AN ALGORITHM FOR FINDING DISTINGUISHED CHAINS OF POLYNOMIALS

by
Alexandru Zaharescu

Abstract. Saturated distinguished chains of polynomials over a local field *K* have been introduced in [9] in order to study the structure of irreducible polynomials in one variable over *K*. We provide an algorithm for finding a saturated distinguished chain of polynomials associated to a given irreducible polynomial *f(X) 0 K[X].*

1. INTRODUCTION

The problem of describing the structure of irredncible polynomials in one variable over a local field *K* has been studied in [9]. In the process, the notion of a saturated distinguished chain of polynomials over *K* was defined in [9], and Iater studied also in [2], [7] and [8]. Knowing a saturated distinguished chain for a given element a0k, where k denotes a fixed algebraic closure of K , can be helpful in various problems. One reason is that we can use such a chain to construct an integral basis of *K(a)* over *K,* following the procedure explained in [9], Remark 4.7. The shape of such a basis may be useful in practice, for instance it has been used in [61 in order to show that the Ax-Sen constant vanishes for deeply ramified extensions (in the seuse of Coates-Greenberg [4]).

A constructive way to produce all the irreducible polynomials in one variable over *K* is described in [9], via an operation of lifting. Starting with a linear polynomial *go(X),* by applying repeatedly such an operation of lifting one can construct chains ofirreducible polynomials $(g_o(X), g_1(X), \ldots, g_r(X))$ such that $1 = \deg g_o < \deg g_1 < \ldots < \deg g_r$. It is shown in [9] that for any irreducible polynomial *g(X)* over *K*, there exists a chain of lifting polynomials as above such that $g_r(X) = (X)$. Conversely, starting with an irreducible polynomial *f(X)* over *K*, one associates to *f(X)* so-called saturated distinguished chains of polynomials. These are certain chains of irreducible polynomials over *K*, $(f_o(X), f_1(X),..., f_s(X))$, with $f_o(X) = f(X)$ and $\deg f_o > \deg f_1 > \ldots > \deg f_s = 1$. As described in [9], there is an intimate connection between chains of lifting polynomials and saturated distinguished chains of polynomials over *K*. As mentioned above, one has a constructive way of producing chains of lifting polynomials, assuming that one knows the structure of irreducible polynomials over the residue field of K and its finite field extensions. Saturated distinguished chains of polynomials associated to a given irreducible polynomial *f(X)* over *K* are usually provided in a less canonical way.

In this paper we present an algorithm for finding a saturated distinguished chain of

polynomials for a given irreducible polynomial $f(X)$ over K. We will restrict to the case when K coincides with the field Q_p of p-adic numbers for some prime number p (although the method works in more generality). Thus, given any polynomial $f(X)$ $Q_p[X]$, the algorithm described below verifies first if $f(X)$ is irreducible over Q_p or not, and in case $f(X)$ is irreducible, it enables one to find, after finitely many steps, a saturated distinguished chain of polynomials associated to $f(X)$ over Qp.

2. NOTATIONS, DEFINITIONS AND GENERAL RESULTS

In this section we present some general definitions and results concerned with residual transcendental extensions of a valuation, lifting polynomials, and distinguished pairs and distinguished chains of polynomials over a local field. The reader interested only in the actual algorithm for finding saturated distinguished chains of polynomials may skip most of this section, read the definition of a distinguished pair, respectively a distinguished chain of polynomials, and then go directly to the next section. For a reader who is interested in the general theory of saturated distinguished chains of polynomials, and their relationship with residual transcendental extensions of valuations and with lifting polynomials, this section presents an abstract of some of the basic notions, definitions and results.

We consider a field K of characteristic zero, which is complete with respect to a rank one and discrete valuation v (see [3], [5], [10]). Let $\bar{K}$ be a fixed algebraic closure of K and denote also by v the unique extension of v to $\bar{K}$. If $K \phi L \phi \bar{K}$ is an intermediate field, we denote $G(L) = \{v(x) : x 0 L\}$. As usual, $G(K)$ will be identified with the ordered group $\mathbf{Z}$ of rational integers, and for every intermediate field L, $G(L)$ will be viewed as a subgroup of the additive group Q.

