SOME ANALYSIS IN A NON-ARCHIMEDEAN FIELD

By

LEONARD LEON PALMER

Bachelor of Science in Education
Southeast Missouri State College
Cape Girardeau, Missouri
1958

Master of Arts
University of Illinois
Urbana, Illinois
1961

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, 1971

SOME ANALYSIS IN A NON-ARCHIMEDEAN FIELD

Thesis Approved:

Jeanne Agnew
Thesis Adviser

Shair Ahmad

D B Aichele

John Jewett

D Durham
Dean of the Graduate College

ACKNOWLEDGMENTS

It is my pleasant duty to thank the members of my advisory committee. First I would like to thank Dr. John Jewett, my committee chairman, and Dr. Douglas Aichele. Dr. Shair Ahmad deserves special thanks for serving on my committee and taking the time to read the manuscript for my dissertation. I especially want to thank my thesis adviser, Dr. Jeanne Agnew, for her encouragement and counsel during the preparation of this dissertation. The time and effort she has given on my behalf is greatly appreciated.

A special thanks to typist Cynthia Wise for her help in typing the dissertation.

Finally, I wish to express my gratitude to my wife, Pat, for her sacrifices during my graduate study.

TABLE OF CONTENTS

CHAPTER I

INTRODUCTION

The valuation-theoretic approach is used in conducting current research in algebraic number theory and algebraic geometry. Many books written on algebraic number theory in the past decade emphasize this approach [18]. In addition, this valuable concept is applied to such research areas as diophantine equations [7], theory of algebraic function fields [3] and topics in number theory [5].

However, the student arriving on the threshold of graduate studies in mathematics has probably not heard of the term valuation or even of p-adic numbers. Furthermore, there is very little literature available that is suitable for a student at this stage. Many of the published books which discuss valuations claim to be self contained, but such works as Schilling's, "The Theory of Valuations" [16] are for the advanced student. Typical of comments found is "articles are all self-contained, in the sense that they can be read without extensive prior knowledge of number theory." This statement occurs in the introduction of "Studies in Number Theory" [7]. However, on page 94 of the 1970 January issue of "The American Mathematical Monthly" a review of this book states that "The paper by D. J. Lewis on p-adic methods seems to be the most difficult to follow and may require frequent consultation of references."

While much of the literature is on a level somewhat more advanced than the mathematical maturity of the beginning graduate, it is felt that the concepts and their implications can be made accessible to these students. In addition to their value in research, the fields of p-adic numbers are very interesting to study. Of further interest is the analysis that may be carried on in these fields. In the study of these fields we see such common areas as algebra, number theory and analysis combined in conducting research.

This paper is intended to help fill the gap that now exists in the literature on valuation theory and p-adic numbers at the advanced undergraduate or beginning graduate level. It would be studied at a time when the student is in the transitional period of leaving behind undergraduate mathematics and embarking on graduate level courses. Some of the purposes to be served would include (1) to strengthen the student's background and promote the development of mathematical maturity, (2) to stimulate an interest in a new and unfamiliar area of mathematics, (3) to reinforce the concepts acquired in undergraduate mathematics by investigating these concepts in a different setting, and (4) to present a study where algebra, number theory and analysis are combined and used in arriving at new conclusions. The material in this study could probably be used best in a seminar or for independent study.

Finally, this study is not intended to be a treatise on valuation theory and p-adic methods. It is written for the student who is beginning graduate studies. The accomplished mathematician is not only encouraged, but urged, to proceed directly to such publications as Artin [3], Schilling [16], or O'Meara [12].

In preparation for the development of p-adic numbers and valuation theory, some of the important properties of algebraic systems, number theory and analysis, to be used in the subsequent discussion will be reviewed here. The reader who is already familiar with these concepts may proceed directly to Chapter II.

Sets and Mappings

Suppose A and B are two sets. If with each element a in A there is associated a unique element b in B, we say that there is a mapping or function f of A into B and write $f(a) = b$. If $f(a) = f(b)$ implies that $a = b$, f is said to be one to one. If for each b in B there exists an element a in A such that $f(a) = b$, then f is called an onto mapping.

Let f be a mapping of A into B. Then for a subset E of A the image set $f(E)$ is the set $\{f(x): x$ is in $E\}$. For a subset D of B the pre-image set is $f^{-1}(D) = \{x: f(x)$ is in $D\}$. Now if f is a mapping of A into B and E is a subset of A, the restriction of f to E, denoted by $f|_E$ is $f|_E(x) = f(x)$ where x is in E. A relation in a set S is a subset of ordered pairs (a,b) of the product set $S \times S$. If $\sim$ is a relation and (a,b) is in $\sim$, we say that "a is in the relation $\sim$ to b" and write $a \sim b$.

Let S be a set and let $\sim$ designate a relation defined between elements of S such that, given any two elements a and b in S, $a \sim b$ is either true or false. The relation is called an equivalence relation if it satisfies the following conditions:

(a) $a \sim a$ for all a in S (reflexivity);

(b) $a \sim b$ implies $b \sim a$ (symmetry); and

(c) $a \sim b$ and $b \sim c$ implies $a \sim c$ (transitivity).

Suppose that S is a set and $\sim$ is an equivalence relation defined on S. Let $[a] = \{x \text{ in } S: x \sim a\}$. This set is called an equivalence class.

Theorem 1.1. If S is a set with an equivalence relation defined on S, then S is decomposed into disjoint equivalence classes.

We denote this by $S = \bigcup[a]$. Here it is understood that the union is taken only over certain elements in S so that the sets are disjoint.

Algebraic Systems

A group is a set with an operation "$\cdot$" such that $a \cdot b$ is in G whenever a and b are in G, and for which the following properties are satisfied:

(a) for all a, b, and c in G, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;

(b) there is an element e in G such that for each a in G, $a \cdot e = e \cdot a = a$;

(c) for each a in G there is an element a^{-1} in G such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

If for all a and b in G, $a \cdot b = b \cdot a$, then g is said to be an abelian group (commutative). A subset H of G is called a subgroup of G if H is also a group. A group G is said to be cyclic if there exists an element g in G such that for each h in G, $h = g^n$ for some integer n. The element g is called a generator of G. The number of elements in a group is said to be the order of the group. A group is said to be finite if it has a finite number of elements. Otherwise, it has infinite order. The order of a group G is denoted by $|G|$.

Let G be a group with the operation "$\cdot$" and H a group with an operation "$*$". A mapping f of G into H such that

$$f(a \cdot b) = f(a)*f(b)$$

is called a homomorphism of G into H. The mapping f is called a <u>monomorphism</u> if f is one to one. If $f(G) = H$ then f is said to be an <u>epimorphism</u> of G onto H. A mapping f that is both a monomorphism and an epimorphism is called an <u>isomorphism</u>. In this case G and H are said to be <u>isomorphic</u>.

Define a relation $\sim$ on Z by $a \sim b$ if and only if m divides $a - b$ for a positive integer m. We say that a is congruent to b modulo m and write $a \equiv b(\text{mod } m)$. Let $Z_m = \{[0],[1], \ldots, [m - 1]\}$ and define an operation "+" on Z_m by $[a] + [b] = [a + b]$. This operation is well defined and Z_m is a cyclic group since

$$n[a] = \sum_{k=1}^{n} [a] = [na]$$

for each integer n.

<u>Theorem 1.2</u>. A cyclic group of order m is isomorphic to Z_m. A cyclic group of infinite order is isomorphic to Z.

By this theorem we see all infinite cyclic groups have two generators, since Z has generators 1 and -1. Let G be a group and H a subgroup of G. Let $aH = \{ah\colon h \text{ is in } H\}$. This set is called a left coset. Similarly, Ha is a right coset. For two subgroups H and K of G, $HK = \{hk\colon h$ is in H and k is in $K\}$. The subgroup H is called a normal subgroup of $aHa^{-1} = H$ for all a in G. Suppose a and b are in G and H is a normal subgroup of G, then

$$aH \cdot bH = abH^2 = abH.$$

With this definition $G/H = \{aH\colon a$ is in $G\}$ is a group referred to as the <u>factor group</u> (quotient). If G is a finite group then

$$|G/H| = |G|/|H|.$$

The mapping from G onto G/H defined by $f(a) = aH$ is a homomorphism.

A set R together with two operations "+" and "$\cdot$" is called a commutative ring if the following properties are satisfied:

(a) R is an abelian group under addition;

(b) for a, b, and c in R, $(a\cdot b)\cdot c = a\cdot(b\cdot c)$;

(c) for a and b in R, $a\cdot b = b\cdot a$; and

(d) for a, b, and c in R, $a\cdot(b + c) = a\cdot b + b\cdot c$.

A ring is called a commutative ring with unity if there exists an element e in R such that $a\cdot e = a$ for all a in R. The identity for addition will be denoted by 0 and the identity for multiplication by 1. A ring R such that $a\cdot b = 0$ implies $a = 0$ or $b = 0$ is called an <u>integral domain</u>. The set $R^* = R - \{0\}$ denotes the set of all non-zero elements of R. Now if for each a in R^* there is an a^{-1} in R^* such that $a\cdot a^{-1} = 1$ then R is called a <u>field</u>. Only a commutative ring with unity will be considered in further discussion and will simply be referred to as a ring. It is customary to denote a ring by the symbol $(R,+,\cdot)$, emphasizing it is a set with two operations. Similarly, $(G,\cdot)$ is used to denote groups. In this study the practice will be adopted to simply use the symbol R for $(R,+,\cdot)$ and likewise G for $(G,\cdot)$.

A non-empty subset S of a ring R is a subring if it is a ring. The set S is a subring if and only if $a - b$ and ab are in S whenever a and b are in S. If R is a field and S is also a field, then we call S a subfield of R. We say a non-empty subset I of R is an ideal of R if (a) $a - b$ is in I whenever a and b are in R, and (b) for each r in R and a in I ra is in I. An ideal I is always a subring of R and under addition I is a normal subgroup of the additive group R. Let

$$R/I = \{a + I\colon a \text{ is in } R\}$$

and define addition and multiplication by

$$(a + I) + (b + I) = (a + b) + I$$

and

$$(a + I)(b + I) = ab + I.$$

These are well defined operations and R/I is a ring. If we form a set S by choosing an element from each coset $(a + I)$ in R/I such that $R = \bigcup(a + I)$ and the sets $(a + I)$ are pairwise disjoint, then S is called a complete residue system for the ring R/I.

A mapping from a ring R to a ring T is a ring homomorphism if $f(a + b) = f(a) + f(b)$ and $f(a\cdot b) = f(a)\cdot f(b)$. The same terminology is used for rings as for groups. The mapping from R to R/I defined by $f(a) = a + I$ is a ring homomorphism called the natural homomorphism. For a ring homomorphism f the set $\ker f = \{x: f(x) = 0\}$ is called the kernel of f. This set is always an ideal in R. The function f is a monomorphism if $\ker f = \{0\}$. If f is a ring homomorphism from a ring R to a ring $f(R)$ then $R/(\ker f)$ is isomorphic to $f(R)$.

Suppose R is an integral domain. The set

$$\{(a,b): a \text{ and } b \text{ are in } R \text{ and } b \neq 0\}$$

is called the set of quotients of R. The relation defined on the set of quotients by "$(a,b) \sim (c,d)$ if and only if $ad = bc$" is an equivalence relation. Let F be the set of all equivalence classes of the set of quotients of R and define "+" and "$\cdot$" by

$$[a,b] + [c,d] = [ad + bc,bd]$$

and

$$[a,b]\cdot[c,d] = [ac,bd].$$

With this definition F is a field, called the field of quotients of R. The mapping $f(a) = [a,1]$ defines an isomorphism of R into F. We say that R is embedded in F.

Let m be a positive integer and r an element of a ring R. Then

$$mr = \sum_{i=1}^{m} r$$

and $(-m)r = m(-r)$. If there exists a least positive integer m such that $mr = 0$ for all r in R, then we say that R has characteristic m. If no such positive integer exists, R has characteristic zero. For an integral domain either m is a prime or $m = 0$. The set Z_p, for a prime p is a field with characteristic p. In a field with characteristic p we have that $(a + b)^{p^n} = a^{p^n} + a^{p^n}$ for each a and b in F and each positive integer n.

Any field F is called a *prime* field if the only subfield of F is F itself. If F' is a prime field that is also a subfield of F then F' is called a prime subfield of F. Every field F of characteristic 0 contains a unique prime field isomorphic to the rational integers. If the characteristic of F is p then F contains a unique prime field isomorphic to Z_p. Any field F with a prime field isomorphic to the rational numbers contains a subring isomorphic to Z. In this sense we say that an integer n is in F. What we actually mean is $n \cdot 1$ is in F, where 1 is the unity of F.

For an ideal I of R, I is called a *principal ideal* if $I = \{ax\colon x \in R\}$. A ring R is called a *principal ideal ring* if every ideal I of R is a principal ideal. An ideal P of R is called a *prime ideal* if ab in P implies that a is in P or b is in P. An ideal M of R is maximal if $M \neq R$, and whenever N is an ideal in R such that $M \subset N \subset R$, then either $M = N$ or $N = R$. Any ideal I of R containing 1 is equal to R. For an ideal M of R, R/M is a field if and only if M is a maximal ideal.

The set

$$R[x] = \left\{ \sum_{i=0}^{n} a_i x^i \colon a_i \text{ is in } R \text{ and } n \text{ is a positive integer} \right\}$$

is a ring with the usual definitions of addition and multiplication of polynomials. The ring R is a subring of $R[x]$. The ring $R[x]$ is an integral domain whenever R is. The quotient field of $R[x]$ is denoted by $R(x)$. Suppose $f(x) \not\equiv 0$ and $g(x)$ are elements of $R[x]$.

There exist unique elements $q(x)$ and $r(x)$ of $R[x]$ such that $f(x) = g(x)q(x) + r(x)$ where $r(x) \equiv 0$ or the degree of $r(x)$ is less than the degree of $g(x)$. If $r(x) \equiv 0$ then we say $g(x)$ divides $f(x)$ and write $g(x)|f(x)$. If $f(x)$ is in $R[x]$ then $x - s$ is a factor of $f(x)$ if and only if $f(s) = 0$. A polynomial $f(x)$ in $F[x]$, where F is a field and the degree of $f(x)$ is one or greater, is said to be irreducible if $f(x) = h(x)g(x)$ implies that $h(x)$ is a constant or $h(x)$ is a constant multiple of $f(x)$.

Let R be an integral domain. For a and b in R, we say a divides b if there exists an element c in R such that $b = ac$. We say that a in R is a <u>unit</u> in R if there is an element b in R such that $a \cdot b = 1$. The elements a and b are <u>associates</u> if there exists a unit u such that $b = a \cdot u$. The relation "is an associate of" is an equivalence relation. A non-unit a is called a <u>prime</u> if whenever $a|bc$, then either $a|b$ or $a|c$. An integral domain R is a <u>unique factorization domain</u> if each non-zero, non-unit a of R can be expressed uniquely as

$$a = u \prod_{i=1}^{n} b_i,$$

where u is a unit and the b_i's are primes. A principal ideal domain is a unique factorization domain. An element d in a unique factorization is called a <u>greatest common divisor</u> of a and b if d divides both a and b and for each e that divides both a and b, e divides d. In a unique foractorization domain a greatest common divisor always exists and is denoted by (a,b). It is unique up to associates.

Let K be a field which is a subfield of some field E. Then E is said to be an extension field of K. If E is an extension field of K then E is a vector space over K. The degree of E over K is the dimension of E as a vector space over K. The degree of E over D is denoted by $[E:K]$.

Theorem 1.3. If F is a finite extension of E and E is a finite extension of K then $[F:K] = [F:E][E:K]$.

Definition 1.4. An element α in E is said to be algebraic over K if there exist elements $a_0, a_1, \ldots, a_n$ in K such that

$$a_0 + a_1\alpha + \ldots + a_n\alpha^n = 0.$$

Suppose E is an extension field of K and α is in E. Let $K(\alpha) = \bigcap E_i$, where $K \subset E_i$ and α is in E_i. Then $K(\alpha)$ is the smallest field containing both K and α, and

$$K(\alpha) = \left\{ \sum_{i=0}^{s} a_i\alpha^i : a_i \text{ is in } K \text{ and } s \text{ is a positive integer} \right\}.$$

Theorem 1.5. The element α in E is algebraic over K if and only if $K(\alpha)$ is a finite extension.

The element α in E is said to be algebraic of degree n over K if it satisfies a non-zero polynomial over K of degree n but no non-zero polynomial of lower degree.

Theorem 1.6. If α is algebraic of degree n over K then $[K(\alpha):K] = n$.

Definition 1.7. If E is an extension field of the rational numbers Q, and α is algebraic over Q, then α is said to be an algebraic number.

The algebraic numbers in an extension field form a field.

Definition 1.8. If $p(x)$ is in $K[x]$ then an element α in an extension field E of K is called a root of $p(x)$ if $p(\alpha) = 0$ in $E[x]$.

Theorem 1.9. If $p(x)$ is a polynomial in $K[x]$ of degree $n \geqq 1$ and is irreducible over K, then there is an extension E of K, such that $[E:K] = n$, and $p(x)$ has a root in E.

If $p(x)$ is an irreducible polynomial then the ideal $(p(x))$ is a maximal ideal in $K[x]$ and $K[x]/(p(x))$ is a field. This field has a root of $p(x)$ and $K[x]/(p(x))$ is isomorphic to $K(\alpha)$ where $p(\alpha) = 0$. The set $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis for $K(\alpha)$ over K.

Theorem 1.10. If α is algebraic over K, it has a unique irreducible minimal polynomial.

Let α be algebraic over K, and let $p(x)$ be its minimal polynomial of degree n. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be the roots of $p(x)$ in some extension field where $\alpha = \alpha_1$. These n numbers are distinct and are called the conjugates of α over K.

Any polynomial satisfied by α over K contains the minimal polynomial of α as a factor. Since $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis for

$K(\alpha)$ over K every element β in $K(\alpha)$ can be expressed uniquely in the form

$$(1.1) \qquad \beta = a_0 + a_1\alpha^1 + \ldots + a_{n-1}\alpha^{n-1} = r(\alpha),$$

where the a_i are in K and n is the degree of α over K.

Definition 1.11. Let $K(\alpha)$ be a finite extension of K and suppose β is in $K(\alpha)$. The conjugates of β for $K(\alpha)$ are $\beta_i = r(\alpha_i)$ where the α_i are the conjugates of α and $r(\alpha_i)$ is defined by replacing α by α_i in (1.1).

The polynomial

$$f(x) = \prod_{i=1}^{n} (x - r(\alpha_i))$$

is a polynomial over K called the field polynomial for β. If β is in $K(\alpha)$ and $g(x)$ is the minimum polynomial for β of degree m then $f(x) = [g(x)]^{n/m}$. If β is in E and E is of degree n over K then β has n conjugates $\beta_1, \beta_2, \ldots, \beta_n$ for E.

Definition 1.12. The norm of β is defined by

$$N(\beta) = N\beta = \prod_{i=1}^{n} \beta_i.$$

Theorem 1.13. $N\beta$ is in K.

Proof: See Pollard, p. 72.

In particular if

$$f(x) = \prod_{i=1}^{n} (x - \beta_i) = \sum_{i=0}^{n} a_i x^i$$

is the field polynomial for β then $N\beta = (-1)^n a_0$. If

$$g(x) = x^m + b_1 x^{m-1} + \ldots + b_m$$

is the minimum polynomial for β then $N\beta = (\pm b_m)^{n/m}$ where $m|n$.

Theorem 1.14. $N(\beta\gamma) = N(\beta)N(\gamma)$.

Proof: See Pollard, p. 72.

Number Theory

The rational integers will be referred to in this study as integers. The integers form a unique factorization domain. For any two integers a and b, (a,b) exists and $(a,b) = as + bt$ for some integers s and t. If $(a,b) = 1$, we say a and b are relatively prime.

Let $\emptyset(m)$ denote the number of positive integers less than or equal to m and relatively prime to m. We have

$$\emptyset(m) = \prod_{i=1}^{k} p_i^{\alpha_i - 1} (p - 1)$$

where

$$m = \prod_{i=1}^{k} p_i^{\alpha_i}.$$

Theorem 1.15. (Euler's Theorem) If $(a,m) = 1$ then $a^{\emptyset(m)} \equiv 1 \pmod{m}$.

Theorem 1.16. (Fermat's Theorem) If p is a prime and if $(a,p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$.

Theorem 1.17. The linear congruence $ax \equiv b \pmod{m}$ has a solution if and only if $(a,m)|b$.

Consider the quadratic congruence $x^2 \equiv a \pmod{p}$ where p is a prime. If $(a,p) = 1$ and this congruence has a solution, a is said to be a quadratic residue modulo p. If a is not a quadratic residue modulo p, it is called a quadratic nonresidue modulo p. Let $(a,p) = (b,p) = 1$. The following properties hold:

(a) If a and b are quadratic residues, so is ab.

(b) If a and b are quadratic nonresidues, then ab is a quadratic residue.

(c) If a is a quadratic residue and b is a quadratic nonresidue, then ab is a quadratic nonresidue.

Theorem 1.18. Suppose $(a,p) = 1$. If p is of the form $4k + 1$, then $-a$ is a quadratic residue $\pmod{p}$ if and only if a is a quadratic residue. If p is of the form $4k + 3$ then $-a$ is a quadratic nonresidue $\pmod{p}$ if and only if a is a quadratic residue.

Theorem 1.19. If the prime number p is of the form $8k \pm 1$ then 2 is a quadratic residue $\pmod{p}$. If p is of the form $8k \pm 3$ then 2 is a quadratic nonresidue $\pmod{p}$.

For any integer n and any prime p, $n = p^r m$ where $(p,m) = 1$. The exponent r is said to be the <u>ordinal</u> of n with respect to p and written $\text{ord}_p n = r$. Any integer n can be expressed uniquely in the form

$$n = \sum_{i=0}^{r} a_i p^i,$$

where $0 \leqq a_i \leqq p - 1$.

<u>Theorem 1.20</u>. Suppose n is a positive integer. Let

$$n = \sum_{i=0}^{r} a_i p^i,$$

where $0 \leqq a_i \leqq p - 1$. Then $\text{ord}_p(n!) = \dfrac{n - t_n}{p - 1}$ where

$$t_n = \sum_{i=0}^{r} a_i.$$

<u>Proof</u>: Let $t_0 = 0$. For each k such that $1 \leqq k \leqq n$, we have that

$$k = \sum_{i=m}^{r} b_i p^i$$

where $\text{ord}_p k = m$. Now,

$$k - 1 = -1 + \sum_{i=m}^{r} b_i p^i = \sum_{i=0}^{m-1} (p - 1)p^i + (b_m - 1)p^m + \sum_{i=m+1}^{r} b_i p^i.$$

Hence,

$$t_{k-1} = m(p - 1) + (b_m - 1) + \sum_{i=m+1}^{r} b_i = m(p - 1) + t_k - 1.$$

But this implies that $m = (t_{k-1} - t_k + 1)/(p - 1)$. Therefore,

$$\text{ord}_p(n!) = \sum_{k=1}^{n} \text{ord}_p k = 1/(p - 1) \sum_{k=1}^{n} (t_{k-1} - t_k + 1) = \frac{n - t_n}{p - 1}.$$

Metric Spaces

A <u>metric</u> for a set S is a function d from $S \times S$ into R such that

$$d(x,y) \geqq 0 \text{ with equality only if } x = y,$$

$$d(x,y) = d(y,x),$$

$$d(x,z) \leqq d(x,y) + d(y,z)$$

for each x, y, and z in S. The set S with metric d is a <u>metric space</u>. Elements of the space are called points.

