JOURNAL OF NUMBER THEORY 52, 98–118 (1995)

On the Structure of the Irreducible Polynomials over Local Fields

NICOLAE POPESCU AND ALEXANDRU ZAHARESCU

Institute of Mathematics of Romanian Academy, P.O. Box 1-764, RO-70700, Bucharest, Romania

Communicated by Alan C. Woods

Received April 22, 1990; revised June 30, 1993

The paper is concerned with the structure of irreducible polynomials in one variable over a local field (K, v). The main achievement is the definition of a system $P(f)$ of invariant factors for each monic irreducible polynomial $f \in K[X]$. It is proved that these invariants are characteristic, i.e., by using invariants we may describe the set of irreducible polynomials over a local field. © 1995 Academic Press, Inc.

An old and interesting problem is to study and determine the irreducible polynomials over a field. In this work we define some invariants associated to an irreducible polynomial over a local field and try to investigate the structure of irreducible polynomials. The main tools of this investigation are the results proved in [1, 2, 7] on the residual transcendental extension of a valuation v on a field K to the field $K(X)$, where X is an indeterminate over K.

We hope that the results of this work will be used in the study of the finite extensions of local fields.

Now we present briefly the content of the work.

In the first section there are given the definitions and the fundamental results used in the sequel. Particularly, here is defined the notion of the so-called "lifting polynomial" relative to a r.t. extension. In the second section it is proved that every lifting of an irreducible polynomial is also irreducible (Theorem 2.1). Consequently we reobtain some known criteria of irreducibility and also give new criteria. In Theorem 2.3 it is proved that in some cases every finite extension of a local field is given by an irreducible lifting polynomial.

In Section 3 we define and study the so-called "distinguished pairs." The results of this section will be used in the last section. This last section is the main part of the work. Here is defined the notion of "distinguished chain"

0022-314X/95 $6.00

relative to an irreducible polynomial, and there is emphasis on a sequence of invariants of an irreducible polynomial. It is proved that these invariants are characteristic, i.e., by using invariants, we may describe the set of irreducible polynomials over a local field (Theorem 4.6). As an application it is proved that the invariants of an irreducible polynomial may be used to understand sufficiently well the extension of the natural valuation of a local field K to the field given by the considered polynomial.

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([3, 4, 5, 8]). Let $\bar{K}$ be a fixed algebraic closure of K and denote also by v the unique extension of v to $\bar{K}$. If $K \subseteq L \subseteq \bar{K}$ is an intermediate field, denote: $G(L) = \{v(x);\ x \in L\}$. As usually $G(K)$ will be identified to the ordered group Z of rational integers and for every L, $G(L)$ will be viewed as a subgroup of the additive group Q.

Denote $A(L) = \{x \in L;\ v(x) \geqslant 0\}$ the ring of integers of L. Let $M(L) = \{x \in L;\ v(x) > 0\}$ and let π_L be a *uniformising* element of L. Particularly denote $\pi_K = \pi$. Let $R(L) = A(L)/M(L)$ the *residue field* of L. If $x \in A(L)$ denote by x^* the canonical image of x into $R(L)$. As usually $R(L)$ will be viewed canonically as a subfield of $R(\bar{K})$. Moreover $R(\bar{K})$ is an algebraic clossure of $R(K)$.

Let $K \subseteq L_1 \subseteq L_2 \subseteq \bar{K}$ be intermediate fields such that L_2/K is a finite extension. Then $R(L_2)/R(L_1)$ is a finite extension and the number $f(L_2/L_1) = [R(L_2):R(L_1)]$ will be called the *inertial degree* of L_2 relative to L_1. The quotient group $G(L_2)/G(L_1)$ is finite and its index will be denoted by $e(L_2/L_1)$ and will be called the *ramification index* of L_2 relative to L_1. It is well known (see [3, Ch. IV]) that $f(L_2/L_1)\, e(L_2/L_1) = [L_2:L_1]$.

If $K \subseteq L \subseteq \bar{K}$ and $a \in \bar{K}$, then the *degree* $[L(a):L]$ of a *relative to* L will be denoted by $\deg_L a$ (or simply by deg a when $L = K$).

If $f \in A(K)[X]$, $f = a_0 X^n + a_1 X^{n-1} + \cdots + a_n$ we denote

$$\bar{f} = a_0^* X^n + a_1^* X^{n-1} + \cdots + a_n^* \in R(K)[X]$$

and we say that $\bar{f}$ is the *residue polynomial* in $R(K)[X]$ of the polynomial f.

2. If $a \in \bar{K}$ and $\delta \in Q$, we may define, for any $F \in \bar{K}[X]$,

$$F(x) = c_0 + c_1(x-a) + \cdots + c_n(x-a)^n,$$

$$w(F) = \inf_{0 \leqslant i \leqslant n} \{v(c_i) + i\delta\}.$$

In this manner we obtain a valuation of $\bar{K}[X]$ (and canonically on $\bar{K}(X)$) which is a residual transcendental (r.t.) extension of $(\bar{K}, v)$ (i.e., the residual field of w is transcendental over $R(\bar{K})$) and it is called "the r.t. extension of $(\bar{K}, v)$ defined by inf, a and δ.

An element $(a, \delta) \in \bar{K} \times Q$ will be called *minimal* with respect to K if for every $b \in \bar{K}$ the condition $v(a-b) \geqslant \delta$ implies $[K(a):K] \leqslant [K(b):K]$.

The word "minimal" was suggested by the fact that this definition is equivalent to the following: (a, δ) is minimal if there is no pair (a', δ) with $\deg a' < \deg a$ such that both pairs define the same r.t. extension w on $\bar{K}(X)$.

If $a \in \bar{K} \backslash K$, denote $\omega(a) = \sup\{v(a-a')\}$ where a' runs over all conjugates of a over K, and $a' \neq a$. By Krasner's Lemma (see [2, p. 66]) it follows that

Remark 1.1. Let a be separable over K. If $\delta > \omega(a)$ then (a, δ) is a minimal pair.

Let (a, δ) be a minimal pair and let f be the monic minimal polynomial of a over K. Let $a = a_1, a_2, \ldots, a_n$ be all the roots of f and let us put:

$$\gamma = \sum_{i=1}^{n} \inf(v(a-a_i), \delta).$$

If $F \in K[X]$, we decompose F after the powers of f:

$$F = F_0 + F_1 f + \cdots + F_t f^t, \qquad \deg F_i < \deg f,\ i = 0, \ldots, t.$$

Then we define:

$$w(F) = \inf_{0 \leqslant i \leqslant t} (v(F_i(a)) + i\gamma) \tag{1}$$

In [1] (see also [7]) it is proved the following result:

THEOREM 1.2. *Let (a, γ) be a minimal pair with respect to K. Then the assignment* (1) *defines a valuation on $K[X]$ (and canonically on $K(X)$) which is the restriction of the valuation w defined on $\bar{K}(X)$ by* inf, a *and* δ. *Moreover one has:*

(a) *The value group of w is canonically isomorphic to $G(K(a)) + Z\gamma$.*

(b) *Let e be the smallest non-zero positive integer such that $e\gamma \in G(K(a))$. Let $h \in K[X]$, $\deg h < \deg f$ such that $w(h(X)) = v(h(a)) = e\gamma$. Then $r = f^e/h$ is an element of $K(X)$ such that $w(r) = 0$, the image r^* of r in the residue field of w (denoted k_w), is transcendental over $R(K)$ and one has*

$$k_w \simeq R(K(a))(r^*).$$

Here the isomorphism is canonic: for any $F \in K[X]$ *with* $\deg F < \deg a$ *we have* $w(F) = w(F(a))$, $(F/F(a))^* = 1$ *and the above isomorphism becomes an equality in the residue field of* w.

