THE JOURNAL OF SYMBOLIC LOGIC
Volume 66, Number 3, Sept. 2001

EXISTENCE OF PRIME ELEMENTS IN RINGS OF GENERALIZED POWER SERIES

DANIEL PITTELOUD

Abstract. The field $K((G))$ of generalized power series with coefficients in the field K of characteristic 0 and exponents in the ordered additive abelian group G plays an important role in the study of real closed fields. Conway and Gonshor (see [2, 4]) considered the problem of existence of non-standard irreducible (respectively prime) elements in the huge "ring" of omnific integers, which is indeed equivalent to the existence of irreducible (respectively prime) elements in the ring $K((G^{\leq 0}))$ of series with non-positive exponents. Berarducci (see [1]) proved that $K((G^{\leq 0}))$ does have irreducible elements, but it remained open whether the irreducibles are prime i.e., generate a prime ideal. In this paper we prove that $K((G^{\leq 0}))$ does have prime elements if $G = (\mathbb{R}, +)$ is the additive group of the reals, or more generally if G contains a maximal proper convex subgroup.

§1. Introduction.

We begin with some preliminaries on generalized power series.

- If K is any field and G any ordered additive abelian group, $K((G))$ is the set of all formal series

$$a = \sum_{\gamma \in G} a_\gamma x^\gamma, \text{ where } a_\gamma \in K \quad \forall \gamma \in G,$$

having well-ordered support $S_a := \{\gamma \in G : a_\gamma \neq 0\}$.
With obvious operations $+$ and $\cdot$, $K((G))$ is a field (Hahn 1907 , see [5]). If K is an ordered field, so is $K((G))$: We simply put $a = \sum_{\gamma \in G} a_\gamma x^\gamma > 0$ iff $a_\delta > 0$, where $\delta := \min S_a$.
- $K((G))$ is called the field of generalized power series with coefficients in K and exponents in G.
- $K((G^{\leq 0}))$ denotes the subring of $K((G))$ whose series have their support included in $G^{\leq 0} := \{\gamma \in G : \gamma \leq 0\}$.

From now on, K will always denote a field of characteristic 0 and G an ordered additive abelian divisible group.

These fields $K((G))$ play an important role in the theory of real closed fields because if K is real closed and G is divisible, then $K((G))$ is still real closed (see e.g., [12]).

Moreover, it is a classical fact that if F is a real closed field, then F embeds in some $\mathbb{R}((G))$, see [6].

Received February 15, 1999; revised March 15, 2000.
Supported by the Swiss National Foundation

0022-4812/01/6603-0013/$2.10

Generalized power series and some variants have been studied by van den Dries, Ecalle, van der Hoeven, Macintyre, Marker, Ressayre and others, in connection with the study of asymptotic functions and o-minimal structures (see e.g., [13, 14, 15, 3, 16, 11, 10]).

Very recently, Berarducci (see [1]) proved that $K((G^{\leq 0}))$ does have irreducible elements, hence answering a question of Conway and Gonshor (see [2, 4]).

In order to prove the existence of irreducibles, Berarducci introduces an ordinal valued map $v_0 : K((G^{\leq 0})) \longrightarrow OR$ (see section 2).

He first considers the case of the additive group of the reals $G = (\mathbb{R}, +)$ and shows that $v_0(bc)$ can be computed in terms of $v_0(b)$ and $v_0(c)$ using the natural product, by the formula $v_0(bc) = v_0(b) \odot v_0(c)$ (see section 2). And then to deal with the general case (i.e., non - archimedean groups) he uses an idea of Gonshor and Mourgues.

He left open the question whether $K((G^{\leq 0}))$ contains prime elements (i.e., elements generating prime ideals) even if $G = (\mathbb{R}, +)$.

We prove that this is the case if $G = (\mathbb{R}, +)$ or more generally if G contains a maximal convex proper subgroup (e.g., $G = \mathbb{R}^{\alpha}$ with lexicographic order, α ordinal).

More precisely we show that:

1. If G is archimedean (i.e., G is isomorphic to a subgroup of $G = (\mathbb{R}, +)$), then all $\omega-$series (and some $\omega + 1-$series) whose support is cofinal to 0 are prime in $K((G^{\leq 0}))$.
2. If G contains a maximal proper convex subgroup, $K((G^{\leq 0}))$ contains primes of type $\omega + 1$.

However, for general groups G the existence of primes is still open, and it is also an open question whether all irreducibles in $K((G^{\leq 0}))$ are prime even if $G = (\mathbb{R}, +)$.

CONTENTS OF THIS PAPER:

REMARK. In our paper [8] we solved affirmatively another question of [1] by proving that the ideal $J \subseteq K((G^{\leq 0}))$ generated by the set of monomials $\{ x^{\gamma} : \gamma \in G$ and $\gamma < 0 \}$ is prime for any G. [It was proved in [1] for $G = (\mathbb{R}, +)$].

The results of this paper and [8] are independent.

§2. The formula (B). In order to prove the existence of irreducibles in $K((G^{\leq 0}))$, Berarducci introduced an "ordinal valuation" $v_0 : K((G^{\leq 0})) \longrightarrow OR$. Before defining this map, we recall some basic definitions which all appear in [1].

DEFINITIONS. Let $b = \sum_{\delta \in \mathbb{R}^{\leq 0}} b_{\delta} x^{\delta} \in K((\mathbb{R}^{\leq 0}))$, and $\gamma \in \mathbb{R}^{<0}$.

