On the Completeness of $R[[X]]$.

R. C. Daileda

1 Introduction: Notation and Terminology

Let R be a ring and $R[[X]]$ the ring of formal power series over R in the variable X. For $f = \sum_i a_i X^i \in R[[X]]$, define the *value* of f at 0 to be $f(0) = a_0$. The evaluation at 0 map $E_0 : R[[X]] \to R$, given by $E_0(f) = f(0)$, is a surjective homomorphism, according to the definitions of power series addition and multiplication. Notice that X is central in $R[[X]]$ since all of its coefficients are central in R. Furthermore, for any $i \geq 0$,

$$fX^i = X^i f = \sum_j (0 + 0 + \cdots + 0 + \underbrace{1a_{j-i}}_{i\text{th term}} + 0 + \cdots + 0)X^j = \sum_{j \geq i} a_{j-i}X^j = \sum_{j \geq 0} a_j X^{j+i}.$$

That is, X distributes through the *infinite* "sum" $\sum_i a_i X^i$. It follows at once that the kernel of E_0 is the ideal $\mathfrak{m} = (X) = X \cdot R[[X]] = R[[X]] \cdot X$, and that

$$\mathfrak{m}^n = (X^n) = \left\{ \sum_i a_i X^i \in R[[X]] \,\middle|\, a_0 = a_1 = \cdots = a_{n-1} = 0 \right\} \tag{1}$$

for all $n \geq 1$. Since $R[[X]]/\mathfrak{m} \cong R$, when R is commutative, $\mathfrak{m}$ is prime if and only if R is a domain, and $\mathfrak{m}$ is maximal if and only if R is a field. In the second case, $f \notin \mathfrak{m}$ if and only if $f(0) \neq 0$ if and only if $f \in R[[X]]^\times$, so that $R[[X]]$ is a local ring.

Although $\mathfrak{m}$ need not be the only maximal ideal in $R[[X]]$ in general ((p) is maximal in $\mathbb{Z}[[X]]$ for every prime p, since it is the kernel of the composite map $\mathbb{Z}[[X]] \to (\mathbb{Z}/p\mathbb{Z})[[X]] \overset{E_0}{\to} \mathbb{Z}/p\mathbb{Z}$.), $\mathfrak{m}$ nonetheless plays a distinguished role in the structure theory of $R[[X]]$. The powers of $\mathfrak{m}$ form a strictly decreasing chain of ideals ($X^n \notin \mathfrak{m}^{n+1}$), and by (1), $\bigcap_{n \geq 1} \mathfrak{m}^n = (0)$. From this it is not hard to deduce that for every $f \in R[[X]]$, there is a unique $n \geq 0$ so that $f \in \mathfrak{m}^n \setminus \mathfrak{m}^{n+1}$. The integer n is called the *order* of f (at zero) and is denoted $\operatorname{ord}(f)$. The existence and uniqueness of $\operatorname{ord}(f)$ can also be deduced directly from (1), where we find that if $f = \sum_i a_i X^i$, then

$$n = \operatorname{ord}(f) = \min\{i \geq 0 \,|\, a_i \neq 0\}.$$

Thus

$$\mathfrak{m}^n = \{f \in R[[X]] \,|\, \operatorname{ord}(f) \geq n\} \quad \text{and} \quad \mathfrak{m}^n \setminus \mathfrak{m}^{n+1} = \{f \in R[[X]] \,|\, \operatorname{ord}(f) = n\}.$$

Thus, $\operatorname{ord}(f) = n$ if and only if $f = X^n g$ for some $g \notin \mathfrak{m}$, i.e. $g(0) \neq 0$. If $f = \sum_i a_i X^i$ has order n, we call a_n the *order coefficient*. It is clear that $a_n = g(0)$.