Moreover if w' *is an* r.t. *extension of* v *to* $K(X)$, *then there exists a pair* (a, δ) *minimal with respect to* K *such that* w' *coincides to the* r.t.-*extension defined by the minmal pair* (a, δ).

3. In what follows we shall consider a minimal pair $(a, \delta) \in \bar{K} \times Q$ and denote by w the r.t. extension of v to $K(X)$. Also we shall preserve all notations stated above. We shall identify the residue field $k_w = R(K(a))(r^*)$ of w to the field $R(K(a))(Y)$, where Y is an indeterminate over $R(K(a))$ (i.e., we shall write $r^* = Y$).

Let $G \in R(K(a))[Y]$ monic and let $m = \deg G$. Let $g \in K[X]$ monic. We shall say that g is a *lifting* of G *relative* to w (or more precisely *relative to* (a, δ, h) if and only if:

(1) $\deg g = em(\deg f)$

(2) $w(g) = mw(h) = me\gamma$ and $(g/h^m)^* = G$.

Remark 1.3. Any $G \in R(K(a))[Y]$, monic, has liftings in $K[X]$.

Proof. If $G = Y^m + c_1 Y^{m-1} + \cdots + c_m$ and $A_i \in K[X]$, $i = 1, 2, \ldots, m$, are such that $\deg A_i < \deg f$, $v(A_i(a)) \geqslant 0$ and $(A_i(a))^* = c_i$, then $g = f^{em} + A_1 h f^{e(m-1)} + \cdots + A_m h^m$ is a lifting of G (for (1) observe that $\deg A_i + \deg h < (\deg f) \cdot \inf(e(K(a)/K), 2) \leqslant \deg f^e$).

We say that the lifting G of g is *trivial* if $\deg g = \deg f$. This situation appear if and only if $\deg G = 1$ and $\gamma = w(f) \in G(K)(a)$. The motivation of this definition will appear later.

2. Irreducibility of the Liftings of Irreducible Polynomials

1. Theorem 2.1. *Let* $G \neq Y$ *be a monic irreducible polynomial of* $R(K(a))[Y]$. *Then any lifting* g *of* G *is an irreducible polynomial of* $K[X]$.

Proof. Let $m = \deg G$ and let us assume that g is not irreducible. Then we may write

$$g = pq,$$

where p, q are both non-constant polynomials of $K[X]$. Now let

$$p = p_0 + p_1 f + \cdots + p_t f^t + \cdots, \qquad \deg p_i < \deg f, \quad i = 0, \ldots, t, \ldots$$

$$q = q_0 + q_1 f + \cdots + q_u f^u + \cdots, \qquad \deg q_j < \deg f, \quad j = 0, \ldots, u, \ldots$$

be the corresponding f-expansion of p and q. Denote by t, respectively by u the smallest positive integer such that

$$w(p) = \inf_i (v(p_i(a)) + i\gamma) = v(p_t(a)) + t\gamma$$

$$w(q) = \inf_i (v(q_i(a)) + i\gamma) = v(q_u(a)) + u\gamma$$

We have

$$w(g) = me\gamma = w(p) + w(q) = v(p_t(a)) + v(q_u(a)) + (t+u)\gamma.$$

Since $w(g) \in G(K(a))$, it follows that $t+u$ is divisible by e. Let

$$t = t_1 e + t_0 \qquad 0 \leqslant t_0 < e$$

$$u = u_1 e + u_0 \qquad 0 \leqslant u_0 < e$$

Then $t_0 + u_0 = ec$, where $c = 0$ or 1. We may write

$$\frac{f^{ec}g}{h^{m+c}} = \left(\frac{pf^{u_0}}{p_t h^{m_1}}\right) \cdot \left(\frac{qf^{t_0}p_t}{h^{m+c-m_1}}\right), \tag{2}$$

where m_1 is choosed such that the first factor of the right side (and thus the second too) has valuation zero. From (2) we obtain in $R(K(a))[Y]$ an equality of the form:

$$Y^c G = HQ. \tag{3}$$

If $t_0 > 0$ then $u_0 > 0$ and these would imply that H and Q have no constant term, which is false since $c \leqslant 1$ and $G \neq Y$. Therefore we must have $t_0 = u_0 = 0$. Then (3) together with the irreducibility of G implies that, say, Q is constant. To finish the proof it is now sufficient to note that $\deg p \leqslant \deg g = e \deg G = e \deg H \leqslant \deg p$. Hence q is constant; and so g is irreducible as claimed.

2. At this point we shall derive some consequences of Theorem 2.1. These may be considered as criteria of irreducibility.

PROPOSITION 2.2. *Let*

$$g = X^m + a_1 X^{m-1} + \cdots + a_{m-1} X + a_m$$

be a polynomial of $K[X]$. *Assume that* $v(a_m) = s$ *is a positive integer relatively prime to* m. *Then* g *is an irreducible polynomial if and only if* $v(a_i) > is/m$, $1 \leqslant i \leqslant m-1$.

Proof. The necessity of these conditions follows from the relations between the roots and coefficients of g and the fact that all the roots of g have the same valuation s/m (note that the inequalities are strictly since $v(a_i) \in Z \not\ni is/m$. For the sufficience, observe firstly that the pair $(0, s/m) \in K \times Q$ is minimal with respect to K. Let w be the r.t. extension defined by this pair. The element r of Theorem 1.2 is $r = X^m/\pi^s$ (i.e., we may take $h = \pi^s$). If $G = Y + (a_m/\pi^s)^* \in R(K)[Y]$, then g is a lifting of G and so is irreducible.

A special case ($s = 1$) of Proposition 2.2 is the well known Eisenstein criteria of irreducibility.

3. The monic polynomial $f \in A(K)[X]$ is called *unramified* if $\bar{f}$, the residue of f in $R(K)[X]$, is irreducible and separable. Let $a_1, \ldots, a_n$ be the roots of f in $\bar{K}$. It is clear that for any root a of f one has $v(a) = 0$, and so for any positive rational number s/e, $(e, s) = 1$, the pair $(a, s/e) \in \bar{K} \times Q$ is a minimal one. The extension $K(a)/K$ is separable and π is also an uniformising element of $K(a)$. A polynomial of the form

$$h = f^e + a_1 f^{e-1} + \cdots + a_e,$$

where $a_i \in A(K)[X]$, $\deg a_i < \deg f$, $\overline{a_i} = 0$, $1 \leqslant i \leqslant e$, and $(a_e/\pi)^* \neq 0$ will be called an *f-Eisenstein polynomial.* If $f = X$ we obtain the classical Eisenstein polynomials. Other special cases are described in [7] (Theorem 1). Every f-Eisenstein polynomial is lifting of a polynomial like $G = Y + c$, $c \neq 0$ of $R(K)[Y]$ relative to the valuation w of $K(X)$ defined by the minimal pair $(a, 1/e)$, and so by Theorem 2.1 is irreducible.

