JOURNAL OF ALGEBRA **173**, 566–586 (1995)

Special Properties of Generalized Power Series

PAULO RIBENBOIM

Department of Mathematics and Statistics, Queen's University, Kingston, Ontario K7I3N6, Canada

Communicated by David Buchsbaum

Received July 25, 1993

This is a sequel to my previous papers on generalized power series. For the convenience of the reader I gather in the first section the definitions and results which shall be required. Any missing proof is either very easy or is already in one of the above quoted papers. After the preliminaries, I characterize (under suitable conditions) the generalized power series which are powers; the essential idea is to extend the validity of the usual binomial series. A short section gives conditions for a ring of generalized power series to be a real ring. As known, the ring of usual power series with coefficients in a field, in any number of indeterminates, is a unique factorization domain. I show that the result holds for generalized power series with exponents in a free-ordered monoid which is noetherian and narrow. This leads to interesting examples of unique factorization domains. Completely integrally closed domains of generalized power series are also characterized in terms of their ring of coefficients and monoid of exponents. The final section is devoted to seminormal domains. The main results about usual power series are extended to generalized power series.

1. PRELIMINARIES

(A) *Monoids*

A *monoid* is a set endowed with an associative, commutative binary operation and having a neutral element. Unless stated otherwise, the operation shall be written additively and the neutral element will be denoted by 0.

Let S be a monoid. The element $t \in S$ is *cancellative* when the following property holds: if $s, s' \in S$ and $s + t = s' + t$, then $s = s'$. Let $C(S)$ be the set of cancellative elements of S. The monoid S is *cancellative* when $S = C(S)$.

If S is a cancellative monoid, the *group of differences*, defined in the usual way, is denoted by $\hat{S} = S - S$.

0021-8693/95 $6.00

Let $G(S) = \{s \in S \mid \text{there exists } t \in S \text{ such that } s + t = 0\}$; then $G(S)$ is the largest subgroup of the monoid S.

The monoid S is *torsion-free* when the following property holds: if $s, t \in S$, $k \geq 1$ is an integer and $ks = kt$, then $s = t$.

A subset T of S is a *set of generators* of S if every $s \in S$ may be written in the form $s = \sum_{i=1}^{m} k_i t_i$ with $m \geq 0$, $k_i \geq 1$, and $t_1, \ldots, t_m \in T$.

A subset T of S is *independent* when the following condition holds: if $\sum_{t \in T} k(t)t = \sum_{t \in T} k'(t)t$ (with $k(t), k'(t)$ natural numbers such that only finitely many are different from 0), then $k(t) = k'(t)$ for every $t \in T$.

S is a *free monoid* if it has an independent set of generators.

If S is a free monoid, then S is torsion-free and cancellative.

If $n \geq 1$ and $X \subseteq S$, I shall use the notation $nX = \{x_1 + \cdots + s_n \mid s_1, \ldots, s_n \in X\}$.

(B) *Ordered Sets*

Let $(S, \leq)$ be an ordered set. It is not assumed that $\leq$ is a total order, nor is it excluded that $\leq$ be the trivial order ($s \leq t$ only when $s = t$).

$(S, \leq)$ is *artinian* (resp., noetherian) if every strictly descending (resp. ascending) sequence of elements of S is finite.

$(S, \leq)$ is *narrow* if every subset of pairwise order-incomparable elements of S is finite.

(1.1). S is finite if and only if S is artinian, noetherian, and narrow.

(1.2). S is artinian and narrow if and only if the following condition holds: if $(s_n)_{n \geq 1}$ is any sequence of elements of S, there exists a sequence $n_1 < n_2 < \cdots$ such that $s_{n_1} \leq s_{n_2} \leq \cdots$.

If $(S_i, \leq_i)$ (for $i \in I$) is a family of ordered sets, the product order $\leq$ on $S = \prod_{i \in I} S_i$ is defined componentwise: $(s_i)_i \leq (t_i)_i$ when $s_i \leq_i t_i$ for every $i \in I$.

(1.3). If $(S_i, \leq_i)$ are artinian and narrow sets (for $i = 1, \ldots, n$), then $(\prod_{i=1}^{n} S_i, \leq)$ (where $\leq$ is the product order) is artinian and narrow.

Let $\leq, \leq'$ be orders on the set S. If $s \leq t$ implies $s \leq' t$ (for all $s, t \in S$), then $\leq$ is said to be *coarser* than $\leq'$, and $\leq'$ is said to be *finer* than $\leq$.

(1.4). Assume that $\leq$ is coarser than $\leq'$, and let $X \subseteq S$. If X is $\leq$-narrow, then X is $\leq'$-narrow. If X is $\leq'$-artinian, then it is $\leq$-artinian. If X is both $\leq$-artinian and $\leq$-narrow, then it is also $\leq'$-artinian and $\leq'$-narrow.

(C) *Ordered Monoids*

Let $(S, \leq)$ be an *ordered monoid*, that is, $(S, \leq)$ is an ordered set, S is a monoid, and the order $\leq$ is compatible with the operation: if $s, s', t \in S$ and $s \leq s'$, then $s + t \leq s' + t$.

$(S, \leq)$ is a *strictly ordered monoid* if, moreover, $s, s', t \in S$ and $s < s'$ imply $s + t < s' + t$. In this situation, $\leq$ is said to be a *strict order*. Thus, if S is cancellative or the order is trivial then $(S, \leq)$ is a strictly ordered monoid.

An element t of the ordered monoid $(S, \leq)$ is $\leq$*-cancellative* when $s + t \leq s' + t$ implies $s \leq s'$. The set $C_{\leq}(S)$ of all $\leq$-cancellative elements is a submonoid of $C(S)$. $(S, \leq)$ is said to be $\leq$*-cancellative* when $S = C_{\leq}(S)$. It follows that S is cancellative and the order $\leq$ is strict. If $(S, \leq)$ is totally ordered, or if S is cancellative and the order is trivial, then it is $\leq$-cancellative. Also, every ordered group is $\leq$-cancellative.

If S is cancellative and $\leq$ is a compatible order on S, define $s \leq' t$ if there exists $u \in S$ such that $s + u \leq t + u$. Then $\leq'$ is a compatible order on S, finer than $\leq$ and S is $\leq'$-cancellative.

If S is $\leq$-cancellative, the order $\leq$ of S extends naturally to a compatible order, still denoted $\leq$, on the group of differences $\hat{S} = S - S$. If the order $\leq$ on S is total, resp. trivial, then its extension to $\hat{S}$ satisfies the same property.

If S is a torsion-free group and $\leq$ is a compatible order on S, then $\leq$ extends naturally to a compatible order, still denoted $\leq$, on the smallest divisible group Q containing S. If the order on S is total, resp. trivial, then so is its extension to Q.

(1.5). If the monoid S has a compatible strict total order, then S is cancellative and torsion-free.

The following result is important:

(1.6). If S is a cancellative and torsion-free monoid, if $\leq$ is any compatible order on S, there exists a compatible total order $\leq'$ on S, which is finer than $\leq$.

(1.7). If X, Y are artinian and narrow subsets of the ordered monoid $(S, \leq)$, then $X + Y = \{s + t \mid s \in X, t \in Y\}$ is artinian and narrow.

