ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 2, Number 2, Spring 1972

ON THE WEIERSTRASS PREPARATION THEOREM

MATTHEW O'MALLEY

Introduction. Suppose that R is a commutative ring with identity, X is an indeterminate over R, and $S = R[[X]]$ is the formal power series ring. In [**1**, §3, Proposition 6], the following result (Weierstrass Preparation Theorem) is proved when R is a local ring, complete in its maximal ideal adic topology: Suppose that $f = \sum_{i=0} a_i X^i \in S$, where, for some $n \geqq 1$, a_n is a unit of R and $(a_0, a_1, \cdots, a_{n-1}) \subseteq M$, the maximal ideal of R. Then there exists a unique pair u, $F \in S$ such that u is a unit of S and F is a monic polynomial of degree n with the property that the coefficients of X^i in F, for $i < n$, are elements of M, and such that $f = uF$.

In this paper we extend this result, together with Proposition 5 of [**1**, §3] and its Corollary, to the case when R is any commutative ring with identity and $f = \sum_{i=0} a_i X^i$ satisfies the property that, for some $n \geqq 1$, a_n is a unit of R, while the ideal $A = (a_0, a_1, \cdots, a_{n-1})$ generates a complete Hausdorff topology on R.

In §1 we give the notation and terminology used throughout the paper, and we prove three results needed in §2. §2 contains our main results.

All rings considered in this paper are assumed to be commutative and to contain an identity element. The symbols ω and ω_0 are used throughout the paper to denote the sets of positive and nonnegative integers, respectively. A collection of ideals $\{A_k\}_{k \in \omega}$ of the ring R will be called a *d-sequence* provided that for any n, $m \in \omega$ there exists a $u \in \omega$, depending on n and m, such that $A_u \subseteq A_n \cap A_m$.

1. **Preliminaries.** Let R be a ring, and let Ω be the topology induced on R by the d-sequence $\{A_k\}_{k \in \omega}$ of R. We write (R, Ω) to denote the topological ring R under the topology Ω. It is well known that (R, Ω) is Hausdorff if and only if $\bigcap_{k \in \omega} A_k = (0)$. We say that (R, Ω) is *complete* if each Cauchy sequence of R converges to a point of R. If there exists an ideal M of R such that $M^k = A_k$ for each $k \in \omega$, then the topology Ω is called the M-adic topology, and we write (R, M) instead of (R, Ω) in this case.

(1.1) LEMMA. *Let R be a ring and suppose that the topology Ω induced on R by the d-sequence $\{A_k\}_{k \in \omega}$ of R is Hausdorff. Then,*

Received by the editors December 9, 1970.
AMS 1970 *subject classifications.* Primary 13J05, 13J10; Secondary 32B05.

if $c \in R$ and if each Cauchy sequence of $(R, (c))$ converges in (R, Ω), then $(R, (c))$ is a complete Hausdorff space. ((c) denotes the ideal of R generated by c.) Moreover, c belongs to the Jacobson radical of R.

PROOF. Let $c \in R$, and suppose that $(R, (c))$ satisfies the hypothesis of the lemma. Then the proof of Theorem (4.2) of [2] shows that for any $\beta \in S = R[[X]]$ with constant term c, there exists an R-endomorphism ϕ of S mapping X onto β. But, since (R, Ω) is Hausdorff, $(R, (c))$ is Hausdorff, and, therefore, by [2, Theorem (4.10)], $(R, (c))$ is complete. Moreover, by [2, Lemma (5.1)], c belongs to the Jacobson radical of R.

As a special case of Lemma (1.1), we observe that if Ω is the A-adic topology for some ideal A of R, then, for any $c \in A$, $(R, (c))$ is a complete Hausdorff space if R is complete and Hausdorff in the A-adic topology. Furthermore, A is contained in the Jacobson radical of R.

Our next result relates a topological property of R to that of S. Namely, if A is an ideal of the ring R, then $\{A^k[[X]]\}_{k \in \omega}$ is a d-sequence of ideals of S, and hence induces a topology Λ on S. ($A^k[[X]]$ denotes the set of all power series in S all of whose coefficients are elements of the ideal A^k of R.) We show that R is complete in the A-adic topology if and only if S is complete under the topology Λ. Since $\bigcap_{k \in \omega}(A)^k = (0)$ if and only if $\bigcap_{k \in \omega}(A^k[[X]]) = (0)$, it will follow that (R, A) is a complete Hausdorff space if and only if (S, Λ) is a complete Hausdorff space.