The following result shows that f-Eisenstein polynomials define almost all finite extensions of K.

THEOREM 2.3. *Let $K \subseteq L \subset \bar{K}$ be such that L/K is a finite extension and $R(L)/R(K)$ is separable. Then there exists an unramified polynomial f, an f-Eisenstein polynomial g and root b of g such that $L = K(b)$.*

Proof. According to [8, p. 66] there exists an element $b \in L$ such that $A(L) = A(K)[b]$ and that an uniformising element of L is of the form $q(b)$ where $q \in A(K)[X]$ is monic and $\deg q = f(L/K)$. Let g be the minimal monic polynomial of b over K. We shall prove that g is an f-Eisenstein polynomial, where f is an unramified polynomial of $K[X]$.

First we observe that $R(L) = R(K)[b^*]$. Let $t(X)$ be the minimal polynomial of b^* over $R(K)$ and let $f \in A(K)[X]$ be monic and such that $\bar{f} = t$. Since g is irreducible, it follows (by Hensel's Lemma) that $\bar{g}$ is a power of the irreducible polynomial $\bar{f}$. Hence one has

$$g = f^e + \pi g_1, \; g_1 \in A(K)[X], \qquad \deg g_1 < \deg g.$$

Let us write $g_1 = a'_1 f^{e-1} + \cdots + a'_e$ where $a'_i \in A(K)$, $\deg a'_i < \deg f$, $1 \leqslant i \leqslant e$, and:

$$g = f^e + a_1 f^{e-1} + \cdots + a_e, a_i = \pi a'_i, \qquad 1 \leqslant i \leqslant e$$

Since f is an unramified polynomial we see by the last equality that g is an f-Eisenstein polynomial as claimed.

3. Distinguished Pairs

1. Actually we know that a lifting g of an irreducible monic polynomial $G(Y) \neq Y$ is irreducible. This gives us the possibility of constructing an irreducible polynomial g starting from a known quadruple (f, γ, h, G). We ask now about the converse: Is any irreducible monic polynomial g of $K[X]$ a lifting of an irreducible polynomial $G(Y) \neq Y$ with respect to a certain r.t. extension w of v to $K(X)$?

It is easy to prove that the answer is yes.

For, let g be irreducible and a a root of g. Let $c \in K$ be such that $v(c)$ is enough large. Let $f = g - c$ and let a_1 be a root of f for which $\delta = v(a - a_1)$ is greatest. Then $K(a) = K(a_1)$, and (a_1, δ) is a minimal pair. If w is the r.t. extension defined by this minimal pair, then in Theorem 1.2 one has: $\gamma = \sum \inf(v(a_1 - a'), \delta) = v(f(a)) = v(c) \in G(K)$ (here a' runs over all the roots of f) and so $r = f/c$. It is easy to see that g is a lifting of $G = Y + 1$ with respect to w.

This answer to the above question is not useful in our work to describe the set of all irreducible polynomials over K, because of the triviality (in the sens of our definition) of the lifting which was constructed. The reason for working only with non-trivial liftings lies in the fact that to know the g's rests in the known of the quadruples (f, γ, h, G). If we suppose that the irreducible polynomials over the finite extensions of $R(K)$ (i.e. the G's) are "known" and if we ignore for the moment the trubles created by γ and h, then we may start an inductive process to construct the irreducible polynomials over K from those of *smaller* degree.

So we ask now: is any irreducible polynomial g a nontrivial complete lifting?

We shall prove that the answer is yes.

2. At this point we shall define the notion of "distinguished pair" which will be the main tool in the study of the above problem. A pair (a, b) of elements from $\bar{K}$ is said to be "*distinguished*" if the following conditions hold.

(1°) $\deg a > \deg b$.

(2°) If $c \in \bar{K}$ and $\deg c < \deg a$ then $v(a-c) \leqslant v(a-b)$.

(3°) If $c \in \bar{K}$ and $\deg c < \deg b$ then $v(a-c) < v(a-b)$.

In other words, (a, b) is distinguished if b is an element of $\bar{K}$ of minimal degree for which $v(a-b) = \sup\{v(a-c)),\ c \in \bar{K},\ \deg c < \deg a\}$.

If (a, b) is distinguished, then $a \in \bar{K}$. Conversely, if $a \in \bar{K}$ then there exists (infinitely many) elements $b \in \bar{K}$ for which (a, b) is distinguished (for this, observe that the set $\{v(a-c);\ \deg c < \deg a\}$ has a greatest element, since it is bounded, e.g., by $\omega(a)$). Moreover the number $\deg b$ is an invariant of a; it is a divisor of $\deg a$ (as we shall prove latter) which will be termed as "*an invariant factor for a.*"

Since the valuation v is Henselian, for every $\tau \in \mathrm{Gal}(\bar{K}/K)$ one has (a, b) is distinguished if and only if $(\tau(a), \tau(b))$ is distinguished.

As a consequence $\deg b$ is in fact an invariant of the minimal polynomial f of a over K.

Given two irreducible monic polynomials over K, f and g we shall say that (g, f) is a *distinguished pair*, if there exists a root a of g and a root b of f such that (a, b) is a "distinguished pair." It is clear that in this definition we may replace the expression "there exists a $\cdots$ and b" with any of the two expressions; "for any a $\cdots$ there exists b"; "for any b $\cdots$ there exists a".

We proceed now to show that the lifting polynomials are closely related to the distinguished pairs.

3. THEOREM 3.1. *The notations and hypotheses are as in Theorem* 1.2. *As usual denote* $r^* = Y$ *and* G *be an irreducible polynomial of* $R(K(a))[Y]$, $G \neq Y$. *If* g *is a nontrivial lifting of* G *into* $K[X]$ *then* (g, f) *is an distinguished pair.*

THEOREM 3.2. *Let* (g, f) *be a distinguished pair and* a *a root of* f. *Then there exists,* γ, h *as in Theorem* 1.2 *and* $G \in R(K(a))[Y]$, *irreducible,* $G \neq Y$, *such that* g *is a (nontrivial) lifting of* G.

Proof of Theorem 3.1. Let θ be a root of g such that $v(\theta - a)$ is greatest. We shall prove that (θ, a) is a distinguished pair.

The condition (1°) is fulfilled, since the lifting is nontrivial.

Now let w be the valuation on $\bar{K}(X)$ defined by inf, a and δ. Since, for $m = \deg G$ one has $(g/h^m)^* = G$, then by ([2]), Proposition 1.1) there exists a root θ' of gh such that $v(\theta' - a) \geqslant \delta$. Furthermore, since $\deg h < \deg f$ and since (a, δ) is a minimal pair it follows that θ' is necessarily a root of g.

Therefore by the choice of θ one has $v(\theta - a) \geqslant \delta$. Now we shall prove that in fact one has:

$$v(\theta - a) = \delta. \tag{4}$$

For, if not, then one has

$$w(g) = \sum_i w(X - \theta_i) = \sum \inf(\delta, v(a - \theta_i)) < v(g(a))$$

where $emn = \deg g$ and θ_i, $1 \leqslant i \leqslant emn$ are all the roots of g in $\bar{K}$. Let

$$g = f^{em} + A_1 f^{em-1} + \cdots + A_{em}, \qquad \deg A_i < \deg f, \quad 1 \leqslant i \leqslant em \tag{5}$$

The previous inequality shows that $w(A_{em}) = v(A_{em}(a)) = v(g(a)) > w(g)$. But this implies that $G = (g/h^m)^* = Y^m + (A_1/h)^* Y^{m-1} + \cdots + (A_{(m-1)e}/h^{m-1})^* Y$, which is false since G is irreducible and $G \neq Y$.

