ANALYSIS IN AN ALGEBRAICALLY CLOSED

NON-ARCHIMEDEAN FIELD

By

JOHN ELDON ATKINSON

Bachelor of Science
Kansas State Teachers College
Emporia, Kansas
1957

Master of Science
Kansas State Teachers College
Emporia, Kansas
1964

Submitted to the Faculty of the Graduate College
of the Oklahoma State University
in partial fulfillment of the requirements
for the Degree of
DOCTOR OF EDUCATION
July, 1972

ANALYSIS IN AN ALGEBRAICALLY CLOSED

NON-ARCHIMEDEAN FIELD

Thesis Approved:

Jeanne Agnew
Thesis Adviser

E. K. McLachlan

R. T. Alciatore

D B Aichele

D Durham
Dean of the Graduate College

ACKNOWLEDGMENTS

Foremost among those to whom gratitude is due is my thesis adviser, Dr. Jeanne Agnew. Her counsel and encouragement, not only during the preparation of this dissertation but throughout my graduate study at this institution, are greatly appreciated. I also wish to extend thanks to Dr. E. K. McLachlan for his interest in my progress and for his service as committee chairman. My thanks go also to Dr. Douglas Aichele and to Dr. Robert Alciatore for their efforts in my behalf as committee members.

Finally, to my wife Barbara and to my sons John and Keith, a very special thanks for their patience and encouragement during the past few years.

TABLE OF CONTENTS

LIST OF TABLES

Table | Page

LIST OF FIGURES

Figure | Page

CHAPTER I

INTRODUCTION

Among the topics encountered in real analysis are limits, continuous functions, differentiable functions, integrals, sequences, series and functions defined by power series. A discussion of any of the above relies heavily upon the absolute value function. The absolute value function is an example of a larger class of non-negative real valued functions called valuations.

<u>Definition</u> 1.1. Let F be a field and R be the real field. A mapping $\phi: F \to R$ is a <u>valuation on</u> $\underline{F}$ if and only if each of the following properties is satisfied:

i. $\phi(x) \geq 0$ for every $x \in F$;

ii. $\phi(x) = 0$ if and only if $x = 0$;

iii. $\phi(xy) = \phi(x)\phi(y)$;

iv. $\phi(x + y) \leq \phi(x) + \phi(y)$.

<u>Example</u> 1.2. (a) The absolute value function is a valuation on the field of rational numbers.

(b) The modulus function is a valuation on the complex field.

The following theorem is easily established from the definition of valuation.

<u>Theorem</u> 1.3. If ϕ is a valuation on the field F, then:

i. $\phi(1) = \phi(-1) = 1$;

ii. $\phi(-x) = \phi(x)$ for every $x \in F$;

iii. $\phi(x - y) \leq \phi(x) + \phi(y)$;

iv. $\phi\left(\frac{x}{y}\right) = \frac{\phi(x)}{\phi(y)}$ provided $\phi(y) \neq 0$.

Non-Archimedean Valuations

One property of the real number system with absolute value is that given any two non-zero numbers a and b, there is a positive integer n such that $|na| > |b|$. This property is called the Archimedean Property of the reals. In particular, for every positive integer $n > 1$, $|n| > 1$. It will be seen that not all valuations have this property.

<u>Definition</u> 1.4. Let ϕ be a valuation on field F. If, for every $n = 1 + 1 + \cdots + 1$, $\phi(n) \leq 1$, then ϕ is a <u>non-archimedean valuation</u> on F.

The following theorem provides a commonly used characterization of a non-archimedean valuation. The proof can be found in Snook [16].

<u>Theorem</u> 1.5. Let ϕ be a valuation on field F. Then ϕ is a non-archimedean valuation if and only if $\phi(a + b) \leq \max\{\phi(a),\phi(b)\}$ for any pair $a,b \in F$.

The property $\phi(a + b) \leq \max\{\phi(a),\phi(b)\}$ is called the <u>non-archimedean property</u>. It is clear that the non-archimedean property implies the triangle inequality $\phi(a + b) \leq \phi(a) + \phi(b)$. Usually, when the valuation is non-archimedean, property iv. of Definition 1.1 is replaced by the non-archimedean property.

<u>Theorem</u> 1.6. If ϕ is a non-archimedean valuation, then $\phi(x + y) = \max\{\phi(x),\phi(y)\}$ whenever $\phi(x) \neq \phi(y)$ [16, p. 54].

<u>Definition</u> 1.7. A field F with non-archimedean valuation ϕ is called a <u>non-archimedean field</u>.

Outline of Study

Since non-archimedean valuations and absolute value have similar properties, it is reasonable to consider concepts of analysis relative to a non-archimedean field. This type of study is presented in an expository paper by Palmer [14] entitled "Some Analysis in a Non-Archimedean Field."

The present study considers analysis in an algebraically closed extension of a non-archimedean field. It is accurate to consider this study as a sequel to Palmer's, and his work will be referenced frequently. Those results essential to the present study are listed as needed.

The background required for this study includes analysis through advanced calculus (complex variables would be helpful but not essential), algebra at the level of Herstein [9] and number theory as presented in Agnew [2].

In the remainder of this chapter a particular non-archimedean field called the p-adic numbers is discussed and some of Palmer's results relative to this field are listed. Also, some special topics to be utilized later are presented here. Chapter II pertains to continuous and differentiable functions. That chapter also includes a non-archimedean analogue of Weierstrass' Approximation Theorem of real analysis. In Chapter III, an algebraically closed extension of the p-adic numbers is considered. The major accomplishment of that chapter is the demonstration that the non-archimedean valuation extends to the algebraically closed field. In Chapter IV, power series are considered in some detail. A geometric device called Newton's polygon is developed and employed to determine the radius of convergence and to help locate the zeros of a power series. That chapter culminates with a non-archimedean form of Weierstrass' Factorization Theorem. The last chapter shows that by a suitably defined analogue of the complex line integral, analogues of several standard theorems of complex analysis can be established. Included are Cauchy's Integral Theorem, Cauchy's Integral Formula, the Maximum Modulus Principle and Liouville's Theorem.

The p-adic Number Field

The non-archimedean field upon which this study is based is called the field of p-adic numbers and is denoted by Q_p. Some of the important properties of Q_p are listed below. For a complete development, the reader is referred to Agnew [2].

(1) Each $\alpha \in Q_p$ can be uniquely expressed in the form

$$\alpha = p^k \sum_{n=0}^{\infty} a_n p^n$$

where $0 \leq a_n \leq p - 1$ for each $n = 0,1,2, \ldots,$ $a_0 \neq 0$ and k is a rational integer. This is called the canonical representation of α.

(2) The non-archimedean valuation on Q_p is denoted by $| \, |_p$ and $|\alpha|_p = \left(\frac{1}{p}\right)^k$ where α is given in the canonical representation above.

(3) The set $O_p = \{\alpha \in Q_p : |\alpha|_p \leq 1\}$ is the ring of p-adic integers. The units in O_p are those elements of O_p such that $|\alpha|_p = 1$.

(4) The field Q_p is complete with respect to the valuation $| \, |_p$.

(5) The field Q_p is a discrete field, that is, its value group given by $V_{Q_p} = \{|x|_p : x \in Q_p, \ x \neq 0\}$ is an infinite cyclic group with generator $1/p$.

The Ordinal Function

The remainder of this chapter is devoted to several special topics which will be utilized in later chapters. The first of these is a real valued function defined on an arbitrary non-archimedean field. There is no assumption that the field is discrete.

Definition 1.8. Let F be a field with non-archimedean valuation ϕ. The ordinal function is defined on F by

$$\operatorname{ord}(x) = \begin{cases} -\log_p \phi(x) & \text{if } x \neq 0 \\ \infty & \text{if } x = 0 \end{cases} .$$

For example, let $\alpha = p^k \epsilon$ where ϵ is a unit in Q_p. Since $|(p^k \epsilon)|_p = \left(\frac{1}{p}\right)^k$, then $\operatorname{ord} \alpha = -\log_p \left(\frac{1}{p}\right)^k = k$.

Theorem 1.9. If $x,y \in F$, then $\operatorname{ord} xy = \operatorname{ord} x + \operatorname{ord} y$.

Proof: This follows from

$$\text{ord } xy = -\log_p \phi(xy) = -[\log_p \phi(x) + \log_p \phi(y)]$$
$$= \text{ord } x + \text{ord } y.$$

Theorem 1.10. Suppose $x_n \neq 0$ for $n = 1,2, \ldots$. Then $\lim x_n = 0$ if and only if $\lim \text{ord } x_n = \infty$.

Proof: Suppose $\lim x_n = 0$. Then, given any $M > 0$ there exists an N such that $\phi(x_n) < p^{-M}$ whenever $n \geq N$. Thus, $\log_p \phi(x_n) < \log_p p^{-M} = -M$ so that $\text{ord } x_n > M$ whenever $n \geq N$. Conversely, suppose $\lim \text{ord } x_n = \infty$. Then, given any ϵ such that $1 > \epsilon > 0$, choose an M such that $p^{-M} \leq \epsilon$. There exists an N such that $\text{ord } x_n > M$ so that $-\log_p \phi(x_n) > -\log_p p^{-M} \geq -\log_p \epsilon$. It follows that $\phi(x_n) < \epsilon$ whenever $n \geq N$.

Theorem 1.11. If $x, y \in F$, then

$$\text{ord}(x + y) \geq \min\{\text{ord } x, \text{ord } y\}.$$

Proof: Since F is non-archimedean, $\phi(x + y) \leq \max\{\phi(x), \phi(y)\}$. It follows that $\log_p \phi(x + y) \leq \max\{\log_p \phi(x), \log_p \phi(y)\}$ so that

$$\text{ord}(x + y) = -\log_p \phi(x + y)$$
$$\geq \min\{-\log_p \phi(x), -\log_p \phi(y)\}$$
$$= \min\{\text{ord } x, \text{ord } y\}.$$

Corollary 1.12. If $\text{ord } x \neq \text{ord } y$ then $\text{ord}(x + y) = \min\{\text{ord } x, \text{ord } y\}$.

Proof: The proof follows from Theorem 1.11 and Theorem 1.6.

In later chapters there will be occasion to determine ord $n!$. Palmer [14] showed that

$$\operatorname{ord} n! = \frac{n - t_n}{p - 1}$$

where the canonical form of n is $n = a_0 + a_1 p + \cdots + a_k p^k$ and $t_n = a_0 + a_1 + \cdots + a_k$.

Example 1.13. Let $p = 5$ and $n = 87$. Since $87 = 2 + 2p + 3p^2$, then $t_{87} = 7$ and $\operatorname{ord} 87! = \frac{87 - 7}{5 - 1} = 20$.

Theorem 1.14. Let M and N be rational integers with $M \geq N$ and canonical representations given by $M = a_0 + a_1 p + \cdots + a_m p^m$ and $N = b_0 + b_1 p + \cdots + b_k p^k$. Then

$$\operatorname{ord} \binom{M}{N} = \sum_{i=0}^{m} \delta_i$$

where $\delta_{-1} = 0$ and for $i \geq 0$

$$\delta_i = \begin{cases} 1 & \text{if } a_i < b_i + \delta_{i-1}, \\ 0 & \text{if } a_i \geq b_i + \delta_{i-1}. \end{cases}$$

Proof: Let the canonical representation of $M - N$ be given by $M - N = c_0 + c_1 p + \cdots + c_m p^m$ where it is understood that some of the last c_i may be zero. It follows that

$$\sum_{i=0}^{j} c_i p^i \equiv \sum_{i=0}^{j} (a_i - b_i) p^i \bmod p^{j+1}$$

for $j = 0,1,2, \ldots, m$. Let $\delta_{-1} = 0$ and, for $i \geq 0$,

$$\delta_i = \begin{cases} 1 & \text{if } a_i < b_i + \delta_{i-1}, \\ 0 & \text{if } a_i \geq b_i + \delta_{i-1}. \end{cases}$$

Then for $i = 0,1,2, \ldots, m$, $c_i + b_i - a_i = \delta_i p - \delta_{i-1}$ so that

$$\begin{aligned} t_{M-N} + t_N - t_M &= \sum_{i=0}^{m} (\delta_i p - \delta_{i-1}) \\ &= (p - 1) \sum_{i=0}^{m} \delta_i + \delta_m. \end{aligned}$$

Since $\binom{M}{N} = \dfrac{M!}{N!(M - N)!}$ it follows that

$$\begin{aligned} \operatorname{ord} \binom{M}{N} &= \operatorname{ord} M! - \operatorname{ord} N! - \operatorname{ord}(M - N)! \\ &= \frac{M - t_M}{p - 1} - \frac{N - t_N}{p - 1} - \frac{(M - N) - t_{M-N}}{p - 1} \\ &= \frac{t_N + t_{M-N} - t_M}{p - 1}. \end{aligned}$$

Thus,

$$\operatorname{ord} \binom{M}{N} = \sum_{i=0}^{m} \delta_i + \frac{\delta_m}{p - 1}.$$

It remains to show that $\delta_m = 0$. If $M = N$, then $a_i = b_i$ for all i so that $\delta_m = 0$. If $M > N$, then there is a subscript r such that $a_r > b_r$ and $a_i \geq b_i$ for $r < i \leq m$. It follows that $\delta_m = 0$. This completes the proof of the theorem.

Example 1.15. Let $M = 212$, $N = 108$ and $p = 5$. Then $M = 2 + 2p + 3p^2 + 1p^3$ and $N = 3 + 1p + 4p^2$ so that

$$\sum_{i=0}^{3} \delta_i = 1 + 0 + 1 + 0 = 2.$$

Hence, $\operatorname{ord}\binom{212}{108} = 2$.

Example 1.16. Let $M = p^{k+j}$ and $N = p^k$. Then $\delta_i = 0$ for $0 \leq i < k$ and $\delta_i = 1$ for $k \leq i < k + j$ so that $\operatorname{ord}\binom{p^{k+j}}{p^k} = j$.

The next theorem shows that M can be replaced by any p-adic integer.

Theorem 1.17. Let $\alpha \in O_p$ and N be a rational integer with canonical representations given by

$$\alpha = \sum_{i=0}^{\infty} a_i p^i \quad \text{and} \quad N = \sum_{i=0}^{k} b_i p^i.$$

Then,

$$\operatorname{ord}\binom{\alpha}{N} = \sum_{i=0}^{\infty} \delta_i$$

where $\delta_{-1} = 0$ and for $i \geq 0$,

$$\delta_i = \begin{cases} 1 & \text{if } a_i < b_i + \delta_{i-1}, \\ 0 & \text{if } a_i \geq b_i + \delta_{i-1}. \end{cases}$$

Proof: Suppose the canonical representation of α is infinite. Since the canonical representation of N is finite, there exists a first non-zero coefficient of α beyond a_k, call it a_{k+j}. Let $M = a_0 + a_1 p + \cdots + a_k p^k + a_{k+j} p^{k+j}$. It will be shown that $\operatorname{ord}\binom{\alpha}{N} = \operatorname{ord}\binom{M}{N}$ and that

$$\operatorname{ord}\binom{M}{N} = \sum_{i=0}^{\infty} \delta_i .$$

To establish the first of these note that $\operatorname{ord}(\alpha - i) = \operatorname{ord}(M - i)$ for each $i = 0,1,2, \ldots, N-1$. Thus,

$$\operatorname{ord} \prod_{i=0}^{N-1} (\alpha - i) = \operatorname{ord} \prod_{i=0}^{N-1} (M - i)$$

so that $\operatorname{ord}\binom{\alpha}{N} = \operatorname{ord}\binom{M}{N}$.

To establish that

$$\operatorname{ord}\binom{M}{N} = \sum_{i=0}^{\infty} \delta_i ,$$

note that $\delta_i = 0$ for every $i \geq k + j$ so that

$$\sum_{i=0}^{\infty} \delta_i = \sum_{i=0}^{k+j-1} \delta_i = \operatorname{ord}\binom{M}{N}.$$

Now suppose α has a finite canonical representation. In this case α is a rational integer M. If $M \geq N$ then Theorem 1.14 applies. If $M < N$, then $\binom{M}{N} = 0$ and

$$\sum_{i=0}^{\infty} \delta_i = \infty = \text{ord } 0 = \text{ord}\left(\frac{M}{N}\right).$$

This completes the proof of Theorem 1.17.

Example 1.18. For $p = 5$ the canonical representation of $1/2$ is $3 + 2p + 2p^2 + \cdots + 2p^n + \cdots$. The following is a list of ordered pairs $\left(N, \text{ord}\left(\frac{1/2}{N}\right)\right)$ for

$N = 0,1,2, \ldots, 15$: (0,0), (1,0), (2,0), (3,0), (4,1), (5,0), (6,0), (7,0), (8,0), (9,1), (10,0), (11,0), (12,0), (13,0), (14,2), (15,1).

Elementary Symmetric Polynomials

The final remarks in this introductory chapter concern elementary symmetric polynomials. Suppose $f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$. Then $f(x) = x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} - \cdots + (-1)^n \sigma_n$ where

$$\sigma_1 = \alpha_1 + \alpha_2 + \cdots + \alpha_n,$$

$$\sigma_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \cdots + \alpha_1\alpha_n + \alpha_2\alpha_3 + \cdots + \alpha_{n-1}\alpha_n,$$

$$\vdots$$

$$\sigma_m = \sum \alpha_{i_1}\alpha_{i_2} \cdots \alpha_{i_m},$$

the sum taken over all possible combinations of subscripts, $1 \leq i_1 < i_2 < \cdots < i_m \leq n$. The polynomials $\sigma_1, \sigma_2, \ldots, \sigma_n$ are called the <u>elementary symmetric polynomials</u> for $\alpha_1, \alpha_2, \ldots, \alpha_n$. For example, if $n = 4$, then the symmetric polynomials are

$$\sigma_1 = \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4,$$

$$\sigma_2 = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_4,$$

$$\sigma_3 = \alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \alpha_1\alpha_3\alpha_4 + \alpha_2\alpha_3\alpha_4,$$

$$\sigma_4 = \alpha_1\alpha_2\alpha_3\alpha_4.$$

For each $k = 1,2, \ldots,$ let

$$s_k = \sum_{i=0}^{n} \alpha_i^k.$$

It can be shown that the following relationships hold: (See Van der Waerden, [17], p. 101.) If $1 \leq k \leq n$, then

$$s_k - s_{k-1}\sigma_1 + \cdots + (-1)^{k-1}s_1\sigma_{k-1} + (-1)^k k\sigma_k = 0$$

and if $k > n$ then

$$s_k - s_{k-1}\sigma_1 + \cdots + (-1)^n s_{k-n}\sigma_n = 0.$$

The importance of symmetric polynomials relative to this study concerns roots of unity. Suppose $\alpha_1, \alpha_2, \ldots, \alpha_n$ are the nth roots of unity in an algebraically closed field. Since

$$\begin{aligned} x^n - 1 &= (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n) \\ &= x^n - \sigma_1 x^{n-1} + \cdots + (-1)^n \sigma_n, \end{aligned}$$

Then, by equating coefficients, it follows that $\sigma_1 = \sigma_2 = \cdots = \sigma_{n-1} = 0$ and $\sigma_n = (-1)^{n+1}$. Therefore, for each k such that $1 \leq k < n$, $s_k = 0$, that is,

$$\sum_{i=1}^{n} \alpha_i^k = 0$$

for $k = 1,2, \ldots, n-1$. Also, since $s_n + (-1)^n n\sigma_n = 0$ and $\sigma_n = (-1)^{n+1}$, it follows that $s_n - n = 0$. Thus,

$$\sum_{i=1}^{n} \alpha_i^n = n.$$

Example 1.19. The four 4th roots of unity in the complex plane are 1, i, -1, $-i$. Then $s_1 = 1 + i + -1 + -i = 0$, $s_2 = 1 + -1 + 1 + -1 = 0$, $s_3 = 1 + -i + -1 + i = 0$ and $s_4 = 1 + 1 + 1 + 1 = 4$.

CHAPTER II

CONTINUOUS FUNCTIONS

This chapter begins with a summary of some results from Palmer [14] which are pertinent to later work. The chief contribution is the presentation of the p-adic counterparts of certain reals situations not discussed in Palmer. Henceforth, the p-adic valuation $| \, |_p$ will be denoted by $| \, |$.

<u>Definition</u> 2.1. Suppose $f: A \to B$ and α is a limit point of A. Then

$$\lim_{x \to \alpha} f(x) = \beta$$

if and only if for any $\epsilon > 0$, there is a $\delta > 0$ such that $|x - \alpha| \leq \delta$, $x \varepsilon A$ implies $|f(x) - \beta| < \epsilon$.

Whenever the limit exists, it must be unique.

The usual characterization of limit in terms of convergent sequences holds, that is,

$$\lim_{x \to \alpha} f(x) = \beta$$

if and only if for every sequence $\{\alpha_n\}$ in A converging to α with $\alpha_n \neq \alpha$,

$$\lim_{n \to \infty} f(\alpha_n) = \beta.$$

Theorem 2.2. Suppose $f: A \to B$ and α is a limit point of A. Then $\lim_{x \to \alpha} f(x)$ exists if and only if for any $\epsilon > 0$, there is a $\delta > 0$ such that $|x - y| \leq \delta$ implies $|f(x) - f(y)| < \epsilon$.

Definition 2.3. Let $f: A \to B$. The function is continuous at point $\alpha \in A$ if and only if

$$\lim_{x \to \alpha} f(x) = f(\alpha).$$

The function is continuous on the set A if and only if it is continuous at each point of A.

Theorem 2.4. If f and g are each continuous at point α then $f + g$ and fg are each continuous at α and f/g is continuous at α provided $g(\alpha) \neq 0$.

Theorem 2.5. If f is continuous at α and g is continuous at $f(\alpha)$, then the composition $g \circ f$ is continuous at α.

Definition 2.6. A sequence of functions $\{f_n\}$ defined on set A converges to a function f if and only if for each $x \in A$

$$\lim_{n \to \infty} f_n(x) = f(x).$$

The function f is called the limit function of the sequence $\{f_n\}$.

Definition 2.7. A sequence of functions $\{f_n\}$ defined on set A converges uniformly to a function f if and only if for any $\epsilon > 0$, there is an integer N such that $n \geq N$ implies $|f_n(x) - f(x)| < \epsilon$ for every $x \in A$.

Theorem 2.8. A sequence of functions $\{f_n\}$ defined on a set A converges uniformly to a function f if and only if for any $\epsilon > 0$ there is an integer N such that $n \geq N$ implies $|f_{n+1}(x) - f_n(x)| < \epsilon$ for each $x \in A$.

Theorem 2.9. Suppose $\{f_n\}$ converges uniformly to f on A. If for each n, f_n is continuous at α, then f is continuous at α.

Definition 2.10. Suppose $\{f_n\}$ is defined on A. The series $\sum f_n(x)$ converges to a limit function f defined on A if and only if

$$\lim_{N \to \infty} \sum_{n=1}^{N} f_n(x) = f(x)$$

for each $x \in A$.

Definition 2.11. A series $\sum f_n(x)$ converges uniformly to a limit function f if and only if

$$\left\{ \sum_{n=1}^{N} f_n(x) \right\}_{N=1}^{\infty}$$

converges uniformly to $f(x)$.

Theorem 2.12. The series $\sum f_n(x)$ converges uniformly on set A if and only if for every $\epsilon > 0$ there is an N such that $n \geq N$ implies $|f_n(x)| < \epsilon$ for every $x \in A$.

Theorem 2.13. Suppose $\sum f_n(x)$ converges uniformly to $f(x)$. If for each n, f_n is continuous at α, then f is continuous at α.

<u>Theorem</u> 2.14. Let $\{b_n\}$ be a sequence in Q_p such that $\lim b_n = 0$. If for each n, $|f_n(x)| \leq |b_n|$ for each $x \in A$, then $\sum f_n(x)$ converges uniformly on A.

Uniform Approximation

<u>Definition</u> 2.15. A set A in Q_p is <u>compact</u> if every open covering of A contains a finite subcovering.

<u>Theorem</u> 2.16. Let $K \subset Q_p$. Then K is <u>compact</u> if and only if K is closed and bounded. [16].

Since any two discs in Q_p are either disjoint or nested, it follows that every compact subset in Q_p can be partitioned into a finite number of pairwise disjoint subsets. This allows the following definition of a step function on a compact set in Q_p.

<u>Definition</u> 2.17. Let D be a disc in Q_p. A function f defined on D is a <u>step function on D</u> if and only if there is a partition of D by a finite collection of discs D_i such that, for each i, $i = 1,2, \ldots, n$, the function f is constant on D_i. If K is a compact set in Q_p, a function f is a <u>step function on K</u> if and only if there is a step function F on a disc D such that F is an extension of f. The collection of discs $\{D_1,D_2, \ldots, D_n\}$ is called the partition associated with the step function F.

Characteristic functions are often used to designate a step function. For example, if f is a step function on a disc D with the collection $\{D_1,D_2, \ldots, D_n\}$ as the associated partition, then

$$f(x) = \sum_{i=1}^{n} a_i \emptyset_i(x)$$

where a_i is the constant value of f on D_i and $\emptyset_i$ is the characteristic function of D_i.

