Bull. Korean Math. Soc. **40** (2003), No. 3, pp. 509–520

INTEGRAL BASES OVER p-ADIC FIELDS

ALEXANDRU ZAHARESCU

ABSTRACT. Let p be a prime number, $\mathbf{Q}_p$ the field of p-adic numbers, K a finite extension of $\mathbf{Q}_p$, $\bar{K}$ a fixed algebraic closure of K and $\mathbf{C}_p$ the completion of $\bar{K}$ with respect to the p-adic valuation. Let E be a closed subfield of $\mathbf{C}_p$, containing K. Given elements $t_1, \ldots, t_r \in E$ for which the field $K(t_1, \ldots, t_r)$ is dense in E, we construct integral bases of E over K.

1. Introduction

Let p be a prime number, $\mathbf{Q}_p$ the field of p-adic numbers, K a finite extension of $\mathbf{Q}_p$, $\bar{K}$ a fixed algebraic closure of K and $\mathbf{C}_p$ the completion of $\bar{K}$ with respect to the p-adic valuation. Given a finite extension L of K, it is known (see Serre [10], p. 57) that there are elements $\theta \in L$ for which the elements $1, \theta, \theta^2, \ldots, \theta^{d-1}$, with $d = [L : K]$, form an integral basis of L over K. In that case one has $O_K[\theta] = O_L$, where O_K, O_L denote the rings of integers in K and respectively L. If an element $\alpha \in L$ is given and we only know that α is a generator of L over K, that is $L = K(\alpha)$, then an integral basis of L over K can be constructed by following the procedure from [8], Remark 4.7. This basis is defined in terms of the so-called saturated distinguished chains for α, which have been introduced in [8], and studied also in [1], [6] and [7]. The shape of such a basis may be useful in practice, for instance it has been used in [5] in order to show that the Ax-Sen constant vanishes for deeply ramified extensions (in the sense of Coates-Greenberg [4]). In this paper we consider the case when several elements $\alpha_1, \ldots, \alpha_r \in L$ are given such that $K(\alpha_1, \ldots, \alpha_r) = L$, and one wants to find an integral basis of L over K. We work in the following more general context. Let E be a closed subfield of $\mathbf{C}_p$, not necessarily finite over K, and let $t_1, \ldots, t_r$ be elements of E such that the field $K(t_1, \ldots, t_r)$ is dense in E. Then we

Received September 5, 2002.
2000 Mathematics Subject Classification: 11S99.
Key words and phrases: p-adic fields, integral bases, admissible polynomials.

show how one can construct, in terms of $t_1, \dots, t_r$, an integral basis of E over K. In case $r = 1$ such a basis has been constructed in [1]. For a general r, we associate to any $\mathbf{t} = (t_1, \dots, t_r) \in \mathbf{C}_p^r$ certain sequences $\big(M_k(X_1, \dots, X_r)\big)_{k \in \mathcal{N}(\mathbf{t})}$ of polynomials in r variables $X_1, \dots, X_r$ with coefficients in K, and call them normalized sequences for $\mathbf{t}$ over K. Then we show that for any such normalized sequence of polynomials, the sequence $\big(M_k(t_1, \dots, t_r)\big)_{k \in \mathcal{N}(\mathbf{t})}$ forms an integral basis of E over K. We also consider the effect of the action of the Galois group $Gal_{cont}(\mathbf{C}_p/K)$ on our bases. If $t_1, \dots, t_r \in \mathbf{C}_p$ and $\sigma \in Gal_{cont}(\mathbf{C}_p/K)$, then the $r-$tuples $(t_1, \dots, t_r)$ and $(\sigma(t_1), \dots, \sigma(t_r))$ produce the same normalized sequences of polynomials. We will show that a converse also holds, and in order to prove that result we first establish a criterion which uses the p-adic valuation to identify the conjugates of a given element $\mathbf{t} \in \mathbf{C}_p^r$.

2. Admissible polynomials

In what follows K will be a fixed finite extension of $\mathbf{Q}_p$. Denote by v the p-adic valuation on $\mathbf{C}_p$, normalized by $v(p) = 1$. Let π_K be a uniformising element of K. If $e(K/\mathbf{Q}_p)$ denotes the ramification index of K over $\mathbf{Q}_p$, then $v(\pi_K) = \frac{1}{e(K/\mathbf{Q}_p)}$. Next, let us fix an order $\leq$ on $\mathbf{N}^r$ which makes $\mathbf{N}^r$ a well ordered set. One such possible order is to put $\mathbf{m} \leq \mathbf{n}$ provided that $m_1 + \cdots + m_r \leq n_1 + \cdots + n_r$, and to choose the lexicographical order for those $r-$tuples $\mathbf{m}$ for which the total degree $m_1 + \cdots + m_r$ is the same.

Another class of examples of orders is obtained as follows. Let $\eta = (\eta_1, \dots, \eta_r)$, where $\eta_1, \dots, \eta_r$ are positive real numbers, linearly independent over $\mathbf{Q}$. Define the $\eta-$degree of $\mathbf{m}$ to be

$$\deg_\eta \mathbf{m} = \eta_1 m_1 + \cdots + \eta_r m_r \,. \tag{2.1}$$

Here all the $r-$tuples $\mathbf{m} \in \mathbf{N}^r$ have distinct degrees. Then set $\mathbf{m} \leq \mathbf{n}$ if and only if $\deg_\eta \mathbf{m} \leq \deg_\eta \mathbf{n}$.