In proving (2°) let us suppose that there exists $c \in \bar{K}$, $v(\theta - c) > \delta = v(\theta - a)$. Then denoting by $a = a_1, \ldots, a_n$ the roots of f, one has

$$\left(\frac{f(c)}{f(\theta)}\right)^* = \left(1 + \frac{c - \theta}{\theta - a_1}\right)^* \cdots = 1. \tag{6}$$

In the same manner, we obtain for any polynomial $F \in K[X]$, whose degree is $< n$, that one has: $v(F(c)) = v(F(\theta)) = v(F(a)) = w(F)$, and

$$\left(\frac{F(c)}{F(\theta)}\right)^* = \left(\frac{F(a)}{F}\right)^* = 1. \tag{7}$$

This shows that in $G(\bar{K})$ and respectively in $R(\bar{K})$ one has

$$G(K(a)) \subseteq G(K(c)) \qquad \text{and} \qquad R(K(a)) \subseteq R(K(c)). \tag{8}$$

Moreover from our choice of θ it follows easily that $v(\theta - a_i) = \inf(v(\theta - a), v(a - a_i))$, $1 \leqslant i \leqslant n$. Then (4) and (6) implies

$$\gamma = w(f) = v(f(\theta)) = v(f(c)) \in G(K(c)). \tag{9}$$

By (8) and (9) we derive that

$$e(K(a)/K) \cdot e \text{ divides } e(K(c)/K). \tag{10}$$

Furthermore by (6) and (7) it follows

$$(r(\theta))^* = (r(c))^*. \tag{11}$$

Now we return to the decomposition (5). By (6), (7), (11) and the condition $g(\theta) = 0$ there results easily $G(r(c)^*) = G(r(\theta)^*) = 0$. Since G is an

irreducible polynomial it follows that $f(K(c)/K(a)) \geqslant m$. By this inequality and (10) it follows:

$$\deg c = f(K(c)/K)\, e(K(c)/K) \geqslant m \cdot f(K(a)/K) \cdot e(K(a)/K) \cdot e = \deg g$$

which proves (2°). Finally, (3°) follows from (4) since (a, δ) is a minimal pair. The proof of Theorem 3.1. is complete.

Proof of Theorem 3.2. Let θ be a root of g for which $v(\theta - a)$ is greatest. Then (θ, a) is a distinguished pair. Let $\delta = v(\theta - a)$. From (3°) it follows that (a, δ) is a minimal pair.

Let w be the valuation on $K(X)$ defined by $w = w|_{K(X)}$ and γ, e, h and r as in Theorem 1.2. We shall prove that there exists $G \in R(K(a))[Y]$, monic, irreducible and $G \neq Y$ such that g is a complete lifting of G with respect to (a, δ, h). The nontriviality of this lifting will follow from (1°).

For the moment we note that (3°) implies

$$w(F) = v(F(a)) = v(F(\theta)) \qquad \text{and} \qquad \left(\frac{F(a)}{F(\theta)}\right)^* = \left(\frac{F(a)}{F}\right)^* = 1$$

for any $F \in K[X]$ with $\deg F < \deg a$. We have thus the inclusions:

$$G(K(a)) \subseteq G(K(\theta)); \qquad R(K(a)) \subseteq R(K(\theta)).$$

Since $v(f(\theta)) = w(f) = \gamma$, we see that $e(K(a)/K) \cdot e$ divides $e(K(\theta)/K)$. Also $f(K(a)/K)$ divides $f(K(\theta)/K)$. As a consequence $m = \deg g/(e \deg f)$ is an integer and we may write:

$$g = f^{em} + a_1 f^{em-1} + \cdots + A_{em}, \qquad \text{where} \quad \deg A_i < \deg f = n$$

Let $\theta_1 = \theta, \ldots, \theta_{em}$ be the roots of g. One has $w(X - \theta_i) = \inf(\delta, v(a - \theta_i)) = v(a - \theta_i)$ and so:

$$w(g) = v(g(a)) = v(A_{em}(a)) = w(A_{em}) \tag{12}$$

Using now the formula (which is valid for any two irreducible monic polynomials over a Henselian field and any two roots of them)

$$\frac{v(g(a))}{\deg g} = \frac{v(R(g, f))}{\deg g \cdot \deg f} = \frac{v(f(\theta))}{\deg f}$$

(where $R(g, f)$ is the resultant of g and f). We obtain

$$w(g) = v(g(a)) = em\gamma = w(h^m) \tag{13}$$

Hence $w(A_i f^{em-i}) \geqslant em\gamma$ for any i (the equality being possible only for i multiple of e; and we may write

$$(g/h^m)^* = (r^*)^m + \left(\frac{A_e}{h}\right)^* (r^*)^{m-1} + \cdots + \left(\frac{A_{em}}{h^m}\right)^* \tag{14}$$

By (12), (13) and (14) there results that g is a lifting of $G = Y^m + (A_{e/h})^* Y^{m-1} + \cdots + \cdots + (A_{em/h^m})^* \in R(K(a))[Y]$. It remains to be shown that G is irreducible (the condition $G \neq Y$ follows from (12)). For this it is enough to prove that

(A) $[R(K(\theta)) : R(K(a))] = m$

(B) $v(r(\theta)) = 0$ and $(r(\theta))^*$ is a root of G.

(C) $R(K(\theta))$ is generated over $R(K(a))$ by $(r(\theta))^*$.

Since $e(K(\theta)/K)\, f(K(\theta)/K) = \deg g = em \deg f = emf(K(A)/K)\, e(K(a)/K)$, (A) will be proved if we show that $G(K(\theta))$ is generated by $G(K(a))$ and γ.

Now if $\gamma_1 \in G(K(\theta))$, let $g_1 \in K[X]$ be such that $\deg g_1 < \deg g$ and $v(g_1(\theta)) = \gamma_1$. If $c_1, c_2, \ldots$ are the roots of g_1 then (2°) implies that $v(\theta - c_i) = \inf(v(\theta - a), v(a - c_i)) = w(X - c_i)$ hence $\gamma_1 = \sum_i v(\theta - c_i) = \sum_i w(X - c_i) = w(g_1)$, and this proves (A) since $G(K(X))$ is generated by $G(K(a))$ and γ.

From $v(f(\theta)) = \gamma$ and $v(h(\theta)) = w(h(X))$ it follows that $v(r(\theta)) = 0$. Moreover, one has

$$\left(\frac{A_{ie}}{h^i}\right)^* = \left(\frac{A_{ie}(a)}{h^i(a)}\right)^* = \left(\frac{A_{ie}(\theta)}{h^i(\theta)}\right)^*, \qquad i = 1, \ldots, m$$

By these equalities and the relations $g(\theta) = 0$ we obtain $G(r(\theta)^*) = 0$ which proves (B).

