J. Math. Kyoto Univ. (JMKYAZ)
43-1 (2003), 125–137

Good elements and metric invariants in B_{dR}^{+}

By

Victor Alexandru, Nicolae Popescu and Alexandru Zaharescu

Abstract

Let p be a prime, $\mathbb{Q}_p$ the field of p-adic numbers and $\bar{\mathbb{Q}}_p$ a fixed algebraic closure of $\mathbb{Q}_p$. B_{dR}^{+} is the ring of p-adic periods of algebraic varieties over p-adic fields introduced by Fontaine. For each n one defines a canonical valuation w_n on $\bar{\mathbb{Q}}_p$ such that B_{dR}^{+}/I^n becomes the completion of $\bar{\mathbb{Q}}_p$ with respect to w_n, where I is the maximal ideal of B_{dR}^{+}. An element $\alpha \in \bar{\mathbb{Q}}_p^*$ is said to be good at level n if $w_n(\alpha) = v(\alpha)$ where v denotes the p-adic valuation on $\bar{\mathbb{Q}}_p$. The set $\mathcal{G}_n$ of good elements at level n is a subgroup of $\bar{\mathbb{Q}}_p^*$. We prove that each quotient group $\bar{\mathbb{Q}}_p^*/\mathcal{G}_n$ is a torsion group and that each quotient $\mathcal{G}_1/\mathcal{G}_n$ is a p-group. We also show that a certain sequence of metric invariants $\{l_n(Z)\}_{n\in\mathbb{N}}$ associated to an element $Z \in B_{dR}^{+}$, is constant.

1. Introduction

Let p be a prime number, $\mathbb{Q}_p$ the field of p-adic numbers, $\bar{\mathbb{Q}}_p$ a fixed algebraic closure of $\mathbb{Q}_p$ and $\mathbb{C}_p$ the completion of $\bar{\mathbb{Q}}_p$ with respect to the unique extension of the p-adic valuation v on $\mathbb{Q}_p$. B_{dR}^{+} denotes the ring of p-adic periods of algebraic varieties defined over local (p-adic) fields as considered by J.-M. Fontaine in [Fo]. It is a topological local ring with residue field $\mathbb{C}_p$ (see the section Notations) and it is endowed with a canonical, continuous action of $G\colon = \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. Let I be its maximal ideal and let $B_n\colon = B_{dR}^{+}/I^n$. Then B_{dR}^{+} (and B_n for each $n \geq 1$) is canonically a $\overline{\mathbb{Q}}_p$-algebra and moreover $\overline{\mathbb{Q}}_p$ is dense in B_{dR}^{+} (and in each B_n respectively) if we consider the "canonical topology" on B_{dR}^{+} which is finer than the I-adic topology (see [F-C]).

In [I-Z1] a canonical sequence of valuations $\{w_n\}_n$ on $\bar{\mathbb{Q}}_p$ is defined such that for each n, w_n induces the canonical topology in B_n, thus B_n becomes the completion of $\bar{\mathbb{Q}}_p$ with respect to w_n. Naturally, one is more interested in B_{dR}^{+} itself than in the B_n's and for this reason it would be useful to know how the topology on $\bar{\mathbb{Q}}_p$ induced by w_n is changing as $n \to \infty$.

Let $\alpha \in \bar{\mathbb{Q}}_p^*$. From the definition of the valuations w_n we know that

$$v(\alpha) \geq w_1(\alpha) \geq w_2(\alpha) \geq \cdots \geq w_n(\alpha) \geq \cdots .$$

2000 *Mathematics Subject Classification(s).* 11S99

Received March 26, 2001
Revised April 8, 2002

We say that α is "good" at level n if $w_n(\alpha) = v(\alpha)$. Let $\mathcal{G}_n$ be the set of good elements of $\bar{\mathbb{Q}}_p^*$ at level n. We will see that each $\mathcal{G}_n$ is a subgroup of $\bar{\mathbb{Q}}_p^*$. Therefore we have a filtration

$$\bar{\mathbb{Q}}_p^* \supseteq \mathcal{G}_1 \supseteq \mathcal{G}_2 \supseteq \cdots \supseteq \mathcal{G}_n \supseteq \cdots .$$

Our object in this paper is to study how far is a given element α of $\bar{\mathbb{Q}}_p^*$ from being good at various levels. With this in mind we study the structure of the quotient groups $\mathcal{H}_n := \bar{\mathbb{Q}}_p^*/\mathcal{G}_n$. We prove that one can raise any α to a certain power to make it good at a given level n, in other words one has the following:

Theorem 1. *For any $n \geq 1$, $\mathcal{H}_n$ is a torsion group.*

The structure of $\mathcal{H}_1$ is easily described : one has a canonical isomorphism

$$\mathcal{H}_1 \cong \mathbb{Q}/\mathbb{Z}.$$

In what follows we are mainly concerned with the quotients

$$\mathrm{Ker}(\mathcal{H}_n \to \mathcal{H}_1) \cong \mathcal{G}_1/\mathcal{G}_n.$$

We will prove the following:

Theorem 2. *For any $n \geq 2$ the quotient $\mathcal{G}_1/\mathcal{G}_n$ is a p-group.*

As an application of the above results we answer a question raised in [I-Z2] concerning certain metric invariants for elements in B_{dR}^+. As was pointed out in [I-Z2], although the topology on B_{dR}^+ does not come from a canonical metric the B_n's do have canonical metric structures. This shows us a way to obtain metric invariants for elements in B_{dR}^+, by sending them canonically to any B_n and recovering various metric invariants from those metric spaces.