Let us fix an order on $\mathbf{N}^r$ as above. Arrange the elements of $\mathbf{N}^r$ in increasing oder,

$$\mathbf{m}_0 < \mathbf{m}_1 < \mathbf{m}_2 < \cdots < \mathbf{m}_k < \cdots \,, \tag{2.2}$$

where the inequalities in (2.2) are with respect to this fixed order. Let ϕ be the induced monotonic one-to-one map from $\mathbf{N}$ to $\mathbf{N}^r$, that is, $\phi(k) = \mathbf{m}_k$ for any $k \in \mathbf{N}$. Consider the ring of polynomials in r variables $X_1, \dots, X_r$ over K. If $k \in \mathbf{N}$ and $\phi(k) = (m_1, \dots, m_r) \in \mathbf{N}^r$, we define the degree of the monomial $X_1^{m_1} \cdots X_r^{m_r}$ to be $\deg(X_1^{m_1} \cdots X_r^{m_r}) = k$.

Thus for each $k \in \mathbf{N}$ there exists exactly one monomial of degree k. For any nonzero polynomial $P(X_1, \ldots, X_r) \in K[X_1, \ldots, X_r]$ we define $\deg P(X_1, \ldots, X_r)$ to be the largest of the degrees of its monomials. We put $\deg 0 = -\infty$. One easily sees that

$$\deg(P) = 0 \text{ if and only if } 0 \neq P \text{ is constant,} \tag{2.3}$$

$$\deg(P+Q) \leq \max\{\deg P, \deg Q\}, \text{ with equality if } \deg P \neq \deg Q, \tag{2.4}$$

and

$$\deg(cP) = \deg P \text{ for any } 0 \neq c \in K. \tag{2.5}$$

The leading coefficient in a polynomial $P(X_1, \ldots, X_r)$ is the coefficient corresponding to the monomial of highest degree in $P(X_1, \ldots, X_r)$. A polynomial is said to be monic if its leading coefficient is 1.

In what follows we work with a fixed order on $\mathbf{N}^r$ as above. Let $\mathbf{t} = (t_1, \ldots, t_r) \in \mathbf{C}_p^r$ and let $k \in \mathbf{N}$. We define an *admissible polynomial of degree k for $\mathbf{t}$ over K* to be any monic polynomial $P(X_1, \ldots, X_r) \in K[X_1, \ldots, X_r]$ of degree k such that

$$v(P(t_1, \ldots, t_r)) \geq v(Q(t_1, \ldots, t_r)), \tag{2.6}$$

for any monic polynomial $Q(X_1, \ldots, X_r) \in K[X_1, \ldots, X_r]$ of degree k. A sequence $(f_k)_{k \in \mathbf{N}}$ with the property that for any k, f_k is an admissible polynomial of degree k for $\mathbf{t}$ over K will be called an *admissible sequence of polynomials for $\mathbf{t}$ over K*. The existence of admissible sequences of polynomials for any $\mathbf{t} \in \mathbf{C}_p^r$ follows from the next lemma.

LEMMA 1. *Fix a finite extension K of $\mathbf{Q}_p$ and an order on $\mathbf{N}^r$ as above. Then, for any $\mathbf{t} \in \mathbf{C}_p^r$ and any $k \in \mathbf{N}$ there exists an admissible polynomial of degree k for $\mathbf{t}$ over K.*

Proof. Let $\mathbf{t} = (t_1, \ldots, t_r) \in \mathbf{C}_p^r$ and $k \in \mathbf{N}$. Denote

$$\gamma_k(\mathbf{t}) = \sup\{v(G(t_1, \ldots, t_r)) : G \in K[X_1, \ldots, X_r], G \text{ monic}, \deg G = k\}. \tag{2.7}$$

Here $\gamma_k(\mathbf{t}) \in (-\infty, \infty]$. In order to finish the proof of the lemma we need to show that the supremum on the right side of (2.7) is attained. Let $(\rho_m)_{m \in \mathbf{N}}$ be a strictly increasing sequence of real numbers with $\lim_{m \to \infty} \rho_m = \gamma_k(\mathbf{t})$. For any m, denote

$$\mathcal{F}_m = \{f \in K[X_1, \ldots, X_r] : f \text{ monic}, \deg f = k, v(f(t_1, \ldots, t_r)) \geq \rho_m\}. \tag{2.8}$$

Evidently one has the inclusions $\mathcal{F}_0 \supseteq \mathcal{F}_1 \supseteq \cdots \supseteq \mathcal{F}_m \supseteq \cdots$. Since $\rho_m < \gamma_k(\mathbf{t})$ for any m, it follows that all the sets $\mathcal{F}_m$ are nonempty. For any

nonzero polynomial $f(X_1,\dots,X_r)\in K[X_1,\dots,X_r]$, let $b(f)\in\mathbf{Z}$ denote the smallest integer number for which the polynomial $\pi_K^{b(f)}f(X_1,\dots,X_r)$ belongs to $O_K[X_1,\dots,X_r]$. Note that if $f(X_1,\dots,X_r)$ is monic then $b(f)\geq 0$. Next, for any $m\in\mathbf{N}$ we set

$$b_m=\min\{b(f): f(X_1,\dots,X_r)\in\mathcal{F}_m\}. \tag{2.9}$$

One clearly has $0\leq b_0\leq b_1\leq\cdots\leq b_m\leq\cdots$. We claim that there is a natural number m^* such that