Since $\mathfrak{m}^m \mathfrak{m}^n = \mathfrak{m}^{m+n}$ and $\mathfrak{m}^m + \mathfrak{m}^n \subset \mathfrak{m}^{\min\{m,n\}}$ for all $m, n \geq 0$, for $f, g \in R[[X]]$ we have

$$\operatorname{ord}(fg) \geq \operatorname{ord}(f) + \operatorname{ord}(g), \tag{2}$$
$$\operatorname{ord}(f + g) \geq \min\{\operatorname{ord}(f), \operatorname{ord}(g)\}. \tag{3}$$

In some situations we can be more precise. Suppose $m = \operatorname{ord}(f)$ and $n = \operatorname{ord}(g)$, and write $f = X^m \widetilde{f}$, $g = X^n \widetilde{g}$ with $\widetilde{f}, \widetilde{g} \in R[[X]]$ satisfying $\widetilde{f}(0) \neq 0$, $\widetilde{g}(0) \neq 0$. Then

$$fg = X^{m+n} \widetilde{f}\widetilde{g},$$

and $(\widetilde{f}\widetilde{g})(0) = \widetilde{f}(0)\widetilde{g}(0)$. If at least one of $\widetilde{f}, \widetilde{g}$ is not a zero divisor, then $(\widetilde{f}\widetilde{g})(0) \neq 0$, and we find that

$$\mathrm{ord}(fg) = m + n = \mathrm{ord}(f) + \mathrm{ord}(g).$$

A different restriction yields equality in (3). First, since $-f = X^m(-\widetilde{f})$ and $\widetilde{(-)f}(0) = -\widetilde{f}(0) \neq 0$, we have $\mathrm{ord}(-f) = \mathrm{ord}(f)$. Suppose $\mathrm{ord}(f) > \mathrm{ord}(g)$. Then $\mathrm{ord}(f+g) \geq \min\{\mathrm{ord}(f), \mathrm{ord}(g)\} = \mathrm{ord}(g)$ and so

$$\mathrm{ord}(g) = \mathrm{ord}(g + f - f) \geq \min\{\mathrm{ord}(g+f), \mathrm{ord}(-f)\} \geq \mathrm{ord}(g).$$

It follows that $\min\{\mathrm{ord}(f+g), \mathrm{ord}(f)\} = \mathrm{ord}(g)$ and hence

$$\mathrm{ord}(f+g) = \mathrm{ord}(g) = \min\{\mathrm{ord}(f), \mathrm{ord}(g)\} \tag{4}$$

when $\mathrm{ord}(g) < \mathrm{ord}(f)$. Notice that f and g are interchangeable, so it suffices to assume $\mathrm{ord}(f) \neq \mathrm{ord}(g)$ in order to reach equality (4).

The order of a power series in some sense measures its size. But a series with a large order is highly divisible by X, so "vanishes" to a high degree at $X = 0$. So it is natural to think of such a series as nearly zero, which is commensurate with the convention that $\mathrm{ord}(0) = \infty$. So we really want to think of $f \in R[[X]]$ with $\mathrm{ord}(f) \gg 1$ large as "small." This is easily arranged as follows. Choose any $\alpha \in (0, 1)$ and for $f \in R[[X]]$ define it *absolute value* to be

$$|f| = \alpha^{\mathrm{ord}(f)},$$

where $\alpha^\infty = 0$. Then $|f| \to 0$ as $\mathrm{ord}(f) \to \infty$. The inequalities (3) and (2) become

$$|fg| \leq |f| \cdot |g|, \tag{5}$$
$$|f+g| \leq \max\{|f|, |g|\}, \tag{6}$$

for all $f, g \in R[[X]]$. As above, equality holds in (5) when the product of the (nonzero) order coefficients of f and g is nonzero, in particular whenever R is free from zero divisors. On the other hand, equality in (6) guaranteed whenever $|f| \neq |g|$. Furthermore, $|f| = 0$ if and only if $\mathrm{ord}(f) = \infty$, which only happens when $f = 0$.