1. $b_{|\gamma} := \sum_{\delta \leq \gamma} b_{\delta} x^{\delta}$ is the truncation of b at γ.
2. $b^{|\gamma} := x^{-\gamma} b_{|\gamma}$
3. $J := \{ b \in K((\mathbb{R}^{\leq 0})) : \exists \gamma < 0$ such that $S_b \leq \gamma$ i.e., $\alpha \leq \gamma \ \forall \alpha \in S_b \}$.

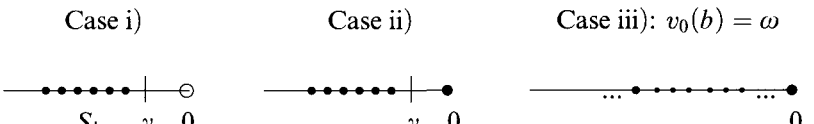

FIGURE 1

REMARK. It is easy to prove that J is an ideal of $K((\mathbb{R}^{\leq 0}))$, which is generated by the set of monomials with negative exponents.

NOTATIONS.

1) OR denotes the class of all ordinals.
2) Lim denotes the class of all limit ordinals.
3) ot abbreviates order type.
4) C.n.f. abbreviates Cantor normal form.
5) If $X, Y \subseteq \mathbb{R}$ and $\gamma \in \mathbb{R}$, $X \leq Y$ means $x \leq y \ \forall x \in X \forall y \in Y$, $X \leq \gamma$ means $X \leq \{\gamma\}$, $\mathbb{R}^{<\gamma} := \{\delta \in \mathbb{R} : \delta < \gamma\}$ etc...
6) If $X \subseteq \mathbb{R}$, $X^* := X \setminus \{0\}$.
7) If $b \in K((\mathbb{R}^{\leq 0}))$, $ot(b) := ot(S_b)$.

DEFINITION. of $v_0 : K((\mathbb{R}^{\leq 0})) \longrightarrow OR$.
Let $b \in K((\mathbb{R}^{\leq 0}))$ (Refer to figure 1).

i) If there is some $\gamma \in \mathbb{R}^{<0}$ such that $S_b \leq \gamma$, then $v_0(b) := 0$.
ii) If there is some $\gamma \in \mathbb{R}^{<0}$ such that $S_b \setminus \{0\} \leq \gamma$ and $0 \in S_b$, then $v_0(b) := 1$.
iii) Otherwise, $v_0(b) := \omega^\delta$, where δ is defined by $\text{ot}(S_b \cap [-\varepsilon, 0[) = \omega^\delta$ for $\varepsilon > 0$ sufficiently small.

REMARKS.

1) $b = c \bmod (J)$ iff $v_0(b - c) = 0$.
2) If $b \neq 0, v_0(b^{|\gamma}) < v_0(b)$ for all $\gamma \in \mathbb{R}^{<0}$ sufficiently close to 0.
3) If we are in Case iii) of the definition of v_0 and if $\text{ot}(S_b \setminus \{0\}) \overset{C.n.f.}{=} \omega^{\alpha_1} + ... + \omega^{\alpha_n}$ (with $\alpha_1 \geq ... \geq \alpha_n > 0$), then $v_0(b) = \omega^{\alpha_n}$.

Berarducci's formula, which we call **(B)**, states that

$$v_0(bc) \overset{(B)}{=} v_0(b) \odot v_0(c) \quad \forall\, b, c \in K((\mathbb{R}^{\leq 0}))\,,$$

where $\odot$ denotes the commutative (natural) product of ordinals (see [9]).

The main tool for proving **(B)** is the convolution formula:
If $b, c \in K((\mathbb{R}^{\leq 0}))$ and $\gamma \in \mathbb{R}^{<0}$, then

$$(bc)^{|\gamma} = \sum_{\beta_i + \xi_i = \gamma} b^{|\beta_i} c^{|\xi_i} \bmod (J) \qquad \text{(C)}$$

REMARKS.

1) For each $\gamma \in \mathbb{R}^{<0}$, there is only a finite number of pairs $(\beta, \xi) \in \mathbb{R}^{\leq 0} \times \mathbb{R}^{\leq 0}$ such that $b^{|\beta} c^{|\xi} \neq 0 \bmod (J)$. Hence the right member of (C) does make sense.
2) (C) holds for a product of several factors: $(b_1 b_2 ... b_n)^{|\gamma} = \sum_{\beta_1 + ... + \beta_n = \gamma} b_1^{|\beta_1} ... b_n^{|\beta_n} \bmod (J)$.

Finally let us recall the following facts (see [1]) which we will repeatedly use (without mention) in all this paper.

LEMMA 2.1. *Let* $b, c \in K((\mathbb{R}^{\leq 0}))$.

a) $v_0(b+c) \leq max(v_0(b), v_0(c))$

b) $v_0(b+c) = max(v_0(b), v_0(c))$ *if* $v_0(b) \neq v_0(c)$

c) $v_0(bc) = v_0((b - b_{|\gamma})(c - c_{|\eta}))$ *for all* γ, η *sufficiently close to* 0

d) $v_0(bc) = v_0(b) \odot v_0(c)$.