<u>Definition</u> 2.18. Suppose $A \subset K$ and f is a function defined on A. If, given $\epsilon > 0$, there is a function F defined on K such that for every $x \in A$, $|F(x) - f(x)| < \epsilon$, then F is a <u>uniform approximation of f on A</u>. Equivalently, F uniformly approximates the function f on A.

The next theorem shows that a continuous function on a bounded set has a step function which approximates it uniformly.

<u>Theorem</u> 2.19. Let A be a subset of a compact set $K \subset Q_p$. If f is a continuous function defined on A, then there is a step function F defined on K such that F approximates f uniformly on A.

Proof: Since K is compact, there is a disc D containing K. If it is shown that there is a p-adic step function F defined on D such that F uniformly approximates f on A, then F restricted to K is the desired function. Thus, it suffices to assume in the beginning that K is a disc. Let $\epsilon > 0$ be chosen.

Since f is continuous on A and A is compact, there is a positive integer N such that $x,y \in A$ and $|x - y| < p^{-N}$ imply $|f(x) - f(y)| < \epsilon$. Furthermore, it may be assumed without loss of generality that p^{-N} is less than the radius of the disc K. Now K is partitioned by a finite number of discs of radius p^{-N}. Let

$D_1, \ldots, D_n$ denote the discs that have a non-empty intersection with A. The step function F is defined as follows:

For each $i = 1,2, \ldots, n$ pick $x_i \varepsilon D_i \cap A$. Then $F(x) = f(x_i)$ if $x \varepsilon D_i$, $i = 1,2, \ldots, n$ and $F(x) = 0$ if

$$x \varepsilon K \smallsetminus \bigcup_{i=1}^{n} D_i .$$

Since F is constant on each of a finite number of discs in a partition of K, F is a step function on K. By the way in which the discs are determined, $x \varepsilon A$ implies $|f(x) - F(x)| = |f(x) - f(x_i)|$ for some i such that x and x_i are in the same disc D_i of radius p^{-N}. Therefore, $|f(x) - F(x)| < \epsilon$ so that the step function F approximates the function f uniformly on the set A.

The above result is not essentially different from its real analysis counterpart, but the next result will display an interesting contrast. In the case of real step functions, the endpoints of the subintervals are generally points of discontinuity for the step function. The reason for this is that an endpoint is a point of accumulation of two distinct subintervals. In the p-adic situation, this does not occur since discs in Q_p are both open and closed.

Theorem 2.20. If A is a compact subset of Q_p and f is a step function on A, then f is continuous on A.

Proof: Pick $\epsilon > 0$. For any $x \varepsilon A$, the definition of step function implies there is a disc D such that $x \varepsilon D$ and f is constant on $D \cap A$. Suppose the radius of D is δ. Let y be any point of $D \cap A$. Then, since any point of D may be taken as its center, $|x - y| \leq \delta$. But $y,x \in D$ imply $|f(x) - f(y)| = 0 < \epsilon$ so that f is continuous on A.

An Extension Theorem

As stated earlier, a major objective is the proof of Weierstrass' Approximation Theorem. There are two more preliminary results to establish. The first is concerned with extending a continuous function to a larger compact set.

Theorem 2.21. Let K be a compact subset of Q_p and A be a closed subset of K. If f is a continuous p-adic function defined on A, then there is a continuous function F defined on K such that F extends f, that is, for every $x \in A$, $F(x) = f(x)$.

Proof: The proof will be accomplished by constructing a uniformly convergent sequence of continuous functions $\{f_n\}$ such that the limit function F extends f. In particular, each function f_n will be a step function that uniformly approximates f.

By Theorem 2.20, there is a step function f_1 defined on K such that $|f_1(x) - f(x)| < 1$ for every $x \in A$. According to the definition of step function, there is a finite collection of pairwise disjoint discs $\mathfrak{D}_0$ covering A and such that f_1 is constant on each member of $\mathfrak{D}_0$. For each $D \in \mathfrak{D}_0$ such that $D \cap A \neq \emptyset$, Theorem 2.20 again implies there is a step function g_1 defined on D such that $|g_1(x) - f(x)| < p^{-1}$ for every $x \in A$. Furthermore, it may be assumed that the norm of the partition of D associated with g_1 is not greater than the norm of $\mathfrak{D}_0$. (The norm of a partition by discs is the radius of the largest disc in the partition. It is denoted by $N(\mathfrak{D})$.)

Define f_2 on K as follows: Let $x \in K$. Since $\mathfrak{D}_0$ covers K, $x \in D$ for some $D \in \mathfrak{D}_0$. Then

$$f_2(x) = g_1(x) \quad \text{if} \quad D \cap A \neq \emptyset$$

and

$$f_2(x) = f_1(x) \quad \text{if} \quad D \cap A = \emptyset.$$

Since $|g_1(x) - f(x)| < p^{-1}$ and $f_2(x) = g_1(x)$ for each $x \in A$, it follows that $|f_2(x) - f(x)| < p^{-1}$ for every $x \in A$. Also, since the members of $\mathfrak{D}_0$ are pairwise disjoint and f_2 is defined to be constant on each member of a finite partition by discs of each member of $\mathfrak{D}_0$, it follows that f_2 is a step function on K. Let $\mathfrak{D}_1$ denote the partition associated with f_2. Then $N(\mathfrak{D}_1) \leq N(\mathfrak{D}_0)$.

Now suppose $f_1, \ldots, f_{n-1}$ have been defined so that for each i:

a) f_i is a step function on K such that $x \in A$ implies $|f_i(x) - f(x)| < p^{-i}$;

b) if $\mathfrak{D}_i$ denotes the partition of K associated with f_i, then $N(\mathfrak{D}_i) \leq N(\mathfrak{D}_{i-1})$.

Then for each $D \in \mathfrak{D}_{n-1}$ such that $D \cap A \neq \emptyset$, let g_n be a step function on D such that:

1) $|g_n(x) - f(x)| < p^{-n}$ for every $x \in A$; and

2) the norm of the partition of D associated with g is less than $N(\mathfrak{D}_{n-1})$.

Define f_n on K as follows: Let $x \in K$ so that $x \in D$ for some $D \in \mathfrak{D}_{n-1}$. Then

$$f_n(x) = g_n(x) \quad \text{if} \quad D \cap A \neq \emptyset$$

and

$$f_n(x) = f_{n-1}(x) \quad \text{if} \quad D \cap A = \emptyset.$$

Thus, f_n is a step function on K such that for each $x \in A$, $|f_n(x) - f(x)| = |g_n(x) - f(x)| < p^{-n}$ and $N(\mathfrak{D}_n) \leq N(\mathfrak{D}_{n-1})$.

Therefore, a sequence of step functions on K has been defined by induction. Each step function is continuous. It remains to show that f_n converges uniformly to an extension of f.

Two cases need to be considered. If $x \in A$, then

$$\begin{aligned} |f_n(x) - f_{n-1}(x)| &= |f_n(x) - f(x) + f(x) - f_{n-1}(x)| \\ &\leq \max\{|f_n(x) - f(x)|, |f(x) - f_{n-1}(x)|\} \\ &< p^{-(n-1)}. \end{aligned}$$

If $x \notin A$, then either $f_n(x) = f_{n-1}(x)$ or $x \in D_n$ where $D_n \in \mathfrak{D}_n$ and $D_n \cap A \neq \emptyset$. In the latter case, there is a disc $D_{n-1} \in \mathfrak{D}_{n-1}$ such that $D_n \subset D_{n-1}$. Let x_n be an element in $D_n \cap A$. Since $f_n(x)$ agrees with the step function $g_n(x)$ on D_n, $f_n(x) = g_n(x) = g_n(x_n)$. Similarly, $f_{n-1}(x) = g_{n-1}(x) = g_{n-1}(x_n)$. Then

$$\begin{aligned} |f_n(x) - f_{n-1}(x)| &= |f_n(x) - f(x_n) + f(x_n) - f_{n-1}(x)| \\ &= |g_n(x) - f(x_n) + f(x_n) - g_{n-1}(x)| \\ &= |g_n(x_n) - f(x_n) + f(x_n) - g_{n-1}(x_n)| \\ &\leq \max\{|g_n(x_n) - f(x_n)|, |f(x_n) - g_{n-1}(x_n)|\} \\ &< p^{-(n-1)} \quad \text{by the definition of } g_n \text{ and } g_{n-1}. \end{aligned}$$

Thus, it has been established that the sequence of step functions f_n is uniformly convergent on K. Let $F = \lim_{n \to \infty} f_n$. Since each step function f_n is continuous, F is continuous.

It remains to prove that F extends f. For any $\epsilon > 0$, there is an N such that $|f_n(x) - f(x)| < \epsilon$ and $|F(x) - f_n(x)| < \epsilon$ whenever $n \geq N$. Consider

$$\begin{aligned}|F(x) - f(x)| &= |F(x) - f_n(x) + f_n(x) - f(x)| \\ &\leq \max\{|F(x) - f_n(x)|, |f_n(x) - f(x)|\} \\ &< \epsilon.\end{aligned}$$

Since $|F(x) - f(x)| < \epsilon$ for every ϵ, $F(x) - f(x) = 0$ and the proof of Theorem 2.21 is complete.

Weierstrass' Approximation Theorem

Since Weierstrass' Theorem deals with the approximation of a function by a polynomial, it is reasonable that a polynomial with somewhat predictable behavior may be useful. The next lemma provides some information about the polynomial $h(x) = 1 - x^{p-1}$ which will be utilized in the proof of Weierstrass' Approximation Theorem.

Lemma 2.22. Suppose $h(x) = 1 - x^{p-1}$. Then

$$|(h(x))^{p^n}| = |x|^{(p-1)p^n} \quad \text{if} \quad |x| > 1,$$

$$|(h(x))^{p^n}| \leq p^{-p^n} \quad \text{if} \quad |x| = 1,$$

and

$$|(h(x))^{p^n} - 1| \leq p^{-n} \quad \text{if} \quad |x| < 1.$$

Proof: Suppose $|x| > 1$. Then

$$(h(x))^{p^n} = \left(1 - x^{p-1} \right)^{p^n}$$

$$= \sum_{k=0}^{p^n} \binom{p^n}{k} \left(-x^{p-1} \right)^k.$$

For each k, $0 \leq k < p^n$,

$$\left| \binom{p^n}{k} x^{(p-1)k} \right| \leq \left| x^{(p-1)k} \right| < \left| x^{(p-1)p^n} \right|.$$

Therefore, $|(h(x))^{p^n}| = |x^{(p-1)p^n}|$ whenever $|x| > 1$.

Suppose $|x| = 1$. Then $x = a_0 + a_1 p + \cdots$, with $a_0 \neq 0$. Thus, $x = a_0 + p\alpha$ where $\alpha \in O_p$ and $x^{p-1} = a_0^{p-1} + p\beta$ for some $\beta \in O_p$. Since $0 < a_0 < p$, by Fermat's Theorem, $a_0^{p-1} \equiv 1 \bmod p$. Combining this result with $x^{p-1} = a_0^{p-1} + p\beta$, it is seen that there is an $\eta \in O_p$ such that $h(x) = 1 - x^{p-1} = p\eta$. Thus, $(h(x))^{p^n} = p^{p^n}\eta'$ where $\eta' \in O_p$ so that $|(h(x))^{p^n}| \leq p^{-p^n}$ whenever $|x| = 1$.

Finally, suppose $|x| < 1$. Then $x = p\alpha$ for some $\alpha \in O_p$ so that $x^{p-1} = p^{p-1}\alpha^{p-1}$. This implies

$$\left(1 - x^{p-1} \right)^p = \sum_{k=0}^{p} \binom{p}{k} \left(-x^{p-1} \right)^k$$

$$= \sum_{k=0}^{p} \binom{p}{k} (-1)^k (p\alpha)^{k(p-1)}.$$

Since $\binom{p}{1} = p$, then $p^p | \binom{p}{k} p^{k(p-1)}$ for every $k = 1, 2, \ldots, p$.

Thus, $\left(1 - x^{p-1}\right)^p = 1 + p^p\beta$ for some $\beta \in O_p$ from which it follows that

$$(h(x))^{p^n} = \left(1 - x^{p-1}\right)^{p^n} = \left(1 + p^p\beta\right)^{p^{n-1}}$$

$$= \sum_{k=0}^{p^{n-1}} \binom{p^{n-1}}{k} p^{kp}\, \beta^k.$$

To complete the proof of $|(h(x))^{p^n} - 1| \le \frac{1}{p^n}$, it suffices to show that

$$p^n \,\Big|\, \binom{p^{n-1}}{k} p^{kp}$$

for each $k = 1, 2, \ldots, p^{n-1}$.

Suppose $p \neq k$. Then according to Theorem 1.14, $\operatorname{ord}\binom{p^{n-1}}{k} = n$. Thus, $p^n \,\Big|\, \binom{p^{n-1}}{k} p^{kp}$ whenever $p \neq k$.

Suppose $k = p^j m$ where $(m,p) = 1$ and $j > 0$. Then, by Theorem 1.14 again, $\operatorname{ord}\binom{p^{n-1}}{k} = n - j - 1$. Therefore, since $\operatorname{ord} p^{kp} = kp = mp^{j+1}$, then

$$\operatorname{ord}\binom{p^{n-1}}{k} p^{kp} = \operatorname{ord}\binom{p^{n-1}}{k} + \operatorname{ord} p^{kp} = n - j - 1 + mp^{j+1}.$$

Since $mp^{j+1} > j + 1$, it follows that $p^n \,\Big|\, \binom{p^{n-1}}{k} p^{kp}$ whenever $p \,|\, k$.

This completes the proof of Lemma 2.22.

<u>Theorem</u> 2.23. (Weierstrass' Approximation Theorem for the p-adic field Q_p) Let K be a compact subset of the p-adic field Q_p. If f is a

continuous function from K into Q_p, then, for any $\epsilon > 0$, there is a polynomial function g with coefficients in Q_p such that $|f(x) - g(x)| < \epsilon$ for every $x \in K$.

Proof: The proof will be accomplished by establishing each of the following:

1. The characteristic function of a disc in Q_p can be uniformly approximated by a polynomial.

2. The function f extends to a uniformly continuous function F on a disc containing the given compact set K.

3. The function F can be uniformly approximated by a polynomial.

Let α be in Q_p and let r and s be two rational integers such that $r < s$. Let $\emptyset$ be the characteristic function of the disc $D(\alpha,p^{-s})$. Since $r < s$, the disc $D(\alpha,p^{-s})$ is contained in the disc $D(\alpha,p^{-r})$. It will be shown by induction on the difference $s - r$ that the characteristic function $\emptyset$ on the smaller disc $D(\alpha,p^{-s})$ can be uniformly approximated on the larger disc by a polynomial.

Since the disc $D(\alpha,p^{-r})$ is the image under a translation of $D(0,p^{-r})$, assume $\alpha = 0$.

Suppose $s - r = 1$ and $\epsilon > 0$. For each $n > 0$ define a polynomial $g_n(x) = (h(p^{-r}x))^{p^n}$ where h is the polynomial defined in Lemma 2.22. It will be shown that for every $x \in D(0,p^{-r})$, $|\emptyset(x) - g_n(x)| \leq \frac{1}{p^n}$ so that, by choosing $n \geq -\log_p \epsilon$, the function $\emptyset$ is uniformly approximated on $D(0,p^{-r})$ by g_n.

If $x \in D(0,p^{-s})$ then $|x| \leq p^{-s} = p^{-(r+1)}$ so that $|p^{-r}x| < 1$. By Lemma 2.22, this implies $|\emptyset(x) - g_n(x)| = |1 - (h(p^{-r}x))^{p^n}| \leq \frac{1}{p^n}$.

If $x \in D(0,p^{-r}) \smallsetminus D(0,p^{-s})$, then $\emptyset(x) = 0$ and, since $s - r = 1$, $|x| = p^{r}$ so that $|p^{-r}x| = 1$. Therefore, $|\emptyset(x) - g_n(x)| = |g_n(x)| = |(h(p^{-r}x))^{p^n}| \leq \frac{1}{p^n}$.

This completes the first step of the induction since, for $s - r = 1$, the function $\emptyset$ is uniformly approximated on $D(0,p^{-r})$ by the polynomial g_n whenever n is such that $\frac{1}{p^n} < \epsilon$.

Now suppose $s - r = k$ and assume that for every pair of discs $D(0,p^{-r'})$ and $D(0,p^{-s'})$ with $0 < s' - r' < k$, the function defined to be identically 1 on $D(0,p^{-s'})$ and zero elsewhere can be uniformly approximated on $D(0,p^{-r})$ by a polynomial. It will be shown that the above assumption implies that the function $\emptyset$ which is 1 on $D(0,p^{-s})$ and 0 on $D(0,p^{-r}) \smallsetminus D(0,p^{-s})$ is uniformly approximated on the disc $D(0,p^{-r})$ by a polynomial.

Let ϵ be chosen such that $0 < \epsilon < 1$. Consider the discs $D(0,p^{-s})$ and $D(0,p^{-s+1})$. By assumption, there exists a polynomial h_1 such that for $x \in D(0,p^{-s})$, $|1 - h_1(x)| < \epsilon$ and for $x \in D(0,p^{-s+1}) \smallsetminus D(0,p^{-s})$, $|h_1(x)| < \epsilon$. Since the set $D(0,p^{-r}) \smallsetminus D(0,p^{-s+1})$ is closed and bounded, it is compact. Therefore, the polynomial function h_1 is bounded there so that there is a positive real number $M \geq 1$ such that $|h_1(x)| \leq M$ for every $x \in D(0,p^{-r}) \smallsetminus D(0,p^{-s+1})$. Again, by the inductive assumption, there is a polynomial h_2 such that for every $x \in D(0,p^{-s+1})$, $|1 - h_2(x)| < \frac{\epsilon}{M}$ and for every $x \in D(0,p^{-r}) \smallsetminus D(0,p^{-s+1})$, $|h_2(x)| < \frac{\epsilon}{M}$. Now consider the polynomial $g(x) = h_1(x)h_2(x)$. If $x \in D(0,p^{-s})$, write $g(x) = 1 - (1 - h_1(x)) - (1 - h_2(x)) + (1 - h_1(x))(1 - h_2(x))$ so that $|g(x) - 1| \leq \max\{|1 - h_1(x)|, |1 - h_2(x)|, |(1 - h_1(x))(1 - h_2(x))|\}$. Since $D(0,p^{-s}) \subset D(0,p^{-s+1})$, $\frac{\epsilon}{M} \leq \epsilon$ and $\epsilon^2 < \epsilon$, the above inequality implies $|g(x) - 1| < \epsilon$ for every $x \in D(0,p^{-s})$. If $x \in D(0,p^{-s+1}) \setminus D(0,p^{-s})$ write $g(x) = h_1(x) - h_1(x)(1 - h_2(x))$ so that $|g(x)| \leq \max\{|h_1(x)|, |h_1(x)(1 - h_2(x))|\}$. Again, since $\frac{\epsilon}{M} < \epsilon$, this implies $|g(x)| < \epsilon$.

Finally, if $x \in D(0,p^{-r}) \setminus D(0,p^{-s+1})$ then $|g(x)| = |h_1(x)h_2(x)| < M \cdot \frac{\epsilon}{M} = \epsilon$. This completes the proof by induction.

It follows from the above argument that for any $\alpha \in Q_p$ and any two discs $D(\alpha,p^{-s})$ and $D(\alpha,p^{-r})$, with $r < s$, the characteristic function of the smaller disc $D(\alpha,p^{-s})$ is uniformly approximated on the disc $D(\alpha,p^{-r})$ by some polynomial. Furthermore, since any point of a disc in Q_p may be taken as its center, if $\alpha \in D(0,p^{-r})$ and $s > r$, then $D(\alpha,p^{-s}) \subset D(0,p^{-r})$ and the characteristic function of $D(\alpha,p^{-s})$ is uniformly approximated on $D(0,p^{-r})$ by some polynomial.

From the hypothesis of Weierstrass' Theorem, f is a continuous function defined on a compact set K. Let $D(0,p^{-r})$ be a disc containing K. By Theorem 2.21, there is a function F defined on $D(0,p^{-r})$ such that F extends f, that is, $F(x) = f(x)$ for every $x \in K$, and, furthermore, F is uniformly continuous on $D(0,p^{-r})$. Thus, if $\epsilon > 0$ and $x \in D(0,p^{-r})$, then there is a disc $D(x,p^{-s})$ such that for every $y \in D(x,p^{-s})$, $|F(x) - F(y)| < \epsilon$. Now the collection of all such discs covers $D(0,p^{-r})$, and, since $D(0,p^{-r})$ is compact, there is a finite collection $\{D(x_1,p^{-s_1}), \ldots, D(x_n,p^{-s_n})\}$ covering $D(0,p^{-r})$. Furthermore, since any two discs in Q_p are either disjoint or nested, it may be assumed that the discs $D(x_1,p^{-s_1}), \ldots, D(x_n,p^{-s_n})$ are pairwise disjoint.

Since F extends f, the objective of uniformly approximating f on K will be accomplished when F is uniformly approximated on $D(0,p^{-r})$ by some polynomial g. Let $\emptyset_i$ denote the characteristic function of the disc $D(x_i,p^{-s_i})$ and g_i a polynomial that uniformly approximates $\emptyset_i$ on the disc $D(0,p^{-r})$. The candidate for g is given by

$$g(x) = \sum_{i=1}^{n} F(x_i)g_i(x).$$

In particular, let g_i be such that for every $x \in D(0,p^{-r})$, $|g_i(x) - \emptyset_i(x)| < \frac{\epsilon}{M}$ where M is an upper bound of $|F(x)|$ on the compact set $D(0,p^{-r})$. To prove that g uniformly approximates F on $D(0,p^{-r})$, suppose $x \in D(0,p^{-r})$. Then,

$$\begin{aligned}\left|F(x) - g(x)\right| &= \left|\sum_{i=1}^{n} \emptyset_i(x)F(x) - \sum_{i=1}^{n} F(x_i)g_i(x)\right| \\ &= \left|\sum_{i=1}^{n} (\emptyset_i(x)F(x) - F(x_i)g_i(x))\right| \\ &\leq \max_i \{|\emptyset_i(x)F(x) - F(x_i)g_i(x)|\}.\end{aligned}$$

Now,

$$\begin{aligned}&|\emptyset_i(x)F(x) - F(x_i)g_i(x)| \\ &\qquad = |\emptyset_i(x)F(x) - \emptyset_i(x)F(x_i) + \emptyset_i(x)F(x_i) - F(x_i)g_i(x)| \\ &\qquad \leq \max\{|\emptyset_i(x)(F(x) - F(x_i))|, |F(x_i)(\emptyset_i(x) - g_i(x))|\}.\end{aligned}$$

By the way in which the discs $D(x_i,p^{-s_i})$ were chosen and the fact that $\emptyset_i$ is the characteristic function on $D(x_i, p^{-s_i})$, it follows that $|\emptyset_i(x)(F(x) - F(x_i))| < \epsilon$ for every $x \in D(0,p^{-r})$. Also, since g_i uniformly approximates $\emptyset_i$,

$$|F(x_i)(\emptyset_i(x) - g_i(x))| = |F(x_i)||\emptyset_i(x) - g_i(x)| < M \cdot \frac{\epsilon}{M} = \epsilon .$$

Thus, for each $i = 1,2, \ldots, n$, $|\emptyset_i(x)F(x) - F(x_i)g_i(x)| < \epsilon$ for every $x \in D(0,p^{-r})$. This implies $|F(x) - g(x)| < \epsilon$ for every $x \in D(0,p^{-r})$ so that the polynomial g uniformly approximates the function F on the disc $D(0,p^{-r})$ which in turn implies that the given function f is uniformly approximated by a polynomial. This completes the proof of Weierstrass' Approximation Theorem.

Differentiable p-adic Functions

Since the concept of differentiation stems from the definition of limit and since the basic properties of limits are unaffected by the non-archimedean property, it is not surprising that a great many of the definitions and theorems relating to derivatives carry over unchanged from elementary calculus. Some of these are listed below.

Definition 2.24. Let $f: A \to B$. The function f is differentiable at α if and only if $\lim_{x \to \alpha} \frac{f(x) - f(\alpha)}{x - \alpha}$ exists. If the limit exists, it is denoted by $f'(\alpha)$ and is called the derivative of f at α. If $f'(\alpha)$ exists for every $\alpha \in A$, then f is differentiable on A.

Theorem 2.25. If f is differentiable at α then f is continuous at α.

Theorem 2.26. Let f and g be differentiable at α. Then:

1. $(f + g)'(\alpha) = f'(\alpha) + g'(\alpha)$;

2. $(fg)'(\alpha) = f(\alpha)g'(\alpha) + g(\alpha)f'(\alpha)$;

3. $\dfrac{f(\alpha)}{g(\alpha)} = \dfrac{g(\alpha)f'(\alpha) - f(\alpha)g'(\alpha)}{g(\alpha)^2}$, provided $g(\alpha) \neq 0$; and

4. $(f \circ g)'(\alpha) = f'(g(\alpha))g'(\alpha)$, provided f is differentiable at $g(\alpha)$.