I shall sometimes consider ordered monoids satisfying the following condition:

$$0 \leq s \quad \text{for every } s \in S. \tag{S0}$$

If (S0) holds, then $G(S) = \{0\}$. If $(S, \leq)$ satisfies (S0), if $\leq$ is coarser than $\leq'$, then $(S, \leq')$ satisfies also (S0).

(1.8). Let $(S, \leq)$ be an ordered monoid. If X is an artinian and narrow subset of S, such that $0 \leq s$ for every $s \in X$, then the submonoid of S generated by X is also artinian and narrow.

The proof of the above result is in [Ri3]; it requires a lemma of Erdős and Radò quoted in [Hi] (see for example [Ro] for a simple proof).

As is shown in [Ri3], the above result implies

(1.9). Let $(S, \leq)$ be a strictly ordered monoid, let X be an artinian and narrow subset of S, such that $0 < s$ for every $s \in X$. Then, for every $t \in S$, there exists an integer $k(t) \geq 1$ such that if $n \geq k(t)$ then $t \notin nX$.

The following result is in [El-Ri]:

(1.10). Let $(S, \leq)$ be an ordered monoid and assume that S is torsion-free. Then the following conditions are equivalent:

(a) If $s, t \in S$, there exists an integer $k \geq 1$ such that $ks \leq kt$ or $kt \leq ks$.

(b) There exists a compatible total order $\leq'$ on S, finer than $\leq$, namely $s \leq' t$ if and only if there exists an integer $k \geq 1$ such that $ks \leq kt$.

The order $\leq$ is said to be a *subtotal order* when the above conditions are satisfied.

If S is a torsion-free and $\leq$-cancellative monoid, if $\leq$ is a compatible subtotal order, then its natural extension to $\hat{S} = S - S$ is still a subtotal order.

(D) *Generalized Power Series*

Let R be a commutative ring, let $(S, \leq)$ be a strictly ordered monoid. Let $A = [[R^{S, \leq}]]$ be the set of all maps $f: S \to R$ such that $\operatorname{supp}(f) = \{s \in S | f(s) \neq 0\}$ is artinian and narrow. On A, the addition is defined pointwise.

If $f_1, \ldots, f_n \in A$ and $s \in S$, let $X_s(f_1, \ldots, f_n) = \{(t_1, \ldots, t_n) \in S^n | f_1(t_1) \neq 0, \ldots, f_n(t_n) \neq 0$ and $t_1 + \cdots + t_n = s\}$.

(1.11). For all $s \in S$ and $f_1, \ldots, f_n \in A$, the set $X_s(f_1, \ldots, f_n)$ is finite.

Define the operation of convolution $*$ on A, as follows:

$$(f * g)(s) = \sum_{(t, u) \in X_s(f, g)} f(t) g(u).$$

With these operations, A is a commutative ring, with unit element e, namely

$$\begin{cases} e(0) = 1 \\ e(s) = 0 \quad \text{if } s \in S, s \neq 0. \end{cases}$$

The elements of A are called *generalized power series with coefficients in R and exponents in S.*

For simplicity, if k is a positive integer I write $f^k = f * \cdots * f$ (k times).

Note that if $f, g \in A$, then

$$\operatorname{supp}(f + g) \subseteq \operatorname{supp}(f) \cup \operatorname{supp}(g),$$
$$\operatorname{supp}(f * g) \subseteq \operatorname{supp}(f) + \operatorname{supp}(g).$$

R is canonically embedded as a subring of A and S is canonically embedded as a submonoid of the monoid $(A, *)$, by the mapping $s \in S \mapsto e_s \in A$, where

$$\begin{cases} e_s(s) = 1 \\ e_s(t) = 0 \quad \text{if } t \in S, t \neq s. \end{cases}$$

(1.12). If $\leq$, $\leq'$ are compatible strict orders on the monoid S and $\leq$ is coarser than $\leq'$, if $A = [[R^{S,\leq}]]$ and $A' = [[R^{S,\leq'}]]$, then A is a subring of A'. If $(S, \leq)$ is narrow, then $A = A'$.

(1.13). A is a domain if and only if R is a domain and S is torsion-free and cancellative.

The proof is in [Ri2].

For the next result, see [El-Ri]:

(1.14). A is a field if and only if R is a field, S is a torsion-free group, and $\leq$ is a subtotal order.

The following result will also be needed:

(1.15). Let S be torsion-free and cancellative. Then A is a reduced ring if and only if R is a reduced ring.

For the proof, see [Ri2].

Let $U(R)$, resp. $U(A)$, denote the group of units of the ring R, resp. A.

(1.16). Assume that $(S, \leq)$ satisfies condition (S0) and let $f \in A$. Then $f \in U(A)$ if and only if $f(0) \in U(R)$.

For the proof see [Ri3].

If $f \in A$, $f \neq 0$, denote by $\pi(f)$ the set of minimal elements of $\mathrm{supp}(f)$; then $\pi(f)$ is a non-empty finite set, consisting of pairwise order incomparable elements. If $\pi(f)$ consists only of one element s, we write $\pi(f) = s$.

(1.17). Let f, g be non-zero elements of A. Assume that $\pi(f) = s$ is a $\leq$-cancellative element of S and $f(s)g(t) \neq 0$ for every $t \in \pi(g)$. Then $\pi(f * g) = s + \pi(g)$.

Proof. First, I show that $s + \pi(g) \subseteq \pi(f * g)$. Let $t \in \pi(g)$, then $(f * g)(s + t) = \Sigma f(u)g(v)$ (sum extended over all $(u, v) \in X_{s+t}(f, g)$).

Then $s \leq u$, so $s + v \leq u + v = s + t$. Since s is $\leq$-cancellative, $v \leq t$ and since $g(v) \neq 0$ then $v = t$, and $u = s$ because the order $\leq$ is strict. Thus $(f * g)(s + t) = f(s)g(t) \neq 0$, by hypothesis.

If $w < s + t$ and $w \in \mathrm{supp}(f * g)$, then $0 \neq (f * g)(w) = \Sigma f(u)g(v)$ (sum extended over all $(u, v) \in X_w(f, g)$).

Then $s \leq u$, $s + v \leq u + v = w < s + t$, and since s is $\leq$-cancellative, $v < t \in \pi(g)$, which is absurd.

This shows that $s + \pi(g) \subseteq \pi(f * g)$.

Conversely, let $w \in \pi(f * g)$, so $0 \neq (f * g)(w) = \Sigma f(u)g(v)$ (sum extended over all $(u, v) \in X_w(f, g)$).

Then $s \leq u$; since $g(v) \neq 0$, there exists $t \in \pi(g)$, such that $t \leq v$, therefore $s + t \leq u + v = w$. But $s + t \in s + \pi(g) \subseteq \pi(f * g)$, hence $s + t = w$, showing that $\pi(f * g) \subseteq s + \pi(g)$. ∎

As a corollary, $\pi(e_s * g) = s + \pi(g)$, whenever s is a $\leq$-cancellative element.

Another corollary is the following:

(1.18). Let f be a non-zero element of A. Assume that $\pi(f) = s$ is a $\leq$-cancellative element of S and $f(s)^k \neq 0$ (for $k \geq 1$). Then $\pi(f^k) = k\pi(f)$.

2. Powers

I keep the same notations.

(2.1). Let $n \geq 2$ and assume that $A = A^n$.

(i) If A is a domain, then $R = R^n$ and $S = nS$.

(ii) If S satisfies condition (S0) then $R = R^n$.

