

A STUDY OF P-ADIC NUMBER FIELDS

By

Verbal Merle Snook
"

Bachelor of Science
University of Oregon
Eugene, Oregon
1956

Master of Science
University of Oregon
Eugene, Oregon
1962

Master of Arts
University of Illinois
Urbana, Illinois
1962

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
May 1970

OKLAHOMA
STATE UNIVERSITY
LIBRARY
OCT 15 1970

A STUDY OF P-ADIC NUMBER FIELDS

Thesis Approved:

Jeanne Agnew

Thesis Adviser

E. K. Mc Jackson

William Marsden

D. Durham

Dean of the Graduate College

762809.

ACKNOWLEDGMENTS

I am greatly indebted to Dr. Jeanne Agnew for the guidance and assistance which she has provided during the preparation of this thesis. I am thankful to Dr. E. K. McLachlan for his counsel and advice as committee chairman. I am also grateful to Dr. W. Ware Marsden and Dr. Vernon Troxel for serving as committee members.

Finally, I express gratitude to my wife, Carrol, and my daughters, Pamela, Nancy, and Fern for the many sacrifices which they made during the completion of my program of study and the preparation of this thesis.

TABLE OF CONTENTS

| Chapter | Page |
|---|------|
| I. INTRODUCTION | 1 |
| Sets | 3 |
| Algebraic Systems | 4 |
| Number Theory | 7 |
| Order | 7 |
| Metric Spaces | 8 |
| Infinite Series | 11 |
| Vector Spaces | 12 |
| II. THE P-ADIC NUMBER FIELDS | 15 |
| The p-adic Integers | 16 |
| The p-adic Numbers | 28 |
| The p-value Function | 31 |
| Sequences of p-adic Numbers | 34 |
| Infinite Series Representation of p-adic Numbers | 39 |
| A Geometric Model for R_p | 45 |
| III. COMPLETIONS OF THE RATIONAL NUMBERS | 51 |
| Valuations | 51 |
| Non-Archimedean Valuations | 53 |
| Equivalent Valuations | 56 |
| Ostrowski's Theorem | 61 |
| Discrete Valuations | 64 |
| IV. SOME CONSEQUENCES OF THE NON-ARCHIMEDEAN PROPERTY | 67 |
| Ideals of $(0, +, \cdot)$ | 67 |
| Compactness \mathbb{P} | 74 |
| Connectedness | 78 |
| Non-Archimedean Metric Spaces | 79 |
| V. NON-ARCHIMEDEAN NORMED LINEAR SPACES | 84 |
| Normed Linear Spaces | 84 |
| The $\ \cdot \ $ -Topology | 88 |
| Discrete Non-Archimedean Normed Linear Spaces | 93 |
| Topological Linear Spaces | 96 |
| Extension of Linear Functions | 101 |
| A SELECTED BIBLIOGRAPHY | 115 |

LIST OF FIGURES

| Figure | Page |
|---|------|
| 1. E_1^k with $1 \leq k \leq 4$ | 46 |
| 2. Rational Integers Less Than 25 Which Are 5-adic Units | 48 |
| 3. The Relationship Between $p^m \epsilon$, $p^{-m} \epsilon$, and ϵ for ϵ a Unit and $m \geq 0$ | 49 |
| 4. Arcs Containing the Non-Zero Residue Classes of 0_5 Modulo $(5)^2$ | 72 |

CHAPTER I

INTRODUCTION

Even though most formal mathematics education through the undergraduate years centers around the real number systems, there are many other number systems which are useful in mathematical investigations. The p -adic number fields are examples. These fields were introduced by Kurt Hensel in connection with the problem of determining when a polynomial equation in several variables has a solution. Since Hensel's original investigations, p -adic numbers have found extensive applications in algebraic number theory. In many areas of number theoretic investigations, their importance is comparable to the importance of the reals. Weil (19) states in his introduction to Basic Number Theory:

In the days of Dirichlet and Hermite, and even of Minkowski, the appeal to "continuous variables" in arithmetical questions may well have seemed to come out of a magician's bag of tricks. In retrospect, we see now that the real numbers appear there as one of the infinitely many completions of the prime field, one which is neither more or less interesting to the arithmetician than its p -adic companions, and there is at least one language and one technique, ..., for bringing them all together under one roof and making them cooperate for a common purpose.