Denote $A(L) = \{x\ 0\ L : v(x) \geq 0\}$, the ring of integers of L. Let $M(L) = \{x\ 0\ L : v(x) > 0\}$, and denote by π_L a uniformizing element of L. Let $R(L) = A(L)/M(L)$, the residue field of L. If $x 0 A(L)$, denote by x^* the canonical image of x in $R(L)$. As usual, $R(L)$ will be viewed canonically as a subfield of $R(\bar{K})$. Moreover, $R(\bar{K})$ is an algebraic closure of $R(K)$. We will assume that $R(K)$ is a perfect field.

Let $K \phi L_1 \phi L_2 \phi \bar{K}$ be intermediate fields such that L_2 is a finite extension of K. Then $R(L_2)/R(L_1)$ is a finite extension, and the number $f(L_2/L_1 = [R(L_2) : R(L_1)]$ is called the inertial degree of L_2 relative to L_1. The quotient group $G(L_2)/G(L_1)$ is finite. Its index, denoted by $e(L_2/L_1)$, is 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 $K \phi L \phi \bar{K}$ and $a\ 0\ \bar{K}$, 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 $f\ 0 A(K)[X]$, $f = a_o X^n + a_1 X^{n-1} + \ldots + a_n$, we denote

$$\bar{f} = a^{*}{}_{o}X^{n} + + \ldots + 0\, R(K)[X],$$

the canonical image of f in $R(K)[X]$.

If $a\ 0\ \bar{K}$ and $*\ 0\ Q$, we define, for any $F(X) = c_o + c_l\,(X - a) + \ldots + c_n,(X - a)^n\ 0\ \bar{K}[X]$,

$$w(F) := \inf_{0 \le i \le n} \{v(c_i) + i*\}.$$

In this way one obtains a valuation w on $\bar{K}$[X], which extends canonically to a valuation on $\bar{K}$(X), and which is a residual transcendental (r.t. for short) extension of ($\bar{K}$,v), in the sense that the residual field of w is transcendental over $R(\bar{K})$. This valuation w is called the r.t. extension of ($\bar{K}$,v) defined by *inf*, a and $*$.

An element $(a, *)\ 0\ \bar{K}\ x\ Q$ is said to be minimal with respect to K if for every $b\ 0\ \bar{K}$ the condition $v(a-b) \ge *$ implies $[K(a):K] \le [K(b):K]$. The word minimal was suggested by the fact that this definition is equivalent to the following: $(a, *)$ is a minimal pair if there is no pair $(a', *)$ with $\deg a' < \deg a$ such that both pairs define the same residual transcendental extension w on $\bar{K}[X]$.

If $a\ 0\ \bar{K}\ \setminus K$, we denote $\omega(a) = \sup\{v(a - a')\}$ where a' runs over the set of all the conjugates of a over K, with $a' \neq a$. By Krasners Lemma (see [3], p. 66) it follows that for any $a\ 0\ \bar{K}\ \setminus K$ and for any $* > \omega(a)$, the pair $(a,*)$ is a minimal pair.

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

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

If $F\ 0\ K[X]$, we write F in the form

$$F = F_0 + F_1 f + \ldots + F_t f^t,\ \deg F_i < \deg f,\ i = 0,1,\ldots,t.$$

Then we define

$$w(f) = \inf_{0 \le i \le t} \left(v(F_i(a)) + i\gamma\right) \tag{2.1}$$

In [1] it is proved the following result.

Theorem 1. Let $(a,*)$ be a minimal pair with respect to K. Then the assignment (2.1) defines a valuation w on $K[X]$, and canonically on $K(X)$, which coincides with the restriction of the valuation on $\bar{K}\ (X)$ defined by *inf*, a and $*$.

Moreover one has:

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

(ii) 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 $K(X)$ for which $w(r) = 0$, the image r^* of r in the residue field k_w of w is transcendental over $R(K)$ and k_w is isomorphic to $R(K(a))(r')$. This isomorphism is canonic: for any $F \in K[X]$ with $\deg F < \deg a$ we have $w(F(X)) = w(F(a))$, $(F(X)/F(a))^* = 1$ 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 $(a, *)$ which is minimal with respect to K and such that w' coincides with the r. t. extension defined by the minimal pair $(a, *)$.