Proof. (i) By (1.13), R is a domain and S is a cancellative and torsion-free monoid. By (1.6), S has a compatible strict total order $\leq'$ finer than $\leq$.

Let $A' = [[R^{S,\le'}]]$, so by (1.12) A is a subring of A'. For every $h \in A'$, let $\pi'(h)$ denote the $\le'$-smallest element of supp(h).

Let $r \in R$; I may assume $r \neq 0$. There exists $f \in A$ such that $re = f^n$, so $f \neq 0$. This relation holds also in A', hence $0 = \pi'(f^n) = n\pi'(f)$, and therefore $0 = \pi'(f)$. Write $f = f(0)e + f'$, where $f' \in A, 0 <' \pi'(f')$. Then $re = f(0)^n e + f''$, with $f'' \in A$, $0 <' \pi'(f'')$, and I conclude that $r = f(0)^n \in R^n$.

Let $s \in S$. By hypothesis, there exists $g \in A$ such that $e_s = g^n$; hence $s = \pi'(g^n) = n\pi'(g) \in nS$.

(ii) Let $r \in R$; I may assume $r \neq 0$. Then $re = f^n$, with $f \in A$. Hence $r = f^n(0) = \Sigma f(s_1) \cdots f(s_n)$ (sum extended over $X_0(f, \ldots, f)$. Since $r \neq 0$, this set is not empty.

If $f(s_1) \neq 0, \ldots, f(s_n) \neq 0$ and $s_1 + \cdots + s_n = 0$, by (S0) (and noting that the order $\le$ is strict) $s_1 = \cdots = s_n = 0$. This shows that $X_0(f, \ldots, f)$ consists only of $(0, 0, \ldots, 0)$ and $r = f(0)^n$. ∎

(2.2). Let $g \in A$ be such that $\text{supp}(g) \subseteq \{s \in S \mid 0 < s\}$.

(i) For every $s \in S$, there exists $k(s) \ge 1$ such that $g^l(s) = 0$ for every $l \ge k(s)$.

(ii) If $(r_l)_{l \ge 0}$ is any sequence of elements of R, denote by $\Sigma_{l=0}^{\infty} r_l g^l$ the mapping $s \in S \mapsto \Sigma_{l=0}^{k(s)-1} r_l g^l(s) \in R$. Then $\Sigma_{l=0}^{\infty} r_l g^l \in A$.

Proof. (i) This follows at once from (1.9).

(ii) It is clear from (i) that the mapping $\Sigma_{l=0}^{\infty} r_l g^l$ is well defined. Moreover, $\text{supp}(\Sigma_{l=0}^{\infty} r_l g^l) \subseteq \bigcup_{l=0}^{\infty} l\, \text{supp}(g)$. By (1.8), $\bigcup_{l=0}^{\infty} l\, \text{supp}(g)$ is artinian and narrow, hence $\Sigma_{l=0}^{\infty} r_l g^l \in A$. ∎

If $g \in A$ is such that $\pi(g) \subseteq \{s \in S \mid 0 < s\}$, I define the mapping

$$\varphi_g \colon R[[Z]] \to A$$

from the ring of usual formal power series in the determinant Z, into A, by letting

$$\varphi_g\left(\sum_{i=0}^{\infty} r_i Z^i\right) = \sum_{i=0}^{\infty} r_i g^i.$$

(2.3). φ_g is a ring-homomorphism.

Proof. Since φ_g transforms sums into sums, it suffices to verify that if $\rho = \Sigma_{j=0}^{\infty} r_j Z^j$, $\rho' = \Sigma_{k=0}^{\infty} r'_k Z^k$, and $\rho'' = \rho \cdot \rho' = \Sigma_{i=0}^{\infty} r''_i Z^i$ with $r''_i = \Sigma_{j+k=i} r_j r'_k$, then $\varphi_g(\rho'') = \varphi_g(\rho) * \varphi_g(\rho')$.

If $s \in S$, consider the finite set $X = X_s(\sum_{j=0}^{\infty} r_j g^j, \sum_{k=0}^{\infty} r'_k g^k)$.

With the notations of (2.2), let $N_1 \geq k(s)$ and also $N_1 \geq k(t)$, for every $t \in S$ such that there exists $(t, u) \in X$; let $N_2 \geq k(s)$ and also $N_2 \geq k(u)$, for every $u \in S$ such that there exists $(t, u) \in X$; let $N = N_1 + N_2$. Note that $X = X_s(\sum_{j=0}^{N_1} r_j g^j, \sum_{k=0}^{N_2} r'_k g^k)$. It follows that

$$\begin{aligned}
\left(\sum_{i=0}^{\infty} r''_i g^i\right)(s) &= \left(\sum_{i=0}^{N} r''_i g^i\right)(s) \\
&= \left[\left(\sum_{j=0}^{N_1} r_j g^j\right) * \left(\sum_{k=0}^{N_2} r'_k g^k\right)\right](s) \\
&= \sum_{(t,u)\in X} \left(\sum_{j=0}^{N_1} r_j g^j\right)(t) \left(\sum_{k=0}^{N_2} r'_k g^k\right)(u) \\
&= \sum_{(t,u)\in X} \left(\sum_{j=0}^{\infty} r_j g^j\right)(t) \left(\sum_{k=0}^{\infty} r'_k g^k\right)(u) \\
&= \left[\left(\sum_{j=0}^{\infty} r_j g^j\right) * \left(\sum_{k=0}^{\infty} r'_k g^k\right)\right](s),
\end{aligned}$$

concluding the proof. ∎

Denote by v_p the p-adic valuation (where p is any prime).

The following result is probably known:

LEMMA. *Let $m, k \geq 2$ and let p be a prime number not dividing m. Then*

(i) $v_p(k!) \leq v_p[(m-1)(2m-1) \cdots ((k-1)m-1)]$, *for every $k \geq 1$.*

(ii) *If R is a ring such that m is invertible in R, then, for every $k \geq 1$*

$$\begin{aligned}
\binom{\frac{1}{m}}{k} &= \frac{1}{m}\left(\frac{1}{m}-1\right)\left(\frac{1}{m}-2\right)\cdots\left(\frac{1}{m}-(k-1)\right)\Big/k! \\
&= (-1)^{k-1}(m-1)(2m-1)\cdots((k-1)m-1)/\left(m^k \times k!\right) \\
&\in R.
\end{aligned}$$

Proof. (i) For every $e \geq 1$, there exists an integer a_e, $1 \leq a_e \leq p^e - 1$, such that $a_e m \equiv 1 \pmod{p^e}$.

