

Formal power series with cyclically ordered exponents

M. Giraudet, F.-V. Kuhlmann, G. Leloup

January 26, 2003

Abstract. We define and study a notion of ring of formal power series with exponents in a cyclically ordered group. Such a ring is a quotient of various subrings of classical formal power series rings. It carries a two variable valuation function. In the particular case where the cyclically ordered group is actually totally ordered, our notion of formal power series is equivalent to the classical one in a language enriched with a predicate interpreted by the set of all monomials.

1 Introduction

Throughout this paper, k will denote a commutative ring with unity. Further, C will denote a *cyclically ordered* abelian group, that is, an abelian group equipped with a ternary relation (\cdot, \cdot, \cdot) which has the following properties:

- (1) $\forall a, b, c, (a, b, c) \Rightarrow a \neq b \neq c \neq a$
- (2) $\forall a, b, c, (a, b, c) \Rightarrow (b, c, a)$
- (3) $\forall c \in C, (c, \cdot, \cdot)$ is a strict total order on $C \setminus \{c\}$.
- (4) (\cdot, \cdot, \cdot) is compatible, i.e., $\forall a, b, c, d, (a, b, c) \Rightarrow (a + d, b + d, c + d)$.

For all $c \in C$, we will denote by \leq_c the associated order on C with first element c . For $\emptyset \neq X \subset C$, $\min_c X$ will denote the minimum of (X, \leq_c) , if it exists.

For instance, any totally ordered group is cyclically ordered with respect to the following ternary relation: (a, b, c) iff $a < b < c$ or $b < c < a$ or $c < a < b$. Such a cyclically ordered group is called a *linear cyclically ordered group*.

Let us review quickly two basic facts about cyclically ordered groups.

A theorem of Rieger (see [Fu 63], IV, 6, th. 21), shows that there exist a totally ordered abelian group G and a positive element z in G , such that the subgroup $\mathbb{Z}z$ generated by z is cofinal in G and $C \simeq G/\mathbb{Z}z$, cyclically ordered in the following way: for all $a, b, c \in G$, $(a + \mathbb{Z}z, b + \mathbb{Z}z, c + \mathbb{Z}z)$ holds if and only if there exist $a' \in a + \mathbb{Z}z, b' \in b + \mathbb{Z}z, c' \in c + \mathbb{Z}z$ such that one of $0 \leq a' < b' < c' < z$ or $0 \leq b' < c' < a' < z$ or $0 \leq c' < a' < b' < z$ holds.

Let $l(G)$ be the maximal convex subgroup of G not containing z ; i.e., $l(G)$ is the largest proper convex subgroup of G . Note that $l(G) \subseteq]-z, z[$. Then the restriction

of the canonical epimorphism $p : G \rightarrow C$ to $l(G)$ is a monomorphism of totally ordered groups. Its image $l(C)$ is called the *linear part of C* because it is the largest totally ordered subgroup of C with respect to the ordering \leq_ϵ that we will define in Section 4.

By Swirczkowski's theorem (see [Sw 59]), $C/l(C)$ embeds in the multiplicative group of all complex numbers of absolute value 1.

In Section 2 we define $k[[C]]$, the ring of formal power series with coefficients in k and exponents in C , and $k[C]$, its ring of polynomials, in such a way that they coincide with the classical notions when C is a linear cyclically ordered group.

In Section 3, we prove the following:

Proposition 1 *There exists a subring A of $k[[G]]$ such that $A/(1 - X^z)A \simeq k[[C]]$.*

For such a ring A , let p_A be the canonical mapping from A onto $A/(1 - X^z)A$.

In Section 4, we give some examples of units and zero divisors in $k[[C]]$. Then, we prove:

Proposition 2 (a) *The semi-group of all zero divisors of $k[[C]]$ is the union of the following two subsets:*

- the p_A -image of the semi-group of all zero-divisors of A ,
- the p_A -image of the set of all elements σ such that $\sigma A \cap (1 - X^z)A \neq \sigma(1 - X^z)A$.

(b) *The group of all units of $k[[C]]$ is the p_A -image of the semi-group of all elements σ such that $\sigma A + (1 - X^z)A = A$.*

Theorem 3 *If $k[[C]]$ is a field, then k is a field, C is torsion free and $C/l(C)$ embeds in the group of all roots of unity. Conversely, if k is a field, C is torsion free and $C/l(C)$ is finite, then $k[[C]]$ is a field.*

Open Problem: Suppose that $k[[C]]$ is a field. Does this imply that $C/l(C)$ must be finite?

Theorem 4 *$k[C]$ is an integral domain if and only if k is an integral domain and C is torsion free.*

Open Problem: Is it true that $k[[C]]$ is an integral domain if and only if C is torsion free and k is an integral domain?

In Section 5 we define the *cyclic valuation* on $k[[C]]$ as a mapping v from $C \times k[[C]]$ onto $C_\infty := C \cup \{\infty\}$ (with $a <_b \infty$ for all $a, b \in C$). This extends the classical notion of a valuation in a natural way. Indeed, if C is a linear cyclically ordered group, then the usual valuation can be defined first order by means of the $v(a, \cdot)$, $a \in C$.

The first order properties of the cyclic valuations can be stated in several languages which we will compare, and which we will use to define the first order notion of a cyclically valued ring. Then, we prove:

Theorem 5 *A domain R is a subring of a ring $k[[C]]$, for some domain k , if and only if the following conditions hold:*

- (a) C is isomorphic to a subgroup C' of the group of units of R ,
- (b) there is a mapping $v : C \times R \rightarrow C \cup \{\infty\}$ such that (R, v) is a cyclically valued ring,
- (c) for all σ in R , the set $\{v(a, \sigma) \mid a \in C\}$ is well-ordered.

Throughout this paper, \mathbb{N} will denote the semi-group of all non-negative integers, and $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$ will denote the set all positive integers.

2 Definition of formal power series

A subset S of C will be called *well-ordered* if the totally ordered set (S, \leq_0) is well-ordered. It is not difficult to check that S is well-ordered if and only if, for all (or for some) $c \in C$, the totally ordered set (S, \leq_c) is well-ordered.