$$b_{m^*}=b_{m^*+1}=\cdots=b_m=\cdots. \tag{2.10}$$

In order to prove the claim, let us choose for any $m\in\mathbf{N}$ a polynomial $f_m(X_1,\dots,X_r)\in\mathcal{F}_m$ for which the minimum is attained on the right side of (2.9). Thus $b(f_m)=b_m$. Denote $g_m=\pi_K^{b_m}f_m$, so that $g_m\in O_K[X_1,\dots,X_r]$ and g_m is primitive for any m. Let us assume that $b_m\to\infty$ as $m\to\infty$. Consider the sequence of polynomials $\big(g_m\big)_{m\in\mathbf{N}}$. Since O_K is compact, there exists a subsequence $\big(g_{m_j}\big)_{j\in\mathbf{N}}$ of $\big(g_m\big)_{m\in\mathbf{N}}$ for which the sequence of coefficients corresponding to any given monomial is convergent. In the limit we obtain a polynomial $g(X_1,\dots,X_r)\in O_K[X_1,\dots,X_r]$, which is also primitive, and hence it is not the zero polynomial. Note that the leading coefficient of g_m equals $\pi_K^{b_m}$, which goes to zero as $m\to\infty$, by the above assumption that $\lim_{m\to\infty}b_m=\infty$. Therefore the degree of $g(X_1,\dots,X_r)$ will be strictly smaller than k. As a consequence, for any $m\in\mathbf{N}$ the polynomial $h_m:=f_m-\pi_K^{-b_m}g$ will be monic and of degree k. On the other hand, along the subsequence $\big(m_j\big)_{j\in\mathbf{N}}$ we have $g_{m_j}(t_1,\dots,t_r)\to g(t_1,\dots,t_r)$. Thus $v(g_{m_j}(t_1,\dots,t_r))\to v(g(t_1,\dots,t_r))$ as $j\to\infty$. Since

$$v(g_{m_j}(t_1,\dots,t_r))=v(\pi_K^{b_{m_j}}f_m(t_1,\dots,t_r))\geq\frac{b_{m_j}}{e(L/K)}+\rho_{m_j}, \tag{2.11}$$

and since the right side of (2.11) goes to infinity as $j\to\infty$, we deduce that $g(t_1,\dots,t_r)=0$. Therefore

$$v(h_m(t_1,\dots,t_r))=v(f_m(t_1,\dots,t_r))\geq\rho_m, \tag{2.12}$$

for any $m\in\mathbf{N}$. Choose now a j large enough so that each coefficient of the polynomial $\Big(g_{m_j}(X_1,\dots,X_r)-g(X_1,\dots,X_r)\Big)$ is divisible by π_K. Then $\pi_K^{b_{m_j}-1}h_{m_j}=\frac{1}{\pi_K}(g_{m_j}-g)\in O_K[X_1,\dots,X_r]$. This contradicts the definition of b_{m_j}, since h_{m_j} is monic, of degree k, and by (2.12) it follows that $h_{m_j}\in\mathcal{F}_{m_j}$. This proves (2.10). Next, from (2.10) and the fact that $\pi^{-b_{m^*}}O_K$ is compact, it follows that if we choose for each

$m \geq m^*$ a polynomial $f_m \in \mathcal{F}_m$ satisfying $b(f_m) = b_m = b_{m^*}$, there is a subsequence $\left(f_{m_j}\right)_{j\in\mathbf{N}}$ of $\left(f_m\right)_{m\in\mathbf{N}}$ which converges to a polynomial $f \in K[X_1, \ldots, X_r]$. This polynomial f is monic, of degree k, and one has $\lim_{j\to\infty} f_{m_j}(t_1, \ldots, t_r) = f(t_1, \ldots, t_r)$. Since $v(f_{m_j}(t_1, \ldots, t_r)) \geq \rho_{m_j}$ for any j, we see that $v(f(t_1, \ldots, t_r)) = \gamma_k(\mathbf{t})$, and this completes the proof of the lemma.

3. Integral bases

Let us fix K and an order on $\mathbf{N}^r$ as before, and choose a $\mathbf{t} = (t_1, \ldots, t_r) \in \mathbf{C}_p^r$. Let $\left(f_k\right)_{k\in\mathbf{N}}$ be an admissible sequence of polynomials for $\mathbf{t}$ over K, and let $\gamma_k(\mathbf{t})$ be defined by (2.7). Thus

$$v(f_k(t_1, \ldots, t_r)) = \gamma_k(\mathbf{t}), \tag{3.1}$$

for any $k \in \mathbf{N}$. Denote

$$\mathcal{N}(\mathbf{t}) = \{k \in \mathbf{N} : \gamma_k(\mathbf{t}) < \infty\}. \tag{3.2}$$

Thus $f_k(t_1, \ldots, t_r) \neq 0$ for any $k \in \mathcal{N}(\mathbf{t})$, and $f_k(t_1, \ldots, t_r) = 0$ for any $k \in \mathbf{N} \setminus \mathcal{N}(\mathbf{t})$. Next, for any $k \in \mathcal{N}(\mathbf{t})$ let $l_k = [e(K/\mathbf{Q}_p) \cdot \gamma_k(\mathbf{t})] \in \mathbf{Z}$, where $[\cdot]$ denotes the integer part function. Then set

$$M_k(X_1, \ldots, X_r) = \pi_K^{-l_k} f_k(X_1, \ldots, X_r) \in K[X_1, \ldots, X_r]. \tag{3.3}$$

