WEIERSTRASS PREPARATION THEOREM

ROY EDUARDO YARANGA ALMEIDA

1. Introduction

The purpose of this note is to establish a version of the Weierstrass Preparation Theorem that is sufficient to prove Strassmann's theorem. We restrict our attention to analytic functions on the closed unit disk over $\mathbb{Z}_p$.

We begin by introducing the ring of analytic power series on $\mathbb{Z}_p$ together with the notion of Strassmann number, and then we prove a division lemma in this ring. Using this result, we establish a version of the Weierstrass Preparation Theorem, obtaining a factorization of a nonzero analytic function into a polynomial factor and a unit. Finally, we apply this factorization to prove Strassmann's theorem, which gives an upper bound for the number of zeros of a convergent p-adic power series in terms of its Strassmann number.

For further background on p-adic analysis, see [1]. A more comprehensive treatment can be found in [2].

2. Preliminaries

Definition 2.1. The *ring of p-adic integers* $\mathbb{Z}_p$ is the completion of $\mathbb{Z}$ with respect to $|\cdot|_p$. Concretely,

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}.$$

It is a local ring with unique maximal ideal $\mathfrak{m}_p = p\mathbb{Z}_p = \{x \in \mathbb{Z}_p : |x|_p < 1\}$ and residue field $k = \mathbb{Z}_p/\mathfrak{m}_p \cong \mathbb{Z}/p\mathbb{Z}$.

Definition 2.2. The *ring of analytic power series* on the closed unit disk is

$$A_1 = \Big\{ f = \sum_{n\geq 0} a_n X^n \in \mathbb{Z}_p[[X]] : \lim_{n\to\infty} |a_n|_p = 0 \Big\}.$$

For $f \in A_1$ we define the norm $\|f\| = \max_{n\geq 0} |a_n|_p$ (which exists since $|a_n|_p \to 0$). Each element of A_1 defines a continuous function $f : \mathbb{Z}_p \to \mathbb{Z}_p$ by substitution; convergence follows from $|a_n|_p \to 0$ and the ultrametric inequality.

Date: 28-09-2025.

Definition 2.3. For a nonzero $f = \sum a_n X^n \in A_1$, the *Strassmann number* $s(f)$ is the largest index $N \geq 0$ such that $|a_N|_p = \|f\|$, that is,

$$s(f) = \max\big\{N \geq 0 : |a_N|_p = \|f\|\big\}.$$

Equivalently, $|a_N|_p = \max_n |a_n|_p$ and $|a_n|_p < |a_N|_p$ for all $n > N$.

Lemma 2.4. *A_1 is complete with respect to the norm $\|\cdot\|$.*

Proof. Let (f_i) be a Cauchy sequence in A_1, where $f_i(X) = \sum_{n\geq 0} a_{i,n} X^n$. Given $\varepsilon > 0$, there exists M such that $\|f_i - f_j\| < \varepsilon$ for all $i, j > M$, which means $|a_{i,n} - a_{j,n}|_p < \varepsilon$ for all n and all $i, j > M$. In particular, for each fixed n, the sequence $(a_{i,n})_i$ is Cauchy in $\mathbb{Z}_p$. By completeness of $\mathbb{Z}_p$, there exists $a_n = \lim_{i\to\infty} a_{i,n}$.

Let $f(X) = \sum_{n\geq 0} a_n X^n$. Taking the limit $j \to \infty$ in $|a_{i,n} - a_{j,n}|_p < \varepsilon$ gives $|a_{i,n} - a_n|_p \leq \varepsilon$ for all n and all $i > M$, so $\|f_i - f\| \leq \varepsilon$ for $i > M$, that is, $f_i \to f$ in norm.

It remains to show that $f \in A_1$. Given $\varepsilon > 0$, fix some $i > M$. Since $f_i \in A_1$, there exists M_i such that $|a_{i,n}|_p < \varepsilon$ for all $n > M_i$. Then for $n > M_i$:

$$|a_n|_p \leq |a_n - a_{i,n}|_p + |a_{i,n}|_p < \varepsilon + \varepsilon = 2\varepsilon.$$

Hence $a_n \to 0$ and $f \in A_1$. ∎

Lemma 2.5. *The subspace $\mathbb{Z}_p[X]$ is dense in A_1.*

Proof. Let $f(X) = \sum_{n\geq 0} a_n X^n \in A_1$. For each $k \geq 0$ define the truncation $f_k(X) = \sum_{n=0}^{k} a_n X^n \in \mathbb{Z}_p[X]$. Then

$$\|f - f_k\| = \max_{n>k} |a_n|_p \xrightarrow{k\to\infty} 0,$$

since $a_n \to 0$. Hence $f_k \to f$ and $\mathbb{Z}_p[X]$ is dense in A_1. ∎

3. The Division Lemma

Lemma 3.1. *Let $g(X) = b_0 + b_1 X + \cdots + b_N X^N \in \mathbb{Z}_p[X]$ be a polynomial with $|b_N|_p = \|g\|$. For every $f \in A_1$ there exist unique $q \in A_1$ and $r \in \mathbb{Z}_p[X]$ with $\deg r < N$ such that*

$$f = g \cdot q + r,$$

and moreover $\|f\| \geq \|g\|\|q\|$ and $\|f\| \geq \|r\|$.