Let now $(a,*) \in \bar{K} \times Q$ be a minimal pair, and denote by w the corresponding r. t. extension of v to $K(X)$. We identify the residue field $k_w = R(K(a))(r^*)$ of w with the field of rational functions $R(K(a))(Y)$ in one variable Y over the field $R(K(a))$, i.e. we shall write $r^* = Y$
Let $G \in R(K(a))[Y]$ be monic and let $m = \deg G$. A monic polynomial $g \in K[X]$ is said to be a lifting of G with respect to w (or with respect to a, $*$ and h) provided one has

$$\deg g = e m \deg f,$$
$$w(g(X)) = m w(h(X)) = m e \gamma$$

and

$$\left(\frac{g}{h^m}\right)^* = G$$

One says that the lifting g of G is trivial if $\deg g = \deg f$. This situation appears exactly when $\deg G = 1$ and $\gamma = w(f) \in G(K(a))$.
Theorem 2. ([9], Theorem 2.1) Let $G \in R(K(a))[Y]$, $G \neq Y$, G monic and irreducible. Then any lifting g of G in $K[X]$ is irreducible over K.
The connection between lifting polynomials and the so-called distinguished pairs of polynomials has also been investigated in [9].

A pair (a, b) of elements from $\bar{K}$ is said to be a distinguished pair, provided one has

$$\deg a > \deg b,$$
$$v(a-c) \leq v(a-b)$$

for any $c \in \bar{K}$ with $\deg c < \deg a$, and

$$v(a - c) < v(a - b)$$

for any $c \in \bar{K}$ with $\deg c < \deg b$.
Given two irreducible polynomials $f, g \in K[X]$, one says that (g, f) is a distinguished pair if there exist a root a of g and a root b of f such that (a, b) is a distinguished pair. It is easy to see that if (g, f) is a distinguished pair of polynomials, then for any root a of g there exists a root b of f such that (a, b) is a distinguished pair, and for any root b of f there exists a root a of g such that (a, b) is a distinguished pair.
The following two results establish the connection between lifting polynomials and

distinguished pairs.

Theorem 3. ([9], Theorem 3.1) Notations and hypotheses are as in Theorem 1 above Let $G \in R(K(a))[Y]$, $G \neq Y$, G monic and irreducible. If g is a nontrivial lifting of G in $K[X]$ then (g, f) is a distinguished pair.

Theorem 4. ([9], Theorem 3.2) Let (g, f) be a distinguished pair of polynomials and let a be a root of f. Then there exist γ, h as in Theorem 1 , and there exists $G \in R(K(a))[Y]$, $G \neq Y$, G monic and irreducible such that g is a nontrivial lifting of G.

Let $a \in \bar{K}$. If $a_0, \ldots, a_s \in R$, one says 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 $i \in \{1,\ldots,s\}$. The integer s is called the length of the chain $(a_0, \ldots, a_s)$. A distinguished chain $(a_0, \ldots, a_s)$ for a is said to be saturated if there is no distinguished chain $(b_0, \ldots, br)$ for a, with $r > s$, such that $\{a_0, \ldots, a_s\} \subset \{b_0, \ldots, b_r\}$. One shows that $(a_0, \ldots, a_s)$ is saturated if and only if $a_s \in K$ .Let $f_0 = f, f_1, \ldots, f_s$ be monic, irreducible polynomials over K. One says that $(f_0, \ldots, f_s)$ is a (saturated) distinguished chain for f if there exist roots $ao = a, a_1, \ldots, a_s$ of $f_0, f_1, \ldots, f_s$ respectively such that $(a_0, \ldots, a_s)$ is a (saturated) distinguished chain for a. The following three results capture some of the basic properties of saturated distinguished chains.

Theorem 5. ([9], Proposition 4.1). If $(a_0, \ldots, a_s)$ is a distinguished chain, then

$$G(K(a_s)) \subset G(K(a_{s-1})) \subset \ldots \subset G(K(a_o)),$$

and

$$R(K(a_s)) \subset R(K(a_{s-1})) \subset \ldots \subset R(K(a_o)),$$

Theorem6. ([9], Proposition 4.2). Let $(a_0, \ldots, a_s)$ and $(b_0, \ldots, br)$ be twosaturated distinguished chains for a. Then $s = r$.

Moreover if $c_i \in \{a_i, b_i\}$, $1 \leq i \leq s$, then $(c_0, \ldots, c_s)$ is also a saturated distinguished chain for a.