In particular, for any element Z in B_{dR}^+ whose projection in $\mathbb{C}_p$ is transcendental over $\mathbb{Q}_p$ one defines at each level $n \geq 1$ a certain metric invariant $l_n(Z) \in \mathbb{R} \cup \{\infty\}$ of Z (see Section 4 below). The question is to describe for a fixed Z the behavior of the sequence $\{l_n(Z)\}_{n\in\mathbb{N}}$. One has the following rather surprising:

Theorem 3. *For any element Z in B_{dR}^+ whose projection in $\mathbb{C}_p$ is transcendental over $\mathbb{Q}_p$ the sequence $\{l_n(Z)\}_{n\in\mathbb{N}}$ is constant*:

$$l_1(Z) = l_2(Z) = \cdots = l_n(Z) = \cdots .$$

We obtain in this way a metric invariant $l(Z) = l_n(Z)$ for any $n \geq 1$ which depends on Z only.

Acknowledgements. We are very grateful to the referee who provided us with the simpler approach described in the last section of the paper.

2. Notations, Definitions and Results

Let p be a prime number, $K = \mathbb{Q}_p^{ur}$ the maximal unramified extension of $\mathbb{Q}_p, \overline{K}$ a fixed algebraic closure of K and $\mathbb{C}_p$ the completion of $\overline{K}$ with respect to the unique extension v of the p-adic valuation on $\mathbb{Q}_p$ (normalized such that $v(p) = 1$). All the algebraic extensions of K considered in this paper will be contained in $\overline{K}$. Let L be such an algebraic extension. We denote by $G_L\colon = \mathrm{Gal}(\overline{K}/L)$, $\hat{L}$ the (topological) closure of L in $\mathbb{C}_p$, O_L the ring of integers in L and m_L its maximal ideal. If $K \subset L \subset F \subset \overline{K}$, and F is a finite extension of L, $\Delta_{F/L}$ denotes the different of F over L.

If A and B are commutative rings and $\phi\colon A \to B$ is a ring homomorphism we denote by $\Omega_{B/A}$ the B-module of Kähler differentials of B over A, and $d\colon B \to \Omega_{B/A}$ the structural derivation.

Let A be a Banach space whose norm is given by the valuation w and suppose that the sequence $\{a_m\}$ converges in A to some α. We will write this: $a_m \stackrel{w}{\to} \alpha$.

We now recall some of the main results and definitions from [Fo], [F-C] and [I-Z1]. We first recall the construction of B_{dR}^+, which is due to J.-M. Fontaine in [Fo]. Let R denote the set of sequences $x = (x^{(n)})_{n\geq 0}$ of elements of $O_{\mathbb{C}_p}$ which verify the relation $(x^{(n+1)})^p = x^{(n)}$. Let's define: $v_R(x)\colon = v(x^{(0)})$, $x + y = s$ where $s^{(n)} = \lim_{n\to\infty}(x^{(n+m)} + y^{(n+m)})^{p^m}$ and $xy = t$ where $t^{(n)} = x^{(n)}y^{(n)}$. With these operations R becomes a perfect ring of characteristic p on which v_R is a valuation. R is complete with respect to v_R. Let $W(R)$ be the ring of Witt vectors with coefficients in R and if $x \in R$ we denote by $[x]$ its Teichmüller representative in $W(R)$. Denote by θ the homomorphism $\theta\colon W(R) \to O_{\mathbb{C}_p}$ which sends $(x_0, x_1, \ldots, x_n, \ldots)$ to $\sum_{n=0}^{\infty} p^n x_n^{(n)}$. Then θ is surjective and its kernel is principal. Let also θ denote the map $W(R)[p^{-1}] \to \mathbb{C}_p$. We denote $B_{dR}^+\colon = \lim_{\leftarrow} W(R)[p^{-1}]/(\mathrm{Ker}(\theta))^n$. Then θ extends to a continuous, surjective ring homomorphism $\theta = \theta_{dR}\colon B_{dR}^+ \to \mathbb{C}_p$ and we denote $I\colon = \mathrm{Ker}(\theta_{dR})$ and $I_+\colon = I \bigcap W(R)$. Let $\epsilon = (\epsilon^{(n)})_{n\geq 0}$ be an element of R, where $\epsilon^{(n)}$ is a primitive p^n-th root of unity such that $\epsilon^{(0)} = 1$ and $\epsilon^{(1)} \neq 1$. Then the power series

$$\sum_{n=1}^{\infty}(-1)^{n-1}([\epsilon] - 1)^n/n$$

converges in B_{dR}^+, and its sum is denoted by $t\colon = \log[\epsilon]$. It is proved in [Fo] that t is a generator of the ideal I, and as $G_K\colon = \mathrm{Gal}(\overline{K}/K)$ acts on t by multiplication with the cyclotomic character, we have $I^n/I^{n+1} \cong \mathbb{C}_p(n)$, where the isomorphism is $\mathbb{C}_p$-linear and G_K-equivariant. Therefore for each integer $n \geq 2$, if we denote by $B_n\colon = B_{dR}^+/I^n$ we have an exact sequence of G_K-equivariant homomorphisms