Given a prime number p , the key to conceiving of the corresponding p -adic number field as a completion of the rational numbers is to replace the concept of absolute value with divisibility by powers of p . Distinct primes yield distinct number fields. Hence there are infinitely many such number fields. The completion process is readily accessible to students at the advanced level and is the procedure fol-

lowed in the mathematical literature when the p -adic number fields are considered. However the completion process does not reveal the nature of a p -adic number.

The purpose of this study is 1) to provide a development of p -adic numbers that is accessible to senior mathematics majors, 2) to reveal the nature of p -adic numbers in relationship to the real numbers, and 3) to consider some algebraic and topological properties of these number systems. The Hahn-Banach theorem for non-archimedean normed linear spaces, as developed in Chapter V, provides an interesting application of several characteristic properties of the p -adic number fields. After such a development, the p -adic number systems are available as a source of examples to illustrate and, coupled with the real numbers where corresponding properties do not always hold, to accentuate specific mathematical concepts.

Books by Borevich and Shafarevich (3) and Bachman (1) are the major references for Chapter II. Bachman is also a source for the material of Chapter III. However a paper on "Global Fields" by Cassels (4) is another reference for Chapter III. Cassel's material is more general than the results for p -adic numbers in particular but adapts well to the p -adic situation. A modification of some of his results appear in the first part of Chapter IV. The material on non-archimedean normed linear spaces derives from papers by Cohen (5) and Ingleton (7). The hint of the possibility of unifying all these sources into the present form comes from Monna's (13) paper.

Before beginning the development of the p -adic numbers, a brief review of some important properties of the real numbers is given. Key concepts are defined, symbolism is explained, and some elementary rela-

relationships between the basic concepts are stated. The reader who is already familiar with these results may proceed directly to Chapter II.

Sets

If S and T are arbitrary sets, then the set

$$S \times T = \{(s, t) : s \in S \text{ and } t \in T\}$$

is the cartesian product of S and T . The elements of $S \times T$ are ordered pairs. A relation between S and T is any subset of $S \times T$ while a relation on S is any subset of $S \times S$. Let \sim be a relation on S . If a pair (s, t) is an element of \sim , it is customary to write $s \sim t$ or $t = \sim(s)$.

Definition 1.1. A relation \sim is an equivalence relation on S if

$$(1.1) \quad a \sim a,$$

$$(1.2) \quad a \sim b \text{ implies } b \sim a,$$

$$(1.3) \quad a \sim b \text{ and } b \sim c \text{ implies } a \sim c$$

for each a , b , and c in S .

A partition of a set S is a representation of S as the union of non-empty mutually disjoint subsets of S . Given an equivalence relation \sim on S , the set

$$[s] = \{t : s \sim t \text{ and } t \in S\}$$

is an equivalence class. The collection of all equivalence classes, S/\sim , is a partition of S and is called the quotient set of S with respect to \sim . Conversely, let $P = \{P_\lambda : \lambda \in \Lambda\}$ be a partition of a set S . Then \sim , defined by

$$a \sim b \text{ if and only if } a \text{ and } b \text{ are in } P_\lambda \text{ for some } \lambda \text{ in } \Lambda,$$

is an equivalence relation.

A relation f from S into T is a function if $t = f(s)$ and $u = f(s)$

implies $t = u$. The image of S under f is the set

$$f(S) = \{t: s \in S \text{ and } t = f(s)\}.$$

If $f(S) = T$, then f is said to be onto T . The function f is a 1-1 function if $f(s) = f(u)$ implies $s = u$. The set

$$f^{-1} = \{(t,s): (s,t) \in f\}$$

is the inverse of f. If X is a subset of T , then the set

$$f^{-1}(X) = \{s: f(s) \in X \text{ and } s \in S\}$$

is the inverse image of X. A binary operation on S is a function from $S \times S$ into 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 $\{t_n\}$ 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 $\{u_n\}$ are equal, $\{s_n\} = \{u_n\}$, if and only if $s_n = u_n$ for each $n \geq 0$.