As a consequence of the convolution formula (for several factors) and Lemma 2.1, we get the following:

COROLLARY 2.2. Let $a, b \in K((\mathbb{R}^{\leq 0}))$ be such that $v_0(a) = \omega$ and $v_0(b) = \omega^{\delta+n}$, where $\delta \in \text{Lim} \cup \{0\}$ and $n \in \mathbb{N}$. Let $\gamma \in \mathbb{R}^{<0}$. Then for each $k \geq 1$ we have

$$(a^k b)^{|\gamma} = k a^{k-1} a^{|\gamma} b + a^k b^{|\gamma} + \varepsilon, \text{ where } v_0(\varepsilon) < \omega^{\delta+n+k-1}.$$

§3. Primes in $K((\mathbb{R}^{\leq 0}))$. We prove in this section that if $a \in K((\mathbb{R}^{\leq 0}))$ is of order type ω or $\omega + 1$ and satisfies $v_0(a) = \omega$, then a is prime in $K((\mathbb{R}^{\leq 0}))$.

In particular, this implies that Conway's series $x^{-1} + x^{-1/2} + x^{-1/3} + \ldots + 1$ is prime in the model of open induction $\mathbb{R}((\mathbb{R}^{<0})) \oplus \mathbb{Z}$.

Now let us give the general idea of the proof.

Assume that a is fixed as above, and let $b, c, d \in K((\mathbb{R}^{\leq 0}))$ be such that $ab = cd$. We want to prove that $a \mid c$ or $a \mid d$ in $K((\mathbb{R}^{\leq 0}))$. [$a \mid c$ means a divides c].

The idea (given in Lemma 3.1 below) is to transform the equation $ab = cd$ into a simpler one, where it is easier to see that $a \mid c$ or $a \mid d$.

We are then led to associate a complexity to such equations in such a way that the complexity of the new equation is smaller than that of the initial one.

If we succeed in doing this, it is clear that we will get the result by induction on the complexity of the equation.

REMARKS.

1) When we speak of the complexity of the equation $ab = cd$, we have to be careful: If say $cd = c'd'$, does it follow that the complexity of $ab = cd$ is the same of that of $ab = c'd'$? We will make this very precise later.

2) For this proof by induction on the complexity of the equation, some experimental computations show that we have to consider all equations of the form $a^k b = c^l d$, (a fixed, $k, l \in \mathbb{N}^*$, $b, c, d \in K((\mathbb{R}^{\leq 0}))$).

Following these general ideas we will first prove that a is "almost" prime (see Proposition 3.2). It will follow quite easily that a is prime (see Theorem 3.3).

DEFINITIONS. Let $\alpha \in \text{OR}$ and let $a, b \in K((\mathbb{R}^{\leq 0}))$.

1. $a = b \bmod (J_{\omega^\alpha})$ iff $v_0(b - a) < \omega^\alpha$.
2. $a \mid b \bmod (J_{\omega^\alpha})$ iff $\exists\, e, \varepsilon \in K((\mathbb{R}^{\leq 0}))$ such that $b = ae + \varepsilon$ and $v_0(\varepsilon) < \omega^\alpha$.

LEMMA 3.1. *Let* $a, b, c, d \in K((\mathbb{R}^{\leq 0}))$ *be such that* $v_0(a) = \omega$, $v_0(b) = \omega^{\delta+n}$, $v_0(c) = \omega^{\delta_1+r}$, $v_0(d) = \omega^{\delta_2+s}$; *where* $\delta, \delta_1, \delta_2 \in Lim \cup \{0\}$ *and* $n, r, s \in \mathbb{N}$. *Let* $k, l \in \mathbb{N}^*$ *and assume that* $a^k b = c^l d \bmod (J_{v_0(a^k b)})$. *Let* $\gamma \in S_a \setminus \{0\}$ *be fixed sufficiently close to* 0, *and assume furthermore that* $a^{k-1} \mid c^{|\gamma} \bmod (J_{\omega^{\delta_1+r-1}})$ *if* $r \geq 1$; $a \not\mid c \bmod (J_{v_0(c)})$ *and* $a \not\mid d \bmod (J_{v_0(d)})$. *Then there exist* $b', c', d' \in K((\mathbb{R}^{\leq 0}))$ *such that* $a^{k+1} b' = (c')^l d'$

mod $(J_{v_0(a^{k+1}b')})$, $v_0(c') = v_0(c)$, $v_0(d') = v_0(d)$, *and* $v_0(b') < v_0(b)$. *Moreover we have* $a \not| c'$ *mod* $(J_{v_0(c')})$ *and* $a \not| d'$ *mod* $(J_{v_0(d')})$.

PROOF. As $a^k b = c^l d \bmod (J_{\omega^{\delta+n+k}})$, Corollary 2.2 yields

$$(*) \qquad ka^{k-1}a^{|\gamma}b + a^k b^{|\gamma} = lc^{l-1}c^{|\gamma}d + c^l d^{|\gamma} \; mod\,(J_{\omega^{\delta+n+k-1}}).$$

By dividing if necessary a and d by ka_γ and $(ka_\gamma)^k$ respectively, we can as well assume that $ka^{|\gamma} = 1 \bmod (J)$.