(1.2) LEMMA. *Let A be an ideal of the ring R. Then (R, A) is complete if and only if (S, Λ) is complete.*

PROOF. Suppose that (S, Λ) is complete and let $\{c_n\}_{n \in \omega}$ be a Cauchy sequence of (R, A). Since $A^k \subseteq A^k[[X]]$ for each $k \in \omega$, it follows that $\{c_n\}_{n \in \omega}$ is Cauchy in (S, Λ) and hence, there exists $g = \sum_{i=0}^{\infty} a_i X^i \in S$ such that $c_n \to g$ in (S, Λ). But clearly this implies that $c_n \to a_0$ in (R, A). Consequently, (R, A) is complete.

The converse follows from the proof of Lemma (4.6) of [2].

We note that for any ideal A of the ring R, $A^n S = (AS)^n$ for each $n \in \omega$, and, if A is finitely generated, then $A^n S = A^n[[X]]$. Hence, if A is finitely generated, then Λ is the AS-adic topology on S, and Lemma (1.2) shows that R is complete in the A-adic topology if and only if S is complete in the AS-adic topology.

We conclude this section with a result needed in the proof of Theorem (2.6). The proof is straightforward and we omit it.

(1.3) LEMMA. *Let $\beta = \sum_{i=0}^{\infty} a_i X^i \in S$ and let A denote the ideal $\bigcap_{k \in \omega}(a_0)^k$ of R. Then $\bigcap_{k \in \omega}(\beta)^k \subseteq A[[X]]$, where (β) denotes the*

ideal of S generated by β. Therefore, if $(R, (a_0))$ is Hausdorff, then $(S, (\beta))$ is Hausdorff.

2. **The Weierstrass Preparation Theorem.** In this section we give our main results. The proof of our first theorem follows closely the proof of Proposition 5 of [1, p. 38], and we only sketch the proof here.

(2.1) THEOREM. *Let R be a ring with identity and let $f = \sum_{i=0}^{\infty} a_i X^i \in S$. Suppose that, for some $n \geqq 1$, a_n is a unit of R, and that the ideal $A = (a_0, a_1, \cdots, a_{n-1})$ of R generates a complete Hausdorff topology on R. If M is the R-submodule of S generated by $\{1, X, \cdots, X^{n-1}\}$, then S is the direct sum of M and fS.*

PROOF. (i) We first observe that $fS \cap M = (0)$. For if

$$\left(\sum_{i=0}^{\infty} b_i X^i \right) \cdot f = r_0 + r_1 X + \cdots + r_{n-1} X^{n-1},$$

where $b_i, r_i \in R$ for each i, then the proof of Proposition 5 given in [1, p. 38] shows that $b_i \in \bigcap_{k \in \omega} (A)^k$ for each $i \in \omega_0$. Hence, since (R, A) is Hausdorff, b_i (and, therefore, r_i) is zero for each i. Thus, $fS \cap M = (0)$. It should be noted that the proof of (i) depends only on the conditions that (R, A) is Hausdorff and that a_n is a unit of R.

(ii) We show that $S = fS + M$. If $g = \sum_{i=n}^{\infty} a_i X^{i-n}$, then g is a unit of S, and $f - X^n g = \sum_{i=0}^{n-1} a_i X^i$. Moreover, if $-h = -\sum_{i=0}^{\infty} h_i X^i = (f - X^n g) g^{-1}$, then $h_i \in A$ for each $i \in \omega_0$.