Let $M = (m-1)(2m-1)\cdots((k-1)m-1)$ and $M_e = \{b \mid 1 \le b \le k-1,\ bm \equiv 1 \pmod{p^e}\}$. Let $s_e = [(k-1-a_e)/p^e]$. Then

$$\begin{aligned}\#M_e &= \#\{i \mid 0 \le i \le s_e, (a_e+i)m \equiv 1 \pmod{p^e}\}\\ &= 1 + s_e.\end{aligned}$$

Since $a_e + 1 \le p^e$ then $[k/p^e] \le 1 + [(k-1-a_e)/p^e]$, hence as it is obvious

$$\begin{aligned}v_p(k!) &= \left[\frac{k}{p}\right] + 2\left(\left[\frac{k}{p^2}\right] - \left[\frac{k}{p}\right]\right) + \cdots\\ &\quad + e\left(\left[\frac{k}{p^e}\right] - \left[\frac{k}{p^{e-1}}\right]\right) + \cdots\\ &= \left[\frac{k}{p}\right] + \left[\frac{k}{p^2}\right] + \cdots + \left[\frac{k}{p^e}\right] + \cdots\\ &\le (1+s_1) + (1+s_2) + \cdots + (1+s_e) + \cdots\\ &= \#M_1 + \#M_2 + \cdots + \#M_e + \cdots\\ &= \#M_1 + 2(\#M_2 - \#M_1) + \cdots + e(\#M_e - \#M_{e-1}) + \cdots\\ &= v_p(M).\end{aligned}$$

(ii) This follows at once from (i), since m is invertible in R and $M/k!$ is p-integral for every prime p not dividing m. ∎

(2.4). Let $m \ge 2$ and assume that m is invertible in the ring R. Let $g \in A$ be such that $\pi(g) \subseteq \{s \in S \mid 0 < s\}$ and let

$$h = e + \binom{\frac{1}{m}}{1} g + \binom{\frac{1}{m}}{2} g^2 + \binom{\frac{1}{m}}{3} g^3 + \cdots.$$

Then $h \in A$ and $h^m = e + g$.

Proof. First observe that $h \in A$, by (2.2) and the above lemma.
In $R[[Z]]$ the following identity holds:

$$\left[1 + \binom{\frac{1}{m}}{1} Z + \binom{\frac{1}{m}}{2} Z^2 + \cdots\right]^m = 1 + Z.$$

Applying the ring-homomorphism φ_g, it follows that

$$h^m = \left[e + \binom{\frac{1}{m}}{1} g + \binom{\frac{1}{m}}{2} g^2 \cdots \right]^m = e + g. \quad \blacksquare$$

(2.5). Let $m \geq 2$ be invertible in the ring R. If $f \in U(A)$, $\pi(f) = s \in mG(S)$, and $f(s) \in U(R)^m$, then $f \in U(A)^m$.

Proof. Let $s = mt$ and $f(s) = r^m$, with $t \in G(S)$, $r \in U(R)$.

Let $h = f(s)^{-1} e_{-s} * f$. Thus $h \in U(A)$, since $-s$ is $\leq$-cancellative, by the special case of (1.17), $\pi(h) = \{0\}$ and $h(0) = 1$.

Hence $h = e + g$, where $g \in A$, $g = 0$, or $\text{supp}(g) \subseteq \{s \in S | 0 < s\}$. By (2.4) there exists $k \in A$ such that $k^m = e + g = h$. It follows that $(re_t * k)^m = f(s)e_s * h = f$. Since $f \in U(A)$ then $re_t * k \in U(A)$, thus $f \in U(A)^m$. $\blacksquare$

Here is a corollary:

(2.6). Let $m \geq 2$ be invertible in the ring R and assume that $(S, \leq)$ satisfies condition (S0). Assume also that $U(R) = U(R)^m$. Then $U(A) = U(A)^m$.

Proof. Let $f \in U(A)$ and $e = f * g$ with $g \in A$. Then $1 = \Sigma f(s)g(t)$ (sum extended over all couples (s, t) such that $0 = s + t$, $f(s) \neq 0$, $g(t) \neq 0$). By (S0), necessarily $s = t = 0$, hence $\pi(f) = \{0\}$ and $f(0) \in U(R) = U(R)^m$. By (2.5), $f \in U(A)^m$. $\blacksquare$

3. Real Rings

Recall that the ring R is said to be a *real ring* if the following condition is satisfied: if $r_1, \ldots, r_m \in R$ and $\Sigma_{i=1}^m r_i^2 = 0$, then $r_1 = \cdots = r_m = 0$.

In particular, a real ring is reduced (i.e., it has no nilpotent elements different from 0). Indeed, if $r^m = 0$, if $m \leq 2^n$, then also $r^{2^n} = 0$; it follows successively that $r^{2^{n-1}} = 0, \ldots, r^2 = 0$ and $r = 0$.

It is clear that if A is a real ring then its subring R is also a real ring.

Also, S is torsion-free, because if $s \in S$, $k \geq 1$, and $ks = 0$, then $0 = e_{ks} = e_s^k$; if $k \leq 2^m$ then $e_s^{2^m} = 0$, so $e_s^{2^{m-1}} = \cdots = e_s^2 = e_s = 0$, hence $s = 0$.

(3.1). Assume that S is torsion-free and cancellative. If R is a real ring, then A is a real ring.

Proof. Let $f_1, \ldots, f_m \in A$ be such that each $f_i \neq 0$ and $\Sigma_{i=1}^m f_i^2 = 0$. Let $\leq'$ be a strict total order on S, finer than $\leq$. A is a subring of $A' = [[R^{S, \leq'}]]$, hence the relation $\Sigma_{i=1}^m f_i^2 = 0$ still holds in A'. Let $s = \min_{1 \leq i \leq m}\{\pi'(f_i)\}$ (in $(S, \leq')$). Then $0 = (\Sigma_{i=1}^m f_i^2)(2s) = \Sigma_{i=1}^m f_i^2(2s) = \Sigma_{i=1}^m [f_i(s)]^2$. Since R is a real ring, then $f_i(s) = 0$ for every $i = 1, \ldots, m$, which is a contradiction. ∎

4. Unique Factorization Domains

For the next result I need the following fact. Let R be a ring, let $(Y_i)_{i \in I}$ be a family of indeterminates. The ring $R[[Y_i]]_{i \in I}$, of power series in the indeterminates Y_i and coefficients in R, consists of the series $\Sigma r_M M$ (sum over all monomials $M = \prod_{j=1}^k Y_{i_j}^{e_j}$, with $i_1, \ldots, i_k \in I$, $e_j \geq 1$, and with coefficients $r_M \in R$).

Cashwell and Everett [Ca-Ev] (see also Liu [Li]) have shown that if R is a field, then $R[[Y_i]]_{i \in I}$ is a unique factorization domain.

(4.1). Let R be a field, assume that the ordered set $(S, \leq)$ is artinian and narrow and that S is a free monoid. Then A is a unique factorization domain.

Proof. Since S is a free monoid, then it is torsion-free and cancellative. Thus, by (1.13), A is a domain.

Since S is artinian and narrow, then $A = R^S$ (the set of mappings from S to R).

Let T be a set of free generators of the monoid S and let $R[[Y_t]]_{t \in T}$ be the ring of formal power series with coefficients in R, in the indeterminates Y_t $(t \in T)$. Since R is a field, then $R[[Y_t]]_{t \in T}$ is a unique factorization domain, it suffices to establish a ring-isomorphism $\varphi: A \to R[[Y_t]]_{t \in T}$.