Proof. Let $f \in \mathbb{Z}_p[X]$ be a polynomial. By Euclidean division in $\mathbb{Q}_p[X]$, there exist unique $q, r \in \mathbb{Q}_p[X]$ with $\deg r < N$ and $f = gq + r$. We will show that $\|f\| \geq \|g\|\|q\|$ and $\|f\| \geq \|r\|$.

Without loss of generality we may assume $|b_N|_p = \|g\| = 1$. Let

$$c = \max\{\|q\|, \|r\|\}.$$

If $c \leq \|f\|$ there is nothing to prove. Suppose for contradiction that $c > \|f\|$. Dividing the identity $f = gq + r$ by c gives $f' = gq' + r'$, where

$$f' = \frac{f}{c}, \qquad q' = \frac{q}{c}, \qquad r' = \frac{r}{c}.$$

By construction, $\max\{\|q'\|, \|r'\|\} = 1$, while $\|f'\| = \|f\|/c < 1$. So all coefficients of f' lie in $\mathfrak{m}_p$, meaning $\overline{f'} = 0$. Reducing $f' = gq' + r'$ modulo $\mathfrak{m}_p$:

$$0 = \bar{g}\,\bar{q}' + \bar{r}'.$$

Since $|b_N|_p = 1$ we have $\deg(\bar{g}) = N$, and $\deg(\bar{r}') < N$. If $\bar{q}' \neq 0$ then $\deg(\bar{g}\,\bar{q}') \geq N$, which is incompatible with $\deg(\bar{r}') < N$. Hence $\bar{q}' = 0$, and then $\bar{r}' = 0$. Therefore $\|q'\| < 1$ and $\|r'\| < 1$, contradicting $\max\{\|q'\|, \|r'\|\} = 1$.

This contradiction shows that $c \leq \|f\|$, i.e., $\|f\| \geq \|q\|$ and $\|f\| \geq \|r\|$. Rescaling (without assuming $|b_N|_p = 1$) gives $\|f\| \geq \|g\|\|q\|$ and $\|f\| \geq \|r\|$.

We now prove uniqueness. Suppose $gq + r = gq' + r'$ with $\deg r, \deg r' < N$. Then $g(q - q') = r' - r$. The right-hand side is a polynomial of degree $< N$. Dividing $r' - r$ by g using the argument above, the unique quotient is $q - q'$ and the unique remainder is 0. But $\deg(r' - r) < N = \deg g$, so the quotient of the Euclidean division of $r' - r$ by g must be 0. Hence $q - q' = 0$ and $r' - r = 0$, i.e., $q = q'$ and $r = r'$.

Now let $f \in A_1$ and let (f_k) be a sequence of polynomials with $f_k \to f$ in A_1 (Lemma 2.5). For each k, write $f_k = gq_k + r_k$ for the division obtained above. Subtracting consecutive divisions:

$$f_{k+1} - f_k = g(q_{k+1} - q_k) + (r_{k+1} - r_k).$$

Since $\deg(r_{k+1} - r_k) < N$, this is the Euclidean division of $f_{k+1} - f_k$ by g. Applying the norm estimates:

$$\|q_{k+1} - q_k\| \leq \|g\|^{-1}\|f_{k+1} - f_k\|, \qquad \|r_{k+1} - r_k\| \leq \|f_{k+1} - f_k\|.$$

Since $f_k \to f$, we have $\|f_{k+1} - f_k\| \to 0$, so (q_k) and (r_k) are Cauchy.

By completeness of A_1 (Lemma 2.4), there exist $q = \lim q_k \in A_1$ and $r = \lim r_k \in A_1$. Since each r_k is a polynomial of degree $< N$ and $r_k \to r$, the limit r is a polynomial of degree $< N$. Passing to the limit in $f_k = gq_k + r_k$ gives $f = gq + r$. The norm estimates are preserved in the limit. ∎

4. The Weierstrass Preparation Theorem

Theorem 4.1 (Weierstrass Preparation)**.** Let $f = \sum_{n\geq 0} a_n X^n \in A_1$ be nonzero, and let $N = s(f)$, so that

$$|a_N|_p = \|f\| \quad \text{and} \quad |a_n|_p < \|f\| \text{ for all } n > N.$$

Then there exist a polynomial $g(X) \in \mathbb{Z}_p[X]$ of degree N and a series $h(X) \in A_1$ such that:

(i) $f(X) = g(X)\,h(X)$,
(ii) $|b_N|_p = \|g\|$ (where $g = \sum b_i X^i$),
(iii) $h(X) = 1 + \sum_{n\geq 1} c_n X^n$ with $|c_n|_p < 1$ for all $n \geq 1$.

In particular, h has no zeros in $\mathbb{Z}_p$.