Theorem7. ([9], Proposition 4.3). Let $a \in \bar{K}$, let $(a_0, \ldots, a_s)$ and $(b_0, \ldots, b_s)$ be two saturated distinguished chains for a, and let f_i, g_j be the minimalpolynomials of a_i and b_j respectively. Then for any $i \in \{1, \ldots, s\}$ one has

$$v(a_{i-1} - a_i) = v(b_{i-1} - b_i),$$
$$v(f_i(a_{i-1})) = v(g_i(b_{i-1})),$$
$$G(K(a_i)) = G(K(b_i)),$$

and

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

Moreover if we replace the condition $b_0 = a$ in the hypothesis by the condition $b_0 = \sigma(a)$ where $\sigma \in Gal(\bar{K}/K)$ then all the above relations remain valid,with the only exception that in the last relation instead of equality we have a canonical $R(K)$ - isomorphism.

3. FINDING SATURATED DISTINGUISHED CHAINS

In what follows we fix a prime number p and let $K = Q_p$. Choose a monic polynomial $f(X)\ 0\ Q_p[X], f(X) = X^d + c_1X^{d-1} + \ldots + c_d$.

Our aim is to describe an algorithm which enables one to verify if $f(X)$ is irreducible over Q_p, and, in case it is, to provide an irreducible polynomial $g(X)\ 0\ Q_p[X]$ such that (f, g) is a distinguished pair. Then, by repeatedly applying the same algorithm, after finitely many steps one finds a saturated distinguished chain (fo = f, f_1 = g, f_2, … ,f_s) for f.
We remark that if $a, b\ 0\ \overline{Q}_p$ and (a, b) is a distinguished pair, then (p^ka, p^kb) is also a distinguished pair, for any $k\ 0\ Z$. Thus, by performing if necessary such a transformation to the roots of f , which is achieved by applying an appropriate transformation to the coefficients of f , we may assume in what follows that $c_1, \ldots, c_d$ belong to the ring Zp of p-adic integers. Then, in case f is irreducible over Q_p, any monic, irreducible polynomial g over K for which (f, g) is a distinguished pair , will also have all its coefficients in Zp. Thus in the following it is enouph to work with monic polynomials from $Zp[X]$, and in this set to find one polynomial, call it $g(X)$, for which (f, g) is a distinguished pair. The algorithm explained below is based on the computation of resultants $R(h, f)$ for various monic polynomials $h(X)\ 0\ Zp[X]$ with $\deg h < \deg f$.
If $a_1, \ldots, a_d$ are the roots of f and $\eta_1, \ldots, \eta_r$ are the roots of h, where $r = \deg h \leq d - 1$, then we have

$$v(R(h, f)) = \sum_{1\leq i\leq r} \sum_{1\leq j\leq d} v(\eta_i - a_j)$$

where v denotes the p-adic valuation, normalized such that v(p) = 1 The point here is that the resultant $R(h, f)$ can be written as a determinant involving the coefficients of f and h, and so we do not need to know the roots of f and h, but only the coefficients of these polynomials, in order to be able to compute $R(h, f)$. Thus here and in what follows, when we say that we "know" a polynomial, we mean that we know its coefficients, and we do not mean that its roots are known. In particular, by choosing at the beginning the polynomial f we understand that the coefficients $c_1 , \ldots , c_d$ are given, without implying any knowledge of its roots $a_1, \ldots, a_d$.
Now the first step of our algorithm is to compute the discriminant of f , call it Δ. This is done by taking the resultant of $f(X)$ with $f'(X)$ If it turns out that $\Delta = 0$, then f has multiple roots and so it can not be irreducible. Assume in what follows that $\Delta \neq 0$. Note that since $v(\Delta)$ is a sum of non-negative terms of the form $v(a_i - a_j)$, it follows that each individual term is bounded by $v(\Delta)$, that is,

$$v(a_i - a_j) \leq v(\Delta),$$

for any $1 \leq i \neq j \leq d$. As a consequence, for any $i\ 0\ \{1, \ldots, d\}$ for which $a_i\ \not 0\ Q_p$, we

have

$$w(a_i) := sup\{v(a_i - \sigma(a_j) : \sigma \neq 0 \ Gal(\overline{Q}_p/Qp), \sigma(a_i) \neq ai\} \leq v(\Delta).$$