$$0 \to J_{n+1} \to B_{n+1} \stackrel{\phi_{n+1}}{\to} B_n \to 0,$$

where $J_{n+1} \cong I^n/I^{n+1} \cong \mathbb{C}_p(n)$. This exact sequence is called "the fundamental exact sequence". We denote by $\theta_n\colon B_{dR}^+ \to B_n\colon = B_{dR}^+/I^n$ and by $\eta_n\colon B_n \to \mathbb{C}_p$ the canonical projections induced by θ.

Let us now review Colmez's differential calculus with algebraic numbers as in the Appendix of [F-C]. We should point out that as our K is unramified over $\mathbb{Q}_p$ and so $W(R)$ is canonically an O_K as well as an $O_{\hat{K}}$-algebra, we'll work with $W(R)$ instead of A_{inf}. For each nonnegative integer k, we set $A^k_{inf} \colon = W(R)/I_+^{k+1}$. We define recurrently the sequences of subrings $O^{(k)}_{\overline{K}}$ of $O_{\overline{K}}$ and of $O_{\overline{K}}$-modules $\Omega^{(k)}$ setting: $O^{(0)}_{\overline{K}} = O_{\overline{K}}$ and if $k \geq 1$ $\Omega^{(k)} \colon = O_{\overline{K}} \otimes_{O^{(k-1)}_{\overline{K}}} \Omega^1_{O^{(k-1)}_{\overline{K}}/O_K}$ and $O^{(k)}_{\overline{K}}$ is the kernel of the canonical derivation $d^{(k)} \colon O^{(k-1)}_{\overline{K}} \to \Omega^{(k)}$. Then we have

Theorem 4 (Colmez, Appendice of [F-C], Théorème 1)**.** (i) *If $k \in \mathbf{N}$, then $O^{(k)}_{\overline{K}} = \overline{K} \bigcap (W(R) + I^{k+1})$ and for all $n \in \mathbf{N}$ the inclusion of $O^{(k)}_{\overline{K}}$ in $W(R) + I^{k+1}$ induces an isomorphism*

$$A^k_{inf}/p^n A^k_{inf} \cong O^{(k)}_{\overline{K}}/p^n O^{(k)}_{\overline{K}}.$$

(ii) *If $k \geq 1$, then $d^{(k)}$ is surjective and $\Omega^{(k)} \cong (\overline{K}/\mathbf{a}^k)(k)$, where $\mathbf{a}$ is the fractional ideal of $\overline{K}$ whose inverse is the ideal generated by $\epsilon^{(1)} - 1$ (recall $\epsilon^{(1)}$ is a fixed primitive p-th root of unity).*

Some consequences of this theorem are gathered in the following

Corollary 5. (i) *$A^n_{inf} \cong \overset{\lim}{\leftarrow} (O^{(n)}_{\overline{K}}/p^i O^{(n)}_{\overline{K}})$ and $A^n_{inf} \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong B_{n+1}$ for all $n \geq 0$.*
(ii) *$\Omega^{(n)}$ is a p-divisible and a p-torsion $O_{\overline{K}}$-module.*

In [I-Z1] a sequence $\{w_n\}_n$ of valuations on $\overline{K}$ is defined. We recall the definition and their main properties. For each $n \geq 1$ let $O^{(n)}_{\overline{K}}$ be the subring of $O_{\overline{K}}$ defined above. For $a \in \overline{K}^*$ we define

$$w_n(a) \colon = \max\{m \in \mathbf{Z} | a \in p^m O^{(n-1)}_{\overline{K}}\}.$$

In particular when $n = 1$ one has $w_1(a) = [v(a)]$, where [ ] denotes the integer part function.

Properties of w_n.

a) $w_n(a+b) \geq \min(w_n(a), w_n(b))$ and if $w_n(a) \neq w_n(b)$ then we have equality, for all $a, b \in \overline{K}$.

b) $w_n(ab) \geq w_n(a) + w_n(b)$ for all a, b.

c) $w_n(a) = \infty$ if and only if $a = 0$.

d) $v(a) \geq w_{n-1}(a) \geq w_n(a)$ for all $a \in \overline{K}$ and $n \geq 2$.

e) For each $n \geq 1$ the completion of $\overline{K}$ with respect to w_n is canonically isomorphic to B_n.

f) For each $n \geq 1$, $\sigma \in \mathrm{Gal}(\overline{K}/K)$ and $a \in \overline{K}$ we have $w_n(\sigma(a)) = w_n(a)$.

Remark. If we define the norm $\|a\|_n\colon = p^{-w_n(a)}$ for all $a \in \overline{K}$, then w_n and $\|\cdot\|_n$ extend naturally to B_n which becomes a Banach algebra over $\hat{K}$. Furthermore the canonical maps $\phi_n\colon B_{n+1} \to B_n$ are continuous Banach algebra homomorphisms of norm 1. As mentioned before, $B_{dR}^{+} = \lim_{\leftarrow} B_n$, with transition maps the ϕ's. The canonical topology on B_{dR}^{+} is the projective limit topology, with topology on each B_n induced by w_n.