By multiplying (*) by a and using $a^k b = c^l d \bmod (J_{v_0(a^k b)})$, we get

$$c^l d - lc^{l-1}c^{|\gamma}da - c^l d^{|\gamma}a + a^{k+1}b^{|\gamma} = 0 \; mod\,(J_{v_0(a^k b)}).$$

Elementary algebra shows that this last equation can be written as

$$(**) \qquad (c - c^{|\gamma}a)^l (d - d^{|\gamma}a) - c^{|\gamma}a^2 e + a^{k+1}b^{|\gamma} = 0 \; mod\,(J_{v_0(a^k b)})$$

for some $e \in K((\mathbb{R}^{\leq 0}))$ which is given by

$$e = lc^{l-1}d^{|\gamma} + \Big(\sum_{2 \leq i \leq l} \binom{l}{i} c^{l-i}(c^{|\gamma})^i a^{i-2}\Big)(d - d^{|\gamma}a).$$

Now we consider two cases:

Case 1: $r = 0$

Using Lemma 2.1 and $v_0(c^{|\gamma}) < \omega^{\delta_1}$, we easily prove that $v_0(c^{|\gamma}a^2 e) < v_0(a^k b)$. So we get $a^{k+1}b^{|\gamma} + (c - c^{|\gamma}a)^l (d - d^{|\gamma}a) = 0 \bmod (J_{v_0(a^k b)})$ and we set

$$c' := c - c^{|\gamma}a, \quad d' := d - d^{|\gamma}a \text{ and } b' := b^{|\gamma}.$$

We trivially have $v_0(c') \leq v_0(c)$ and $v_0(d') \leq v_0(d)$ and these inequalities must be equalities otherwise we contradict $a \not| c \bmod (J_{v_0(c)})$ or $a \not| d \bmod (J_{v_0(d)})$.
Moreover, $v_0(b^{|\gamma}) < v_0(b)$ as γ is close to 0, and we have $v_0(a^k b) = v_0(c^l d) = v_0((c')^l d') = v_0(a^{k+1}b')$.
Finally, $a \not| c' \bmod (J_{v_0(c')})$ and $a \not| d' \bmod (J_{v_0(d')})$ because $a \not| c \bmod (J_{v_0(c)})$ and $a \not| d \bmod (J_{v_0(d)})$.

Case 2: $r > 0$

By hypothesis $a^{k-1} | c^{|\gamma} \bmod (J_{\omega^{\delta_1+r-1}})$, hence (**) can be written as

$$(1) \qquad a^{k+1}b' + (c - c^{|\gamma}a)^l (d - d^{|\gamma}a) = 0 \; mod\,(J_{v_0(a^k b)}).$$

We set $c' := c - c^{|\gamma}a$, $d' := d - d^{|\gamma}a$ and we prove exactly as in Case 1 that $v_0(c') = v_0(c), v_0(d') = v_0(d)$, $a \not| c' \bmod (J_{v_0(c')})$ and $a \not| d' \bmod (J_{v_0(d')})$.
As $v_0((c')^l d') = v_0(c^l d) = \omega^{\delta+n+k}$, (1), Lemma 2.1 and (B) imply that $\omega^{\delta+n+k} = v_0(a^{k+1}b') = \omega^{k+1} \odot v_0(b')$. But we also have $\omega^{\delta+n+k} = v_0(a^k b) = \omega^k \odot v_0(b)$.
Hence $v_0(b') < v_0(b)$ and $v_0(a^k b) = v_0(a^{k+1}b')$, which completes the proof of the lemma. ⊣

We now define the **complexity map.**

Let $A := \{u \in K((\mathbb{R}^{\leq 0})) : v_0(u) \geq 1\}$. We set

$$Cpl : A^3 \times \mathbb{N}^* \longrightarrow (OR)^4, \quad (b, c, d, l) \mapsto (v_0(c), v_0(d), l, v_0(b))$$

where $(OR)^4$ is ordered lexicographically.

REMARK. If $a^k b = c^l d \bmod (J_{v_0(a^k b)})$ with a, b, c, d as in Lemma 3.1, then (B) implies that k is determined by b, c, d, l.

DEFINITION. If $u \in K((\mathbb{R}^{\leq 0}))$ and $v_0(u) = \omega^{\alpha+m}$, where $\alpha \in \mathrm{Lim} \cup \{0\}$ and $m \in \mathbb{N}$, then we say that $\gamma \in \mathbb{R}^{<0}$ is a big point of u if $m > 0$ and $v_0(u^{|\gamma}) = \omega^{\alpha+m-1}$.

PROPOSITION 3.2. *Let $a, b, c, d \in K((\mathbb{R}^{\leq 0}))$ be such that $v_0(a) = \omega, v_0(b) = \omega^{\delta+n}, v_0(c) = \omega^{\delta_1+r}, v_0(d) = \omega^{\delta_2+s}$; where $\delta, \delta_1, \delta_2 \in Lim \cup \{0\}$ and $n, r, s \in \mathbb{N}$. Let $k, l \in \mathbb{N}^*$ and assume that $a^k b = c^l d \bmod (J_{v_0(a^k b)})$. Then $a \mid c \bmod (J_{v_0(c)})$ or $a \mid d \bmod (J_{v_0(d)})$.*

PROOF. By induction on the complexity of (b, c, d, l).

Assume that $a^k b = c^l d \bmod (J_{v_0(a^k b)})$ and that the result holds for all $(b', c', d', l') \in A^3 \times \mathbb{N}^*$ such that $Cpl(b', c', d', l') < Cpl(b, c, d, l)$.

We have to prove that $a \mid c \bmod (J_{v_0(c)})$ or $a \mid d \bmod (J_{v_0(d)})$.

By contradiction, suppose that $a \nmid c \bmod (J_{v_0(c)})$ and $a \nmid d \bmod (J_{v_0(d)})$.