In a metric space (S,d), the set

$$S(x,r) = \{y: d(x,y) < r\}$$

is called an <u>open sphere</u> with center x and radius r. The set

$$S[x,r] = \{y: d(x,y) \leqq r\}$$

is a closed sphere with center x and radius r.

Let (S,d) be a metric space. Then X, a subset of S, is <u>open</u> if for each x in X there exists an open sphere $S(y,r)$ such that x is in $S(y,r)$ and $S(y,r)$ is a subset of X. An open sphere is an open set. A point x of a metric space (S,d) is an accumulation point of the set S if every open set containing x also contains a point of S distinct from x. A subset of a metric space is closed if its complement is open. Closed sets contain all their accumulation points. Closed spheres are closed sets. The closure of a set S is the union of S with the set of all accumulation points of S.

A sequence is a function s from the non-negative integers into some set T. It is customary to write s_n instead of $s(n)$ to indicate the sequence value at n and to write $\{s_n\}$ to indicate the sequence. If $\{t_m\}$ is a sequence obtained from $\{s_n\}$ by the deletion of certain elements, the remaining elements retained in their original order, then $\{t_m\}$ is a subsequence of $\{s_n\}$. Two sequences $\{s_n\}$ and $\{t_n\}$ are equal, $\{s_n\} = \{t_n\}$ if and only if $s_n = t_n$ for each $n \geqq 0$. A set X is dense in S if for each s in S there exists a sequence $\{x_n\}$ in X such that $\lim x_n = s$.

Let (S,d) be a metric space. A sequence $\{s_n\}$ of S converges with respect to d to a point s if for each $\varepsilon > 0$ there exists an N such that $d(s_n,s) < \varepsilon$ whenever $n \geqq N$.

Let S and d be respectively, the set of real numbers and the ordinary absolute value function. Suppose $\{s_n\}$ is a sequence of real numbers, and $E = \{s\colon s = \lim s_{n_i}$ for some subsequence $\{s_{n_i}\}\}$. This set contains all subsequential limits with possibly $+\infty$ and $-\infty$. Then we define $\overline{\lim}\, s_n =$ lub of E, where lub stands for the least upper bound of E. Similarly, $\underline{\lim}\, s_n =$ glb of E where glb stands for the greatest lower bound of E. The usual results about sequences in the metric space of real numbers will be assumed.

CHAPTER II

VALUATIONS

The notion of a valuation is encountered at a very early stage by the student of mathematics. The ordinary absolute value function defines a valuation on the set of integers. This function can be extended uniquely to the rational numbers, the quotient field of the integers. A further extension can be made to the field of real numbers in which every Cauchy sequence converges to a real number. With a function similar to the absolute value function this process can be generalized on the set of rationals. The resulting extension field is very interesting and useful in current research. These concepts will be investigated in the ensuing discussion.

Definition 2.1. A valuation is a function v from an integral domain D into the non-negative real numbers such that

$$v(a) \geqq 0 \quad \text{and} \quad v(a) = 0 \quad \text{if and only if} \quad a = 0, \tag{2.1}$$

$$v(ab) = v(a)v(b), \tag{2.2}$$

$$v(a + b) \leqq v(a) + v(b). \tag{2.3}$$

In the theory of valuations the valuation defined here is referred to as "rank one valuation." The rank one valuation defined in definition 2.1 is the most interesting special case in the general theory of valuations. It is of importance in the valuation-theoretic approach to algebraic number theory. In this paper the term "valuation" will refer to a rank one valuation. For a general development the reader is referred to the references [4], [11], [12] or [16] in the bibliography.

Before proceeding further, a clarification of the term "extended" is needed.

Definition 2.2. Suppose K and E are fields with valuations v and v_1, respectively. If K is a subfield of E and for each a in K, $v_1(a) = v(a)$, then v_1 is said to be an extension of v. The valuation v is said to be a restriction of v_1 to K.

Now if v is a valuation defined on an integral domain D and if K is the quotient field of D, define a function v_1 on K by

$$v_1(a/b) = v(a)/v(b) \tag{2.4}$$

for each non-zero element a/b of K, and $v_1(0) = 0$.

Theorem 2.3. The function v_1 is a valuation of K and v_1 restricted to D is the valuation v.

Proof: By definition v_1 is non-negative and $v_1(0) = 0$. The equation

$$v_1\left(\frac{a}{b} \cdot \frac{c}{d}\right) = \frac{v(ac)}{v(bd)} = \frac{v(a)}{v(b)} \cdot \frac{v(c)}{v(d)} = v_1\left(\frac{a}{b}\right) v_1\left(\frac{c}{d}\right)$$

shows v_1 satisfies (2.2). Now,

$$v_1\left(\frac{a}{b} + \frac{c}{d}\right) = v_1\left(\frac{ad + bc}{bd}\right) = \frac{v(ad + bc)}{v(bd)} \leq \frac{v(ad) + v(bc)}{v(bd)}$$

$$= \frac{v(a)}{v(b)} + \frac{v(c)}{v(d)} = v_1(a/b) + v_1(c/d).$$

Therefore, v_1 satisfies (2.3). For each a in D, $a = ab/b$ and $v_1(a) = v(ab)/v(b) = v(a)$. Hence, v_1 restricted to D is the valuation v.

Note further that if v_1 and v_2 are both valuations defined on the quotient field K of D satisfying (2.4) that for each a/b in K,

$$v_1(a/b) = v(a)/v(b) = v_2(a/b).$$

In other words, v_1 is the only extension of v defined on K in this manner. Since this extension process of valuations can be carried out on any integral domain, further discussion will be primarily concerned with valuations defined on a field K.

Property (2.2) states that a valuation v is a homomorphism from the multiplicative group of a field K into the non-negative real numbers. Consequently, v satisfies the following properties:

$$(2.5) \qquad v(1) = 1,$$

$$(2.6) \qquad v(a^{-1}) = v(a)^{-1},$$

and

$$(2.7) \qquad v(a/b) = v(a)/v(b).$$

Furthermore, $v(-1)v(-1) = v(1) = 1$, which implies

$$(2.8) \qquad v(-1) = 1.$$

Now,

$$v(a) - v(b) = v(a + b - b) - v(b) \leq v(a + b) + v(b) - v(b) = v(a + b).$$

Similarly, $v(b) - v(a) \leq v(a + b)$. Therefore, v satisfies

(2.9) $$|v(a) - v(b)| \leq v(a + b).$$

Definition 2.4. A valuation v that satisfies the stronger inequality $v(a + b) \leq \max \{v(a), v(b)\}$ is called a non-archimedean valuation. All others are called archimedean valuations.

The following theorem gives a characterization of a non-archimedean valuation.

Theorem 2.5. For a valuation, v, the following statements are equivalent:

(2.10) v is a non-archimedean valuation

(2.11) $v(a) \leq 1$ implies $v(1 + a) \leq 1$

(2.12) $v(n) \leq 1$ for all natural numbers n.

Proof: (2.10) implies (2.11):

Suppose v is non-archimedean and $v(a) \leq 1$. Then

$$v(1 + a) \leq \max \{v(a), 1\} = 1.$$

(2.11) implies (2.12):

Now $v(1) = 1$ by (2.5). Suppose $v(k) \leq 1$, then

$$v(k + 1) \leq 1$$

and (2.11) follows by induction

(2.12) implies (2.10):

Without loss of generality, suppose $v(a) \leq v(b)$. Then,

$$v(a^{n-i}b^{i}) = v(a^{n-i})v(b^{i}) = [v(a)]^{n-i}[v(b)]^{i} \leq [v(b)]^{n} = [\max\{v(a),v(b)\}]^{n}.$$

Since $v\left[\binom{n}{i}\right] \leq 1$ we have that

$$[v(a + b)]^{n} = v[(a + b)^{n}] = v\left(\sum_{i=0}^{k}\binom{n}{i}a^{n-i}b^{i}\right) \leq (n + 1)[\max\{v(a),v(b)\}]^{n}.$$

Thus,

$$v(a + b) \leq \sqrt[n]{(n + 1)}\ \max\{v(a),v(b)\}.$$

If we consider the limit as n becomes infinite then

$$v(a + b) = \lim v(a + b) \leq \lim \sqrt[n]{(n + 1)}\ \max\{v(a),v(b)\} = \max\{v(a),v(b)\}.$$

The following theorem and especially its corollaries are very useful in some of the theorems to follow.

Theorem 2.6. If v is a non-archimedean valuation on k and $v(a) > v(b)$ then $v(a + b) = v(a)$.

Proof: Since $v(b) < v(a)$ we have

$$\begin{aligned} v(a) = v(a + b - b) &\leq \max\{v(a + b),v(b)\} = v(a + b) \\ &\leq \max\{v(a),v(b)\} = v(a). \end{aligned}$$

Therefore,

$$v(a) = v(a + b).$$

Corollary 2.7. If v is a non-archimedean valuation on k and $v(a) \neq v(b)$ then $v(a + b) = \max\{v(a),v(b)\}$.

Corollary 2.8. If v is a non-archimedean valuation on k and $v(a_1) > v(a_i)$, $i = 2, 3, \ldots, n$, then $v(a_1 + a_2 + \ldots + a_n) = v(a_1)$.

Corresponding to theorem 2.5 the following characterization is given for an archimedean valuation.

Theorem 2.9. For a valuation v the following statements are equivalent:

(2.13) v is archimedean

(2.14) $v(n) > 1$ for any natural number $n \geqq 2$.

Proof: (2.13) implies (2.14):

Suppose there exists an integer $m \geqq 2$ such that $v(m) \leqq 1$. For each integer $n \geqq 2$ the division algorithm can be used repeatedly to write

$$n = \sum_{i=0}^{k} a_i m^i,$$

where $0 \leqq a_i \leqq m - 1$ and $a_k \neq 0$. Since $m^k \leqq n < m^k + 1$, we have that $k \leqq \log_m n$. Now for any integer j,

$$v(j) \leqq \sum_{i=1}^{j} v(1) = |j|$$

so that,

$$v(n) = v\left(\sum_{i=0}^{k} a_i m^i\right) \leqq \sum_{i=0}^{k} v(a_i)v(m^i) \leqq \sum_{i=0}^{k} v(a_i) \leqq \sum_{i=0}^{k} a_i \leqq \sum_{i=0}^{k} (m - 1)$$

$$= (m - 1)(1 + k) \leqq (m - 1)(1 + \log_m n).$$

Hence, for any positive integer s,

$$[v(n)]^s = v(n^s) \leq (m - 1)(1 + \log_m n^s) = (m - 1)(1 + s \cdot \log_m n).$$

Therefore,

$$v(n) \leq \lim_{s\to\infty} \sqrt[s]{(m - 1)(1 + s \cdot \log_m n)} = 1.$$

By (2.12) of theorem 2.5 we have that v is non-archimedean, which is a contradiction.

(2.14) implies (2.13):

By part (2.12) of theorem 2.5, if v is non-archimedean then $v(n) \leq 1$ for all natural numbers n. This statement is the contrapositive of the statement we wish to prove.

Several examples will now be considered. As mentioned previously, the ordinary absolute value function is a valuation on the set of rational numbers. This same function is a valuation on the field of real numbers as well as the field of complex numbers. Since $|n| > 1$ for any natural number $n \geq 2$, it follows that the absolute value function is an archimedean valuation. A similar example follows.

Example 2.10. Let C be the set of complex numbers and define $v(a) = |a|^r$ for a in C and $0 < r \leq 1$, where r is a real number. Properties (2.2) and (2.3) follow from the corresponding properties of the absolute value function. Property (2.3) follows also since for $|a| \geq |b|$ we have,

$$v(a + b) = |a + b|^r = |a|^r \; |1 + b/a|^r \leq |a|^r \, (1 + |b/a|)^r$$

$$\leq |a|^r \; (1 + |b/a|) \leq |a|^r \; (1 + |b/a|^r) = v(a) + v(b).$$

Example 2.11. Let D be a unique factorization domain and suppose K is the field of quotients of D. For a fixed prime π in D and for any element x in K, x has the form $x = \pi^k(a/b)$ where a, b and π are pairwise relatively prime. Define a function v on K by letting $v(x) = c^k$, where c is a real number such that $0 < c \leq 1$. Properties (2.2) and (2.3) follow readily. By definition of v, if $v(x) \leq 1$ for $x = \pi^k(a/b)$ then $k \geq 0$, a and b are relative prime, and $\pi \nmid b$. Then $1 + x = 1 + a/b = (a + b)/b$ where $\pi \nmid b$ so that $v(1 + x) \leq 1$. By theorem 2.5, v is a non-archimedean valuation.

As a special case of example 2.11, consider the set of Gaussian integers $G = \{a + bi\colon a$ and b are in Z and $i = \sqrt{-1}\}$. The set of Gaussian integers is a unique factorization domain and $1 + 2i$ is a prime element. If G' denotes the quotient field of G then each element x in G can be written as $x = (1 + 2i)^h(\alpha/\beta)$ where α, β and $1 + 2i$ are pairwise relatively prime. Define a mapping v by $v(x) = c^h$ for $0 < c \leq 1$. Then v will be a non-archimedean valuation.

Another unique factorization domain is the set of integers Z which has the rational numbers as a quotient field. For each prime p of Z a mapping may be defined on Q by setting $v(x) = c^h$, where $x = p^h(a/b)$, $0 < c \leq 1$, and $(a,b) = (a,p) = (b,p) = 1$. This discussion gives another example of a non-archimedean valuation.

Definition 2.12. The valuations defined on Q by using a fixed prime p are called p-adic valuations. If c is taken to be $1/p$ the resulting valuation is referred to as the normalized p-adic valuation, and will be denoted by $|\ |_p$.

Example 2.13. Let $C(z)$ be the set of all meromorphic functions of a complex variable z defined on a Riemann surface. Each function $f(z)$ of $C(z)$ has a laurent expansion of the form

$$f(z) = \sum_{n=-k}^{\infty} a_n(z - z_o)^n$$

where $k \geq 0$ and z_o is a fixed complex number. Define a function v by $v[f(z)] = c^h$ where c is a real number such that $0 < c \leq 1$, and a_h is the first non-zero coefficient in the laurent expansion of $f(z)$. Let $v(0) = 0$ for the zero function. With this definition the function v is a non-archimedean valuation defined on $C(z)$.

Finally, we can define a trivial valuation on a field K in the following manner.

Example 2.14. Define a function on a field K by $v(a) = 1$ for each a in K such that $a \neq 0$, and $v(0) = 0$. Since

$$v(a + b) = 1 = \max\{v(a), v(b)\}$$

for each a and b in K the trivial valuation is a non-archimedean valuation. For $c = 1$ in Example 2.11 we have the trivial valuation.

For any field K of characteristic p, a non-archimedean valuation is the only valuation that can be defined as shown in the next theorem.

Theorem 2.15. If K is a field of characteristic p with a valuation v then v is non-archimedean.

Proof: For each a and b in K, $(a + b)^{p^n} = a^{p^n} + b^{p^n}$. Thus,

$$\begin{aligned}[v(a + b)]^{p^n} &= v[(a + b)^{p^n}] = v(a^{p^n} + b^{p^n}) \\ &\leq v(a^{p^n}) + v(b^{p^n}) = [v(a)]^{p^n} + [v(b)]^{p^n} \\ &\leq 2[\max\{v(a),v(b)\}]^{p^n}.\end{aligned}$$

Therefore,

$$v(a + b) \leq \sqrt[p^n]{2}\max\{v(a),v(b)\}.$$

The same argument used in theorem 2.5 shows that

$$v(a + b) \leq \max\{v(a),v(b)\}.$$

Equivalent Valuations

Definition 2.16. Two non-trivial valuations v_1 and v_2 defined on a field K are said to be equivalent if $v_1(a) < 1$ implies $v_2(a) < 1$.

Theorem 2.17. Equivalence of valuations is an equivalence relation.

Proof: See Mosley, p. 47 or Snook, p. 58.

In example 2.10 it was shown that the absolute value function defined on the set of complex numbers can be used to define a valuation for each real number r such that $0 < r \leq 1$. In an analogous manner a non-archimedean valuation may be defined on a field K for each real number r, for which $0 < r \leq 1$. It is not too surprising to find that equivalent valuations are related in this manner.

Theorem 2.18. If v_1 and v_2 are equivalent valuations then $v_1(a) = [v_2(a)]^r$ for some real number r.

Proof: See Mosley, p. 48 or Snook, p. 56.

At this time it is convenient to define what is meant by the limit of a sequence in a valuated field K. The definition is stated exactly as it occurs in the case when K is the field of real numbers and the valuation is the ordinary absolute value.

Definition 2.19. Let K be a field with a valuation v. A sequence $\{a_n\}$ from K is said to converge to the element a of K if for each real number $\varepsilon > 0$ there is a natural number N such that

$$v(a_n - a) < \varepsilon$$

whenever $n \geqq N$.

To denote that a sequence $\{a_n\}$ converges to a, the same notation will be used here that is used for the absolute value, namely, $\lim_{n\to\infty} a_n = a$ or briefly, $\lim a_n = a$.

Definition 2.20. Two valuations v_1 and v_2 determine the same convergence criteria if for each sequence $\{x_n\}$ there exists an x such that $\lim v_1(x_n - x) = 0$ if and only if $\lim v_2(x_n - x) = 0$.

The following theorem gives another characterization of equivalent valuations.

Theorem 2.21. Two non-trivial valuations v_1 and v_2 defined on a field K are equivalent if and only if they determine the same convergence criterion.

Proof: See Snook, p. 59.

Metric Properties of a Valuated Field

A failing of the set of rational numbers is the fact that bounded Cauchy sequences of rationals exist which do not converge in this set. Some of the most interesting Cauchy sequences of rational numbers such as

$$\left\{\left(1 + \frac{1}{n}\right)^n\right\}$$

do not converge to rational numbers. In this sense the rationals are somewhat incomplete.

One method to remedy this situation is to construct the set of real numbers by means of Cauchy sequences of rational numbers. In this process the convergence of sequences is defined in terms of the absolute value function. Since the absolute value function is a valuation, it seems probable that this process could be generalized for any field with a given valuation. This is actually the case, and in the ensuing discussion it will be demonstrated that an arbitrary field with a given valuation can be extended to a so-called complete field where all Cauchy sequences have a limit. A few familiar definitions are needed.

Definition 2.22. Let K be a field with a valuation v. A sequence $\{a_n\}$ from K is a Cauchy sequence with respect to the valuation v

if for each real number $\varepsilon > 0$ there is a natural number N such that $v(a_m - a_n) < \varepsilon$ whenever $m, n > N$. The sequence $\{a_n\}$ is bounded if there is a positive real number M such that $v(a_n) < M$ for each natural number n.

Definition 2.23. The sequence $\{a_n\}$ is a null sequence with respect to the valuation v provided that for each $\varepsilon > 0$ there is a natural number N such that $v(a_n) < \varepsilon$ whenever $n > N$.

With these definitions many theorems about limits can be proved in exactly the same manner as those of elementary calculus. The proofs depend on the fact that the range of a valuation is a subset of the non-negative real numbers. The theorems are stated here without proof.

Theorem 2.24. If $\{a_n\}$ converges to s and also to t then $s = t$.

Theorem 2.25. Every convergent sequence is a Cauchy sequence.

Theorem 2.26. Every Cauchy sequence is bounded.

Theorem 2.27. If $\{a_n\}$ converges to s and $\{b_n\}$ converges to t then

(a) $\lim ca_n = cs$,

(b) $\lim (c + a_n) = c + s$,

(c) $\lim (a_n + b_n) = s + t$,

(d) $\lim a_n b_n = st$,

(e) if $t \neq 0$ and $b_n \neq 0$ for all n then $\lim (a_n/b_n) = s/t$.

The next theorem will be very useful in later discussion.

Theorem 2.28. Suppose K is a field with a valuation. If $\lim a_n = a$ then $\lim v(a_n) = v(a)$.

Proof: For each $\varepsilon > 0$ there exist an N such that for $n \geqq N$, $v(a_n - a) < \varepsilon$. By (2.9), $|v(a_n) - v(a)| < \varepsilon$ so that

$$\lim v(a_n) = v(a).$$

Definition 2.29. A field K is said to be complete with respect to a valuation v if every Cauchy sequence has a limit in K.

The real numbers are complete with respect to the ordinary absolute value function, a fact that will be accepted here.

Let B, C and M denote, respectively, the set of all bounded sequences, the set of all Cauchy sequences and the set of all null sequences of a field K with respect to a given valuation. In the sequel the completion process is outlined in a number of lemmas, some of which are stated without proof.

Lemma 2.30. $M \subset C \subset B$.

Lemma 2.31. If $\{a_n\}$ is a Cauchy sequence containing a null subsequence, then $\{a_n\}$ is a null sequence.

Proof: Suppose $\{a_{n_i}\}$ is a null subsequence of $\{a_n\}$. Choose $\varepsilon > 0$. There exists an N_1 such that for $n_i \geqq N_1$, $v(a_{n_i}) < \varepsilon/2$. There exists an N_2 such that for m, $n > N_2$, $v(a_m - a_n) < \varepsilon/2$. This implies that $v(a_m) < v(a_n) + \varepsilon/2$. Now if m, $n_i > \max\{N_1,N_2\}$ then $v(a_m) < v(a_{n_i}) + \varepsilon/2 < \varepsilon$. Hence, $\{a_n\}$ is a null sequence.

The next lemma is a consequence of the preceeding one.

Lemma 2.32. If $\{a_n\}$ is a Cauchy sequence which is not a null sequence then there exists a real number $\delta > 0$ and an N such that $v(a_n) > \delta$ whenever $n > N$.

Lemma 2.33. If $\{a_n\}$ and $\{b_n\}$ are in C then $\{-a_n\}$, $\{a_n + b_n\}$ and $\{a_n b_n\}$ are in C.

Lemma 2.34. If $\{a_n\}$ and $\{b_n\}$ are in M then $\{-a_n\}$, $\{a_n + b_n\}$ and $\{a_n b_n\}$ are in M.

With the aid of Lemma 2.32 two binary operations can be defined on C that will make it a commutative ring with unity. Let the sum and product of sequences be defined by

$$\{a_n\} + \{b_n\} = \{a_n + b_n\} \tag{2.15}$$

and

$$\{a_n\} \cdot \{b_n\} = \{a_n b_n\}. \tag{2.16}$$

Lemma 2.35. The set C with addition and multiplication defined by (2.15) and (2.16) is a commutative ring with unity.

Lemma 2.36. The set M is a maximal ideal in C.