A particularly well-behaved class of functions are those represented by power series. Palmer [14] shows that a power series $\sum b_n(x - a)^n$ converges for all x such that

$$|x - a| < \rho = \frac{1}{\overline{\lim} \sqrt[n]{|b_n|}} .$$

The real number ρ is called the radius of convergence of the given power series where it is understood that $\rho = 0$ if $\overline{\lim} \sqrt[n]{|b_n|} = \infty$ and $\rho = \infty$ if $\overline{\lim} \sqrt[n]{|b_n|} = 0$.

Definition 2.27. A function f defined by

$$f(x) = \sum_{n=0}^{\infty} b_n(x - a)^n$$

is an analytic function.

Theorem 2.28. Suppose

$$f(x) = \sum_{n=0}^{\infty} b_n(x - a)^n$$

has a non-zero radius of convergence ρ. Then each of the following is true:

1. $f(x)$ is continuous at each x such that $|x - a| < \rho$.

2. The series $\sum b_n(x - a)^n$ converges uniformly for each x such that $|x - a| \leq t < \rho$.

3. The derived series $\sum nb_n(x - a)^{n-1}$ converges for $|x - a| < \rho$.

4. If $|x - a| < \rho$, then $f'(x) = \lim_{h \to 0} \frac{f(x + h) - f(x)}{h}$ exists and is given by the derived series.

5. The usual rules of differentiation hold for sums, products, quotients, and compositions of analytic functions.

6. For each n, $b_n = \frac{f^{(n)}(a)}{n!}$.

7. If f and g are both analytic in $D(a,r)$ with $f'(x) = g'(x)$ for x in $D(a,r)$ then there is a constant c such that $f(x) = g(x) + c$ for each x in $D(a,r)$.

Proof: Proofs are given by Palmer for an arbitrary non-archimedean field in [14].

Several analytic functions discussed by Palmer will be referred to in later chapters. For reference, some of these are listed in the following table.

TABLE I

ANALYTIC FUNCTIONS

Name	Representation	ρ
Geometric	$(1 - x)^{-1} = \sum_{n=0}^{\infty} x^n$	1
Binomial	$(1 + x)^{\alpha} = \sum_{n=0}^{\infty} \binom{\alpha}{n} x^n, \quad \alpha \in 0_p$	$\geq p^{-1/(p-1)}$
Logarithm	$\log(1 + x) = \sum_{n=1}^{\infty} \frac{(-1)^{n-1} x^n}{n}$	1
Exponential	$\exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!}$	$p^{-1/(p-1)}$

In real analysis, two functions whose derivatives are the same function must differ by a constant. While Theorem 2.26 shows that this property holds for analytic p-adic functions, it does not hold for all pairs of differentiable p-adic functions. In the following example, a function is given which is not constant on any disc and yet its derivative is zero everywhere.

Example 2.29. Let $x \in 0_p$ have the canonical representation $x = a_0 + a_1 p + \cdots + a_n p^n + \cdots$. Define $f: 0_p \to 0_p$ by $f(x) = a_0 + a_1 p^2 + \cdots + a_n p^{2n} + \cdots$.

By uniqueness of the canonical representation of a p-adic integer, it follows that f is one-to-one so that f is not the constant function on any disc. To see that f has a derivative equal to zero everywhere, suppose $x, y \varepsilon 0_p$ such that $|x - y| = p^{-N}$. Then the first N coefficients of the canonical representations for x and y must agree. It follows that $|f(x) - f(y)| = p^{-2N}$. Therefore, $\left|\frac{f(x) - f(y)}{x - y}\right| = p^{-N}$ so that $\lim_{y \to x} \left|\frac{f(x) - f(y)}{x - y}\right| = 0$ for every $x \varepsilon 0_p$.

This chapter will be concluded with an example of a p-adic function which is continuous everywhere in 0_p but is nowhere differentiable.

Example 2.30. For each $x \varepsilon 0_p$, define $f(x)$ by $f(x) = a_0^2 + a_1^2 p + \cdots + a_n^2 p^n + \cdots$ where $x = a_0 + a_1 p + \cdots + a_n p^n + \cdots$ is the canonical representation.

Since $|a_n| \leq 1$, it follows that $\lim a_n^2 p^n = 0$ so that the function f is well defined. To see that f is continuous at $\alpha \varepsilon 0_p$, let $\epsilon > 0$ be chosen and pick N such that $p^{-N} < \epsilon$. Then for any $h = p^N \beta$ where $\beta \varepsilon 0_p$, it follows that

$$f(\alpha + h) = a_0^2 + a_1^2 p + \cdots + a_{N-1}^2 p^{N-1} + (a_N + b_0)^2 p^N$$
$$+ \cdots + (a_{N+k} + b_k)^2 p^{N+k} + \cdots$$

so that $|f(\alpha + h) - f(\alpha)| \leq p^{-N} < \epsilon$. Therefore, f is continuous at α.

To prove that f is not differentiable anywhere in 0_p, suppose to the contrary that $f'(\alpha)$ exists for some $\alpha \varepsilon 0_p$. Then for any ϵ such that $1 > \epsilon > 0$, there is a δ such that whenever $|h| < \delta$, $\left|\frac{f(\alpha + h) - f(\alpha)}{h} - f'(\alpha)\right| < \epsilon$.

Pick N such that $p^{-N} < \delta$. If $p \neq 2$ then there exist two rational integers k_1 and k_2 such that $k_1 \neq k_2$, neither k_1 nor k_2 equals a_N, and $0 \leq k_i < p$ for $i = 1,2$. Let $h_1 = (k_1 - a_N)p^N$ and $h_2 = (k_2 - a_N)p^N$ so that

$$x + h_i = a_0 + a_1 p + \cdots + a_{N-1} p^{N-1} + k_i p^N + a_{N+1} p^{N+1} + \cdots$$

for $i = 1,2$. It follows that

$$\frac{f(\alpha + h_i) - f(\alpha)}{h_i} = \frac{(k_i^2 - a_N^2)p^N}{(k_i - a_N)p^N} = k_i + a_N,$$

$i = 1,2$. Hence,

$$\begin{aligned} 1 &= |k_1 - k_2| = |(k_1 + a_N) - (k_2 + a_N)| \\ &= \left|\frac{f(\alpha + h_1) - f(\alpha)}{h_1} - \frac{f(\alpha + h_2) - f(\alpha)}{h_2}\right| \\ &\leq \max\left\{\left|\frac{f(\alpha + h_1) - f(\alpha)}{h_1}\right|, \left|\frac{f(\alpha + h_2) - f(\alpha)}{h_2}\right|\right\} \\ &< \epsilon. \end{aligned}$$

This is a contradiction since $\epsilon < 1$. It follows that f is not differentiable at any point of 0_p.

CHAPTER III

AN ALGEBRAICALLY CLOSED NON-ARCHIMEDEAN FIELD

In previous chapters the p-adic field Q_p has been the major focus of attention. Comparisons with the real field R have shown that Q_p and R have many similarities as well as many interesting contrasts. In this chapter the analogies will be carried further. In particular, since the real field is embedded in the complex field C, it is natural to seek a field in which Q_p is embedded and which may have properties analogous to those of C. This chapter is devoted to the development of such a field.

The following plan will be adopted. Since any field has an extension field in which every polynomial has a root, there is a field C_p extending the p-adic field Q_p such that every polynomial over C_p has a root in C_p. It will be shown that the non-archimedean valuation on Q_p extends to C_p. Finally, it will be established that if necessary, the field C_p can be completed to form a complete non-archimedean valuated field T_p in which every polynomial has a root.

Extension Fields

Some concepts related to field extensions are needed.

Definition 3.1. A field K is an extension field of field k if k is isomorphic to a subfield of K. (Henceforth, k will be identified with its isomorphic copy in K.) An extension field K is an <u>algebraic extension</u> of k if every element of K is algebraic over k, that is, every element of K is a root of some polynomial $f(x) \in F[x]$.

<u>Definition</u> 3.2. A field K is <u>algebraically closed</u> if every non-constant polynomial in $K[x]$ has at least one root in K. If K is an algebraically closed algebraic extension of field k, then K is an <u>algebraic closure</u> of k.

<u>Example</u> 3.3. The complex field C is an algebraic closure of the real field R.

To see this, recall the Fundamental Theorem of Algebra which states that every non-constant polynomial in $C[x]$ has at least one root in C. Also, since the real field is isomorphic to a subfield of C, the complex field is an extension field of the real field R. Finally, given any $\alpha = a + bi \in C$, α is a root of $x^2 - 2ax + a^2 + b^2 \in R[x]$. It follows that C is an algebraic closure of R.

The above example provides motivation to seek an algebraic closure of the p-adic field Q_p.

One of the standard results in a first year course in Abstract Algebra is that, given any irreducible polynomial $g(x) \in k[x]$, there is an algebraic extension K of k such that $g(x)$ has a root in K. The field K is called a <u>simple algebraic extension</u> of k. This process can be repeated until an extension K' of k is obtained such that all roots of the original polynomial $g(x)$ are contained in K'. In fact, by using arguments involving Zorn's Lemma or one of its equivalent forms, it can be shown that given any field k, there exists an algebraic extension of k which contains all roots of all polynomials in $k[x]$. That is, any field has an algebraic closure. For a proof using Transfinite Induction, the reader is referred to Vander der Waerden [17].

The next several theorems are essentially those found in McCarthy [12], pages 84-87. For brevity, some will be stated without proof. The first of these shows that any algebraic extension of Q_p contains a subring having at least some of the properties anticipated for a ring of integers in a valuated field.

Theorem 3.4. Let K be an extension field of a non-archimedean field k. Then there is a subring $\mathfrak{D}$ of K such that

i. $\mathfrak{D}$ contains the ring of integers of k.

ii. $\mathfrak{D} \neq K$.

iii. If $a \in K$ then either $a \in \mathfrak{D}$ or $a^{-1} \in \mathfrak{D}$.

Since $\mathfrak{D}$ is a subring of K containing the integers of k, $\mathfrak{D}$ contains 1. But, $\mathfrak{D} \neq K$ so that $\mathfrak{D}$ has both units and non-units. Let $\mathfrak{P}$ be the set of non-units in $\mathfrak{D}$, that is

$$\mathfrak{P} = \{a \in \mathfrak{D}: \; a^{-1} \notin \mathfrak{D}\}.$$

It can be shown that $\mathfrak{P}$ is an ideal of $\mathfrak{D}$.

Let K^* denote the group of non-zero elements of K and let U_K denote the group of units in $\mathfrak{D}$. Since U_K is a subgroup of K^*, it makes sense to consider the quotient group K^*/U_K. Similarly, consider k^*/U_k. Now the mapping $h\colon k^*/U_k \to K^*/U_K$ defined by

$$h(aU_K) = aU_K$$

is a homomorphism. Also, since $h(aU_k) \varepsilon U_K$ if and only if $a \varepsilon U_k$, h is an isomorphism. Thus, k^*/U_k may be considered as a subgroup of K^*/U_K.

Let $V_k = \{|x|_k : x \varepsilon k^*, \ ||_k$ the valuation$\}$. The set V_k is called the <u>value group</u> of k. The valuation $||_k$ is a homomorphism and V_k is a multiplicative subgroup of the positive reals. Since the kernel of $||_k$ is the group of units U_k, there is an isomorphism ϕ from the quotient group k^*/U_k onto the group V_k such that $\phi(aU_k) = |a|_k$.

<u>Definition</u> 3.5. An abelian group G is an <u>ordered abelian group</u> if there is a linear order $<$ defined on G such that for a, b, and c in G, if $a < b$ then $ac < bc$.

Since V_k is a subgroup of the positive reals, V_k is an ordered abelian group. The next definition provides a linear ordering on the quotient group k^*/U_k so that it will be an ordered abelian group.

<u>Definition</u> 3.6. Let aU_k and bU_k be elements of k^*/U_k. Define $aU_k < bU_k$ if and only if ab^{-1} is an integer in k.

<u>Theorem</u> 3.7. The quotient group k^*/U_k is an ordered abelian group with respect to the linear ordering $<$.

Proof: First it will be shown that the relation $<$ is a linear ordering of k^*/U_k. Suppose $aU_k < bU_k$ and $bU_k < cU_k$. Then $ab^{-1} \varepsilon \mathfrak{G}$ and $bc^{-1} \varepsilon \mathfrak{G}$ where $\mathfrak{G}$ denotes the set of integers in k. Then $ac^{-1} = (ab^{-1})(bc^{-1}) \varepsilon \mathfrak{G}$ so that $aU_k < cU_k$. Next suppose $aU_k < bU_k$ and $bU_k < cU_k$. Then $ab^{-1} \varepsilon \mathfrak{G}$ and $ba^{-1} \varepsilon \mathfrak{G}$ and, since

$(ab^{-1})^{-1} = ba^{-1}$, $ab^{-1} \varepsilon U_k$. Thus, $aU_k = bU_k$. Finally, suppose $aU_k \neq bU_k$ so that $ab^{-1} \notin U_k$. Since either $ab^{-1} \varepsilon \mathfrak{G}$ or $ba^{-1} \varepsilon \mathfrak{G}$, then either $aU_k < bU_k$ or $bU_k < aU_k$. Therefore, k^*/U_k is linearly ordered by $<$.

To complete the proof, suppose aU_k, bU_k and cU_k are elements in k^*/U_k with $aU_k < bU_k$. Then $ab^{-1} \varepsilon \mathfrak{G}$ so that $ac(bc)^{-1} \varepsilon \mathfrak{G}$. Thus, $acU_k < bcU_k$. This establishes that k^*/U_k is an ordered abelian group.

Next, an ordering on K^*/U_K will be defined such that, when restricted to k^*/U_k, the ordering coincides with that given in Definition 3.6. Anticipating this, the same symbol will be used.

Definition 3.8. Let aU_K and bU_K be elements in K^*/U_K. Then $aU_K < bU_K$ if and only if $ab^{-1} \varepsilon \mathfrak{D}$.

Theorem 3.9. The quotient group K^*/U_K is an ordered abelian group with respect to the linear ordering $<$.

Proof: The proof is identical with the proof of Theorem 3.7 with $\mathfrak{G}$ replaced by $\mathfrak{D}$.

Recall that the present objective is to prove that the non-archimedean valuation on k extends to an arbitrary extension field K. There are still a few preliminary results which must be established. An isomorphism ϕ from one ordered abelian group to another is order preserving if $\phi(a) < \phi(b)$ whenever $a < b$. The next theorem states that under suitable conditions, an order preserving isomorphism defined on a subgroup extends to the group.

Theorem 3.10. Let G be an ordered abelian group and H be a subgroup of G such that:

i. there is an order preserving isomorphism ϕ from H into the multiplicative group of positive reals, R^+, and

ii. for each $a \in G$, there is a positive integer n such that $a^n \in H$.

Then there is an order preserving isomorphism ψ from G into R^+ such that $\psi(a) = \phi(a)$ for every $a \in H$.

Proof: See McCarthy, page 86.

The following lemma and its corollary are used in the proof of the major result of this section.

Lemma 3.11. Let K be an algebraic extension of a non-archimedean field k. For a, b and c in K^* with $a + b \neq 0$, if $aU_K < bU_K$ then $(a + b)U_K < bU_K$. Furthermore, if $aU_K \neq bU_K$ then $(a + b)U_K = bU_K$.

Proof: If $aU_K < bU_K$, then $ab^{-1} \in \mathfrak{D}$ so that $ab^{-1} + 1 \in \mathfrak{D}$. Then, since $(a + b)b^{-1} = ab^{-1} + 1$, $(a + b)b^{-1} \in \mathfrak{D}$ and it follows that $(a + b)U_K < bU_K$. In particular,

$$[(a + b) - a]U_K < (-a)U_K = aU_K$$

and

$$[(a + b) - a]U_K < (a + b)U_K.$$

Now suppose $bU_K \neq aU_K$. Since $bU_K = [(a + b) - a]U_K$, there are two cases to consider. In one case, $(a + b)U_K < aU_K$. But then

$bU_K = [(a + b) - a]U_K < aU_K < bU_K$ which implies $aU_K = bU_K$. Since this is contrary to the hypothesis, the other case must hold, namely, $aU_K < (a + b)U_K$. Thus, $bU_K = [(a + b) - a]U_K < (a + b)U_K$. Since also $(a + b)U_K < bU_K$, the lemma is established.

Corollary 3.12. Let $a_1, a_2, \ldots, a_n \in K^*$ be such that $a_1 + a_2 + \cdots + a_n \neq 0$ and $a_2 + \cdots + a_n \neq 0$. If $a_i U_K < a_1 U_K$ and $a_i U_K \neq a_1 U_K$ for $i = 2, 3, \ldots, n$, then $(a_1 + \cdots + a_n)U_K = a_1 U_K$.

Proof: Lemma 3.11 establishes this result for $n = 2$. Suppose it holds for $n = j$, $j \geq 2$. Then

$$(a_1 + \cdots + a_j + a_{j+1})U_K = ((a_1 + \cdots + a_j) + a_{j+1})U_K.$$

By the induction hypothesis, $(a_1 + \cdots + a_j)U_K = a_1 U_K$ and $a_{j+1}U_K < a_1 U_K \neq a_{j+1}U_K$. It follows from Lemma 3.11 that $(a_1 + \cdots + a_j + a_{j+1})U_K = a_1 U_K$.

Extension of the Valuation

Finally, the major objective of this section can be realized. The next theorem shows that the non-archimedean valuation defined on Q_p extends to any algebraic extension of Q_p. In particular, it extends to the algebraic closure C_p.

Theorem 3.13. Let k be a non-archimedean field with valuation $|\,|_k$ and let K be any algebraic extension of k. Then there is a non-archimedean valuation $|\,|_K$ on K such that $|a|_K = |a|_k$ for every $a \in k$.

Proof: The proof will utilize Theorem 3.10. It will be shown that the quotient groups K^*/U_K and k^*/U_k satisfy the hypotheses of that theorem. First, it must be shown that there is an order preserving isomorphism from k^*/U_k into R^+. Recall the isomorphism ϕ given by $\phi(aU_k) = |a|_k$ where $||_k$ is the valuation on k. Suppose $aU_k < bU_k$, then ab^{-1} is an integer in k so that $|ab^{-1}|_k \leq 1$ and, therefore, $|a|_k \leq |b|_k$. Thus, $\phi(aU_k) \leq \phi(bU_k)$ whenever $aU_k < bU_k$ so that ϕ is an order preserving isomorphism.

Next, it must be shown that given any $aU_K \in K^*/U_K$, there is a positive integer m such that $(aU_K)^m \in k^*/U_k$. In view of the identification of k^*/U_k in K^*/U_K, it suffices to show that $a^m \in k^*$. To this end, let $aU_K \in K^*/U_K$. Since $a \in K^*$ and K is an algebraic extension of k, a is a root of some polynomial in $k[x]$. Let $g(x)$ be the minimal polynomial of a, that is, $g(x)$ is the monic, irreducible polynomial of least degree such that $g(a) = 0$. Suppose

$$g(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1} + c_nx^n$$

so that $c_0 \neq 0$ and $c_n = 1$.

There are two cases to consider. In one case, there may be two integers i and j with $0 \leq i < j \leq n$ such that $c_i \neq 0$, $c_j \neq 0$ and $c_ia^iU_K = c_ja^jU_K$. Then $c_ia^i(c_ja^j)^{-1} \in U_K$ so that $c_ic_j^{-1}a^{i-j} \in U_K$ and, hence, $c_ic_j^{-1}U_K = a^{j-i}U_K$. Since $c_ic_j^{-1}U_K \in k^*/U_k$, it follows that $(aU_K)^{j-i} \in k^*/U_k$. In the other case, for each choice of i and j, $c_ia^iU_K \neq c_ja^jU_K$. Then, since K^*/U_K is linearly ordered by $<$, there is a positive integer q such that $c_ia^iU_K < c_qa^qU_K$ for $1 \leq i \leq n$, $i \neq q$. Also, $c_1a + \cdots + c_na^n = -c_0 \neq 0$ so that

$(c_1a + \cdots + c_na^n)U_K = (-c_0)U_K$. Since $g(x)$ is the minimal polynomial of a,

$$\sum_{\substack{i=1\\ i\neq q}}^{n} c_i a^i \neq 0.$$

Thus, by Corollary 3.12 $(c_1a + \cdots + c_na^n)U_K = c_qa^qU_K$ so that $c_qa^qU_K = (-c_0)U_K$. Then

$$(aU_K)^q = a^qU_K = (-c_0c_q^{-1})U_K \in k^*/U_k.$$

Therefore, for any $aU_K \in K^*/U_K$, there is a positive integer m such that $(aU_K)^m \in k^*/U_k$.

Since the hypotheses of Theorem 3.10 are satisfied, there is an order preserving isomorphism ψ from K^*/U_K into R^+ such that $\psi(aU_K) = |a|_k$ for every $a \in k$. Define a mapping $|\,|_K$ from K into the reals R as follows:

$$|a|_K = \psi(aU_K) \quad \text{if} \quad a \neq 0$$

$$|a|_K = 0 \quad \text{if} \quad a = 0.$$

It will be shown that $|\,|_K$ is a non-archimedean valuation on K.

Certainly $|a|_K \geq 0$ and $|a|_K = 0$ only if $a = 0$. It remains to be shown that $|ab|_K = |a|_K|b|_K$ and that $|a + b|_K \leq \max\{|a|_K, |b|_K\}$ for every $a,b \in K$. Suppose one of a or b is zero. Then $|ab|_K = 0 = |a|_K|b|_K$ and $|a + b|_K = \max\{|a|_K, |b|_K\}$. Now suppose neither a nor b is zero. Then

$$|ab|_K = \psi(abU_K) = \psi[(aU_K)(bU_K)]$$
$$= \psi(aU_K)\psi(bU_K) = |a|_K|b|_K.$$

Thus, in all cases, $|ab|_K = |a|_K|b|_K$ whenever a and b are in K.

Now suppose neither a nor b is zero but $a + b = 0$. Then $|a + b|_K < \max\{|a|_K, |a|_K\}$. Finally, assume $a + b \neq 0$ and, without loss of generality, $|a|_K \leq |b|_K$. Then, since ψ is order preserving, $aU_K < bU_K$. By Lemma 3.12, $(a + b)U_K < bU_K$ so that $\psi[(a + b)U_K] \leq \psi(bU_K)$ and, hence, $|a + b|_K \leq |b|_K = \max\{|a|_K, |b|_K\}$. Thus, it has been established that $||_K$ is a non-archimedean valuation on the algebraic extension field K of k. And, since $|a|_K = |a|_k$ whenever $a \in k$, the theorem is proved.

Although Theorem 3.13 establishes the existence of an extension of a non-archimedean valuation to an arbitrary algebraic extension, it does not settle the question of uniqueness. Palmer [14] included results which state that in the case of a finite algebraic extension of a complete non-archimedean field, the extension of the valuation is unique.

These results are stated in the next theorem.

Theorem 3.14. If k is a complete non-archimedean field with valuation $||_k$ and if K is a finite algebraic extension of k, then there is a unique extension of $||_k$ to a non-archimedean valuation $||_K$ on K. Furthermore, K is complete with respect to $||_K$.

Proof: See Palmer, pp. 126-129.

Under similar hypotheses, the question of uniqueness of the valuation on an algebraic closure is settled by the next theorem.

Theorem 3.15. Let k be a complete non-archimedean field. If K is an algebraic closure of k, then the extension of the valuation $||_k$ on k to a valuation on K is unique.

Proof: Suppose $||_1$ and $||_2$ are distinct extensions of $||_k$. Then there is an element $a \varepsilon K$ such that $|a|_1 \neq |a|_2$. Let k' be a finite algebraic extension of k containing a. Since k' is a subfield of K, the valuations $||_1$ and $||_2$, restricted to k', are distinct non-archimedean valuations on a finite extension of k. But, according to Theorem 3.14, this is impossible. Thus, the extension of a valuation to an algebraic closure of k is unique.

Completion of the Algebraic Closure

Now it may happen that an algebraic closure is not complete with respect to the unique valuation extending $||_k$. However, any problems created by this can be resolved if it can be shown that the completion of an algebraic closure is algebraically closed. This is the final objective of this chapter.

Lemma 3.16. Let k be a complete non-archimedean field. Then the mapping $\phi: k[x] \to R$ defined by

$$\phi(a_0 + a_1x + \cdots + a_nx^n) = \max\{|a_0|, |a_1|, \ldots, |a_n|\}$$

is a non-archimedean valuation on the ring of polynomials $k[x]$.

Proof: Certainly for $f(x) \varepsilon k[x]$, $\phi(f(x)) = 0$ if and only if $f(x)$ is the zero polynomial in $k[x]$. Now suppose

$$f(x) = a_0 + a_1x + \cdots + a_nx^n$$

and

$$g(x) = b_0 + b_1x + \cdots + b_mx^m$$

where, without loss of generality, it is assumed that $m \leq n$ and, therefore, $b_j = 0$ for $j > m$. Then

$$\begin{aligned}\phi(f(x) + g(x)) &= \max_{0\leq i\leq n} \{|a_i + b_i|\} \leq \max_{0\leq i\leq n} \{\max(|a_i|,|b_i|)\} \\ &= \max\left\{\max_{0\leq i\leq n} |a_i|, \max_{0\leq i\leq n} |b_i|\right\} \\ &= \max\{\phi(f(x)),\phi(g(x))\}.\end{aligned}$$

To complete the proof of the lemma, it must be shown that

$$\phi(f(x)g(x)) = \phi(f(x))\phi(g(x)).$$

Now $f(x)g(x) = c_0 + c_1x + \cdots + c_{m-n}x^{m+n}$ where $c_t = \sum_{i+j=t} a_ib_j$.