3. Good elements

We'll work with a slightly more general definition than the one from the introduction, when we only considered good elements α from $\bar{\mathbb{Q}}_p^*$.

Definition. An element $z \in B_n$ is called good if $w_n(z) = v(\eta_n(z))$. An element Z in B_{dR}^{+} is said to be good at a given level n if its image in B_n is a good element of B_n.

We have the following

Proposition 6. (i) *If $x, y \in B_n$ are good then xy is good.*
(ii) *If $z \in B_n$ is good then $\phi_n(z)$ is a good element of B_{n-1}.*
(iii) *For each $n \geq 1$, $\mathcal{G}_n$ is a subgroup of $\bar{\mathbb{Q}}_p^*$.*

Proof. For (i) note that $w_n(xy) \geq w_n(x)+w_n(y) = v(\eta_n(x))+v(\eta_n(y)) = v(\eta_n(xy))$ but $w_n(xy) \leq v(\eta_n(xy))$.

For (ii) note that $w_{n-1}(\phi_n(z)) \geq w_n(z) = v(\eta_n(z)) \geq w_{n-1}(\phi_n(z)))$.

In order to prove (iii) it remains to show that for any element $\alpha \in \bar{\mathbb{Q}}_p^*$ which is good in B_n, α^{-1} is also good in B_n.

We prove this by induction on n. For $n = 1$ the statement is clear: α is good if and only if $v(\alpha) \in \mathbb{Z}$, in which case α^{-1} will have the same property.

Let us assume that the statement holds true for $n-1$ and let us prove it for n. Assume α is good at level n. By (ii) we know that α is also good in B_{n-1} and from the induction hypothesis it follows that α^{-1} is good in B_{n-1}. By multiplying α if necessary by a power of p we may assume that $w_n(\alpha) = 0$. Then

$$0 = v(\alpha) = v(\alpha^{-1}) = w_{n-1}(\alpha^{-1}).$$

This shows that α and α^{-1} lie in $O_{\overline{K}}^{(n-2)}$. We can then differentiate the equality $1 = \alpha \cdot \alpha^{-1}$ to obtain:

$$0 = \alpha d^{(n-1)}(\alpha^{-1}) + \alpha^{-1} d^{(n-1)}(\alpha).$$

We multiply this equality by $\alpha^{-1} \in O_{\overline{K}}^{(n-2)}$ to put it in the form:

$$0 = d^{(n-1)}(\alpha^{-1}) + \alpha^{-2} d^{(n-1)}(\alpha).$$

Since $w_n(\alpha) = 0$ we have $\alpha \in O_{\overline{K}}^{(n-1)}$, thus $d^{(n-1)}(\alpha) = 0$. Therefore $d^{(n-1)}(\alpha^{-1}) = 0$ from which it follows that $\alpha^{-1} \in O_{\overline{K}}^{(n-1)}$, $w_n(\alpha^{-1}) = 0$ and hence α^{-1} is good in B_n. □

In order to prove Theorem 1 we also need the following:

Lemma 7. *Let $n \geq 2$. For any $y \in B_{n-1}$ there exists $x \in B_n$ with $\phi_n(x) = y$ such that $w_n(x) = w_{n-1}(y)$.*

This is Proposition 5.2 (i) from [I-Z1]. We use it to derive:

Lemma 8. *For any $n \geq 2$ and any $z \in B_n$ there exists $i \in J_n$ such that $w_n(z-i) = w_{n-1}(\phi_n(z))$.*

This follows immediately by applying the above lemma to $\phi_n(z)$: there exists $x \in B_n$ with $\phi_n(x) = \phi_n(z)$ such that $w_n(x) = w_{n-1}(\phi_n(z))$. If we now write $x = z - i$ then we have $\phi_n(i) = 0$, so $i \in J_n$ and the lemma is proved.

By a repeated application of this lemma we obtain the following:

Corollary 9. *For any $n \geq 2$ and any $z \in B_n$ there exists $i \in I_n$ such that $w_n(z-i) = w_1(\eta_n(z))$.*

Corollary 10. *Let $n \geq 2$ and $z \in B_n$ such that $v(\eta_n(z)) \in \mathbb{Z}$. Then there exists $i \in I_n$ such that $z - i$ is good in B_n.*

Corollary 11. *Let $n \geq 2$ and $z \in B_n$ such that $\phi_n(z)$ is good in B_{n-1}. Then there exists $i \in J_n$ such that $z - i$ is good in B_n.*

We now prove the following

Lemma 12. *Let $z \in B_n$ with $\eta_n(z) \in O_{\mathbb{C}_p}$. Then the sequence $\{z^m\}_{m \in \mathbb{N}}$ is bounded in B_n.*