As for (C), let $\mu \in R(K(\theta))$ and let $F \in K[X]$, such that $\deg F < \deg g$, $v(F(\theta)) = 0$, and $(F(\theta))^* = \mu$. Let us write

$$F = C_0 + C_1 f + \cdots + C_s f^s, \qquad \text{where} \quad \deg C_i < \deg f.$$

Then as in (A), $w(F) = v(F(\theta)) = 0$, hence $w(C_i f^i) \geqslant 0$ for $0 \leqslant i \leqslant s$.

Moreover since $w(C_i) = w(C_i(\theta))$ and $w(f) = \gamma = v(f(\theta))$, it follows that all the terms in the right side of the equality

$$F(\theta) = C_0(\theta) + C_1(\theta) f(\theta) + \cdots + C_s(\theta) f^s(\theta)$$

has an image in $R(K(\theta))$ and so

$$\mu = (F(\theta))^* = \sum (C_i(\theta) f^i(\theta))^* \tag{15}$$

Now, if e/i, then $w(C_i f^i) \neq 0$, hence (15) become

$$\mu = \sum_{1 \leqslant ej \leqslant s} (C_{ej}(\theta) f^{ej}(\theta))^* = \sum (C_{ej}(\theta) h^j(\theta))^* (r(\theta))^{*j} \in R(K(a))[(r(\theta))^*]$$

which proves (C). The proof of Theorem 3.2 is now complete.

4. We end this section with a consequence of the proof of Theorem 3.2.

Remark 3.3. (Fundamental principle). Let a, $\theta \in \bar{K}$ be such that $v(\theta - a) > v(a - b)$ for any $b \in \bar{K}$ with $\deg b < \deg a$. Then one has the natural inclusions: $G(K(a)) \subseteq G(K(\theta))$ and $R(K(a)) \subseteq R(K(\theta))$. Moreover one has

$$e(K(a/K)/e(K(\theta)/K)$$

$$f(K(a)/K)/f(K(\theta)/K)$$

$$\deg a/\deg \theta$$

The proof follows as in the proof of Theorem 3.2, by showing that $v(F(a)) = v(F(\theta))$ and $(F(a)/F(\theta))^* = 1$ for any $F \in K[X]$ with $\deg F < \deg a$.

Finally we remark that this principle is in consense with Krasner's principle ([3, p. 66]); it has weaker hypothesis and conclusions.

4. Invariant Factors for an Irreducible Polynomial

1. Let $a \in \bar{K}$. If $a_0, \ldots, a_s \in \bar{K}$ we say that $(a_0, \ldots, a_s)$ is a *distinguished chain for* a if $a_0 = a$ and (a_{i-1}, a_i) is a distinguished pair for any i, $1 \leqslant i \leqslant s$. The integer s will be called the length of the chain $(a_0, a_1, \ldots, a_s)$.

We say that the distinguished chain $(a_0, \ldots, a_s)$ for a is *saturated* if there is no distinguished chain $(b_0, \ldots, b_r)$ for a such that $(a_0, \ldots, a_s) \subseteq (b_0, \ldots, b_r)$. From 3.2. $(a_0, \ldots, a_s)$ is saturated if and only if $a_s \in K$.

Let $f = f_0, \ldots, f_s$ be irreducible monic polynomials over K. We say that $(f_0, \ldots, f_s)$ is a (*saturated*) *distinguished chain* for f if there exist roots $a = a_0, \ldots, a_s$ of $f = f_0, \ldots, f_s$ respectively such that $(a_0, \ldots, a_s)$ is a (saturated) distinguished chain for a. (In the following, we shall use the abreviations "s.d.c. for a" and "s.d.c. for f").

We summarise the properties of these chains in the following three propositions:

Proposition 4.1. *If $(a_0, \ldots, a_s)$ is a distinguished chain then*

(1) $G(K(a_0)) \supseteq G(K(a_1)) \supseteq \cdots \supseteq G(K(a_s))$

(2) $R(K(a_0)) \supseteq R(K(a_1)) \supseteq \cdots \supseteq R(K(a_s))$.

Moreover, if for any i, $1 \leqslant i \leqslant s$, f_i is the monic minimal polynomial of a_i, $\gamma_i = v(f_i(a_{i-1}))$, $e_i = e(K(a_i), \gamma_i)$ (i.e., the smallest rational positive integer such that $e_i\gamma_i \in G(K(a_i)))$, $h_i \in K[X]$, $\deg h_i < \deg f_i$, $v(h_i(a_i)) = e_i\gamma_i$ then the quotient group $G(K(a_{i-1}))/G(K(a_i))$ is ciclic of order e_i, generated by the image of γ_i and $R(K(a_{i-1}))$ is generated over $R(K(a_i))$ by $(f_i(a_{i-1})^{e_i}/h_i(a_i))^*$.

The proof follows from the proof of Theorem 3.2 in a canonical way.

PROPOSITION 4.2. *Let* $(a_0, ..., a_s)$ *and* $(b_0, ..., b_r)$ *be two* s.d.c. *for* a. *Then* $s = r$. *Moreover if* $c_i \in \{a_i, b_i\}$, $1 \leqslant i \leqslant s$ *then* $(c_0, ..., c_s)$ *is also a* s.d.c. *for* a.

Proof. Let $n = \deg a$. For any i, $1 \leqslant i \leqslant n-1$, let us denote $t_i(a) = \sup\{v(\alpha - a),\ \alpha \in \bar{K},\ \deg \alpha \leqslant i\}$. Then one has: $t_1(a) \leqslant \cdots \leqslant t_{n-1}(a)$. We consider the set: $S(a) = \{i;\ t_i \neq t_{i-1}\}$ (by convention $1 \in S(a)$) and we put it in the form: $S(a) = \{n_1, n_2, ..., n_k\}$, where $n_1 > n_2 > \cdots > n_k = 1$ depends only on a and K.

The pair (a, a_1) being distinguished, we get

$$v(a - a_1) = t_{n_1}(a) \qquad \text{and} \qquad \deg a_1 = n_1$$

Also, we have $v(\alpha - a) = v(\alpha - a_1)$ for $\deg \alpha < n_1$, hence $t_i(a) = t_i(a_1)$, for $i < n_1$, and we derive that

$$S(a) = S(a_1) \cup \{\deg a_1\}$$

Since $(a_1, a_2, ..., a_s)$ is a s.d.c. for a_1, we may continue the preceding argument to obtain for any i: $v(a - a_i) = t_{n_i}(a)$ and $\deg a_i = n_i$. Thus

$$S(a) = \{\deg a_1, \deg a_2, ..., \deg a_s\}$$

which implies $s = r$. Since $\inf\{v(b_{i-1} - a_i),\ v(a_{i-1} - b_i)\} \geqslant t_{n_i}(a) = t_{(n_{i-1}-1)}(a_{i-1}) = t_{(n_{i-1}-1)}(b_{n-1})$ it follows that (b_{i-1}, a_i) and (a_{i-1}, b_i) are distinguished pairs and this proves the second part of Proposition 4.2.

PROPOSITION 4.3. *Let* $a \in \bar{K}$, *let* $(a_0, ..., a_s)$ *and* $(b_0, .., b_s)$ *be two* s.d.c. *for* a, *and let* f_i, g_j *be the minimal polynomials of* a_i *and* b_j *respectively. Then for any* i, $1 \leqslant i \leqslant s$ *one has*

(1) $v(a_{i-1} - a_i) = v(b_{i-1} - b_i)$

(2) $v(f_i(a_{i-1})) = v(g_i(b_{i-1}))$

(3) $G(K(a_i)) = G(K(b_i))$

(4) $R(K(a_i) = R(K(b_i))$.