- if $k = 1$, applying Lemma 3.1 we get $a^2 b' = (c')^l d' \bmod (J_{v_0(a^2 b')})$.
  As $(v_0(c'), v_0(d'), l) = (v_0(c), v_0(d), l)$ and $v_0(b') < v_0(b)$, we have $Cpl(b', c', d', l) < Cpl(b, c, d, l)$.
  Hence by induction we get $a \mid c' \bmod (J_{v_0(c')})$ or $a \mid d' \bmod (J_{v_0(d')})$, which contradicts Lemma 3.1.
- Assume now $k > 1$.
  Let $\gamma \in S_a \setminus \{0\}$ be fixed, sufficiently close to 0. As $a^k b = c^l d \bmod (J_{\omega^{\delta+n+k}})$, Corollary 2.2 yields

$$(*) \qquad a^{k-1} b + a^k b^{|\gamma} = l c^{l-1} c^{|\gamma} d + c^l d^{|\gamma} \ mod (J_{\omega^{\delta+n+k-1}}).$$

[As in Lemma 3.1, we can assume that $k a^{|\gamma} = 1 \bmod (J)$].

Case 1: γ is a big point of d.

Multiplying (*) by c and using $a^k b = c^l d \bmod (J_{v_0(a^k b)})$, we get

$$(1) \qquad a^{k-1} b' = c^{l+1} d^{|\gamma} \ mod (J_{\omega^{\delta_1 \odot (l+1) \oplus \delta_2 + r(l+1)+s-1}}) \text{ for some } b' \in A.$$

As $Cpl(b', c, d^{|\gamma}, l+1) < Cpl(b, c, d, l)$, we have by induction $a \mid c \bmod (J_{v_0(c)})$ or $a \mid d^{|\gamma} \bmod (J_{v_0(d^{|\gamma})})$.

By assumption $a \nmid c \bmod (J_{v_0(c)})$ so $a \mid d^{|\gamma} \bmod (J_{v_0(d^{|\gamma})})$.

Write $d^{|\gamma} = ae + \varepsilon$, where $v_0(\varepsilon) < v_0(d^{|\gamma})$. By substituting this in (1), dividing by a and using (B), we get $a^{k-2} b' = c^{l+1} e \ mod (J_{\omega^{\delta_1 \odot (l+1) \oplus \delta_2 + r(l+1)+s-2}})$.

By induction we get as before $a \mid e \bmod (J_{\omega^{\delta_2+s-2}})$, and so $a^2 \mid d^{|\gamma} \bmod (J_{v_0(d^{|\gamma})})$.

Applying again induction $(k-3)$- times, we get

$$(**) \qquad a^{k-1} \mid d^{|\gamma} mod (J_{v_0(d^{|\gamma})}).$$

By substituting (**) in (*), we get $a^{k-1} b_0 = c^{|\gamma} c^{l-1} d \bmod (J_{\omega^{\delta+n+k-1}})$ for some $b_0 \in A$.

a) Assume that γ is a big point of c

As $v_0(c^{|\gamma}) < v_0(c)$ (γ is close to 0), we have $Cpl(b_0, c^{|\gamma}, c^{l-1} d, 1) < Cpl(b, c, d, l)$. Hence by induction $a \mid c^{|\gamma} \bmod (J_{v_0(c^{|\gamma})})$ or $a \mid c^{l-1} d \bmod (J_{\omega^{\delta_1 \odot (l-1) \oplus \delta_2 + r(l-1)+s}})$.

Assume that $a \mid c^{l-1} d \bmod (J_{\omega^\theta})$, where $\theta := \delta_1 \odot (l-1) \oplus \delta_2 + r(l-1) + s$.

As $Cpl(-, c, d, l-1) < Cpl(b, c, d, l)$, we get by induction $a \mid c \bmod (J_{v_0(c)})$ or $a \mid d \bmod (J_{v_0(d)})$, a contradiction.

So $a \not\mid c^{l-1}d \bmod (J_{\omega^\theta})$ and we prove as above that $a^{k-1} \mid c^{|\gamma} \bmod (J_{v_0(c^{|\gamma})})$.

As $a^{k-1} \mid c^{|\gamma} \bmod (J_{v_0(c^{|\gamma})})$, we can apply Lemma 3.1 for the equation $a^k b = c^l d \bmod (J_{v_0(a^k b)})$, and we get $a^{k+1}b' = (c')^l d' \bmod (J_{v_0(a^{k+1}b')})$.

As $(v_0(c'), v_0(d'), l) = (v_0(c), v_0(d), l)$ and $v_0(b') < v_0(b)$, it follows that $Cpl(b', c', d', l) < Cpl(b, c, d, l)$. Hence by induction we get $a \mid c' \bmod (J_{v_0(c')})$ or $a \mid d' \bmod (J_{v_0(d')})$, which contradicts Lemma 3.1.

b) Assume that γ is not a big point of c

Then by (*)

$$a^{k-1}b + a^k b^{|\gamma} = c^l d^{|\gamma} mod (J_{\omega^{\delta+n+k-1}}). \tag{2}$$

Now remember that $a^{k-1} \mid d^{|\gamma} \bmod (J_{v_0(d^{|\gamma})})$ (see (**)), and write

$$d^{|\gamma} = ea^{k-1} + \varepsilon, \text{ where } v_0(\varepsilon) < v_0(d^{|\gamma}). \tag{3}$$