The proof is by induction on n. The case $n = 1$ follows from the hypothesis of the Lemma. Assume now that the statement holds true for $n - 1$ and prove it for n. The sequence $\{\phi_n(z^m)\}$ is bounded in B_{n-1} thus there exists r (which depends on $(n-1)$ and on $\phi_n(z)$) such that $w_{n-1}(p^r \phi_n(z)^m) \geq 0$ for every m. Let's now fix an m. We choose a sequence $\{\alpha_k\}_{k \in \mathbb{N}}$ in $\bar{K}$ such that $\alpha_k \to^{w_n}_{(k\to\infty)} z$. Then $\alpha_k^m \to^{w_n}_{(k\to\infty)} z^m$ and in particular $w_n(\alpha_k^m) = w_n(z^m)$ for k large enough. Since $\alpha_k = \eta_n(\alpha_k) \to_{k\to\infty} \eta_n(z)$ we also have $\alpha_k \in O_{\bar{K}}$ for large k. Similarly $\alpha_k = \phi_n(\alpha_k) \to \phi_n(z)$ so $w_{n-1}(p^r \alpha_k^m) = w_{n-1}(p^r \phi_n(z)^m) \geq 0$.

We now know how to compute $w_n(\beta_{m,k})$ where $\beta_{m,k} = p^r \alpha_k^m$.

We have: $\beta_{1,k}\beta_{m,k} = p^r \beta_{m+1,k}$. Since $w_{n-1}(\beta_{1,k}) \geq 0$, $w_{n-1}(\beta_{m,k}) \geq 0$ and $w_{n-1}(\beta_{m+1,k}) \geq 0$ we can differentiate the above equality and obtain:

$$\beta_{m,k} d\beta_{1k} + \beta_{1,k} d\beta_{m,k} = p^r d\beta_{m+1,k}. \tag{3.1}$$

It now follows that for each m and the corresponding chosen large enough k we either have:

$p^r d\beta_{m+1,k} = 0$ and then for this m we have

$$0 \leq w_n(p^r \beta_{m+1,k}) = w_n(p^{2r} \alpha_k^{m+1}) = w_n(p^{2r} z^{m+1}),$$

which implies $w_n(z^{m+1}) \geq -2r$, or we have:

$p^r d\beta_{m+1,k} \neq 0$ and then at least one of the two terms from the Left Hand Side of (3.1) is nonzero and moreover we have:

(3.2)
$$\begin{aligned} r + w_n(p^r z^{m+1}) &= r + w_n(\beta_{m+1,k}) \\ &\geq \min\{v(\beta_{m,k}) + w_n(\beta_{1,k}), v(\beta_{1,k}) + w_n(\beta_{m,k})\} \\ &= \min\{v(p^r \eta_n(z)^m) + w_n(p^r z), v(p^r \eta_n(z)) + w_n(p^r z^m)\} \\ &= 2r + \min\{v(\eta_n(z)^m) + w_n(z), v(\eta_n(z)) + w_n(z^m)\}. \end{aligned}$$

Since $v(\eta_n(z)) \geq 0$ from (3.2) we get:

$$w_n(z^{m+1}) \geq \min\{w_n(z), w_n(z^m)\}.$$

It is now clear by induction on m that:

$$w_n(z^m) \geq \min\{w_n(z), -2r\}$$

for any $m \geq 1$ and this completes the proof of the lemma. □

Theorem 1 is implied by the following more general:

Theorem 13. *For any $z \in B_n$ there exists $m \in \mathbb{N}^*$ such that z^m is good.*

Proof. Our proof is by induction on n. The case $n = 1$ is clear: here one only needs to choose an m such that $v(z^m) \in \mathbb{Z}$, then $w_1(z^m) = v(z^m)$ and z^m is good.

Let us assume that the statement holds true for $n - 1$ and let us prove it for n. Let $z \in B_n$. From the induction hypothesis we know that there exists $m_0 \geq 1$ such that $\phi_n(z)^{m_0}$ is good in B_{n-1}. Then Corollary 11 can be applied to z^{m_0}. It follows that there exists $i \in J_n$ such that $y = z^{m_0} - i$ is good in B_n.

As a consequence, y^m is good in B_n for any $m \geq 1$, so:

$$w_n(y^m) = v(\eta_n(y)^m) = mv(\eta_n(y)) = m_0 m v(\eta_n(z)) = v(\eta_n(z^{m_0 m})).$$

On the other hand since $i^2 = 0$ one has:

$$y^m = (z^{m_0} - i)^m = z^{m_0 m} - miz^{m_0(m-1)}$$

from which it follows:

$$w_n(z^{m_0 m}) \geq \min\{w_n(y^m), w_n(miz^{m_0(m-1)})\}.$$

We derive:

$$\begin{aligned} 0 &\geq w_n(z^{m_0 m}) - v(\eta_n(z^{m_0 m})) \\ &\geq \min\{0, w_n(miz^{m_0(m-1)}) - m_0 m v(\eta_n(z))\} \end{aligned} \tag{3.3}$$

Here one has:

$$(3.4)\quad w_n(miz^{m_0(m-1)}) - m_0 m v(\eta_n(z)) \geq v(m) + w_n(i) + w_n(z^{m_0(m-1)}) - m_0 m v(\eta_n(z)).$$

We set $l = m_0 v(\eta_n(z))$ and $u = z^{m_0} p^{-l}$. Note that y being good, $l = v(\eta_n(y)) = w_n(y) \in \mathbb{Z}$. Note also that $\eta_n(u) \in O_{C_p}$. From Lemma 12 it follows that the sequence $\{u^m\}_{m\in N}$ is bounded in B_n. In other words, the sequence $\{w_n(u^m)\}_{m\in N}$ is bounded from below.