Moreover if we change the condition $b_0 = a$ *in the hypothesis with the condition* $b_0 = \tau(a)$ *where* $\tau \in \mathrm{Gal}(\bar{K}/K)$ *then all the conclusions remain valid with the only exception that in* (4) *instead of equality we have a canonically* $R(K)$*-isomorphism.*

Proof. Since $(\tau^{-1}(b_0), ..., \tau^{-1}(b_r))$ is a s.d.c. for $\tau^{-1}(b)$ it is clear that we may restrict to the case $b_0 = a$.

(1) is obvious: $v(a_{i-1} - a_i) = v(a - a_i) = t_{n_i}(a) = v(b_{i-1} - b_i)$.

To prove (2) let $\delta_i = t_{n_i}(a)$ and observe that

$$v(f_i(a_{i-1})) = v(f_i(a)) = \frac{\deg f_i}{\deg f_0} v(f_0(a_i)) = \frac{n_i}{n} \sum_{a''} \inf(\delta_i, v(a - a''))$$

which depends only on a and i.

(3) follows by induction on i (starting from $i = s$, where $K(a_s) = K(b_s) = K$ and continuing in decreasing order) using (2) and Proposition 4.1.

In order to prove (4) we consider for a fixed i the valuation w_i on $K(X)$ defined by the pair (a_i, δ_i). The restriction of w_i to $K(X)$ is an r.t. extension of v to $K(X)$, and it is easy to see that both (a_i, δ_i) and (b_i, δ_i) are minimal pairs which define w_i. By Theorem 1.2, one has $R(K(a_i)) = R(K(b_i))$ (the algebraic closure of $R(K)$ into k_{w_i}). The proof of Proposition 4.3 is finished.

The number s stated in Proposition 4.3. will be called the *length* of $f = f_0$ and will be denoted by $l(f)$. The integers $\deg a_i$, $e(K(a_i)/K)$ and $f(K(a_i)/K)$ for $0 \leqslant i \leqslant s$, will be called the *invariant factors for* f (over K) and will be denoted correspondingly by $N_i(f)$, $E_i(f)$ and $F_i(f)$, or simply by N_i, E_i and F_i when f is fixed (the word factors is suggested by the divisibility relations between them).

Remark 4.4. Between the numbers $e_i = e(K(a_i); \gamma_i)$ from Proposition 4.1. and $E_i(f)$ there exists the relation

$$(e(K(a_i), \gamma_i) = \frac{E_{i-1}}{E_i}.$$

2. By *the system of invariants for* (the irreducible and monic) *polynomial* f we shall mean the following picture:

$$P(f) = \begin{pmatrix} N_0 & N_1 & \cdots & N_{l(f)} \\ E_0 & E_1 & \cdots & E_{l(f)} \\ F_0 & F_1 & \cdots & F_{l(f)} \\ & \delta_1 & \cdots & \delta_{l(f)} \\ & \gamma_1 & \cdots & \gamma_{l(f)} \end{pmatrix}$$

where $\delta_i = v(a_{i-1} - a_i)$, $\gamma_i = v(f_i(a_{i-1}))$ are as in Proposition 4.3.

It is natural to ask if one has a picture P with arbitrary numbers and length (m instead of $l(f)$) in what conditions there exists an irreducible

polynomial $f \in K[X]$ such that $P = P(f)$? The following relations are obviously necessary:

(1) N_i, E_i, F_i are positive integers and δ_i, γ_i are rational numbers (not necessarily positive).

(2) E_i/E_{i-1}, $1 \leqslant i \leqslant m$, $E_m = 1$

(3) F_i/F_{i-1}, $1 \leqslant i \leqslant m$, $F_m = 1$

(4) $N_i = E_i F_i$, $1 \leqslant i \leqslant m$

(5) $N_0 > N_1 > \cdots > N_m$

(6) $\gamma_i = (s_i/E_{i-1})$, where $(s_i, E_{i-1}/E_i) = 1$, $1 \leqslant i \leqslant m$.

This follows from Proposition 4.1 since

$$G(K(a_{i-1}))/G(K(a_i)) \simeq \frac{1}{E_{i-1}} Z \Big/ \frac{1}{E_i} Z$$

(7) $\delta_1 > \delta_2 > \cdots > \delta_m$

Also there are relations between γ_i and δ_i, involving elements which are not in P:

$$\gamma_i = v(f_i(a_{i-1})) = \sum_{a'} \inf(\delta_i, v(a_i - a')),$$

where a' runs over all the roots of f_i.

The study of some properties related with the roots of f_i will be the subject of a future work. For the moment we are interested in the question regarding the "reduced" picture P_r and $P_r(f)$ which is obtained from P and $P(f)$ respectively by the elimination of the fourth row. This problem happens to have a simple answer. More exactly we claim firstly that a new necessary condition is:

(7') $(\gamma_1/N_1) > (\gamma_2/N_2) > \cdots > (\gamma_m/N_m)$

and secondly that (1)–(6) and (7') are sufficient for the existence of an f for which $P_r(f) = P_r$.

The necessity of (7') follows from the relations:

$$\begin{aligned}\frac{\gamma_i}{N_i} &= \frac{v(f_i(a_{i-1}))}{N_i} = \frac{1}{N_i} \sum_{a' \text{ root of } f_i} \inf(\delta_i, v(a_i - a')) \\ &> \frac{1}{N_i} \sum_{a' \text{ root of } f_i} \inf(\delta_{i+1}, v(a_1 - a')) = \frac{v(f_i(a_{i+1}))}{\deg f_i} \\ &= \frac{v(f_{i+1}(a_i))}{\deg f_{i+1}} = \frac{\gamma_{i+1}}{N_{i+1}}.\end{aligned}$$

The above inequality is strictly, as show the terms where $a' = a_i$.

For the second part of our assertion we construct a sequence of monic irreducible polynomials: $f_m, f_{m-1}, ..., f_0$ together with a sequence $a_m, a_{m-1}, ..., a_0$ of their roots (respectively), such that $(a_0, a_1, ..., a_m)$ is a s.d.c. and that

$$P_r(f_i) = \begin{pmatrix} N_i & N_{i+1} \cdots & N_m \\ E_i & \cdots & E_m \\ F_i & \cdots & F_m \\ & \gamma_{i+1} & \gamma_m \end{pmatrix}, \qquad i = m, m-1, ..., 0$$