Let $\alpha \in S$. By recursion on j, we define a set of elements $q^{(j)}$ of S in the following way:

Let $q^{(0)}$ be the unique element of S satisfying

$$\alpha \equiv X^n q^{(0)} \pmod{M}. \tag{2.2}$$

For $j \in \omega_0$, let $q^{(j)} = \sum_{i=0}^{\infty} q_i^{(j)} X^i$, where, for $j \geqq 1$,

$$q_i^{(j)} = \sum_{k=0}^{i+n} h_k q_{i+n-k}^{(j-1)}. \tag{2.3}$$

It follows that, for $j \geqq 1$,

$$X^n q^{(j)} \equiv h q^{(j-1)} \pmod{M}. \tag{2.4}$$

Since $h_i \in A$ for each i, it follows from (2.3), by induction on n, that $q_i^{(j)} \in A^j$ for all $i \in \omega_0$ and each $j \in \omega$. It follows, therefore, that $\{\sum_{j=0}^{t} q^{(j)}\}_{t \in \omega_0}$ is a Cauchy sequence of S in the topology Λ induced on S by the sequence of ideals $\{A^k[[X]]\}_{k \in \omega}$. Thus, since (R, A) is a complete Hausdorff space, it follows from Lemma (1.2) that

(S, Λ) is a complete Hausdorff space. Therefore, there exists a unique element $q \in S$ such that q is the limit of the sequence $\{\sum_{j=0}^{t} q^{(j)}\}_{t \in \omega_0}$ in (S, Λ). From (2.2) and (2.4) we have that

$$\alpha + h\left(\sum_{j=0}^{t-1} q^{(j)}\right) \equiv X^n\left(\sum_{j=0}^{t} q^{(j)}\right) (\text{mod } M),$$

for each $t \in \omega$, and hence

$$\alpha + h\left(\sum_{j=0}^{t-1} q^{(j)}\right) - X^n\left(\sum_{j=0}^{t} q^{(j)}\right) = m_t \in M,$$

for each $t \in \omega$. Thus, since the limit on the left exists in (S, Λ), the limit on the right exists, and we have that

$$\alpha + hq - X^n q = \lim_t m_t.$$

Therefore,

$$\alpha = (X^n - h)q + \lim_t m_t$$

$$= fg^{-1}q + \lim_t m_t,$$

where $fg^{-1}q \in fS$. Thus, it suffices to show that M is closed in (S, Λ). But this is straightforward and we omit it.

Note that the proof of the equality of $fS \cap M = (0)$ shows that f is regular (not a zero divisor) in S. From this fact, it follows that if $\alpha = hf + \sum_{i=0}^{n-1} r_i X^i = h_1 f + \sum_{i=0}^{n-1} u_i X^i$ are two representations for α as an element of $fS + M$, then $h = h_1$ and $r_i = u_i$ for $0 \leqq i \leqq n - 1$.

If $g = \sum_{i=0}^{\infty} c_i X^i \in S$, where R is complete and Hausdorff in the (c_0)-adic topology, then [2, Theorems (4.2) and (4.3)] shows that there exists a unique R-endomorphism ϕ_g of S that maps X onto g. We denote the range of ϕ_g by $R[[g]]$.

In particular, if $f = \sum_{i=0}^{\infty} a_i X^i \in S$, and if f satisfies the hypothesis of Theorem (2.1), then it follows from Lemma (1.1) that R is complete and Hausdorff in the (a_0)-adic topology. Thus, there exists a unique R-endomorphism ϕ_f of S such that $\phi_f(X) = f$. We next show that, for any $f \in S$ satisfying the hypothesis of Theorem (2.1), ϕ_f is one-to-one. We make use of [3] to prove a more general result than this.

(2.5) LEMMA. *Let $g \in S$ and suppose that there exists an R-endomorphism ψ of S mapping X onto g. If T denotes the range of ψ, and if g satisfies the following conditions:*

(i) *g is regular in T, and*

(ii) $gT \cap R = (0)$,

then ψ is one-to-one. In particular, if f satisfies the hypothesis of Theorem (2.1), *then ϕ_f is one-to-one.*

PROOF. Let $h = \sum_{j=0}^{\infty} h_j X^j \in S$ and suppose that $\psi(h) = 0$. By [3, Result (2.1)], $\psi(h)$ is a limit point in $(T, (gT))$ of the sequence $\{\sum_{j=0}^{n} h_j g^j\}_{n \in \omega_0}$.