The shift from $\mathrm{ord}(\cdot)$ to $|\cdot|$ is mainly psychological. One is easily computed from the other, and any proof using the absolute value can easily be reformulated in terms of the order, and vice versa. However, the absolute value allows us to efficiently bring topological ideas into play. Specifically, for $f, g \in R[[X]]$, define the *distance* between them to be

$$d(f, g) = |f - g|.$$

We claim that d is an ultrametric on $R[[X]]$. Let $f, g, h \in R[[X]]$. Being an integral power of a positive real number (or zero), $d(f, g) \geq 0$, and $d(f, g) = 0$ if and only if $\mathrm{ord}(f - g) = \infty$, which is equivalent to $f - g = 0$, or $f = g$. Because $\mathrm{ord}(f - g) = \mathrm{ord}(g - f)$, $d(f, g) = d(g, f)$. Finally, we have

$$d(f, g) = |f - h + h - g| \leq \max\{|f - h|, |h - g|\} = \max\{d(f, h), d(h, g)\},$$

which is the required ultrametric inequality.

2 $R[[X]]$ as a Topological Ring

The topology on $R[[X]]$ induced by the ultrmetric d is called the $\mathfrak{m}$-*adic topology*. What does a ball in this topology look like? Let $f \in R[[X]]$ and $\epsilon > 0$. If $\epsilon \leq 1$, Then $d(f, g) < \epsilon$ if and only if $\mathrm{ord}(f - g) > \frac{\log \epsilon}{\log \alpha}$. As the order always belongs to $\mathbb{N}_0$, if M is the least positive integer greater than $\frac{\log \epsilon}{\log \alpha}$, then $d(f, g) < \epsilon$ if and only if $f - g \in \mathfrak{m}^M$. That is, if and only if $g \in f + \mathfrak{m}^M$. If $\epsilon > 1$, then $d(f, g) < \epsilon$ for all $g \in R[[X]]$, which means the ϵ-ball centered at f is all of $R[[X]]$, or $f + \mathfrak{m}^0$. So every open balls centered at f is an additive coset $f + \mathfrak{m}^M$ for some $M \in \mathbb{N}_0$. Conversely, $g \in f + \mathfrak{m}^M$ if and only if $\mathrm{ord}(f - g) \geq M$. Because we are dealing with integers, this is equivalent to the strict inequality $\mathrm{ord}(f - g) > M - \frac{1}{2}$, which occurs if and only if $|f - g| < \alpha^{M-\frac{1}{2}}$. Hence, the open balls centered at f in the $\mathfrak{m}$-adic topology are *precisely* the cosets $f + \mathfrak{m}^M$, $M \in \mathbb{N}_0$. Of course, one can eschew the use of $|\cdot|$ entirely and construct the $\mathfrak{m}$-adic topology directly by showing that the cosets of the powers of $\mathfrak{m}$ are a basis for a topology on $R[[X]]$, but in the author's opinion the use of the absolute value streamlines the process and makes the resulting topology somewhat more intuitive.

Proposition 1. *The sets $f + \mathfrak{m}^M$, where $f \in R[[X]]$ and $M \in \mathbb{N}$, form a basis for the $\mathfrak{m}$-adic topology on $R[[X]]$.*