By substituting (3) in (2), we get $a^{k-1}b + a^k b^{|\gamma} = c^l e a^{k-1} \bmod (J_{\omega^{\delta+n+k-1}})$. Hence

$$b + ab^{|\gamma} = c^l e \; mod (J_{v_0(b)}). \tag{4}$$

We have to consider two subcases:

i) γ is a big point of b

Substituting (4) in the initial equation $a^k b = c^l d \bmod (J_{v_0(a^k b)})$, we get $a^k(-ab^{|\gamma} + c^l e) = c^l d \bmod (J_{v_0(a^k b)})$, whence

$$a^{k+1}(-b^{|\gamma}) = c^l(d - a^k e) mod (J_{v_0(a^{k+1}(-b^{|\gamma}))}).$$

As $Cpl(-b^{|\gamma}, c, d - a^k e, l) < Cpl(b, c, d, l)$, we have by induction $a \mid c \bmod (J_{v_0(c)})$ or $a \mid d - a^k e \bmod (J_{v_0(d)})$.

Both are impossible because if $a \mid d - a^k e \bmod (J_{v_0(d)})$, then $a \mid d \bmod (J_{v_0(d)})$.

ii) γ is a not big point of b

Then equation (4) reduces to $b = c^l e \bmod (J_{v_0(b)})$. Substituting this in the initial equation $a^k b = c^l d \bmod (J_{v_0(a^k b)})$, we get

$$a^k c^l e = c^l d \; mod (J_{v_0(a^k b)}), \text{ hence } a^k e = d \; mod (J_{v_0(d)}).$$

So $a \mid d \bmod (J_{v_0(d)})$, a contradiction. This completes the proof of Case 1 (i.e., if γ is a big point of d).

Case 2: γ is not a big point of d.

Then (*) yields

$$a^{k-1}b + a^k b^{|\gamma} = lc^{l-1}c^{|\gamma}d \; mod (J_{\omega^{\delta+n+k-1}}). \tag{5}$$

a) Assume that γ is a big point of c

By (5) we have $a^{k-1} \mid c^{|\gamma}c^{l-1}d \bmod (J_{\omega^{\delta+n+k-1}})$. We are now exactly in the same situation as in Case 1a), and so we get a contradiction.

b) Assume that γ is not a big point of c

(5) yields $a^{k-1}b + a^k b^{|\gamma} = 0 \bmod (J_{\omega^{\delta+n+k-1}})$, whence $b + ab^{|\gamma} = 0 \bmod (J_{v_0(b)})$.

Substituting this in the initial equation $a^k b = c^l d \bmod (J_{v_0(a^k b)})$, we get

$$a^{k+1}(-b^{|\gamma}) = c^l d \; mod (J_{v_0(a^{k+1}(-b^{|\gamma}))}).$$

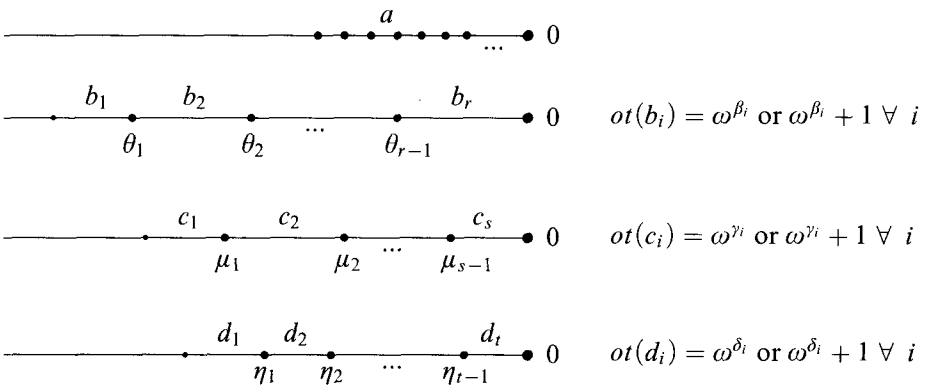

FIGURE 2

As $Cpl(-b^{|\gamma}, c, d, l) < Cpl(b, c, d, l)$, we have by induction $a \mid c \bmod (J_{v_0(c)})$ or $a \mid d \bmod (J_{v_0(d)})$, a contradiction.

This completes the proof of Proposition 3.2. ⊣

We are now ready to prove the main result.

NOTATION. If $u \in K((\mathbb{R}^{\leq 0}))$, u^L denotes the supremum of S_u : $u^L := \sup(S_u) \in \mathbb{R}^{\leq 0}$.

THEOREM 3.3. *Let $a \in K((\mathbb{R}^{\leq 0}))$ of order type ω or $\omega+1$, and such that $v_0(a) = \omega$. Then a is prime in $K((\mathbb{R}^{\leq 0}))$.*

PROOF. Assume that $ab = cd$ for some $b, c, d \in K((\mathbb{R}^{\leq 0}))$.

Multiplying b, c, d by $x^{-b^L}, x^{-c^L}, x^{-d^L}$ respectively, we can as well assume that $b^L = c^L = d^L = 0$.

We prove that $a|c$ or $a|d$ by induction on $ot(c) \oplus ot(d)$: [$\oplus$ denotes the natural sum of ordinals, see e.g., [9]].

First observe that if b, c or d is 0, then the result is obvious because $a \mid 0$. So assume $b \neq 0, c \neq 0, d \neq 0$.