Proof: M is closed under addition and subtraction by Lemma 2.34. Suppose $\{a_n\}$ is a sequence in C and $\{b_n\}$ is a sequence in M. Let B be a bound for $\{a_n\}$. For each $\varepsilon > 0$ there is an N such that for $n > N$, $v(b_n) < \varepsilon/B$. Hence,

$$v(a_n b_n) = v(a_n)v(b_n) \leq Bv(b_n) < \varepsilon.$$

This verifies M is an ideal in C. To show maximality suppose there is an ideal I in C distinct from M such that $M \subset I \subset C$. There is a sequence $\{a_n\}$ in I such that $\{a_n\}$ is not in M. Since $\{a_n\}$ is a non-null sequence there exists an N_1 and a $\delta > 0$ such that for each $n > N_1$, $v(a_n) > \delta$. Define a sequence $\{b_n\}$ by letting $b_n = 0$ for $n \leq N_1$ and $b_n = 1/a_n$ for $n > N_1$. For $\varepsilon > 0$ there exists an N_2 such that for m, $n > N_2$, $v(a_m - a_n) < \varepsilon \cdot \delta^2$. If $N = \max\{N_1, N_2\}$ then for n, $m \geqq N$

$$v(b_m - b_n) = v(1/a_m - 1/a_n) = \frac{v(a_n - a_m)}{v(a_n)v(a_m)} < \frac{\varepsilon\delta^2}{\delta^2} = \varepsilon.$$

Hence, $\{b_n\}$ is a Cauchy sequence. Let $\{c_n\}$ be the sequence defined by $c_n = 1$ for $n \leq N_1$ and $c_n = 0$ for $n > N_1$. Now $\{c_n\}$ is in $M \subset I$ and $\{a_n b_n\}$ is in I which implies $\{1\} = (\{c_n\} + \{a_n b_n\})$ is in I. Therefore, $I = C$ and M is a maximal ideal.

<u>Lemma 2.37</u>. The quotient ring C/M is a field.

<u>Definition 2.38</u>. Denote C/M by E. For $\{a_n\} + M$ in E define $v_1(\{a_n\} + M) = \lim v(a_n)$.

<u>Lemma 2.39</u>. v_1 is a valuation on the field E.

<u>Proof</u>: Since $|v(a_m) - v(a_n)| \leq v(a_m - a_n)$ and $\{a_n\}$ is a Cauchy sequence, the sequence $\{v(a_n)\}$ is a Cauchy sequence of real numbers. This implies the $\lim v(a_n)$ exists since the real numbers are complete. Therefore, v_1 is well defined. To establish (2.1) of definition 2.1, if $v_1(a_n + M) = 0$ then $\lim v(a_n) = 0$. This means that $\{a_n\}$ is a null sequence and $\{a_n\} + M = M$, where M is the zero of the quotient

ring E. When $\{a_n\}$ is a non-null sequence

$$v_1(a_n + M) = \lim v(a_n) > 0.$$

The following equations,

$$\begin{aligned} v_1[(\{a_n\} + M) + (\{b_n\} + M)] &= v_1(\{a_n + b_n\} + M) \\ (2.17) \qquad &= \lim v(a_n + b_n) \leq \lim v(a_n) + \lim v(b_n) \\ &= v_1(\{a_n\} + M) + v_1(\{b_n\} + M) \end{aligned}$$

$$\begin{aligned} v_1[(\{a_n\} + M)(\{b_n\} + M)] &= v_1(\{a_nb_n\} + M) \\ (2.18) \qquad &= \lim v(a_nb_n) = \lim v(a_n)\lim v(b_n) \\ &= v_1(\{a_n\} + M)v_1(\{b_n\} + M) \end{aligned}$$

serve to establish (2.2) and (2.3) of definition 2.1. Therefore, v_1 is a valuation on the field E.

Lemma 2.40. The field K is isomorphic to a subfield of E.

Proof: For each a in K the element $a^* = \{a\} + M$ is in E. Let f be defined by $f(a) = a^*$. Now $a = b$ implies that $a^* = b^*$, or $f(a) = f(b)$. If $f(a) = f(b)$ then $\{a\} + M = \{b\} + M$. Hence, $\{a - b\} + M = M$ and $\{a - b\}$ is a null sequence. But this implies $a = b$. From the equations

$$f(a + b) = (a + b)^* = a^* + b^* = f(a) + f(b)$$

and

$$f(ab) = (ab)^* = a^*b^* = f(a)f(b)$$

we can deduce that f is an isomorphism.

In further discussion the symbol a^* will denote the coset $\{a\} + M$ where $\{a\}$ is a constant sequence in K. The field K is isomorphic to the field $f(K) \subset E$, and we may consider K as a subfield of E. The element a of K is to be identified with a^* of E in the same sense that the natural number n is identified as the integer n^+.

Definition 2.41. If two fields K and K' are isomorphic and the isomorphism preserves distances then K and K' are said to be isometric.

Lemma 2.42. The field K and $f(K)$ are isometric.

Proof: For each a^* in $f(K)$,

$$v_1(a^*) = v_1(\{a\} + M) = \lim v(a) = v(a).$$

Therefore, $v_1(a^* - b^*) = v_1\{(a - b)^*\} = v(a - b)$.

Theorem 2.43. The field $f(K)$ is dense in E.

Proof: Let α be an element of E. We will show that there is a sequence in $f(K)$ that converges to α. Now $\alpha = \{a_n\} + M$ where $\{a_n\}$ is a sequence in K. For each term a_m of the sequence $\{a_n\}$ in K there is an element a_m^* in $f(K)$. Now

$$\alpha - a_m^* = \{a_n - a_m\}_{n=1}^{\infty} + M.$$

Since $\{a_n\}$ is a Cauchy sequence, for each $\varepsilon > 0$ there is an N such that for n and $m \geqq N$ we have that $v(a_n - a_m) < \varepsilon/2$. Then for $m \geqq N$,

$$v_1(\alpha - a_m^*) = \lim v_1(a_n - a_m) \leqq \varepsilon/2 < \varepsilon.$$

Therefore, the sequence $\{a_m^*\}$ converges to α.

Theorem 2.44. The field E is complete.

Proof: Let $\{\alpha_n\}$ be a Cauchy sequence in K. Since $f(K)$ is dense in E there is a sequence $\{a_m^{(n)*}\}$ in $f(K)$ such that

$$\alpha_n = \lim a_m^{(n)*}.$$

For each n choose a term $a_{(n)}^*$ of the sequence $\{a_m^{(n)*}\}$ such that $v_1(\alpha_n - a_{(n)}^*) < 1/n$. By this process we can construct a sequence $\{a_{(n)}^*\}$ in $f(K)$. This sequence determines the sequence $\{a_{(n)}\}$ in K. Now K and $f(K)$ are isometric. Thus, for each $\varepsilon > 0$, there is an N such that for k and $n \geqq N$,

$$v(a_{(n)} - a_{(k)}) = v_1(a_{(n)}^* - \alpha_n) + v_1(\alpha_n - \alpha_k) + v_1(\alpha_k - a_{(n)}^*)$$

$$< 1/n + \varepsilon/2 + 1/k < \varepsilon.$$

This implies that $\{a_{(n)}\}$ is a Cauchy sequence in K so that $\alpha = \{a_{(n)}\} + M$ is in E. Now

$$\lim_{n\to\infty} v_1(\alpha - a_{(n)}^*) = \lim_{n\to\infty} \lim_{n\to\infty} v(a_{(m)} - a_{(n)}) = 0$$

which implies that $\alpha = \lim a_{(n)}^*$.

$$v_1(\alpha - \alpha_n) \leq v_1(\alpha - a^*_{(n)}) + v_1(a^*_{(n)} - \alpha_n).$$

The last two terms can be made as small as we please. Therefore,

$$\alpha = \lim \alpha_n$$

and E is complete.

The preceeding theorems and lemmas demonstrate how a given field K with a valuation v can be embedded in a field E where all Cauchy sequences of E converge to an element of E. This process is a generalization of the Cantor method of completing the rationals with respect to the absolute value function. For each a in K we have an element a^* in E and $v_1(a^*) = \lim v(a) = v(a)$. By the identification of a with a^*, we see that $v_1(a) = v(a)$. In this sense the valuation v_1 on E is an extension of the valuation v on K.

Valuation Rings

Associated with any field having a non-archimedean valuation is a special ring referred to as a valuation ring. This ring contains the ring of integers as a subset. It also has the property that it has a unique maximal ideal. There are many similarities between this ring and the ring of integers which will be investigated in the ensuing discussion.

Definition 2.45. For a field K with a non-archimedean valuation v let $V = \{a \text{ in } K: v(a) \leq 1\}$ and $P = \{a \text{ in } K: v(a) < 1\}$.

The following theorems follow rather easily.

Theorem 2.46. Suppose K is a field with a set V defined above. Then v is an integral domain and K is the field of quotients of V.

Proof: That V is a ring with unity follows from the following statements:

$$v(a - b) \leq \max\{v(a), v(b)\} \leq 1$$

$$v(ab) = v(a)v(b) \leq 1$$

for each a and b in V, and

$$v(1) = 1.$$

The ring V is an integral domain since it is a subring of a field. For each a in K, if $v(a) \leq 1$ then a is in V. If $v(a) > 1$ then $v(a^{-1}) < 1$ and a^{-1} is in V. Hence, $a = 1/(a^{-1})$ and a is a quotient of elements of V.

Theorem 2.47. P is a unique maximal ideal of V.

Proof: Suppose a and b are in P, then

$$v(a - b) \leq \max\{v(a), v(b)\} < 1,$$

which implies a - b is in P. For each a in V and b in P we have $v(ab) = v(a)v(b) < 1$. This implies ab is in P. Therefore, P is an ideal in V. Now if I is an ideal of V such that

$$P \subset I \subset V$$

and $P \neq I$, then there is an a in I that is not in P. But then $v(a) = 1$ and also $v(a^{-1}) = v(a)^{-1} = 1$. Thus a^{-1} is in V and $1 = aa^{-1}$ is in I. Therefore, I = V and P is a maximal ideal in

V. If M is any ideal of V such that $P \neq M$ then there is an element a of M such that a is not in P. As argued previously, $M = V$. Therefore, any proper ideal of V is contained in P.

Since P is a maximal ideal of V the quotient ring V/P is a field.

Definition 2.48. The field V/P is called the associated residue class field.

For any valuation v let $v(K^*) = \{x: \ x = v(a) \ \text{for some} \ a \in K^*\}$ where $K^* = K - \{0\}$.

Theorem 2.49. $v(K^*)$ is a multiplicative subgroup of the non-negative real numbers.

Proof: For each x and y in K^*, $x = v(a)$ and $y = v(b)$ for some a and b in K^*. Hence, $xy = v(a)v(b) = v(ab)$ is in $v(K^*)$. We also have $x^{-1} = v(a)^{-1} = v(a^{-1})$ is in $v(K^*)$. Therefore, $v(K^*)$ is a multiplicative subgroup of the non-negative real numbers.

Definition 2.50. The group $v(K^*)$ is called the value group for the valuation v. The non-archimedean valuation v is called discrete whenever its value group $v(K^*)$ is an infinite cyclic group.

An example of a discrete valuation was given in example 2.11. The p-adic numbers arise from the completion of the rational numbers with respect to a discrete valuation of this type. The following theorem is valid for non-archimedean valuations in general. It will be important later for a characterization of elements in a complete field with respect to a discrete valuation.

Theorem 2.51. If K is a field with a non-archimedean valuation v and E is the completion of K then $v(K^*) = v(E^*)$.

Proof: Suppose α is a non-zero element of E, then $\alpha = \lim a_n$ where $\{a_n\}$ is a sequence in K. There is an N such that for $n > N$, $v(\alpha - a_n) < v(\alpha)$. Therefore, by Corollary 2.7,

$$v(a_n) = v[\alpha + (a_n - \alpha)] = v(\alpha).$$

This implies that $v(\alpha)$ is in $v(K^*)$ and we have that

$$v(E^*) \subset v(K^*) \subset v(E^*).$$

Denote the valuation ring and maximal ideal of E by V_1 and P_1, respectively. If V denotes the valuation ring of K and a is in V then a is in V_1 since $v(a) \leq 1$. Therefore, $V \subset V_1$. Similarly, $P \subset P_1$.

Theorem 2.52. The field V_1/P_1 is isomorphic to V/P.

Proof: Let $\alpha = \lim a_n$ where $\{a_n\}$ is a sequence in V. Since $v(a_n) \leq 1$ we have that $v(a) = \lim v(a_n) \leq 1$ and α is in V_1. Therefore, V_1 is the closure of V. Similarly, P_1 is the closure of P. Define a mapping g from V/P into V_1/P_1 by the relation $g(a + P) = a + P_1$. If $a + P = b + P$ then $a - b$ is in P which is contained in P_1. Thus, $a + P_1 = b + P_1$. Since

$$(a + b) + P_1 = (a + P_1) + (b + P_1)$$

and

$$ab + P_1 = (a + P_1)(b + P_1)$$

we see that g is a homomorphism. For some N we have $v(\alpha - a_N) < 1$ which implies $\alpha - a_N$ is in P_1 and thus $\alpha + P_1 = a_N + P_1$. But then $g(a_N + P) = a_N + P_1 = \alpha + P_1$ implying g is an epimorphism. Finally, if $g(a + P) = P_1$ then $a + P_1 = P_1$ and we have $v(a) < 1$. Therefore, a is in P and $a + P = P$. With this result we have that g is an isomorphism.

Consider now the set $1 + P = \{1 + x\colon x$ is in $P\}$. This set under the operation of multiplication is a group and will be of considerable importance later when the logarithm function is considered.

Theorem 2.53. The set $1 + P$ is a group under multiplication.

Proof: For each x in P we have $v(x) < 1$ and by corollary 2.7 $v(1 + x) = 1$. If y is in P then

$$v(x + y + xy) \leq \max\{v(x), v(y), v(xy)\} < 1.$$

Hence, $(1 + x)(1 + y)$ is in $1 + P$. Now if $1 + x$ is in $1 + P$ then $v[(-x)/(1 + x)] = v(-x)/v(1 + x) = v(x) < 1$. Hence, $(1 + x)^{-1}$ is in $1 + P$ since $(1 + x)^{-1} = 1 + (-x)/(1 + x)$. Now $v(0) < 1$ and the element $1 + 0$ is the identity for $1 + P$. Therefore, $1 + P$ is a multiplicative group.

The discrete valuations defined in definition 2.50 will be of primary interest in the remaining discussion. Some theorems characterizing a complete field with a discrete valuation will now be given.

Theorem 2.54. Suppose v is a discrete valuation. There is an element π in K^* such that $v(\pi) < 1$ and $v(\pi)$ generates $v(K^*)$.

Furthermore, $v(\pi)$ is the largest of all $v(a)$ in $v(K^*)$ such that $v(a) < 1$.

Proof: Since $v(K^*)$ is an infinite cyclic group there exists an element π in K^* such that $v(\pi)$ and $v(\pi)^{-1}$ generate $v(K^*)$. Now one of $v(\pi)$ or $v(\pi)^{-1}$ is less than one. We may suppose $v(\pi) < 1$. Suppose a is in K^* and $v(a) < 1$. Then for some positive integer h, $v(a) = [v(\pi)]^h < v(\pi)$.

Actually the theorem says more than π is in K. The element π is in the ideal P of V. This element plays a distinct role in a field with a discrete valuation. It is a prime in the set V and each element α in K can be expressed in the form $\alpha = \pi^n\varepsilon$ where n is an integer and ε is a unit. If α is in the ring V this expression is similar to the expression of an integer n as a product of primes. In the ring V we have only one prime whereas in the ring of integers there are infinitely many. These properties will be verified in the discussion that follows.

Another special set associated with a non-archimedean valuation is the set of units.

Definition 2.55. For a non-archimedean valuation v the set of units for v is the set $U = V - P = \{a \in V: v(a) = 1\}$.

Theorem 2.56. The set U is a group with respect to multiplication.

Proof: This follows rather easily since $v(ab) = v(a)v(b) = 1$ and $v(a^{-1}) = v(a)^{-1} = 1$ whenever a and b are in U.

Theorem 2.57. If E is the completion of K with respect to a discrete valuation and α is in K then $\alpha = \pi^n\varepsilon$ for some integer n and ε in U.

Proof: For each α in K there is an integer n such that

$$v(\alpha) = [v(\pi)]^n = v(\pi^n).$$

Now $v(\alpha/\pi^n) = 1$ and $v(\pi^n/\alpha) = 1$. Hence, $\alpha/\pi^n = \varepsilon$ where ε is a unit in V, or equivalently, $\alpha = \pi^n\varepsilon$.

Theorem 2.58. The element π of V is a prime.

Proof: Suppose $\pi|ab$. Then $\pi d = ab$ for some d in V and

$$v(a)v(b) = v(ab) = v(d\pi) \leq v(\pi) < 1.$$

Either $v(a) < 1$ or $v(b) < 1$. Then $a = \pi^h\varepsilon_1$ or $b = \pi^j\varepsilon_2$ where h and k are non-negative integers. Hence, either π divides a or π divides b.

Corollary 2.59. For a discrete valuation v,

$$P = \pi V = \{\pi x;\ x \text{ is in } V\}.$$

Theorem 2.60. If π_1 is another prime in V then $\pi = \pi_1\varepsilon$ where ε is a unit.

Proof: By theorem 2.54, we have that $v(\pi_1) \leq v(\pi)$ which implies π_1 is in P. Therefore, $\pi|\pi_1$ and π and π_1 are associates.

In this sense the prime π is unique in V. An interesting divisibility property holds for a discrete valuation ring V.

Theorem 2.61. In a discrete valuation ring V, x divides y if and only if $v(x) \geqq v(y)$.

Proof: Suppose x and y are in V. There exist units ε_1 and ε_2 in V such that $x = \pi^h \varepsilon_1$ and $y = \pi^k \varepsilon_2$ for some non-negative integers h and k. If x divides y then there is a w in V with $w = \pi^m \varepsilon_3$ such that $y = xw$. Now $y = \pi^k \varepsilon_2 = \pi^h \varepsilon_1 \, \pi^m \varepsilon_3 = xw$. Hence, $v(y) = v(\pi)^k = v(\pi)^h v(\pi)^m \leqq v(\pi)^h = v(x)$.

Conversely, if $v(y) \leqq v(x)$ then $k \geqq h$ and

$$y = (\pi^{k-h} \varepsilon^{-1} \varepsilon_2)(\pi^h \varepsilon_1).$$

Therefore, x divides y.

With this background it is now time to investigate a very interesting field with a discrete non-archimedean valuation. For any prime p in Z, any integer $n = p^r m$ where $(p,m) = 1$. Define a valuation on Z by the following relationship:

$$(2.19) \qquad |n|_p = \begin{cases} p^{-r} & \text{if } n \neq 0 \\ 0 & \text{if } n = 0. \end{cases}$$

As in example 2.11 this gives rise to a non-archimedean valuation defined on the integral domain Z. This valuation can be extended uniquely to the quotient field Q of Z. A further extension can be made in which Q is embedded in a complete field denoted by Q_p. Now every element x in Q_p is of the form $\pi^h \varepsilon$ where π is a prime in the valuation ring V. For each integer n we have $v(n) \leqq 1$ and thus $Z \subset V$. Since p and π are both primes in V, we must have that p and π are associates and we can use p for the prime element in V. The extended valuation v_1 of $| \ |_p$ on Z to Q_p is also denoted by $| \ |_p$ and is referred to as the normalized p-adic valuation. The field Q_p is called the _field of p-adic numbers_ and the ring V is denoted by 0_p. It is called the _ring of p-adic integers_. A further characterization of this field will be given in the next chapter after the topic of series in non-archimedean valuated fields has been investigated. For a very interesting exposition of p-adic number fields the reader would be advised to read the references [2] or [15] in the bibliography.

The next theorem completely characterizes non-archimedean valuations on the set of rational numbers.

Theorem 2.62. Every nontrivial non-archimedean valuation of Q is equivalent to one of the p-adic valuations.

Proof: Suppose v is a non-trivial non-archimedean valuation on Q. Since $Z \subset V$ the set $P \cap Z$ is an ideal in Z. For ab in $P \cap Z$ the relation $v(a)v(b) = v(ab) < 1$ implies either $v(a) < 1$ or $v(b) < 1$. Hence, either a or b is in $P \cap Z$ and the ideal $P \cap Z$ is a prime ideal in Z. Now $P \cap Z \neq Z$, for $P \cap Z = Z$ would imply that $v(1) < 1$. Also, $P \cap Z \neq (0)$, for $P \cap Z = (0)$ would imply that $v(n) = 1$ for each non-zero element in Z and v would be the trivial valuation. Then $P \cap Z = (p)$ for some prime in Z. For any m in Z, $v(m) < 1$ if and only if p divides m. For a in Q, $a = p^r(m/n)$ where $(p,m) = (p,n) = (m,n) = 1$ and r is an integer. Then $v(a) = v[p^r(m/n)] = v(p)^r$. Therefore, v is a p-adic valuation which is equivalent to $| \ |_p$.

This theorem is part of a theorem due to Ostrowski which states that the only non-trivial valuations defined on the rational numbers are the ordinary absolute value and the p-adic valuations. The references [5] and [15] are recommended for this theorem.

CHAPTER III

INFINITE SERIES IN A NON-ARCHIMEDEAN VALUATED FIELD

Infinite Series

The theory of infinite series plays an essential role in real and complex analysis. In these fields a limit is defined using the ordinary absolute value function. In Chapter II we saw that the absolute value function is a valuation. Now we might ask, if we choose a different valuation, defined on a complete field, can a similar theory of infinite series be developed? In a non-archimedean complete field, a theory of infinite series can be developed. Many of the theorems about infinite series in the real number field have an analogue in a complete non-archimedean field. Further, the notion of "absolute convergence" required in some of the theorems in the real and complex numbers is not needed in a complete non-archimedean field.

In this chapter a theory of infinite series will be developed in a complete non-archimedean field. The succeeding discussion will be restricted to fields of this type.

Definition 3.1. If $\{a_n\}$ is a sequence, define a sequence of partial sums by

$$s_n = \sum_{i=0}^{n} a_i,$$

$n = 1, 2, 3, \ldots$. If the sequence $\{s_n\}$ has a limit s, the series

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

is said to converge to s. We write

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

Theorem 3.2. The series

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

converges in K if and only if $\{a_n\}$ is a null sequence in K.

Proof: Suppose

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

converges. Then the sequence $\{s_n\}$ is a Cauchy sequence. For each $\varepsilon > 0$ there is an N such that for $n \geqq N$,

$$v(a_n) = v(s_{n+1} - s_n) < \varepsilon.$$

Conversely, if $\{a_n\}$ is a null sequence then for each $\varepsilon > 0$ there is an N such that for $n \geqq N$, $v(a_n) < \varepsilon$. But for $m > n$,

$$v(s_m - s_n) = v\left[\sum_{i=n+1}^{m} a_i\right] \leq \max\{v(a_m), v(a_{m-1}), \ldots, v(a_{n+1})\} < \varepsilon.$$

Therefore, $\{s_n\}$ is a Cauchy sequence in the complete field K and must converge.

This theorem presents a contrast to the situation with respect to absolute value. It shows that the series

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

converges if $\lim a_n = 0$.