Lemma 2.1 *The sum of any two well-ordered subsets of C is well-ordered.*

Proof. Let S_1 and S_2 be two well-ordered subsets and $S = S_1 + S_2 = \{c_1 + c_2 \mid c_1 \in S_1, c_2 \in S_2\}$. The ordered set (C, \leq_0) is isomorphic to the subset $[0, z[$ of G . S_1 and S_2 are isomorphic to well-ordered subsets \tilde{S}_1 and \tilde{S}_2 of $[0, z[$, and $\tilde{S}_1 + \tilde{S}_2$ is a well-ordered subset of $[0, 2z[$. $S_1 + S_2$ is isomorphic to $((\tilde{S}_1 + \tilde{S}_2) \cap [0, z]) \cup (((\tilde{S}_1 + \tilde{S}_2) \cap [z, 2z]) - z)$, and this set is well-ordered. Hence $S_1 + S_2$ is well-ordered. \square

For all $\sigma \in k^C$, the set $\text{Supp}(\sigma) := \{c \in C \mid \sigma(c) \neq 0\}$ is called the *support* of σ . We denote by $k[[C]]$ the subset of k^C of all elements with well-ordered support. An element σ of $k[[C]]$ will be written in the form $\sigma = \sum_{c \in S} \sigma_c X^c$, where S is well-ordered, and for all c in S , $\sigma_c = \sigma(c)$. We call σ a *cyclic formal power series*. Note that if $\sigma_c = 0$ for all $c \notin S \cap S'$, then $\sum_{c \in S} \sigma_c X^c = \sum_{c \in S'} \sigma_c X^c$.

We let $k[C]$ be the subset of $k[[C]]$ of elements with finite support. An element of $k[C]$ will be called a *polynomial*.

We define addition on $k[[C]]$ by:

$$\sigma + \sigma' = \sum_{c \in S \cup S'} (\sigma_c + \sigma'_c) X^c,$$

and multiplication by:

$$\sigma \cdot \sigma' = \sum_{c \in S + S'} \left(\sum_{d \in S, d' \in S', d + d' = c} \sigma_d \cdot \sigma'_{d'} \right) X^c.$$

The small Σ is the symbol for a series, the large \sum represents the sum in the ring. Indeed, like in classical power series, one can prove that if S and S' are well-ordered, then for all $c \in S + S'$, there is only a finite number of $(d, d') \in S \times S'$ such that $d + d' = c$.

It is routine to prove that $(k[[C]], +, \cdot)$ is a ring, and $(k[C], +, \cdot)$ is a subring of $(k[[C]], +, \cdot)$.

Note that k is embedded in $k[C]$ in a natural way. Hence we will consider it as a subring of $k[C]$, the elements of k being the functions with support $\{0\}$. Also note that any ring of formal power series is a ring of cyclic formal power series.

3 Cyclic versus classical formal power series rings

In this section, we focus on connections between rings of formal power series with exponents in a cyclically ordered group, and rings of formal power series with exponents in a totally ordered group. We set some notations which we will use throughout this paper:

- $G_+ := \{g \in G \mid g \geq 0\}$.
- p is the canonical map from G onto C .
- $k[G]$ is the ring of polynomials with (possibly negative) exponents in G and coefficients in k .
- If $k[[C]]$ or $k[C]$ is an integral domain, then its fraction field is denoted $k((C))$ or $k(C)$, respectively.

Note that, if k is a field, then the fraction field $k((G))$ of $k[[G_+]]$ is equal to $k[[G]]$ because G is totally ordered. It is also equal to $\bigcup_{g \in G_+} X^{-g}k[[G_+]]$. Nothing of this kind holds for $k[[C]]$ (see Section 4), which need not even be an integral domain.

In order to prove that $k[[C]]$ is isomorphic to quotients of classical power series rings, we define the following subsets of $k[[G]]$:

$$A_M := \{\sigma \in k[[G]] \mid \forall c \in C, p^{-1}(\{c\}) \cap \text{Supp}(\sigma) \text{ is finite and } p(\text{Supp}(\sigma)) \text{ is well-ordered}\}.$$

$$A_{M+} := \{\sigma \in A_M \mid \text{Supp}(\sigma) \geq 0\}.$$

$$A_m := \{\sigma \in A_M \mid \text{Supp}(\sigma) \text{ is bounded}\}.$$

$$A_{m+} := A_{M+} \cap A_m.$$

$$A_0 := \{\sigma \in A_M \mid \text{Supp}(\sigma) \subset [0, z]\}.$$

A_0 is an additive subgroup of $k[[G]]$ but, in general, not a subring.

Observe that we can't drop the condition “ $p(\text{Supp}(\sigma))$ is well-ordered” in the definition of the ring A_M . Indeed, we can find a subset S of G which is well-ordered although $p(S)$ is not. Take $G = \mathbb{Q}$ (the group of rational numbers) and $z = 1$. Then $S = \{n + \frac{1}{n} \mid n \in \mathbb{N}^*\}$ is well-ordered, while $p(S) = \{\frac{1}{n} \mid n \in \mathbb{N}^*\}$ is not well-ordered.

Lemma 3.1 *The sets A_M and A_m are subrings of $k[[G]]$, A_{M+} and A_{m+} are subrings of $k[[G_+]]$.*

Proof. Note that these sets are non-empty because they contain 0 and $1 = X^0$.

We prove here that A_M is a subring of $k((G))$, the other proofs being similar. Take $\sigma, \sigma' \in A_M$. Then $\text{Supp}(-\sigma) = \text{Supp}(\sigma)$, hence $-\sigma \in A_M$. Further, $p(\text{Supp}(\sigma + \sigma')) \subset p(\text{Supp}(\sigma) \cup \text{Supp}(\sigma')) = p(\text{Supp}(\sigma)) \cup p(\text{Supp}(\sigma'))$ is well-ordered. For all $c \in C$, $p^{-1}(c) \cap (\text{Supp}(\sigma) \cup \text{Supp}(\sigma')) = (p^{-1}(c) \cap \text{Supp}(\sigma)) \cup (p^{-1}(c) \cap \text{Supp}(\sigma'))$ is finite. Hence, $\sigma + \sigma' \in A_M$.

