<s$.

According to 1) in Theorem 2.10 one has

$$\Delta(b)\leq\delta(b)+\frac{v(n_0)}{n_0-1}\leq\delta(b)+\frac{h_0\,v(p)}{p^{h_0}-1}\ .$$

Furthermore according to 2) in Theorem 2.10 one has: $\Delta(b)=\Delta(b_1)$, or $\Delta(b_1)\geq\delta(b)$, and so:

$$\Delta(b)\leq\Delta(b_1)+\frac{h_0\,v(p)}{p^{h_0}-1}\ .$$

By repeating these considerations for $b_1,b_2,...,b_{s-1}$, one obtains finally:

$$\Delta(b)\geq\sum\frac{h_i\,v(p)}{p^{h_i}-1}+\delta(b_{s-1})\ .$$

Now since one has

$$\sum_{t\geq 1}\frac{t}{p^t-1}<\frac{p}{(p-1)^3}$$

then 1) follows with $c=b_s$, since $v(b_{s-1}-b_s)=v(b-b_s)$.

Now let $p=0$. Let $b_1=b,...,b_n$ be all conjugates of b. Then $c=\frac{b_1+...+b_n}{n}\in K$, and $v(b-c)\geq\Delta(b)$. The equality follows since $\omega(b)=\Delta(b)$.

The Corollary 2.12 may be utilised to develop so-called Continuous Galois Theory over the local field K.

Remark 2.13. According to ($J\cdot Ax$, [Proposition 1, Corollary 2 to Lemma 6] published in Journal of Algebra, 15 (1970), 417–428) there are stronger result: for any $b\in\bar{K}$, there exists $c\in K$ such that:

i) $v(b-c) \geq \Delta(b) - \frac{p\,v(p)}{(p-1)^2}$, if $\operatorname{char} K = 0$ and $\operatorname{char} R(K) \neq 0$;

ii) $v(b-c) = \Delta(b)$ if $\operatorname{char} K = \operatorname{char} R(K)$ and K is perfect.

ACKNOWLEDGEMENT – The first author wishes to thank the University of Kuwait and the members of the Math. Dept. for their warm hospitality during a visit in May 1994. This paper was writen in part during that visit.

REFERENCES

[1] Alexandru, V., Popescu, N. and Zaharescu, A. – A theorem of characterization of residual transcendental extensions of a valuation, *J. Math. Kyoto Univ.,* 28(4) (1988), 579–592.

[2] Alexandru, V., Popescu, N. and Zaharescu, A. – Minimal pairs of a residual transcendental extension of a valuation, *J. Math. Kyoto Univ.,* 30 (1990), 207–225.

[3] Artin, E. – *Algebraic Numbers and Algebraic Functions*, Gordon and Breach, Science Publishers, N.Y., London, Paris, 1967.

[4] Borevich, Z.I. and Shafarevich, I.R. – *Number Theory* (russian), Izd. Nauka, Moscow, 1972.

[5] Popescu, L. and Popescu, N. – Sur la définition des prolongements residuels transcendante d'une valuation sur un corps K a $K(X)$, *Bull. Math. Sci. Math. de la R.S. Roumanie,* 33(81), No. 3 (1989), 257–264.

[6] Popescu, N. and Zaharescu, A. – On the structure of irreducible polynomials over local, *J. Numb. Theory,* 52(1) (1995), 98–118.

[7] Popescu, N. and Zaharescu, A. – *On the roots of a class of lifting polynomials* (to appear).

[8] Serre, J.P. – *Corps Locaux*, Hermann, Paris, 1962.

[9] Weiss, E. – *Algebraic Number Theory*, McGraw–Hill Book Company, Inc., 1963.

Nicolae Popescu,
Institute of Mathematics of the Romanian Academy,
P.O. Box 1-764, RO-70700 Bucharest – ROMANIA

and

Alexandru Zaharescu,
Institute of Mathematics of the Romanian Academy,
P.O. Box 1-764, RO-70700 Bucharest – ROMANIA