Note first that $\phi(f(x)g(x)) \leq \phi(f(x))\phi(g(x))$.

Let $f(x) = f_1(x) + f_2(x)$ where a term a_kx^k of $f(x)$ is a term of $f_1(x)$ if and only if $|a_k| = \max_{0\leq i\leq n} \{|a_i|\}$ and a_jx^j is a term of $f_2(x)$ if and only if $|a_j| < \max_{0\leq i\leq n} \{|a_i|\}$. Similarly, let $g(x) = g_1(x) + g_2(x)$ where $g_1(x)$ contains all terms of $g(x)$ with maximum valuation. Thus,

$$f(x)g(x) = f_1(x)g_1(x) + f_1(x)g_2(x) + f_2(x)g_1(x) + f_2(x)g_2(x).$$

Now $\phi(f_1(x)g_2(x)) \leq \phi(f_1(x))\phi(g_2(x)) < \phi(f_1(x))\phi(g_1(x))$. Similarly, $\phi(f_2(x)g_1(x)) < \phi(f_1(x))\phi(g_1(x))$ and $\phi(f_2(x)g_2(x)) < \phi(f_1(x))\phi(g_1(x))$.

Consider $f_1(x)g_1(x) = c_0 + c_1x + \cdots + c_{p+q}x^{p+q}$. Then $|c_{p+q}| = |a_pb_q| = |a_p||b_q| = |a_i||b_j|$ for every pair of coefficients a_1 and b_j of $f_1(x)$ and $g_1(x)$, respectively. It follows that

$$\left|c_t\right| = \left|\sum_{i+j=t} a_ib_j\right| \leq \max_{i+j=t}\left\{\left|a_ib_j\right|\right\} = \left|a_pb_q\right| = \left|c_{p+q}\right|.$$

According to the definition of the mapping ϕ,

$$\phi(f_1(x)g_1(x)) = \max_{0\leq t\leq p+q}\{|c_t|\} = |c_{p+q}|.$$

Since $|c_{p+q}| = |a_p||b_q| = \phi(f_1(x))\phi(g_1(x))$, it follows that $\phi(f_1(x)g_1(x)) = \phi(f_1(x))\phi(g_1(x))$. Since $\phi(f(x)) = \phi(f_1(x))$, $\phi(g(x)) = \phi(g_1(x))$ and

$$\phi(f_1(x)g_1(x)) > \phi(f_1(x)g_2(x) + f_2(x)g_1(x) + f_2(x)g_2(x)),$$

it follows that

$$\phi(f(x)g(x)) = \phi(f_1(x)g_1(x)) = \phi(f_1(x))\phi(g_1(x)) = \phi(f(x))\phi(g(x)).$$

This completes the proof of Lemma 3.16.

<u>Lemma</u> 3.17. If K is algebraically closed and $f(x)$ and $g(x)$ are monic polynomials of degree n in $K[x]$ such that $\phi(f(x) - g(x)) < \epsilon$ then for any root β of $g(x)$ there is a root α of $f(x)$ such that $|\beta - \alpha| < A\sqrt[n]{\epsilon}$ where A is an upper bound of the valuations of the coefficients of $f(x)$ and $g(x)$.

Proof: Note first that the valuation of any root of $g(x)$ (or of $f(x)$) is bounded above by A. To see this, suppose $|\beta| > A$. Then

$$g(\beta) = b_0 + b_1\beta + \cdots + b_{n-1}\beta^{n-1} + \beta^n.$$

Since $|b_i\beta^i| \leq A|\beta^i| < |\beta^{i+1}|$ for $i = 0,1, \ldots, n-1$, it follows that $|g(\beta)| = |\beta^n| \neq 0$, contradicting the fact that β is a root.

Now suppose $\phi(f(x) - g(x)) < \epsilon$. Since K is algebraically closed, there exist n roots of $f(x)$, $\alpha_1, \alpha_2, \ldots, \alpha_n$. Then if β is a root of $g(x)$,

$$\begin{aligned} |f(\beta)| &= |f(\beta) - g(\beta)| \\ &= |a_0 - b_0 + (a_1 - b_1)\beta + \cdots + (a_{n-1} - b_{n-1})\beta^{n-1}| \\ &\leq \max_{0 \leq i \leq n-1} \{|a_i - b_i||\beta^i|\}. \end{aligned}$$

Since $|\beta| \leq A$ and $A \geq 1$, then $|\beta^i| \leq A^n$. Also since $\phi(f(x) - g(x)) < \epsilon$ then $|a_i - b_i| < \epsilon$ for each $i = 0,1, \ldots, n-1$. It follows that $|f(\beta)| < \epsilon A^n$.

Now

$$f(x) = \prod_{k=1}^{n} (x - \alpha_k)$$

so that

$$f(\beta) = \prod_{k=1}^{n} |\beta - \alpha_k| < \epsilon A^n.$$

Therefore, there is at least one root α of $f(x)$ which satisfies the relation $|\beta - \alpha| < A\sqrt[n]{\epsilon}$. This completes the proof.

The final objective of proving the existence of an algebraically closed extension of the p-adic field Q_p which is complete with respect to an extension of the non-archimedean valuation on Q_p is at last within reach.

Theorem 3.18. Let K be an algebraically closed non-archimedean field. Then the completion $\hat{K}$ is algebraically closed.

Proof: Let $f(x) = a_0 + a_1x + \cdots + a_nx^n$ be an irreducible polynomial in $\hat{K}[x]$. Without loss of generality it may be assumed that $f(x)$ is monic, that is, $a_n = 1$. The proof will be accomplished by showing that $f(x)$ has a root in $\hat{K}$, and this will be done by producing a Cauchy sequence in K whose limit is the desired root.

Since $a_i \varepsilon \hat{K}$, then for each $i = 0,1, \ldots, n-1$ there is a Cauchy sequence

$$\left\{ b_{i,j} \right\}_{j=1}^{\infty}$$

in K such that $\{b_{i,j}\}$ converges to a_i. Let $f_j(x)$ be the polynomial in $K[x]$ given by

$$f_j(x) = b_{0,j} + b_{1,j}x + \cdots + b_{n-1,j}x^{n-1} + x^n.$$

Now choose M_1 such that $\max\limits_{0 \leq i \leq n-1} \{|b_{i,m} - a_i|\} < 1/2$ for every $m \geq M_1$. Similarly, for each integer $k > 1$, choose M_k such that $M_k > M_{k-1}$ and $\max\limits_{0 \leq i \leq n-1} \{|b_{i,m} - a_i|\} < (1/2)^k$ for every $m \geq M_k$.

Let $A = \max\{|a_0|, |a_1|, \ldots, |a_{n-1}|, 1\} + 1$. Then, by the way in which M_1 was chosen, A is an upper bound of the valuations of the coefficients of $f_m(x)$ for every $m \geq M_1$. Thus, by successive applications of Lemma 4.19, if β_{k-1} is a root of $f_{M_{k-1}}(x)$, then there is a root β_k of $f_{M_k}(x)$ such that $|\beta_k - \beta_{k-1}| < A(\sqrt[n]{1/2})^k$. Therefore, $\{\beta_k\}$ is a Cauchy sequence in K. Since $\hat{K}$ is the completion of K, there is a β in K such that $\{\beta_k\}$ converges to β.

By the way in which the polynomials $f_j(x)$ are defined, $\{f_j(\beta)\}$ converges to $f(\beta)$. Since $\{f_j(\beta)\}$ converges to zero, β must be a root of $f(x)$. This completes the proof.

Since the completion of a field with respect to a non-archimedean valuation is again a non-archimedean field, the final objective of this chapter has been accomplished. Let T_p denote a complete algebraically closed extension of the p-adic field Q_p. In later chapters analogies between T_p and the complex field C will be explored.

CHAPTER IV

POWER SERIES

The theory of infinite series over a non-archimedean field has been well developed in several sources. Actually, there are only a few significant differences between the non-archimedean and real situations. Perhaps the most notable distinction is that for convergence of a series $\sum a_n$ in a non-archimedean field, it is sufficient that the sequence $\{a_n\}$ converges to zero. Of course, this is not the case for real series as the harmonic series $\sum 1/n$ shows. Also, the theory of power series with coefficients in a non-archimedean field offers few surprises. For a good exposition of power series and functions defined by power series, that is, analytic functions, the reader is referred to Palmer [14], Chapters 4 and 5.

This chapter will consider analytic functions on an algebraically closed extension T_p of the p-adic field Q_p. In particular, the first objective will be the development of a device called Newton's Polygon. Then Newton's Polygon will be used to examine analytic functions including the determination of the domain of convergence and the location of zeros.

Consider analytic functions defined by

$$f(x) = \sum_{n=0}^{\infty} b_n(x - a)^n$$

where $a, b_0, b_1, \ldots$ are in T_p. As in real series, the radius of convergence ρ is given by $1/\rho = \overline{\lim} \sqrt[n]{|b_n|}$ where it is understood that the series converges for every $x \in T_p$ if $\overline{\lim} \sqrt[n]{|b_n|} = 0$ and converges only for $x = a$ if $\overline{\lim} \sqrt[n]{|b_n|} = \infty$.

Newton Diagram

In order to develop Newton's Polygon for power series, it is necessary to consider first a set of points referred to as the Newton diagram for the power series. For definiteness, it will be assumed that the analytic functions in question are expressible as power series with coefficients in the p-adic field Q_p.

Recall that for each $x \neq 0$, ord x is defined by $\text{ord } x = -\log_p x$.

Definition 4.1. Let a function f be defined by a power series over Q_p,

$$f(x) = \sum_{n=0}^{\infty} b_n (x - a)^n.$$

The set of points in the Cartesian plane given by

$$T = \{(n, \text{ord } b_n) : \; n = 0,1,2, \ldots, \quad b_n \neq 0\}$$

is called the Newton diagram for the series.

The next theorem shows that the radius of convergence of the power series can be expressed in terms of the slopes of lines joining the origin to the points of the Newton diagram.

<u>Theorem</u> 4.2. Let the power series

$$\sum_{n=0}^{\infty} b_n (x - a)^n$$

have a radius of convergence ρ. If

$$-\infty < \underline{\lim} \frac{\text{ord } b_n}{n} < \infty,$$

then

$$\log_p \rho = \underline{\lim} \frac{\text{ord } b_n}{n} ;$$

if

$$\underline{\lim} \frac{\text{ord } b_n}{n} = -\infty,$$

then

$$\rho = 0;$$

and if

$$\underline{\lim} \frac{\text{ord } b_n}{n} = \infty,$$

then

$$\rho = \infty.$$

Proof: Suppose

$$-\infty < \underline{\lim} \frac{\text{ord } b_n}{n} < \infty.$$

Then, since

$$|b_n| = \left(\frac{1}{p} \right)^{\text{ord } b_n},$$

it follows that

$$\sqrt[n]{|b_n|} = \left(\frac{1}{p}\right)^{\frac{\text{ord } b_n}{n}}$$

Thus,

$$\frac{1}{\rho} = \overline{\lim}\left(\frac{1}{p}\right)^{\frac{\text{ord } b_n}{n}}$$

so that

$$\rho = \underline{\lim}\ p^{\frac{\text{ord } b_n}{n}} .$$

It follows that

$$\log_p \rho = \underline{\lim} \frac{\text{ord } b_n}{n} .$$

Now suppose

$$\underline{\lim} \frac{\text{ord } b_n}{n} = -\infty.$$

This implies

$$\overline{\lim}\ \sqrt[n]{|b_n|} = \overline{\lim}\left(\frac{1}{p}\right)^{\frac{\text{ord } b_n}{n}} = \infty$$

so that $\rho = 0$. Finally, if

$$\underline{\lim} \frac{\text{ord } b_n}{n} = \infty,$$

then

$$\overline{\lim}\ \sqrt[n]{|b_n|} = \overline{\lim}\left(\frac{1}{p}\right)^{\frac{\text{ord } b_n}{n}} = 0$$

so that $\rho = \infty$.

Palmer [14] showed that the radius of convergence of the exponential series

$$\sum_{n=0}^{\infty} \frac{1}{n!} x^n$$

is given by $\rho = p^{-1/(p-1)}$. The following example shows that Theorem 4.2 may be used to obtain the same result.

<u>Example</u> 4.3. Radius of convergence of

$$\sum_{n=0}^{\infty} \frac{1}{n!} x^n.$$

Let $n = a_0 + a_1 p + \cdots + a_k p^k$, $a_k \neq 0$ and $t_n = a_0 + a_1 + \cdots + a_k$ then

$$\text{ord } n! = \frac{n - t_n}{p - 1}$$

so that

$$\frac{\text{ord } n!}{n} = \frac{1}{p-1}\left(1 - \frac{t_n}{n}\right).$$

Now $n \geq p^k$ implies $k \leq \log_p n$ and, since $t_n < (k+1)p$, it follows that

$$\frac{t_n}{n} < \frac{(k+1)p}{n} \le \frac{p \log_p n}{n} + \frac{p}{n} .$$

Therefore,

$$\lim_{n \to \infty} \frac{t_n}{n} = 0$$

so that $\lim\limits_{n \to \infty} \frac{\text{ord } n!}{n} = \frac{1}{p-1}$. Since $b_n = \frac{1}{n!}$, it follows that

$$\lim \frac{\text{ord } b_n}{n} = \lim_{n \to \infty} \frac{-\text{ ord } n!}{n}$$
$$= \frac{-1}{p-1} .$$

Therefore, the radius of convergence $\rho = p^{-1/(p-1)}$ as expected. Figure 1 shows the first few points in the Newton diagram for the series

$$\sum_{n=0}^{\infty} \frac{1}{n!} x^n$$

when $p = 3$.

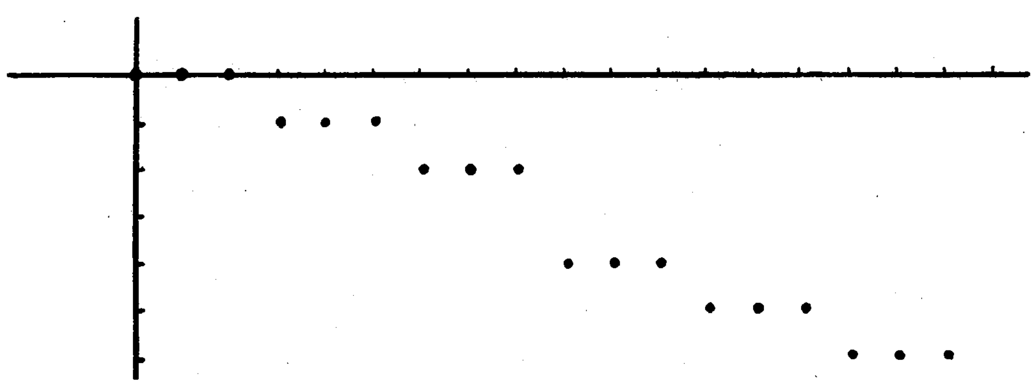

Figure 1. Newton Diagram for Exponential Series

Newton Polygon

The Newton polygon for a power series will be developed by a construction utilizing the Newton diagram. Once defined, it will be shown that the Newton polygon determines the radius of convergence and also provides information about the location of the zeros of the power series. The definition of a lower support line for a given set is needed.

Definition 4.4. Suppose T is a subset of the plane and that L is a non-vertical line with equation $y = mx + b$. Then L is a lower support line of T if and only if:

1. for every $(x_1,y_1) \in T$, $y_1 \geq mx_1 + b$, and
2. if $b' > b$, then there is a point $(x_0,y_0) \in T$ such that $y_0 < mx_0 + b'$.

Note that if T is a finite set and L is a lower support line, then L contains at least one point of T. On the other hand, if T is infinite, then T may have a lower support line which does not intersect T. For example, if T is the right branch of the hyperbola

$$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1,$$

then the asymptote $y = -\frac{b}{a}$ is a lower support line of T which does not intersect T.

Consider a power series

$$\sum_{n=0}^{\infty} b_n(x - a)^n.$$

It will be assumed that $b_0 \neq 0$ and that there is at least one other non-zero coefficient. It will be shown that if the Newton diagram T has a lower support line, then it has a lower support line through the point $B_0 = (0, \text{ord } b_0)$. To see this support line L with equation $y = mx + b$ is a lower support line T. If B_0 is on L, then the conclusion holds. If B_0 is not on L, then B_0 is above L, that is, ord $b_0 > b$. Let point B be the intersection of line L and the vertical line $x = 1$. Then the line L' through B_0 and B is also a lower support line of T. Figure 2 illustrates the situation.

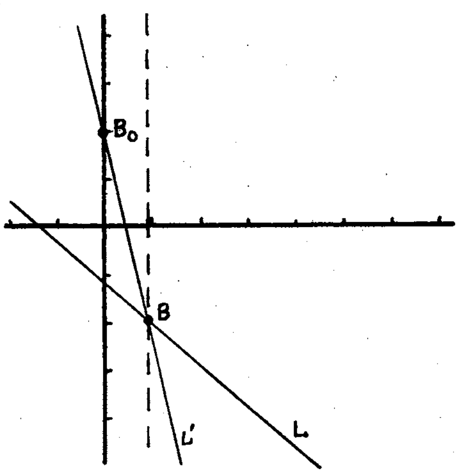

Figure 2. Lower Support Line Through the First Point

If all points of T are above line L, then all points of T are above L'.

It should be noted that a Newton diagram T need not have any lower support line. For example, consider the series

$$\sum_{n=0}^{\infty} p^{-n^2} x^n.$$

Then $T = \{(n,-n^2): n = 0,1,2, \ldots\}$. Since for any choice of m and b, an n can be found large enough so that $-n^2 < mn + b$, there is no lower support line for T. By Theorem 4.2,

$$\underline{\lim} \frac{\text{ord } b_n}{n} = \lim -n = -\infty$$

so that the radius of convergence is 0.

Now suppose a Newton diagram T has a lower support line. Consider the set of all lower support lines through $B_0 = (0, \text{ord } b_0)$. Since there is a point in T besides B_0, there is a lower support line L_0 having maximum slope m_0. It may happen that T has no lower support line with slope greater than m_0. In this case, the Newton polygon consists only of the ray

$$\{(x,y): (x,y) \in L_0, \; x \geq 0\}$$

which is denoted by L_0^+.

On the other hand, suppose T has a lower support line with slope $m > m_0$. It will be shown that L_0 contains at least two but only a finite number of points in T. Now the equation of line L_0 is $y = m_0 x + \text{ord } b_0$ and the equation of line L is $y = mx + b$. Since L_0 has maximum slope, it follows that $b < \text{ord } b_0$. It will be shown first that L_0 contains only finitely many points of T. Suppose otherwise and pick N such that $N(m - m_0) > \text{ord } b_0 - b$. Since L_0 contains infinitely many points of T there is an $n' \geq N$ such that $\text{ord } b_{n'} = m_0 n' + \text{ord } b_0$. Then, for that n',

$$\begin{aligned}
\text{ord } b_{n'} - mn' &= \text{ord } b_{n'} - n'(m_0 + (m - m_0)) \\
&= \text{ord } b_{n'} - n'm_0 - n'(m - m_0) \\
&= \text{ord } b_0 - n'(m - m_0) \\
&< \text{ord } b_0 - (\text{ord } b_0 - b) \\
&= b.
\end{aligned}$$

Therefore, $\text{ord } b_{n'} < n'm + b$ so that $y = mx + b$ is not a lower support line of T. Thus, if T has a lower support line with slope greater than m_0, then line L_0 has only finitely many points of T.

Since B_0 is on L_0, it remains to be shown that L_0 contains at least one more point of T. As before, L is a lower support line of T having equation $y = mx + b$ with $m > m_0$ and $b < \text{ord } b_0$. Let point (a,c) be the intersection of L and L_0. By considering the minimum vertical distance between the line L_0 and the points $(n, \text{ord } b_n)$ of T for $1 \leq n \leq [a] + 1$, as well as the vertical distance between L_0 and L at $x = [a] + 1$, it may be verified that if B_0 is the only point of T on L_0, then there is a lower support line through B_0 with slope greater than m_0. (See Figure 3.) Since this contradicts the way in which L_0 is determined, it follows that if T has a lower support line with slope greater than m_0 then L_0 has at least two points of T.

The construction of the Newton polygon in the case T has a lower support line with slope $m > m_0$ can now be continued as follows.

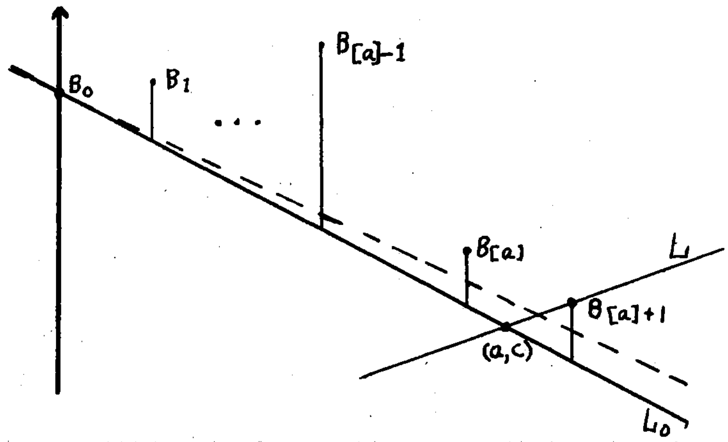

Figure 3. Lower Support Line Contains Finitely Many Points

Let B_1 be the point in T and on L_0 having maximum abscissa. Then if T has no points with abscissa greater than that of B_1, the power series is a polynomial in which case let L_1^+ denote the vertical ray upward with endpoint B_1. In this case, the Newton polygon consists of the segment $\overline{B_0B_1}$ together with the ray L_1^+.

If T has points with abscissa greater than that of B_1, then there is a lower support line L_1 of T through B_1 and having maximum slope m_1. The above argument can be repeated so that either T has no lower support line with slope greater than m_1 or else there is a lower support line L having slope $m > m_1$. In the first case, let L_1^+ denote the ray on L_1 having endpoint B_1. In this case, the Newton polygon consists of $\overline{B_0B_1} \cup L_1^+$. In the second case, L_1 contains at least two but finitely many points of T. Let B_2 be the point of T on L_1 having maximum abscissa. The above discussion can be repeated to find either a ray L_2^+ or else a segment $\overline{B_2B_3}$ on the lower support line L_2.

Now suppose there is a lower support line L_n through point B_n of T such that L_n has maximum slope m_n. If there is no lower support line of T with slope greater than m_n and let L_n^+ denote the ray on L_n with endpoint B_n and such that the points on L_n^+ have abscissas greater than that of B_n. If there is a lower support line with slope greater than m_n, then there is a point B_{n+1} on L_n and in T having maximum abscissa. If T has no point with greater abscissa than that of B_{n+1}, then let L_{n+1}^+ denote the vertical ray with endpoint B_{n+1}. If T has points with greater abscissa than that of B_{n+1}, then let L_{n+1} be the lower support line through B_{n+1} having maximum slope.

The following definition can be given as a summary of the above discussion.

Definition 4.5. Let T be the Newton diagram for a power series

$$\sum_{n=0}^{\infty} b_n(x - a)^n$$

such that $b_0 \neq 0$ and the series is not a constant function. The Newton polygon for the series is defined as follows:

1. If for every positive integer n there is a lower support line L_n containing B_n and B_{n+1} then the Newton polygon is the union of line segments

$$\bigcup_{n=0}^{\infty} \overline{B_n B_{n+1}} .$$

2. If T has no lower support line with slope greater than that of L_n, the lower support line through B_n then the Newton diagram is the union $\overline{B_0B_1} \cup \overline{B_1B_2} \cup \cdots \cup \overline{B_{n-1}B_n} \cup L_n^+$.

3. If T has no point with abscissa greater than that of B_n then the Newton polygon is the union $\overline{B_0B_1} \cup \cdots \cup \overline{B_{n-1}B_n} \cup L_n^+$.

The segments $\overline{B_nB_{n+1}}$ are called sides of the Newton polygon, and the ray L_n^+ is called the terminal side. If a Newton polygon does not contain a terminal side, then it is called an infinite Newton polygon; otherwise, it is called finite. The following example shows that an infinite Newton polygon does exist.