Set $S := \text{Supp}(\sigma)$ and $S' := \text{Supp}(\sigma')$. We have that $\text{Supp}(\sigma\sigma') \subset S + S'$. Furthermore, the mapping $p : G \rightarrow C$ is a group homomorphism, hence $p(S + S') = p(S) + p(S')$ is well-ordered by Lemma 2.1. It follows that $p(\text{Supp}(\sigma\sigma'))$ is well-ordered. Now, take any $c \in C$ and assume that $p^{-1}(\{c\}) \cap \text{Supp}(\sigma\sigma')$ is infinite. Set $H := \{h \in S \mid \exists h' \in S', p(h + h') = c\}$, $H' := \{h' \in S' \mid \exists h \in S, p(h + h') = c\}$. Then one of H and H' is infinite. But, since each element in $p(S)$ has finitely many pre-images, H is finite if and only if $p(H)$ is, and the same holds for H' and $p(H')$, where $p(H)$ and $p(H')$ are both well-ordered in C_0 . Assume for instance, that $p(H)$ is infinite, hence it contains an infinite

increasing sequence, then $p(H')$ contains an infinite decreasing sequence, a contradiction. Consequently, $\sigma\sigma' \in A_M$. \square

Proposition 1 can be rephrased as follows:

Proposition 3.2 *Let A stand for any of the rings A_{M+} , A_M , A_{m+} , A_m , then $k[[C]] \simeq A/(1 - X^z)A$.*

Proof. We first prove this proposition for $A = A_M$. We define $p'_A : A_M \rightarrow k[[C]]$. For an element $\sum_{g \in S} \sigma_g X^g$ in A_M , we set

$$p'_A(\sum_{g \in S} \sigma_g X^g) = \sum_{c \in p(S)} \left(\sum_{h \in S \cap p^{-1}(\{c\})} \sigma_h \right) X^c \in k[[C]].$$

This definition makes sense because for each c in $p(S)$, $S \cap p^{-1}(\{c\})$ is a finite set. It is routine to check that the map p'_A is a ring epimorphism.

Take

$$\sigma = \sum_{g \in S} \sigma_g X^g \in A_M$$

and assume that S is the support of σ . We have $X^{-g_0}\sigma \in A_+$ for $g_0 = \min(\text{Supp}(\sigma))$. Therefore, we may assume that $\sigma \in A_{M+}$. We have

$$p'_A(\sigma) = \sum_{c \in p(S)} \left(\sum_{h \in S \cap p^{-1}(\{c\})} \sigma_h \right) X^c.$$

Hence,

$$p'_A(\sigma) = 0 \text{ if and only if, for all } c \in p(S), \sum_{h \in S \cap p^{-1}(\{c\})} \sigma_h = 0.$$

We assume $p'_A(\sigma) = 0$ and prove that $\sigma = (1 - X^z)\sigma'$ for some $\sigma' \in A_M$. For $c \in C$, we will denote by \tilde{c} the unique element of $[0, z[$ such that $p(\tilde{c}) = c$. Set $\tilde{S} := \{\tilde{c} \mid c \in p(S)\} = [0, z[\cap(p^{-1}(p(S)))$. Since $p(S)$ is well-ordered and isomorphic to \tilde{S} , $\tilde{S} + \mathbb{N}z$ is well-ordered too.

For $c \in p(S)$, $p^{-1}(\{c\}) = \tilde{c} + \mathbb{Z}z$, and $S \cap p^{-1}(\{c\})$ is finite. Let m_c and n_c in \mathbb{N} be such that $\sigma_{\tilde{c}+m_c \cdot z} \neq 0$, $\sigma_{\tilde{c}+n_c \cdot z} \neq 0$, and for $n > n_c$ or $n < m_c$, $\sigma_{\tilde{c}+n \cdot z} = 0$. It follows that

$$\sigma_{\tilde{c}+n_c \cdot z} = -\sigma_{\tilde{c}+m_c \cdot z} - \sigma_{\tilde{c}+(m_c+1) \cdot z} - \cdots - \sigma_{\tilde{c}+(n_c-1) \cdot z}.$$

For all $c \in p(S)$ and $m_c \leq i < n_c$, set $\sigma'_{\tilde{c}+i \cdot z} := \sigma_{\tilde{c}+m_c \cdot z} + \sigma_{\tilde{c}+(m_c+1) \cdot z} + \cdots + \sigma_{\tilde{c}+i \cdot z}$; otherwise set $\sigma'_g := 0$. Further, set

$$\sigma' = \sum_{g \in \tilde{S} + \mathbb{N}z} \sigma'_g X^g.$$

This is an element of A_{M+} since $\tilde{S} + \mathbb{N}z$ is well-ordered, and for all $c \in C$, $p^{-1}(\{c\}) \cap \text{Supp}(\sigma')$ is either empty or bounded above by $\tilde{c} + n_c z$ showing that its cardinality is at most n_c . Write

$$(1 - X^z)\sigma' = \sum_{g \in G} \sigma''_g X^g \in k[[G]].$$

If $g \notin \text{Supp}(\sigma') \cup (z + \text{Supp}(\sigma'))$, then $\sigma''_g = 0$. If $g \in \text{Supp}(\sigma') \cup (z + \text{Supp}(\sigma'))$, then there are $c \in p(S)$ and $m_c \leq i \leq n_c$ with $g = \tilde{c} + i \cdot z$. We have:

$$\sigma''_g = \begin{cases} \sigma'_{\tilde{c}+m_c \cdot z} = \sigma_{\tilde{c}+m_c \cdot z} & \text{if } i = m_c \\ \sigma'_{\tilde{c}+i \cdot z} - \sigma'_{\tilde{c}+(i-1) \cdot z} = \sigma_{\tilde{c}+i \cdot z} & \text{if } m_c < i < n_c \\ -\sigma'_{\tilde{c}+(n_c-1) \cdot z} = -\sigma_{\tilde{c}+m_c \cdot z} - \sigma_{\tilde{c}+(m_c+1) \cdot z} - \cdots - \sigma_{\tilde{c}+(n_c-1) \cdot z} = \sigma_{\tilde{c}+n_c \cdot z} & \text{if } i = n_c . \end{cases}$$

It follows that $(1 - X^z)\sigma' = \sigma$, that is, $\sigma \in (1 - X^z)A_M$.

Since p'_A is a ring homomorphism and $p'_A(1 - X^z) = 0$, we have shown that $\ker p_A = (1 - X^z)A_M$, and therefore, $k[[C]] \simeq A_M/(1 - X^z)A_M$. Observe that p'_A is indeed the canonical mapping p_A .