Fix $k \in \omega$. We show that $h_j = 0$ for $0 \leqq j \leqq k$. Note that T contains $R[g]$, the subring of S consisting of all elements of the form $\sum_{i=0}^{u} r_i g^i$, $r_i \in R$. Now, since $\psi(h) = 0$, we have that $\sum_{j=0}^{n} h_j g^j \to 0$ in $(T, (gT))$, and therefore, for $(g^{k+1}T)$, a neighborhood of 0, there exists $N \in \omega$, $N > k$, such that $\sum_{j=0}^{n} h_j g^j \in (g^{k+1}T)$ for $n \geqq N$. Let $\sum_{j=0}^{n} h_j g^j = g^{k+1}\alpha$, $\alpha \in T$. Then,

$$h_0 = -g\left(\sum_{j=1}^{n} h_j g^{j-1} - g^k \alpha\right),$$

and, hence, by (ii), $h_0 = 0$.

Suppose we have shown that $h_j = 0$ for $0 \leqq j < r \leqq k$. We show that $h_r = 0$. By the induction hypothesis, we have $\sum_{j=r}^{n} h_j g^j = g^{k+1}\alpha$, and thus, $g^r(\sum_{j=r}^{n} h_j g^{j-r} - g^{k+1-r}\alpha) = g^r u = 0$. Since $u \in T$, it follows from (i) that $u = \sum_{j=r}^{n} h_j g^{j-r} - g^{k+1-r}\alpha = 0$. Thus

$$h_r = -g\left(\sum_{j=r+1}^{n} h_j g^{j-(r+1)} - g^{k-r}\alpha\right),$$

and therefore, $h_r = 0$. It follows, by induction, that $h_j = 0$ for $0 \leqq j \leqq k$, and thus, since k was arbitrary, we have that $h = 0$. This completes the proof.

Our next result corresponds to the Corollary to Proposition 5 of [**1**, p. 40].

(2.6) THEOREM. *Let $f \in S$ and suppose that f satisfies the hypothesis of Theorem* (2.1). *Then $\{1, X, \cdots, X^{n-1}\}$ is a free-module basis for S over $R[[f]]$. Furthermore, the unique R-endomorphism ϕ_f of S mapping X onto f is one-to-one.*

PROOF. We have already observed the last statement of the theorem (Lemma (2.5)). We prove the first part of the theorem in a series of steps.

For each $k \in \omega$, let T_k denote $f^{k-1}R + f^{k-2}R + \cdots + fR + R$, the R-submodule of $R[f]$ consisting of all terms of the form: $\sum_{i=0}^{k-1} r_i f^i$, $r_i \in R$. (Note that $T_1 = R$.) We first observe that, for any $k \in \omega$,

$$S = f^k S + T_k \cdot 1 + T_k \cdot X + \cdots + T_k \cdot X^{n-1}. \tag{2.7}$$

The case for $k = 1$ is proved in Theorem (2.1), and, for $k > 1$, the proof follows easily by induction on k.

We next observe that, for any $k \in \omega$,

$$f^k S \cap [T_k \cdot 1 + T_k \cdot X + \cdots + T_k \cdot X^{n-1}] = (0). \tag{2.8}$$

Again the case for $k = 1$ is proved in Theorem (2.1). We suppose that (2.8) is valid for $k = u$, and we let

$$gf^{u+1} = \sum_{j=0}^{n-1} \left(\sum_{i=0}^{u} r_i^{(j)} f^i \right) X^j,$$

where $g \in S$, $r_i^{(j)} \in R$ for all i, j. It follows that

$$gf^{u+1} = \left(\sum_{j=0}^{n-1} r_u^{(j)} X^j \right) f^u + \sum_{j=0}^{n-1} \left(\sum_{i=0}^{u-1} r_i^{(j)} f^i \right) X^j,$$

and hence,

$$\left[gf - \sum_{j=0}^{n-1} r_u^{(j)} X^j \right] f^u = \sum_{j=0}^{n-1} \left(\sum_{i=0}^{u-1} r_i^{(j)} f^i \right) X^j.$$