Algebraic Systems

A set S is closed under an operation if the image of the operation is in S . An algebraic system is a set S that is closed under one or two operations. Groups, rings, integral domains, and fields are algebraic systems. A commutative ring with unity and without divisors of zero is an integral domain. An integral domain where every non-zero element has an inverse is a field.

Let $(G,+)$ denote a group. An equivalence relation \sim on G is compatible with $+$ on G if $x \sim y$ and $w \sim z$ implies that $x + w \sim y + z$ for all $w, x, y,$ and z in G . If \sim is compatible with $+$, then $+$ induces an

operation $+$ on G/\sim defined by

$$[x] +_{\sim} [y] = [x + y].$$

The algebraic system $(G/\sim, +_{\sim})$ is a group. Let H be a subset of G such that $(H, +)$ is a group. Then $(H, +)$ is a subgroup of $(G, +)$. If $(G, +)$ is commutative, then for each x in G the set $x + H = \{x + h : h \in H\}$ is a coset of H . The collection of cosets of H , G/H , is a partition of G .

Theorem 1.2. Let $(G, +)$ be a commutative group and let \sim be an equivalence relation on G compatible with $+$. Then $([0], +)$ is a subgroup of $(G, +)$. The equivalence relation determined by $G/[0]$ is \sim and $(G/[0], +_{\sim})$ is the quotient group $(G/\sim, +_{\sim})$.

It is usual to denote both addition in G and addition in G/\sim by $+$. The context makes clear which addition is intended. Operations are subscripted only for emphasis.

Let $(M, +, \cdot)$ denote a ring. Let N be a subset of M . Then $(N, +, \cdot)$ is a subring of $(M, +, \cdot)$ if $(N, +, \cdot)$ is a ring. If N is a subset of M , then $(N, +, \cdot)$ is a subring of $(M, +, \cdot)$ if and only if $x - y$ and $x \cdot y$ are in N whenever x and y are in N . An ideal of $(M, +, \cdot)$ is a subring $(K, +, \cdot)$ of $(M, +, \cdot)$ such that for each x in K and y in M , $x \cdot y$ is in K . If an ideal contains the unity of the ring, then the ideal is the ring. The ideal $(K, +, \cdot)$ is a principal ideal if there exists k in K such that for each h in K , $h = k \cdot x$ with x in M . The element k is said to generate $(K, +, \cdot)$. A principal ideal generated by k is denoted by $((k), +, \cdot)$. The ideal $(K, +, \cdot)$ is maximal if K is not M and if whenever $(P, +, \cdot)$ is an ideal such that P properly contains K , then $P = M$. And $(K, +, \cdot)$ is prime if $x \cdot y$ an element of K implies that x is in K or y is in K .

If \sim is an equivalence relation on M compatible with both $+$ and \cdot ,

then $([0], +, \cdot)$ is an ideal of $(M, +, \cdot)$. As for $+$, so \cdot induces an operation on M/\sim defined by

$$[x] \cdot [y] = [x \cdot y].$$

Furthermore if \sim is defined on M by

$$(1.4) \quad x \sim y \text{ if and only if } x - y \text{ is in } K,$$

then \sim is an equivalence relation on M that is compatible with both $+$ and \cdot . Hence $M/K = M/\sim$.

Theorem 1.3. If $(M, +, \cdot)$ is a commutative ring with unity and \sim is an equivalence relation on M compatible with both $+$ and \cdot , then $(M/\sim, +, \cdot)$ is a commutative ring with unity.

Theorem 1.4. If $(M, +, \cdot)$ is a commutative ring with unity and if $(K, +, \cdot)$ is an ideal of $(M, +, \cdot)$, then $(K, +, \cdot)$ is maximal if and only if $(M/K, +, \cdot)$ is a field.