Let $s, f, g \in R[[X]]$. Suppose that $f + g = s$. Then for any $M \in \mathbb{N}$, $(f + \mathfrak{m}^M) + (g + \mathfrak{m}^M) = (f + g) + \mathfrak{m}^M = s + \mathfrak{m}^M$. If $A : R[[X]]^2 \to R[[X]]$ is the addition function $A(f, g) = f + g$, this proves that $A((f + \mathfrak{m}^M) \times (g + \mathfrak{m}^M)) \subset s + \mathfrak{m}^M$ or $(f + \mathfrak{m}^M) \times (g + \mathfrak{m}^M) \subset A^{-1}(s + \mathfrak{m}^M)$. This shows that $A^{-1}(s + \mathfrak{m}^M)$ is open in $R[[X]]^2$, and hence that A is continuous. If $p \in R[[X]]$ and $fg = p$, then $(f + \mathfrak{m}^M) \cdot (g + \mathfrak{m}^M) \subset fg + \mathfrak{m}^M + \mathfrak{m}^{2M} = fg + \mathfrak{m}^M = p + \mathfrak{m}^M$. Therefore if $M : R[[X]]^2 \to R[[X]]$ is the multiplication function $M(f, g) = fg$, then $(f + \mathfrak{m}^M) \times (g + \mathfrak{m}^M) \subset M^{-1}(p + \mathfrak{m}^M)$, which proves that M is continuous as well. Lastly, the negation function $N : R[[X]] \to R[[X]]$ is continuous since it's invertible and $N(f + \mathfrak{m}^M) = -f + \mathfrak{m}^M$. This entire discussion goes to show that under the $\mathfrak{m}$-adic topology, $R[[X]]$ is a *topological ring.*

Proposition 2. *When endowed with the $\mathfrak{m}$-adic topology, $R[[X]]$ is a topological ring.*

3 Completeness of $R[[X]]$

Let $\{f_n\}$ be a sequence of power series in $R[[X]]$. The notions of convergent sequences and Cauchy sequences are defined using d in the usual way. Suppose $\{f_n\}$ converges to $f \in R[[X]]$. Fix an index $i_0 \in \mathbb{N}_0$. Choose $N \in \mathbb{N}$ so that $d(f_n, f) < \alpha^{i_0}$ for $n \geq N$. Then $\operatorname{ord}(f_n - f) > i_0$ for $n \geq N$. This means that the i_0 coefficient of $f_n - f$ is zero for $n \geq N$. If we write $f_n = \sum_i a_{ni} X^i$ and $f = \sum_i a_i X^i$, then we find that $a_{n,i_0} = a_{i_0}$ for $n \geq N$. In other words, the i_0-*coefficient sequence* $\{a_{n,i_0}\}_{n \in \mathbb{N}}$ stabilizes (is eventually constant). Since i_0 was arbitrary, we find that if $f_n \to f$, then for each $i \in \mathbb{N}_0$, the coefficient sequence $\{a_{ni}\}_{n \in \mathbb{N}}$ stabilizes. The converse also holds. For suppose that $\{a_{ni}\}_{n \in \mathbb{N}}$ stabilizes for all i. For each i let a_i denote the eventual constant value of $\{a_{ni}\}_{n \in \mathbb{N}}$ and set $f = \sum_i a_i X^i$. Let $M \in \mathbb{N}$ and choose N so large that $a_{ni} = a_i$ for all $n \geq N$ and $i \leq M$. That is, N is chosen so that the first $M + 1$ coefficient sequences are stable for $n \geq N$; this is possible because we are only considering a finite number of sequences. Then for $n \geq N$ and $i \leq M$, the ith coefficient of $f_n - f$ is $a_{ni} - a_i = 0$. This means that $f_n - f \in \mathfrak{m}^{M+1}$ or $d(f_n, f) = |f_n - f| \leq \alpha^{M+1} < \alpha^M$ for $n \geq N$. Since $M \in \mathbb{N}$ was arbitrary, and α^M decreases to zero as $M \to \infty$, it follows that $f_n \to f$.