If A stands for A_{M+} , A_m or A_{m+} , then $\ker p'_A[A = \ker p'_A \cap A = (1 - X^z)A_M \cap A = (1 - X^z)A$. \square

Since $A_0 \cup \{X^z\}$ generates A_{m+} , we have:

Remark 3.3 The family of all subrings A of A_M containing X^z and such that $p_A(A) = k[[C]]$ can be ordered by inclusion. Its smallest element is A_{m+} . Indeed, any element σ of A_M is equivalent modulo $(1 - X^z)A_M$ to an element of A_0 , namely $(p_A[A_0])^{-1}(p_A(\sigma))$.

4 Units and zero divisors

It is not difficult to see that $k[[C]]$ may contain zero divisors. For example, let $m > 1$ be an integer and suppose that there is some $g \in G$ such that $mg = z$. Then

$$(1 - X^g)(1 + X^g + X^{2g} + \cdots + X^{(m-1)g}) = 1 - X^z \in p_A^{-1}(\{0\}) .$$

Since $C \simeq G/\mathbb{Z}z$ where G is torsion free, such m and g exist if and only if C is not torsion free. Therefore, we have shown:

Lemma 4.1 *If $k[[C]]$ is an integral domain, then C is torsion free.*

Trivial examples of units are the elements X^c , with $c \in C$. The following properties of cyclically ordered groups will provide less trivial examples.

Definition 4.2 We set $P := \{c \in C \mid (0, c, -c)\}$. From the general properties of cyclically ordered groups, we know that there exists at most one element of order 2, which we shall denote by ϵ . Hence, C is a disjoint union $C = P \cup -P \cup \{c \mid c = -c\}$, where $\{c \mid c = -c\}$ has one or two elements. If there is such an ϵ in C , then we have $b \leq_0 \epsilon \leq_0 -a$ for all $(a, b) \in P \times P$. If not, then ϵ will denote the element of the Dedekind completion of (C, \leq_0) such that for any $a, b \in P$, $b \leq_0 \epsilon \leq_0 -a$. In both cases, we define \leq_ϵ by: $a \leq_\epsilon b$ if and only if either $(a, b) \in -P \times (P \cup \{0\})$, or $(a, b) \in (-P \times (-P \cup \{0\})) \cup ((P \cup \{0\}) \times P)$ and $a \leq_0 b$.

The linear part $l(C)$ of C defined in the introduction is the largest totally ordered subgroup of (C, \leq_ϵ) . (C is a linear cyclically ordered group if and only if $C = l(C)$.) As

mentioned, $l(C)$ is the image of the maximal convex subgroup $l(G)$ of G not containing z under the canonical epimorphism $p : G \rightarrow C$. Its restriction to $l(G)$ is a monomorphism of totally ordered groups. We lift this monomorphism to $k[[l(G)]]$ by setting $p_l(\lambda X^g) = \lambda X^{p_l(g)}$ for $\lambda \in k$ and $g \in l(G)$, and then using additivity and multiplicativity, such that p_l becomes a field embedding. Via this embedding, we can assume $k[[l(G)]] \subset k[[C]]$.

If k is a field, then every element of $k[[l(G)]] \setminus \{0\}$ and every non-zero monomial is a unit in $k[[C]]$. But $k[[C]]$ may also contain units which are not monomials and do not belong to $k[[l(G)]]$. Indeed, let $m > 1$ be an integer. If λ_1, λ_2 are elements of k such that $\lambda_1^m - \lambda_2^m = 1$ and if there exists g such that $mg = z$, then

$$(\lambda_1 - \lambda_2 X^g)(\lambda_1^{m-1} + \lambda_1^{m-2} \lambda_2 X^g + \cdots + \lambda_2^{m-1} X^{(m-1)g}) = (\lambda_1^m - \lambda_2^m X^z) \in p_A^{-1}(\{1\})$$

For example, if $2g = z$, $(\sqrt{2} + X^g)(\sqrt{2} - X^g) = 2 - X^z \in p_A^{-1}(\{1\})$.

Let us give yet another example of a unit. Let q be a positive integer and G be the subgroup of $\mathbb{Q} \overline{\times} \mathbb{Q}$ generated by $(1, 0) = z$, $(0, 1)$ and $(\frac{1}{q}, \frac{1}{q})$. Now let $C := G/(\mathbb{Z}z)$, $k := \mathbb{Q}$, $c := p(\frac{1}{q}, \frac{1}{q}) \in C$, $S_i := \{p(\frac{i}{q}, n + \frac{i}{q}) \mid n \in \mathbb{N}\} = ic + p(\{0\} \times \mathbb{N})$ for $0 \leq i \leq q-1$, $S := \bigcup_{j=0}^{q-1} S_j$, and $\sigma := \sum_{s \in S} X^s = \sum_{n \in \mathbb{N}} X^{p(0,n)}(1 + X^c + \cdots + X^{(q-1)c})$. Then $\sigma \in k[[C]]$ because S is a well-ordered subset of C . Since $X^{qc} = X^{p(0,1)}$, we have:

$$\begin{aligned} (1 - X^c)\sigma &= (1 - X^c) \sum_{n \in \mathbb{N}} X^{p(0,n)} (1 + X^c + \cdots + X^{(q-1)c}) \\ &= (1 - X^{qc}) \sum_{n \in \mathbb{N}} X^{p(0,n)} = \sum_{n \in \mathbb{N}} X^{p(0,n)} - \sum_{n \in \mathbb{N}^*} X^{p(0,n)} = 1. \end{aligned}$$

Hence, $1 - X^c$ and σ are units.

Proof of Proposition 2.

(a) First we note that $1 - X^z$ is not a zero divisor. Indeed, 1 is a regular element, hence for all σ in A , the lowest element of the support of σ remains the lowest element of the support of $(1 - X^z)\sigma$. It follows that if $\sigma_1 \notin (1 - X^z)A$ and there exists σ_2 such that $\sigma_1 \sigma_2 = 0$, then we can assume that $\sigma_2 \notin (1 - X^z)A$. Consequently, $p_A(\sigma_1)$ is a zero divisor in $k[[C]]$.