Example 1.5. Let $(Q, +, \cdot)$ denote the rational number field and let S be the collection of all sequences of rational numbers. The operations $+$ and \cdot induce corresponding operations on S defined by

$$\{s_n\} + \{u_n\} = \{s_n + u_n\}$$

and

$$\{s_n\} \cdot \{u_n\} = \{s_n \cdot u_n\}.$$

The algebraic structure $(S, +, \cdot)$ is a commutative ring with unity.

Let $(H, +)$ and (K, \oplus) be algebraic systems. An isomorphism from $(H, +)$ onto (K, \oplus) is a 1-1 function from H onto K such that

$$(1.5) \quad f(x + y) = f(x) \oplus f(y)$$

for all x and y in H . Also if $(H, +, \cdot)$ and (K, \oplus, \odot) are algebraic systems, then an isomorphism from $(H, +, \cdot)$ onto (K, \oplus, \odot) is a 1-1 function

from H onto K such that (1.5) holds and

$$(1.6) \quad f(x \cdot y) = f(x) \circ f(y)$$

for all x and y in H . If there exists an isomorphism between two mathematical systems, then the two systems are isomorphic.

Number Theory

Let $(\mathbb{Z}, +, \cdot)$ denote the ring of integers. A relation on \mathbb{Z} , $\equiv (\text{mod } m)$, defined by

$$x \equiv y (\text{mod } m) \text{ if and only if } m \text{ divides } x - y$$

is an equivalence relation on \mathbb{Z} . Furthermore $x \equiv y (\text{mod } m)$ and $w \equiv z (\text{mod } m)$ implies that $x + w \equiv y + z (\text{mod } m)$ and $x \cdot w \equiv y \cdot z (\text{mod } m)$.

If $x \equiv y (\text{mod } m)$, then y is said to be a residue of x modulo m . The equivalence class $[x]$ determined by $\equiv (\text{mod } m)$ contains all residues of x modulo m and is called a residue class modulo m . If $[x]$ is a residue class modulo m , then $[x]$ contains a unique non-negative integer z less than m .

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

Theorem 1.6. (Euler's Theorem) If a and m are relatively prime, then $a^{\phi(m)} \equiv 1 (\text{mod } m)$.

Theorem 1.7. The linear congruence $ax \equiv b (\text{mod } m)$ has a solution if and only if the greatest common divisor of a and m divides b .

Order

A set S is partially ordered by a binary relation \leq on S if

$$x \leq y \text{ and } y \leq z \text{ implies that } x \leq z,$$

$$x \leq x,$$

and

$$x \leq y \text{ and } y \leq x \text{ implies that } x = y$$

whenever x , y , and z are in S . A subset X of a partially ordered set S is bounded above if there exists an element m of S such that $x \leq m$ for each x in X . The element m is an upper bound for X . An upper bound is a least upper bound for X if for every upper bound M for X , $m \leq M$. The concepts of bounded below, lower bound, and greatest lower bound are similarly defined. A set is bounded if it is bounded below and bounded above. The set S is completely ordered if it is partially ordered and if for each x and y in S , either $x \leq y$ or $y \leq x$.

Metric Spaces

Definition 1.8. A metric for a set S is a function d from $S \times S$ into \mathbb{R} such that

$$(1.7) \quad d(x,y) \geq 0 \text{ with equality only if } x = y,$$

$$(1.8) \quad d(x,y) = d(y,x),$$

$$(1.9) \quad d(x,z) \leq d(x,y) + d(y,z)$$

for each x , y , and z in S . The set S with metric d is a metric space and is denoted by (S,d) . Elements of a metric space are called points.

Absolute value is a function from the set of real numbers onto the non-negative real numbers defined by

$$\begin{aligned} |x| &= x, \text{ if } x \geq 0 \\ &= -x, \text{ if } x < 0. \end{aligned}$$

The absolute value function satisfies the following conditions:

$$(1.10) \quad |x| \geq 0 \text{ with equality only if } x = 0,$$

$$(1.11) \quad |xy| = |x| \cdot |y|,$$

$$(1.12) \quad |x + y| \leq |x| + |y|$$

for each x and y in \mathbb{R} . Furthermore

$$(1.13) \quad ||x| - |y|| \leq |x - y|$$

whenever x and y are real numbers. If d is defined from $\mathbb{R} \times \mathbb{R}$ into \mathbb{R} by $d(x,y) = |x - y|$, then d is a metric on \mathbb{R} and (\mathbb{R}, d) is a metric space.