Proof. Define

$$g_1(X) = a_0 + a_1 X + \cdots + a_N X^N, \qquad h_1(X) = 1.$$

By definition of $s(f)$, the coefficients of f beyond degree N satisfy $|a_n|_p < \|f\|$, so

$$\delta := \frac{\|f - g_1\|}{\|f\|} = \frac{\max_{n>N} |a_n|_p}{\|f\|} < 1.$$

If f is a polynomial of degree N then $\delta = 0$ and $f = g_1 \cdot 1$ is the desired factorization. Otherwise $0 < \delta < 1$. One checks that $\|g_1\| = |a_N|_p = \|f\|$ and $\|f - g_1 h_1\| \leq \delta \|f\|$.

Suppose we have constructed $g_i \in \mathbb{Z}_p[X]$ of degree N and $h_i \in A_1$ satisfying:

- $g_i(X) = a_N X^N +$ lower-degree terms, $\|g_i\| = \|f\|$,
- $\|h_i - 1\| \leq \delta$,
- $\|f - g_i h_i\| \leq \delta^i \|f\|$.

Apply Lemma 3.1 to divide $f - g_i h_i$ by g_i:

$$f - g_i h_i = g_i \cdot q_i + r_i, \quad \deg r_i < N,$$

with $\|q_i\| \leq \delta^i$ and $\|r_i\| \leq \delta^i \|f\|$. Set $g_{i+1} = g_i + r_i$ and $h_{i+1} = h_i + q_i$. Then:

$$\begin{aligned} f - g_{i+1} h_{i+1} &= f - (g_i + r_i)(h_i + q_i) \\ &= f - g_i h_i - q_i g_i - r_i h_i - r_i q_i \\ &= (f - g_i h_i - g_i q_i - r_i) + r_i(1 - h_i - q_i) \\ &= r_i(1 - h_i - q_i), \end{aligned}$$

where in the last step we used $f - g_i h_i = g_i q_i + r_i$. Therefore:

$$\|f - g_{i+1} h_{i+1}\| \leq \|r_i\| \cdot \max\{\|1 - h_i\|,\, \|q_i\|\} \leq \delta^i \|f\| \cdot \delta = \delta^{i+1} \|f\|.$$

Since $\deg r_i < N$, the leading term of g_{i+1} agrees with that of g_i, so $\|g_{i+1}\| = \|f\|$. Also $\|h_{i+1} - 1\| \leq \delta$.

Finally, the estimates $\|g_i - g_{i+1}\| = \|r_i\| \leq \delta^i \|f\|$ and $\|h_i - h_{i+1}\| = \|q_i\| \leq \delta^i$ show that (g_i) and (h_i) are Cauchy in A_1. By completeness (Lemma 2.4), they converge to g and h in A_1. Since each g_i has degree exactly N (adding r_i of degree $< N$ does not affect the leading term), the limit g is a polynomial of degree N. Passing to the limit in $f = g_i h_i + (f - g_i h_i)$ gives $f = gh$. Properties (i)–(iii) are inherited from the construction. ∎

5. Strassmann's Theorem

Lemma 5.1. *The series h obtained in Theorem 4.1 has no zeros in $\mathbb{Z}_p$.*

Proof. By construction, $h = 1 + \sum_{n\geq 1} c_n X^n$ with $|c_n|_p < 1$ for all $n \geq 1$, and $h \in A_1$, so $c_n \to 0$. For any $z \in \mathbb{Z}_p$ we have $|z|_p \leq 1$, so $|c_n z^n|_p \leq |c_n|_p \to 0$, which guarantees convergence of $\sum_{n\geq 1} c_n z^n$. By the ultrametric inequality:

$$|h(z) - 1|_p = \left|\sum_{n\geq 1} c_n z^n\right|_p \leq \max_{n\geq 1} |c_n|_p < 1.$$

Hence $|h(z)|_p = |h(z) - 1 + 1|_p = 1 \neq 0$, so $h(z) \neq 0$. ∎

Theorem 5.2 (Strassmann)**.** Let $f \in A_1$ be nonzero. Then f has at most $s(f)$ zeros in $\mathbb{Z}_p$.

Proof. Let $N = s(f)$. By Theorem 4.1, $f = g \cdot h$ where $g \in \mathbb{Z}_p[X]$ has degree N and $h \in A_1$ has no zeros in $\mathbb{Z}_p$ (Lemma 5.1). Every zero of f in $\mathbb{Z}_p$ is therefore a root of g. Since g is a polynomial of degree N over the field $\mathbb{Q}_p$, it has at most N roots in $\mathbb{Q}_p$, and in particular at most N roots in $\mathbb{Z}_p$. Hence f has at most $s(f)$ zeros in $\mathbb{Z}_p$. ∎

References

[1] N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta-Functions*, Graduate Texts in Mathematics 58, Springer, Second Edition, 1984.

[2] A. M. Robert, *A Course in p-adic Analysis*, Graduate Texts in Mathematics 198, Springer, 2000.

Euler Circle, Mountain View, CA 94040
Email address: r.yaranga.almeida@gmail.com