Note that $v(M_k(t_1, \ldots, t_r)) \geq 0$ while $v(\frac{1}{\pi_K} M_k(t_1, \ldots, t_r)) < 0$, for any $k \in \mathcal{N}(\mathbf{t})$. We call the sequence $\left(M_k(X_1, \ldots, X_r)\right)_{k\in\mathcal{N}(\mathbf{t})}$ a *normalized sequence of polynomials for* $\mathbf{t}$ *over* K. Here the set $\mathcal{N}(\mathbf{t})$ may be finite or infinite. Let $E \subseteq \mathbf{C}_p$ denote the completion of the field $K(t_1, \ldots, t_r)$, and $O_E = \{z \in E : v(z) \geq 0\}$ the ring of integers of E. We show that for any normalized sequence $\left(M_k(X_1, \ldots, X_r)\right)_{k\in\mathcal{N}(\mathbf{t})}$ for $\mathbf{t}$ over K, the sequence $\left(M_k(t_1, \ldots, t_r)\right)_{k\in\mathcal{N}(\mathbf{t})}$ forms an integral basis of E over K.

THEOREM 1. *Let K be a finite extension of $\mathbf{Q}_p$ and fix an order on $\mathbf{N}^r$ which makes $\mathbf{N}^r$ a well ordered set. Choose a $\mathbf{t} = (t_1, \ldots, t_r) \in \mathbf{C}_p^r$ and let E denote the closure of the field $K(t_1, \ldots, t_r)$ in $\mathbf{C}_p$. Then for any normalized sequence of polynomials $\left(M_k(X_1, \ldots, X_r)\right)_{k\in\mathcal{N}(\mathbf{t})}$ for $\mathbf{t}$ over K, the sequence $\left(M_k(t_1, \ldots, t_r)\right)_{k\in\mathcal{N}(\mathbf{t})}$ forms an integral basis of E over K. More precisely:*
(i) *For any $y \in E$ there exists a unique sequence $\left(c_k\right)_{k\in\mathcal{N}(\mathbf{t})}$ in K, with $c_k \to 0$ as $k \to \infty$, such that $y = \sum_k c_k M_k(t_1, \ldots, t_r)$.*

(ii) *Let* $y \in E$, $y = \sum_k c_k M_k(t_1, \dots, t_r)$, *with* $c_k \in K$ *for all* $k \in \mathcal{N}(\mathbf{t})$ *and* $c_k \to 0$ *as* $k \to \infty$. *Then* $v(y) = \min_k v(c_k M_k(t_1, \dots, t_r))$.
(iii) *Let* $y \in E$. *Then* $y \in O_E$ *if and only if* $y = \sum_k c_k M_k(t_1, \dots, t_r)$ *with* $c_k \in O_K$ *for all* $k \in \mathcal{N}(\mathbf{t})$ *and* $c_k \to 0$ *as* $k \to \infty$.

Proof. It is easy to see that (iii) follows from (i), (ii) and the fact that for any $k \in \mathcal{N}(\mathbf{t})$ and $c \in K$, one has $cM_k(t_1, \dots, t_r) \in O_E$ if and only if $c \in O_K$. We now proceed to prove (ii). Let $y \in E$, $y = \sum_k c_k M_k(t_1, \dots, t_r)$ with $c_k \in K$ for all $k \in \mathcal{N}(\mathbf{t})$ and $c_k \to 0$ as $k \to \infty$. We need to show that

$$v(y) = \min_{k \in \mathcal{N}(\mathbf{t})} v(c_k M_k(t_1, \dots, t_r)). \tag{3.4}$$

Note that the minimum is attained on the right side of (3.4) since $v(c_k) \to \infty$ as $k \to \infty$. Let $d \in \mathcal{N}(\mathbf{t})$ be the largest natural number for which $v(c_d M_d(t_1, \dots, t_r)) = \min_k v(c_k M_k(t_1, \dots, t_r))$. We clearly have $v(y) \geq v(c_d M_d(t_1, \dots, t_r))$. Let us assume that $v(y) > v(c_d M_d(t_1, \dots, t_r))$. Write y in the form $y = y_1 + y_2$, where $y_1 = \sum_{k \leq d} c_k M_k(t_1, \dots, t_r)$ and $y_2 = \sum_{k > d} c_k M_k(t_1, \dots, t_r)$. Since $v(c_k M_k(t_1, \dots, t_r)) > v(c_d M_d(t_1, \dots, t_r))$ for any $k > d$, it follows that $v(y_2) > v(c_d M_d(t_1, \dots, t_r))$. Thus $v(y_1) \geq \min\{v(y), v(y_2)\} > v(c_d M_d(t_1, \dots, t_r))$. Consider the polynomial

$$G(X_1, \dots, X_r) = \frac{\pi_K^{l_d}}{c_d} \sum_{k \leq d} c_k M_k(X_1, \dots, X_r) \in K[X_1, \dots, X_r]. \tag{3.5}$$

Let us remark that $G(X_1, \dots, X_r)$ is monic, of degree d, and

$$v(G(t_1, \dots, t_r)) = v\Big(\frac{\pi_K^{l_d}}{c_d} y_1\Big) > v(\pi_K^{l_d} M_d(t_1, \dots, t_r)). \tag{3.6}$$

This contradicts the fact that $\pi_K^{l_d} M_d(X_1, \dots, X_r)$ is an admissible polynomial of degree d for $\mathbf{t}$ over K. Therefore (3.4) holds true, and this proves (ii). It remains to prove (i).