Therefore, by the induction hypothesis and since f is regular in S, we have that

$$gf - \sum_{j=0}^{n-1} r_u^{(j)} X^j = 0,$$

and

$$\sum_{j=0}^{n-1} \left(\sum_{i=0}^{u-1} r_i^{(j)} f^i \right) X^j = 0.$$

In particular, since $gf = \sum_{j=0}^{n-1} r_u^{(j)} X^j$, it follows from the case for $k = 1$ that $g = 0$, and we have proved (2.8). We note that it follows from the proof of (2.8) that if $\sum_{j=0}^{n-1} (\sum_{i=0}^{k} r_i^{(j)} f^i) X^j = 0$ for any $k \in \omega_0$, then $r_i^{(j)} = 0$ for all i, j. From this observation and from (2.8), it follows that if $\alpha \in S$ and if

$$\alpha = f^k s_k + \sum_{j=0}^{n-1} \left(\sum_{i=0}^{k-1} r_i^{(j)} f^i \right) X^j,$$

and

$$\alpha = f^{k+r} s_{k+r} + \sum_{j=0}^{n-1} \left(\sum_{i=0}^{r+(k-1)} t_i^{(j)} f^i \right) X^j$$

are two representations for α as an element of

$$f^k S + T_k \cdot 1 + T_k \cdot X + \cdots + T_k \cdot X^{n-1},$$

and

$$f^{k+r} S + T_{k+r} \cdot 1 + T_{k+r} \cdot X + \cdots + T_{k+r} \cdot X^{n-1},$$

respectively, then $r_i^{(j)} = t_i^{(j)}$ for each j and for $0 \leqq i \leqq k-1$. Hence, in our representation for α, as $k \to \infty$, the $r_i^{(j)}$ for $i < k$ remain fixed, and, in this sense, are independent of k.

Let $\alpha \in S$ and suppose that

$$\left\{ f^k s_k + \sum_{j=0}^{n-1} \left(\sum_{i=0}^{k-1} r_i^{(j)} f^i \right) X^j \right\}_{k \in \omega}$$

is the collection of representations of α as an element of the sets $\{f^k S + T_k \cdot 1 + T_k \cdot X + \cdots + T_k \cdot X^{n-1}\}_{k \in \omega}$. We show that

$$(2.9) \quad \alpha = \sum_{i=0}^{\infty} r_i^{(0)} f^i + \left(\sum_{i=0}^{\infty} r_i^{(1)} f^i \right) X + \cdots + \left(\sum_{i=0}^{\infty} r_i^{(n-1)} f^i \right) X^{n-1}.$$

This will show that

$$S = R[[f]] \cdot 1 + R[[f]] \cdot X + \cdots + R[[f]] \cdot X^{n-1}.$$

To prove (2.9), we show that the sequence of points

$$\left\{ f^k s_k + \sum_{j=0}^{n-1} \left(\sum_{i=0}^{k-1} r_i^{(j)} f^i \right) X^j \right\}_{k \in \omega} = \{\alpha\}_{k \in \omega}$$

of S converges in the (f)-adic topology on S to the right-hand side of (2.9). Hence, since $\{\alpha\}_{k \in \omega} \to \alpha$, and since S is Hausdorff in the (f)-adic topology (Lemma (1.3)), it will follow that (2.9) is true. Let $(f)^m$ be a neighborhood of 0 in $(S, (f))$ and choose $k \geqq m$. Then

$$\sum_{j=0}^{n-1} \left(\sum_{i=0}^{\infty} r_i^{(j)} f^i \right) X^j - \left(f^k s_k + \sum_{j=0}^{n-1} \left(\sum_{i=0}^{k-1} r_i^{(j)} f^i \right) X^j \right)$$

$$= \sum_{j=0}^{n-1} \left(\sum_{i=k}^{\infty} r_i^{(j)} f^i \right) X^j - f^k s_k$$

$$= f^k \left(\left[\sum_{j=0}^{n-1} \left(\sum_{i=0}^{\infty} r_{i+k}^{(j)} f^i \right) X^j \right] - s_k \right) \in (f)^k \subseteq (f)^m.$$

Finally, we observe that arguments similar to those already used in the proof show that $\{1, X, \cdots, X^{n-1}\}$ is a free basis, and we omit the proof.