Assume that σ_1 is a regular element. Then $p_A(\sigma_1)$ is a non-trivial zero divisor if and only if $p_A(\sigma_1) \neq 0$ and there exists $\sigma_2 \in A$ such that $p_A(\sigma_2) \neq 0$ and $p_A(\sigma_1)p_A(\sigma_2) = 0$, or equivalently:

(*) $\sigma_1 \notin (1 - X^z)A$ and there exist $\sigma_2 \notin (1 - X^z)A$, $\tau \in A$ such that $\sigma_1 \sigma_2 = (1 - X^z)\tau$.

Now consider the condition $\sigma_1 A \cap (1 - X^z)A \neq \sigma_1(1 - X^z)A$. This is equivalent to $\exists \sigma_2 \in A$, $\exists \tau \in A$, $\sigma_1 \sigma_2 = (1 - X^z)\tau$ and $\sigma_1 \sigma_2 \notin \sigma_1(1 - X^z)A$ (because $\sigma_1(1 - X^z)A \subset \sigma_1 A \cap (1 - X^z)A$). Since σ_1 is a regular element, this condition is equivalent to (*).

(b) For all $\sigma \in A$,

$$\begin{aligned} p_A(\sigma) \text{ is a unit} &\Leftrightarrow \exists \sigma', p_A(\sigma \sigma') - 1 = 0 \\ &\Leftrightarrow \exists \sigma', \sigma \sigma' - 1 \in (1 - X^z)A \\ &\Leftrightarrow \exists \sigma', \exists \tau, \sigma \sigma' - 1 = (1 - X^z)\tau \\ &\Leftrightarrow \exists \sigma', \exists \tau, \sigma \sigma' + (1 - X^z)\tau = 1. \end{aligned}$$

□

Proof of Theorem 3.

First assume that $k[[C]]$ is a field. Take $\sigma \in k \setminus \{0\}$, that is, $\text{Supp}(\sigma) = \{0\}$, and let σ^{-1} be the inverse of σ in $k[[C]]$. $\{0\} = \text{Supp}(\{1\}) = \text{Supp}(\sigma\sigma^{-1}) = \text{Supp}(\sigma^{-1})$ (because $\sigma \in k$), hence $\sigma^{-1} \in k$. Therefore, k is a field. From Lemma 4.1, it follows that C is torsion free.

We know that $C/l(C)$ embeds in the multiplicative group of all complex numbers of absolute value 1. We prove that, under our present hypothesis, every element of $C/l(C)$ must be a root of unity. In order to deduce a contradiction, assume that there exists $g \in G$ such that $l(G) < g < z + l(G)$ and that the class \bar{g} of g modulo $l(G)$ and the class \bar{z} of z modulo $l(G)$ are rationally independent. Set $c := p(g) \in C$, $c \neq 0$, and $\sigma := (1 - X^c)$, and let $\sigma^{-1} := \sum_{s \in C} \lambda_s X^s$ be the inverse of $(1 - X^c)$ in $k[[C]]$. Then $1 = \sum_{s \in C} (\lambda_s - \lambda_{s-c}) X^s$. Hence, for all $s \in C$,

$$\lambda_s - \lambda_{s-c} = \begin{cases} 0 & \text{if } s \neq 0 \\ 1 & \text{if } s = 0 \end{cases}$$

If $\lambda_0 \neq 0$, then $\lambda_{nc} = \lambda_0 \neq 0$ for all $n > 0$. If $\lambda_0 = 0$, then $\lambda_{-c} = 1 \neq 0$, and $\lambda_{-nc} = \lambda_{-c} = 1 \neq 0$ for all $n > 0$. Assume $\lambda_{nc} \neq 0$ for all $n > 0$ (the case of $\forall n > 0, \lambda_{nc} \neq 0$ for all $n > 0$ is similar, because $0 \neq -c \in C$).

The quotient group $\Gamma = G/l(G)$ is archimedean because $\mathbb{Z}z$ is cofinal in G . In the archimedean group Γ , \bar{z} and \bar{c} are rationally independent, hence the image of $\mathbb{Z}\bar{c}$ in the quotient group $\Gamma/(\mathbb{Z}\bar{z})$ is dense. In particular, it is not well-ordered. This implies that $\{nc \mid n > 1\}$ is a subset of $\text{Supp}(\sigma^{-1})$ which is not well-ordered: a contradiction.

Now assume that C is torsion free and $C/l(C)$ is finite. Let n be the cardinality of $C/l(C)$; then $C/l(C)$ is isomorphic to the group of all n^{th} roots of unity. By hypothesis, there exist g in C and l in $l(C)$ such that $ng = l$ and C is the disjoint union $l(C) \cup (g + l(C)) \cup \dots \cup ((n-1)g + l(C))$. Note that, for every element c of C , nc belongs to $l(C)$. For c_1 and c_2 in C we set $c_1 <' c_2 \Leftrightarrow nc_1 <_{\epsilon} nc_2$. Then $(C, <')$ is a totally ordered group. Let $S \subset C$. Then there exist subsets S_0, S_1, \dots, S_{n-1} of $l(C)$ such that $S = S_0 \cup (g + S_1) \cup \dots \cup ((n-1)g + S_{n-1})$. It follows that S is well-ordered in $(C, <_{\epsilon})$ if and only if S_0, S_1, \dots, S_{n-1} are well-ordered, if and only if S is well-ordered in $(C, <')$. Hence, $k[[C]]$ is isomorphic to $k[[l(C)]] [Y]$, with $Y^n = X^l \in k[[l(C)]]$. In particular, $k[[C]]$ is a field. □

From Lemma 4.1, we see that a necessary condition for $k[[C]]$ to be an integral domain is that C is torsion free. Another condition is that k be an integral domain. We shall prove that for the ring of polynomials $k[C]$, these conditions are also sufficient. For this purpose, we need the following well known lemma.

Lemma 4.3 *Let k be a field containing a primitive n -th root of unity ζ , where $n \geq 2$. Then $1 - X^n = \prod_{i=0}^{n-1} (\zeta^i - X)$. Let $P(X) = 1 + \dots$ and $Q(X) = 1 + \dots$ be two polynomials of $k[X]$ such that $P(X)Q(X) = 1 - a^n X^n$, with $a \in k$. Then, there exists a partition $\{I, J\}$*

of $\{0, \dots, n-1\}$ such that $P(X) = (\prod_{i \in J} \zeta^i) \prod_{i \in I} (\zeta^i - aX)$ and $Q(X) = (\prod_{i \in I} \zeta^i) \prod_{i \in J} (\zeta^i - aX)$. In particular, $P(X)$ and $Q(X)$ belong to $\mathbb{Z}(\zeta)[aX]$.