Let $y \in E$. We want to find a sequence $(c_k)_{k \in \mathcal{N}(\mathbf{t})}$ in K with $c_k \to 0$ as $k \to \infty$, such that $y = \sum_k c_k M_k(t_1, \dots, t_r)$. By Theorem 7 from [2] we know that the ring $K[t_1, \dots, t_r]$ is dense in the closure E of the field $K(t_1, \dots, t_r)$. Choose a sequence of polynomials $(P_m(X_1, \dots, X_r))_{m \in \mathbf{N}}$ in $K[X_1, \dots, X_r]$ such that

$$P_m(t_1, \dots, t_r) \to y \text{ as } m \to \infty. \tag{3.7}$$

For each $m \in \mathbf{N}$ denote $d_m = \deg P_m(X_1, \dots, X_r)$. Let $(f_k)_{k \in \mathbf{N}}$ be an admissible sequence of polynomials for $\mathbf{t}$ over K, with $f_k(X_1, \dots, X_r) =$

$\pi_K^{l_k} M_k(X_1, \ldots, X_r)$ for any $k \in \mathcal{N}(\mathbf{t})$, while for $k \notin \mathcal{N}(\mathbf{t})$ we allow f_k to be any admissible polynomial of degree k for $\mathbf{t}$ over K. Next, we write each polynomial P_m as a finite linear combination of our admissible sequence of polynomials $(f_k)_{k \in \mathbf{N}}$,

$$P_m(X_1, \ldots, X_r) = \sum_{j=0}^{d_m} a_{m,j} f_j(X_1, \ldots, X_r). \tag{3.8}$$

Since $f_j(t_1, \ldots, t_r) = 0$ for $j \notin \mathcal{N}(\mathbf{t})$, from (3.8) we derive

$$P_m(t_1, \ldots, t_r) = \sum_{\substack{0 \le j \le d_m \\ j \in \mathcal{N}(\mathbf{t})}} a_{m,j} f_j(t_1, \ldots, t_r). \tag{3.9}$$

We put (3.9) in the form

$$P_m(t_1, \ldots, t_r) = \sum_{j \in \mathcal{N}(\mathbf{t})} c_{m,j} M_j(t_1, \ldots, t_r), \tag{3.10}$$

for any $m \in \mathbf{N}$, where $c_{m,j} = \pi_K^{l_j} a_{m,j}$ for $j \le d_m$ and $c_{m,j} = 0$ for $j > d_m$. The sequence $(P_m(t_1, \ldots, t_r))_{m \in \mathbf{N}}$ being convergent, by (ii) it follows that for each $j \in \mathcal{N}(\mathbf{t})$ the sequence $(c_{m,j})_{m \in \mathbf{N}}$ is a Cauchy sequence in K. Let $c_j = \lim_{m \to \infty} c_{m,j} \in K$. We claim that $c_j \to 0$ as $j \to \infty$. Indeed, fix an $\epsilon > 0$ and choose an $m_\epsilon \in \mathbf{N}$ such that $v(y - P_m(t_1, \ldots, t_r)) \ge \frac{1}{\epsilon}$ for any $m \ge m_\epsilon$. Then for any $j \in \mathcal{N}(\mathbf{t})$ and any $m, n \ge m_\epsilon$ we have on one hand

$$\begin{aligned} & v(P_m(t_1, \ldots, t_r) - P_n(t_1, \ldots, t_r)) \\ \ge\ & \min\{v(y - P_m(t_1, \ldots, t_r)), v(y - P_n(t_1, \ldots, t_r))\} \ge \frac{1}{\epsilon}, \end{aligned} \tag{3.11}$$

and on the other hand we have

$$\begin{aligned} & v(P_m(t_1, \ldots, t_r) - P_n(t_1, \ldots, t_r)) \\ =\ & \min_{k \in \mathcal{N}(\mathbf{t})} v((c_{m,k} - c_{n,k}) M_k(t_1, \ldots, t_r)) \\ \le\ & v(c_{m,j} - c_{n,j}) + v(M_j(t_1, \ldots, t_r)) \\ <\ & v(c_{m,j} - c_{n,j}) + \frac{1}{e(K/Q_p)}. \end{aligned} \tag{3.12}$$

Combining (3.11) and (3.12) we find that

$$v(c_{m,j} - c_{n,j}) > \frac{1}{\epsilon} - \frac{1}{e(K/Q_p)}. \tag{3.13}$$

If we let $n \to \infty$ while keeping j and m fixed, from (3.13) it follows that

$$v(c_{m,j} - c_j) > \frac{1}{\epsilon} - \frac{1}{e(K/\mathbf{Q}_p)}, \tag{3.14}$$

for any $m \geq m_\epsilon$ and any $j \in \mathcal{N}(\mathbf{t})$. In particular, for $m = m_\epsilon$ and $j > d_{m_\epsilon}$ one has $c_{m_\epsilon,j} = 0$, and (3.14) implies

$$v(c_j) > \frac{1}{\epsilon} - \frac{1}{e(K/\mathbf{Q}_p)}, \tag{3.15}$$

for any $\epsilon > 0$ and any $j > d_{m_\epsilon}$. This shows that $c_j \to 0$ as $j \to \infty$. Let us consider the element $z \in E$ given by

$$z = \sum_{k \in \mathcal{N}(\mathbf{t})} c_k M_k(t_1, \ldots, t_r). \tag{3.16}$$