Considering the Cantor normal form $\omega^{\beta_1} + \omega^{\beta_2} + \ldots + \omega^{\beta_r}$ of S_b ($\beta_1 \geq \beta_2 \geq \ldots \geq \beta_r \geq 0$), it is clear that we can write in a unique way $b = b'_1 + b'_2 + \ldots + b'_r$ such that

i) $S_{b'_1} < S_{b'_2} < \ldots < S_{b'_r} \leq 0$

ii) $ot(b'_i) = \omega^{\beta_i} \; \forall \, i$.

We now slightly modify the $b'_i s$ in the following way:

Put $\theta_i := \sup S_{b'_i} \; \forall \, i$ (so $\theta_1 < \theta_2 < \ldots < \theta_{r-1} \leq \theta_r = 0$) and define inductively $b_1 := b_{|\theta_1}$ and $b_i := b_{|\theta_i} - b_{|\theta_{i-1}}$ for $i \geq 2$. Then we have:

i) $b = b_1 + b_2 + \ldots + b_r$ (if $b_r = 0$ remove b_r)

ii) $S_{b_i} < S_{b_{i+1}} \; \forall \, i$

iii) $\omega^{\beta_i} \leq ot(b_i) \leq \omega^{\beta_i} + 1 \; \forall \, i$.

We do the same for c and d (see Figure 2, where we assume that $v_0(b), v_0(c), v_0(d)$ are > 1).

As $ab = cd$, using (B) and the convolution formula it is easy to prove that $\theta_1 = \mu_1 + \eta_1$, $\beta_1 + 1 = \gamma_1 \oplus \delta_1$, and $x^{-\theta_1} ab_1 = (x^{-\mu_1} c_1)(x^{-\eta_1} d_1) \bmod (J_{\omega^{\beta_1 + 1}})$.

By Proposition 3.2, $a \mid x^{-\mu_1} c_1 \bmod (J_{\omega^{\gamma_1}})$ or $a \mid x^{-\eta_1} d_1 \bmod (J_{\omega^{\delta_1}})$.

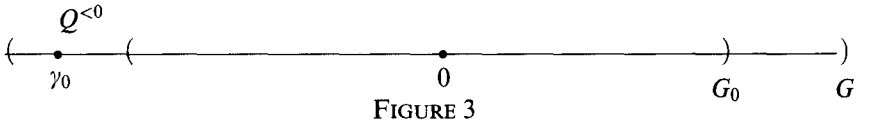

FIGURE 3

Assume that $a \mid x^{-\mu_1}c_1 \bmod (J_{\omega^{\gamma_1}})$ and write

$$x^{-\mu_1}c_1 = ea + \varepsilon, \text{ where } v_0(\varepsilon) < \omega^{\gamma_1}. \tag{6}$$

By replacing e by $e - e_{|\alpha}$ for $\alpha \in \mathbb{R}^{<0}$ sufficiently close to 0, we still have an equality like (6) and we can assume that $ot(ea) = \omega^{\gamma_1}$ or $\omega^{\gamma_1} + 1$. [If α is close to 0, $ot(e - e_{|\alpha}) = \omega^{\delta}$ or $\omega^{\delta} + 1$ for some ordinal δ. Using (B), Lemma 2.1 and the convolution formula we get $ot((e - e_{|\alpha})a) = \omega^{\gamma_1}$ or $\omega^{\gamma_1} + 1$].

Hence it is easy to conclude that $ot(\varepsilon) < \omega^{\gamma_1}$ (and not only $v_0(\varepsilon) < \omega^{\gamma_1}$).
By (6), $ab = cd \Rightarrow ab = (c_1 + c_2 + \ldots + c_s)d = (ex^{\mu_1}a + x^{\mu_1}\varepsilon + c_2 + \ldots + c_s)d$, whence

$$a(b - x^{\mu_1}ed) = (x^{\mu_1}\varepsilon + c_2 + \ldots + c_s)d.$$

$ot(x^{\mu_1}\varepsilon + c_2 + \ldots + c_s) \oplus ot(d) < ot(c) \oplus ot(d)$ because $(ot(x^{\mu_1}\varepsilon) < \omega^{\gamma_1} \leq ot(c_1)$ and c_1 is the first part of the C.n.f. of c).

Hence we get by induction $a \mid x^{\mu_1}\varepsilon + c_2 + \ldots + c_s$ or $a \mid d$.

But if $a \mid x^{\mu_1}\varepsilon + c_2 + \ldots + c_s$, then by (6) $a \mid x^{\mu_1}(x^{-\mu_1}c_1 - ea) + c_2 + \ldots + c_s$ whence $a \mid -x^{\mu_1}ea + c$. So $a \mid c$ and we are done. ⊣

§4. Primes in $K((G^{\leq 0}))$ when G admits a maximal proper convex subgroup. We first consider the case where G is archimedean.

THEOREM 4.1. *Let G be an ordered abelian divisible archimedean group.*

Let $a \in K((G^{\leq 0}))$ be of order type ω or $\omega + 1$ and such that $S_a \setminus \{0\}$ is cofinal to 0. Then a is prime in $K((G^{\leq 0}))$.

PROOF. As G is archimedean, G embeds in $\mathbb{R}$. So we can assume that $G \subseteq \mathbb{R}$. Suppose that $ab = cd$ for some $b, c, d \in K((G^{\leq 0}))$. Then $ab = cd$ in $K((\mathbb{R}^{\leq 0}))$, and by Theorem 3.3 $\exists u \in K((\mathbb{R}^{\leq 0}))$ such that, say, $c = au$.