Let $f \in A = R^S$; if $s \in S$ it may be written in unique way in the form $s = \Sigma_{j=1}^k e_j t_j$ (with $t_j \in T$, $e_j \geq 1$, $k \geq 0$); denote by M_s the monomial $M_s = \prod_{j=1}^k Y_{t_j}^{e_j}$. Define

$$\varphi(f) = \sum_{s \in S} f(s) M_s.$$

It is clear that φ is bijective and also that $\varphi(f + g) = \varphi(f) + \varphi(g)$ and $\varphi(f * g) = \varphi(f)\varphi(g)$. Indeed,

$$\begin{aligned}\varphi(f * g) &= \sum_{s \in S} (f * g)(s) M_s = \sum_{s \in S} \sum_{u+v=s} f(u) g(v) M_u M_v \\ &= \Big(\sum_{u \in S} f(u) M_u\Big)\Big(\sum_{v \in S} g(v) M_v\Big) = \varphi(f)\varphi(g).\end{aligned}$$

Thus φ is a ring-isomorphism, concluding the proof. ∎

EXAMPLE. Let $(t_n)_{n \geq 1}$ be a sequence of natural numbers greater than 1, such that for each $n \geq 1$ there exists a prime p which divides t_n, but p does not divide $t_1, t_2, \ldots, t_{n-1}$. Let $S^{\bullet}$ be the multiplicative monoid generated by $(t_n)_{n \geq 1}$; it is a submonoid of the multiplicative cancellative monoid $\mathbb{N}_{>0}$. Then $S^{\bullet}$ is a free monoid, and $(t_n)_{n \geq 1}$ is a system of free generators. Indeed, if $\prod_{i=1}^{k} t_i^{d_i} = \prod_{i=1}^{k} t_i^{e_i}$ with $d_i, e_i \geq 0$, $\max\{d_k, e_k\} \neq 0$, by cancellation (which is valid in $\mathbb{N}_{>0}$) I may assume, for example, $d_k > 0$, $e_k = 0$. Let p be a prime such that $p | t_k, p \nmid t_1 t_2 \cdots t_{k-1}$. This contradicts the unique factorization of integers as products of primes.

Let $S = \{\log s | s \in S^{\bullet}\}$, thus S is a free additive monoid of positive real numbers, which may be endowed with the total order $\leq$ induced by the usual order of $\mathbb{R}$. Since $(S, \leq)$ is artinian, if R is any field then A is a unique factorization domain.

For example, I may take $t_n = F_n$ (the nth Fibonacci number) for $n \neq 1, 2, 6, 12$, because each such Fibonacci number has a primitive prime factor (see Carmichael [Ca] or Ribenboim [Ri5]).

5. Completely Integrally Closed Domains

Let R be a domain and let K be its field of fractions. Recall that R is a *completely integrally closed domain* when the following property is satisfied:

If $x \in K$ and there exists $r \in R$, $r \neq 0$, such that $rx^n \in R$ for every $n \geq 1$, then $x \in R$.

Similarly, let S be a cancellative monoid and let $\hat{S} = S - S$ be the group of differences. S is said to be a *completely integrally closed monoid* when the following condition is satisfied:

If $t \in \hat{S}$ and there exists $s \in S$, such that $s + nt \in S$ for every $n \geq 1$, then $t \in S$.

Let R be a domain, $(S, \leq)$ a $\leq$-cancellative ordered monoid.

(5.1). If A is a completely integrally closed domain, then R is a completely integrally closed domain and S is a completely integrally closed monoid.

Proof. Let K be the field of fractions of R and let L be the field of fractions of A, hence K is a subfield of L.

Let $x \in K$ and assume that there exists $r \in R$, $r \neq 0$, such that $rx^n \in R$ for every $n \geq 1$. Let $f = xe$ and $g = re$, so $f \in L$, $g \in A$, and $g * f^n = (rx^n)e \in A$ for every $n \geq 1$. By hypothesis, $f \in A$, so $x \in R$.

Now let $t \in \hat{S}$ and assume that there exists $s \in S$ such that $s + nt \in S$, for every $n \geq 1$. Note that the order $\leq$ on S extends to a compatible order still denoted $\leq$, on $\hat{S}$ and $A \subseteq [[R^{\hat{S}, \leq}]]$. If $t = s_1 - s_2$ (with $s_1, s_2 \in S$) then $e_t \in [[R^{\hat{S}, \leq}]]$ and $e_{s_1} = e_{s_2} * e_t$, so $e_t \in L$. Moreover, $e_s * (e_t)^n = e_{s+nt} \in A$ for every $n \geq 1$. Hence $e_t \in A$ and therefore $t \in S$. ∎

(5.2). Assume that R is a completely integrally closed domain and that $(S, \leq)$ is a subtotally ordered, $\leq$-cancellative monoid, which is torsion-free and completely integrally closed. Then A is a completely integrally closed domain.

Proof. Let K be the field of fractions of A, let $\hat{S}$ be the group of differences of S, endowed with the natural extension of the order of S. Let $B = [[K^{\hat{S}, \leq}]]$; since $(\hat{S}, \leq)$ is a subtotally ordered torsion-free group by (1.14), B is a field, hence it contains the field of fractions L of A.

Let $f \in L$ and assume that there exists $g \in A$, $g \neq 0$, such that $g * f^n \in A$ for every $n \geq 1$. Identifying f with an element of B, let $X = \operatorname{supp}(f) \cap S \cap f^{-1}(R)$, hence X is artinian and narrow.

Define $f_S: S \to R$ by putting

$$f_S(s) = \begin{cases} f(s) & \text{if } s \in X \\ 0 & \text{if } s \notin X. \end{cases}$$

So $\operatorname{supp}(f_S) = X$, hence $f_S \in A$.

Let $f' = f - f_S \in L \subseteq B$. Then $\operatorname{supp}(f') \cap S \cap f'^{-1}(R) = \varnothing$ because if $s \in S$, $f'(s) \in R$, and $f'(s) \neq 0$, then $s \notin X$, hence $f(s) \in R$, so $s \in X$, which is absurd.

It suffices to show that $f' = 0$ and I assume $f' \neq 0$. Then

$$g * f'^n = g * (f - f_S)^n = g * f^n - \binom{n}{1} g * f^{n-1} * f_S + \binom{n}{2} g * f^{n-2} * f_S^2 - \cdots + (-1)^n g * f_S^n \in A$$

by hypothesis.

Since $\hat{S}$ is a torsion-free group, there exists a compatible strict total order $\leq'$ on $\hat{S}$, finer than $\leq$. Let $t_1 = \pi'(f')$, $s_1 = \pi'(g) \in S$. A is a subring of $A' = [[R^{S, \leq'}]]$.

By (1.17), for every $n \geq 1$, $\pi'(g * f'^n) = s_1 + nt_1 \in S$ because $g * f'^n \in A$. Thus $t_1 \in S$.

Similarly, $(g * f'^n)(s_1 + nt_1) = g(s_1)f'^n(nt_1) = g(s_1)[f'(t_1)]^n \in R$ for every $n \geq 1$. Thus $f'(t_1) \in R$. I conclude that $t_1 \in \operatorname{supp}(f') \cap S \cap f'^{-1}(R) = \varnothing$, and this is absurd, completing the proof. ∎

As a corollary, we have the following.

(5.3). Assume that R is a completely integrally closed domain and that $(S, \leq)$ is a totally ordered completely integrally closed monoid. Then A is a completely integrally closed domain.

Proof. This is just a special case of the preceding result. ∎

Here it should be noted that a similar result cannot hold for the property of being integrally closed. Indeed, it is known that there exists an integrally closed domain R such that the usual ring of formal power series $R[[X]]$ is not integrally closed (see, for example, Bourbaki [Bo, p. 76, Exercise 27] or Brewer [Br]).

6. Seminormal Rings

The concept of seminormality has been studied by various authors; I refer the reader to the paper by Brewer and Nichols [Br-Ni] which is directly relevant.

A ring R is *seminormal* when the following property is satisfied: if $b, c \in R$ and $b^2 = c^3$, then there exists $a \in R$ such that $b = a^3$ and $c = a^2$.