We start from $a_m = 0$ and $f_m = X$ which satisfies

$$P_r(f_m) = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}.$$

Suppose we have defined $f_m, f_{m-1}, ..., f_i$ and $a_m, ..., a_i$. The function $\rho: R \to R$, $\rho(t) = \sum_{a' \text{ root of } f_i} \inf(t, v(a_i - a'))$ is continuous, increasing and onto. Let $\delta_i = \rho^{-1}(\gamma_i) \in Q$. Let $\delta_{i+1} = v(a_i - a_{i+1})$. From the inductive hypothesis one knows that

$$\frac{\gamma_{i+1}}{N_{i+1}} = \frac{v(f_{i+1}(a_i))}{\deg f_{i+1}} = \frac{v(f_i(a_{i+1}))}{\deg f_i} = \frac{1}{N_i}\rho(\delta_{i+1})$$

and we obtain from (7'): $\delta_{i+1} = \rho^{-1}((N_i/N_{i+1})\gamma_{i+1}) < \rho^{-1}(\gamma_i) = \delta_i$. Since (a_i, a_{i+1}) is a distinguished pair, it follows that (a_i, δ_i) is a minimal pair. Let w be the r.t. extension of v to $K(X)$ defined by (a_i, δ_i). According to the notations stated in Theorem 1.2 let $h_i \in K[X]$ such that $\deg h_i < \deg f_i = n_i$ and $w(h_i) = v(h_i(a_i)) = (e_{i-1}/e_i)\gamma_i$ and let $r_i = f_i^{(e_{i-1}/e_i)}/h_i$. From the above condition (6), and Theorem 1.2 it follows that $w(r_i) = 0$, r_i^* is transcendental over $R(K)$ and that $k_w = R(K(a_i))(r_i^*)$. Let G_i be a monic irreducible polynomial of degree F_{i-1}/F_i over $R(K(a_i))$, let f_{i-1} be a lifting of G_i with respect to (a_i, δ_i, h_i) and let a_{i-1} be a root of f_{i-1} for which $v(a_{i-1} - a_i)$ is greatest. Then f_{i-1} and a_{i-1} have the required properties.

Indeed, the above condition (4) implies $\deg f_{i-1} = n_{i-1}$ and (5) shows that the lifting (G_i, f_{i-1}) is non-trivial, so we can apply Theorem 3.1 to conclude the inductive step. Therefore we have obtained the following:

THEOREM 4.5. *A reduced picture P_r is of the form $P_r(f)$ if and only if it satisfies the above conditions* (1)–(6) *and* (7').

The constructive proof of this Theorem has two ineffective points (we remind that the problems regarding G_i are ignored; the aim of our paper

is to reduce the study of irreducible polynomials over K to the study of the irreducible polynomials over the finite extensions of $R(K)$). The first is the choice of h_i and the second is the construction of f_{i-1} from f_i, a_i, δ_i and G_i. We look now for a canonical way of choosing h_i. In order to do this, we observe that the number $v(h_i(a_i)) = (E_{i-1}/E_i)\,\gamma_i \in (1/E_i)Z$ has a unique representation in the form

$$\frac{E_{i-1}}{E_i}\gamma_i = \sum_{1<j\leqslant m} c_{ij}E_j + c_i,$$

where c_i, $c_{ij} \in Z$ and $0 \leqslant c_{ij} < (E_{j-1}/E_j$ for $i < j \leqslant m$. Hence we may choose

$$h_i = \pi^{c_i} \prod_{i<j\leqslant m} f_j^{c_{ij}}, \qquad (\pi = \pi_k)$$

because for $j > i$ one has $\gamma_i = v(f_j(a_{j-1})) = v(f_j(a_i))$ (the condition $\deg h_i < n_i$ is then easily verified).

3. In the proof of Theorem 4.5, $G_1, \ldots, G_m$ are irreducible monic polynomials over some fields $k_1 \supseteq \cdots \supseteq k_m = R(K)$, respectively, such that for $i < m$, k_i is generated over k_{i+1} by a root of G_{i+1}. Such a system $(G_1, \ldots, G_m)$ will be called a *tower system of irreducible polynomials for* $R(K)$. We can introduce an equivalence relation "$\sim$" between tower systems:

$(G_1, \ldots, G_m) \sim (H_1, \ldots, H_m)$ if and only if there exists $\tau \in \mathrm{Gal}(R(\bar{K})(Y)/R(K)(Y))$ such that $\tau(G_i) = H_i$ for $1 \leqslant i \leqslant m$.

By a *lifting system* (over K) we shall mean a system $S = (a_m; \gamma_1, \ldots, \gamma_m; (G_1, \ldots, G_m))$, where $a_m \in K$, $(G_1, \ldots, G_m)$ is an equivalence class of tower systems for $R(K)$, $\gamma_1, \ldots, \gamma_m \in Q$ and such that if $c_1, \ldots, c_m$ are the denominators of $\gamma_1, \ldots, \gamma_m$, respectively, one has

(α) $\gamma_{i-1} > \gamma_i \deg G(c_i/(c_i, [c_{i+1}, \ldots, c_m]))$

(β) If $j \in \{1, \ldots, m\}$ is such that c_j divides $[c_{j+1}, \ldots, c_m]$, then $\deg G_j > 1$ (here $[c_{i+1}, \ldots, c_m]$ is the least common multiple of $c_{i+1}, \ldots, c_m$ and is 1 by convention if $i = m$; (moreover (x, y) is the greatest common divisor of x and y).

The conditions stated in this definition comes clearly from the above conditions (1)–(6) and (7').

By a *lifting chain* with respect to S, we mean a s.d.c. $(f_0, f_1, \ldots, f_m)$ of irreducible polynomials over K such that $f_m = X - a_m$ and for $1 \leqslant i \leqslant m$, f_{i-1} is a lifting of G_i with respect to $((a_i, \delta_i, h_i)$ where a_i is a root of f_i, $\delta_i = \rho_i^{-1}(\gamma_i)$, (where, $\rho_i : R \to R$ is defined by: $\rho_i(t) = \sum_{a' \text{ root of } f_i} \inf(t, v(a_i - a'))$, and $h_i \in K[X]$ is chosed in the above canonical

manner such that $\deg h_i < \deg f_i$ and $v(h_i(a_i)) = e_i\gamma_i$ (here as usual e_i is the smallest positive integer such that $e_i\gamma_i \in G(K(a_i))$).

It is easy to see that the above definition does not depend on the choice of the representative $(G_1, ..., G_m)$ in the given equivalence class.

We denote by $\mathrm{Irr} = \mathrm{Irr}(K)$, $SDC = SDC(K)$ and $LS = LS(K)$ respectively: the set of irreducible polynomials, the set of s.d.c. and the set of lifting systems over K.

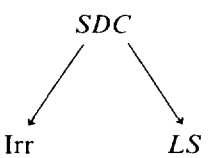
If $S \in LS$ and $C \in SDC$ is a lifting chain for S, we say that S is *a projection* of C into LS.

Also, if C is a s.d.c. for f, we say that f is the projection of C into Irr and we denote it by $\mathrm{pr}_0(C)$.

Now, we are ready to give the following characterisation result of irreducible polynomials over K.

THEOREM 4.6. (a) *Any $C \in SDC$ has a unique projection into LS, denoted by* $\mathrm{pr}(C)$.

(b) *The maps*



are onto.

(c) *Let $S \in LS$, $S = (a_m, \gamma_1, ..., \gamma_m; (G_1, ..., G_m))$. Then* all *the elements $f \in \mathrm{pr}_0(\mathrm{pr}^{-1})(S)$ have the same length $l(f) = m$, the same invariants $\gamma_1, ..., \gamma_m$ which are those of S, and the same invariant factors, which are given, for $0 \leqslant i \leqslant m-1$, by*

$$\begin{aligned} F_i &= \prod_{i<j<m} \deg G_i \\ E_i &= [c_{i+1}, ..., c_m] \\ N_i &= E_i F_i, \end{aligned} \tag{16}$$

where $c_1, ..., c_m$ are the denominators of $\gamma_1, ..., \gamma_m$.