The reader may recall the well-known example of the series

$$\sum_{n=1}^{\infty} 1/n$$

which diverges in the reals while $\lim 1/n = 0$.

The concept of absolute convergence remains the same for non-archimedean valuations as it is for absolute value.

Definition 3.3. The series

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

converges absolutely if the series

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

converges in the real numbers.

Theorem 3.4. Absolute convergence implies convergence.

Proof: If the series

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

converges then $\lim a_n = 0$. But then

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

converges by theorem 3.2.

The series

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

may converge while the series

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

diverges. The next example illustrates this possibility.

Example 3.5. Define a sequence $\{a_n\}$ in Q_p by $a_n = p$ for $1 \leq n \leq p$ and $a_n = p^k$ if

$$1 + \sum_{i=1}^{k-1} p^i \leq n \leq \sum_{i=1}^{k} p^i.$$

The series

$$\sum_{n=1}^{\infty} a_n$$

formed from this sequence converges because $\lim |a_n|_p = 0$. However, we see that

$$\sum_{i=1}^{p} |a_i|_p = 1$$

and

$$\sum_{i=1}^{r} |a_i|_p = k,$$

where

$$r = \sum_{i=1}^{k} p^i.$$

Therefore, the series

$$\sum_{n=1}^{\infty} |a_n|_p$$

diverges.

Theorem 3.6. If $v(a_n) \leq b_n$ for $n \geqq N$, where N is a fixed integer and $\{b_n\}$ is a sequence of real numbers, and if

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

converges then

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

converges.

Proof: Since

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

converges, $\lim b_n = 0$ and thus $\lim v(a_n) = 0$. But then $\lim a_n = 0$ and the series

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

converges.

What is needed here is a test for the convergence or divergence of an infinite series. The next theorem gives such a test, commonly referred to as the "root test".

Theorem 3.7. For a given series

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

let $a = \overline{\lim} \sqrt[n]{v(a_n)}$. Then

(a) if $a < 1$ the series

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

converges, and

(b) if $a > 1$ the series

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

diverges.

(c) if $a = 1$ the series

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

may either converge or diverge.

Proof: Suppose $a < 1$. There is a real number b such that $a < b < 1$ and an N such that for $n \geqq N$, $\sqrt[n]{v(a_n)} < b$. This implies that $\lim v(a_n) \leqq \lim b^n = 0$. Therefore, $\{a_n\}$ is a null sequence and

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

converges. Now suppose $a > 1$. There is a subsequence $\{a_{n_i}\}$ such that $\lim \sqrt[n_i]{v(a_{n_i})} = a$. Then for infinitely many terms

$$\sqrt[n_i]{v(a_{n_i})} > 1.$$

Therefore, $\lim a_n \neq 0$, and the series

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

diverges.

Consider the series

$$\sum_{n=1}^{\infty} (p^n + 1)$$

in Q_p. For this series $a = \lim \sqrt[n]{|p^n + 1|_p} = 1$. This series is seen to diverge since $\lim |p^n + 1|_p = 1 \neq 0$.

Now let $[\log n]$ denote the greatest integer less than or equal to $\log n$. The series

$$\sum_{n=1}^{\infty} p^{[\log n]}$$

converges because $\lim \left|p^{[\log n]}\right|_p = 0$. We have $\lim \frac{[\log n]}{n} = 0$ so that

$$a = \lim \sqrt[n]{\left|p^{[\log n]}\right|_p} = \lim \left[1/\left(p^{[\log n]}\right)^{\frac{1}{n}}\right] = 1.$$

All rearrangements of terms of a convergent infinite series converge to the same limit in a non-archimedean field.

Definition 3.8. Let

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

be an infinite series. If g is any one one-to-one function of the set $\{1, 2, 3, \ldots\}$ onto $\{1, 2, 3, \ldots\}$, then the infinite series

$$\sum_{n=1}^{\infty} a_{g(n)}$$

is called a rearrangement of the series

$$\sum_{n=1}^{\infty} a_n.$$

Theorem 3.9. Let

$$\sum_{n=1}^{\infty} a_n$$

be a series converging to s and

$$\sum_{n=1}^{\infty} a_{g(n)}$$

any rearrangement of

$$\sum_{n=1}^{\infty} a_n.$$

Then the series

$$\sum_{n=1}^{\infty} a_{g(n)}$$

converges to s.

Proof: For each n let

$$s_n = \sum_{i=1}^{n} a_i$$

and

$$s'_n = \sum_{i=1}^{n} a_{g(i)}.$$

Since $\{s_n\}$ converges to s and $\{a_n\}$ is a null sequence, for each $\varepsilon > 0$ there is an N such that for $n \geqq N$, $v(s_n - s) < \varepsilon/2$ and $v(a_n) < \varepsilon/2$. Since g is one-to-one, for some $M \geqq N$ we have $\{1, 2, \ldots, N\} \subset \{g(1), \ldots, g(M)\}$. Therefore, for $n \geqq M$,

$$\begin{aligned} v(s_n' - s) &\leqq v(s_n' - s_n) + v(s_n - s) \\ &\leqq \max\{v(a_{N+1}), \ldots, v(a_n)\} + v(s_n - s) \\ &< \varepsilon/2 + \varepsilon/2 = \varepsilon. \end{aligned}$$

The following theorem for non-archimedean valuations is an immediate consequence of the corresponding result for sequences.

Theorem 3.10. Suppose

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

and

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

converges to s and t respectively. Then for any c and d in K the series

$$\sum_{n=0}^{\infty} (ca_n + db_n)$$

converges to $cs + dt$.

Proof:

$$\sum_{n=0}^{\infty} (ca_n + db_n) = \lim_{n\to\infty} \sum_{i=0}^{n} (ca_i + db_i)$$

$$= c\left(\lim_{n\to\infty} \sum_{i=0}^{n} a_i\right) + d\left(\lim_{n\to\infty} \sum_{i=0}^{n} b_i\right) = cs + dt.$$

There are several ways to define the product of two series. The purpose of this paper will be best served if the definition of a product of two series includes the multiplication of polynomials as a special case. For this reason the following definition is given.

Definition 3.11. Let

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

and

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

be two infinite series. For each n, define

$$c_n = \sum_{i=0}^{n} a_i b_{n-i}.$$

The infinite series

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

is called the "Cauchy product" of the two given series.

An immediate question is whether the series

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

converges. The answer is affirmative, if the given series converge.

Lemma 3.12. If

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

converges and $\{b_n\}$ is null sequence then the sequence

$$\left\{\sum_{i=0}^{n} a_i b_{n-i}\right\}$$

is a null sequence.

Proof: Since $\{a_n\}$ and $\{b_n\}$ are null sequences there is an M_1 and an M_2 such that $v(a_n) < M_1$ and $v(b_n) < M_2$. For each $\varepsilon > 0$ there is an N such that for $n \geqq N$, $v(a_n) < \varepsilon/2M_2$ and $v(b_n) < \varepsilon/2M_1$. Therefore, for $n \geqq 2N$,

$$v\left(\sum_{i=0}^{n} a_i b_{n-i}\right) \leqq v\left(\sum_{i=0}^{N} a_i b_{n-i}\right) + v\left(\sum_{i=N+1}^{n} a_i b_{n-i}\right)$$

$$\leqq \max_{1 \leqq i \leqq N} \{v(a_i)v(b_{n-i})\} + \max_{N+1 \leqq i \leqq n} \{v(a_i)v(b_{n-i})\}$$

$$< M_1 \max_{1 \leqq i \leqq n} \{v(b_{n-i})\} + M_2 \max_{N+1 \leqq i \leqq n} \{v(a_i)\}$$

$$< M_1 \cdot \varepsilon/2M_1 + M_2 \cdot \varepsilon/2M_2 = \varepsilon.$$

Theorem 3.13. Suppose

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

converges to s and

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

converges to t. Then

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

converges to st.

Proof: Let

$$A_n = \sum_{i=0}^{n} a_i, \quad B_n = \sum_{i=0}^{n} c_i, \quad C_n = \sum_{i=0}^{n} c_i$$

and $d_n = B_n - t$. For each n,

$$C_n = \sum_{i=0}^{n} c_i = \sum_{k=0}^{n} \sum_{i=0}^{k} a_i b_{n-i} = a_0 B_n + a_1 B_{n-1} + \dots + a_n B_0$$

$$= a_0(t + d_n) + a_1(t + d_{n-1}) + \dots + a_n(t + d_0)$$

$$= A_n t + \sum_{i=0}^{n} a_i d_{n-i}.$$

Since

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

converges and $\{d_n\}$ is a null sequence, by the previous lemma the sequence

$$\left\{\sum_{i=0}^{n} a_i d_{n-i}\right\}$$

is a null sequence. Therefore,

$$\sum_{n=0}^{\infty} c_n = \lim_{n\to\infty} C_n = \lim_{n\to\infty} A_n t + \lim_{n\to\infty} \sum_{i=0}^{n} a_i d_{n-i} = st.$$

Power Series

With this background it is now time to take up a special type of infinite series called a power series. Since this kind of series is first encountered in elementary calculus, many of the results will not be new. However, recall that we are dealing with a non-archimedean valuation. Many of the series which converge with respect to the absolute value function diverge with respect to a different valuation. Others have a somewhat different circle of convergence with respect to a non-archimedean valuation. Some of the power series of calculus will be investigated in the sequel.

Definition 3.14. For a given sequence $\{a_n\}$ in a complete non-archimedean field K the series

$$\sum_{n=0}^{\infty} a_n x^n \tag{3.1}$$

is called a power series for x in K.

In the field K two possibilities exist for the series (3.1) for a given choice of x. Either the series will converge or it will diverge. The next theorem gives a condition for convergence.

Theorem 3.15. Let

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

be a power series in a complete field K and let $a = \overline{\lim} \sqrt[n]{v(a_n)}$. If $a \neq 0$ let $r = 1/a$; if $a = +\infty$ let $r = 0$ and if $a = 0$ let $r = +\infty$. Then the series

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

(a) converges for $v(x) < r$ or for $v(x) = r$ and $\lim a_n r^n = 0$, and

(b) diverges for $v(x) > r$ or $v(x) = r$ and $\lim a_n r^n \neq 0$.

Proof: By theorem 3.7 the series

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

converges whenever $v(x)/r = \overline{\lim} \sqrt[n]{v(a_n)v(x)} = \overline{\lim} \sqrt[n]{v(a_n x^n)} < 1$ which implies convergence for $v(x) < r$. Similarly, the series diverges for $v(x) > r$. If $v(x) = r$ then the series converges for $\lim a_n r^n = 0$ and diverges for $\lim a_n r^n \neq 0$ by theorem 3.2.

In the preceeding theorem r is called the radius of convergence for the series (3.1) and the set of all x such that $v(x) < r$ is called the circle of convergence.

A very useful and familiar series is the "geometric series". This series will turn out to be the derivative of the logarithm function to be considered later.

Example 3.16. For $v(x) < 1$ the series

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

converges to $1/(1-x)$.

Now $v(x^n) = [v(x)]^n$ and $v(x) < 1$ imply that $\lim v(x^n) = 0$. Hence, $\lim x^n = 0$. Therefore,

$$(1 - x) \sum_{n=0}^{\infty} x^n = (1 - x) \lim_{n\to\infty} \sum_{i=0}^{n} x^i = \lim_{n\to\infty} (1 - x^{n+1}) = 1 - \lim_{n\to\infty} x^{n+1} = 0$$

which implies

$$\sum_{n=0}^{\infty} x^n = 1/(1 - x).$$

With example 3.16 and theorem 3.13 the negative binomial theorem can be established for non-archimedean valuations. But first a definition is needed.

Definition 3.17. For positive integers n and i define the symbol

$$\binom{n}{i} = \frac{n!}{i!(n - i)!} \quad \text{and} \quad \binom{n}{0} = 1.$$

Note that

$$\sum_{i=0}^{n} \binom{i+1}{1} = \sum_{i=0}^{n} (i+1) = \frac{(n+1)(n+2)}{2} = \binom{n+2}{2}.$$

This identity suggests the following generalization

$$(3.2) \qquad \sum_{i=0}^{n} \binom{n+i}{1} = \binom{n+i+1}{i+1}$$

which can be established by induction on n.

Example 3.18. The Binomial Theorem for negative exponents.

$$(3.3) \qquad \sum_{n=0}^{\infty} \binom{n+i-1}{i-1} x^n = \frac{1}{(1-x)^i} \quad \text{for} \quad v(x) < 1.$$

Since $\binom{n+i-1}{i-1}$ is an integer and $v(x) < 1$,

$$v\left[\binom{n+i-1}{i+1} x^n\right] = v\left[\binom{n+i-1}{i+1}\right] [v(x)]^n \to 0 \quad \text{as} \quad n \to \infty.$$

Hence, the series (3.3) converges. For $i = 1$ the series is just the geometric series of example 3.16. For $i = 2$,

$$\frac{1}{(1-x)^2} = \frac{1}{1-x} \cdot \frac{1}{1-x} = \sum_{n=0}^{\infty} x_n \cdot \sum_{n=0}^{\infty} x_n = \sum_{n=0}^{\infty} \left(\sum_{i=0}^{n} 1 \cdot 1 \right) x^n$$

$$= \sum_{n=0}^{\infty} (n+1)x^n = \sum_{n=0}^{\infty} \binom{n+1}{1} x^n.$$

Again an induction argument is needed. Suppose for $i = m$,

$$\frac{1}{(1-x)^m} = \sum_{n=0}^{\infty} \binom{n+m-1}{m-1} x^n .$$

Then for $i = m + 1$,

$$\frac{1}{(1-x)^{m+1}} = \frac{1}{(1-x)^m} \cdot \frac{1}{(1-x)} = \sum_{n=0}^{\infty} \binom{n+m-1}{m-1} x^n \cdot \sum_{n=0}^{\infty} x^n$$

$$= \sum_{n=0}^{\infty} \left[\sum_{k=0}^{n} \binom{k+m-1}{m-1} \right] x^n = \sum_{n=0}^{\infty} \binom{n+m}{m} x^n .$$

Later the Binomial series will be established which is a general form of the series (3.3). Other power series of interest to be considered here are the logarithm and exponential series. These series will be examined in the field Q_p of p-adic numbers.

Example 3.19. The Logarithm series is defined by

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

This series converges for all x such that $|x|_p < 1$. To see this, write $n = p^r m$ where $(m,p) = 1$. Then $1 \leq |1/n|_p = p^r \leq n$ and hence, $1 \leq \sqrt[n]{|1/n|_p} \leq \sqrt[n]{n}$. Therefore, $\lim \sqrt[n]{|1/n|_p} = 1$ and (3.4) converges for $|x|_p < 1$. Actually, this series converges on the maximal ideal P of the valuation ring 0_p.

So far in the p-adic numbers the geometric, negative binomial and logarithm series seem similar to their counterparts defined on the reals with respect to the absolute value function. There we have convergence for $|x| < 1$ which is similar to $|x|_p < 1$. However, when the exponential series is considered the situation is quite different.

Example 3.20. The Exponential series is defined by

$$\sum_{n=0}^{\infty} \frac{x^n}{n!} \; . \tag{3.5}$$

This series converges for all x such that $|x|_p < p^{-1/(p-1)}$. By (1.20) of Chapter I, $\operatorname{ord}_p n! = \frac{n - t_n}{p - 1}$, where

$$n = \sum_{i=0}^{r} a_i p^i, \quad t_n = \sum_{i=0}^{r} a_i$$

and $0 \leq a_i \leq p - 1$. Then

$$|1/n!|_p = p^{\left(\frac{n-t_n}{p-1}\right)}.$$

Now

$$t_n = \sum_{i=0}^{r} a_i \leq \sum_{i=0}^{r} (p - 1) = r(p - 1)$$

so that $1 \leq \sqrt[n]{p^{t_n/(p-1)}} \leq \sqrt[n]{p^r} \leq \sqrt[n]{n}$. Hence, $\lim \sqrt[n]{p^{t_n/(p-1)}} = 1$. Therefore,

$$\lim \sqrt[n]{|1/n!|_p} = \lim \sqrt[n]{p^{\left(\frac{n-t_n}{p-1}\right)}} = p^{1/(p-1)} \lim \sqrt[n]{p^{-t_n/(p-1)}} = p^{1/(p-1)}$$

so that (3.5) converges for all x such that $|x|_p < p^{-1/(p-1)}$. Now $1 < p^{1/(p-1)} < p$ so that $1/p < 1/p^{-1/(p-1)} < 1$. Therefore, if

$|x|_p \leqq 1/p$ then $|x|_p < p^{-1/(p-1)}$ and the series converges. This result seems rather strange since $\mathrm{ord}_p x$ is always an integer for x in Q_p. The answer lies in an algebraic extension of Q_p.

For any series of the form

$$\sum_{n=r}^{\infty} a_n \pi^n$$

where for each n, a_n is in V of a complete discrete field K,

$$v\left[\sum_{i=r}^{m} a_i \pi^i - \sum_{i=r}^{n} a_i \pi^i\right] = v\left[\pi^{n+1} \sum_{i=n+1}^{m} a_i \pi^{i-1}\right] \leqq v(\pi^{n+1}),$$

with $m > n$.

Since $\lim\,[v(\pi)]^{n+1} = 0$, the sequence

$$\left\{\sum_{i=r}^{n} a_i \pi^i\right\}$$

is a Cauchy sequence in K. Hence, there is an α in K such that

$$\alpha = \sum_{n=r}^{\infty} a_n \pi^n .$$

An interesting fact about a field of this kind is that each α in K can be represented in this form.

Theorem 3.21. Let K be a complete discrete field with a valuation v. Let S be a complete residue system for the associated residue field V/P. Then each α in K can be written uniquely in the form

(3.6) $$\alpha = \sum_{n=r}^{\infty} a_n \pi^n$$

where $v(\alpha) = [v(\pi)]^r$, r is an integer, a_n is in S for each n, and a_r is not in P.

Proof: If $\alpha = 0$ then

$$\alpha = \sum_{n=0}^{\infty} 0 \cdot \pi^n.$$

Suppose α is in K and $\alpha \neq 0$. Then $\alpha = \pi^r \varepsilon$ for some r and some unit ε in V. There is an a_r in S such that a_r is not in P and $\alpha/\pi^r + P = a_r + P$. Hence, $\alpha/\pi^r - a_r$ is in P and $v[\alpha/\pi^r - a_r] < 1$. Thus, $v[\alpha - a_r\pi^r] < v(\pi^r)$ and $\alpha - a_r\pi^r = c_1$ where $v(c_1) \leq v(\pi^{r+1})$. Now $v[c_1/(\pi^{r+1})] \leq 1$ so there is an element a_{r+1} in S such that $v[c_1/(\pi^{r+1}) - a_{r+1}] < 1$, or

$$v[c_1 - a_{r+1}\pi^{r+1}] \leq v(\pi^{r+1}).$$

There is a c_2 such that $c_1 - a_{r+1}\pi^{r+1} = c_2$. We now have

$$\alpha = a_r\pi^r + a_{r+1}\pi^{r+1} + c_2.$$

Repeating this process h times gives

$$\alpha = a_r\pi^r + \ldots + a_{r+h}\pi^{r+h} + c_{h+1}$$

where $v[c_{h+1}] \leq v(\pi^{r+h+1})$. Since $v(c_{h+1}) < v(\pi^{r+h+1})$, $\lim c_{h+1} = 0$

and we must have

$$\alpha = \sum_{n=r}^{\infty} a_n \pi^n .$$

Now suppose

$$\alpha = \sum_{n=r}^{\infty} b_n \pi^n$$

where each b_n is in S and b_r is not in P. If $a_i \neq b_i$ for some i, let m be the smallest integer such that $a_m \neq b_m$. Then

$$0 = \sum_{n=m}^{\infty} (a_n - b_n)\pi^n = \pi^m \sum_{n=m}^{\infty} (a_n - b_n)\pi^{n-m}$$

which implies that

$$(b_m - a_m) = \pi \sum_{n=m+1}^{\infty} (a_n - b_n)\pi^{n-m-1}$$

Thus, $v(b_m - a_m) < 1$ and $b_m + P = a_m + P$. But this implies a_m and b_m are in the same residue class and by the choice of S, $a_m = b_m$. Of course, a different choice for S would result in different a_n's in the series expansion.

According to theorem 3.21 each element α of the field Q_p can be written as

$$\alpha = \sum_{n=r}^{\infty} a_n p^n .$$

One choice for a complete residue system is the set

$$S = \{0, 1, 2, \ldots, p-1\}.$$

When this set is used the resulting series expansion is called the canonical representation for α in Q_p. If r is a non-negative integer, then

$$\sum_{n=r}^{\infty} a_n p^n = \lim \sum_{i=r}^{n} a_i p^i$$

where

$$\left\{ \sum_{i=r}^{n} a_i p^i \right\}$$

is a sequence of integers. Let

$$x_n = \sum_{i=r}^{n} a_i p^i.$$

The sequence $\{x_n\}$ has the following property:

(3.7) $$x_{n-1} \equiv x_n \bmod p^n$$

On the set of all sequences of integers satisfying (3.7) define a relation by

(3.8) $\{x_n\} \sim \{y_n\}$ if and only if $x_n \equiv y_n (\text{mod } p^{n+1})$ for each n.

This relation defines an equivalence relation on the set of all sequences of integers that satisfy (3.7). With the resulting set of equivalent classes the set of p-adic integers can be constructed. The field Q_p is constructed as a quotient field of 0_p.

For a development along these lines refer to [2] or [15] in the bibliography.

Some of the essential theorems of Q_p will be stated here, where all series representations are canonical.

(3.9) Every positive integer has finite series representation.

(3.10) For α in 0_p, $\alpha = \sum_{n=0}^{\infty} a_n p^n$.

(3.11) An integer b is a unit if and only if $(b,p) = 1$.

(3.12) A rational number r/s is a unit if and only if

$$(r,p) = (s,p) = (r,s) = 1.$$

(3.13) $$-p^r = p^r \sum_{n=0}^{\infty} (p-1)p^n.$$

(3.14) An element α in Q_p is rational if and only if its canonical expansion, $\sum_{n=r}^{\infty} a_n p^n$, where $|\alpha|_p = |p|_p^r$, is periodic.

For proofs of these theorems see [2] or [15] of the bibliography. The arithmetic in a field Q_p is interesting and a few examples will be considered here. In the field Q_3 the series expansion of -264 can be found by expressing -264 as $465 - 3^6$. Now the series expansion of 465 is

$$465 = 0 + 2 \cdot 3 + 0 \cdot 3^2 + 2 \cdot 3^3 + 2 \cdot 3^4 + 1 \cdot 3^5$$

and using (3.13) the series expansion for -3^6 is

$$-3^6 = 3^6 \sum_{n=0}^{\infty} 2\cdot 3^n.$$

Therefore, the series expansion for -264 is given by

$$-264 = 0 + 2\cdot 3 + 0\cdot 3^2 + 2\cdot 3^3 + 2\cdot 3^4 + 1\cdot 3^5 + 3^6 \sum_{n=0}^{\infty} 2\cdot 3^n.$$

Using (3.14) it is easy to show that the set of rationals Q is not complete in Q_p. The partial sums of the series

$$\sum_{n=1}^{\infty} p^{\left(\frac{n(n-1)}{2}\right)}$$

form a Cauchy sequence, but the series is not periodic and cannot represent a rational number in Q_p.