Example 4.6. The Newton polygon for

$$\sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n} x^n.$$

The Newton diagram $T = \{(n, -\text{ord } n): n = 1,2, \ldots\}$. Now $\text{ord } n = k$ whenever $p^k | n$ and $p^{k+1} \nmid n$. Let L_k denote the line through the points $(p^k,-k)$ and $(p^{k+1},-k - 1)$. It will be shown that L_k is a lower line of support of T for each $k = 0,1, \ldots$. The equation of L_k is

$$y + k = \frac{-1}{p^{k+1} - p^k} (x - p^k).$$

To show that L_k is a lower support line for T, let $n = p^j n_0$ where $(n_0,p) = 1$, that is, n_0 and p are relatively prime. Then, since $\text{ord } n = j$, it suffices to show that

$$-j + k \geq \frac{-1}{p^{k+1} - p^k} (p^j n_0 - p^k)$$

or, equivalently,

$$j - k \leq \frac{1}{p^{k+1} - p^k} (p^j n_0 - p^k).$$

Let $q = j - k$. If $q = 0$, then, since $n_0 \geq 1$,

$$\frac{1}{p^{k+1} - p^k} (p^j n_0 - p^k) = \frac{1}{p - 1} (n_0 - 1) \geq 0 = q.$$

If $q < 0$, then

$$\frac{1}{p^{k+1} - p^k} (p^j n_0 - p^k) \geq \frac{1}{p - 1} (p^q - 1) > -1 \geq q.$$

Finally, suppose $q > 0$. Now $q - 1 \geq \log_p q$ so that $p^{q-1} \geq q$ and, hence, $p^q \geq pq$. Since $q \geq 1$, it follows that $p^q - 1 \geq pq - q$ and, therefore, $\frac{1}{p - 1} (p^q - 1) \geq q$. Since

$$\frac{1}{p^{k+1} - p^k} (p^j n_0 - p^k) \geq \frac{1}{p - 1} (p^q - 1),$$

it has been established that

$$j - k \leq \frac{1}{p^{k+1} - p^k} (p^j n_0 - p^k).$$

Therefore, for any $k = 0,1,2, \ldots,$ the line L_k is a lower line of support for the Newton diagram T.

Since the slope of L_k is given by

$$m_k = \frac{-1}{p^k(p - 1)} ,$$

it is clear that the Newton polygon contains a countably infinite number of line segments. Figure 4 illustrates the Newton polygon for

$$\sum_{n=1}^{\infty} \frac{(-1)^n}{n} x^n$$

when $p = 3$.

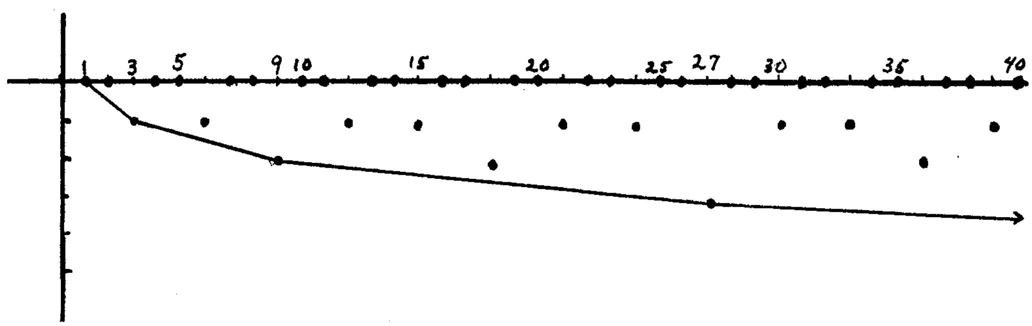

Figure 4. Newton Polygon for Logarithm Series

By the way in which the Newton polygon is defined, if $\{m_i\}$ is the sequence of slopes of the sides, then $\{m_i\}$ is monotonic increasing.

The major result of this section can now be established. This theorem shows how the radius of convergence can be obtained from the slopes of the sides of the Newton polygon.

<u>Theorem</u> 4.7. Let $\{m_i\}$ be the sequence of slopes for the Newton polygon of the power series

$$\sum_{n=0}^{\infty} b_n(x - a)^n$$

having radius of convergence $\rho > 0$. Then $\log_p \rho = \underset{i \to \infty}{\text{limit}}\, m_i$ if the Newton polygon is infinite, and $\log_p \rho = m_n$ if m_n is the slope of the terminal side L_n^+.

Proof: If the Newton polygon has a vertical side, then the power series is simply a polynomial so that the radius of convergence is infinite. Thus, the theorem holds in this special case.

In view of Theorem 4.2, it suffices to show that

$$\underline{\lim}\, \frac{\text{ord } b_n}{n} = \underset{i \to \infty}{\text{limit}}\, m_i .$$

Let

$$m = \underset{i \to \infty}{\text{limit}}\, m_i \quad \text{and} \quad \alpha = \underline{\lim}\, \frac{\text{ord } b_n}{n} .$$

Assume first that both m and α are finite and that $m \neq \alpha$. Let L be a line with equation $y = \frac{m + \alpha}{2} x$. If $\alpha < m$, then $\alpha < \frac{m + \alpha}{2} < m$. Since $\frac{m + \alpha}{2} = \alpha + \frac{m - \alpha}{2}$, the definition of $\underline{\lim}$ implies there are infinitely many n such that

$$\frac{\text{ord } b_n}{n} < \frac{m + \alpha}{2} .$$

Thus, there are infinitely many points of the Newton diagram T which are below the line L.

On the other hand, since $\{m_i\}$ is an increasing sequence, $\frac{m + \alpha}{2} < m$ implies there is a lower support line L_k with slope $m_k > \frac{m + \alpha}{2}$. But this implies there are only finitely many points of T below L which contradicts the previous statement. Therefore, $\alpha \geq m$.

If $\alpha > m$ then $\frac{m + \alpha}{2} > \alpha$ so that, according to the definition of $\underline{\lim}$, there is an N such that

$$\frac{\text{ord } b_n}{n} > \frac{m + \alpha}{2}$$

for every $n \geq N$. This implies that $B_n \varepsilon T$ is above the line L for every $n \geq N$. Since there are only finitely many points $B_k \varepsilon T$ with $k < N$, there is a lower support line of T with slope $\frac{m + \alpha}{2} > m$. But the sequence of slopes is a monotonic increasing sequence so that there is no lower support line of T with slope greater than m. Hence, $\alpha \leq m$. It follows that $\alpha = m$.

Now suppose m is finite, and α is not finite. Then let L have equation $y = (m + 1)x$ if $\alpha = \infty$, and $y = (m - 1)x$ if $\alpha = -\infty$. Then essentially the same arguments as before yield contradictions. Finally, suppose $m = \infty$. Let L be the line $y = (\alpha + 1)x$ if α is finite, and let L be the line $y = x$ if $\alpha = -\infty$. Again the definition of $\underline{\lim}$ implies there are infinitely many points of T below line L. But since there is a lower support line with slope greater than that of L, this is a contradiction. Since whenever a Newton polygon exists, either $\operatorname*{limit}_{i \to \infty} m_i > -\infty$ or else the slope of L_n^+ is greater than $-\infty$. The proof of Theorem 4.7 is complete.

The following examples utilize Theorem 4.7.

Example 4.8. The radius of convergence of

$$\sum_{n=1}^{\infty} \frac{(-1)^n}{n} x^n.$$

According to Example 4.6, the slopes of the sides of the Newton polygon are given by

$$m_k = \frac{-1}{p^k(p-1)}$$

so that $\operatorname*{limit}_{k \to \infty} m_k = 0$. Thus, by Theorem 4.7, $\rho = 1$. To see that this agrees with Theorem 4.2, note that $n \geq p^{\text{ord } n}$ so that $\log_p n \geq \text{ord } n$ and, hence,

$$\frac{\log_p n}{n} \geq \frac{\text{ord } n}{n} .$$

Since

$$\operatorname*{limit}_{n \to \infty} \frac{\log_p n}{n} = 0,$$

it follows that $\operatorname*{limit}_{n \to \infty} \frac{\text{ord } n}{n} = 0$. Thus,

$$\log_p \rho = \underline{\lim} \frac{\text{ord } b_n}{n} = \underline{\lim} \frac{-\text{ord } n}{n} = 0$$

so that $\rho = 1$.

Example 4.9. The radius of convergence of the binomial series

$$\sum_{n=0}^{\infty} \binom{\alpha}{n} x^n.$$

The coefficients $\binom{\alpha}{n}$ are given by $\frac{(\alpha-1)(\alpha-2)\cdots(\alpha-n+1)}{n!}$ where α may be any p-adic integer. If α is a positive rational integer than the series is actually a polynomial and the series converges for all x. If, on the other hand, α is a p-adic integer which is not a non-negative rational integer then the canonical representation of α is infinite, say

$$\alpha = a_0 + a_1p + a_2p^2 + \cdots + a_kp^k + \cdots .$$

It was shown by Palmer [14] that in this case the radius of convergence is at least $p^{-1/(p-1)}$. By applying Theorem 4.7, it can be established that the radius of convergence ρ is equal to 1. It suffices to show that the x-axis is the terminal ray in the Newton polygon for

$$\sum_{n=0}^{\infty} \binom{\alpha}{n} x^n.$$

Recall that according to Theorem 1.17, given the rational integer $N = b_0 + b_1p + \cdots + b_kp^k$ and the p-adic integer $\alpha = a_0 + a_1p + \cdots + a_kp^k + \cdots$, then

$$\operatorname{ord} \binom{\alpha}{N} = \sum_{i=0}^{\infty} \delta_i$$

where $\delta_{-1} = 0$ and

$$\delta_i = \begin{cases} 1 & \text{if } a_i < b_i + \delta_{i-1} \\ 0 & \text{if } a_i \geq b_i + \delta_{i-1} \end{cases} .$$

Thus, for every $n_k = a_0 + a_1p + \cdots + a_kp^k$,

$$\operatorname{ord}\binom{\alpha}{n_k} = 0.$$

Since $\operatorname{ord}\binom{\alpha}{n} \geq 0$ for every n, and there are infinitely many choices for n such that $\operatorname{ord}\binom{\alpha}{n} = 0$, it follows that the x-axis is the terminal side of the Newton polygon for the binomial series

$$\sum_{n=0}^{\infty} \binom{\alpha}{n} x^n$$

whenever α is a p-adic integer having an infinite canonical representation. Thus, $\log_p \rho = 0$ and, therefore, $\rho = 1$.

Figure 5 illustrates the Newton diagram for

$$\sum_{n=0}^{\infty} \binom{1/2}{n} x^n$$

where $p = 3$. Recall that the canonical representation of $1/2$ is $2 + 1 \cdot 3 + 1 \cdot 3^2 + 1 \cdot 3^3 + \cdots$. Thus, for example, since $25 = 1 + 2 \cdot 3 + 2 \cdot 3^2$, then $\operatorname{ord}\binom{1/2}{25} = 0 + 1 + 1 = 2$. Similarly, since $37 = 1 + 0 \cdot 3 + 1 \cdot 3^2 + 1 \cdot 3^3$, then $\operatorname{ord}\binom{1/2}{37} = 0 + 0 + 0 + 0 = 0$.

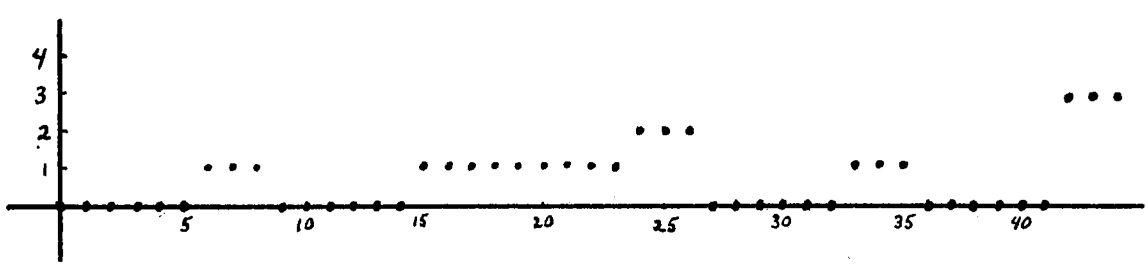

Figure 5. Newton Diagram for Binomial Series

Hensel's Lemma

As indicated earlier, Newton's polygon is useful in locating the zeros of certain power series. Before this topic can be discussed, it will be necessary to prove an important theorem called Hensel's Lemma for power series. Palmer [14] proved a form of Hensel's Lemma which states that under suitable conditions a polynomial in $O_p[x]$ can be written as the product of two non-constant polynomials. The form to be established here states that under similar conditions, a convergent power series with coefficients in the p-adic integers O_p can be written as the product of a polynomial and another convergent power series. Several definitions, lemmas and theorems are needed first.

<u>Definition</u> 4.10. Let A_n be the ideal $p^n O_p$ and let η be the canonical homomorphism from O_p onto O_p/A_n. Then $\eta_n: O_p[x] \to O_p/A_n[x]$ is defined by

$$\eta_n(a_0 + a_1x + \cdots + a_sx^s) = \eta(a_0) + \eta(a_1)x + \cdots + \eta(a_s)x^s$$

Since η is a homomorphism, it follows that η_n is a homomorphism.

<u>Definition</u> 4.11. If

$$f(x) = \sum_{k=0}^{\infty} a_k x^k \quad \text{and} \quad g(x) = \sum_{k=0}^{\infty} b_k x^k$$

are power series over O_p and A_n is the ideal $p^n O_p$, then define $f \equiv g \bmod A_n$ if and only if for every $k \geq 0$, $p^n | (a_k - b_k)$.

Note that in the above definition one or both of f and g may be polynomials. It is immediate that the relation $\equiv \bmod A_n$ is an equivalence relation.

Theorem 4.12. If f is a power series over 0_p and g_n is a sequence of polynomials such that $f \equiv g_n \bmod A_n$ for every $n \geq 1$, then the sequence converges uniformly and $\lim g_n = f$.

Proof: Since $f \equiv g_n \bmod A_n$, then for every x in the domain of f, $f(x) \equiv g_n(x) \bmod p^n$. For $\epsilon > 0$, choose an $N > 0$ such that for all $n \geq N$, $1/p^n < \epsilon$. Since $p^n | (f(x) - g_n(x))$ for every n, then for $n \geq N$, $|f(x) - g_n(x)| \leq 1/p^n < \epsilon$ for every x. Therefore, the sequence g_n converges uniformly to f.

Theorem 4.13. If $\{g_n\}$ is a sequence of polynomials with coefficients in 0_p such that for each $n = 0,1,2, \ldots,$ $g_n \equiv g_{n+1} \bmod A_n$, then $\{g_n\}$ converges uniformly on $|x| \leq 1$ to a function g such that g is represented by a power series with coefficients in 0_p.

Proof: Since $g_n \equiv g_{n+1} \bmod A_n$ implies p^n divides every coefficient of the polynomial $g_n - g_{n+1}$, it follows that for every $\epsilon > 0$, there is an N such that whenever $n \geq N$, then $|g_n(x) - g_{n+1}(x)| < \epsilon$ for every $|x| \leq 1$. For functions defined on a non-archimedean field, this is a sufficient condition for uniform convergence. Thus, the sequence $\{g_n\}$ converges uniformly on $|x| \leq 1$. Let g be the limit function. To see that g is represented by a power series suppose the polynomial g_n is given by

$$g_n(x) = a_{n,0} + a_{n,1}x + \cdots + a_{n,s(n)}x^{s(n)}.$$

Then $g_n \equiv g_{n+1} \bmod A_n$ implies $p^n | (a_{n,j} - a_{n+1,j})$ for each $j \geq 0$. Therefore, every sequence

$$\left\{ a_{n,j} \right\}_{n=0}^{\infty}$$

converges to a point in O_p. For each $j \geq 0$, let $\lim_{n \to \infty} a_{n,j} = b_j$. Then the power series

$$g(x) = \sum_{n=0}^{\infty} b_n x^n$$

is the limit of the sequence g_n.

<u>Corollary</u> 4.14. If for each n, g_n is a monic polynomial of degree s, then the limit function g is a monic polynomial of degree s.

Proof: Since $a_{n,s} = 1$ for every n and $a_{n,j} = 0$ for every n and $j > s$, then $b_s = 1$ and $b_j = 0$ for $j > s$.

<u>Corollary</u> 4.15. For every n, $g \equiv g_n \bmod A_n$.

Proof: As in the proof of the Theorem, let

$$g(x) = \sum_{k=0}^{\infty} b_k x^k$$

where b_k is the p-adic limit of the coefficients of x^k in the polynomials $g_n(x) = a_{n,0} + a_{n,1}x + \cdots + a_{n,s}x^s$. Then for large enough N, $p^n | (b_k - a_{N,k})$ and, since $g_n \equiv g_{n+1} \bmod A_n$ for every n, it follows that $p^n | (a_{n,k} - a_{N,k})$ so that $p^n | (b_k - a_{n,k})$.

The next two lemmas will be used in the proof of Hensel's Lemma. Their proofs are found in the Appendix.

Lemma 4.16. Let G and H be polynomials in $0_p[x]$ with G monic. Then G and H are relatively prime in $0_p[x]$ if and only if $\eta_n(G)$ and $\eta_n(H)$ are relatively prime in $0_p/A_n[x]$ for $n = 1,2,3, \ldots$.

Proof: See Appendix.

Lemma 4.17. Let G and H be two polynomials with coefficients in ring R. If G is monic and G and H are relatively prime in $R[x]$ with $\deg G = s$, then for every non-zero polynomial $Q \in R[x]$, there exists a unique pair of polynomials U and V such that $Q = UG + VH$ with $V = 0$ or $\deg V < s$.

Proof: See Appendix.

For convenience, when $n = 1$, the homomorphism η_n of Definition 4.10 will be denoted by

$$\eta_1(a_0 + a_1x + \cdots + a_sx^s) = \overline{a_0} + \overline{a_1x} + \cdots + \overline{a_sx}^s.$$

In the next definition, this notation is extended to power series.

Definition 4.18. If

$$f(x) = \sum_{n=0}^{\infty} a_nx^n$$

is a power series over 0_p, then let $\overline{f}$ denote the power series over $0_p/A_1$ such that

$$\overline{f}(x) = \sum_{n=0}^{\infty} \overline{a_n} x^n.$$

Lemma 4.19. If f and g are power series over O_p, then $\overline{f + g} = \overline{f} + \overline{g}$ and $\overline{fg} = \overline{f}\ \overline{g}$.

Proof: If a_k and b_k are corresponding coefficients of f and g, respectively, then $\overline{a_k + b_k} = \overline{a_k} + \overline{b_k}$ and

$$\overline{\sum_{i=0}^{k} a_i b_{k-i}} = \sum_{i=0}^{k} \overline{a_i b_{k-i}}$$

imply $\overline{f + g} = \overline{f} + \overline{g}$ and $\overline{fg} = \overline{f}\ \overline{g}$.

If

$$f(x) = \sum_{n=0}^{\infty} a_n x^n$$

converges for every x such that $|x| \leq 1$, then, in particular, the series

$$\sum_{n=0}^{\infty} a_n$$

converges. Therefore, the sequence $\{a_n\}$ is a null sequence in O_p so that for every non-negative integer k there exists a positive integer N_k such that $p^k | a_n$ whenever $n \geq N_k$. Thus, there exists only a finite number of k such that $p^k \nmid a_n$. This allows the following definition.

Definition 4.20. Let

$$f(x) = \sum_{n=0}^{\infty} a_n x^n$$

converge for every x such that $|x| \le 1$. For each non-negative integer k, define γ_k to be the largest subscript n such that $p^{k+1} \nmid a_n$.

Since $p^{k+1} | a_n$ implies $p^k | a_n$, it follows that $\gamma_k \le \gamma_{k+1}$ for $k = 0,1,2, \ldots$.

To illustrate the definition of γ_k, suppose

$$f(x) = (1 + p) + x + (p^2 + p^3)x^2 + px^3 + (p^3 - p^4)x^4 + a_5x^5 + \cdots$$

where $a_n = p^n$ for $n \ge 5$. Then $\gamma_0 = 1$, $\gamma_1 = 3$, $\gamma_2 = 3$, $\gamma_3 = \gamma_4 = 4$, and if $n \ge 5$ then $\gamma_n = n$.

Consider the power series

$$f(x) = \sum_{n=0}^{\infty} a_n x^n$$

convergent for all x such that $|x| \le 1$. Let Q_k be the polynomial of degree γ_k defined by

$$Q_k(x) = \sum_{n=0}^{\gamma_k} a_n x^n.$$

In view of Definition 4.11, and since $p^{k+1} | a_n$ for every $n > \gamma_k$, it follows that $Q_{k+1} \equiv Q_k \bmod A_{k+1}$ and $f \equiv Q_k \bmod A_{k+1}$.

Finally, Hensel's Lemma can be established. Throughout the statement and proof, $\mathfrak{D}$ will denote the set of all x such that $|x| \leq 1$.

Theorem 4.21. (Hensel's Lemma) Let

$$f(x) = \sum_{n=0}^{\infty} a_n x^n$$

be a power series which converges everywhere in $\mathfrak{D}$. Suppose there exist two polynomials G and H in $\overline{O_p}[x] = O_p/A_1[x]$ such that:

i. G is monic of degree s.

ii. G and H are relatively prime.

iii. $\overline{f} = GH$.

Then there exists a pair g,h such that:

i'. g is a monic polynomial of degree s in $O_p[x]$ and $\overline{g} = G$.

ii'. h is a power series which converges everywhere in $\mathfrak{D}$ and $\overline{h} = H$.

iii'. $f = gh$.

Proof: The overall plan is to define by induction two convergent sequences of polynomials in $O_p[x]$, $\{g_n\}$ and $\{h_n\}$, such that their limit functions g and h have the properties i', ii', and iii'.

Specifically, the sequences $\{g_n\}$ and $\{h_n\}$ will have the following properties:

(1) For every $n \geq 0$, g_n is monic of degree s, $\overline{g_n} = G$ and $g_n \equiv g_{n+1} \bmod A_{n+1}$ for $n \geq 0$.

(2) For every $n \geq 0$, $\overline{h_n} = H$, $h_n \equiv h_{n+1} \bmod A_{n+1}$.

(3) $f \equiv g_n h_n \bmod A_{n+1}$ for $n \geq 0$.

(4) $\deg h_n = \gamma_n - s$.

Suppose for the moment that sequences $\{g_n\}$ and $\{h_n\}$ satisfying properties 1, 2, 3 and 4 have been obtained. Then, by Theorem 4.13 $g_n \equiv g_{n+1} \bmod A_n$ implies $\{g_n\}$ converges uniformly to a function g which is expressed as a power series. Also, according to Corollary 4.15, $g \equiv g_n \bmod A_n$ for every n. This, in turn, implies $g \equiv g_n \bmod A_1$. In other words, $\overline{g} = \overline{g_n} = G$ for $n = 1,2,\ldots$. By Corollary 4.14, g is a monic polynomial of degree s. Similarly, $\{h_n\}$ converges to a power series h such that $\overline{h} = H$. Also, $\deg h_n = \gamma_n - s$ and $\deg g_n = s$ imply $\deg h_n g_n = \gamma_n$. Finally, by Theorem 4.12 if $g_n h_n \equiv f \bmod A_n$ then the sequence $\{g_n h_n\}$ converges to f. Thus, $gh = f$.

To begin the definition of the sequences $\{g_n\}$ and $\{h_n\}$ define the polynomials g_0 and h_0 by $g_0(x) = b_0 + b_1 x + \cdots + b_{s-1}x^{s-1} + x^s$ where the given polynomial in $O_p/A_1[x]$ is

$$G(x) = \overline{b_0} + \overline{b_1}x + \cdots + \overline{b_{s-1}}x^{s-1} + x^s$$

and

$$h_0(x) = c_0 + c_1 x + \cdots + c_t x^t$$

where

$$H(x) = \overline{c_0} + \overline{c_1}x + \cdots + \overline{c_t}x^t,$$

$\overline{c_t} \neq 0$. Clearly, $\overline{g_0} = G$, $\overline{h_0} = H$ and, since $\overline{f} = GH$, then

$f \equiv g_0h_0 \bmod A_1$. Since $\overline{f} = GH$, it follows that $\deg H = \deg \overline{f} - \deg G = \gamma_0 - s$. Therefore, since $\deg h_0 = \deg H$, $\deg h_0 = \gamma_0 - s$.

In order to obtain polynomials g_1 and h_1, consider the polynomial Q_1 consisting of the first $\gamma_1 + 1$ terms of the power series f, $Q_1(x) = a_0 + a_1x + \cdots + a_Nx^N$, where $N = \gamma_1$. Since $\gamma_1 \geq \gamma_0$, then $\overline{f} = \overline{Q_1}$. According to Lemma 4.17, there exists a unique pair of polynomials U_1, V_1 such that $Q_1 - g_0h_0 = U_1g_0 + V_1h_0$ with $\deg V_1 < s = \deg g_0$. Since $\overline{f} = \overline{g_0h_0}$, then $\overline{Q_1 - g_0h_0} = \overline{Q_1} - \overline{g_0h_0} = \overline{f} - \overline{g_0h_0} = 0$, so that $\overline{U_1g_0} + \overline{V_1h_0} = 0$. Since $\overline{g_0}$ and $\overline{h_0}$ are relatively prime, $\overline{U_1g_0} + \overline{V_1h_0} = 0$ implies either $\overline{U_1} = \overline{V_1} = 0$ or else $\overline{g_0} | \overline{V_1}$. If $\overline{g_0} | \overline{V_1}$, then $\deg \overline{g_0} \leq \deg \overline{V_1} \leq \deg V_1 < s = \deg g_0 = \deg \overline{g_0}$. This is a contradiction so that $\overline{U_1} = \overline{V_1} = 0$.