Using (ii) it follows from (3.14) that for any $\epsilon > 0$ and any $m \geq m_\epsilon$ one has

(3.17)

$$v(P_m(t_1, \ldots, t_r) - z) = \min_{j \in \mathcal{N}(\mathbf{t})} v((c_{m,j} - c_j) M_j(t_1, \ldots, t_r)) \geq \frac{1}{\epsilon} - \frac{1}{e(K/\mathbf{Q}_p)}.$$

Therefore $P_m(t_1, \ldots, t_r) \to z$ as $m \to \infty$. Comparing this with (3.7) we see that $z = y$, and (3.16) gives the desired expression of y in terms of our sequence $\big(M_k(t_1, \ldots, t_r)\big)_{k \in \mathcal{N}(\mathbf{t})}$. Lastly, the uniqueness of such an expression follows easily from (ii). This completes the proof of the theorem. □

4. Conjugates and normalized sequences of polynomials

We keep the notations from previous sections. Denote as usual the group of continuous automorphisms of $\mathbf{C}_p$ over K by $Gal_{cont}(\mathbf{C}_p/K)$. If $\mathbf{t} = (t_1, \ldots, t_r)$, $\mathbf{t}' = (t'_1, \ldots, t'_r) \in \mathbf{C}_p^r$ and if there exists $\sigma \in Gal_{cont}(\mathbf{C}_p/K)$ such that $\sigma(t_j) = t'_j$ for any $j \in \{1, \ldots, r\}$ we say that $\mathbf{t}$ and $\mathbf{t}'$ are conjugate over K. Note that if $\mathbf{t}$ and $\mathbf{t}'$ are conjugate over K then $\mathcal{N}(\mathbf{t}) = \mathcal{N}(\mathbf{t}')$, and a sequence $\big(M_k(X_1, \ldots, X_r)\big)_{k \in \mathcal{N}(\mathbf{t})}$ is a normalized sequence of polynomials for $\mathbf{t}$ over K if and only if it is a normalized sequence of polynomials for $\mathbf{t}'$ over K. We ask whether a converse of this statement also holds. In order to provide an answer to this question we first prove the following lemma, which generalizes the criterion from Remark 3.6 of [1].

LEMMA 2. *Let* $\mathbf{t} = (t_1, \ldots, t_r), \mathbf{t}' = (t'_1, \ldots, t'_r)$ *be elements of* C_p^r. *Then* $\mathbf{t}$ *and* $\mathbf{t}'$ *are conjugate over* K *if and only if* $v(P(t_1, \ldots, t_r)) = v(P(t'_1, \ldots, t'_r))$ *for any polynomial* $P(X_1, \ldots, X_r) \in K[X_1, \ldots, X_r]$.

Proof. If $\mathbf{t} = (t_1, \ldots, t_r), \mathbf{t}' = (t'_1, \ldots, t'_r)$ are conjugate over K then evidently $P(t_1, \ldots, t_r)$ and $P(t'_1, \ldots, t'_r)$ are conjugate over K, and so they have the same valuation. Conversely, let us assume that $\mathbf{t} = (t_1, \ldots, t_r), \mathbf{t}' = (t'_1, \ldots, t'_r) \in \mathbf{C}_p^r$ are such that $v(P(t_1, \ldots, t_r)) = v(P(t'_1, \ldots, t'_r))$ for any $P(X_1, \ldots, X_r) \in K[X_1, \ldots, X_r]$. We denote by E the closure of the field $K(t_1, \ldots, t_r)$ in $\mathbf{C}_p$, and by E' the closure of $K(t'_1, \ldots, t'_r)$ in $\mathbf{C}_p$. By Theorem 7 from [2] we know that $K[t_1, \ldots, t_r]$ is dense in E and $K[t'_1, \ldots, t'_r]$ is dense in E'. Next, let us consider the canonical morphisms of rings $\phi : K[X_1, \ldots, X_r] \to K[t_1, \ldots, t_r]$ and $\phi' : K[X_1, \ldots, X_r] \to K[t'_1, \ldots, t'_r]$ given by $\phi(P(X_1, \ldots, X_r)) = P(t_1, \ldots, t_r)$ and respectively $\phi'(P(X_1, \ldots, X_r)) = P(t'_1, \ldots, t'_r)$, for any $P(X_1, \ldots, X_r) \in K[X_1, \ldots, X_r]$. Let us observe that

$$\begin{aligned}(4.1)\quad \operatorname{Ker}\phi &= \{P(X_1, \ldots, X_r) \in K[X_1, \ldots, X_r] : v(P(t_1, \ldots, t_r)) = \infty\} \\ &= \{P(X_1, \ldots, X_r) \in K[X_1, \ldots, X_r] : v(P(t'_1, \ldots, t'_r)) = \infty\} = \operatorname{Ker}\phi'.\end{aligned}$$