The next example is useful and uses some of the previous theory.

Example 3.22. The polynomial $x^{p-1} - 1$ has $p-1$ distinct roots in Q_p.

To establish this fact consider the series

$$(3.15) \qquad a + \sum_{n=1}^{\infty} \left(a^{p^n} - a^{p^{n-1}}\right) = \lim a^{p^n},$$

where a is in the set $\{1, 2, \ldots, p-1\}$. Now

$$a^{p^n} - a^{p^{n-1}} = a^{p^{n-1}}\left[a^{(p^{n-1})(p-1)} - 1\right]$$

and since $a^{(p^{n-1})(p-1)} \equiv 1(\mathrm{mod}\ p^n)$ by Euler's theorem, we have

$$\left| a^{p^n} - a^{p^{n-1}} \right|_p \leq |p|_p^n.$$

Therefore, $\lim \left(a^{p^n} - a^{p^{n-1}}\right) = 0$ and (3.15) converges. Let $\alpha = \lim a^{p^n}$, then

$$\alpha^{p-1} = \lim a^{p^n(p-1)} = \lim (1 + c_n p^n) = 1 + \lim c_n p^n = 1.$$

There are p-1 choices for a, and hence p-1 choices for α. If we have

$$\alpha = a + \sum_{n=1}^{\infty} \left(a^{p^n} - a^{p^{n-1}}\right) = b + \sum_{n=1}^{\infty} \left(b^{p^n} - b^{p^{n-1}}\right)$$

where a and b both belong to $\{1, 2, \ldots, p-1\}$ then

$$a - b = \sum_{n=1}^{\infty} \left(b^{p^n} - b^{p^{n-1}}\right) - \sum_{n=1}^{\infty} \left(a^{p^n} - a^{p^{n-1}}\right).$$

Therefore, $a \equiv b (\text{mod } p)$ and hence, $a = b$.

Infinite Products

A theory of infinite products can be developed for a non-archimedean valuated field in much the same manner as it is developed on the real or complex numbers with respect to the absolute value. Many of the same proofs can be established and these can be simplified somewhat for a non-archimedean valuation.

Definition 3.23. For a sequence $\{b_n\}$ in a non-archimedean field define a sequence of partial products $\{p_n\}$ by

$$p_n = \prod_{i=0}^{n} b_i$$

where $b_i \neq 0$ for each i. If $\lim p_n$ exists and $\lim p_n = \alpha \neq 0$ then we set

$$\alpha = \prod_{n=0}^{\infty} b_n = \lim p_n.$$

If $\lim p_n = 0$ then $\{p_n\}$ is said to diverge to 0. We call

$$\prod_{n=0}^{\infty} b_n$$

an infinite product.

Again, as in the case for infinite sums, the ensuing discussion will consider infinite products in a complete non-archimedean valuated field K. Similar to the case for infinite series, a Cauchy criterion for infinite products can be established.

Theorem 3.24. The infinite product

$$\prod_{n=0}^{\infty} b_n$$

converges if and only if for each $\varepsilon > 0$ there exists an N such that $n \geqq N$ implies that

(3.16) $$v(b_n - 1) < \varepsilon.$$

Proof: Suppose $\{p_n\}$ converges to $\alpha \neq 0$. There exist an M such that $v(p_n) > M$, since $p_n \neq 0$ for each n. For each $\varepsilon > 0$ there is an N such that $n \geqq N$ implies that $v(p_n - p_{n-1}) < \varepsilon \cdot M$. But then $v(b_n - 1) < \varepsilon M/v(p_{n-1}) < \varepsilon$.

Now suppose for $\varepsilon = 1/2$ there is an N_1 such that for $n \geqq N_1$, $v(b_n - 1) < 1/2$. We must have $v(b_n) \geqq 1$ for otherwise $v(b_n) < 1$ implies that $v(b_n - 1) = \max\{v(b_n),1\} = 1 > 1/2$. Similarly, $v(b_n) > 1$ implies that $v(b_n - 1) = \max\{v(b_n),1\} = v(b_n) > 1/2$. Thus, $v(b_n) = 1$ for $n \geqq N_1$. Let $v(p_{N_1}) = M$. Then for $n \geqq N_1$,

$$v(p_n) = v(p_{N_1})v\left(\prod_{i=N_1+1}^{n} b_i\right) = v(p_{N_1}) = M. \tag{3.17}$$

For each $\varepsilon > 0$ there is an N_2 such that for $n \geqq N_2$,

$$v(b_n - 1) < \varepsilon/M. \tag{3.18}$$

If $N > \max\{N_1,N_2\}$ then both (3.17) and (3.18) are satisfied and

$$v(p_n - p_{n-1}) = v(p_{n-1})v(b_n - 1) = Mv(b_n - 1) < \varepsilon.$$

Therefore, $\{p_n\}$ is a Cauchy sequence and must converge in K.

To enlarge the class of infinite products it is desirable to allow zero factors as given in the next definition.

Definition 3.25. (a) Given an infinite product

$$\prod_{n=0}^{\infty} b_n$$

with finitely many zero factors, let N be a positive integer such that all factors $b_{N+1}, b_{N+2}, \ldots$ are non-zero and let m be any integer greater than N. Then

$$\lim \prod_{i=N+1}^{m} b_i$$

exists and

$$\lim \prod_{i=0}^{m} b_i$$

is defined to be

$$\prod_{i=0}^{N} b_i \cdot \lim \prod_{i=N+1}^{m} b_i .$$

(b) Given an infinite product

$$\prod_{n=0}^{\infty} b_n$$

with infinitely many zero factors the product is said to diverge to zero.

For infinite sums we had convergence of the series

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

if and only if $\lim a_n = 0$. A similar result holds for infinite products which makes tests for convergence in a non-archimedean field somewhat easier than in the real case with the absolute value. If the infinite product

$$\prod_{n=0}^{\infty} b_n = b \neq 0$$

we have

$$\lim b_n = \lim \left(\prod_{i=1}^{n} b_i\right) \Big/ \left(\prod_{i=1}^{n-1} b_i\right) = b/b = 1.$$

If we set $b_n = 1 + a_n$ then $\lim a_n = \lim (b_n - 1) = 0$. Hence, if the infinite product

$$\prod_{n=0}^{\infty} (1 + a_n) = b \neq 0,$$

then $\lim a_n = 0$.

Theorem 3.26. The product

$$\prod_{n=0}^{\infty} (1 + a_n)$$

converges if and only if $\lim a_n = 0$.

Proof: The preceeding discussion verifies that convergence of

$$\prod_{n=0}^{\infty} (1 + a_n) \tag{3.19}$$

implies $\lim a_n = 0$. Conversely, suppose that for $\varepsilon > 0$ there is an n such that for $n \geqq N$, $v(a_n) < \varepsilon$. Then $v(b_n - 1) = v[(1 + a_n) - 1]$. Therefore, by theorem 3.24, (3.19) converges.

Corollary 3.27. The infinite product

$$\prod_{n=0}^{\infty} (1 + a_n)$$

converges if and only if

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

converges.

Proof: The product

$$\prod_{n=0}^{\infty} (1 + a_n)$$

converges if and only if $\lim a_n = 0$, that is, if and only if

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

converges.

In the case of the reals $\lim a_n = 0$ does not imply convergence of

$$\prod_{n=0}^{\infty} (1 + a_n).$$

For example,

$$\prod_{n=1}^{\infty} (1 + 1/n)$$

is divergent since $p_n = n + 1$, while $\lim 1/n = 0$.

A definition of absolute convergence may be given for infinite products as was given for infinite series.

Definition 3.28. The infinite product

$$\prod_{n=0}^{\infty} (1 + a_n)$$

is said to converge absolutely if

$$\prod_{n=0}^{\infty} [1 + v(a_n)]$$

converges.

Theorem 3.29. Absolute convergence of

$$\prod_{n=0}^{\infty} (1 + a_n)$$

implies convergence.

Proof: If

$$\prod_{n=0}^{\infty} [1 + v(a_n)]$$

converges then $\lim v(a_n) = 0$ in the reals. But then $\lim a_n = 0$ and hence,

$$\prod_{n=0}^{\infty} (1 + a_n)$$

converges.

The following examples are given to help illustrate the principles involved.

Example 3.30. Let a be an element in a non-archimedean valued field such that $v(a) < 1$. Then the infinite product

$$\prod_{n=0}^{\infty}\left(1 + a^{2^n}\right) = 1/(1-a).$$

Since $\lim a^{2^n} = 0$ the given product converges. By induction it can be established that

$$\prod_{i=0}^{n}\left(1 + a^{2^i}\right) = \sum_{i=0}^{2^{n+1}-1} a^i.$$

Hence, by example 3.16

$$\prod_{n=0}^{\infty}\left(1 + a^{2^n}\right) = \lim \prod_{i=0}^{n}\left(1 + a^{2^i}\right) = \lim \sum_{i=0}^{2^{n+1}-1} a^i = \sum_{n=0}^{\infty} a^n = 1/(1-a).$$

Note that

$$(1 + a) \prod_{n=1}^{\infty}\left(1 + a^{2^n}\right) = 1/(1-a)$$

or

$$\prod_{n=1}^{\infty}\left(1 + a^{2^n}\right) = 1/(1-a^2).$$

If

$$\prod_{n=k}^{\infty}\left(1 + a^{2^n}\right) = 1/\left(1-a^{2^k}\right)$$

then using the same procedure,

$$\left(1 + a^{2^k}\right) \prod_{n=k+1}^{\infty} \left(1 + a^{2^n}\right) = 1/\left(1-a^{2^k}\right)$$

or

$$\prod_{n=k+1}^{\infty} \left(1 + a^{2^n}\right) = 1/\left(1-a^{2^{k+1}}\right).$$

By induction

$$\prod_{n=m}^{\infty} \left(1 + a^{2^n}\right) = 1/\left(1-a^{2^m}\right).$$

<u>Example 3.31</u>. Each α in Q_p can be expressed in the form

$$a_0 p^r \prod_{n=1}^{\infty} (1 + c_n p^n),$$

where c_n is in the valuation ring V. By theorem 3.21

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

where $0 \leq a_n \leq p-1$. For $n \geq 2$, each partial sum s_{n-1} of

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

has the property that $|s_{n-1}|_p = |a_0|_p = 1$ by corollary 2.7. Then $|a_n/s_{n-1}|_p \leq 1$ and $|(a_n/s_{n-1})p^n|_p \leq p^{-n}$. Hence, $\lim (a_n/s_{n-1})p^n = 0$ and the product

$$a_0 p^r \prod_{n=1}^{\infty} [1 + (a_n/s_{n-1})p^n]$$

converges. By induction

$$a_0 p^r \prod_{i=1}^{n} [1 + (a_i/s_{i-1})p^i] = p^r \sum_{i=0}^{n} a_i p^i$$

and we have

$$a_0 p^r \prod_{n=1}^{\infty} [1 + (a_n/s_{n-1})p^n] = \lim a_0 p^r \prod_{i=1}^{n} [1 + (a_i/s_{i-1})p^i]$$

$$= \lim p^r \sum_{i=1}^{n} a_i p^i = p^r \sum_{n=0}^{\infty} a_n p^n = \alpha.$$

Since the a_n's are unique, we also have that the c_n's are unique where $c_n = a_n/s_{n-1}$ for each n.

CHAPTER IV

SEQUENCES AND SERIES OF FUNCTIONS

When we consider analysis in the field of real or complex numbers the concept of limit is defined in terms of the absolute value function. Theorems involving this concept depend on the fact that the value group for the absolute value function is an ordered subset of the non-negative real numbers. For example, in case of complex analysis the theorems depend on the ordering of the value group. The theorems involving infinite series in the preceeding chapter did not require that the series be defined on an ordered field.

In the case of a complete field with respect to a non-archimedean valuation v the value group is an ordered subset of the non-negative real numbers. A natural undertaking would be to consider the concepts of analysis in a non-archimedean complete field. One would suspect that many of these concepts would be immediately applicable, but would possibly take different forms in some cases.

Definition 4.1. Let $\{f_n\}$ be a sequence of functions defined on a set S. If the sequence of numbers $\{f_n(x)\}$ converges for each x in S, we define a function f by

$$f(x) = \lim f_n(x). \tag{4.1}$$

The sequence $\{f_n\}$ is said to converge on S and f is called the limit function of $\{f_n\}$.

For a sequence of functions $\{f_n\}$ and an x in S let

$$s_n(x) = \sum_{i=0}^{n} f_i(x).$$

Definition 4.2. If $\{s_n(x)\}$ converges for every x in S we define a function f by

$$f(x) = \sum_{n=0}^{\infty} f_n(x). \tag{4.2}$$

The function f is called the sum of the series

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

The concept of continuity in a complete non-archimedean valuated field K is defined in the usual way.

Definition 4.3. Let S be a subset of K and suppose f is a function from S into K. If a is in S, f is continuous at a if and only if for each $\varepsilon > 0$ there is a $\delta > 0$ such that for $v(x - a) < \delta$ and x in S, we have $v(f(x) - f(a)) < \varepsilon$. The function f is said to be continuous on S if f is continuous at each a in S. We write $\lim\limits_{x\to a} f(x) = f(a)$.

With the aid of this definition the following theorems can be proven in the same manner as they are proven in elementary calculus on the field of real numbers with respect to the absolute value function.

Theorem 4.4. Suppose f and g are continuous at a in S. Then

(a) $f + g$ is continuous at a;

(b) fg is continuous at a; and

(c) if $g(a) \neq 0$, then f/g is continuous at a.

Theorem 4.5. Suppose f is a function defined on S and g is a function defined on S' where $f(S) \subset S'$. If f is continuous at a and g is continuous at $f(a)$, then $f \circ g$ is continuous at a.

Theorem 4.6. Suppose f is a function defined on S. Then f is continuous at a if and only if for each sequence $\{x_n\}$ in S converging to a, the sequence $\{f(x_n)\}$ converges to $f(a)$.

A problem which arises is whether a function defined by (4.2) is continuous when each function in the sequence is continuous. Stated in another way the problem is whether

$$(4.3) \qquad \lim_{x\to a}\lim_{n\to\infty}\sum_{i=0}^{n} f_i(x) = \lim_{n\to\infty}\lim_{x\to a}\sum_{i=0}^{n} f_i(x).$$

This may not be the case as seen in the next example.

Example 4.7. For each n let $f_n(x) = \{x/(1 + x)\}^n$ where $K = Q_p$ and $|x|_p < 1$. Then $|x/(1 + x)|_p < 1$ so that

$$f(x) = \sum_{n=0}^{\infty} \{x/(1 + x)\}^n = 1 + x$$

for $x \neq 0$ and $f(0) = 0$. Now

$$\lim_{x\to 0}\lim_{n\to\infty}\sum_{i=0}^{n} f_i(x) = \lim_{x\to 0}(1 + x) = 1$$

and

$$\lim_{n\to\infty}\lim_{x\to 0}\sum_{i=0}^{n} f_i(x) = 0$$

so that (4.3) is not valid.

This example shows that one cannot be careless about interchanging the limit process. For (4.3) to be valid a stronger definition is needed than 4.1. The convergence in definition 4.1 is referred to as "pointwise convergence."

Definition 4.8. A sequence of functions $\{f_n\}$ is said to converge uniformly on S to a function f if for every $\varepsilon > 0$ there is an integer N such that $n \geqq N$ implies that

$$v(f_n(x) - f(x)) < \varepsilon \quad \text{for all } x \text{ in } S. \tag{4.4}$$

This definition implies pointwise convergence. The series

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

converges uniformly on S if the sequence

$$\left\{\sum_{i=0}^{n} f_i(x)\right\}$$

converges uniformly on S.

Theorem 4.9. The sequence of functions $\{f_n\}$ defined on S converges uniformly on S if and only if for every $\varepsilon > 0$ there is an N such that for $n \geqq N$

$$v(f_{n+1}(x) - f_n(x)) < \varepsilon \text{ for each } x \text{ in } S. \tag{4.5}$$

Proof: Suppose $\{f_n\}$ converges uniformly on S to f. There is an N such that $n \geqq N$ implies that $v(f_n(x) - f(x)) < \varepsilon/2$ for all x in S. Therefore,

$$v(f_{n+1}(x) - f_n(x)) \leqq v(f_{n+1}(x) - f(x)) + v(f(x) - f_n(x)) < \varepsilon.$$

Conversely, suppose (4.5) is valid. For a given x in S, $\{f_n(x)\}$ is a Cauchy sequence and converges in K. Let

$$f(x) = \lim f_n(x).$$

Choose $\varepsilon > 0$. There is an N such that for $n \geqq N$,

$$v(f_n(x) - f_{n+1}(x)) < \varepsilon/2$$

for each x in S. Now for each k,

$$v(f_n(x) - f_{n+k}(x)) \leqq \max\{v(f_n(x) - f_{n+1}(x)), \ldots, v(f_{n+k-1}(x) - f_{n+k}(x))\}$$
$$< \varepsilon/2.$$

Therefore, $v(f_n(x) - f(x)) = \lim\limits_{k\to\infty} v(f_n(x) - f_{n+k}(x)) \leqq \varepsilon/2 < \varepsilon$ for each $n \geqq N$ and every x in S.

For a sequence of functions $\{f_n\}$ defined on S let

$$s_n(x) = \sum_{i=0}^{n} f_i(x),$$

for each n. Suppose

$$f(x) = \lim s_n(x) = \sum_{n=0}^{\infty} f_n(x).$$

For a series defined in this manner theorem 4.9 takes the following form.

Theorem 4.10. The series

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

converges uniformly on S if and only if for every $\varepsilon > 0$ there is an N such that $n \geqq N$ implies $v(f_n(x)) < \varepsilon$ for every x in S.

The Weierstrass M-test takes the following simple form in a non-archimedean field.

Theorem 4.11. Let $\{M_n\}$ be a sequence of non-negative numbers such that $v(f_n(x)) \leqq M_n$ for each n and for each x in S. If $\lim M_n = 0$, then

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

converges uniformly.

Proof: Choose $\varepsilon > 0$. There is an N such that $n \geqq N$ implies $v(f_n(x)) \leqq M_n < \varepsilon$ for each x in S. But then $\{f_n(x)\}$ is a null sequence. Hence,

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

converges. Since N does not depend on x this convergence is uniform.

Theorem 4.12. Suppose $\{f_n\}$ converges uniformly to f on S. If a is an accumulation point of S and if each f_n is continuous at a then f is continuous at a.

Proof: For $\varepsilon > 0$ there is an N such that $n \geqq N$ implies $v(f_n(x) - f(x)) < \varepsilon/3$ for each x in S. Since $f_N(x)$ is continuous at a there is a δ such that $v(x - a) < \delta$ implies

$$v(f_N(x) - f_N(a)) < \varepsilon/3.$$

Therefore,

$$\begin{aligned} v(f(x) - f(a)) &\leqq v(f(x) - f_N(x)) + v(f_N(x) - f_N(a)) + v(f_N(a) - f(a)) \\ &< \varepsilon. \end{aligned}$$

Corollary 4.13. Suppose

$$\left\{\sum_{i=0}^{n} f_i(x)\right\}$$

converges uniformly to $f(x)$. If each f_i is continuous at a in S then f is continuous at a.

Note that this corollary allows us to write

$$(4.6) \qquad \lim_{x\to a} \sum_{n=0}^{\infty} f_n(x) = \sum_{n=0}^{\infty} \lim_{x\to a} f_n(x).$$

Corollary 4.14. If $\{f_n\}$ is a sequence of continuous functions on S and if $\{f_n\}$ converges uniformly on S then f is continuous on S.

For the remainder of this chapter we shall be interested in those functions represented by a power series of the form

$$(4.7) \qquad f(x) = \sum_{n=0}^{\infty} a_n x^n = \lim \sum_{i=0}^{n} a_i x^i.$$

Here we have a sequence of functions $\{a_n x^n\}$, where each function is continuous. The partial sums are defined by

$$s_n(x) = \sum_{i=0}^{n} a_i x^i$$

and are also continuous. Functions defined by (4.7) are called analytic functions.

Theorem 4.15. Suppose the function f is defined by (4.7) and the series converges for $v(x) < r$. Then the convergence is uniform for $v(x) \leq t < r$. The function is continuous for each x such that $v(x) < r$.

Proof: Now the series

$$\sum_{n=0}^{\infty} v(a_n)t^n$$

converges in the real numbers for $t < r$. Since $v(a_n x^n) \leq v(a_n)t^n$ and $\lim v(a_n)t^n = 0$, theorem 4.11 applies. Therefore, f converges uniformly for $v(x) \leq t < r$. By theorem 4.12 f is continuous.

Suppose f is an analytic function which converges for $v(x) < r$. If $v(a) < r$ then $v(x - a) \leq \max\{v(x),v(a)\} < r$ so that

$$f(x) = \sum_{n=0}^{\infty} a_n(x - a)^n \tag{4.8}$$

converges for $v(x - a) < r$. As a matter of convenience the discussion that follows will be concerned with functions of the form (4.7) rather than (4.8).

Definition 4.16. The derivative of

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

is defined to be

$$f'(x) = \sum_{n=1}^{\infty} na_n x^{n-1}.$$

The nth derivative will be denoted by $f^n(x)$.

Note that this definition says to take the derivative of power series we differentiate each term $a_n x^n$.

Theorem 4.17. If

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

for $v(x) < r$ then f' exists and has the same domain of convergence as f.

Proof: Since $n = p^r m$ where $(p,m) = 1$, we have $1/n \leq 1/p^r \leq 1$. Now $v(n) = 1/p^r$ so that $1/n \leq v(n) \leq 1$. This implies that $\lim \sqrt[n]{v(n)} = 1$. Therefore, $\overline{\lim} \sqrt[n]{v(na_n)} = \overline{\lim} \sqrt[n]{v(a_n)}$, and we have that f and f' have the same domain of convergence.

Corollary 4.18. With the same hypothesis as theorem 4.17 f has derivatives of all orders which are given by

$$(4.9) \qquad f^k(x) = \sum_{n=k}^{\infty} n(n-1) \ldots (n-k+1)\, a_n x^{n-k}$$

$$= \sum_{n=0}^{\infty} (n+k)(n+k-1) \ldots (n+1)\, a_{n+k} x^n.$$

We also have

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

This representation is unique in the domain of convergence of f.

Proof: Suppose (4.9) is valid for $k = m$. Then for $k = m + 1$

$$\begin{aligned} f^{m+1}(x) &= [f^m(x)]' \\ &= \sum_{n=m+1}^{\infty} (n + m) \ldots (n + 1)\, na_{n+m}x^{n-1} \\ &= \sum_{n=0}^{\infty} (n + m + 1) \ldots (n + 1)\, a_{n+m+1}x^n. \end{aligned}$$

The corollary follows by induction. We have $f^k(0) = k!a_k$ so that $a_k = f^k(0)/k!$. Let

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

If $f(x) = g(x)$ in the domain of convergence of f then

$$a_n = \frac{f^n(0)}{n!} = \frac{g^n(0)}{n!} = b_n.$$

Theorem 4.19. If f and g are functions which converge for $v(x) < r$ and $f'(x) = g'(x)$ then $f(x) = g(x) + c$.