Swan [Sw] gave another characterization of seminormal rings, in terms of their Picard group, but this will not be required here.

Costa [Co] showed (I repeat his simple proof) the following

(6.1). If R is seminormal, then R is reduced.

Proof. Let $b \in R$ be such that $b^k = 0$; if $2^{m-1} < k \leq 2^m$ (with $m \geq 1$), let $c = b^{2^{m-1}}$, hence $c^2 = 0$.

I shall show that $c = 0$, and then the argument may be repeated, leading eventually to $b = 0$.

First $c^2 = 0$, $c^3 = 0$, hence there exists $a \in R$ such that $c = a^3$ and $c = a^2$. It follows that $c = a^3 = ac$, therefore $c = a^2c = c^2 = 0$. ∎

Clearly, every field is a seminormal ring.

It is also very easy to show that every unique factorization domain is seminormal.

If R is a subring of T, R is said to be *seminormal* in T when the following property holds: if $b \in T$ and $b^2, b^3 \in R$ then $b \in R$.

The following rephrasement of the definition is almost immediate:

(6.2). If R is a subring of T, then R is seminormal in T if and only if the following condition is satisfied: if $a \in T$ and there exists k_0 such that $a^k \in R$ for every $k \geq k_0$, then $a \in R$.

Proof. It is clear that the property indicated implies that R is seminormal in T (taking $k_0 = 2$).

Conversely, let R be seminormal in T, let $a \in T$, and let $k_0 \geq 1$ be the smallest exponent such that $a^k \in R$ for every $k \geq k_0$. If $k_0 > 1$ then $(a^{k_0-1})^2 \in R$, $(a^{k_0-1})^3 \in R$, so $a^{k_0-1} \in R$, which is absurd. Therefore $k_0 = 1$, hence $a \in R$. ∎

It follows at once from the definition:

(6.3). If $R \subseteq T \subseteq U$ (where R, T are subrings of the ring U), if R is seminormal in T and T is seminormal in U, then R is seminormal in U.

It is also easily seen:

(6.4). Let R be a subring of the ring T.

(i) If T is reduced and R is seminormal, then R is seminormal in T.

(ii) If T is seminormal and R is seminormal in T, then R is seminormal.

Thus, a domain is seminormal if and only if it is seminormal in its field of fractions.

A monoid S is said to be *seminormal* when the following condition holds: if $s, t \in S$ and $2s = 3t$, there exists $q \in S$, such that $s = 3q$ and $t = 2q$.

It is clear that every group is seminormal. It is also very easy to show that every free monoid is seminormal.

Let Q be a monoid and let S be a submonoid. S is said to be *seminormal* in Q when the following condition holds: if $s \in Q$ and $2s, 3s \in S$, then $s \in S$.

The proof of the next proposition is omitted, since it is exactly like the proof of (6.2):

(6.5). Let S be a submonoid of Q. Then S is seminormal in Q if and only if the following condition holds: if $q \in Q$ and there exists $k_0 \geq 1$ such that $kq \in S$ for every $k \geq k_0$, then $q \in S$.

S is said to be (2.3)-*torsion-free* when the following condition holds: if $s, t \in S$, $2s = 2t$, and $3s = 3t$, then $s = t$.

(6.6). Let S be a submonoid of the seminormal monoid Q.

(i) If S is (2, 3)-torsion-free and seminormal, then S is seminormal in Q.

(ii) If S is seminormal in Q, then S is seminormal.

Proof. (i) Let $q \in Q$ be such that $2q, 3q \in S$. Since $3(2q) = 2(3q)$, there exists $t \in S$ such that $2q = 2t$ and $3q = 3t$. By hypothesis, $q = t \in S$.

(ii) Let $s, t \in S$ be such that $2s = 3t$. Then there exists $q \in Q$ such that $s = 3q$, $t = 2q$. By hypothesis, $q \in S$ hence S is seminormal. ∎

In particular, if S is a torsion-free, cancellative, seminormal monoid, then S is seminormal in $\hat{S}$.

Let R be a subring of T, let $(S, \leq)$ be an ordered submonoid of $(Q, \leq)$. Let $A = [[R^{S, \leq}]]$ and $B = [[T^{Q, \leq}]]$. Then A may be identified with a subring of B, namely if $f \in A$ its canonical image in B is such that $f(q) = 0$ for every $q \in Q \setminus S$.

The following result is trivial:

(6.7). If A is seminormal in B, then R is seminormal in T and S is seminormal in Q.

Proof. Let $t \in T$ be such that $t^2, t^3 \in R$. So $te \in B$ is such that $(te)^2, (te)^3 \in A$; hence by hypothesis, $te \in A$, thus $t \in R$.

Let $q \in Q$ be such that $2q, 3q \in S$. Then $(e_q)^2 = e_{2q} \in A$, $(e_q)^3 = e_{3q} \in A$. Hence $e_q \in A$, so $q \in S$. ∎

I give the analogous result.

(6.8). Let S be torsion-free and cancellative. If A is a seminormal ring, then R is seminormal and S is a seminormal monoid.

Proof. Let $r_1, r_2 \in R$ be such that $r_1^2 = r_2^3$; we may assume $r_1, r_2, \neq 0$. Then $(r_1 e)^2 = (r_2 e)^3$, hence there exists $f \in A$, $f \neq 0$, such that $r_1 e = f^3$ and $r_2 e = f^2$.

By (1.6) there exists a compatible strict total order $\leq'$ on S, finer than $\leq$; as before, we denote by $\pi'(f)$ the $\leq'$-smallest element of supp(f). A is a subring of $A' = [[R^{S, \leq'}]]$.

Then $0 = \pi'(f^2)$. Since A is seminormal, then by (6.1) it is a reduced ring. It follows from (1.15) that R is reduced, hence by (1.18) $0 = \pi'(f^2) = 2\pi'(f)$. Since S is torsion-free, then $\pi'(f) = 0$ and I may write $f = f(0)e + f'$ where $f' \in A$ and $0 <' \pi'(f')$. Hence

$$r_1 e = f^2 = f(0)^2 e + f_1'',$$

$$r_2 e = f^3 = f(0)^3 e + f_2'',$$

where $f_1'', f_2'' \in A$ and $0 <' \pi'(f_1'')$, $0 <' \pi'(f_2'')$. Thus $r_1 = f(0)^2$, $r_2 = f(0)^3$, showing that R is a seminormal ring.

Now let $s_1, s_2 \in S$ be such that $2s_1 = 3s_2$. Then $(e_{s_1})^2 = e_{2s_1} = e_{3s_2} = (e_{s_2})^3$. By hypothesis, there exists $f \in A$ such that $e_{s_1} = f^3$, $e_{s_2} = f^2$. Then by (1.18) $s_1 = \pi'(f^3) = 3\pi'(f)$, $s_2 = \pi'(f^2) = 2\pi'(f)$, proving that S is seminormal. ∎

I shall now study the converse of the above statements.

The following result is an extension of a theorem for formal power series by Brewer and Nichols [Br-Ni]:

(6.9). Let $(Q, \leq)$ be a torsion-free and cancellative ordered monoid, let T be a ring. We assume that the ordered submonoid $(S, \leq)$ is seminormal in $(Q, \leq)$ and that the subring R is reduced and seminormal in T. Then $A = [[R^{S, \leq}]]$ is seminormal in $B = [[T^{Q, \leq}]]$.