The polynomials g_1 and h_1 may now be defined as follows:

$$g_1 = g_0 + V_1 \quad \text{and} \quad h_1 = h_0 + U_1.$$

To see that property (1) for $n = 1$ is satisfied, note first that $\deg V_1 < s = \deg g_0$ implies $\deg g_1 = \deg(g_0 + V_1) = s$. Since g_0 is monic, g_1 is monic. Also, $\overline{V_1} = 0$ implies $g_1 \equiv g_0 \bmod A_1$ and that $\overline{g_1} = \overline{g_0} = G$.

Property (2) for $n = 1$ is easily shown since $\overline{U_1} = 0$ implies $\overline{h_1} = \overline{h_0} + \overline{U_1} = \overline{h_0} = H$ and also $h_1 \equiv h_0 \bmod A_1$.

To prove property (3) for $n = 1$, note that

$$\begin{aligned} g_1h_1 &= (g_0 + V_1)(h_0 + U_1) \\ &= g_0h_0 + U_1g_0 + V_1h_0 + V_1U_1 \\ &= Q_1 + V_1U_1. \end{aligned}$$

Since $U_1 \equiv 0 \bmod A_1$ and $V_1 \equiv 0 \bmod A_1$, then $U_1V_1 \equiv 0 \bmod A_2$. Therefore, $g_1h_1 \equiv Q_1 \bmod A_2$. Since $f \equiv Q_1 \bmod A_2$, it follows that

$$f \equiv g_1h_1 \bmod A_2.$$

It remains to be shown that $\deg h_1 = \gamma_1 - s$. Since $g_1h_1 = Q_1 + V_1U_1$, then

$$\deg g_1 + \deg h_1 \leq \max\{\deg Q_1, \deg V_1 + \deg U_1\}$$

or

$$s + \deg h_1 \leq \max\{\gamma_1, \deg V_1 + \deg U_1\}$$

with equality holding if $\gamma_1 \neq \deg V_1 + \deg U_1$. On the other hand, since $Q_1 = g_0h_0 + g_0U_1 + h_0V_1$ and $\deg Q_1 = \gamma_1$, then

$$\begin{aligned} \gamma_1 &\leq \max\{\deg g_0h_0, \deg g_0U_1, \deg h_0V_1\} \\ &= \max\{s + \gamma_0 - s, s + \deg U_1, \gamma_0 - s + \deg V_1\}. \end{aligned}$$

Since $\deg V_1 < s$, then $\gamma_1 \leq \max\{\gamma_0, s + \deg U_1\}$ with equality holding if $\gamma_0 \neq s + \deg U_1$.

Suppose $\gamma_0 > s + \deg U_1$. Then $\gamma_1 = \gamma_0$ and, since $s + \deg U_1 > \deg V_1 + \deg U_1$, it follows that $\gamma_1 > \deg V_1 + \deg U_1$ so that $s + \deg h_1 = \gamma_1$.

Suppose $\gamma_0 < s + \deg U_1$. Then $\gamma_1 = s + \deg U_1 > \deg V_1 + \deg U_1$ so that again $s + \deg h_1 = \gamma_1$.

Finally, if $\gamma_0 = s + \deg U_1$, then $\gamma_1 \leq \gamma_0$. Since, also, $\gamma_1 \geq \gamma_0$, then $\gamma_1 = \gamma_0 = s + \deg U_1 > \deg V_1 + \deg U_1$ so that again $s + \deg h_1 = \gamma_1$. Therefore, in all cases

$$\deg h_1 = \gamma_1 - s.$$

This completes the induction step for $n = 1$.

To complete the definition of the sequences $\{g_n\}$ and $\{h_n\}$, suppose polynomials $g_1, g_2, \ldots, g_n$ and $h_1, h_2, \ldots, h_n$ satisfying properties (1), (2), (3) and (4) have been constructed. Let $Q_{n+1}(x) = a_0 + a_1 x + \cdots + a_N x^N$ where $N = \gamma_{n+1}$ and consider $Q_{n+1} - g_n h_n \in O_p[x]$. By Lemma 4.17, there exist polynomials U_{n+1} and V_{n+1} in $O_p[x]$ such that $Q_{n+1} - g_n h_n = U_{n+1} g_n + V_{n+1} h_n$ with $\deg V_{n+1} < s$ or $V_{n+1} = 0$. By the induction hypothesis, $f \equiv g_n h_n \bmod A_{n+1}$ and by the definition of Q_{n+1}, $f \equiv Q_{n+1} \bmod A_{n+2}$. It follows that $Q_{n+1} - g_n h_n \equiv 0 \bmod A_{n+1}$ and, therefore, $U_{n+1} g_n + V_{n+1} h_n \equiv 0 \bmod A_{n+1}$. By Lemma 4.16, the images of g_n and h_n are relatively prime in $O_p/A_{n+1}[x]$. As in the proof of $\overline{U_1} = \overline{V_1} = 0$, it follows that $U_{n+1} \equiv 0 \bmod A_{n+1}$ and $V_{n+1} \equiv 0 \bmod A_{n+1}$.

Define $g_{n+1} = g_n + V_{n+1}$ and $h_{n+1} = h_n + U_{n+1}$. It remains to show that properties (1), (2), (3) and (4) hold.

Now $\deg V_{n+1} < s$ implies $\deg g_{n+1} = s$ and since g_n is monic, g_{n+1} is monic. Also, $V_{n+1} \equiv 0 \bmod A_{n+1}$ implies $g_{n+1} \equiv g_n \bmod A_{n+1}$ and $\overline{g_{n+1}} = \overline{g_n + V_{n+1}} = \overline{g_n} = G$. Thus, (1) is satisfied for $n + 1$. Similarly, $U_{n+1} \equiv 0 \bmod A_{n+1}$ implies $h_{n+1} \equiv h_n \bmod A_{n+1}$ and $\overline{h_{n+1}} = \overline{h_n + U_{n+1}} = \overline{h_n} = H$. This proves property (2).

To prove that $\deg h_{n+1} = \gamma_{n+1} - s$, note that

$$g_{n+1}h_{n+1} = (g_n + V_{n+1})(h_n + U_{n+1})$$
$$= Q_{n+1} + V_{n+1}U_{n+1}.$$

This implies

$$s + \deg h_{n+1} \leq \max\{\gamma_{n+1}, \deg V_{n+1} + \deg U_{n+1}\}$$

with equality if $\gamma_{n+1} \neq \deg V_{n+1} + \deg U_{n+1}$.

Thus, it suffices to show that $\gamma_{n+1} > \deg V_{n+1} + \deg U_{n+1}$. To see that this is the case, note that $Q_{n+1} = g_nh_n + g_nU_{n+1} + h_nV_{n+1}$ implies $\gamma_{n+1} \leq \max\{\gamma_n, s + \deg U_{n+1}\}$ with equality if $\gamma_n \neq \deg U_{n+1} + s$. With essentially the same arguments used in the case $n = 1$, it is seen that

$$\gamma_{n+1} \geq s + \deg U_{n+1} > \deg V_{n+1} + \deg U_{n+1}.$$

Therefore, $s + \deg h_{n+1} = \gamma_{n+1}$ so that property (4) is established for the case $n + 1$.

The proof of property (3) for $n + 1$ follows from

$$g_{n+1}h_{n+1} = Q_{n+1} + U_{n+1}V_{n+1}$$

since $U_{n+1} \equiv 0 \mod A_{n+1}$ and $V_{n+1} \equiv 0 \mod A_{n+1}$ imply $U_{n+1}V_{n+1} \equiv 0 \mod A_{n+2}$ so that $g_{n+1}h_{n+1} \equiv Q_{n+1} \mod A_{n+2}$. Since $Q_{n+1} \equiv f \mod A_{n+2}$, it follows that $f \equiv g_{n+1}h_{n+1} \mod A_{n+2}$.

This completes the definition by induction of the sequences $\{g_n\}$ and $\{h_n\}$ having properties (1), (2), (3) and (4). As indicated earlier, Hensel's Lemma now follows from Theorems 4.12 and 4.13 and its corollaries.

Zeros of a Power Series

The next objective of this chapter is to locate as far as possible the zeros of certain power series. As in complex analysis, if $x = a$ is a zero of $f(x)$, then there is a positive integer m such that

$$f(x) = (x - a)^m \sum_{n=m}^{\infty} b_n (x - a)^{n-m}$$

where $b_m \neq 0$. Thus, it suffices to consider the zeros of a power series of the form

$$\sum_{n=0}^{\infty} b_n (x - a)^n$$

where $b_0 \neq 0$.

Also, since

$$f(x) = \sum_{n=0}^{\infty} b_n (x - a)^n$$

has a zero at $x = x_0$ if and only if

$$F(x) = \sum_{n=0}^{\infty} b_n x^n$$

has a zero at $x = x_0 - a$, only power series of the form

$$\sum_{n=0}^{\infty} b_n x^n$$

with $b_0 \neq 0$ need to be considered.

The next result applies to any convergent power series with coefficients in Q_p. It provides a sufficient condition for a power series to have no zeros on a given circle.

Theorem 4.22. Suppose

$$f(x) = \sum_{n=0}^{\infty} b_n x^n$$

has a non-zero radius of convergence, $b_n \in Q_p$ and $b_0 \neq 0$. Suppose, also, that line L with slope m is a lower support line of the Newton diagram T. If L contains exactly one point of T, then $f(x)$ has no zeros on the circle $C_{-m} = \{x \in T_p\colon |x| = p^m\}$.

Proof: Let $A_j = (j, \text{ord } b_j)$ be the point of T on L. Then the equation of L is $y = mx + \text{ord } b_j - mj$. To prove that $f(x)$ has no zeros on C_{-m} suppose $x_0 \in C_{-m}$ so that $\text{ord } x_0 = -m$. Since $\text{ord } b_j x_0^j = \text{ord } b_j + j \text{ ord } x_0$, the equation for line L can be written as $y = (-\text{ord } x_0)x + \text{ord } b_j x_0^j$. Since A_j is the only point of the Newton diagram on L, then for $n \neq j$, $\text{ord } b_n > (-\text{ord } x_0)n + \text{ord } b_j x_0^j$. Thus, $\text{ord } b_n x_0^n > \text{ord } b_j x_0^j$ for all $n \neq j$. This implies $|b_n x_0^n| < |b_j x_0^j|$ for all $n \neq j$ which in turn implies

$$\left| \sum_{n=0}^{\infty} b_n x_0^n \right| = \left| b_j x_0^j \right|.$$

Since $A_j \in T$ implies $|b_j| \neq 0$ and $x_0 \in C_{-m}$ implies $x_0^j \neq 0$, it follows that $|f(x_0)| = |b_j x_0^j| \neq 0$. Thus, if there is exactly one point of T on L, then no point of C_{-m} is a zero of $f(x)$.

By applying Theorem 4.22, it may be quite easy to show that $f(x) = b_0 + b_1 x + \cdots + b_n x^n \in Q_p[x]$ has no zeros in Q_p. Since p^m is in the value group of Q_p if and only if m is a rational integer, it follows that f has zeros in Q_p only if the Newton polygon has a side having rational integral slope. Thus, $px^2 - 1$ has no roots in Q_p for any p since the slope of the only segment in the Newton polygon is $1/2$ and $p^{1/2}$ is not in the value group of Q_p.

A similar application of Theorem 4.22 settles the question of whether T_p is a discrete non-archimedean field.

Theorem 4.23. Let T_p be a complete non-archimedean field which is an algebraic closure of Q_p. Then the value group V of T_p is not a cyclic group.

Proof: Suppose T_p is discrete. Then there is a real number π with $0 < \pi < 1$ such that π generates the value group V. Then $1 < 1/\pi$ so that $0 < \log_p(1/\pi) = -\log_p \pi$. Choose a positive integer k such that $0 < 1/k < -\log_p \pi$. Consider the polygon $f(x) = px^k - 1$ so that the Newton diagram for $f(x)$ has two points $(0,0)$ and $(k,1)$, and the only side has slope $1/k$. Since T_p is algebraically closed, $f(x)$ has k zeros in T_p and, in view of Theorem 4.22, all are on the circle $C_{-1/k} = \{x \in T_p : |x| = p^{1/k}\}$. A contradiction will be obtained by showing that $p^{1/k}$ is not in the value group V.

Suppose $p^{1/k}$ is in V. Then there is a rational integer j such that $p^{1/k} = \pi^j$. Then $1/k = j \log_p \pi$ and, since $1/k > 0$ and $\log_p \pi < 0$, this implies $j < 0$. On the other hand, $1/k < -\log_p \pi$ implies $j \log_p \pi < -\log_p \pi$ so that $j > -1$. In view of this contradiction, it follows that T_p is not a discrete non-archimedean field.

By an argument similar to the above, it can be shown that the value group of T_p must include at least the set $\{p^r : r$ is a rational number$\}$.

The final objective of this chapter is to prove an analogue of Weierstrass' Factorization Theorem. Several lemmas and theorems are needed first.

The first of these shows that under suitable conditions a power series over Q_p can be transformed into a power series f_1 over 0_p such that $\overline{f_1}$ is a polynomial.

<u>Lemma</u> 4.24. Let

$$f(x) = \sum_{n=0}^{\infty} b_n x^n$$

be a power series over 0_p with $b_0 \neq 0$ and having radius of convergence $\rho \neq 0$. If L is a lower support line containing a side $\overline{B_N B_{N+1}}$ of the Newton polygon for f, then there is a power series

$$f_1(x) = \sum a_n x^n$$

over 0_p such that

$$\overline{f_1}(x) = \overline{a_j} x^j + \overline{a_{j+1}} x^{j+1} + \cdots + x^{j+s}$$

with $\overline{a_j} \neq 0$.

Proof: Let L be the line of slope m containing the given side of the Newton polygon. Let $A_j = (j, \text{ord } b_j) = B_N$ and $A_k = (k, \text{ord } b_k) = B_{N+1}$. If $x_0 \in C_{-m}$, then, as in the proof of Theorem 4.22, $\text{ord } b_k = (-\text{ord } x_0)k + \text{ord } b_j x_0^j$. It follows that $\text{ord } b_k x_0^k = \text{ord } b_j x_0^j$. Also, since L is a lower line of support, $\text{ord } b_n \geq (-\text{ord } x_0)n + \text{ord } b_j x_0^j$ for every $n = 0,1,2, \ldots$ so that $\text{ord } b_n x_0^n \geq \text{ord } b_k x_0^k$ for every $n = 0,1,2, \ldots$.

Define the power series f_1 by

$$f_1(x) = b_k^{-1} x_0^{-k} f(x_0, x) = \sum_{n=0}^{\infty} a_n x^n,$$

that is,

$$a_n = \frac{b_n x_0^n}{b_k x_0^k} .$$

The following observations show that the lemma has been established.

1. For every $n \geq 0$, $\text{ord } a_n \geq 0$ so that $a_n \in 0_p$.

2. The coefficient $a_k = 1$ so that $\overline{a_k} = 1$.

3. Since $\text{ord } a_j = \text{ord } b_j x_0^j - \text{ord } b_k x_0^k = 0$, then $\overline{a_j} \neq 0$.

4. If $0 \leq n < j$ or $n > k$, then $\text{ord } a_n > 0$ so that $\overline{a_n} = 0$ for $0 \leq n < j$ or $n > k$.

<u>Corollary</u> 4.25. There is a one-to-one correspondence between the zeros of f on C_{-m} and the zeros of f_1 on C_0.

Proof: According to the way in which f_1 is defined, $x \in C_{-m}$ is a zero of f if and only if xx_0^{-1} is a zero of f_1 on C_0.

The next lemma shows that for a given power series f over O_p there is a polynomial g such that all the zeros of f on C_0 are also zeros of g.

<u>Lemma</u> 4.26. Suppose

$$f(x) = \sum_{n=0}^{\infty} a_n x^n$$

is a power series over O_p such that $a_n \equiv 0 \bmod p$ for $0 \leq n \leq j-1$, a_j is a unit in O_p, $a_k \not\equiv 0 \bmod p$ and $a_n \equiv 0$ for $n > k = j + s$. Then f has s zeros on the unit circle C_0.

Proof: Consider

$$\begin{aligned}\overline{f}(x) &= \overline{a_j}x^j + \overline{a_{j+1}}x^{j+1} + \cdots + x^k \\ &= x^j(\overline{a_j} + \overline{a_{j+1}}x + \cdots + x^s).\end{aligned}$$

and apply Hensel's Lemma. Let $G(x) = \overline{a_j} + \overline{a_{j+1}}x + \cdots + x^s$ and $H(x) = x^j$. Since $a_j \not\equiv 0 \bmod p$, $\overline{a_j} \neq 0$ so that the polynomials G and H are relatively prime. Furthermore, since $\overline{f} = GH$, all the hypotheses of Hensel's Lemma are satisfied. Therefore, there exist a monic polynomial $g \in O_p[x]$ of degree $k - j = s$ and a power series h such that $\overline{g} = G$, $\overline{h} = H$ and the power series $f = gh$.

Suppose $g(x) = c_0 + c_1(x) + \cdots + c_{s-1}x^{s-1} + x^s$. Then $\overline{g} = G$ implies $\overline{c_0} = \overline{a_j} \neq 0$. It will be shown that the only zeros of the power series $f(x)$ on the unit circle C_0 are also zeros of the polynomial g. Let

$$h(x) = \sum_{n=0}^{\infty} c_n x^n.$$

Then $\overline{h}(x) = x^j$ implies ord $c_j = 0$ and ord $c_n > 0$ for every $n \neq j$. Thus, the x-axis is a lower support line containing exactly one point of the Newton diagram for the power series $h(x)$. Then, according to Theorem 4.22, the power series $h(x)$ has no zero on C_0. Therefore, the original power series $f(x)$ and the polynomial $g(x)$ have exactly the same zeros on the unit circle C_0.

Since T_p is algebraically closed, the polynomial g has s zeros in T_p. Let α be a zero of g. It will be shown that $|\alpha| = 1$. Suppose otherwise, that is, suppose $|\alpha| \neq 1$. If $|\alpha| < 1$, then, since $g \in O_p[x]$ with $|c_0| = 1$,

$$\begin{aligned} |g(\alpha)| &= \max\{|c_0|, |c_1\alpha + \cdots + \alpha^s|\} \\ &= |c_0| = 1 \neq 0. \end{aligned}$$

On the other hand, if $|\alpha| > 1$, then $|g(\alpha)| = |\alpha|^s \neq 0$. It follows that all zeros of g are on C_0 and, therefore, the power series f has s zeros on the unit circle C_0.

The results of the preceeding lemmas can be used to show that a power series has only finitely many zeros inside a given circle within the circle of convergence.

Theorem 4.27. Let

$$f(x) = \sum_{n=0}^{\infty} b_n x^n$$

be a power series over Q_p with radius of convergence $\rho \neq 0$. If $m^* < \log_p \rho$, then f has finitely many zeros, $\alpha_1, \alpha_2, \ldots, \alpha_k$ inside or on C_{-m^*}. Furthermore, there is a power series h such that

$$f(x) = \prod_{i=1}^{k} (x - \alpha_i)h(x)$$

where h has radius of convergence ρ.

Proof: Let m be a slope of a side such that $m \leq m^*$. By the Corollary 4.25, there is a power series f_1 such that f_1 has the same number of zeros on C_0 as there are zeros of f on C_{-m}. By Lemma 4.26, there are only a finite number of zeros of f_1 on C_0. Thus, for each $m \leq m^*$, the set of zeros of f on C_{-m} is finite. Since $m^* < \log_p \rho$, there are only a finite number of sides having slopes less than m^*. It follows that there are only finitely many zeros of f inside or on the circle C_{-m^*}.

To prove the second part, note that if α is a zero on C_{-m} of the power series f, then the power series given by

$$h_1(x) = \sum_{n=0}^{\infty} a_n x^n$$

where

$$a_0 = -\frac{b_0}{\alpha}$$

$$a_1 = -\left(\frac{b_1}{\alpha} + \frac{b_0}{\alpha^2}\right)$$

$$\vdots$$

$$a_n = -\left(\frac{b_n}{\alpha} + \frac{b_{n-1}}{\alpha^2} + \cdots + \frac{b_0}{\alpha^{n+1}}\right)$$

is such that $f(x) = (x - \alpha)h_1(x)$ where h_1 has radius of convergence ρ. Similarly, there is a power series h_2 such that if β is a zero of h_1 then $h_1(x) = (x - \beta)h_2(x)$ so that $f(x) = (x - \alpha)(x - \beta)h(x)$. It follows by induction that if $\{\alpha_1, \alpha_2, \ldots, \alpha_k\}$ is the set of zeros of f inside or on C_{-m^*}, then

$$f(x) = \prod_{i=1}^{k} (x - \alpha_i)h(x)$$

where h has no zeros inside or on C_{-m} and h has radius of convergence ρ.

<u>Theorem</u> 4.28. If

$$f(x) = \sum_{n=0}^{\infty} b_n x^n$$

with radius of convergence $\rho \neq 0$ has no zeros inside or on the circle C_{-m}, then the function $f_1(x) = \frac{1}{f(x)}$ is analytic inside C_{-m}.

Proof: Without loss of generality, assume $b_0 = 1$. It can be shown that

$$f_1(x) = \sum_{n=0}^{\infty} a_n x^n$$

where

$$a_0 = 1$$

$$a_1 = -b_1$$

$$a_2 = -b_2 + b_1^2$$

$$a_3 = -b_3 + 2b_1b_2 - a_1^3$$

$$\vdots$$

$$a_n = \sum_k (-1)^k \sum b_{i_1} b_{i_2} \cdots b_{i_k},$$

the second sum taken over all subscripts such that $i_1 + i_2 + \cdots + i_k = n$.

In order to show that the radius of convergence is at least ρ, it suffices to show that

$$\frac{\text{ord } a_n}{n} > m$$

for every n. Equivalently, it suffices to show that $|a_n| < p^{-nm}$ for every n. Now

$$\left| a_n \right| \leq \max\left\{ \left| b_{i_1} b_{i_2} \cdots b_{i_k} \right| : i_1 + i_2 + \cdots + i_k = n \right\}.$$

Since f has no zeros inside or on the circle C_{-m}, then the Newton polygon has no side with slope less than or equal to m. Therefore,

$$\frac{\text{ord } b_j}{j} > m$$

for every j so that $|b_j| < p^{-jm}$ for every j. Thus, if $i_1 + \cdots + i_k = n$, then

$$\left| b_{i_1} b_{i_2} \cdots b_{i_k} \right| < p^{-i_1 m} p^{-i_2 m} \cdots p^{-i_k m} = p^{-nm}$$

so that $|a_n| < p^{-nm}$ as required. This completes the proof.

Definition 4.29. If the radius of convergence of an analytic function f is infinite, then f is an entire function.

The next theorem shows that the only entire functions having no zeros in T_p are constant functions.

Theorem 4.30. If f is an entire function having no zeros, then f is a constant function.

Proof: Suppose

$$f(x) = \sum_{n=0}^{\infty} b_n x^n.$$

Since f has no zeros, then for any m there is no side of the Newton polygon having slope less than or equal to m. It follows that the only possible side is a terminal ray which is vertical. Thus, there is only one non-zero coefficient in the power series and, since f has no zeros, that coefficient must be b_0.

In contrast to the above theorem, there exist non-constant functions which have no zeros. The exponential series of Example 4.3 is not an entire function since its radius of convergence is $p^{-1/(p-1)}$. It can be shown that

$$\exp(x) = \sum_{n=0}^{\infty} \frac{1}{n!} x^n$$

has no zeros in T_p. To see this, consider the line L with equation $y = \frac{-1}{p-1} x$. Since

$$\text{ord}\,\frac{1}{n!} = -\left(\frac{n - t_n}{p - 1}\right) = -\frac{n}{p - 1} + \frac{t_n}{p - 1},$$

it follows that $\text{ord}\,\frac{1}{n!} > \frac{-1}{p - 1}n$ for every $n > 0$. Thus, $(0,0)$ is the only point of T on L and, by Theorem 4.22, there are no zeros of $\exp(x)$ on the circle $C_{-m} = \{x \in T_p : |x| = p^m\}$ where $m = -1/(p - 1)$. By the same theorem, there are no zeros on any circle of smaller radius, and since the series fails to converge at every point x such that $|x| > p^{-1/(p-1)}$, it follows that

$$\sum_{n=0}^{\infty} \frac{1}{n!} x^n$$

has no zeros in T_p.

Weierstrass' Factorization Theorem

Finally, the major result of this section can be established. The following theorem, which may be considered as an analogue of Weierstrass' Factorization Theorem of complex analysis, shows that an entire function can be expressed as the product of linear factors involving all its zeros. Also, given a sequence of points in T_p whose valuations tend to infinity, there is an entire function having precisely those points as zeros.

Theorem 4.31. Let

$$f(x) = \sum b_n x^n,$$

$b_n \in Q_p$ be an entire function. If f has infinitely many zeros which are different from zero, say $\alpha_1, \alpha_2, \ldots, \alpha_n, \ldots,$ then

$$f(x) = A_0 x^k \prod_{i=1}^{\infty} \left(1 - \frac{x}{\alpha_i} \right)$$

where the infinite product converges uniformly in every bounded subset of T_p, and A_0 is a constant in T_p.