Proof: Let

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

Then $h'(x) = f'(x) - g'(x) = 0$. Hence, $a_n - b_n = 0$ for $n \geqq 1$ and $h(x) = a_0 - b_0$. Therefore, $f(x) = g(x) + (a_0 - b_0)$.

Theorem 4.20. If

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

for each x such that $v(x) < r$ then $f'(x) = \lim_{y\to 0} \frac{f(x + y) - f(x)}{y}$.

Proof: We have that

$$(4.10) \quad \frac{f(x + y) - f(x)}{y} = (1/y) \left[\sum_{n=0}^{\infty} a_n(x + y)^n - \sum_{n=0}^{\infty} a_n x^n\right]$$

$$= (1/y) \left[\sum_{n=0}^{\infty} a_n \sum_{i=1}^{n} \binom{n}{i} x^{n-i}y^i\right]$$

$$= \sum_{n=0}^{\infty} a_n \sum_{i=1}^{n} \binom{n}{i} x^{n-i}y^{i-1}.$$

Choose x such that $v(x) < r$. For all y such that $v(x) > v(y) \neq 0$, $v(a_n \binom{n}{i} x^{n-i}y^{i-1}) \leq v(a_n)v(x)^{n-1}$. By theorem 4.11, (4.10) converges uniformly in y. Therefore

$$\lim_{y\to 0} \frac{f(x + y) - f(x)}{y} = \lim_{y\to 0} \sum_{n=0}^{\infty} a_n \sum_{i=1}^{n} \binom{n}{i} x^{n-i}y^{i-1}$$

$$= \sum_{n=0}^{\infty} a_n \lim_{y\to 0} \sum_{i=1}^{n} \binom{n}{i} x^{n-i}y^{i-1}$$

$$= \sum_{n=0}^{\infty} na_n x^{n-1} = f'(x).$$

Once the relationship $f'(x) = \lim \frac{f(x+y) - f(x)}{y}$ has been established for analytic functions the usual theorems about derivatives can be proved in an analogous manner as those in elementary calculus. For the sake of completeness and brevity, these will be stated without proof.

Theorem 4.21. Suppose f and g are differentiable functions defined on S and differentiable at x. Then,

(a) $f + g$ is differentiable at x and

$$(f+g)'(x) = f'(x) + g'(x);$$

(b) fg is differentiable at x and

$$(fg)'(x) = f(x)g'(x) + f'(x)g(x);$$

(c) if $g(x) \neq 0$ then (f/g) is differentiable at $f(x)$ and

$$(f/g)'(x) = \frac{f'(x)g(x) - f(x)g'(x)}{g(x)^2}.$$

Theorem 4.22. Suppose f is defined on S and g is defined on $f(S)$. If f is differentiable at x and g is differentiable at $f(x)$, then $g \circ f$ is differentiable at x and

$$(g \circ f)'(x) = g'(f(x))f'(x).$$

Example 4.23. Let $K = Q_p$. Suppose

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

where $|x|_p < 1$. With the aid of example 3.16, the derivative is given by

$$f'(x) = \sum_{n=1}^{\infty} (-x)^{n-1} = 1/(1 + x).$$

Example 4.24. In the field Q_p let

$$g(x) = \sum_{n=0}^{\infty} \frac{(-1)^{n-1}x^n}{n}$$

and $f(x) = tx$, where t is in 0_p and $|x|_p < 1$. Let $h(x) = g(f(x))$. By example 4.23 and theorem 4.22, $h'(x) = [1/(1 + tx)]\cdot t = t/(1 + tx)$.

Before proceeding to the next theorem, the following observation concerning polynomials is needed.

Let

$$f(x) = \sum_{i=0}^{n} a_i x^i$$

where $a_n = 1$ and the coefficients are in the valuation ring V of a non-archimedean field K. We have that

$$\begin{aligned}(4.11)\qquad f(x + h) &= \sum_{i=0}^{n} a_i(x + h)^i = \sum_{i=0}^{n} a_i \sum_{j=0}^{i} \binom{i}{j} x^{i-j}h^j \\ &= a_0 + (a_1x + a_1h) + (a_2x^2 + 2a_2xh + a_2h^2) \\ &\quad + (a_3x^3 + 3a_3x^2h + 3a_3xh^2 + a_3h^3) + \dots \\ &\quad + (x^n + nx^{n-1}h + \dots + h^n) \\ &= f(x) + hf'(x) + h^2g(x,h).\end{aligned}$$

The function $g(x,h)$ has its coefficients in V when h is in V.

Newton's method gives a way to approximate roots of polynomials in the real numbers. This method of approximating roots has a counterpart in a non-archimedean field which is given in theorem 4.25.

Theorem 4.25. (Newton's Method) Suppose $f(x)$ is a polynomial in a complete field K with respect to a non-archimedean valuation v. Further, suppose $f(x)$ has coefficients in V and a leading coefficient of 1. If there is an α_1 in K such that $v[f(\alpha_1)] < 1$ and $v[f'(\alpha_1)] = 1$, then the sequence $\{\alpha_n\}$, where

$$\alpha_n = \alpha_{n-1} - \frac{f(\alpha_{n-1})}{f'(\alpha_{n-1})} ,$$

converges to a root α in V of $f(x)$.

Proof: Let

$$f(x) = \sum_{i=0}^{n} a_i x_i .$$

We note first that α_1, if it exists cannot have $v(\alpha_1) > 1$. Because a_i belongs to V, $v(a_i\alpha_1^i) \leq v(\alpha_1^i)$ for all $i < n$. If $v(\alpha_1) > 1$, $v(\alpha_1^i) < v(\alpha_1^n)$ for all $i < n$. But then $v(f(\alpha_1)) = v(\alpha_1^n) > 1$, which is a contradiction. Hence, $v(\alpha_1) \leq 1$ and α_1 is in V.

By 4.11,

$$f(\alpha_2) = f\left(\alpha_1 - \frac{f(\alpha_1)}{f'(\alpha_1)}\right) = f(\alpha_1) - \frac{f(\alpha_1)}{f'(\alpha_1)}\cdot f'(\alpha_1) + \left(\frac{f(\alpha_1)}{f'(\alpha_1)}\right)^2 g\left(\alpha_1, \frac{f(\alpha_1)}{f'(\alpha_1)}\right)$$

$$= \left(\frac{f(\alpha_1)}{f'(\alpha_1)}\right)^2 g\left(\alpha_1, \frac{f(\alpha_1)}{f'(\alpha_1)}\right).$$

Since the coefficients of

$$g\left(\alpha_1, \frac{f(\alpha_1)}{f'(\alpha_1)}\right)$$

are in V,

$$v\left[g\left(\alpha_1, \frac{f(\alpha_1)}{f'(\alpha_1)}\right)\right] \leqslant 1.$$

It follows that

$$v[f(\alpha_2)] \leqslant v\left[\frac{f(\alpha_1)}{f'(\alpha_1)}\right]^2 = v[f(\alpha_1)]^2 < 1.$$

Using 4.11 again we have

$$f'(\alpha_2) = f'\left(\alpha_1 - \frac{f(\alpha_1)}{f'(\alpha_1)}\right) = f'(\alpha_1) - \frac{f(\alpha_1)}{f'(\alpha_1)}\, g_1\left(\alpha_1, \frac{f(\alpha_1)}{f'(\alpha_1)}\right).$$

Now

$$v\left[\frac{f(\alpha_1)}{f'(\alpha_1)}\right] < 1 \quad \text{and} \quad v\left[g_1\left(\alpha_1, \frac{f(\alpha_1)}{f'(\alpha_1)}\right)\right] \leqslant 1$$

imply that $v[f'(\alpha_2)] = v[f'(\alpha_1)] = 1$. We now have $v[f(\alpha_2)] < 1$ and $v[f'(\alpha_2)] = 1$ so that α_2 satisfies the same conditions as α_1. Further, $v(\alpha_3 - \alpha_2) = v[f(\alpha_2)] \leqslant [v(f(\alpha_1))]^2$.

Repeating this process, we have inductively that

$$v(\alpha_2 - \alpha_1) = v[f(\alpha_1)]$$

$$v(\alpha_3 - \alpha_2) = v[f(\alpha_2)] \leq [v(f(\alpha_1))]^2$$

$$v(\alpha_4 - \alpha_3) = v[f(\alpha_3)] \leq [v(f(\alpha_2))]^2 \leq [v(f(\alpha_1))]^4$$

$$\cdots$$

$$v(\alpha_n - \alpha_{n-1}) = v[f(\alpha_{n-1})] \leq [v(f(\alpha_1))]^{2^{n-2}}$$

$$\cdots$$

Let

$$\alpha = \alpha_1 + \sum_{n=1}^{\infty} (\alpha_{n+1} - \alpha_n) = \lim \alpha_n .$$

The series for α converges since

$$\lim v(\alpha_{n+1} - \alpha_n) = \lim v[f(\alpha_1)]^{2^{n-1}} = 0.$$

The continuity of f and the relation $v[f(\alpha_n)] \leq v[f(\alpha_1)]^{2^{n-1}}$ imply that $v[f(\alpha)] = \lim v[f(\alpha_n)] \leq \lim v[f(\alpha_1)]^{2^{n-1}} = 0$. Hence, $f(\alpha) = 0$. Further, since $v(\alpha_n - \alpha_1) \leq \max\{v(\alpha_n - \alpha_{n-1}), \ldots, v(\alpha_2 - \alpha_1)\} < 1$ and $v(\alpha - \alpha_1) = \lim v(\alpha_n - \alpha_1) \leq 1$, we have that

$$v(\alpha) \leq \max\{v(\alpha - \alpha_1), v(\alpha_1)\} \leq 1.$$

Therefore, α is in V.

In particular, this theorem applies to the p-adic valuations. The following theorems are applications of Newton's method.

Theorem 4.26. If a is a quadratic residue modulo an odd prime p then $f(x) = x^2 - a$ has two distinct roots in Q_p.

Proof: Suppose a is a quadratic residue modulo p. There is an α_1 such that $\alpha_1^2 \equiv a(\text{mod } p)$. Then $|f(\alpha_1)|_p = |\alpha_1^2 - a| < 1$ while $|f'(\alpha_1)|_p = |2\alpha_1|_p = 1$. By the previous theorem there is an α in 0_p such that $\alpha^2 = a$. Similarly, there is a root β corresponding to $-\alpha_1$.

Corollary 4.27. If $p = 4k + 1$, then $\sqrt{-1}$ is in Q_p.

Proof: This follows since -1 is a quadratic residue modulo p.

Theorem 4.28. If a is a quadratic non-residue modulo an odd prime p then $f(x) = x^2 - a$ is irreducible in Q_p.

Proof: Suppose there is an α in Q_p such that $\alpha^2 - a = 0$. Then $|\alpha^2|_p \leq \max\{|\alpha^2 - a|_p, |a|_p\} \leq 1$. Hence, $|\alpha|_p \leq 1$ which implies α is in 0_p. Then for some integer b, $\alpha + P = b + P$. But then $a + P = \alpha^2 + P = b^2 + P$ and $b^2 \equiv a(\text{mod } p)$. This contradicts the fact that a is a quadratic non-residue. Therefore, $f(x) = x^2 - a$ is irreducible.

Corollary 4.29. If $p = 4k + 3$, then $\sqrt{-1}$ is not in Q_p.

Proof: For primes of this form -1 is a quadratic non-residue.

Elementary p-adic Analytic Functions

The purpose of this section will be to investigate some of the special functions in the p-adic numbers. Certain elementary functions are of interest to students of mathematics, not only because of their usefulness, but for the special properties they possess. The exponential and logarithm functions are examples. These functions are inverse functions that set up an isomorphism between the additive group of real numbers and the multiplicative group of non-negative real numbers. These functions are useful because they give a method for defining the symbol a^b where a and b are real numbers. A question that arises is whether a similar process can be carried on in a p-adic number field Q_p.

A problem presents itself in the study of the logarithm function. In elementary calculus this function is sometimes developed as the definite integral of the function $f(x) = 1/x$. From the properties of the logarithm the exponential function can be developed as the inverse function. Since this avenue is not available here, the study of these two functions and others will be carried out by considering power series.

Definition 4.30. A p-adic analytic function is a convergent power series of the form

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

where a_n and x are in Q_p. The set of all x for which the series converges is called the domain of convergence and will be denoted by D_f.

All polynomials

$$g(x) = \sum_{i=0}^{n} a_i x^i$$

are analytic functions for which the domain of convergence $D_g = Q_p$. By examples 3.16 and 3.18 the functions $h_m(x) = 1/(1-x)^m$ are analytic functions where the domain of convergence is $\{x: |x|_p < 1\}$. By example 3.30 the analytic function h_1 can be expressed as

$$h_1(x) = \prod_{n=0}^{\infty} \left(1 + x^{2^n}\right).$$

The first p-adic analytic function to be considered will be the logarithm function.

Definition 4.31. The logarithm function is defined on Q_p by

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

Many of the familiar properties of the logarithm can now be established for the p-adic number fields, as well as some peculiar to the situation.

Theorem 4.32. The domain of $\log (1 + x)$ is $\{x: |x|_p < 1\}$.

Proof: See example 3.19.

Theorem 4.33. For x in $D_{\log}$,

(a) the derivative of $\log (1 + x)$ is $1/(1 + x)$;

(b) $\log (1 + x)^{-1} = -\log (1 + x)$; and

(c) $|x|_p < p^{-1/(p-1)}$ implies $|\log (1 + x)|_p = |x|_p$.

Proof: (a) $[\log(1+x)]' = 1/(1+x)$ by example 4.23.

(b) If $|x|_p < 1$ then $|x+1|_p = |1|_p = 1$. This implies that $|(-x)/(1+x)|_p < 1$. By part (a) and example 4.24,

$$\begin{aligned}[\log(1+x)^{-1}]' &= [\log(1+(-x)/(1+x))]' \\ &= [1/(1+(-x)/(1+x))]\cdot[-1/(1+x)^2] \\ &= -1/(1+x) = [-\log(1+x)]'.\end{aligned}$$

Hence, $\log(1+x)^{-1} = -\log(1+x) + c$ for all x in $D_{\log}$. To determine c, set $x = 0$. We have $c = 0$ and

$$\log(1+x)^{-1} = -\log(1+x).$$

(c) For $\operatorname{ord} x > 1/(p-1)$,

$$\operatorname{ord}\frac{x^n}{n} - \operatorname{ord} x = (n-1)\operatorname{ord} x - \operatorname{ord} n > (n-1)\left[1/(p-1) - \frac{\operatorname{ord} n}{n-1}\right].$$

Now $n = p^r m$ where $(p,m) = 1$. This implies that

$$(\operatorname{ord} n)/(n-1) = r/(p^r m-1) \leq r/(p^r-1) = r/\left[(p-1)\sum_{i=0}^{r-1} p^i\right] \leq 1/(p-1)$$

since

$$r \leq \sum_{i=0}^{r-1} p^i.$$

Hence, $\operatorname{ord}\frac{x^n}{n} - \operatorname{ord} x > 0$ and we have

$$\left|\frac{(-1)^{n-1}x^n}{n}\right|_p < |x|_p$$

for $n \geq 2$. This implies that for the partial sums $s_n(x)$ of the logarithmic series we have $|s_n(x)|_p = |x|_p$. Now since

$$\log (1 + x) = \lim s_n(x)$$

and

$$\big|\,|\log (1 + x)|_p - |s_n(x)|_p\big| \leq |\log (1 + x) - s_n(x)|_p$$

we have $|\log (1 + x)|_p = \lim |s_n(x)|_p = \lim |x|_p = |x|_p$.

Definition 4.34. The exponential function is defined by

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

Theorem 4.35. The domain of $\exp x$ is $\{x: |x|_p < p^{-1(p-1)}\}$.

Proof: See example 3.20.

Theorem 4.36. For x in $D_{\exp}$,

(a) the derivative of $\exp x$ is $\exp x$;

(b) $\exp (x + y) = (\exp x)(\exp y)$; and

(c) $|(\exp x) - 1|_p = |x|_p$.

Proof: (a)

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

(b) Using the Cauchy product for power series,

$$(\exp x)(\exp y) = \sum_{n=0}^{\infty} \left(\sum_{i=0}^{n} \frac{x^i}{i!} \cdot \frac{y^{n-i}}{(n-i)!} \right) = \sum_{n=0}^{\infty} \frac{1}{n!} \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i}$$

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

(c) Suppose $\text{ord } x > 1/(p-1)$. For $n \geqq 2$,

$$\begin{aligned} \text{ord } (x^n/n!) - \text{ord } x &= n(\text{ord } x) - \text{ord } n! - \text{ord } x \\ &= n(\text{ord } x) - (n-t_n)/(p-1) - \text{ord } x \\ &= (n-1)(\text{ord } x) - n/(p-1) + t_n/(p-1) \\ &> (n-1)/(p-1) - n/(p-1) + t_n/(p-1) \\ &= (t_n - 1)/(p-1) \geqq 0. \end{aligned}$$

Hence, $|x^n/n!|_p < |x|_p$. This implies that $|s_n(x) - 1|_p = |x|_p$, where the $s_n(x)$ are partial sums of the series for $\exp x$. As in the proof of theorem 4.33 (c) we have

$$|(\exp x) - 1|_p = \lim |s_n(x) - 1|_p = \lim |x|_p = |x|_p.$$

<u>Theorem 4.37</u>. If x is in $D_{\exp}$, then

(a) $\log (\exp x) = x$; and

(b) $\exp (\log (1 + x)) = 1 + x$.

<u>Proof</u>: (a) Set $x = 0$: $\exp 0 = 1$ and $\log 1 = 0$. Since

$$|(\exp x) - 1|_p = |x|_p,$$

$\log (\exp x)$ is defined. Now,

$$[\log (\exp x)]' = (\exp x)'/(\exp x) = (\exp x)/(\exp x) = 1.$$

Hence, $\log (\exp x) = x + c$. To determine c set $x = 0$. Since $\log 1 = 0$, this implies $c = 0$. Therefore, $\log (\exp x) = x$.

(b) Let $f(x) = \exp [\log (1 + x)]$. By theorem 4.33 (c),

$$|\log (1 + x)|_p$$

is in $D_{\exp}$ so that f is defined. Now $f'(x) = f(x)/(1+x)$. For $n \geq 2$, $f^n(x) = 0$. In particular, $f^n(0) = 0$. Therefore, the series expansion for f is $f(x) = 1 + x$.

Theorem 4.38. If x and y are in $D_{\exp}$ and

$$\log(1 + x) = \log(1 + y)$$

then $x = y$.

Proof: Now $1 + x = \exp[\log(1 + x)] = \exp[\log(1 + y)] = 1 + y$. This implies that $x = y$.

Theorem 4.39. If x and y are in $D_{\exp}$, and $\exp x = \exp y$ then $x = y$.

Proof: For x and y in $D_{\exp}$, $x = \log(\exp x) = \log(\exp y) = y$.

Theorem 4.40. If x and y are in $D_{\exp}$, then

$$\log(1 + x)(1 + y) = \log(1 + x) + \log(1 + y).$$

Proof: Since $|x + y + xy|_p \leq \max\{|x|_p, |y|_p, |xy|_p\} < p^{-1/(p-1)}$, $\log(1 + x)(1 + y)$ is defined. By theorems 4.37 (b) and 4.36 (b) we have that

$$\begin{aligned}\exp[\log(1 + x)(1 + y)] &= (1 + x)(1 + y)\\ &= \exp[\log(1 + x)]\exp[\log(1 + y)]\\ &= \exp[\log(1 + x) + \log(1 + y)].\end{aligned}$$

Therefore, by theorem 4.39,

$$\log(1 + x)(1 + y) = \log(1 + x) + \log(1 + y).$$

Theorem 4.37 verifies that the functions log and exp are inverse functions. By theorem 4.36 (b) and theorem 4.40 these functions are homomorphisms. Further, theorems 4.38 and 4.39 tell us these functions are isomorphisms. The exponential function maps the additive subgroup P of Q_p onto the multiplicative subgroup $1 + P$ of Q_p (see theorem 2.53). Thus, the groups P and $1 + P$ are isomorphic.

If α is in $1 + P$ ($\alpha \equiv 1 \bmod p$) then $\log \alpha$ is defined to be $\log [1 + (\alpha - 1)]$. With this definition the usual properties of the logarithm function can be established. These are as follows:

(4.12) $$\log \alpha\beta = \log \alpha + \log \beta;$$

(4.13) $$\log (\alpha/\beta) = \log \alpha - \log \beta; \text{ and}$$

(4.14) $$\log \alpha^k = k(\log \alpha) \text{ for an integer } k.$$

The binomial theorem of elementary algebra is valid in any commutative ring with unity and, hence, is true in Q_p. By example 3.18 the binomial theorem for negative exponents also holds for Q_p. Hence, for x in $P \subset Q_p$, $(1 + x)^m$ is defined for any integer m. The next question that arises is whether this expression can be defined for y in Q_p other than integers. The binomial series is valid for y in 0_p.

<u>Definition 4.41</u>. The Binomial series is defined to be

$$(1 + x)^y = \sum_{n=0}^{\infty} \binom{y}{n} x^n$$

where y is in 0_p and

$$\binom{y}{n} = \frac{\prod_{i=0}^{n-1} (y - i)}{n!}$$

if $n \neq 0$. Let $\binom{y}{0} = 1$.

The identity $(-1)^n \binom{n + i - 1}{i - 1} = \binom{-i}{n}$ can be established by induction on n. With this identity, example 3.18 and definition 4.41 we have that

$$1/(1 + x)^i = \sum_{n=0}^{\infty} (-1)^n \binom{n + i - 1}{i - 1} x^n = \sum_{n=0}^{\infty} \binom{-i}{n} x^n = (1 + x)^{-i}.$$

Hence, example 3.18 is a special case of the binomial series. Thus, for y in Z the binomial theorem and the binomial theorem for negative exponents are special cases of this definition. The next question is whether this series converges when y is not in Z.

Theorem 4.42. The binomial series converges for all x such that $|x|_p < p^{-1/(p-1)}$.

Proof: Since $|y - i|_p \leq \max\{|y|_p, |i|_p\} \leq 1$ we have that

$$\left|\binom{y}{n}\right|_p = \left[\prod_{i=0}^{n-1} |y-i|_p\right]/(|n!|_p) \leq 1/(|n!|_p).$$

By the proof of example 3.20

$$r^{-1} = \overline{\lim} \sqrt[n]{\left|\binom{y}{n}\right|_p} \leq p^{1/(p-1)}.$$

Therefore, $r \geq p^{-1/(p-1)}$ and the series converges at least for $|x|_p < p^{-1/(p-1)}$.

Note that the domain of convergence is not completely determined in this theorem.

Theorem 4.43. If y is in 0_p and $|x|_p < p^{-1/(p-1)}$ then $(1 + x)^y = \exp [y \cdot \log (1 + x)]$.