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

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

is called an open sphere with center x and radius r . The set

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

is a closed sphere with center x and radius r .

Let (S, d) be a metric space. Then X , a subset of S , is open 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 . Hence 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. If M is a subset of S , then (M, d) is a metric space. A subset H of M is open in (M, d) if for each x in H there is an open sphere $S(x, r)$ such that the intersection of M and $S(x, r)$ is a subset of H . In some metric spaces, sets are open as well as closed. A metric space (S, d) is connected if no proper subset of S is both open and closed.

Theorem 1.9. A subset M of a space (X, d) is connected if and only if no proper subset of M is both open and closed in (M, d) .

Theorem 1.10. The intersection of any finite collection of open sets is open. The union of any collection of open sets is open.

The collection of all open sets of (S, d) determined by metric d is unique and is called the metric topology for S determined by the metric d . When the metric d for R is determined by absolute value, the metric is said to be induced by $|\cdot|$ and this metric topology is referred to as the $|\cdot|$ -topology for R . The $|\cdot|$ -topology is the usual topology for R .

Suppose (S, d) and (T, \hat{d}) are two metric spaces. The spaces (S, d) and (T, \hat{d}) are isometric if there exists a 1-1 function f from S onto T such that $d(x, y) = \hat{d}(f(x), f(y))$ for all x and y in S . A function f from S into T is continuous at a point x if the inverse image of every open set of (T, \hat{d}) which contains $f(x)$ is an open set of (S, d) . The function f is continuous on S if it is continuous at each point of S .

Theorem 1.11. Let (S, d) and (T, \hat{d}) be two metric spaces. Then a function from S into T is continuous on S if and only if for each x in S and for each $\epsilon > 0$ there exists a $\delta > 0$ such that

$$(1.14) \quad d(f(x), f(y)) < \epsilon \text{ whenever } d(x, y) < \delta$$

with y in S .

A real valued function f is continuous on a subset S of R if and only if for each x in S and for each $\epsilon > 0$ there exists a $\delta > 0$ such that

$$|f(x) - f(y)| < \epsilon \text{ whenever } |x - y| < \delta$$

with y in S .

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

$$(1.15) \quad d(s_n, \ell) < \epsilon \text{ whenever } n \geq N.$$

A sequence which converges with respect to the metric d to a point of the space is called convergent with respect to d . The point ℓ is unique in a metric space and is called the limit of $\{s_n\}$. It is customary to

write $s_n \rightarrow \ell$ or $\lim s_n = \ell$ whenever $\{s_n\}$ converges to ℓ . A sequence $\{s_n\}$ of real numbers converges to a real number ℓ if and only if for each $\varepsilon > 0$ there exists an N such that

$$|s_n - \ell| < \varepsilon \text{ whenever } n \geq N.$$

A sequence $\{s_n\}$ is Cauchy if for each $\varepsilon > 0$ there exists an N such that

$$d(s_n, s_m) < \varepsilon \text{ whenever } m, n \geq N.$$

A sequence $\{s_n\}$ of real numbers is Cauchy if for each $\varepsilon > 0$ there exists an N such that

$$|s_n - s_m| < \varepsilon \text{ whenever } m, n \geq N.$$

A metric space (S, d) is complete with respect to the metric d if every Cauchy sequence of S converges to a point of S . Let (S, d) be a metric space. A nest of closed (open) spheres is a collection of closed (open) spheres that is completely ordered by set inclusion. A metric space (S, d) is spherically complete if every nest of closed spheres has a common point. A set X is dense in S if for each s in S there exists a sequence $\{x_n\}$ in X such that $x_n \rightarrow s$.

Theorem 1.12. Let (S, d) be a metric space. There exists a complete metric space (T, \hat{d}) and a subset T_0 dense in T such that T_0 and S are isometric.

Definition 1.13. A metric space (T, d) is a completion of metric space (S, d) if (T, d) is complete and S is a dense subset of T .