We distinguish two cases, according as to whether f is irreducible or not. Assume first that f is irreducible over Q_p. Then, for any monic polynomial $h(X) \neq 0 \ Zp[X]$ with $deg\ h \leq d-1$ we have

$$(3.1) \quad v(R(h, f)) \leq d(deg\ h)\, v(\Delta).$$

Indeed, if for some such h we have $v(R(h, f)) > d(degh)v(\Delta)$, then there will be roots η_i and a_j of h and f respectively, such that $v(\eta i - aj) > v(\Delta)$. This further implies that $v(\eta i - aj) > w(aj)$, and by Krasner's Lemma it follows that $Q_p(aj) \neq Q_p(\eta_j)$, which is not the case, since $deg\ h < deg\ f$ and f was assumed to be irreducible. This proves (3.1).
Let us assume now that f is not irreducible over Q_p. Then (3.1) fails. In fact, if $f = f_1 f_2$, with $f_1, f_2 \neq 0 \ Zp[X]$, f_1, f_2 monic, $deg\ f_1,\ deg\ f_2 \geq 1$, and if we choose $h = f_1$, then we will have $R(h, f) = 0$,

$$v(R(h, f)) = 4.$$

Putting both cases together, we see that f is irreducible if and only if

(3.2) $sup\{v(R(h, f)) : h \neq 0 \ Zp[X]$, h monic, $deg\ h \leq d-1\} \leq d(d-1)v(\Delta)$

Let us remark that, although the supremum on the left hand side of (3.2) is taken over an infinite set of polynomials, one can check whether (3.2) holds, in finitely many steps. Indeed, if $h_1, h_2 \neq 0 \ Zp[X]$ are both monic, of same *degree* $r \leq d - 1$, say

$$h_1 = X^r + b_1 X^{r-1} + \ldots + b_r,$$

and

$$h_2 = X^r + b_1' X^{r-1} + \ldots + b_r',$$

and if

$$(3.3) \quad v(b_i - b_1') \geq 1 + d(d - 1)v(\Delta), \ 1 \leq i \leq r,$$

then we have

$$(3.4) \quad v(R(h_1, f)) \leq d(d - 1)v(\Delta)$$

if and only if

$$(3.5) \quad v(R(h_2, f)) \leq d(d - 1)v(\Delta).$$

This follows immeruately from the expression of $R(h_1, f)$ and $R(h_2, f)$ as determinants. The inequalities $v(b_i - b_i') \geq 1 + d(d - l)v(\Delta)$ imply that the corresponding entries in these two determinants are congruent modulo $p^{1+d(d-1)v(\Delta)}$. Then, since all the entries in these two determinants are p-adic integers, $R(h_1, f)$ and $R(h_2, f)$ will also be cougruent modulo $p^{1+d(d-1)v(\Delta)}$, and hence one of them is divisible by $p^{1+d(d-1)v(\Delta)}$ if and only if the other is divisible by $p^{1+d(d-1)v(\Delta)}$. So under the assumptions from (3.3), the inequalities

(3.4) and (3.5) are equivalent.
Now any p-adic integer is congruent modulo $p_1+d(d-1)v(\Delta)$ to one of the natural numbers 1, 2, 3, . . . , $p_1+d(d-1)v(\Delta)$. Therefore, if we consider for any $1 \leq r \leq d-1$ the finite set of polynomials M_r defined by

$$M_r = \{h = X^r + b_1X^{r-1} + \ldots + b_r : bj\ 0\{1, 2, \ldots, p1+d(d-1)v(\Delta)\},\ 1 \leq j \leq r\},$$

then any monic polynomial in $Z_p[X]$ of degree r will be congruent modulo $p^{1+d(d-1)v(\Delta)}$ to a polynomial $h(X)$ from M_r, in the sense that the corresponding coefficients of these two polynomials are congruent modulo $p_1+d(d-1)v(\Delta)$. We derive that (3.2) is equivalent to the inequality

$$(3.6) \qquad \max_{1\leq r\leq d-1} \max_{h\in M_r} v(R(h,f)) \leq d(d-1)v(\Delta)$$

In conclusion, f is irreducible if and only if (3.6) holds, and this can be checked in a finite number of steps.
Assume in what follows that f is irreducible. Let us define the quantity

$$(3.7) \qquad p := \max_{1\leq r\leq d-1} \max_{h\in M_r} \frac{v(R(h,f))}{\deg h}$$

We denote by M the subset of $U_{1\leq r\leq d-1}\ M_r$ for which the maximum on the right hand side of (3.7) is attained Thus

$$(3.8) \qquad M = \left\{h \in \cup_{1\leq r\leq d-1} M_r : \frac{v(R(h,f))}{\deg h} = p\right\}$$