Proof. By (1.6) there exists a compatible strict total order $\leq'$ on Q, which is finer than $\leq$. We note that B is a subring of $B' = [[T^{Q, \leq'}]]$ and A is a subring of $A' = [[R^{S, \leq'}]]$.

For each $f \in B$, $f \neq 0$, denote by $\pi'(f)$ the smallest element of supp(f) (in the order $\leq'$). Note that supp(f) is $\leq$-artinian and $\leq$-narrow, hence it is a well-ordered subset of $(Q, \leq')$, by (1.4).

I divide the proof into several parts.

(1) Let $f \in B$, $f \neq 0$, and assume that $f^2, f^3 \in A$; let $\pi'(f) = s$. Then $f(s) \in R$ and $s \in S$.

Indeed, $f^2(2s) = f(s)^2$, $f^3(3s) = f(s)^3$, thus $f(s)^2, f(s)^3 \in R$, hence by hypothesis, $f(s) \in R$.

Since R is reduced, by (1.18), $\pi'(f^2) = 2\pi'(f) = 2s \in S$, $\pi'(f^3) = 3\pi'(f) = 3s \in S$. But S is seminormal in Q, hence $s \in S$.

(2) I introduce the following definition.

Let $t, q \in$ supp(f), with $t \leq' q$. We say that (t, q) satisfies condition $(**)$ when the following is true:

For every $m \geq 0$, for every subset $\{u_1, \ldots, u_m\}$ of supp(f) such that $t <' u_1 <' \cdots <' u_m \leq' q$, for all integers $n_1 \geq 1, \ldots, n_m \geq 1$:

$$f(t)\prod_{i=1}^{m} f(u_i)^{n_i} \in R$$

and

$$t + \sum_{i=1}^{m} n_i u_i \in S.$$

I say that t satisfies condition $(*)$ when (t, q) satisfies $(**)$, for all $q \in$ supp(f), such that $t \leq' q$.

(3) I show that s satisfies $(*)$.

First I note that (s, s) satisfies $(**)$, since $s \in S$, $f(s) \in R$.

Let $s \leq' q$, with $q \in \operatorname{supp}(f)$. I show that if (s, q') satisfies $(**)$ for every $q' \in \operatorname{supp}(f)$ such that $s \leq' q' <' q$, then (s, q) satisfies $(**)$.

Let

$$f_q(u) = \begin{cases} f(u) & \text{if } u <' q \\ 0 & \text{if } q \leq' u. \end{cases}$$

Let $n \geq 1$, arbitrary, and consider $g_n = f(s)e_s * f^2 * (f - f_q)^n = \sum_{k=0}^{n} \binom{n}{k}(-1)^k f^{n-k+2} * f(s)e_s * f_q^k$.

By hypothesis $f^{n-k+2} \in A$ for every $k \geq 0$.

Also, $\operatorname{supp}(f(s)e_s * f_q^k) \subseteq s + \operatorname{supp}(f_q^k)$. If $v \in \operatorname{supp}(f_q^k)$ then

$$\left(f(s)e_s * f_q^k\right)(s + v) = f(s) \sum f_q(v_1)^{n_1} \cdots f_q(v_l)^{n_l}$$

(sum for all $(v_1, \dots, v_l)$ such that each $v_i \in \operatorname{supp}(f_q)$, $n_1 + \cdots + n_l = k$, $n_1 v_1 + \cdots + n_l v_l = v$; hence $v_i <' q$ for each i).

By (1.11), the number of summands is finite, hence there exists $q' \in \operatorname{supp}(f)$, such that $q' <' q$ and $v_i \leq' q'$ for each v_i in any one summand. By hypothesis, (s, q') satisfies $(**)$, hence $(f(s)e_s * f_q^k)(e + v) \in R$, and also $s + \sum_{i=1}^{l} n_i v_i \in S$, for each summand. Thus $f(s)e_s * f_q^k \in A$ for $0 \leq k \leq n$, hence $g_n \in A$, for every $n \geq 1$. In particular, since R is reduced, then $\pi'(g_n) = 3s + nq \in S$, for every $n \geq 1$ and $g_n(3s + nq) = f(s)^3 f(q)^n \in R$.

Let $b = f(s)\prod_{i=1}^{m} f(u_i)^{n_i} f(q)^l$, with $s <' u_i <' q$ (for each i), $m \geq 0$, $n_i \geq 1$, $l \geq 0$.

If $k \geq 4$, then

$$b^k = f(s)^{k-4}\left[f(s)\prod_{i=1}^{m} f(u_i)^{kn_i}\right]\left[f(s)^3 f(q)^{kl}\right] \in R.$$

Hence by (6.2), $b \in R$.

Let $w = s + \sum_{i=1}^{m} n_i u_i + lq$, with $s <' u_i <' q$ (for each i), $m \geq 0$, $n_i \geq 1$, $l \geq 0$.

Again, if $k \geq 4$ then

$$kw = (k-4)s + \left[s + \sum_{i=1}^{m} kn_i u_i\right] + (3s + klq) \in S.$$

By (6.5), $w \in S$.

This shows that (s, q) satisfies $(**)$.

Since $\operatorname{supp}(f)$ is $\leq'$-well ordered, then (s, q) satisfies $(**)$, for every $q \in \operatorname{supp}(f)$, showing that s satisfies $(*)$.

(4) I show that if $t \in \operatorname{supp}(f)$, then t satisfies $(*)$.

Otherwise, there exists the $\leq'$-smallest $t \in \operatorname{supp}(f)$, not satisfying $(*)$. By (3), $t \neq s$.

Let $f_t^* = f - f_t$, where f_t is defined as was f_q. Thus $f_t^* \in B$, $\pi'(f_t^*) = t$, and $f_t^*(t) = f(t)$.

Also,

$$(f_t^*)^2 = f^2 - 2f_t * f + (f_t)^2,$$

$$(f_t^*)^3 = f^3 - 3f_t * f^2 + 3(f_t)^2 * f - (f_t)^3.$$

But v satisfies $(*)$, for every $v \in \operatorname{supp}(f)$, $v <' t$. Hence $f_t * h \in A$ for every $h \in B$, such that $\operatorname{supp}(h) \subseteq \bigcup_{n=1}^{\infty} n \operatorname{supp}(f)$.

In particular, $(f_t)^2, (f_t)^3, (f_t)^2 * f,\ f_t * f^2 \in A$, showing that $(f_t^*)^2, (f_t^*)^3 \in A$.

Noting that $\pi'(f_t^*) = t$ and that for $t \leq' q$, $q \in \operatorname{supp}(f)$ if and only if $q \in \operatorname{supp}(f_t^*)$, it follows from (3), that t satisfies $(*)$, which is contrary to the hypothesis.

(5) End of the proof:

If $t \in \operatorname{supp}(f)$, then (t, t) satisfies $(**)$, hence $t \in S$, $f(t) \in R$. This shows that $f \in A$. ∎

The results which follow also generalize the corresponding facts about power series rings, established in [Br-Ni]. The proof of the next proposition does not appeal to the characterization of seminormal rings in terms of the Picard group, since in the present situation the ring of formal power series over a field—which is the unique factorization domain—is replaced by the ring of generalized power series with coefficients in a field; according to (4.1), the latter ring is a unique factorization domain in certain cases, but it is not expected to be generally so.