(d) *Let $f \in \mathrm{Irr}$. Then* all *the elements $S \in \mathrm{pr}(\mathrm{pr}_0^{-1}(f))$, $S = (a_m; \gamma_1 \cdots \gamma_m, (G_1 \cdots G_m))$ have the same m, $\gamma_1, ..., \gamma_m$, $\deg G_1, ..., \deg G_m$, they define the same circle $\{x \in \bar{K};\ v(x - a_m) \geqslant \delta_m\}$ in $\bar{K}$, and the same (up to $R(\bar{K})/R(K)$ automorphisms) tower of fields: $R(K) = k_m \subseteq k_{m-1} \subseteq k_0 \subset R(\bar{K})$, where k_{i-1} is generated over k_i by a root of G_i, for $1 \leqslant i \leqslant m$.*

Proof. Since a great part of the proof is contained in our previous results, we shall note now only few facts.

If $C \in SDC$ then using Theorem 4.5 we get elements a_m, $\gamma_1, \ldots, \gamma_m$, $G_1, \ldots, G_m$, which, by the results of this section gives an $S \in LS$. Moreover a_m is the root of f_m, $\gamma_1, \ldots, \gamma_m$ are invariants of f, the valuations w_i (defined by: a_i = root of f_i and $\delta_i = \rho_i^{-1}(\gamma_i)$), h_i (given canonically) and the rational fractions r_i depends (modulo a K-automorphism of $\bar{K}$) only on C. Hence $G_i = (f_{i-1}/h_i^{\deg G_i})^*$ depends only on C and $S = \mathrm{pr}(C)$ is uniquely determined.

On the other hand let $S \in LS$. If we define F_i, E_i and N_i by (16), then the relations (1)–(6) and (7′) are easily satisfied, and we may apply the proof of Theorem 4.5 to see that $\mathrm{pr}^{-1}(S) \neq \emptyset$. The other assertions follows now immediately from the results of this section (we note only that the circle from (d), which is identical to the circle $\{x \in \bar{K};\ v(x-a) \geqslant \gamma_m\}$, where a is any root of f, is exactly the domain of values of a_m when S ranges over $\mathrm{pr}(\mathrm{pr}_0^{-1}(f))$.

4. We end this paper with a discussion on the second ineffective point in the proof of Theorem 4.5, namely the lifting $(f_i, a_i, \gamma_i, h_i, G_i)$ of f_{i-1}. Of course, we have a way of choosing f_{i-1}, which is given by Remark 1.3. But we want to describe the set of *all* polynomials g which are liftings of $(f_i, a_i, \gamma_i, h_i, G_i)$.

Let g_0 be a fixed lifting (e.g., given by Remark 1.3), and let g be another lifting of $(f_i, a_i, \gamma_i, h_i, G_i)$. Then one has:

$$\begin{aligned} \deg(g - g_0) &< \deg g_0 \\ w(g - g_0) &> w(g_0) \end{aligned} \tag{17}$$

Writing $g - g_0 = \sum_{0 \leqslant k < (n_{i-1}/n_i)} A_k f_i^k$, then (17) is equivalent to a system of inequalities of the form

$$v(A_k(a_i)) > s_{ki},$$

where s_{ki} are known rational numbers.

This requires practically the *knowing* of v on $K(a_i)$ (i.e., the knowing of $v(A_k(a_i))$ if the coefficients of A_k are known). This problem is not at all clear for a general extension $K(a)$ of K, but it is solvable by induction in our case, using the already known properties of v with respect to $K(a_{i+1}), \ldots, K(a_m) = K$. More exactly if $A \in K[X]$, $\deg A < \deg f_i$ and if we put A in the form

$$A = \sum_{0 \leqslant j_{i+1} < (n_i/n_{i+1})} f_{i+1}^{j_{i+1}} \sum_{0 \leqslant j_{i+2} < (n_{i+1}/n_{i+2})} f_{i+2}^{j_{i+2}} \cdots \sum_{0 \leqslant j_m < n_{m-1}} f_m^{j_m} C_{j_1, \ldots, j_m},$$

where $c_{j_1 \cdots j_m} \in K$, then

$$v(A(a_i)) = \inf_{j_{i+1}, \ldots, j_m} \left(v(c_{j_1 \cdots j_m}) + \sum_{i < k \leqslant m} j_k \gamma_k \right)$$

Returning to the polynomial g, we put it in the form

$$g = X^{n_i - 1} + \sum_{0 \leqslant j_i < (n_{i-1}/n_i)} f_i^{j_i} \cdot \sum_{0 \leqslant j_{i+1} < (n_i/n_{i+1})} f_{i+1}^{j_{i+1}}, \ldots, \sum_{0 \leqslant j_m < n_{m-1}} f_m^{j_m} C_{j_1, \ldots, j_m}$$

and we obtain

g verifies (17) if and only if the coefficients $c_{j_1 \cdots j_m}$ vary in some circles of known radius and of centers determined by g_0.

In this way we see that the general lifting process can be described in a constructive manner.

Remark 4.7. Let K_1 be a finite extension of K. If one knows a generator θ of K_1/K and a s.d.c. $(f_0, f_1, \ldots, f_m)$ for the minimal polynomial f_0 of θ, one may construct an integral basis of K_1 over K in the following way:

Let us denote

$$\Delta_{j_1 \cdots j_m} = \prod_{k=1}^{m} f_k(\theta)^{j_k}, \qquad \text{where} \quad 0 \leqslant j_k < (n_{k-1}/n_k)$$

and

$$d_{j_1 \cdots j_m} = [v(\Delta_{j_1 \cdots j_m})] \qquad \text{(the integral part)}$$

The relations like (18) show that the elements

$$\{\pi_K^{-d_{j_1 \cdots j_m}} \Delta_{j_1 \cdots j_m}\} \qquad 0 \leqslant j_1 < (n_0/n_1)$$

$$\cdots$$

$$0 \leqslant j_m < (n_{m-1}/n_m)$$

form an integral basis of K_1 relative to K.

As a final remark we note that from the above invariants of θ we may obtain an invariant of K_1, namely the discriminant.

REFERENCES

1. V. ALEXANDRU, N. POPESCU, AND A. ZAHARESCU, A theorem of characterization of residual transcendental extensions of a valuation, *J. Math. Kyoto Univ.* **28**, No. 4 (1988), 579–592.
2. V. ALEXANDRU, N. POPESCU, AND A. ZAHARESCU, Minimal pairs of a residual transcendental extension of a valuation, *J. Math. Kyoto Univ.* **30** (1990), 207–225.

3. E. ARTIN, "Algebraic Numbers and Algebraic Functions," Gordon and Breach, New York/London/Paris, 1967.
4. Z. I. BOREVICI AND I. R. SAFAREVICI, "Number Theory," Izd. Nauka, Moscow, 1972. [Russian]
5. H. HASSE, "Number Theory," Springer-Verlag, Berlin/Heidelberg/New York, 1980. [English Translation]
6. N. POPESCU, Sur une classe de polynomes irréducibles, *C.R. Acad. Sci. Paris* **297** (1983), 9–11.
7. L. POPESCU AND N. POPESCU, Sur la définition des prolongements résiduels transcendents d'une valuation sur un corps K à $K(X)$, *Bull. Math. Sci. Math. R.S. Roumanie* **33** (81), No. 3 (1989), 257–264.
8. J. P. SERRE, "Corps Locaux," Hermann, Paris, 1962.