So the convergent sequences are exactly those sequences whose coefficient sequences all stabilize. This means that if $\{f_n\}$ converges to f, then for any $I \in \mathbb{N}_0$, by choosing N sufficiently large, the first I coefficients of f_n and f agree, for $n \geq N$. What about Cauchy sequences? By the usual argument, every convergent sequence is Cauchy. Is the converse true? It turns out that the answer is "yes," and we will prove that this is the case by showing that every Cauchy sequence has stabilizing coefficient sequences. Fix $i_0 \in \mathbb{N}_0$. Choose $N \in \mathbb{N}$ so large that $d(f_m, f_n) < \alpha^{i_0}$ for all $m, n \geq N$. Then, in particular, $d(f_N, f_n) < \alpha^{i_0}$ for all $n \geq N$. In terms of the order, this says $\operatorname{ord}(f_N - f_n) > i_0$ for $n \geq N$. This implies that $a_{N,i_0} - a_{n,i_0} = 0$, or $a_{n,i_0} = a_{N,i_0}$ for $n \geq N$. Hence $\{a_{n,i_0}\}_{n \in N}$ stabilizes. As i_0 was arbitrary, this is true of every coefficient sequence, and our claim is proven.

Proposition 3. *Let $\{f_n\}$ be a sequence in $R[[X]]$. The following are equivalent.*

1. *$\{f_n\}$ is convergent in $R[[X]]$.*
2. *Every coefficient sequence of $\{f_n\}$ stabilizes.*
3. *$\{f_n\}$ is a Cauchy sequence.*

Our main result is now an immediate corollary of Proposition 3.

Theorem 1. *The power series ring $R[[X]]$ is complete in the $\mathfrak{m}$-adic topology.*

Coupled with the ultrametric property of d, the completeness of $R[[X]]$ has the following interesting consequence regarding the summability of infinite series.

Corollary 1. *Let $\{f_n\}$ be a sequence in $R[[X]]$. The infinite series $\sum_n f_n$ converges in $R[[X]]$ if and only if $f_n \to 0$.*

Proof. For $n \in \mathbb{N}$, let $s_n = \sum_{1\le i\le n} f_i$ be the nth partial sum of the series. We need to show that $\{s_n\}$ converges if and only if $f_n \to 0$. The forward implication is standard: if $s_n \to s$, then $s_{n-1} \to s$, so that $f_n = s_n - s_{n-1} \to s - s = 0$. To prove the converse, begin by observing that for $m < n$, we have

$$d(s_m, s_n) = |s_m - s_n| = \left|\sum_{i=m+1}^{n} f_i\right| \le \max_{m<i\le n}\{|f_i|\}$$

by the ultrametric inequality (6).[1] If $f_n \to 0$, given $\epsilon > 0$ there is an $N \in \mathbb{N}$ so that $|f_n| < \epsilon$ for $n \ge N$. So if $n > m \ge N$, we have

$$d(s_m, s_n) \le \max_{m<i\le n}\{|f_i|\} < \epsilon.$$

Hence $\{s_n\}$ is a Cauchy sequence, and therefore convergent by completeness. □

Corollary 1 shows that if $f = \sum_i a_i X^i \in R[[X]]$, then the partial sums $s_n = \sum_{0\le i\le n} a_i X^i$ form a convergent sequence. If $n \ge N$, then $\operatorname{ord}(f - s_n) \ge n+1 > N$. Hence, $d(f, s_n) < \alpha^N$ for $n \ge N$, from which we conclude that $s_n \to f$. That is,

$$f = \sum_i a_i X^i = \lim_{n\to\infty} \sum_{i=0}^{n} a_i X^i. \tag{7}$$

The sum on the left is a formal power series, nothing more than a symbolic container for the sequence $\{a_i\}$ of coefficients. The equality (7) tells us that if we use the $\mathfrak{m}$-adic topology, then f is, indeed, the sum of the infinite series suggested by the notation. Moreover, because the partial sums in (7) are all polynomials, we arrive at another corollary.

Corollary 2. *In the $\mathfrak{m}$-adic topology, the ring of polynomials $R[X]$ is dense in $R[[X]]$.*

One power series operation that can be irritating to treat directly is composition. However, it is readily treatable from the topological point of view. If $f = \sum_i a_i X^i \in R[[X]]$ and $g \in \mathfrak{m}$, then $\operatorname{ord}(a_i g^i) \ge \operatorname{ord}(a_i) + i \operatorname{ord}(g) \ge i$, which means that $a_i g^i \to 0$. Therefore the infinite series

$$f \circ g = \sum_{i=0}^{\infty} a_i g^i$$

converges in $R[[X]]$, by Lemma 7. This is the *composition* of f with g.