(6.10). Let R be a seminormal ring. Let $(S, \leq)$ be a $\leq$-cancellative subtotally ordered monoid, which is torsion-free and seminormal. Then $A = [[R^{S, \leq}]]$ is seminormal.

Proof. R is seminormal, hence reduced, so it is a subring of a product $\prod_{i \in I} D_i$, where each D_i is a domain. Let K_i be the field of fractions of D_i.

Since $(S, \leq)$ is $\leq$-cancellative, its order extends canonically to an order, still denoted $\leq$, on the group of differences $\hat{S}$, which is still torsion-free; moreover, $(\hat{S}, \leq)$ is subtotally ordered.

By (1.14), $L_i = [[K_i^{\hat{S}, \leq}]]$ is a field. Hence $\prod_{i \in I} L_i$ is seminormal; since $R \subseteq \prod_{i \in I} D_i \subseteq \prod_{i \in I} K_i$ and R is seminormal, by (6.4) R is seminormal in $\prod_{i \in I} K_i$. On the other hand, S is seminormal in $\hat{S}$ by (6.6). It follows from (6.9) that $A = [[R^{S, \leq}]]$ is seminormal in $[[\prod_{i \in I} K_i^{\hat{S}, \leq}]] = \prod_{i \in I}[[K_i^{\hat{S}, \leq}]] = \prod_{i \in I} L_i$. By (6.4), A is seminormal. ∎

In particular, if R is a seminormal ring, if $(S, \leq)$ is a totally ordered seminormal monoid, then A is seminormal.

In this way it is possible to obtain many interesting examples of seminormal rings.

I shall indicate other sufficient conditions on R and $(S, \leq)$ for the ring A to be seminormal.

I introduce the following definition. Let $m \geq 2$; the ordered monoid is $\leq$ *-m-cancellative* when the following condition holds: if $s, t \in S$ and $ms \leq mt$, then $s \leq t$.

(6.11). Assume that R is a field of characteristic 2 (resp. 3) and that $(S, \leq)$ is an ordered torsion-free group which is $\leq$ -2-cancellative (resp. $\leq$ -3-cancellative). Then $A = [[R^{S, \leq}]]$ is seminormal.

Proof. Let $f, g \in A$ be such that $f^2 = g^3$, $f, g \neq 0$. Let $\leq'$ be a compatible total order on the torsion-free group S, which is finer than $\leq$ and let $A' = [[R^{S, \leq'}]]$. So A is a subring of A'. By (1.14), A' is a field, so it is seminormal. Hence there exists $k \in A'$ such that $f = k^3$, $g = k^2$.

Under the first hypothesis, I show that $\mathrm{supp}(g) = \{2s | s \in \mathrm{supp}(k)\}$. Indeed, let $g(t) \neq 0$, that is, $k^2(t) = \sum_{u+v=t} k(u)k(v) \neq 0$. If $u \neq v$ then $k(u)k(v) + k(v)k(u) = 2k(u)k(v) = 0$, because $2R = 0$. From $k^2(t) \neq 0$, there exists $s \in S$ such that $t = 2s$, with $k(s) \neq 0$, so $\mathrm{supp}(g) \subseteq \{2s | s \in \mathrm{supp}(k)\}$, and conversely. Since $\mathrm{supp}(g)$ is narrow, and S is $\leq$ -2-cancellative it follows that $\mathrm{supp}(k)$ is also narrow. Since $\mathrm{supp}(g)$ is artinian, then so is $\mathrm{supp}(k)$; thus $k \in A$.

The proof is similar under the second hypothesis. ∎

(6.12). Assume that R is a seminormal ring of residual characteristics equal to 2 (resp. 3). Let $(S, \leq)$ be a $\leq$ -cancellative torsion-free ordered monoid, which is seminormal and $\leq$ -2-cancellative (resp. $\leq$ -3-cancellative). Then $A = [[R^{S, \leq}]]$ is seminormal.

Proof. Let $(P_i)_{i \in I}$ be the family of minimal non-zero prime ideals of R, let $D_i = R/P_i$ and let K_i be the field of quotients of D_i. By hypothesis each field K_i has characteristic 2 (resp. 3). I note that $R \subseteq \prod_{i \in I} D_i \subseteq \prod_{i \in I} K_i$.

Let $\hat{S}$ be the group of differences of S and denote still by $\leq$ the order extension of $\leq$ to $\hat{S}$; clearly, $\hat{S}$ is $\leq$ -2-cancellative (resp. $\leq$ -3-cancellative). By (6.11), $L_i = [[K_i^{\hat{S}, \leq}]]$ is seminormal. Hence $\prod_{i \in I} L_i$ is seminormal. Since R is seminormal, by (6.4) it is seminormal in $\prod_{i \in I} K_i$. By (6.6), S is seminormal in $\hat{S}$. By (6.9), A is seminormal in $[[\prod_{i \in I} K_i^{\hat{S}, \leq}]] \cong \prod_{i \in I} L_i$. Finally, by (6.4), A is seminormal. ∎

References

[Bo] N. Bourbaki, "Algèbre Commutative," Chap. V, Hermann, Paris, 1964.

[Br] J. W. Brewer, "Power Series over Commutative Rings," Dekker, New York, 1981.

[Br-Ni] J. W. Brewer and W. D. Nichols, Seminormality in power series rings, *J. Algebra* **82** (1983), 282–284.

[Ca] R. D. Carmichael, On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$, *Ann. of Math.* **15** (1913), 30–70.

[Ca-Ev] E. D. Cashwell and C. J. Everett, Formal power series, *Pacific J. Math.* **13** (1963), 45–64.

[Co] D. Costa, Seminormality and projective modules, *in* "Proc., Séminaire d'Algèbre Paul Dubreil et Marie-Paule Malliavin, Paris, 1981," Lecture Notes in Mathematics, Vol. 924, pp. 400–412, Springer-Verlag, New York/ Berlin, 1981.

[De-Du] D. Deckard and L. K. Durst, Unique factorization in power series rings and semigroups, *Pacific J. Math.* **16** (1966), 239–242.

[El-Ri] G. A. Elliott and P. Ribenboim, Fields of generalized power series, *Arch. Math.* **54** (1990), 365–371.

[Er-Ra] P. Erdős and R. Radò, Unpublished manuscript, quoted in [Hi].

[Hi] G. Higman, Ordering by divisibility in abstract algebras, *Proc. London Math. Soc. (3)* **2** (1952), 326–336.

[Li] C.-P. Liu, The ring of formal power series in a countably infinite number of indeterminates, *Dissertation Abstracts* **24** (1964).

[Ri1] P. Ribenboim, Generalized power series rings, *in* "Lattices, Semigroups and Universal Algebra" (J. Almeida, G. Bordalo, and P. Dwinger, Eds.), pp. 271–277, Plenum, New York, 1990.

[Ri2] P. Ribenboim, Rings of generalized power series: Nilpotent elements, *Abh. Math. Sem. Univ. Hamburg* **61** (1991), 15–33.

[Ri3] P. Ribenboim, Rings of generalized power series. II. Units, zero-divisors, and semi-simplicity, *J. Algebra* **168** (1991), 71–89.

[Ri4] P. Ribenboim, Noetherian rings of generalized power series, *J. Pure Appl. Algebra* **79** (1990), 293–312.

[Ri5] P. Ribenboim, "The Book of Prime Number Records," Springer-Verlag, New York, 1988.

[Ro] G. Rosenstein, "Linear Orderings," Academic Press, New York, 1982.