Next, we denote by M^* the subset of M consisting of the polyuomials from M of smallest degree, and denote this degree by r^*. So

$$(3.9) \qquad r^* = min\ \{\ deg\ h : h\ 0\ M\},$$

and

$$(3.10) \qquad M^* = \{h\ 0\ M : deg\ h = r^*\}$$

Note that $p,\ M,\ r^*$ and M^* can all be found after a finite amount of computation. We claim that any polynomial $g(X)\ 0\ M^*$ is irreducible, and (f,g) is a distinguished pair.
In order to prove the claim, fix a polynomial $g(X)0\ M^*$, and let $H(X)0\ Zp[X]$ be a monic, irreducible polynomial such that (f, H) is a distinguised pair. Say

$$H(X) = X^r + B_1X^{r-1} + \ldots + B_r$$

Let $h(X) \in M_r$,

$$h(X) = X^r + b_1X^{r-1} + \ldots + b_r$$

such that

$$v(B_i - b_i) \geq 1 + d(d-1)v(\Delta),$$

for any $i \in \{1, \ldots, r\}$. Then we know that

$$v(R(H, f)) = v(R(h, f)) \leq d(d-1)v(\Delta)$$

Combining this relation with the definition of M and with the assumption that $g(X) \in M^* \setminus M$, we find that

(3.11) $$\frac{v(R(H,f))}{r} = \frac{v(R(h,f))}{r} \leq \rho = \frac{v(R(g,f))}{r^*}$$

Let $\eta_1, \ldots, \eta_r$ and $\theta_1, \ldots, \theta_{r^*}$ denote the roots of H and g respectively Then from (3.11) we obtain

(3.12) $$\frac{1}{r}\sum_{1\leq i\leq r} v(f(\eta_i)) \leq \frac{1}{r^*}\sum_{1\leq k\leq r^*} v(f(\theta_k))$$

Since $H(X)$ is irreducible, the elements $f(\eta_i)$, $1 \leq i \leq r$ are conjugate over Q_p, and hence they all have the same valuation. In other words, the sum on the left hand side of (3.12) consists of r equal terms. We do not know yet that $g(X)$ is irreducible, so we do not know that the sum on the right hand side of (3.12) consists of r^* equal terms. In any case, from (3.12) it follows that there exists a root θ_k of g for which $v(f(\theta_k))$ is larger than or equal to each of the (equal) terrns from the sum on the left side of (3.12). Let us take an arbitrary root θ_k of g for which

$$v(f(\theta_k)) \geq v(f(\eta_i)), 1 \leq i \leq r$$

Let now a_j be one of the roots of f which is closest to θ_k, so

(3.14) $$v(\theta_k - a_j) \geq v(\theta_k - a_s), 1 \leq s \leq d$$

Since we work in an ultrametric space, from (3.14) it follows that

(3.15) $$v(\theta_k - a_s) = \min\{v(\theta_k - a_j), v(aj - a_s)\}$$

for $1 \leq s \leq d$. Next, let η_i be one of the roots of H which is closest to a_j .
Then a_j will be one of the roots of f which is closest to η_i,

(3.16) $$v(\eta_i - a_j) \geq v(\eta_i - a_s), 1 \leq s \leq d \text{ ,}$$

and we have as above

(3.17) $v(\eta_i - a_s) = \min\{v(\eta_i - a_j), v(aj - a_s)\}$

for $1 \leq s \leq d$. Combining (3.13) with (3.15) and (3.17) we find that

$$\sum_{1\leq s\leq d} \min\{v(\eta_i - a_j), v(a_j - a_s)\} = \sum_{1\leq s\leq d} v(\eta_i - a_j) = v(f(\eta_i)) \leq v(f(\theta_k)) =$$
$$= \sum_{1\leq s\leq d} v(\theta_k - a_s) = \sum_{1\leq s\leq d} \min\{v(\theta_k - a_j), v(a_j - a_s)\}$$

This further implies that

(3.18) $v(\eta_i - a_j) \leq v(\theta_k - a_j)$

By (3.16) and the ful:*t* that *(f,H)* is a distinguished pair, it follows that (a_j, η_i) is a distinguished pair. Then, by the definition of a distinguished pair and the fact that *deg* $\theta_k \leq$ *deg* $g < d$ we see that in (3.18) the right side can not be strictly greater than the left side. Therefore