Infinite Series

Given the sequence $\{s_n\}$ of a field $(F, +, \cdot)$, the expression

$$\sum_{n=0}^{\infty} s_n = s_0 + s_1 + \dots + s_n + \dots$$

is an infinite series. Addition of infinite series is defined by

$$\sum_{n=0}^{\infty} s_n + \sum_{n=0}^{\infty} u_n = \sum_{n=0}^{\infty} (s_n + u_n).$$

Multiplication of an infinite series by an element a in F is defined by

$$a \sum_{n=0}^{\infty} s_n = \sum_{n=0}^{\infty} a s_n.$$

It is impossible by the usual definition of addition in the field to assign a field element as the sum of $\sum_{n=0}^{\infty} s_n$. But it is possible to construct a sequence of partial sums, $\{\sum_{k=0}^n s_k\}$. If F has a metric structure and $\sum_{k=0}^n s_k \rightarrow \ell$, then ℓ is the sum of the series and it is customary to write $\sum_{k=0}^{\infty} s_k = \ell$. If $\sum_{k=0}^{\infty} s_k = \ell$, then $s_n \rightarrow 0$ and the sum of $\sum_{k=0}^{\infty} s_k$ is not affected by regrouping terms as long as the order of the terms remain unchanged. If $\sum_{k=0}^{\infty} \hat{s}_k = \hat{\ell}$ also, then $a \sum_{k=0}^{\infty} s_k + b \sum_{k=0}^{\infty} \hat{s}_k = a\ell + b\hat{\ell}$ for each a and b in F .

Vector Spaces

A vector space over a field $(F, +, \cdot)$ is an algebraic system $(V, F, +, \cdot)$ such that $(V, +)$ is a commutative group and \cdot is a function from $F \times V$ into V such that

$$a \cdot (x + y) = a \cdot x + a \cdot y,$$

$$(a + b) \cdot x = a \cdot x + b \cdot x,$$

$$(a \cdot b) \cdot x = a \cdot (b \cdot x), \text{ and}$$

$$1 \cdot x = x$$

for all x and y in V and all a and b in F . The dual usage of "+" and " \cdot " should be noted. Elements of V are called vectors, elements of F are called scalars, and \cdot is called scalar multiplication. Both scalar multiplication and multiplication of scalars are indicated by juxtaposition.

Let W be a nonempty subset of V . Then $(W, F, +, \cdot)$ is a subspace of

$(V, F, +, \cdot)$ if x and y in W and a in F implies $x + y$ and ax are in W . Every vector space contains $(\{0\}, F, +, \cdot)$ as a trivial subspace. This subspace will not be considered in the remainder of this paper. Let S be a subset of V and let $L(S)$ be the set of all elements of the form

$$a_1x_1 + a_2x_2 + \dots + a_nx_n,$$

where n is any positive integer, x_1, x_2, \dots, x_n are any elements of S , and a_1, a_2, \dots, a_n are any scalars. Then $(L(S), F, +, \cdot)$ is a subspace of $(V, F, +, \cdot)$ and is called the subspace generated by S . The set S is called the set of generators of $L(S)$.

A set of vectors $\{x_1, x_2, \dots, x_n\}$ is linearly independent if $a_1x_1 + a_2x_2 + \dots + a_nx_n = 0$ implies $a_1 = a_2 = \dots = a_n = 0$. If a set $B = \{x_1, x_2, \dots, x_n\}$ is a subset of V such that $L(B) = V$, then B spans V . If B is linearly independent and spans V , then B is a basis for V . Suppose there exists some positive integer n such that V contains a set of n vectors which are linearly independent, while every set of $n+1$ vectors in V is not linearly independent. Then $(V, F, +, \cdot)$ is finite dimensional and n is the dimension of $(V, F, +, \cdot)$. If $(V, F, +, \cdot)$ is of dimension n , then there exists a linearly independent subset $S = \{v_1, v_2, \dots, v_n\}$ of V such that for each x in V there exists scalars a_k , $1 \leq k \leq n$, such that

$$x = a_1v_1 + a_2v_2 + \dots + a_nv_n.$$

Under these circumstances, it is often convenient to write

$$V = Fv_1 + Fv_2 + \dots + Fv_n.$$

A vector space which is not finite dimensional is infinite dimensional.