Conversely, if $\{\alpha_n\}$ is a sequence of non-zero elements of T_p such that $\lim |\alpha_n| = \infty$, then there is an entire function ϕ having zeros at each α_n such that

$$\phi(x) = \prod_{i=1}^{\infty} \left(1 - \frac{x}{\alpha_i} \right).$$

Proof: The second part will be established first. Let $\{\alpha_n\}$ be any sequence of non-zero elements in T_p such that $\{|\alpha_n|\}$ is monotonic increasing and $\lim |\alpha_n| = \infty$. It will be established that

$$\prod_{i=1}^{\infty} \left(1 - \frac{x}{\alpha_i} \right)$$

defines an entire function having zeros at each α_n. It will be shown first that the sequence of partial products,

$$\left\{ \prod_{i=1}^{N} \left(1 - \frac{x}{\alpha_i} \right) \right\},$$

converges uniformly to a function $\phi(x)$ in a bounded set $S \subset D_r = \{x \in T_p : |x| \leq r\}$. Let

$$\phi_N(x) = \prod_{i=1}^{N} \left(1 - \frac{x}{\alpha_i} \right) = \frac{(-1)^N}{\alpha_1 \alpha_2 \cdots \alpha_N} \prod_{i=1}^{N} (x - \alpha_i)$$

so that

$$\phi_N(x) = \frac{(-1)^N}{\alpha_1\alpha_2 \cdots \alpha_N}\left[x^N - \sigma_1 x^{N-1} + \cdots + (-1)^N \sigma_N\right]$$

where $\sigma_1, \sigma_2, \ldots, \sigma_N$ are the elementary symmetric functions. The above expression for $\phi_N(x)$ can be written as

$$\phi_N(x) = a_{0,N} + a_{1,N}x + \cdots + a_{N,N}x^N$$

where

$$a_{k,N} = \frac{(-1)^{N-k}\sigma_{N-k}}{\alpha_1\alpha_2 \cdots \alpha_N} .$$

In view of the way the symmetric functions are defined, it follows that

$$a_{k,N} = (-1)^{N-k} \sum \frac{1}{\alpha_{i_1}\alpha_{i_2} \cdots \alpha_{i_k}} ,$$

the sum taken over k subscripts $i_1, \ldots, i_k$ such that $1 \leq i_1 < i_2 < \cdots < i_k \leq N$. It will be shown that the sequence

$$\left\{ a_{k,N} \right\}_{N=1}^{\infty}$$

converges for each k. To see this, note that

$$\left| a_{k,N+1} - a_{k,N} \right| = \left| \frac{1}{\alpha_{N+1}} \sum \frac{1}{\alpha_{i_1}\alpha_{i_2} \cdots \alpha_{i_{k-1}}} \right| ,$$

the sum taken over $k - 1$ subscripts such that $1 \leq i_1 < \cdots < i_{k-1} \leq N$. Then, since $\{|\alpha_n|\}$ is an increasing sequence,

$$\left| a_{k,N+1} - a_{k,N} \right| \leq \left| \frac{1}{\alpha_{N+1}(\alpha_1\alpha_2 \cdots \alpha_{k-1})} \right| .$$

It follows that for each $k > 0$, $\displaystyle\lim_{N \to \infty} |a_{k,N+1} - a_{k,N}| = 0$ so that the sequence

$$\left\{ a_{k,N} \right\}_{N=1}^{\infty}$$

converges. Let $a_k = \displaystyle\lim_{N \to \infty} a_{k,N}$ for $k > 0$ and let $a_0 = 1$.

It will be shown that the power series given by

$$\sum_{k=0}^{\infty} a_k x^k$$

defines an entire function $\phi(x)$ by showing that

$$\lim_{k \to \infty} \frac{\text{ord } a_k}{k} = \infty.$$

Since $\lim |\alpha_n| = \infty$, then there are finitely many α_n inside the unit circle. Let $\{\alpha_1, \alpha_2, \ldots, \alpha_t\}$ be the set of all α_n such that $|\alpha_n| \leq 1$. Pick $j > t$ such that

$$\left| \frac{1}{\alpha_{t+1} \cdots \alpha_j} \right| < \left| \alpha_1 \cdots \alpha_t \right|$$

Then, for $k > j$,

$$\left|a_{k,N}\right| \leq \left|\frac{1}{\alpha_1\alpha_2 \cdots \alpha_k}\right| = \left|\frac{1}{\alpha_1 \cdots \alpha_t}\right| \left|\frac{1}{\alpha_{t+1} \cdots \alpha_t}\right| \left|\frac{1}{\alpha_{j+1} \cdots \alpha_k}\right|$$

$$< \left|\frac{1}{\alpha_{j+1} \cdots \alpha_k}\right| \leq \left|\frac{1}{\alpha_{j+1}}\right|^{k-j}.$$

Since $a_k = \underset{N \to \infty}{\text{limit}}\, a_{k,N}$,

$$\left|a_k\right| \leq \left|\frac{1}{\alpha_{j+1}}\right|^{k-j}$$

so that

$$\log_p\left|a_k\right| \leq (k - j)\log_p \frac{1}{\left|\alpha_{j+1}\right|}.$$

Since $\text{ord } a_k = -\log_p\left|a_k\right|$, it follows that $\text{ord } a_k \geq (k - j)\log_p\left|\alpha_{j+1}\right|$ and, therefore,

$$\frac{\text{ord } a_k}{k} \geq \frac{(k - j)}{k} \log_p\left|\alpha_{j+1}\right|.$$

Now, as $k \to \infty$, the right hand side approaches $\log_p\left|\alpha_{j+1}\right|$. And, since j can be chosen so that $\log_p\left|\alpha_{j+1}\right|$ is arbitrarily large, it follows that

$$\underset{k \to \infty}{\text{limit}} \frac{\text{ord } a_k}{k} = \infty.$$

Therefore, $\phi(x)$ is an entire function.

Since $\alpha_1, \alpha_2, \ldots, \alpha_N$ are the zeros of ϕ_N, it follows that ϕ has zeros at α_n for every n.

To complete the proof of the first part of the theorem, it must be shown that the convergence is uniform on each bounded set in T_p. It suffices to show that, given any $\epsilon > 0$, then, for sufficiently large

N, $|\phi_{N+1}(x) - \phi_N(x)| < \epsilon$ for each $x \in S$. Now

$$\left|\phi_{N+1}(x) - \phi_N(x)\right| = \left|\phi_N(x)\right| \left|\frac{x}{\alpha_{N+1}}\right|$$

$$\leq \left|\phi_N(x)\right| \frac{r}{|\alpha_{N+1}|}$$

for each $x \in S$. Since

$$\frac{r}{|\alpha_{N+1}|}$$

approaches zero as N approaches ∞, it suffices to show the existence of an M such that, for sufficiently large N, $|\phi_N(x)| \leq M$ for each $x \in S$. As before, for some fixed but sufficiently large j,

$$\left|a_{k,N}\right| \leq \left|\frac{1}{\alpha_{j+1}}\right|^{k-j}$$

whenever $k > j$. This implies

$$|a_{k,N}x^k| \leq |a_{k,N}|r^k \leq \frac{r^k}{|\alpha_{j+1}|^{k-j}}$$

for each $x \in S$. It follows that for sufficiently large k, say $k > k_0$, $|a_{k,N}x^k| < 1$ for each $x \in S$. Thus,

$$\left|\sum_{k=k_0+1}^{N} a_{k,N}x^k\right| \leq 1$$

for each $x \in S$ and every $N > k_0$. Let M' be an upper bound of $|a_{0,N} + a_{1,N}x + \cdots + a_{k_0,N}x^{k_0}|$ for $x \in S$. Finally, let

$M = \max\{M', 1\}$. Then

$$\left| \phi_N(x) \right| \leq \left| \sum_{k=0}^{k_0} a_{k,N} x^k + \sum_{k=k_0+1}^{N} a_{k,N} x^k \right|$$

$$< \max\{M', 1\} = M,$$

for each $x \varepsilon S$. Therefore, ϕ_N converges uniformly to ϕ on S. This completes the proof of the second part of Theorem 4.31.

To prove the first part, recall that an analytic function can have only finitely many zeros inside any disc $D_r = \{x \varepsilon T_p: |x| \leq r\}$. Therefore, it may be assumed that the infinite set of zeros can be ordered such that $\{|\alpha_n|\}$ is monotonic increasing with $\lim |\alpha_n| = \infty$.

Let $\{\alpha_1, \alpha_2, \ldots, \alpha_j\}$ be the set of zeros of f in D_r different from zero. Then, if f has $\alpha = 0$ as a zero of multiplicity k,

$$f(x) = x^k \prod_{i=1}^{j} (x - \alpha_i) h(x)$$

where $h(x)$ is an entire function having no zeros in D_r. By Theorem 4.28, the function $\frac{1}{h}$ is analytic inside D_r. Let $h_1(x) = (-1)^j \alpha_1 \alpha_2 \ldots \alpha_j h(x)$. Then

$$f(x) = x^k \prod_{i=1}^{j} \left(1 - \frac{x}{\alpha_i}\right) h_1(x)$$

and $h_1(x)$ is an analytic function having no zeros in D_r.

Let f_1 be the function given by

$$f_1(x) = x^k \prod_{i=1}^{\infty} \left(1 - \frac{x}{\alpha_i}\right).$$

Then f_1/f can be represented as

$$\frac{f_1}{f}(x) = \frac{\prod_{i=j+1}^{\infty}\left(1 - \frac{x}{\alpha_i}\right)}{h_1(x)} .$$

Now both

$$g(x) = \prod_{i=j+1}^{\infty}\left(1 - \frac{x}{\alpha_i}\right) \quad \text{and} \quad h_1(x)$$

are analytic inside D_r and neither has zeros there. Thus, f_1/f is analytic inside D_r and has no zeros there. Since f_1/f is independent of r, it follows that f_1/f is an entire function having no zeros in T_p. By Theorem 4.30, f_1/f is a non-zero constant function, say $1/A_0$. Thus,

$$f(x) = A_0 x^k \prod_{i=1}^{\infty}\left(1 - \frac{x}{\alpha_i}\right)$$

as required.

CHAPTER V

SOME p-ADIC ANALOGUES

The field T_p was developed in Chapter III as a complete non-archimedean field which is an algebraic closure of the p-adic field Q_p. Since this relationship between T_p and Q_p resembles the relationship between the complex field C and the real field R, it seems reasonable to consider analogues of some concepts from complex analysis. Some of these were developed in Chapter IV. The first objective of this chapter is to develop the Schnirelman Integral, a p-adic analogue of the complex line integral. With the aid of the Schnirelman integral analogues of standard results such as the Cauchy Integral Formula, and the Maximum Modulus Principle can be formulated.

For each positive integer n such that $p \neq n$, consider the polynomial $g_n(x) = x^n - 1$. Since T_p is algebraically closed, g_n can be factored into n linear factors

$$g_n(x) = (x - \alpha_{1,n})(x - \alpha_{2,n}) \cdots (x - \alpha_{n,n}).$$

It is easy to show that $|\alpha_{i,n}| = 1$ for $i = 1,2,3, \ldots, n$. To see this, note that $g(\alpha_{i,n}) = 0$ implies $|\alpha_{i,n}^n - 1| = 0$. On the other hand, if $|\alpha_{i,n}^n| \neq 1$, then $|\alpha_{i,n}^n - 1| = \max\{|\alpha_{i,n}^n|, 1\} \neq 0$. It follows that $|\alpha_{i,n}| = 1$.

The next definition is analogous to determining n complex numbers equally spaced around a circle in the complex plane.

Definition 5.1. Let β and δ be fixed points in T_p and $\alpha_{1,n}, \ldots, \alpha_{n,n}$ be the zeros of $x^n - 1$. The set

$$\{\beta + \delta\alpha_{1,n}, \beta + \delta\alpha_{2,n}, \ldots, \beta + \delta\alpha_{n,n}\}$$

is called the discrete circle with center β and radius $r = |\delta|$. The discrete circle is denoted by $C(\beta,\delta,n)$.

It is clear that the discrete circle $C(\beta,\delta,n)$ is a finite set of points on the ordinary circle $C(\beta,|\delta|)$ in T_p. Since T_p is a non-archimedean field, the center of $C(\beta,|\delta|)$ is not unique. On the other hand, the following lemma shows that the center of a discrete circle is unique.

Lemma 5.2. Suppose $|\beta_1 - \beta_2| < |\delta|$ with $\beta_1 \neq \beta_2$. Then $C(\beta_1,\delta,n) \neq C(\beta_2,\delta,n)$.

Proof: Suppose to the contrary that $C(\beta_1,\delta,n) = C(\beta_2,\delta,n)$. Then for each $i = 1,2, \ldots, n$ there is some j such that $\beta_1 + \delta\alpha_{i,n} = \beta_2 + \delta\alpha_{j,n}$. Thus, $\beta_1 - \beta_2 = \delta(\alpha_{j,n} - \alpha_{i,n})$ so that $|\beta_1 - \beta_2| = |\delta||\alpha_{j,n} - \alpha_{i,n}|$. Since $|\beta_1 - \beta_2| < |\delta|$, it follows that $|\alpha_{j,n} - \alpha_{i,n}| > 1$. But $|\alpha_{j,n} - \alpha_{i,n}| \leq \max\{|\alpha_{j,n}|,|\alpha_{i,n}|\} = 1$. This contradiction shows that the discrete circles $C(\beta_1,\delta,n)$ and $C(\beta_2,\delta,n)$ are distinct subsets of $C(\beta,|\delta|)$ whenever $\beta_1 \neq \beta_2$.

The Schnirelman Integral

Definition 5.3. Suppose for each n such that $p \nmid n$ the function f is defined on the discrete circle $C(\beta,\delta,n)$. Then $\int_{\beta,\delta} f$ is defined by

$$\int_{\beta,\delta} f = \lim_{\substack{n \to \infty \\ p \nmid n}} \frac{1}{n} \sum_{i=1}^{n} f(\beta + \delta\alpha_{i,n})$$

provided this limit exists. When $\int_{\beta,\delta} f$ exists, it is called the <u>Schnirelman integral</u> of the function f on the circle $C(\beta,|\delta|)$.

The next theorem shows that the Schnirelman Integral exists for a constant function.

<u>Theorem</u> 5.4. If $f(x) = c$ for every x on $C(\beta,|\delta|)$ then $\int_{\beta,\delta} f = c$.

Proof: Since $\sum_{i=1}^{n} c = nc$ implies $\frac{1}{n} \sum_{i=1}^{n} c = c$, it follows that

$$\int_{\beta,\delta} f = \lim_{\substack{n \to \infty \\ p \nmid n}} \frac{1}{n} \sum_{i=1}^{n} f(\beta + \delta\alpha_{i,n}) = \lim_{\substack{n \to \infty \\ p \nmid n}} c = c.$$

Henceforth,

$$\lim_{\substack{n \to \infty \\ p \nmid n}} \frac{1}{n} \sum_{i=1}^{n} f(\beta + \delta\alpha_{i,n})$$

will be written simply as

$$\lim \frac{1}{n} \sum_{i=1}^{n} f(\beta + \delta\alpha_{i,n})$$

or, by letting $\gamma_{i,n} = \beta + \delta\alpha_{i,n}$, as

$$\lim \frac{1}{n} \sum_{i=1}^{n} f(\gamma_{i,n}).$$

Sometimes a translation is helpful.

Theorem 5.5. If $g(x) = f(x + \beta)$, then

$$\int_{\beta,\delta} f = \int_{0,\delta} g.$$

Proof: This follows immediately since

$$\int_{\beta,\delta} f = \lim \frac{1}{n} \sum f(\beta + \delta\alpha_{i,n})$$
$$= \lim \frac{1}{n} \sum g(\delta\alpha_{i,n}) = \int_{0,\delta} g.$$

The following theorem shows that the Schnirelman Integral has a linearity property expected of an integral.

Theorem 5.6. Suppose f and g are functions such that $\int_{\beta,\delta} f$ and $\int_{\beta,\delta} g$ exist. If c_1 and c_2 are constants in T_p, then

$$\int_{\beta,\delta} (c_1 f + c_2 g)$$

exists and equals

$$c_1 \int_{\beta,\delta} f + c_2 \int_{\beta,\delta} g.$$

Proof: It suffices to show each of the following separately:

a) If c is a constant, then $\int_{\beta,\delta} c\ f = c \int_{\beta,\delta} f$; and

b) $$\int_{\beta,\delta} f + g = \int_{\beta,\delta} f + \int_{\beta,\delta} g.$$

Part (a) follows from

$$\lim \frac{1}{n} \sum_{i=1}^{n} cf(\gamma_{i,n}) = c \lim \frac{1}{n} \sum_{i=1}^{n} f(\gamma_{i,n})$$

where $\gamma_{i,n} = \beta + \delta\alpha_{i,n}$. Similarly,

$$\frac{1}{n} \sum_{i=1}^{n} (f + g)(\gamma_{i,n}) = \frac{1}{n} \sum_{i=1}^{n} f(\gamma_{i,n}) + \frac{1}{n} \sum_{i=1}^{n} g(\gamma_{i,n})$$

and, since the Schnirelman integrals of both f and g exist, part (b) is established. This completes the proof of the theorem.

Corollary 5.7. If $c_1, c_2, \ldots, c_k$ are constants in T_p and $\int_{\beta,\delta} f_i$ exist for $i = 1,2, \ldots, k$, then

$$\int_{\beta,\delta} \sum_{i=1}^{k} c_i f_i = \sum_{i=1}^{k} c_i \int_{\beta,\delta} f_i.$$

Proof: The proof is by induction and the above theorem.

The next theorem shows that the Schnirelman integral of a polynomial is quite easy to evaluate. In fact, the integral of a polynomial is simply the value of that polynomial at the center of the circle.

Theorem 5.8. If $f(x) = a_0 + a_1 x + \cdots + a_k x^k$ is a polynomial with coefficients in T_p then for any β and δ in T_p

$$\int_{\beta,\delta} f = \int_{\beta,\delta} a_0 + a_1 x + \cdots + a_k x^k = a_0 + a_1\beta + \cdots + a_k\beta^k.$$

Proof: In view of the preceding corollary and the fact the Schnirelman Integral of a constant is that constant, it suffices to show that $\int_{\beta,\delta} x^k = \beta^k$ for each positive integer k.

Consider

$$\lim \frac{1}{n} \sum_{i=1}^{n} f(\gamma_{i,n}) = \lim \frac{1}{n} \sum_{i=1}^{n} (\beta + \delta\alpha_{i,n})^k$$

$$= \lim \frac{1}{n} \Big[(\beta + \delta\alpha_{1,n})^k + (\beta + \delta\alpha_{2,n})^k + \cdots + (\beta + \delta\alpha_{n,n})^k \Big].$$

Now

$$(\beta + \delta\alpha_{1,n})^k + (\beta + \delta\alpha_{2,n})^k + \cdots + (\beta + \delta\alpha_{n,n})^k$$

$$= \beta^k + \binom{k}{1}\beta^{k-1}\delta\alpha_{1,n} + \cdots + \binom{k}{k}\delta^k\alpha_{1,n}^k +$$

$$\beta^k + \binom{k}{1}\beta^{k-1}\delta\alpha_{2,n} + \cdots + \binom{k}{k}\delta^k\alpha_{2,n}^k +$$

$$\vdots$$

$$\beta^k + \binom{k}{1}\beta^{k-1}\delta\alpha_{n,n} + \cdots + \binom{k}{k}\delta^k\alpha_{n,n}^k$$

$$= n\beta^k + \binom{k}{1}\beta^{k-1}\delta \sum_{i=1}^{n} \alpha_{i,n} + \binom{k}{2}\beta^{k-2}\delta^2 \sum_{i=1}^{n} \alpha_{i,n}^2$$

$$+ \cdots + \binom{k}{j}\beta^{k-j}\delta^j \sum_{i=1}^{n} \alpha_{i,n}^j + \cdots + \delta^k \sum_{i=1}^{n} \alpha_{i,n}^k.$$

Since the sum of the kth powers of the n roots of unity is zero for $k < n$, then for each $j = 1,2, \ldots, n-1$,

$$\sum_{i=1}^{n} \alpha_{i,n}^{j} = 0.$$

Therefore, $\int_{\beta,\delta} x^k = \lim \frac{1}{n} \beta^k = \beta^k$ so that the theorem follows from Corollary 5.7.

The next theorem shows that the integral is bounded by the maximum value of the function on the circle.

Theorem 5.9. Suppose β and δ are in T_p and f is a function such that:

a) for all $x \in C(\beta,|\delta|)$, $f(x)$ is defined; and

b) $\int_{\beta,\delta} f$ exists, then

$$\left| \int_{\beta,\delta} f \right| \leq \max_{x \in C} \left| f(x) \right|$$

where $C = C(\beta,|\delta|)$.

Proof: Since

$$\int_{\beta,\delta} f = \lim \frac{1}{n} \sum_{i=1}^{n} f(\gamma_{i,n})$$

where the limit is taken over positive integers relatively prime to p, it follows that

$$\left| \int_{\beta,\delta} f \right| = \lim \left| \frac{1}{n} \sum_{i=1}^{n} f(\gamma_{i,n}) \right| = \lim \left| \sum_{i=1}^{n} f(\gamma_{i,n}) \right| .$$

Now,

$$\left|\sum_{i=1}^{n} f(\gamma_{i,n})\right| \leq \max_{1\leq i\leq n}\left\{\left|f(\gamma_{i,n})\right|\right\} \leq \max_{x \varepsilon C}\left|f(x)\right|.$$

Therefore,

$$\left|\int_{\beta,\delta} f\right| \leq \max_{x \varepsilon C}\left|f(x)\right|.$$

The following theorem shows that, as in complex analysis, a uniformly convergent series can be integrated term by term.

Theorem 5.10. Suppose

$$\sum_{i=1}^{\infty} c_i f_i(x)$$

converges uniformly to $f(x)$ on the circle $C(\beta,r) = \{x: |x - \beta| = r\}$ where $r = |\delta|$ for some $\delta \varepsilon T_p$. If, for each $i = 1,2, \ldots,$ the Schnirelman Integral $\int_{\beta,\delta} f_i$ exists, then $\int_{\beta,\delta} f$ exists and

$$\int_{\beta,\delta} f = \sum_{i=1}^{\infty} c_i \int_{\beta,\delta} f_i.$$

Proof: Let $\epsilon > 0$ be chosen. Let

$$F_m = \sum_{i=1}^{m} c_i f_i.$$

By Corollary 5.4,

$$\int_{\beta,\delta} F_m = \sum_{i=1}^{m} c_i \int_{\beta,\delta} f_i.$$

Thus, it suffices to show that

$$\lim_{m \to \infty} \left| \int_{\beta,\delta} f - \int_{\beta,\delta} F_m \right| = 0.$$

To see that this is the case, note that uniform convergence of the series implies there is an M such that for any $x \in C$, $|f(x) - F_m(x)| < \epsilon$ whenever $m \geq M$. An application of Theorem 5.9 yields

$$\left| \int_{\beta,\delta} (f - F_m) \right| \leq \max_{x \in C} \left| f(x) - F_m(x) \right| < \epsilon.$$

It follows that

$$\lim_{m \to \infty} \left| \int_{\beta,\delta} f - \int_{\beta,\delta} F_m \right| = 0$$

and, therefore,

$$\int_{\beta,\delta} f = \sum_{i=1}^{\infty} c_i \int_{\beta,\delta} f_i.$$

It was shown in Theorem 5.8 that the Schnirelman Integral of a polynomial over T_p is the value of the polynomial at the center of the discrete circles. This result extends to convergent power series.

Theorem 5.11. Let $f(x) = a_0 + a_1x + a_2x^2 + \cdots$ be a power series with the non-zero radius of convergence r. If $|\beta| < r$ and $|\delta| < r$, then $\int_{\beta,\delta} f$ exists and $\int_{\beta,\delta} f = f(\beta)$.

Proof: Since $|\beta| < r$ and $|\delta| < r$, then the circle $C(\beta, |\delta|)$ is contained in the disc $D = \{x: |x| < r\}$. Therefore, the power series converges uniformly on $C(\beta, |\delta|)$ so that Theorem 5.10 implies

$$\int_{\beta,\delta} f = \sum_{i=0}^{\infty} a_i \int_{\beta,\delta} x_i = \sum_{i=0}^{\infty} a_i \beta^i = f(\beta).$$

The above result shows that the Schnirelman Integral of a convergent power series depends only on the center of the circle $C(\beta,|\delta|)$ and not upon the choice of δ. This may seem surprising since the center of a circle is not unique. Recall, however, that the Schnirelman Integral is defined in terms of a sequence of discrete circles. Each circle in this sequence has the same center, and the center of a discrete circle is unique.

Cauchy's Integral Theorem

A fundamental result encountered early in the study of complex variables is Cauchy's Integral Theorem. This states that the complex line integral around a simple closed curve in the complex plane is zero provided the function is analytic inside and on that curve. In view of Theorem 5.11, Cauchy's Integral Theorem has no exact analogue in this setting. However, the following might be considered as a p-adic analogue of that theorem.