Proof: Let $f(x) = \exp [y \cdot \log (1 + x)]$. Now,

$$|y \cdot \log (1 + x)|_p = |y|_p |\log (1 + x)|_p \leq |\log (1 + x)|_p = |x|_p < p^{-1/(p-1)}$$

so that $f(x)$ is defined. For $x = 0$, $f(0) = \exp 0 = 1$. By induction it can be shown that

$$f^n(x) = \left[\prod_{i=0}^{n-1} (y-i) \cdot f(x)\right] / (1+x)^n.$$

Hence, $f^n(0)/n! = \binom{y}{n}$ and

$$f(x) = \sum_{n=0}^{\infty} \binom{y}{n} x^n = (1 + x)^y.$$

Corollary 4.44. If s and t are in 0_p and $|x|_p < p^{-1/(p-1)}$, then $(1 + x)^{s+t} = (1 + x)^s (1 + x)^t$.

Proof: Since s and t are in 0_p, $s + t$ is in 0_p and

$$\begin{aligned} (1 + x)^{s+t} &= \exp [(s + t)\log (1 + x)] \\ &= \exp [s \cdot \log (1 + x) + t \cdot \log (1 + x)] \\ &= \exp [s \cdot \log (1 + x)] \cdot [\exp t \cdot \log (1 + x)] \\ &= (1 + x)^s (1 + x)^t. \end{aligned}$$

Corollary 4.45. If s is in 0_p, $|x|_p < p^{-1/(p-1)}$ and $|y|_p < p^{-1/(p-1)}$ then $[(1 + x)(1 + y)]^s = (1 + x)^s(1 + y)^s$.

Proof: For $|x|_p < p^{-1/(p-1)}$ and $|y|_p < p^{-1/(p-1)}$ we have that $|x + y + xy|_p < p^{-1/(p-1)}$. Hence,

$$\begin{aligned}[(1 + x)(1 + y)]^s &= \exp [s\cdot\log (1 + x)(1 + y)] \\ &= \exp [s\cdot\log (1 + x) + s\cdot\log (1 + y)] \\ &= \exp [s\cdot\log (1 + x)] \cdot [\exp [s\cdot\log (1 + y)]] \\ &= (1 + x)^s(1 + y)^s.\end{aligned}$$

Theorem 4.46. If y is in 0_p and $|x|_p < p^{-1/(p-1)}$, then $\log (1 + x)^y = y [\log (1 + x)]$.

Proof: For $n \geqq 2$,

$$\left|\binom{y}{n} x^n\right|_p \leqq \left|\frac{x^n}{n!}\right|_p < |x|_p.$$

Then if $s_n(x)$ is the nth partial sum of the binomial series, $|s_n(x) - 1|_p = |x|_p$. Hence,

$$|(1 + x)^y - 1|_p = \lim |s_n(x) - 1|_p = |x|_p$$

and $\log (1 + x)^y$ is defined. Also,

$$|\log (1 + x)^y|_p = |(1 + x)^y - 1|_p = |x|_p < p^{-1/(p-1)}.$$

Therefore, $\exp [\log (1 + x)^y] = (1 + x)^y = \exp [y \log (1 + x)]$ and by theorem 4.39, $\log (1 + x)^y = y [\log (1 + x)]$.

Corollary 4.47. If s and t are in 0_p and $|x|_p < p^{-1/(p-1)}$, then $[(1 + x)^s]^t = (1 + x)^{st}$.

Proof: By the previous theorem

$$|s[\log (1 + x)]|_p = |\log (1 + x)^s|_p = |x|_p$$

which implies that

$$|\exp[s\cdot\log (1 + x)] - 1|_p = |s\cdot\log (1 + x)|_p = |x|_p < p^{-1/(p-1)}.$$

But this implies that $[(1 + x)^s]^t$ is defined. Therefore,

$$[(1 + x)^s]^t = [\exp (s\cdot\log (1 + x))]^t = \exp \{t\cdot\log [\exp (s\cdot\log (1 + x))]\}$$

$$= \exp [ts\cdot\log (1 + x)] = (1 + x)^{ts} = (1 + x)^{st}.$$

Suppose α is in $1 + P$. Then $\alpha - 1$ is in P. For s in 0_p the symbol α^s is defined to be

$$(4.15) \qquad \alpha^s = [1 + (\alpha - 1)]^s.$$

By theorem 4.42 this expression is well defined. Now suppose α and β are in $1 + P$. If s and t are in 0_p, the following relations are consequences of the previous corollaries and theorems.

$$(4.16) \qquad \alpha^{s+t} = \alpha^s \cdot \beta^t;$$

$$(4.17) \qquad (\alpha\beta)^s = \alpha^s \cdot \beta^s; \text{ and}$$

$$(4.18) \qquad (\alpha^s)^t = \alpha^{st}.$$

The reader has no doubt noticed a distinct difference in defining the symbol a^b in the real numbers by $a^b = \exp [b(\log a)]$ and the definition given here. While this definition has meaning in the reals for a positive and all b, in the field Q_p we are restricted to those elements a in $1 + P$ and b in 0_p. However, with these restrictions in Q_p these concepts are still useful as seen by theorem 4.48 and example 4.52.

The functions defined by the exponential, logarithmic and binomial series are defined for x in $P \subset 0_p$. Furthermore, for x in P these series represent p-adic integers. A further observation is that $\exp 1$ is not defined in Q_p. Hence, we cannot define a number in Q_p in the same manner as $e = \exp 1$ in the reals.

Theorem 4.48. If m is an integer such that $(m,p) = 1$ and α is in $1 + P$ then $f(x) = x^m - \alpha$ has a root in 0_p.

Proof: Since $(m,p) = 1$, $|1/m|_p = 1$ and $1/m$ is in 0_p. Hence, $\alpha^{1/m}$ is in 0_p. By (4.18) $(\alpha^{1/m})^m = \alpha$. Therefore, $x^m - \alpha$ has a root in 0_p.

One further theorem on the binomial series is worth noting.

Theorem 4.49. The derivative of $(1 + x)^y$ is $y(1 + x)^{y-1}$.

Proof: For each n, $n\binom{y}{n} = y\binom{y-1}{n-1}$. Hence,

$$[(1 + x)^y]' = \sum_{n=1}^{\infty} n\binom{y}{n}x^{n-1} = \sum_{n=1}^{\infty} y\binom{y-1}{n-1}x^{n-1}$$

$$= y\sum_{n=0}^{\infty}\binom{y-1}{n}x^n = y(1 + x)^{y-1}.$$

The circular functions can be examined in Q_p, with results similar to those established for the exponential, logarithm and binomial functions. The sine and cosine will be considered here.

Definition 4.50. The sine and cosine functions are defined by

$$\sin x = \sum_{n=0}^{\infty} \frac{(-1)^n x^{2n+1}}{(2n+1)!}$$

and

$$\cos x = \sum_{n=0}^{\infty} \frac{(-1)^n x^{2n}}{(2n)!}$$

respectively.

From previous experience with these functions, one would expect them to have the same radius of convergence as the exponential function.

Theorem 4.51. The sine and cosine series converge for $|x|_p < p^{-1/(p-1)}$.

Proof: The sequences

$$\left\{\sqrt[2n]{|(-1)^n/(2n)!|_p}\right\} \text{ and } \left\{\sqrt[2n+1]{|(-1)^n/(2n+1)!|_p}\right\}$$

are subsequences of $\left\{\sqrt[n]{|1/n!|_p}\right\}$ and since $\lim \sqrt[n]{|1/n!|_p} = p^{1/(p-1)}$ (see example 3.20) we have that

$$\lim \sqrt[2n]{|(-1)^n/(2n)!|_p} = \lim \sqrt[2n+1]{|(-1)^n/(2n+1)!|_p} = p^{1/(p-1)}.$$

Therefore, the sine and cosine series converge for $|x|_p < p^{-1/(p-1)}$.

A natural question that arises is whether

$$(4.19) \qquad \exp(\sqrt{-1}\,x) = \cos x + \sqrt{-1}\sin x$$

for x in $D_{\exp x}$. If $\sqrt{-1}$ is in Q_p then

$$|\sqrt{-1}|_p^2 = |\sqrt{-1}^{\,2}|_p = |-1|_p = 1$$

so that $|\sqrt{-1}|_p = 1$. Hence, if $|x|_p < p^{-1/(p-1)}$, we have that $|\sqrt{-1}\,x|_p < p^{-1/(p-1)}$ which means that $\exp(\sqrt{-1}\,x)$ is defined, which is encouraging. The question to be answered first then is whether $\sqrt{-1}$ is in Q_p. The following example shows this to be the case sometimes.

Example 4.52. Suppose p can be expressed as $p = m^2 + 1$. Then $\sqrt{-1}$ is in Q_p.

We have $|-p|_p < p^{-1/(p-1)}$ and $|1/2|_p = 1$. Hence, by (4.18) and theorem 4.42, $-1 = (1/m^2)[(1 - (m^2 + 1))^{1/2}]^2$. Therefore,

$$\sqrt{-1} = (1/m)\sum_{n=0}^{\infty}\binom{1/2}{n}(-p)^n$$

is in Q_p. So in Q_p $\exp(\sqrt{-1}\,x)$ is defined and,

$$\exp(\sqrt{-1}\,x) = \sum_{n=0}^{\infty}\frac{(\sqrt{-1})^n x^n}{n!} = \sum_{i=0}^{\infty}\frac{(\sqrt{-1})^{2i} x^{2i}}{(2i)!} + \sum_{i=0}^{\infty}\frac{(\sqrt{-1})^{2i+1} x^{2i+1}}{(2i+1)!}$$

$$= \sum_{i=0}^{\infty}\frac{(-1)^i x^{2i}}{(2i)!} + \sqrt{-1}\sum_{i=0}^{\infty}\frac{(-1)^i x^{2i+1}}{(2i+1)!}.$$

Therefore,

$$(4.20) \qquad \exp(\sqrt{-1}\,x) = \cos x + \sqrt{-1}\sin x.$$

The primes in example 4.52 are a special class for which (4.20) is valid in Q_p. By corollary 4.27, $\sqrt{-1}$ is in Q_p whenever p is of the form 4k + 1. For all primes of this form (4.20) is also valid. However, for p = 4k + 3 corollary 4.29 shows that the polynomial $x^2 + 1$ is irreducible in Q_p. An algebraic extension of the field Q_p as well as an extension of the valuation $| \ |_p$ will be required before the relation (4.20) is true in general. This case will have to wait until more theory is developed in the next chapter. The case p = 2 will also be discussed them.

CHAPTER V

EXTENSION OF VALUATIONS

The subject commonly known as algebraic number theory is concerned with factorization in an algebraic number field. By an algebraic number field is meant a finite extension field of the field of rational numbers. There are several approaches to this subject matter, and one of these is the valuation theoretic approach. Since the concept of extension fields plays a central role in the development of algebraic number theory, the question of extending a valuation from a given field to an extension field arises. In Chapter II it was verified that a valuation could be extended from a given field to an extension field that was complete. The general theory of extending valuations is of such magnitude that it cannot be explored in detail in this study. However, the problem of extending a valuation defined on a complete field K to a finite extension field E is within the realm of the theory developed in Chapter II.

The classical theorem known as Hensel's Lemma will be proven. With the resulting corollaries, conclusions can be made about factorization of certain polynomials in a non-archimedean field. Once this lemma is verified, it is possible to prove that a non-archimedean valuation defined on a complete field K can be extended uniquely to a finite extension field E.

Let V be a valuation ring for the non-archimedean valuation v. For any real numbers $r \leq 1$ let $I = \{a: v(x) \leq r\}$.

Theorem 5.1. The set I is an ideal in V.

Proof: See proof of theorem 2.46.

Let π be an element of V. The set of all elements of V such that $v(a) \leq v(\pi)$ form an ideal in V by theorem 5.1.

Definition 5.2. Define the sets J and πV by $J = \{a: v(a) \leq v(\pi)\}$ and $V = \{\pi b: b$ is in $V\}$.

Theorem 5.3. The set πV is an ideal in V and $\pi V = J$.

Proof: For each a in J, $v(a) \leq v(\pi)$ so that $v(a/\pi) \leq 1$. Hence, a/π is in V, so that $a = \pi b$ for some b in V. Therefore, $J \subset \pi V$. For each πb in πV, $v(\pi b) = v(\pi)v(b) \leq v(\pi)$ which implies that πb is in J. Therefore, $J \supset \pi V$ and $J = \pi V$.

Suppose

$$f(x) = \sum_{i=0}^{n} a_i x^i$$

where the coefficients are in πV. Then $f(x)$ is in $\pi V[x]$. Now if $f(x) - g(x)$ is in $\pi V[x]$, the coefficients of $f(x) - g(x)$ are divisible by π.

Definition 5.4. If $f(x) - g(x)$ is in $\pi V[x]$, we write

$$f(x) \equiv g(x) \bmod \pi.$$

Suppose K is a complete field with respect to a non-archimedean valuation v and $\overline{K} = V/P$ is the associated residue field. The canonical mapping of the valuation ring V onto the field $\overline{K}$ defined by $g(a) = a + P = \overline{a}$ is a ring homomorphism. This homomorphism induces a ring homomorphism, h, of $V[x]$ onto $\overline{K}[x]$ defined by

$$(5.1) \qquad h(f(x)) = h\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=0}^{r} \overline{a}_i x^i = \overline{f}(x).$$

Definition 5.5. The polynomial $f(x)$ in $V[x]$ is said to be primitive if $\overline{f}(x) \not\equiv 0$. The polynomial is said to be monic if the leading coefficient is 1.

If

$$f(x) = \sum_{i=0}^{n} a_i x^i$$

and $\overline{f}(x) \not\equiv 0$ then for some a_i, $a_i + P \neq P$. This implies that a_i is not in P so that the greatest common divisor of the coefficients of f is the unity of V. For $K = Q_p$ and $\overline{f}(x) \not\equiv 0$, we have that p does not divide all the coefficients of f. The symbol $\overline{v}(f)$ will be used to denote $\max\{v(a_0), v(a_1), \ldots, v(a_n)\}$. If $\overline{v}(f) \leq 1$ the coefficients of f are in V. For $v(f) = 1$, some coefficient of f is a unit and $\overline{f}(x) \not\equiv 0$.

Theorem 5.6. Suppose K is a complete field with respect to a non-archimedean valuation v, and suppose $v(\pi) < 1$. Further, suppose $\{g_n(x)\}$ is a sequence of polynomials in $V[x]$ such that

(5.2) $$g_n(x) \equiv g_{n-1}(x) \bmod \pi^{n-1} \quad \text{and} \quad \deg g_n(x) = r.$$

Then there exists a polynomial $g(x)$ in $V[x]$ such that

$$g(x) = \lim g_n(x).$$

Proof: Let

$$g_n(x) = \sum_{i=0}^{r} a_i^{(n)} x^i.$$

Since $g_n(x) \equiv g_{n-1}(x) \bmod \pi^{n-1}$, $a_i^{(n)} \equiv a_i^{(n-1)} \bmod \pi^{n-1}$. But then $v(a_i^{(n)} - a_i^{(n-1)}) = v(\pi^{n-1})$ and the sequence $\{a_i^{(n)}\}$ is a Cauchy sequence in K for $i = 0, 1, \ldots, r$. Hence, there is an a_i in K such that $a_i = \lim a_i^{(n)}$. For each n, $v(a_i^{(n)}) \leq 1$ so that $v(a_i) = \lim v(a_i^{(n)}) \leq 1$ and a_i is in V. Let

$$g(x) = \sum_{i=0}^{r} a_i x^i,$$

then $g(x)$ is in $V[x]$ and $g(x) = \lim g_n(x)$.

Theorem 5.7. (Hensel's Lemma) Suppose K is a complete field with respect to a non-archimedean valuation and $f(x)$ is a primitive polynomial of $V[x]$. Suppose further that $g_0(x)$ and $h_0(x)$ are relatively prime polynomials in $\overline{K}[x]$ such that $\overline{f}(x) = g_0(x)h_0(x)$. Then there exists polynomials $g(x)$ and $h(x)$ in $V[x]$ such that

(a) $f(x) = g(x)h(x)$,

(b) $\overline{g}(x) = g_0(x), \overline{h}(x) = h_0(x)$, and

(c) $\deg g(x) = \deg g_0(x)$.

Proof: Let

$$g_0(x) = \sum_{i=0}^{r} \bar{a}_i x^i$$

and

$$h_0(x) = \sum_{i=0}^{t} \bar{b}_i x^i .$$

Without loss of generality, we may choose $g_0(x)$ to be monic. To see this note that we may write $f(x) = g_0(x)h_0(x) = [(\bar{1}/\bar{a}_r)g_0(x)][\bar{a}_r h_0(x)]$. If $\bar{a}_r \neq \bar{1}$, then $(\bar{1}/\bar{a}_r)g_0$ may be chosen in place of g_0. Let $\deg f = s$. Then $\deg \bar{f} \leq s$ so that $\deg h_0 \leq s - r$.

Suppose π is an element in V such that $v(\pi) < 1$. In order to prove the theorem, two sequences of polynomials will be constructed in $V[x]$ by starting with g_0 and h_0 in $\bar{K}[x]$, which satisfy the following conditions:

(5.3) $$f \equiv g_n h_n (\mathrm{mod}\, \pi^n),$$

(5.4) $$g_n \equiv g_{n-1} (\mathrm{mod}\, \pi^{n-1}), \quad h_n \not\equiv h_{n-1} (\mathrm{mod}\, \pi^{n-1}), \quad n > 1,$$

(5.5) $$\bar{g}_n \equiv g_0, \quad \bar{h}_n \equiv h_0, \quad \text{and}$$

(5.6) $$\deg g_n = \deg g_0 = r, \quad \text{and} \quad \deg h_n \leq s - r.$$

Then $g(x) = \lim g_n(x)$ and $h(x) = \lim h_n(x)$ will be the desired polynomials such that $f(x) = g(x)h(x)$.

For the case $n = 1$, we let

$$g_1(x) = \sum_{i=0}^{r} a_i x^i$$

and

$$h_1(x) = \sum_{i=0}^{t} b_i x^i.$$

The polynomials g_0 and h_0 are relatively prime in $\overline{K}[x]$, so that for some polynomials k and ℓ in $V[x]$, $\overline{k}g_0 + \overline{\ell}h_0 = 1$ in $\overline{K}[x]$. We have $\overline{f} - \overline{g_1}\overline{h_1} = \overline{f} - g_0h_0 = 0$ and $\overline{kg_1} + \overline{\ell h_1} - 1 = \overline{k}g_0 + \overline{\ell}h_0 - 1 = 0$ in $\overline{K}[x]$. This implies that the coefficients of these polynomials are in P. Thus, $f - g_1h_1$ and $kg_1 + \ell h_1 - 1$ are in $P[x]$. Let $d = \max\{\overline{v}(f - g_1h_1), \overline{v}(kg_1 + \ell h_1 - 1)\}$. Then $d < 1$. If $d = 0$, then $f - g_1h_1 = 0$ or $f = g_1h_1$, and the theorem is true. If $d \neq 0$, let π be an element of V such that $v(\pi) = d$. The coefficients of $f - g_1h_1$ and $kg_1 + \ell h_1 - 1$ are in the ideal πV so that $f - g_1h_1$ and $kg_1 + \ell h_1 - 1$ are in $\pi V[x]$. We now have that $f \equiv g_1h_1 (\mathrm{mod}\,\pi)$; $\overline{g_1} = g_0$; $\overline{h_1} = h_0$; $\deg g_1 = \deg g_0 = r$; and $\deg h_1 \leqq s - r$.

Suppose now that (5.3),(5.4),(5.5) and (5.6) have been verified for $m = 1, 2, 3, \ldots, n-1$. We want to determine polynomials g_n, h_n, u and t such that

(5.7) $$g_n = g_{n-1} + \pi^{n-1}u \quad\text{and}\quad h_n = h_{n-1} + \pi^{n-1}t.$$

There is a polynomial $w(x)$ such that $f - g_{n-1}h_{n-1} = \pi^{n-1}w$. Because

$$g_nh_n - f = g_{n-1}h_{n-1} - f + \pi^{n-1}(g_{n-1}t + h_{n-1}u) + \pi^{2n-2}uv$$

from (5.7) and $2n - 2 \geqq n$, we have that

$$g_nh_n - f \equiv \pi^{n-1}(g_{n-1}t + h_{n-1}u - w)(\mathrm{mod}\,\pi^n).$$

Hence, $f \equiv g_nh_n(\mathrm{mod}\,\pi^n)$ if and only if we can determine t and u in such a way that

$$g_{n-1}t + h_{n-1}u \equiv w(\mathrm{mod}\,\pi).$$

Now, from the definition of g_1 and h_1 we have $kg_1 + \ell h_1 \equiv 1(\mathrm{mod}\,\pi)$ which implies that

$$(5.8) \qquad wkg_1 + w\ell h_1 \equiv w(\mathrm{mod}\,\pi).$$

By the division algorithm there exists polynomials $q(x)$ and $u(x)$ such that $w(x)l(x) = q(x)g_1(x) + u(x)$ and $\deg u(x) < \deg g_1(x) = r$. Since $g_0(x)$ is monic, $g_1(x)$ can be chosen to be monic. Then the coefficients of $q(x)$ and hence the coefficients of $u(x)$ will be in $V[x]$. Thus, $wkg_1 + w\ell h_1 \equiv (wk + qh_1)g_1 + uh_1 \equiv w(\mathrm{mod}\,\pi)$. Define the polynomial $t(x)$ by replacing all the coefficients of $wk + qh_1$ which are divisible by π, by zero. Then

$$(5.9) \qquad tg_1 + uh_1 \equiv w(\mathrm{mod}\,\pi).$$

Since we have determined t and u, we now define g_n and h_n by (5.7). By (5.4), $g_{n-1} \equiv g_1(\mathrm{mod}\,\pi)$ and $h_{n-1} \equiv h_1(\mathrm{mod}\,\pi)$ so that $g_{n-1}t + h_{n-1}u \equiv g_1t + h_1u \equiv w(\mathrm{mod}\,\pi)$. This verifies (5.3) for $m = n$. Also, (5.4) now follows from (5.7). Since $\pi^{n-1}u$ and $\pi^{n-1}t$ are in $P[x]$, $\overline{g}_n = \overline{g}_{n-1} = g_0$ and $\overline{h}_n = \overline{h}_{n-1} = h_0$ so that (5.5) is satisfied. Only (5.6) remains. Because $\deg u(x) < r$ we have by (5.7) that $\deg g_n = \deg g_{n-1} = r$. Now, if $\deg h_n > s - r$, (5.7) implies that $\deg t > s - r$. Since $\deg w \leq s$ and

$$\deg uh_1 = \deg u + \deg h_1 \leq r + s - r = s$$

by (5.9), we must have that $\deg \overline{tg_1} \leq s$. For $\deg tg_1$ to be greater than s, the coefficient of the term of highest degree in the polynomial tg_1 is divisible by π. In particular, since g_1 is monic, the leading coefficient of t is divisible by π. This is a contradiction; hence, $\deg h \leq s - r$ and (5.6) is satisfied.