Therefore one has an isomorphism of rings $\psi : K[t_1, \ldots, t_r] \to K[t'_1, \ldots, t'_r]$, given by $\psi(P(t_1, \ldots, t_r)) = P(t'_1, \ldots, t'_r)$ for any polynomial $P(X_1, \ldots, X_r) \in K[X_1, \ldots, X_r]$. By our assumption on $\mathbf{t}$ and $\mathbf{t}'$, the isomorphism ψ is also an isometry, and so it extends by continuity to an isomorphism $\psi : E \to E'$. We know from Galois theory in $\mathbf{C}_p$, as developed by Tate [11], Sen [9], Ax [3], that the closed subfields of $\mathbf{C}_p$ are in one-to-one correspondence with the subfields of $\bar{K}$. Thus if we take the algebraic part in E and E', say $L = E \cap \bar{K}$ and $L' = E' \cap \bar{K}$, then E and E' can be recovered from the fields L and L' by taking the topological closure in $\mathbf{C}_p$. Now clearly by restriction ψ produces an isomorphism between L and L', which fixes K. We extend this isomorphism to an automorphism σ of $\bar{K}$ over K, and then we extend σ by continuity to an element of $Gal_{cont}(\mathbf{C}_p/K)$, which we continue to denote by σ. Since ψ and σ have the same restriction to L, and since L is dense in E, it follows that the restriction of σ to E coincides with ψ. In particular $\sigma(t_j) = t'_j$ for any $j \in \{1, \ldots, r\}$, and the lemma is proved. □

We are now ready to prove the following result.

THEOREM 2. *Let* K *be a finite extension of* $\mathbf{Q}_p$ *and fix an order on* $\mathbf{N}^r$ *which makes* $\mathbf{N}^r$ *a well ordered set. Let* $\mathbf{t}$ *and* $\mathbf{t}'$ *be elements of* $\mathbf{C}_p^r$ *such that they have a common normalized sequence of polynomials over* K, *and such that for any* $k \in \mathbf{N} \setminus \mathcal{N}(\mathbf{t})$, $\mathbf{t}$ *and* $\mathbf{t}'$ *have a common*

admissible polynomial of degree k over K. Then $\mathbf{t}$ and $\mathbf{t}'$ are conjugate over K.

Let us remark that in the statement of Theorem 2 it is not enough to assume that $\mathbf{t}$, $\mathbf{t}'$ have a common normalized sequence of polynomials over K, in order to conclude that they are conjugate over K. For instance, if $r = 1$ and t is a root of an Eisenstein polynomial $P(X) = X^d + a_1 X^{d-1} + \cdots + a_{d-1}X + a_d \in O_K[X]$, then, with the natural order on $\mathbf{N}$, $\mathcal{N}(\mathbf{t}) = \{0, 1, \ldots, d-1\}$, and a normalized sequence of polynomials for t over K is given by $M_k(X) = X^k$, $k \in \{0, 1, \ldots, d-1\}$. Thus if t' is a root of another Eisenstein polynomial of same degree d over K, then t, t' will not be conjugate over K while they do have a common normalized sequence of polynomials $\left(X^k\right)_{0 \le k \le d-1}$. In case t is transcendental over K, or more generally in case $\mathbf{t} = (t_1, \ldots, t_r) \in \mathbf{C}_p^r$ with $t_1, \ldots, t_r$ algebraically independent over K, the set $\mathcal{N}(\mathbf{t})$ will coincide with $\mathbf{N}$, and Theorem 2 reduces to the following corollary.

COROLLARY 1. *Let K be a finite extension of $\mathbf{Q}_p$ and fix an order on $\mathbf{N}^r$ which makes $\mathbf{N}^r$ a well ordered set. Let $\mathbf{t} = (t_1, \ldots, t_r) \in \mathbf{C}_p^r$ with $t_1, \ldots, t_r$ algebraically independent over K. If $\mathbf{t}' \in \mathbf{C}_p^r$ is such that $\mathbf{t}$, $\mathbf{t}'$ have a common normalized sequence of polynomials over K, then $\mathbf{t}$ and $\mathbf{t}'$ are conjugate over K.*

Proof of Theorem 2. Let $\mathbf{t}$, $\mathbf{t}' \in \mathbf{C}_p^r$ be as in the statement of the theorem. Let $\left(M_k(X_1, \ldots, X_r)\right)_{k \in \mathcal{N}(\mathbf{t})}$ be a common normalized sequence of polynomials for both $\mathbf{t}$ and $\mathbf{t}'$ over K, and choose for any $k \in \mathbf{N} \setminus \mathcal{N}(\mathbf{t})$ a common admissible polynomial f_k of degree k for both $\mathbf{t}$ and $\mathbf{t}'$ over K. For any $j \in \mathcal{N}(\mathbf{t})$, the leading coefficient of $M_j(X_1, \ldots, X_r)$ will equal $\pi_K^{-l_j}$ for some $l_j \in \mathbf{Z}$. Then $f_j(X_1, \ldots, X_r) := \pi_K^{l_j} M_j(X_1, \ldots, X_r)$ will be a common admissible polynomial of degree j for both $\mathbf{t}$ and $\mathbf{t}'$ over K. We have then a common admissible sequence of polynomials $\left(f_k\right)_{k \in \mathbf{N}}$ for both $\mathbf{t}$ and $\mathbf{t}'$ over K. Take now an arbitrary polynomial $g(X_1, \ldots, X_r) \in K[X_1, \ldots, X_r]$ and write it as a linear combination

$$g(X_1, \ldots, X_r) = \sum_{j=0}^{d} a_j f_j(X_1, \ldots, X_r), \tag{4.2}$$

where $d = \deg g(X_1, \ldots, X_r)$. Since $f_j(t_1, \ldots, t_r) = f_j(t_1', \ldots, t_r') = 0$ for any $j \in \mathbf{N} \setminus \mathcal{N}(\mathbf{t})$, from (4.2) it follows that