As $K((G))$ is a field, $u = c/a \in K((G))$. So $u \in K((\mathbb{R}^{\leq 0})) \cap K((G)) = K((G^{\leq 0}))$ and we are done. ⊣

The proof of the next theorem is exactly the same as in [1], so we only sketch it.

THEOREM 4.2. *Let G be an ordered abelian divisible group which contains a maximal proper convex subgroup G_0. Let Q be a divisible archimedean subgroup of G such that $Q \cap G_0 = \{0\}$.*

Let $a \in K((Q^{<0}))$ be of order type ω such that a is not divisible by any monomial x^{γ} for $\gamma \in Q^{<0}$.

Then $a + 1$ is prime in $K((G^{\leq 0}))$.

PROOF. [First observe that such Q and a always exist: Choose $\gamma_0 \in G^{<0} \setminus G_0$ and set
$Q := \{\frac{p\gamma_0}{q} \ ; \ p \in \mathbb{Z}, q \in \mathbb{Z}^*\}$, $a := \sum_{n \geq 1} x^{\gamma_0/n}$]. See Figure 3.

As G is divisible, there exists a subgroup H of G such that $G = H \oplus G_0$. H can be chosen such that $H \supseteq Q$ because $Q \cap G_0 = \{0\}$. Moreover, as G_0 is a maximal

proper convex subgroup, H is archimedean and the order of G is the lexicographic order on $G = H \oplus G_0$.

Hence there is a canonical ordered fields isomorphism $i : K((G)) \longrightarrow K((G_0))((H))$ and $i(K((G^{\leq 0}))) \subseteq K((G_0))((H^{\leq 0}))$.

As $S_a \subseteq Q$ and $Q \cap G_0 = \{0\}$, $i(a+1)$ has order type $\omega+1$ in $K((G_0))((H^{\leq 0}))$.

Hence $i(a+1)$ is prime in $K((G_0))((H^{\leq 0}))$ by theorem 3.3. So $a+1$ is prime in $K((G^{\leq 0}))$ and we are done. ⊣

EXAMPLE. Let $\alpha \in OR$ and $G = \mathbb{R}^\alpha$ ordered lexicographically, where

$$\mathbb{R}^\alpha := \{(x_0, x_1, ..., x_\beta, ...) \mid x_\beta \in \mathbb{R} \ \forall \beta < \alpha\}.$$

Let $a = x^{-1} + x^{-1/2} + x^{-1/3} + x^{-1/4} + ...$, where $-1/n := (-1/n, 0, 0, 0, ...) \in \mathbb{R}^\alpha \ \forall \ n \in \mathbb{N}^*$. Then $a+1$ is prime in $K((G^{\leq 0}))$.

Acknowledgements. I sincerely thank A.Berarducci for his encouragement on this project and for many helpful discussions.

REFERENCES

[1] A. BERARDUCCI, *Factorization in generalized power series*, ***Transactions of the American Mathematicall Society***, vol. 352 (2000).

[2] J. H. CONWAY, ***On numbers and games***, Academic Press, London, 1976.

[3] J. ECALLE, *Introduction aux fonctions analysables et preuve constructive de la conjecture de Dulac*, ***Actualités Mathematiques***, (1992), Hermann, Paris.

[4] H. GONSHOR, ***An introduction to the theory of surreal numbers***, Cambridge University Press, Cambridge, 1986.

[5] H. HAHN, *Uber die nichtarchimedischen grossensysteme*, ***S.B. Akad. Wiss. Wien. IIa***, vol. 116 (1907), pp. 601–655.

[6] I. KAPLANSKI, *Maximal fields with valuations*, ***Duke Mathematical Journal***, vol. 9 (1942), pp. 303–321.

[7] M. H. MOURGUES and J. P. RESSAYRE, *Every real closed field has an integer part*, this JOURNAL, (1993), pp. 641–647.

[8] D. PITTELOUD, *Algebraic properties in rings of generalized power series*, ***Annals of Pure and Applied Logic***, to appear.

[9] W. POHLERS, *Proof Theory*, (A. Dold, B. Eckmann, and F. Takens, editors), Lectures Notes in Mathematics, no. 1407, Springer-Verlag, Berlin Heidelberg, 1989.

[10] J. P. RESSAYRE, Integers parts of real closed exponential fields, pp. 278–288, Oxford University Press, Oxford, 1993, pp. 278–288, Arithmetic, Proof Theory and Computational Complexity (P. Clote and J. Krajicek, editors).

[11] ———, *Survey on transfinite series and their applications*, 1995, manuscript.

[12] P. RIBENBOIM, *Fields, algebraically closed and others*, ***Manuscripta Mathematica***, vol. 75 (1992), pp. 115–166.

[13] L. VAN DEN DRIES, A. MACINTYRE, and D. MARKER, *The elementary theory of restricted analytic fields with exponentiation*, ***Annals of Mathematics***, vol. 140 (1994), pp. 183–205.

[14] ———, *Logarithmic-exponential power series*, ***Journal of the London Mathematical Society***, vol. 2 (1997), no. 56, pp. 183–205.

[15] ———, *Logarithmic-exponential power series*, preprint, 1998.

[16] J. VAN DER HOEVEN, *Asymptotique automatique*, ***Ph.D. thesis***, Université Paris 7, 1997.

UNIVERSITÉ DE LAUSANNE
INSTITUTE D' INFORMATIQUE
1015 LAUSANNE, SWITZERLAND
E-mail: daniel.pitteloud@math.unige.ch