Now the point is that the Right Hand Side of (3.4) equals:

$$v(m) + w_n(i) - m_0 v(\eta_n(z)) + w_n(u^{m-1}),$$

and this quantity can be made positive by choosing an m with $v(m)$ large enough.

The Left Hand Side of (3.4) will then be positive and hence for such an m the inequalities in (3.3) become equalities. Thus $z^{m_0 m}$ is good in B_n and this completes the proof of the theorem. □

Proof of Theoerm 2. In order to prove the theorem we need to show that for each $n \geq 2$ the quotient $\mathcal{G}_{n-1}/\mathcal{G}_n$ is a p-group.

We start with a remark: If $z \in B_n$ is good and $i \in I_n$ then

$$w_n(z+i) = \min\{w_n(z), w_n(i)\}.$$

Indeed, if $w_n(z+i) > \min\{w_n(z), w_n(i)\}$ then

$$w_n(z) = w_n(i) < w_n(z+i).$$

Since z is good one has

$$w_n(z) = v(\eta_n(z)) = v(\eta_n(z+i)) \geq w_n(z+i).$$

We obtained a contradiction and the remark is proved.

Now let us fix an $n \geq 2$ and assume that $\mathcal{G}_{n-1}/\mathcal{G}_n$ is not a p-group. Then there will be an element $z \in B_n \cap \bar{\mathbb{Q}}_p^*$ and a positive integer q which is not a multiple of p, such that $\phi_n(z)$ is good in B_{n-1}, z^q is good in B_n but z is not good in B_n. By multiplying if necessarily z by a power of p we may assume that $v(\eta_n(z)) = 0$. Thus $w_{n-1}(\phi_n(z)) = 0, w_n(z^q) = 0$ and $w_n(z) < 0$.

From Corollary 11 we know that there exists $i \in J_n$ such that $y = z - i$ is good in B_n. Hence $w_n(y) = 0$.

Now $z^q = (y+i)^q = y^q + qiy^{q-1}$. From the above remark applied to y^q which is good and to qiy^{q-1} which belongs to I_n, it follows that:

$$0 = w_n(z^q) = \min\{w_n(y^q), w_n(qiy^{q-1})\}$$

so $w_n(qiy^{q-1}) \geq 0$. As q was not a multiple of p we get $w_n(iy^{q-1}) \geq 0$. On the other hand note that y is invertible in B_n, more precisely since $z \in \bar{\mathbb{Q}}_p^*$ and

$i^2 = 0$ in B_n we find that $y^{-1} = z^{-1}(1 + z^{-1}i)$. Then from $v(\eta_n(y)) = 0$ and the fact that y is good in B_n it follows as in the proof of Proposition 6 (iii) that y^{-1} is also good. Then y^{1-q} will be good and hence:

$$w_n(y^{1-q}) = v(\eta_n(y^{1-q})) = 0.$$

From this we derive:

$$w_n(i) = w_n(iy^{q-1}y^{1-q}) \geq w_n(iy^{q-1}) + w_n(y^{1-q}) \geq 0.$$

This in turn implies:

$$w_n(z) = w_n(y + i) \geq \min\{w_n(y), w_n(i)\} = 0.$$

We obtained a contradiction, which completes the proof of Theorem 2. □

4. Metric invariants

Let z be an element of B_n which is transcendental over $\mathbb{Q}_p$. For any positive integer m we set:

$$\delta(m, z) = \sup\{w_n(f(z)) : f \in \mathbb{Q}_p[X], monic, \deg f = m\}.$$

It is shown in [I-Z2] that the sup above is attained, and any polynomial for which the sup is attained is called "admissible". An "admissible sequence of polynomials for z" is a sequence $\{f_m(X)\}_{m\geq 0}$ of polynomials with coefficients in $\mathbb{Q}_p$ suct that $f_0(X) = 1$ and $f_m(X)$ is an admissible polynomial of degree m, for any $m \geq 1$. The importance of such sequences lies in the fact that they can be used to construct orthonormal bases for the topological closure E of $\mathbb{Q}_p[z]$ in B_n. More precisely, if $\{f_m(X)\}_{m\geq 0}$ is an admissible sequence of polynomials for z and if we denote $r_m = w_n(f_m(z))$, $M_m(z) = p^{-r_m} f_m(z)$ then the sequence $\{M_m(z)\}_{m\geq 0}$ is an integral, orthonormal basis of E as a Banach space over $\mathbb{Q}_p$. In particular if z is a so called generating element of B_n over $\mathbb{Q}_p$, i.e. if $\mathbb{Q}_p[z]$ is dense in B_n, then the above procedure will exhibit bases of B_n over $\mathbb{Q}_p$. For more details and various related questions see [I-Z2], [A-P-Z] and [P-Z].