$$g(t_1, \ldots, t_r) = \sum_{\substack{0 \le j \le d \\ j \in \mathcal{N}(\mathbf{t})}} c_j M_j(t_1, \ldots, t_r), \tag{4.3}$$

and

$$g(t'_1,\dots,t'_r)=\sum_{\substack{0\le j\le d\\ j\in\mathcal{N}(\mathbf{t})}} c_jM_j(t'_1,\dots,t'_r), \tag{4.4}$$

where $c_j=\pi_K^{l_j}a_j$ for $0\le j\le d$, $j\in\mathcal{N}(\mathbf{t})$. Recall that for any j one has $0\le v(M_j(t_1,\dots,t_r)),v(M_j(t'_1,\dots,t'_r))<v(\pi_K)=1/e(K/Q_p)$. Therefore, by combining (4.3), (4.4) with Theorem 1, (ii) we find that

$$\begin{aligned}\min_{\substack{0\le j\le d\\ j\in\mathcal{N}(\mathbf{t})}} v(c_j) &\le \min_{\substack{0\le j\le d\\ j\in\mathcal{N}(\mathbf{t})}} v(c_jM_j(t_1,\dots,t_r))\\ &= v(g(t_1,\dots,t_r))<\frac{1}{e(K/\mathbf{Q}_p)}+\min_{\substack{0\le j\le d\\ j\in\mathcal{N}(\mathbf{t})}} v(c_j),\end{aligned} \tag{4.5}$$

and similarly

$$\begin{aligned}\min_{\substack{0\le j\le d\\ j\in\mathcal{N}(\mathbf{t})}} v(c_j) &\le \min_{\substack{0\le j\le d\\ j\in\mathcal{N}(\mathbf{t})}} v(c_jM_j(t'_1,\dots,t'_r))\\ &= v(g(t'_1,\dots,t'_r))<\frac{1}{e(K/\mathbf{Q}_p)}+\min_{\substack{0\le j\le d\\ j\in\mathcal{N}(\mathbf{t})}} v(c_j).\end{aligned} \tag{4.6}$$

By (4.5) and (4.6) it follows that

$$\left|v(g(t_1,\dots,t_r))-v(g(t'_1,\dots,t'_r))\right|<\frac{2}{e(K/\mathbf{Q}_p)}, \tag{4.7}$$

for any $g\in K[X_1,\dots,X_r]$. We now fix a polynomial $P(X_1,\dots,X_r)\in K[X_1,\dots,X_r]$ and apply (4.7) with $g=P^n$ for some large natural number n. We find that

$$\begin{aligned}\frac{2}{e(K/\mathbf{Q}_p)} &> \left|v(g(t_1,\dots,t_r))-v(g(t'_1,\dots,t'_r))\right|\\ &= n\left|v(P(t_1,\dots,t_r))-v(P(t'_1,\dots,t'_r))\right|.\end{aligned} \tag{4.8}$$

Letting $n\to\infty$ in (4.8) we obtain

$$v(P(t_1,\dots,t_r))=v(P(t'_1,\dots,t'_r)). \tag{4.9}$$

Since (4.9) holds for any polynomial $P(X_1,\dots,X_r)\in K[X_1,\dots,X_r]$, from Lemma 2 it follows that $\mathbf{t}$ and $\mathbf{t}'$ are conjugate over K, and this completes the proof of the theorem.

References

[1] V. Alexandru, N. Popescu and A. Zaharescu, *On the closed subfields of* $\mathbf{C}_p$, J. Number Theory **68** (1998), no. 2, 131–150.

[2] V. Alexandru, N. Popescu and A. Zaharescu, *The generating degree of C_p*, Canad. Math. Bull. **44** (2001), no. 1, 3–11.
[3] J. Ax, *Zeros of Polynomials Over Local Fields. The Galois Action*, J. Algebra **15** (1970), 417–428.
[4] J. Coates and R. Greenberg, *Kummer theory for abelian varieties over local fields*, Invent. Math. **124** (1996), no. 1-3, 129–174.
[5] A. Iovita and A. Zaharescu, *Galois theory of B_{dR}^{+}*, Compositio Math. **117** (1999), no. 1, 1–31.
[6] K. Ota, *On saturated distinguished chains over a local field*, J. Number Theory **79** (1999), no. 2, 217–248.
[7] A. Popescu, N. Popescu, M. Vajaitu and A. Zaharescu, *Chains of metric invariants over a local field*, Acta Arith. **103** (2002), no. 1, 27–40.
[8] N. Popescu and A. Zaharescu, *On the structure of the irreducible polynomials over local fields*, J. Number Theory **52** (1995), no. 1, 98–118.
[9] S. Sen, *On automorphisms of local fields*, Ann. of Math. (2) **90** (1969), 33–46.
[10] J. P. Serre, *Local fields*, Graduate Texts in Mathematics, 67, Springer-Verlag, New York-Berlin, 1979.
[11] J. Tate, *p – divisible groups*, 1967 Proc. Conf. Local Fields (Driebergen, 1966) pp. 158–183 Springer, Berlin.

Department of Mathematics, University of Illinois at Urbana-Champaign, 1409 W. Green Street, Urbana, IL, 61801, USA
E-mail: zaharesc@math.uiuc.edu