Proposition 4.4 *Assume that k is an integral domain. Then $1 - X^z$ is prime in $k[G_+]$ if and only if z is not divisible by any natural number bigger than 1 in G .*

Proof. First assume that there are two polynomials P and Q in $k[G_+]$ such that $P(X)Q(X) = 1 - X^z$. After multiplying with a suitable constant, we can assume that $P(X) = 1 + \lambda_1 X^{a_1} + \dots$, $Q(X) = 1 + \lambda'_1 X^{b_1} + \dots$. Then $P(X)Q(X) = 1 + \lambda_1 X^{a_1} + \lambda'_1 X^{b_1} + \lambda_1 \lambda'_1 X^{a_1+b_1} + T(X)$, where all terms in $T(X)$ are of degree $> \min(a_1, b_1) > 0$. It follows that $\lambda_1 X^{a_1} + \lambda'_1 X^{b_1} = 0$. In particular, $a_1 = b_1$ and therefore, $\text{Supp}(P) \cap \text{Supp}(Q)$ contains non-zero elements.

Since k is assumed to be an integral domain, we may replace it by its fraction field. So we may assume k is a field. For further purposes, we also assume that k is closed under roots of unity.

Let $D(G)$ be the divisible hull of G . The number of exponents of the polynomials is finite. So we can find rationally independent exponents $\alpha_1, \dots, \alpha_n$, such that z and the exponents of P and Q are all in $\mathbb{N}\alpha_1 + \dots + \mathbb{N}\alpha_n$ (the existence of the α_i 's can be proved by an iterative process like the Algorithm of Perron quoted in [Za 40]). Set $X_1 = X^{\alpha_1}$, \dots , $X_n = X^{\alpha_n}$.

Let $z = c_1\alpha_1 + \dots + c_n\alpha_n$, with $c_i \in \mathbb{N}$, so

$$1 - X^z = 1 - X_1^{c_1} \dots X_n^{c_n}.$$

We have $P(X_1, \dots, X_n)Q(X_1, \dots, X_n) = 1 - X_1^{c_1} \dots X_n^{c_n}$. But $\text{Supp}(P) \cap \text{Supp}(Q)$ contains non-zero elements. Hence there exists i , say $i = n$, such that $\deg_{X_n}(P) \geq 1$ and $\deg_{X_n}(Q) \geq 1$ (hence $c_n = \deg_{X_n}(P) + \deg_{X_n}(Q) \geq 2$). Therefore, P and Q are in $k(X_1^{1/c_n}, \dots, X_{n-1}^{1/c_n})[X_n]$.

Let $\zeta \in k$ be an n -th root of unity, and set $Y := X_1^{c_1/c_n} \dots X_{n-1}^{c_{n-1}/c_n} X_n$. Then, by Lemma 4.3, P and Q are elements of $\mathbb{Z}(\zeta)[Y]$. Furthermore, since $\deg_{X_n}(P) \geq 1$ and $\deg_{X_n}(Q) \geq 1$, we have $\deg_Y(P) \geq 1$ and $\deg_Y(Q) \geq 1$. Set $d := \deg_Y(P)$. Then there exists $r_d \in \mathbb{Z}(\zeta) \setminus \{0\}$ such that one of the monomials in P is $r_d X_1^{dc_1/c_n} \dots X_n^{dc_n/c_n} X_n^d = r_d X^{(d/c_n)(c_1\alpha_1 + \dots + c_n\alpha_n)} = r_d X^{(d/c_n)z}$. Hence $(d/c_n)z \in G$.

Set $\frac{d}{c_n} = \frac{u}{v}$ with u, v in \mathbb{N}^* and $\gcd(u, v) = 1$, and let u', v' in \mathbb{Z} such that $uu' + vv' = 1$. Then $\frac{d}{c_n}z = \frac{u}{v}z$, hence $v'z + u'\frac{u}{v}z = \frac{vv' + uu'}{v}z = \frac{1}{v}z$ and $\frac{1}{v}z \in G$. But $d < c_n$, therefore $v > 1$. Hence z has a proper divisor in G .

If $1 - X^z$ divides $P(X)Q(X)$, then we can assume that $P(X)$, $Q(X)$, and X^z are polynomials (in the usual sense) with a finite number of variables, and they belong to a factorial ring (by embedding k in its fraction field). Therefore, there exist $P_1(X)$ and $Q_1(X)$ such that $P_1(X)Q_1(X) = 1 - X^z$, and as in the previous case, we see that z has a proper divisor. \square

Proof of Theorem 4.

The condition “ z is not divisible by an integer bigger than 1” is equivalent to “ C is torsion free”. Now, Theorem 4 follows from Proposition 4.4. \square

5 Cyclic valuations

In this section, k is an integral domain. If C contains a non-trivial 2-torsion element, then we let ϵ be this element; otherwise, $<_\epsilon$ has been defined in Definition 4.2. We set $C_\epsilon = C \cup \{\epsilon\}$. We define a mapping v from $C_\epsilon \times k[[C]]$ onto C_∞ by setting $v(a, \sigma) = \min_a \text{Supp}(\sigma)$ if $\sigma \neq 0$ and $v(a, 0) = \infty$.

It is routine to check that $(k[[C]], +, v(a, \cdot))$ is a valued group, for every $a \in C_\epsilon$. In particular, for all σ_1 and σ_2 in $k[[C]]$, $v(a, \sigma_1 - \sigma_2) \geq_a \min_a(v(a, \sigma_1), v(a, \sigma_2))$, and if $v(a, \sigma_1) \neq v(a, \sigma_2)$, then $v(a, \sigma_1 - \sigma_2) = \min_a(v(a, \sigma_1), v(a, \sigma_2))$.

The behaviour of the $v(a, \cdot)$'s with respect to multiplication is not trivial. However, observe that for all a, b in C and σ in $k[[C]]$, $v(a, \sigma) = v(b, X^{b-a}\sigma) + a - b$. If τ is a monomial of degree $b - a$, then $v(a, \sigma) = v(b, \tau\sigma) + a - b$.