Returning to the metric invariants $\delta(m, z)$, let us note that for any $m_1, m_2 \geq 1$ one has:

$$\delta(m_1 + m_2, z) \geq \delta(m_1, z) + \delta(m_2, z). \tag{4.1}$$

Indeed, if $f_{m_1}(X)$ and $f_{m_2}(X)$ are admissible polynomials for z of degrees m_1 and m_1 respectively, then

$$\begin{aligned}\delta(m_1, z) + \delta(m_2, z) &= w_n(f_{m_1}(z)) + w_n(f_{m_2}(z)) \\ &\leq w_n(f_{m_1} f_{m_2}(z)) \leq \delta(m_1 + m_2, z).\end{aligned}$$

It is easy to see that the sequence $\{(\delta(m, z))/m\}_{m\geq 1}$ has a limit $l(z)$ in $\mathbb{R} \cup \{\infty\}$. In fact one has:

$$l(z) = \sup\left\{\frac{w_n(g(z))}{\deg g}; g \in \mathbb{Q}_p[X], monic, \deg g > 0\right\}. \tag{4.2}$$

Indeed, let us define $l(z)$ by (4.2) and let us show that

$$\lim_{m\to\infty} \frac{\delta(m,z)}{m} = l(z).$$

Clearly one has

$$\frac{\delta(m,z)}{m} \leq l(z)$$

for any $m \geq 1$ and

$$\sup_{m\geq 1} \frac{\delta(m,z)}{m} = l(z).$$

We need to show that for any real number $l < l(z)$ one has

$$\frac{\delta(m,z)}{m} > l$$

for all m large enough. Fix such an $l < l(z)$ and choose $m_0 \geq 1$ such that

$$\frac{\delta(m_0,z)}{m_0} > l.$$

Now take a large m and write it in the form $m = km_0 + r$ with $0 \leq r < m_0$. By a repeated application of (4.1) we have

$$\delta(m,z) \geq k\delta(m_0,z) + \delta(r,z)$$

from which we obtain:

$$\frac{\delta(m,z)}{m} \geq \frac{\delta(m_0,z)}{m_0} - \frac{r}{mm_0}\delta(m_0,z) + \frac{\delta(r,z)}{m}. \tag{4.3}$$

The Right Hand Side of (4.3) is $> l$ for m large enough and this proves the claim.

Now let Z be an element of B_{dR}^+ whose projection $\theta(Z)$ in $\mathbb{C}_p$ is transcendental over $\mathbb{Q}_p$. Then for each n the image $\theta_n(Z)$ of Z in B_n is transcendental over $\mathbb{Q}_p$ and one can define the metric invariants $l_n(Z) := l(\theta_n(Z))$.

The inequalities between the valuations w_n in combination with (4.2) show that

$$l_1(Z) \geq l_2(Z) \geq \cdots \geq l_n(Z) \geq \cdots .$$

In order to prove Theorem 3 let us fix an element Z as above and an integer $n \geq 2$. We want to show that for any $l < l_1(Z)$ one has $l_n(Z) > l$.

Fix such an $l < l_1(Z)$ and choose a nonconstant polynomial $g(X)$ such that:

$$\frac{v(g(\theta(Z)))}{\deg g} > l.$$

Here we don't have any control on the magnitude of $w_n(g(\theta(Z)))$, which might be much smaller than $v(g(\theta(Z)))$. Now the idea is to consider the contribution in (4.2) of the powers of g. On one hand we have for any $m \geq 1$:

$$\frac{v(g^m(\theta(Z)))}{\deg g^m} = \frac{v(g(\theta(Z)))}{\deg g} > l.$$

On the other hand we know from Theorem 13 applied to the element $g(\theta_n(Z))$ of B_n that there exists an integer $m_1 \geq 1$ such that $g^{m_1}(\theta_n(Z))$ is good in B_n. In other words one has $w_n(g^{m_1}(\theta_n(Z))) = v(g^{m_1}(\theta(Z)))$.

In conclusion we have:

$$l_n(Z) \geq \frac{w_n(g^{m_1}(\theta_n(Z)))}{\deg g^{m_1}} = \frac{v(g^{m_1}(\theta(Z)))}{\deg g^{m_1}} > l$$

and this completes the proof of Theorem 3.

5. A new proof of the results in Section 3

One can prove the results of Section 3 on good elements more easily without using the differential modules of the rings $O_{\overline{K}}^{(n)}$. The proofs below were kindly provided to us by the referee.

Notation.
$A_{inf}^n := W(R)/I_+^{n+1} = \lim_{\leftarrow m} O_{\overline{K}}^{(n)}/p^m O_{\overline{K}}^{(n)}$ $(n \geq 0)$
(A_{inf}^n is p-torsion free and p-adically complete and separated.)
$B_n := B_{dR}^+/I^n = A_{inf}^{n-1} \otimes \mathbb{Q}_p$ $(n \geq 1)$
$w_n(z) := \max\{m \in \mathbb{Z} | z \in p^m A_{inf}^{n-1}\}, z \in B_n$ $(n \geq 1)$
$\eta_n : B_n \to \mathbb{C}_p$
v : the valuation on $\mathbb{C}_p$ normalized by $v(p) = 1$.
$z \in B_n$ is good if and only if $w_n(z) = v(\eta_n(z))$.