REMARK. It should be observed here that Theorem (2.6) has an important application in the generalization of a result of Samuel [4]. In particular, let R be a Noetherian integral domain with identity whose integral closure is a finite R-module, let $S = R[[X]]$, and let $G = \{\phi_i\}_{i=1}^{n}$ be a finite group of R-automorphisms of S. If $f = \prod_{i=1}^{n} \phi_i(X) = \sum_{i=0}^{\infty} a_i X^i$, then it can be shown that the coefficients of f satisfy the hypothesis of Theorem (2.1), and hence, $\{1, X, \cdots, X^{n-1}\}$ is a free-module basis for S over $R[[f]]$. This result is of prime importance in the proof that the ring $S^G = \{h \in S \mid \phi_i(h) = h$ for each $i = 1, \cdots, n\}$ of invariants of G is $R[[f]]$. The details will appear elsewhere.

Next, we give our extension of Proposition 6 of [1, p. 41].

(2.10) THEOREM. *Let R be a ring with identity and let $f = \sum_{i=0}^{\infty} a_i X^i \in S$. Suppose that for some $n \geqq 1$, a_n is a unit of R, and suppose that the ideal $A = (a_0, a_1, \cdots, a_{n-1})$ of R generates a complete Hausdorff topology on R. Then there exists a unique pair u, $F \in S$ such that u is a unit of S, $F = r_0 + r_1 X + \cdots + r_{n-1}X^{n-1} + X^n$, where $r_i \in A$ for each i, and $f = uF$.*

PROOF. By Theorem (2.1), X^n has a unique representation as an element of $fS + M$, where M is the R-submodule of S generated by $\{1, X, \cdots, X^{n-1}\}$. Let

$$X^n = gf + (r_0 + r_1 X + \cdots + r_{n-1}X^{n-1}) . \tag{2.11}$$

Then $gf = X^n - (r_0 + r_1 X + \cdots + r_{n-1}X^{n-1})$. Thus, if $g = \sum_{j=0}^{\infty} g_j X^j$, then the coefficient of X^n in gf is $\sum_{i+j=n} a_i g_j$, and, by definition of equality in S, we have that $\sum_{i+j=n} a_i g_j = 1$. Therefore, $a_n g_0 = 1 - (a_{n-1}g_1 + \cdots + a_0 g_n)$, and, since (R, A) is a complete Hausdorff space, it follows from the remark following Lemma (1.1) that $a_{n-1}g_1 + \cdots + a_0 g_n$ is in the Jacobson radical of R. By [5, Lemma 2, p. 206], it follows that $a_n g_0$ is a unit of R, and therefore g_0 is a unit of R. Thus, g is a unit of S [6, p. 131], and $f = g^{-1}(X^n - r_{n-1}X^{n-1} - \cdots - r_0)$. Since $r_k = \sum_{i+j=k} a_i g_j$ for $0 \leqq k \leqq n - 1$, each $r_k \in A$. Therefore $u = g^{-1}$ and $F = -r_0 - r_1 X - \cdots - r_{n-1}X^{n-1} + X^n$ satisfy the conclusion of the theorem, and $f = uF$.

The uniqueness of u and F follows easily from the uniqueness of the representation (2.11), and we omit the details. This completes the proof.

References

1. N. Bourbaki, *Albèbre commutative.* Chap. 7: *Diviseurs,* Actualités Sci. Indust., no. 1314, Hermann, Paris, 1965. MR **41** #5339.

2. M. O'Malley, *R-automorphisms of* $R[[X]]$, Proc. London Math. Soc. (3) **20** (1970), 60–78. MR **40** #7249.

3. M. O'Malley and C. Wood, *R-endomorphisms of* $R[[X]]$, J. Algebra **15** (1970), 314–327. MR **41** #8407.

4. P. Samuel, *Groupes finis d'automorphismes des anneaux de séries formelles,* Bull. Sci. Math. (2) **90** (1966), 97–101. MR **35** #180.

5. O. Zariski and P. Samuel, *Commutative algebra.* I, Univ. Series in Higher Math., Van Nostrand, Princeton, N. J., 1958. MR **19**, 833.

6. ——, *Commutative algebra.* II, Univ. Series in Higher Math., Van Nostrand, Princeton, N. J., 1960. MR **22** #11006.

NASA Manned Spacecraft Center, Mail Code: ED 3, Houston, Texas 77058