If C is a linear cyclically ordered group, then $k[[C]]$ is the usual ring of formal power series, and we know that there is a canonical valuation defined on $k[[C]]$. This valuation is $v(\epsilon, \cdot)$ but is not among the $v(a, \cdot)$'s, $a \in C$. Indeed, for all $a \in C$, we can find some $\sigma \in k[[C]]$ (for instance, a sum of two monomials) such that $v(\epsilon, \sigma) \neq v(a, \sigma)$.

If C is not a linear cyclically ordered group, then there exist a and b in P with $a+b \in -P$, with P as defined in Definition 4.2. Therefore, $v(\epsilon, 1+X^a) = v(\epsilon, 1+X^b) = 0$, $v(\epsilon, (1+X^a)(1+X^b)) = a+b \neq 0 = v(\epsilon, 1+X^a) + v(\epsilon, 1+X^b)$. Hence, $v(\epsilon, \cdot)$ is not a valuation in the usual sense.

We consider $k[[C]] \cup C_\epsilon$ as a structure of a two-sorted language \mathcal{L} containing the usual function, relation and constant symbols for the ring and the value group sort. Then $\mathcal{L} \cup \{v\}$ will be the language \mathcal{L} together with a function symbol interpreted by the mapping v .

The support mapping is interpretable in the language $\mathcal{L} \cup \{v\}$. Indeed, let $\sigma \in k[[C]]$. Then the support of σ is the set $\text{Supp}(\sigma) = \{v(a, \sigma) \mid a \in C\} \setminus \{\infty\}$. It follows that the set of all monomials and the degree map of monomials are definable in the language $\mathcal{L} \cup \{v\}$. In the same way, the set of all constant polynomials is definable in the language $\mathcal{L} \cup \{v\}$.

Observe that we can also characterize the monomials by other means. Indeed, $\sigma \in k[[C]] \setminus \{0\}$ is a monomial if and only if $\forall \tau \in k[[C]]$, $v(v(0, \sigma), \tau\sigma) = v(0, \sigma) + v(0, \tau)$. If σ is a monomial, its degree is $v(a, \sigma) = v(0, \sigma)$ for all $a \in C$.

Another characterization of the constant polynomials follows from:

Remark 5.1 Let $\sigma \in k[[C]] \setminus \{0\}$, then σ is a constant if and only if one of the following equivalent formulas is satisfied in M .

- (a) $\forall a \in C_\epsilon, \forall \tau \in k[[C]], v(a, \sigma\tau) = v(a, \tau)$.
- (b) $\exists a \in C, \forall \tau \in k[[C]], v(a, \sigma\tau) = v(a, \tau)$.

Proof. If σ is a constant, then (a) holds. (a) \implies (b) is trivial.

Assume that σ is not a constant and take $a \in C$. If $v(a, \sigma) \neq 0$ and if $\tau = 1$, then $v(a, \sigma\tau) \neq v(a, \tau) = 0$. So we suppose that $v(a, \sigma) = 0$. Then there exist $\lambda, \lambda_1 \in k$, $g_1 \in C$, with $\lambda_1 \neq 0 \neq \lambda$, and $0 <_0 g_1 <_0 a$, such that $\sigma = \lambda + \lambda_1 X^{g_1} + \dots$, (necessarily, all the elements of the support are in $[0, a[$, that is, greater than or equal to 0 with respect

to \leq_a). Then set $\tau = X^{a-g_1}$, $v(a, \sigma\tau) = a \neq v(a, \tau)$. This proves that (b) implies that σ is a constant. \square

Before we define structures in the language $\mathcal{L} \cup \{v\}$, we focus on two languages for the rings $k[[C]]$. First, we let M be a unary predicate interpreted by: $M(\sigma) \Leftrightarrow \sigma$ is a monomial. Then we have the following

Proposition 5.2 *In our structure $k[[C]] \cup C_\infty$, the languages $\mathcal{L} \cup \{v\}$ and $\mathcal{L} \cup \{v(0, \cdot), M\}$ are bi-interpretable.*

Proof. The set of all monomials is definable in $\mathcal{L} \cup \{v\}$. Hence, $\mathcal{L} \cup \{v(0, \cdot), M\}$ is interpretable in $\mathcal{L} \cup \{v\}$. Now, let $a \in C$ and $\sigma \in k[[C]]$ and take τ an invertible monomial such that $v(0, \tau) = a$. Then, $v(a, \sigma) = v(0, \tau^{-1}\sigma) + a$. Hence, $\mathcal{L} \cup \{v\}$ is interpretable in $\mathcal{L} \cup \{v(0, \cdot), M\}$. \square

In the ring $k[[C]]$, the multiplicative subgroup $\{X^c \mid c \in C\}$ is isomorphic to the group C . We can introduce a cyclic order on $\{X^c \mid c \in C\}$ which is isomorphic to the cyclic order of C . We can also define a valuation in a different way: set $v'(X^a, \sigma) := X^b$ if and only if $v(a, \sigma) = b$, and for all $a \in C$, set $v'(X^a, 0) := 0$ (the 0 of the ring replaces the ∞ of C). Now, we consider $k[[C]]$ as a structure of a language \mathcal{L}' consisting of the language of rings together with the predicate v , a predicate interpreted by the multiplicative group $\{X^c \mid c \in C\}$, and a predicate for the cyclic order on $\{X^c \mid c \in C\}$, with, for all a, b in C , $(X^a, X^b, 0)$.

Proposition 5.3 *The subgroup $\{X^c \mid c \in C\}$ is not definable in the language $\mathcal{L} \cup \{v\}$.*

Proof. Assume that k is algebraically closed, and that C contains a torsion free divisible subgroup C_1 , such that C_1 is a direct summand, $C = C_1 \oplus C_2$. We know that C_1 is a \mathbb{Q} -vector space, hence it admits a basis. For all element c in this basis, we let α_c be a constant, with $0 \neq \alpha_c \neq 1$. For $c \in C_2$, we set $\alpha_c = 1$, and we extend $c \mapsto \alpha_c$ as an isomorphism from the group C into (k, \cdot) . Now, we set $\forall c \in C$, $\varphi(X^c) := \alpha_c X^c$, and we extend φ to a homomorphism from $k[[C]]$ onto $k[[C]]$, such that the restriction of φ to k is the identity. Then φ induces an $\mathcal{L}' \cup \{v'(X^0, \cdot)\}$ -isomorphism. We have constructed two distinct $\mathcal{L}' \cup \{v'(X^0, \cdot)\}$ -structures on $k[[C]]$. But in both cases, the induced $\mathcal{L} \cup \{v\}$ -structure is the same. It follows that the subgroup $\{X^c \mid c \in C\}$ is not definable in the language $\mathcal{L} \cup \{v\}$. However, it is interpretable because it is isomorphic to the quotient of the group of invertible monomials by the group of invertible constants. \square

The remainder of this section is devoted to the definition of $\mathcal{L} \cup \{v\}$ -structures involving the rings $k[[C]]$. We will specify which of them can be embedded in a ring of formal power series with cyclically ordered exponents.