Lemma 14. *For $z \in A_{inf}^{n-1}$, $z \in (A_{inf}^{n-1})^*$ if and only if $\eta_n(z) \in O_{\mathbb{C}_p}^*$.*

Proof. This follows from the fact that $\eta_n : A_{inf}^{n-1} \to O_{\mathbb{C}_p}$ is surjective and its kernel is a nilpotent ideal. □

Corollary 15. *For a non-zero element z of B_n, z is good if and only if $\eta_n(z) \neq 0$, $v(\eta_n(z)) \in \mathbb{Z}$ and $p^{-v(\eta_n(z))}z \in (A_{inf}^{n-1})^*$.*

Proof. The sufficiency is trivial. If $z \in B_n$ is good and $z \neq 0$, then $v(\eta_n(z)) = w_n(z) \in \mathbb{Z}$. Hence $\eta_n(z) \neq 0$ and $p^{-v(\eta_n(z))}z \in A_{inf}^{n-1}$. Since $\eta_n(p^{-v(\eta_n(z))}z) = p^{-v(\eta_n(z))}\eta_n(z) \in O_{\mathbb{C}_p}^*$, $p^{-v(\eta_n(z))}z \in (A_{inf}^{n-1})^*$ by Lemma 14. □

Corollary 16. *The set of non-zero good elements of B_n is a subgroup of B_n^*.*

Proof. Obvious from Corollary 15. □

Lemma 17. *For $z \in B_n$, $n \geq 2$, if the image $\bar{z}$ of z in B_{n-1} is contained in $(A_{inf}^{n-2})^*$, then there exists an integer $M \geq 0$ such that $z^{p^M} \in (A_{inf}^{n-1})^*$.*

Proof. Let $w \in A_{inf}^{n-1}$ be a lifting of $\bar{z}$. By Lemma 14, $w \in (A_{inf}^{n-1})^*$. Set $a := zw^{-1} - 1$, which is contained in I^{n-1}/I^n, and let M be an integer such that $p^M a \in I_+^{n-1}/I_+^n$. Then, we have $(zw^{-1})^{p^M} = 1 + p^M a \in 1 + I_+^{n-1}/I_+^n \subset (A_{inf}^{n-1})^*$. Hence $z^{p^M} \in (A_{inf}^{n-1})^*$. □

Corollary 18. (1) *For any $z \in B_1 = \mathbb{C}_p$, there exists an integer $m \geq 1$ such that z^m is good.*

(2) *For any $z \in B_n$ such that its image in B_1 is good, there exists an integer $M \geq 1$ such that z^{p^M} is good.*

Proof. (1) follows from $v(\mathbb{C}_p) = \mathbb{Q} \cup \{\infty\}$. For $z \in B_n$, if its image in B_1 is good, $v(\eta_n(z)) \in \mathbb{Z}$. Replacing z with $p^{-v(\eta_n(z))}z$, we may assume $v(\eta_n(z)) = 0$, i.e. $\eta_n(z) \in O^*_{C_p}$. By applying Lemma 17 repeatedly, we see that there exists an integer $M \geq 0$ such that $z^{p^M} \in (A^{n-1}_{inf})^*$ and hence z^{p^N} is a good element. □

V. Alexandru:
University of Bucharest
Department of Mathematics
Str. Academiei 14, RO-70109
Bucharest, Romania

N. Popescu:
Institute of Mathematics
P.O. Box 1-764, RO-70700
Bucharest, Romania
e-mail: Nicolae.Popescu@imar.ro

A. Zaharescu:
Institute of Mathematics
P.O. Box 1-764, RO-70700
Bucharest, Romania and
Department of Mathematics
University of Illinois
at Urbana-Champaign
1409 W. Green Street, Urbana
IL, 61801, Usa
e-mail: zaharesc@math.uiuc.edu

References

[A-P-Z] V. Alexandru, N. Popescu and A. Zaharescu, *On the closed subfields of* $\mathbb{C}_p$, J. Number Theory **68**-2 (1998), 131–150.

[C-G] J. Coates and R. Greenberg, *Kummer theory of abelian varieties*, Invent. Math. **126** (1996), 129–174.

[Fo] J.-M. Fontaine, *Sur certains types de représentations p-adiques du groupe de Galois d'un corps local*; *construction d'un anneau de Barsotti-Tate*, Ann. of Math. **115** (1982), 529–577.

[F-C] ______, *Le corps des périodes p-adique* (*avec une appendice par P. Colmez*), Astérisque **223** (1994), 59–111.

[I-Z1] A. Iovita and A. Zaharescu, *Galois theory of B_{dR}^+*, Compositio Math. **117**-1 (1999), 1–33.

[I-Z2] ———, *Generating elements for B_{dR}^+*, J. Math. Kyoto Univ. **39**-2 (1999), 233–249.

[P1] E. L. Popescu, *A generalization of Hensel's Lemma*, Rev. Roum. Math. Pures Appl. **38**-3 (1993), 802–805.

[P2] ———, *v-basis and Fundamental basis of local fields*, Rev. Roumaine Math. Pures Appl. **45**-4 (2000), 671–680.

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