Theorem 5.12. If

$$f(x) = \sum_{i=0}^{\infty} a_i x^i$$

is a power series with radius of convergence $r > 0$ and if $|\beta| < r$ and $|\delta| < r$, then $\int_{\beta,\delta} (x - \beta)f(x) = 0$.

Proof: $\int_{\beta,\delta} (x - \beta)f(x) = \int_{\beta,\delta} x\, f(x) - \beta \int_{\beta,\delta} f(x)$. Since $x\, f(x)$ is a power series with radius of convergence r, Theorem 5.11 yields $\int_{\beta,\delta} x\, f(x) = \beta\, f(\beta)$. Since $\int_{\beta,\delta} f(x) = f(\beta)$, it follows that

$$\int_{\beta,\delta} (x - \beta)f(x) = \beta\, f(\beta) - \beta\, f(\beta) = 0.$$

Cauchy's Integral Formula

Another basic result in complex analysis is Cauchy's Integral Formula. This theorem assumes that f analytic inside and on a simple closed curve C. Then

$$f(\alpha) = \frac{1}{2\pi i} \int_C \frac{f(z)}{z - \alpha}\, dz.$$

where α is on the interior of C. The striking feature of this theorem is that the values of the function on the interior of C are completely determined by the values on C.

In the work that follows, a p-adic analogue to Cauchy's Integral Formula will be developed. The following special case will be established first.

<u>Theorem</u> 5.13. If k is a rational integer and $k > 0$, then

$$\int_{0,\delta} \frac{1}{(x - \alpha)^k} = \begin{cases} 0 & \text{if } |\alpha| < |\delta| \\ \left(\frac{-1}{\alpha}\right)^k & \text{if } |\alpha| > |\delta| \end{cases}.$$

Proof: Consider

$$(x - \alpha)^{-k} = (-\alpha)^{-k} \sum_{j=0}^{\infty} \binom{-k}{j} \left(\frac{x}{-\alpha} \right)^j .$$

Since the radius of convergence of the binomial series is 1, it follows that the series converges for $|x| < |\alpha|$. Therefore, if $|\alpha| > |\delta|$, Theorem 5.11 implies

$$\int_{0,\delta} \frac{1}{(x - \alpha)^k} = \frac{1}{(0 - \alpha)^k} = \left(\frac{-1}{\alpha} \right)^k .$$

Now suppose $|\alpha| < |\delta|$ so that $|x| = |\delta|$ implies $|\frac{-\alpha}{x}| < 1$. Then

$$(x - \alpha)^{-k} = x^{-k}\left(1 - \frac{\alpha}{x} \right)^{-k} = \sum_{j=0}^{\infty} \binom{-k}{j} \frac{1}{x^k} \left(\frac{-\alpha}{x} \right)^j$$

and the series converges uniformly on $|x| = |\delta|$. Therefore, Theorem 5.10 applies so that it suffices to consider $\int_{0,\delta} x^{-(j+k)}$ for $j \geq 0$. According to the definition

$$\int_{0,\delta} x^{-(j+k)} = \lim \frac{1}{n} \sum_{i=1}^{n} (\delta\alpha_{i,n})^{-(j+k)} .$$

Since the nth roots of unity form an Abelian group, the set $\{\alpha_{1,n}^{-1}, \alpha_{2,n}^{-1}, \ldots, \alpha_{n,n}^{-1}\}$ coincides with the set $\{\alpha_{1,n}, \alpha_{2,n}, \ldots, \alpha_{n,n}\}$. Therefore,

$$\sum_{i=1}^{n} (\delta\alpha_{i,n})^{-(j+k)} = \delta^{-(j+k)} \sum_{i=1}^{n} \alpha_{i,n}^{j+k} .$$

Since

$$\sum_{i=1}^{n} \alpha_{i,n}^{j+k} = 0$$

for every $n > j + k$, it follows that $\int_{0,\delta} x^{-(j+k)} = 0$ for every $j \geq 0$ and, therefore, $\int_{0,\delta} (x - \alpha)^{-k} = 0$ whenever $|\alpha| < |\delta|$. This completes the proof of Theorem 5.13.

Corollary 5.14. If $k > 0$, then

$$\int_{\beta,\delta} \frac{1}{(x - \alpha)^k} = \begin{cases} 0 & \text{if } |\alpha - \beta| < |\delta| \\ \dfrac{1}{(\beta - \alpha)^k} & \text{if } |\alpha - \beta| > |\delta| \end{cases}.$$

Proof: By Theorem 5.5,

$$\int_{\beta,\delta} \frac{1}{(x - \alpha)^k} = \int_{0,\delta} \frac{1}{(x + \beta - \alpha)^k} = \begin{cases} 0 & \text{if } |\alpha - \beta| < |\delta| \\ \dfrac{1}{(\beta - \alpha)^k} & \text{if } |\alpha - \beta| > |\delta| \end{cases}.$$

The next theorem may be considered an analogue of the Cauchy Integral Formula since the value of an analytic function at a point is given in terms of the Schnirelman Integral on a circle about that point.

Theorem 5.15. Suppose

$$f(x) = \sum_{j=0}^{\infty} a_j x^j$$

converges for $|x| < r$ and $|\alpha|$, $|\beta|$, and $|\delta|$ are all less than r. Then

$$\int_{\beta,\delta} \frac{f(x)(x - \beta)}{x - \alpha} = \begin{cases} f(\alpha) & \text{if } |\alpha - \beta| < |\delta| \\ 0 & \text{if } |\alpha - \beta| > |\delta| \end{cases}.$$

Proof: Suppose $|\alpha - \beta| < |\delta|$. Then $|\alpha - \beta| \leq \max\{|\alpha|,|\beta|\} < |\delta|$ so that $|x - \alpha| = |x - \beta| = |\delta|$ for all x such that $|x - \beta| = |\delta|$. Since

$$f(x) = \sum_{j=0}^{\infty} a_j x^j$$

then

$$\frac{f(x)(x - \beta)}{x - \alpha} = \sum_{j=0}^{\infty} \frac{a_j x^j (x - \beta)}{x - \alpha}$$

and the series converges uniformly on $|x - \beta| = |\delta|$.

In the other case, $|\alpha - \beta| > |\delta|$. Then for all x such that $|x - \beta| = |\delta|$, $|x - \alpha| = |x - \beta + \beta - \alpha| = |\alpha - \beta| > |\delta|$. Thus, $\left|\frac{x - \beta}{x - \alpha}\right| < 1$ so that

$$\sum \frac{a_j x^j (x - \beta)}{x - \alpha}$$

converges uniformly on $|x - \beta| = |\delta|$.

In either case, by Theorem 5.7,

$$\int_{\beta,\delta} \frac{f(x)(x - \beta)}{x - \alpha} = \sum_{j=0}^{\infty} a_j \int_{\beta,\delta} \frac{x^j (x - \beta)}{x - \alpha} .$$

Now for $j > 0$,

$$\frac{x^j}{x - \alpha} = \frac{x^j - \alpha^j + \alpha^j}{x - \alpha} = \frac{x^j - \alpha^j}{x - \alpha} + \frac{\alpha^j}{x - \alpha}$$

$$= x^{j-1} + \alpha x^{j-2} + \cdots + \alpha^{j-1} + \frac{\alpha^j}{x - \alpha} .$$

Thus,

$$\int_{\beta,\delta} \frac{x^j(x-\beta)}{x-\alpha} = \int_{\beta,\delta} (x^{j-1} + \cdots + \alpha^{j-1})(x-\beta) + \int_{\beta,\delta} \frac{\alpha^j(x-\beta)}{x-\alpha}$$

$$= \alpha^j \int_{\beta,\delta} \frac{x-\beta}{x-\alpha} .$$

Since $\frac{x-\beta}{x-\alpha} = 1 - \frac{\beta-\alpha}{x-\alpha}$, it follows that for $j \geq 0$,

$$\int_{\beta,\delta} \frac{x^j(x-\beta)}{x-\alpha} = \alpha^j - \alpha^j(\beta-\alpha) \int_{\beta,\delta} \frac{1}{x-\alpha} .$$

If $|\alpha - \beta| < |\delta|$, Corollary 5.14 implies $\int_{\beta,\delta} \frac{1}{x-\alpha} = 0$ so that

$$\int_{\beta,\delta} \frac{f(x)(x-\beta)}{x-\alpha} = \sum_{j=0}^{\infty} a_j\alpha^j = f(\alpha).$$

If $|\alpha - \beta| > |\delta|$, Corollary 5.14 implies $\int_{\beta,\delta} \frac{1}{x-\alpha} = \frac{1}{\beta-\alpha}$ so that for each $j \geq 0$

$$\int_{\beta,\delta} \frac{x^j(x-\beta)}{x-\alpha} = \alpha^j - \alpha^j(\beta-\alpha)\frac{1}{\beta-\alpha} = 0.$$

It follows that $\int_{\beta,\delta} \frac{f(x)(x-\beta)}{x-\alpha} = 0$. This completes the proof of Theorem 5.15.

As in complex analysis, Cauchy's Integral Formula can be extended to derivatives. The following lemma is useful in proving an extension of Theorem 5.15.

Lemma 5.16. Let g be a polynomial such that $\deg g < k$. Then $\int_{\beta,\delta} \frac{g(x)}{(x-\alpha)^k} = 0$ whenever $|\alpha - \beta| < |\delta|$.

Proof: Since $\deg g < k$, $\frac{g(x)}{(x-\alpha)^k}$ can be expressed by partial fractions. Thus, there exist k constants $A_1, A_2, \ldots, A_k$ such that

$$\frac{g(x)}{(x-\alpha)^k} = \frac{A_1}{(x-\alpha)} + \frac{A_2}{(x-\alpha)^2} + \cdots + \frac{A_k}{(x-\alpha)^k}\,.$$

It follows from Corollary 5.14 that

$$\int_{\beta,\delta} \frac{g(x)}{(x-\alpha)^k} = 0.$$

Theorem 5.17. Suppose

$$f(x) = \sum_{j=0}^{\infty} b_j x^j$$

converges for $|x| < r$ and $|\alpha|$, $|\beta|$, and $|\delta|$ are all strictly less than r. If $|\alpha - \beta| < |\delta|$, then

$$\int_{\beta,\delta} \frac{f(x)(x-\beta)}{(x-\alpha)^{n+1}} = \frac{1}{n!} f^{(n)}(\alpha).$$

Proof: Let $n = N$ be fixed. It suffices to assume $\beta = 0$. Then

$$\int_{0,\delta} \frac{f(x)\ x}{(x-\alpha)^N} = \int_{0,\delta} \frac{\sum_{j=0}^{N} b_j x^{j+1}}{(x-\alpha)^N} + \sum_{j=N+1}^{\infty} b_j \int_{0,\delta} \frac{x^{j+1}}{(x-\alpha)^N}\,.$$

According to Lemma 5.16, the first integral of the right hand side is zero. Now for each $j > N$, there exist polynomials Q_j and R_j such that $x^{j+1} = (x-\alpha)^N Q_j(x) + R_j(x)$ where $R_j \equiv 0$ or $\deg R_j < N$. Thus, for each $j > N$,

$$\int_{0,\delta} \frac{x^{j+1}}{(x-\alpha)^N} = \int_{0,\delta} Q_j(x) + \int_{0,\delta} \frac{R_j(x)}{(x-\alpha)^N}$$

$$= \int_{0,\delta} Q_j(x)$$

since Lemma 5.16 applies again. Now the last integral equals $Q_j(0)$ for each j. Thus, it suffices to sum the constant terms of the polynomials Q_j for $j = N+1, N+2, \ldots$. By actually dividing x^{N+1+h} by $(x-\alpha)^N$, it can be shown that the constant term of Q_{N+1+h} is given by $\binom{N+h}{h}\alpha^h$ for $h = 0,1, \ldots$. It follows that

$$\int_{0,\delta} \frac{f(x)\ x}{(x-\alpha)^{N+1}} = \sum_{j=N+1}^{\infty} b_j \int_{0,\delta} Q_j(x)$$

$$= \sum_{h=0}^{\infty} b_{N+1+h} \binom{N+h}{h} \alpha^h.$$

$$= \frac{1}{N!} f^{(N)}(\alpha).$$

This completes the proof.

Maximum Modulus, Cauchy's Inequality, Liouville's Theorem

Analogues of several standard results of complex analysis have already been established. This chapter will be concluded by showing three more. In particular, analogues of the Maximum Modulus Principle, Cauchy's Inequality, and Liouville's Theorem will be established.

One form of the Maximum Modulus Principle of complex analysis asserts that if a non-constant function f is analytic inside and on a simple closed curve C and if M is an upper bound of f on C, then $|f(z)| < M$ for every z inside C. The next theorem shows a corresponding result in T_p.

Theorem 5.18. Suppose

$$f(x) = \sum_{i=0}^{\infty} a_i x^i$$

converges for $|x| < r$. Let $0 < r_0 < r$ and $M \geq |f(x)|$ for every $x \in D[0,r_0]$. Then either $|f(x)|$ is constant on $D(0,r_0)$ or $|f(x)| < M$ for every x in the open disc $D(0,r_0)$.

Proof: Suppose $\alpha,\beta \in D(0,r_0)$ with $|f(\alpha)| > |f(\beta)|$. Pick δ such that $|\delta| = r_0$. Then $|\alpha - \beta| < |\delta|$ and $f(\alpha) = \int_{\beta,\delta} \frac{f(x)(x-\beta)}{x-\alpha}$ and $f(\beta) = \int_{\beta,\delta} f(x)$. Thus,

$$\begin{aligned} |f(\alpha)| &= |f(\alpha) - f(\beta)| \\ &= \left| \int_{\beta,\delta} \frac{f(x)(x-\beta)}{x-\alpha} - \int_{\beta,\delta} f(x) \right| \\ &= \left| \int_{\beta,\delta} \frac{f(x)(\alpha-\beta)}{x-\alpha} \right|. \end{aligned}$$

Since $|\alpha - \beta| < |\delta|$, then for every x such that $|x - \beta| = |\delta|$, $|x - \alpha| = |x - \beta + \beta - \alpha| = |\delta|$. Let C denote the set $\{x \in T_p\colon |x - \beta| = |\delta|\}$. Then according to Theorem 5.9,

$$\begin{aligned} \left| \int_{\beta,\delta} \frac{f(x)(\alpha-\beta)}{x-\alpha} \right| &\leq \underset{x \in C}{\text{maximum}} \left| \frac{f(x)(\alpha-\beta)}{x-\alpha} \right| \\ &= \frac{|\alpha-\beta|}{|\delta|} \underset{x \in C}{\text{maximum}} |f(x)| \\ &< \underset{x \in C}{\text{maximum}} |f(x)| \leq M. \end{aligned}$$

Therefore, $|f(\alpha)| < M$.

As a consequence of Theorem 5.17, the following analogue of Cauchy's Inequality can be established.

Theorem 5.19. Suppose f is analytic in $D(0,r)$. If $0 < r_0 < r$ and $M \geq |f(x)|$ for every $x \in D[0,r_0]$, then for $n = 1,2, \ldots$,

$$\left|\frac{f^{(n)}(x)}{n!}\right| \leq \frac{M}{r_0^n} .$$

Proof: By Theorems 5.17 and 5.9, if $|y| < r_0$ then

$$\left|\frac{f^{(n)}(y)}{n!}\right| = \left|\int_{0,\delta} \frac{f(x)\ x}{(x - y)^{n+1}}\right| \leq \max_{x \in C} \left|\frac{f(x)\ x}{(x - y)^{n+1}}\right|$$

where $C = \{x: |x| = r_0\}$. Since $|y| < r_0$, then $|x - y| = r_0$ for $x \in C$. It follows that

$$\max_{x \in C} \left|\frac{f(x)\ x}{(x - y)^{n+1}}\right| = \max_{x \in C} \frac{|f(x)|}{r_0^n} \leq \frac{M}{r_0^n} .$$

Finally, the p-adic analogue of the Liouville Theorem states that any bounded entire function is a constant function.

Theorem 5.20. If f is an entire function and there is a real number M such that $|f(x)| \leq M$ for every $x \in T_p$, then $f(x) = a_0$ where $f(x) = a_0 + a_1x + \cdots$.

Proof: It suffices to show that $a_n = 0$ for $n = 1,2, \ldots$. Suppose to the contrary that $a_n \neq 0$ for some $n \geq 1$. Let δ be an element in T_p such that $\frac{M}{|\delta|^n} < |a_n|$. According to Theorem 5.19,

$$\left|\frac{f^{(n)}(0)}{n!}\right| \leq \frac{M}{|\delta|^n} .$$

But since $a_n = \frac{f^{(n)}(0)}{n!}$,

$$|a_n| \leq \frac{M}{|\delta|^n} < |a_n| .$$

This contradiction shows that $a_n = 0$ for $n = 1,2, \ldots$.

Conclusion

While further analogies between complex and p-adic analysis will not be pursued in this study, it should be remarked that others do exist. For example, Laurent series can be defined in T_p essentially as in the complex case. Thus, the concept and classification of singularities of analytic functions can be discussed. Meromorphic functions have natural analogies in T_p. The residue of a function can be defined in the usual manner and there is a p-adic analogue of Cauchy's Residue Theorem. The technique of proof, as illustrated earlier in this chapter, somewhat parallels the corresponding proof in complex analysis but utilizes the Schnirelman Integral and its properties.

As a final remark, one quite significant distinction between analysis in T_p and complex analysis will be noted. In complex analysis an analytic function may have an analytic continuation beyond its circle of convergence. That is, if $f(z)$ is an analytic function having radius of convergence r, $0 < r < \infty$, then given a point z_0 in the circle of convergence, $f(z)$ is analytic at z_0. Thus, $f(z)$ can be expressed as a power series developed about $z = z_0$ and the new circle of convergence may include points which are not in the original circle of convergence. In the p-adic situation, however, any two discs are either disjoint or nested. It follows that analytic continuation in the above sense is not possible for analytic functions in T_p. This observation concludes the present study.

SELECTED BIBLIOGRAPHY

1. Adams, William W. "Transcendental Numbers," American Journal of Mathematics, Vol. 88, No. 2 (1966), 279-308.

2. Agnew, Jeanne. Explorations in Number Theory. Monterey, California: Brooks Cole, 1972.

3. Amice, Yvette. "Interpolation p-adic," Bulletin de la Societe Mathematique de France, Vol. 92 (1964), 117-180.

4. Artin, Emil. Algebraic Numbers and Algebraic Functions. New York: Gordon and Breach, 1967.

5. Bachman, G. Introduction to p-adic Numbers and Valuation Theory. New York: Academic Press, 1964.

6. Borevich, Z. I. and I. R. Shafarevich. Number Theory, trans. Newcomb Breenlear. New York: Academic Press, 1966.

7. Bruhat, F. Lectures on Some Aspects of p-adic Analysis, Tata Institute of Fundamental Research, Bombay, India, 1966.

8. Dieudonne, M. Jean. "Sur les Fonctions Continues p-adiques," Bulletin des Sciences Mathematique, 2nd Series, Vol. 68 (1944), 79-95.

9. Herstein, I. N. Topics in Algebra. Waltham, Massachusetts: Blaisdell, 1964.

10. Hille, E. Analytic Function Theory. Waltham, Massachusetts: Blaisdell, 1959.

11. Mahler, K. "An Interpolation Series for Continuous Functions of a p-adic Variable," Journal for the Reine and Ange. Math., Vol. 199 (1956), 23-34.

12. McCarthy, P. J. Algebraic Extensions of Fields. Waltham, Massachusetts: Blaisdell, 1966.

13. Monna, A. F. Analyse Non-Archimedienne. New York: Springer Verlag, 1970.

14. Palmer, Leonard L. "Some Analysis in a Non-archimedean Field." Unpublished doctoral dissertation. (Oklahoma State University, 1971).

15. Sato, D. and E. G. Straus. "p-Adic Proof of Non-existence of Proper Prime Representing Algebraic Functions and Related Problems," Journal of the London Mathematical Society, Vol. 2 (1970), 45-48.

16. Snook, Verbal M. "A Study of p-Adic Number Fields." Unpublished doctoral dissertation. (Oklahoma State University, 1970).

17. Van der Waerden, B. L. Algebra, Volume I. Ungar, New York, 1970.

APPENDIX

This appendix supplies proofs of Lemmas 4.16 and 4.17.

Theorem A.1. Let G and H be polynomials in $O_p[x]$ with G monic. Then G and H are relatively prime in $O_p[x]$ if and only if $\overline{G}$ and $\overline{H}$ are relatively prime in $O_p/A_n[x]$ for $n > 0$.

Proof: For any polynomial $P(x) = a_0 + a_1x + \cdots + a_sx^s$ in $O_p[x]$, let $\overline{P}(x) = \overline{a_0} + \overline{a_1}x + \cdots + \overline{a_s}x^s$ where $\overline{a}$ denotes the image of $a \in O_p$ under the canonical homomorphism from O_p onto O_p/A_n. Since $\overline{UG + VH} = \overline{U}\,\overline{G} + \overline{V}\,\overline{H}$ and $\overline{1} = 1$, then G and H relatively prime implies $\overline{G}$ and $\overline{H}$ are relatively prime.

Conversely, suppose $\overline{G}$ and $\overline{H}$ are relatively prime in $O_p/A_n[x]$. Let $Q \in O_p[x]$ be such that $Q|G$ and $Q|H$. Then it suffices to show that $Q = 1$. Since $Q|G$ and $Q|H$, there exist polynomial R and R' in $O_p[x]$ such that $G = QR$ and $H = QR'$. Furthermore, G is monic implies the high order coefficient of Q is a unit in O_p. Thus, $\deg \overline{Q} = \deg Q$. Since $\overline{G}$ and $\overline{H}$ are relatively prime in $O_p/A_n[x]$, there exist polynomials $\overline{U}$ and $\overline{V}$ in $O_p/A_n[x]$ such that

$$1 = \overline{G}\,\overline{U} + \overline{H}\,\overline{V} = \overline{Q}\,\overline{R}\,\overline{U} + \overline{Q}\,\overline{R}'\,\overline{V}$$

so that

$$1 = \overline{Q}\,(\,\overline{R}\,\overline{U} + \overline{R}'\,\overline{V}\,).$$

This implies $0 = \deg \overline{Q} = \deg Q$. Since Q is monic, $Q = 1$.

<u>Theorem</u> A.2. Let G and H be two polynomials with coefficients in ring R. If G is monic and G and H are relatively prime in $R[x]$ with $\deg G = s$, then for every non-zero polynomial $Q \in R[x]$ there exists a unique pair of polynomials U and V such that $Q = UG + VH$ with $V = 0$ or $\deg V < s$.

Proof: Suppose G and H are relatively prime in $R[x]$. Then there exist polynomials J and K in $R[x]$ such that $JG + KH = 1$. Thus, if Q is any polynomial in $R[x]$ then $Q = QJG + QKH$. Suppose $\deg QK \geq s = \deg G$. Then there exist polynomials A and B in $R[x]$ such that $QK = AG + B$ where either $B = 0$ or $\deg B < s$. Then, substituting for QK in the above equation,

$$Q = QJG + (AG + B)H = (QJ + AH)G + BH.$$

If $U = QJ + AH$ and $V = B$, then the existence part of the theorem is proved.

To prove uniqueness, suppose there is another pair of polynomials U' and V' in $R[x]$ such that $Q = U'G + V'H$ with $\deg V' < s$ or $V' = 0$. Then $U'G + V'H = UG + VH$ implies $(U' - U)G = (V - V')H$. Since G and H are relatively prime, $G|(V - V')H$ implies $G|(V - V')$. Now $\deg(V - V') \leq \max(\deg V, \deg V') < s$. Therefore, $G|(V - V')$ implies $V = V'$ which, in turn, implies $U = U'$. This completes the proof.

VITA

John Eldon Atkinson

Candidate for the Degree of

Doctor of Education

Thesis: ANALYSIS IN AN ALGEBRAICALLY CLOSED NON-ARCHIMEDEAN FIELD

Major Field: Higher Education

Biographical:

Personal Data: Born in Gypsum, Kansas, January 3, 1935, the son of Ted and Mary Atkinson.

Education: Graduated from Dickinson County Community High School, Chapman, Kansas, in May, 1953; attended Bethany College, Lindsborg, Kansas from 1953 to 1955; received Bachelor of Science degree in Education from Kansas State Teachers College, Emporia, Kansas in May, 1957; attended the University of Kansas in 1959-1960; received Master of Science degree from Kansas State Teachers College, Emporia, Kansas in August, 1964; completed requirements for the Doctor of Education degree at Oklahoma State University in July, 1972.

Professional Experience: Mathematics and science teacher, Douglass High School, Douglass, Kansas, 1957-1959; mathematics teacher, Shawnee-Mission High School, Shawnee-Mission, Kansas, 1960-1965; Assistant Professor of Mathematics, Tarkio College, Tarkio, Missouri, 1965-1972; graduate teaching assistant, Oklahoma State University, 1969-1971; Associate Professor of Mathematics, Tarkio College, Tarkio, Missouri, 1972.