Definition 5.4 Let $(R, +, \cdot)$ be a domain, v a mapping from $C \times R$ onto $C \cup \{\infty\}$, and $\sigma \in R$. The *support* of σ is the set $\text{Supp}(\sigma) := \{v(a, \sigma) \mid a \in C\}$; σ is a *monomial* if the support of σ is a singleton. σ is a *constant* if $\sigma = 0$ or $\text{Supp}(\sigma) = \{0\}$. We will say that (R, v) is a *cyclically valued ring* if the following conditions hold.

- (1) For all $a \in C$, $(R, +, v(a, \cdot))$ is a valued group.
- (2) For all $\sigma \in R$ and $a \in C$, if $v(a, \sigma) = a$, then there exists a unique monomial $\mu_{a, \sigma}$ such that $v(a, \sigma - \mu_{a, \sigma}) \neq a$.
- (3) For all $\sigma \in R$ and $a \in C$, $\min_a(\text{Supp}(\sigma))$ exists and is equal to $v(a, \sigma)$.
- (4) For all σ and σ' in R , $\text{Supp}(\sigma\sigma') \subset \text{Supp}(\sigma) + \text{Supp}(\sigma')$.
- (5) For all $n \in \mathbb{N}^*$, $a \in C$, $\sigma \in R$ and $\sigma' \in R$, if $\text{Supp}(\sigma) \cap (a - \text{Supp}(\sigma')) = \{a_1, \dots, a_n\}$, then $\mu_{a, \sigma\sigma'} = \mu_{a_1, \sigma}\mu_{a-a_1, \sigma'} + \dots + \mu_{a_n, \sigma}\mu_{a-a_n, \sigma'}$.

Clearly, in the language $\mathcal{L} \cup \{v\}$, the ring $k[[C]]$ is a cyclically valued ring.

Observe that if (R, v) is a cyclically valued ring, then the set of all constants of R is a subring of R . Indeed, let σ_1 and σ_2 be constants. By condition (4), $\sigma_1\sigma_2$ is a constant. Let $a \in \text{Supp}(\sigma_1 + \sigma_2)$. Then $a = v(a, \sigma_1 + \sigma_2) \geq_a \min_a(v(a, \sigma_1), v(a, \sigma_2)) = 0$. Hence $a = 0$. Theorem 5 now follows from:

Theorem 5.5 *Let (R, v) be a cyclically valued ring with ring of constants k . Assume that the support of every element of R is well-ordered, and that there is an isomorphism $c \mapsto m_c$ from $(C, +)$ to (R, \cdot) such that for all $c \in C$, m_c is a monomial of degree c . Then the cyclically valued ring (R, v) is isomorphic to a subring of $k[[C]]$.*

Proof. Let $\sigma \in R$ and $a \in C$. If $v(a, \sigma) \neq a$, we set $\sigma_a := 0$; if $v(a, \sigma) = a$, we set $\sigma_a := \mu_{a, \sigma}m_a^{-1}$. In any case, σ_a is a constant. We have $\sum_{a \in C} \sigma_a X^a \in k[[C]]$, because the support of σ is well-ordered. Now, we set $\varphi(\sigma) := \sum_{a \in C} \sigma_a X^a$. From (3), we deduce $\forall a \in C, \forall \sigma \in R, v(a, \varphi(\sigma)) = v(a, \sigma)$.

Take $\sigma, \sigma' \in R$. For all $a \in C$, $(\sigma + \sigma')_a = \sigma_a + \sigma'_a$, hence $\varphi(\sigma + \sigma') = \varphi(\sigma) + \varphi(\sigma')$. By (5), we have $\varphi(\sigma\sigma') = \varphi(\sigma)\varphi(\sigma')$. We have proved that φ is a homomorphism.

Assume that $\sigma \neq \sigma'$, and let $a \in \text{Supp}(\sigma - \sigma')$. Then $v(a, \sigma - \sigma') = a$, and

$$\begin{aligned} v(a, (\sigma - \sigma') - (\sigma_a m_a - \sigma'_a m_a)) &= v(a, (\sigma - \sigma_a m_a) - (\sigma' - \sigma'_a m_a)) \\ &\geq_a \min_a(v(a, \sigma - \sigma_a m_a), v(a, \sigma' - \sigma'_a m_a)) \\ &>_a a. \end{aligned}$$

Hence, $v(a, \sigma_a m_a - \sigma'_a m_a) = a$. In particular, $\sigma_a \neq \sigma'_a$. It follows that φ is one-to-one. \square

References

- [Fu 63] L. Fuchs, *Partially ordered algebraic systems*, Pergamon Press (1963).
- [Sw 59] S. Swirczkowski, *On cyclically ordered groups*, Fund. Math. **47** (1959), 161–166.
- [Za 40] O. Zariski, *Local uniformization on algebraic varieties*, Ann. Math. **41** (1940), 852–896.

Michèle Giraudet, Gérard Leloup,
U.P.R.E.S.A. 7056 (Equipe de Logique, Paris VII)
and Département de Mathématiques, Faculté des Sciences,
avenue Olivier Messiaen, 72085 Le Mans Cedex, France
giraudet@logique.jussieu.fr, leloup@logique.jussieu.fr

Franz-Viktor Kuhlmann,
Mathematical Sciences Group, University of Saskatchewan,
106 Wiggins Road, Saskatoon, Saskatchewan, Canada S7N 5E6
email: fvk@math.usask.ca — home page: <http://math.usask.ca/~fvk/index.html>