(3.19) $v(\eta_i - a_j) = v(\theta_k - a_j)$

By combining (3.19) with (315) and (3.17) we obtain

$$v(\eta_i - a_s) = v(\theta_k - a_s)$$

for $1 \leq s \leq d$, and therefore we have equality in (3.13),

(3.20) $v(f(\theta_k)) = v(f(\eta_i)), 1 \leq i \leq r$

Thus we showed that any root θ_k of g which satisfies (313) will also satisfy (3.20). It follows that any root of g satisfies (3.20). Indeed, if there exists a root θ_k, of g for which

$$v(f(\theta_{k_1})) < v(f(\eta_i)),$$

then, from (3.12) we see that there must be another root θ_{k2}, of g for which

$$v(f(\theta_{k_2})) > v(f(\eta_i)), 1 \leq i \leq r$$

In that case θ_{k2}, will satisfy (3.13) without satisfying (3.20), which is impossible. So any root of g satisfies (3.20). It follows that the inequalities (3.12) and (3.11) are in fact equalities. As a consequence, we have $h\ 0\ M.$ Then, by the definition of r^* and the fact that $g\ 0\ M^*,$ we find that

$$r^* \leq r$$

We now return to (3.19), for a fixed root θ_k of g, with a_j and η_i chosen as above. Recall that (a_j, η_i) is a distinguished pair. Then, from the definition of a distinguished pair we know that (3.19) can not hold if $deg\ \theta_k < deg\ \eta_i$. Using this in combination with the inequalities $deg\ \theta_k \leq deg\ g = r^* \leq r = deg\ \eta_i$, we deduce that

(3.21) $deg\ \theta_k = deg\ g = r^* = r = deg\ \eta_i$

As a consequence, the polynomial $g(X)$ is irreducible. Also, from (3.19) and (3.21) it follows that (a_j, θ_k) is a distinguished pair. In conclusion (f, g) is a distinguished pair, as claimed.
We summarize the above results in the following algorithm.

Algorithm for finding saturated distinguished chains of polynomials

Given a monic polynomial $f(X)\ 0\ Z_p[X]$,

$$f(X) = X^d + c_1X^{d-1} + \ldots + c_d,$$

(i) Compute the discriminant Δ of f. If $\Delta = 0$, stop here: f is not irreducible.
(ii) If $\Delta \neq 0$, check the inequality (3.6). If (3.6) fails, stop here: f is not irreducible.
(iii) If (3.6) holds, then f is irreducible. Then proceed to find p, M, r^* and M^*. Select any $g\ 0\ M^*$. Then g is irreducible, and (f, g) is a distinguished pair.
(iv) Apply repeatedly step (iii), in order to find a distinguished chain $(f_o = f, f_1 = g, f_2, \ldots, f_s)$. When the last polynomial in the chain has degree 1, stop here: the chain $(f_o = f, f_1 = g, f_2, \ldots, f_s)$ is a saturated distinguished chain for f.

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** (1988), no. 4, 579-592
[2] V. Alexandru, N. Popescu and A Zaharescu, On the closed subfields, of C_p, J. Number, Theory **68** (1998), no. 2, 131-150
[3] E. Artin, Algebraic numbers and olgebraic functions, Gordon and Breach Science Publishers, New York-London-Paris 1967
[4] J. Coates and R. Greenberg, Kummer theory for abelian varieties over local fields,Invent. Math. **124** {1996), no. 1-3, 129-174
[5] H. Hasse, Number theory, (English Translation) Springer-Verlag, Berlin-New

York, 1980
[6] A. Iovita and A. Zaharescu, Galois theory of B_{dR}^{+}, Compositio Math. **117** {1999), no. 1, 1-31
[7] K. Ota, On s,aturated distinguished chain, over a local field, J. Number, Theory **79** (1999), no. 2, 217-248
[8] A. Popescu, N. Popescu, M. Vajaitu and A. Zaharescu, Chain, of metric invariants over a local field, Acta Arith. **103** (2002), no. 1, 27-40
[9] N. Popescu and A Zaharescu, On the structure of the irreducible polynomial, over Iocal fields J. Number Theory **52** (1995), no. 1, 98-1l8
[10] J. P. Serre, Local fields, Graduate Texts in Mathematics, 67. Springer-Verlag, New York-Berlin, 1979

A ZAHARESCU DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN, 1409 W. GREEN STREET, URBANA, IL, 61801, USA
E-mail address,: zaharesc@math.uiuc.edu