The construction is now complete, and by theorem 5.6 there exists polynomials

$$g(x) = \sum_{i=0}^{r} a_i x^i$$

and

$$h(x) = \sum_{i=0}^{s-r} b_i x^i$$

in $V[x]$ such that $g(x) = \lim g_n(x)$ and $h(x) = \lim h_n(x)$. Hence,

$$f(x) \equiv g_n(x)h_n(x) \equiv g(x)h(x) (\mathrm{mod}\,\pi^n)$$

for each n so that $f(x) = g(x)h(x)$. Finally, $\overline{g} = \overline{g}_n = g_0$ and $\overline{h} = \overline{h}_n = h_0$. Now $\deg g \leq r$ and $\deg h \leq s - r$. But

$$s = \deg f = \deg g + \deg h \leq \deg g + s - r$$

which implies that $\deg g \geq r$. Therefore, $\deg g = r = \deg g_0$. This completes the proof.

The question of deciding whether a given polynomial is irreducible or not can be difficult. This lemma gives criteria which is sufficient to show that a polynomial is reducible. To illustrate this lemma, some examples will be given. Recall that if a polynomial

$$f(x) = \sum_{i=0}^{n} a_i x^i$$

with integer coefficients has a rational root r/s then $r|a_0$ and $s|a_n$. This elementary theorem is very useful in determining when a polynomial is irreducible over Q.

Example 5.8. The polynomial $f(x) = x^2 + 2$ is reducible over Q_3, but not over Q.

The only possible rational roots are ±1 and ±2 so it can be determined that $f(x)$ is irreducible over Q. Now in Q_3 the valuation ring is 0_3 and the unique maximal ideal is P. Since we have that $f(x) \equiv x^2 + 2 \equiv x^2 - 4 \equiv (x - 2)(x + 2)(\text{mod } 3)$ then in $(0_3/P)[x]$, $\overline{f}(x) = (x - \overline{2})(x + \overline{2})$ where $(x - \overline{2}, x + \overline{2}) = 1$. By Hensel's lemma $f(x)$ factors in Q_3.

Example 5.9. The polynomial $f(x) = x^3 - x^2 + x + 4$ is reducible over Q_5, but is irreducible over Q.

By checking ±1, ±2 and ±4, it is seen that $f(x)$ is irreducible over Q. Now

$$f(x) \equiv x^3 - 6x^2 + 11x - 6(\text{mod } 5) \equiv (x - 1)(x^2 - 5x + 6)(\text{mod } 5).$$

Therefore, in $(Q_5/P)[x]$ we can choose $g_0(x) = x - \overline{1}$ and $h_0(x) = x^2 - \overline{5}x + \overline{6}$. Again by Hensel's Lemma, $f(x) = g(x)h(x)$ in Q_5.

With the aid of Hensel's Lemma, we can now prove some corollaries which will be essential in proving that a valuation v can be extended to an extension field where the degree of the extension is finite.

Corollary 5.10. If

$$f(x) = \sum_{i=0}^{n} a_i x^i$$

is an irreducible polynomial over $K[x]$, then

$$\bar{v}(f) = \max\{v(a_0), v(a_1), \ldots, v(a_n)\} = \max\{v(a_0), v(a_n)\}.$$

Proof: First suppose $f(x)$ is primitive. Then $v(f) = 1$ and $v(a_i) = 1$ for some i. If $\max\{v(a_0), v(a_n)\} < 1$, there exists an r such that $v(a_r) = 1$ and $v(a_i) < 1$ for $i = r + 1, \ldots, n$. Now

$$\bar{f}(x) = \sum_{i=0}^{r} \bar{a}_i x^i.$$

Let $g_0(x) = \bar{f}(x)$ and $h_0(x) = 1$. Then $\bar{f}(x) = g_0(x)h_0(x)$ where $(g_0(x), h_0(x)) = 1$ and $\deg g_0(x) = r$. Hence, by Hensel's Lemma $f(x) = g(x)h(x)$ with $\deg g(x) = r$ and $\deg h(x) = s - r$. This contradicts irreducibility. Therefore, $\bar{v}(f) = \max\{v(a_0), v(a_n)\}$.

Suppose f is not primitive. Choose a coefficient b such that $v(b) = \bar{v}(f)$. For each coefficient a_i, $v(b^{-1}a_i) \leq v(b^{-1})v(b) = 1$. Since b is one of the coefficients and $v(b^{-1}b) = 1$, we have that $\bar{v}(b^{-1} f) = 1$. Hence, $\bar{v}(b^{-1}f) = \max\{v(b^{-1}a_0), v(b^{-1}a_n)\}$. From the relation $\bar{v}(b^{-1}f) = v(b^{-1})\bar{v}(f)$, we have that

$$\bar{v}(f) = v(b)\bar{v}(b^{-1}f) = v(b)\max\{v(b^{-1}a_0), v(b^{-1}a_n)\} = \max\{v(a_0), v(a_n)\}.$$

Corollary 5.11. If $f(x) = x^n + b_1x^{n-1} + \ldots + b_n$ is a monic irreducible polynomial in $K[x]$, then $f(x)$ is in $V[x]$ if and only if b_n is in V.

Proof: If $f(x)$ is in $V[x]$, then all coefficients are in V. Conversely, if b_n is in V, then

$$\max\{v(b_n),v(b_{n-1}), \ldots, v(1)\} = \max\{v(b_n),v(1)\} = 1.$$

But then b_i is in V for each i. Therefore, $f(x)$ is in $V[x]$.

Corollary 5.12. Suppose $f(x)$ is in $V[x]$ and that α in $\overline{K}$ is a simple root of $f(x)$. Then there exists an element a in V such that $\overline{a} = \alpha$ and $f(a) = 0$.

Proof: In $\overline{K}[x]$, $\overline{f}(x) = (x - \alpha)h_0(x)$ where $(x - \alpha,h_0(x)) = 1$. Then there exists $g(x)$ and $h(x)$ in $V[x]$ such that $f(x) = g(x)h(x)$ and $\deg g(x) = 1$. Now $g(x) = x - a$ for some a in V. Therefore, $\overline{g}(x) = x - \overline{a} = x - \alpha$ so that $\overline{a} = \alpha$.

Finally, we are prepared to show that valuations can be extended to extension fields of finite degree.

Theorem 5.13. Suppose K is a complete field with respect to a non-archimedean valuation v and E is a finite extension of degree n over K. Then v has an extension v_1 to E defined by

$$v_1(\alpha) = \sqrt[n]{v(N\alpha)} \tag{5.10}$$

for each α in E.

Proof: Since $N\alpha$ is in K by theorem 1.13, we have $v(N\alpha) \geqq 0$ and so $v_1(\alpha) \geqq 0$. If $v_1(\alpha) = 0$, then $v(N\alpha) = 0$. But then $N\alpha = 0$ which implies that $\alpha = 0$. This verifies (2.1). To prove (2.2) suppose α and β are in E. Then

$$v_1(\alpha\beta) = \sqrt[n]{v(N(\alpha\beta))} = \sqrt[n]{v(N\alpha)}\,\sqrt[n]{v(N\beta)} = v_1(\alpha)v_1(\beta).$$

To show that (2.3) is valid, we will verify that $v_1(\alpha) \leq 1$ implies $v_1(1 + \alpha) \leq 1$. For α in E, let $p(x) = x^m + b_1x^{m-1} + \ldots + b_m$ be the irreducible minimum polynomial for α over K. Now if $v_1(\alpha) \leq 1$ then

$$\sqrt[n]{v(N\alpha)} \leq 1$$

and $v(N\alpha) \leq 1$. Since $N\alpha = (\pm b_m)^{n/m}$, we have that $v(\pm b_m) \leq 1$ and $v(b_m) \leq 1$. By Corollary 5.11, $p(x)$ is in $V[x]$ since b_m is in V. But this implies that $b_1, b_2, \ldots, b_m$ are all in V. Let

$$q(x) = p(x - 1).$$

Then $q(1 + \alpha) = p(\alpha) = 0$ and $q(x)$ is the minimum polynomial for $1 + \alpha$. We have that

$$N(1 + \alpha) = (\pm q(0))^{n/m} = \pm[(-1)^m + b_1(-1)^{m-1} + \ldots + b_m]^{m/n},$$

which is an element in V. Therefore,

$$v_1(1 + \alpha) = \sqrt[n]{v(N(1 + \alpha))} \leq 1.$$

This shows that v_1 is a non-archimedean valuation defined on E. For each α in K, $N\alpha = \alpha^n$ so that

$$v_1(\alpha) = \sqrt[n]{v(\alpha^n)} = v(\alpha).$$

Therefore, v_1 is an extension of v.

By theorem 5.13 there always exists a valuation v_1 which is an extension of v from K to E where $[E:K] = n$. Several questions can now be asked. Is the valuation v_1 unique? Is the field E complete with respect to the valuation v_1? If v is a discrete valuation, will v_1 also be discrete? The answer to all these questions is affirmative. We pause to consider an example.

Example 5.14. If $p = 4k + 3$ then $| \ |_p$ can be extended to $Q_p(\sqrt{-1})$.

Since -1 is a quadratic non-residue modulo p, $x^2 + 1$ is irreducible over Q_p by theorem 4.28. Then $x^2 + 1$ has a root $\sqrt{-1}$ in the algebraic extension field $Q_p(\sqrt{-1})$ of degree 2 over Q_p. A basis for $Q_p(\sqrt{-1})$ is $\{1, \sqrt{-1}\}$. If α is in $Q_p(\sqrt{-1})$ then $\alpha = a + b\sqrt{-1}$ for some a and b in Q_p. The conjugate of α is $\alpha_1 = a + b(-\sqrt{-1}) = a - b\sqrt{-1}$ so that $N\alpha = a^2 + b^2$. Then

$$v_1(\alpha) = \sqrt{|a^2 + b^2|_p}.$$

This looks very similar to the extension of the absolute value function from the real numbers to the complex numbers.

Denote v_1 on $Q_p(\sqrt{-1})$ by $| \ |'_p$. Since

$$(|\sqrt{-1}|'_p)^2 = |(\sqrt{-1})^2|'_p = 1$$

we have that $|\sqrt{-1}|'_p = 1$. Now if x is in Q_p and $|x|_p < p^{-1/(p-1)}$ then $|\sqrt{-1}\ x|'_p = |x|'_p = |x|_p < p^{-1/(p-1)}$. Because $|1/n!|'_p = |1/n!|_p$, we see by example 3.20 that exp is defined on $Q_p(\sqrt{-1})$ for all α such that $|\alpha|'_p < p^{-1/(p-1)}$. In particular, for $\alpha = \sqrt{-1}y$ where y is in Q_p, $\exp(\sqrt{-1}y) = \cos y + \sqrt{-1}\sin y$. Suppose $\alpha = x + \sqrt{-1}y$. If $|\alpha|'_p < p^{-1/(p-1)}$, $|x|'_p < p^{-1/(p-1)}$ and $|y|'_p < p^{-1/(p-1)}$ where x

and y are in Q_p then we have

$$\exp(x + \sqrt{-1}y) = (\exp x)(\cos y + \sqrt{-1}\sin y).$$

Theorem 5.15. The valuation v_1 is discrete if and only if v is discrete.

Proof: Suppose v is discrete and π is the prime such that $v(\pi)$ generates $v(K^*)$. For each α in E, $\log v_1(\alpha) = (1/n)\log v(N\alpha)$ where $n = [E:K]$. Now $v(N\alpha) = v(\pi)^h$ for some h. If we choose $v(\pi)$ as a base for the logarithm function then

$$\log v_1(\alpha) = (1/n)\log v(N\alpha) = h/n.$$

Then $v_1(\alpha) = [v(\pi)^{1/n}]^h$. The set $\{[v(\pi)^{1/n}]^k: k$ is in $Z\}$ is an infinite cyclic group generated by $v(\pi)^{1/n}$ so that v_1 is discrete. A similar argument shows that v is discrete whenever v_1 is.

The next theorem is stated to complete the discussion on extensions of valuations started in theorem 5.13.

Theorem 5.16. The field E is complete and the valuation v_1 is unique.

Proof: See Van der Waerden, p. 252 or Mosley, p. 74.

The field Q_p is the quotient field for the ring 0_p. Hence, Gauss' lemma and Eisenstein's Criterion can be proven in the same manner as the proofs given in many beginning abstract algebra books. The theorems are stated as follows.

Theorem 5.17. A polynomial $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$ is irreducible in $V[x]$ if and only if it is irreducible in $K[x]$.

Theorem 5.18. Suppose K is the field Q_p. If all the coefficients of $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$, excluding the leading coefficient, are divisible by p but p^2 does not divide a_0 then f is irreducible.

The last theorem can be generalized by supposing that K is a field with a non-archimedean valuation and that the a_i are in P but that a_0 is not the product of two elements of P. The same conclusion follows. This generalization will not be needed in further discussion here.

Corollary 5.19. The polynomial $f(x) = x^n - p$ is irreducible over Q_p for each n.

Corollary 5.20. The polynomial $f(x) = x^{p-1} + x^{p-2} + \ldots + 1$ is irreducible over Q_p.

Proof: Let

$$g(x) = f(x + 1) = \sum_{i=1}^{p} (x + 1)^{p-i} = \sum_{i=0}^{p-1} \binom{p}{i} x^{p-i-1} \tag{5.11}$$

By theorem 5.18 $g(x)$ is irreducible which implies $f(x)$ is irreducible.

Corollary 5.21. The polynomial $f(x) = x^2 + 1$ is irreducible over Q_2.

Proof: The polynomial $f(x + 1) = x^2 + 2x + 2$ is irreducible over Q_2 by theorem 5.18. Hence, $x^2 + 1$ is irreducible over Q_2.

With the aid of corollary 5.21 and the discussion following example 5.14, we see that $x^2 + 1$ has the root $\sqrt{-1}$ in $Q_2(\sqrt{-1})$ an extension field of degree 2 over Q_2. The valuation $|\ |_2$ can be extended to the valuation $|\ |_2'$ defined on $Q_2(\sqrt{-1})$. In this field $\exp(\sqrt{-1}x) = \cos x + \sqrt{-1}\sin x$ for all x such that $|x|_2 < 1/2$.

Consider the field Q_p for an odd prime p. By corollary 5.20, the polynomial $f(x) = x^{p-1} + \ldots + 1$ is irreducible over Q_p. Let t be a root of f. The element t is a pth root of unity since $0 = (t - 1)(t^{p-1} + \ldots + 1) = t^p - 1$. Furthermore, each element of the set $\{t, t^2, \ldots, t^{p-1}\}$ is a pth root of unity. So $f(x)$ factors over $Q_p(t)$ as

$$f(x) = \prod_{i=1}^{p-1} (x - t^i).$$

Hence, in $Q_p(t)$,

$$p = f(1) = \prod_{i=1}^{p-1} (1 - t^i).$$

This shows that in the extension field $Q_p(t)$, p is not a prime. The polynomial g given by (5.11) is irreducible over Q_p and

$$g(t - 1) = 0.$$

Thus, g is the minimal polynomial for $t - 1$. Hence, the norm for $t - 1$ is given by $N(t - 1) = p$. If $|\ |_p'$ is the extension of $|\ |_p$ to Q_p, we have

$$|t - 1|_p' = \sqrt[p-1]{|N(t - 1)|_p} = p^{-1/(p-1)} < 1.$$

By the same reasoning as in example 3.19, $\log(1 + x)$ converges on $Q_p(t)$ for $|x|'_p < 1$. In particular, $\log t = \log 1 + (t - 1)$ is defined and $0 = \log 1 = \log t^p = p(\log t)$. This implies that $\log t = 0$. Note that in $Q_p(t)$, log is not one-to-one. This follows because $\log t = 0 = \log 1$, but $t \neq 1$.

Suppose $t \neq 1$ and $\log t = 0$. We must have $|t - 1|'_p < 1$. If π is a prime in $Q_p(t)$ such that $|\pi|'_p < 1$ then $t = 1 + \alpha\pi$ for some α in the valuation ring V' of $|\ |'_p$. Then

$$t^p = (1 + \alpha\pi)^p = 1 + p\beta$$

for some β in V'. Hence,

$$|t^p - 1|'_p = |p\beta|'_p \leq |p|'_p = |p|_p = \frac{1}{p} < \left(\frac{1}{p}\right)^{1/(p-1)} < 1.$$

But this implies that t^p is in $1 + P$, where P is the unique maximal ideal for $|\ |_p$. Since the exponential function maps P one-to-one onto $1 + P$, we have $\exp x = t^p$ for some x in P. Hence, $x = \log(\exp x) = \log t^p = p(\log t) = 0$, so that

$$\exp x = \exp 0 = 1.$$

Therefore, $t^p = 1$. We can now state the following theorem.

Theorem 5.22. In the field $Q_p(t)$, $\log t = 0$ if and only if $t^p = 1$.

This theorem is a special case of the next theorem which is valid in an extension field over Q_p. It will be stated here without proof. The interested reader may refer to Schilling, page 179.

Theorem 5.23. If E is an extension field of Q_p, then $\log t = 0$ if and only if $t^{p^s} = 1$ for some positive integer s.

Note in the discussion preceeding theorem 5.22 that $\exp(t - 1)$ is not defined in $Q_p(t)$.

As a final application of theorem 4.26 and Eisenstein's Criterion, it will be demonstrated that the fields Q_p and Q_q are not isomorphic for distinct primes p and q.

Theorem 5.24. For distinct primes p and q the fields Q_p and Q_q are not isomorphic.

Proof: Suppose p and q are odd and p is a quadratic residue modulo q. The polynomial $f(x) = x^2 - p$ has p as a root in Q_q by theorem 4.26. If Q_q is isomorphic to Q_p by the mapping $\emptyset$ then $\emptyset(\sqrt{p})^2 = \emptyset(p) = p$. But then $f(x) = x^2 - p$ has the root $\emptyset(\sqrt{p})$ in Q_p. This contradicts the fact that $f(x) = x^2 - p$ is irreducible in Q_p. If p is a quadratic non-residue modulo p choose an integer r such that $1 < r < p$ and r is a quadratic non-residue modulo q. Then rp is a quadratic residue in Q_q. The polynomial $f(x) = x^2 - rp$ has a root $\sqrt{rp}$ in Q_q. The previous argument will suffice to arrive at a contradiction. Now if $p = 2k + 1$ then by theorem 4.48, the polynomial $f(x) = x^3 - p$ has a root in Q_2. If Q_2 were isomorphic to Q_p, we would have that $f(x) = x^3 - p$ has a root in Q_p. Again we have a contradiction. Therefore, in all cases the fields Q_p and Q_q are not isomorphic for $p \neq q$.

To finish the discussion, it is easy to verify the following theorem.

Theorem 5.25. The field Q_p is not isomorphic to the set R of real numbers.

Proof: The number $\sqrt{p}$ is in R. If R is isomorphic to Q_p, the same proof given in theorem 5.24 will suffice to show $f(x) = x^2 - p$ is reducible in Q_p, giving a contradiction.

Conclusion

The important Reducibility lemma of Hensel was presented in this chapter. Regarding this theorem and valuations, Schilling says:

> The realization of the close connection between the theory of algebraic functions of one variable and the theory of algebraic numbers gave rise to the theory of valuations. The arithmetic approach of Dedekind and Weber to the theory of algebraic functions stimulated the question of whether there is an analogue to the power series expansions associated to a point of a Riemann surface. Hensel discovered such an analogue in his theory of p-adic numbers. He recognized that power series expansions can serve to clarify properties of systems of congruences which frequently occur in the allied theories of algebraic numbers and algebraic functions. In his book "Theorie der algebraischen Zahlen" he stated in 1908 the famous Reducibility Lemma on which a major part of the work on valuations is based.

In this chapter the classical method of extending a valuation with the aid of Hensel's lemma was given. Another approach is to define the equivalent concepts of general valuations, general valuation rings and places. With the aid of Zorn's lemma, an extension theorem for places can be proved. Using this theorem on places, it can be demonstrated that general valuations can be extended. For an approach along these lines, confer with [11] or [16].

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. Belmont, Calif.: Brooks Cole (to be published).

3. Artin, Emil. Algebraic Numbers and Algebraic Functions. New York: Gordon and Breach, 1967.

4. Bachman, G. Introduction to p-adic Numbers and Valuation Theory. New York: Academic Press, 1964.

5. Borevich, Z. I. and I. R. Shafarevich. Number Theory, trans. Newcomb Greenlear, New York: Academic Press, 1966.

6. Bruhat, F. Lectures on Some Aspects of p-adic Analysis, Tata Institute of Fundamental Research, Bombay, India, 1966.

7. LeVeque, W. J., ed. Studies in Number Theory, MAA Studies in Mathematics, The Mathematical Association of America, Vol. 6, 1969, 25-75.

8. Lewis, Donald J. Introduction to Algebra. New York: Harper and Row, 1965.

9. Manis, M. E. "Valuations on a Commutative Ring." Proceedings of the American Mathematical Society, Vol. 20, 1969, 193-198.

10. McCarthy, P. J. Algebraic Extensions of Fields. Waltham, Massachusetts: Blaisdell, 1966.

11. Mosley, Edward N. A Study of Valuations of General Rank. (unpub. doctor's dissertation, Oklahoma State University, 1970)

12. O'Meara, O. T. Introduction to Quadratic Forms. New York: Academic Press, 1963.

13. Pollard, H. The Theory of Algebraic Numbers. New York: Wiley, 1950.

14. Roquette, P. "On the Prolongation of Valuations." Trans. Amer. Math. Soc., Vol. 88, 1958, 42-57.

15. Snook, Verbal M. A Study of p-adic Number Fields. (unpub. doctor's dissertation, Oklahoma State University, 1970)

16. Schilling, O. The Theory of Valuations, Mathematical Surveys, American Mathematical Society, 1950.

17. Van der Waerden, B. Modern Algebra. Ungar, New York, 1949.

18. Weiss, Edwin. Algebraic Number Theory. New York: McGraw-Hill, 1963.

VITA 3

Leonard Leon Palmer

Candidate for the Degree of

Doctor of Education

Thesis: SOME ANALYSIS IN A NON-ARCHIMEDEAN FIELD

Major Field: Higher Education

Biographical:

Personal Data: Born in Bloomfield, Missouri, April 5, 1931, the son of Earnest L. and Louise Palmer.

Education: Attended lower grades at Wolf Lake Elementary School in Wolf Lake, Illinois; graduated from Wolf Lake Community High School, Wolf Lake, Illinois in 1949; received the Bachelor of Science in Education degree from Southeast Missouri State College, Cape Girardeau, Missouri, in August, 1958; received the Master of Arts degree from the University of Illinois in August, 1961; completed requirements for the Doctor of Education degree at Oklahoma State University in July, 1971.

Professional Experience: High School instructor of mathematics, Ironton High School, Ironton, Missouri, 1958-60; instructor of mathematics, Lindbergh Jr. High School, St. Louis County, Missouri, 1961-62; Assistant Professor of Mathematics, Southeast Missouri State College, Cape Girardeau, Missouri, 1962-68; graduate teaching assistant, Department of Mathematics and Statistics, Oklahoma State University, 1968-71; returned to the Department of Mathematics, Southeast Missouri State College, Cape Girardeau, Missouri, June, 1971.