Let a_j, $j \in J$, be coset representatives for $R[[X]]/\mathfrak{m}$. Then $\mathcal{C} = \{a_j + \mathfrak{m}\}_{j\in J}$ is an open cover of $R[[X]]$ by nonempty, pairwise disjoint sets. As such, $\mathcal{C}$ has no proper subcover. So in order for $R[[X]]$ to be compact, it is necessary that $|J| = [R[[X]] : \mathfrak{m}] = |R|$ is finite. The converse is also true, although it's substantially harder to prove. Viewing $R[[X]]$ as $R^{\mathbb{N}_0}$, one can show that the $\mathfrak{m}$-adic topology is just the product topology, provided each factor of R is given the discrete topology. When R is finite, it is compact in the discrete topology, and Tychonoff's theorem then implies that $R^{\mathbb{N}_0}$, and hence $R[[X]]$, is compact. It would be interesting to see a purely ring-theoretic proof thet $R[[X]]$ is compact when R is finite, but it is likely that any such proof would be quite complicated.

[1] Strictly speaking, the ultrametric inequality (6) only applies to sums of two series. Its extension to arbitrary finite sums is easily proven by induction, however.

4 Examples

Let's look at a few power series rings that "occur in nature." A non-Archimedean *local field* is a field F complete with respect to a discrete valuation ν, and with a finite residue field $R/\mathfrak{p}$, where R is the valuation ring and $\mathfrak{p}$ is the valuation ideal of ν. It is a theorem in the theory of local fields that any such F is isomorphic to either a finite extension of the field of p-adic numbers $\mathbb{Q}_p$ (when the characteristic is zero), or the Laurent series ring $\mathbb{F}_q((X))$ over the finite field with q elements (when the characteristic is positive). In the second case the valuation ring is $\mathbb{F}_q[[X]]$ and the valuation ideal is $\mathfrak{m}$.

If F is a field and $a \in F$, there is an embedding $\varphi : F[X] \hookrightarrow F[[X-a]]$ which maps each polynomial to its Taylor expansion at a. Under this embedding, any $f \in F[X]$ satisfying $f(a) \neq 0$ becomes a unit in $F[[X-a]]$. That is, the elements in the complement of the maximal ideal $\mathfrak{m}_a = (X-a)$ become invertible in $F[[X-a]]$. By the universal property of localizations, we obtain an embedding $\widehat{\varphi} : F[X]_{\mathfrak{m}_a} \hookrightarrow F[[X-a]]$, which maps $\frac{f(X-a)}{g(X-a)}$ to $f(X-a)g(X-a)^{-1}$. However, not every power series in $F[[X-a]]$ has this form. One can show that the coefficients of a "rational" power series must satisfy an nth order linear recurrence, which means that a series like $\sum_i (X-a)^{i^2}$ will not be in the image of $\widehat{\varphi}$. But $\overline{\widehat{\varphi}(F[X]_{\mathfrak{m}_a})} \supset \overline{\varphi(F[X])} = F[[X-a]]$, by Corollary 2. All told, this means that the localization $F[X]_{\mathfrak{m}_a}$ is *incomplete* in the $\mathfrak{m}_a$-adic topology, and that $F[[X-a]]$ serves as its completion. This is analogous to the construction of the p-adic integers $\mathbb{Z}_p$, p prime, from $\mathbb{Z}$. One first localizes to $\mathbb{Z}_{p\mathbb{Z}} = \{\frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{N}, p \nmid b\}$, and then completes $\mathbb{Z}_{p\mathbb{Z}}$ in the p-adic topology. The resulting ring $\mathbb{Z}_p$ is not a formal power series ring, but the elements can still be expressed as convergent power series in p.