A vector space over the real number field is called a real vector space.

Vector spaces are also called linear spaces.

Example 1.14. Let $(F, +, \cdot)$ be a field and let $F^n = \{(x_1, x_2, \dots, x_n) : x_i, 1 \leq i \leq n, \text{ is in } F\}$. If addition and scalar multiplication are defined

such that $(x_1, x_2, \dots, x_n) + (y_1, y_2, \dots, y_n) = (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n)$ and $a(x_1, x_2, \dots, x_n) = (ax_1, ax_2, \dots, ax_n)$, then $(F^n, F, +, \cdot)$ is an n -dimensional linear space.

Example 1.15. Let $(F, +, \cdot)$ be a field with a metric topology and let C denote the collection of convergent sequences of F . If addition and scalar multiplication are defined by $\{s_n\} + \{\hat{s}_n\} = \{s_n + \hat{s}_n\}$ and $a\{s_n\} = \{as_n\}$, then $(C, F, +, \cdot)$ is an infinite dimensional linear space.

Let $(V, F, +, \cdot)$ and $(W, F, +, \cdot)$ be two vector spaces over the same field F . Then an isomorphism from $(V, F, +, \cdot)$ onto $(W, F, +, \cdot)$ is a 1-1 function f from V onto W such that

$$(1.16) \quad f(x + y) = f(x) + f(y)$$

$$(1.17) \quad f(a \cdot x) = a \cdot f(x)$$

for each x and y in V and a in F . The function f such that (1.16) and (1.17) hold is a linear function from $(V, F, +, \cdot)$ into $(W, F, +, \cdot)$. A linear functional is a linear function from a vector space into the associated scalar field.

CHAPTER II

THE P-ADIC NUMBER FIELDS

There are rational numbers which cannot be expressed by any terminating decimal series expansion. For example,

$$(2.1) \quad 2/3 = 6 \cdot 10^{-1} + 6 \cdot 10^{-2} + 6 \cdot 10^{-3} + \dots$$

where the expansion continues indefinitely with 6 as the coefficient for every power of 10.

At the elementary level, (2.1) is easily justified. The usual procedure is to let m equal the right-hand side of (2.1) and observe that

$$\begin{aligned} 10m &= 6 + 6 \cdot 10^{-1} + 6 \cdot 10^{-2} + 6 \cdot 10^{-3} + \dots, \\ m &= 6 \cdot 10^{-1} + 6 \cdot 10^{-2} + 6 \cdot 10^{-3} + \dots, \end{aligned}$$

and hence that $9m = 6$. Therefore $m = 2/3$ and (2.1) is acceptable.

To make the explanation of (2.1) exact, basic properties of convergent infinite series are required. Since the series $\sum_{n=1}^{\infty} 6 \cdot 10^{-n}$ is a convergent geometric series with $r = 1/10 < 1$, there exists an m in \mathbb{R} such that $\sum_{n=1}^{\infty} 6 \cdot 10^{-n} = m$. Therefore

$$10 \sum_{n=1}^{\infty} 6 \cdot 10^{-n} - \sum_{n=1}^{\infty} 6 \cdot 10^{-n}$$

converges to $9m$. But

$$10 \left\{ \sum_{k=1}^n 6 \cdot 10^{-k} \right\} - \left\{ \sum_{k=1}^n 6 \cdot 10^{-k} \right\} = \{6 - 10^{-n}\}$$

and $\{6 - 10^{-n}\}$ converges to 6. Hence $9m = 6$, $m = 2/3$, and (2.1) holds.

Even though

$$(2.2) \quad 2/3 = 4 + 1 \cdot 5 + 3 \cdot 5^2 + 1 \cdot 5^3 + 3 \cdot 5^4 + \dots$$

with 3 and 1 alternating as coefficients in the series expansion looks

strange, an elementary motivation for the statement that $2/3$ is in some sense equal to

$$4 + 1 \cdot 5 + 3 \cdot 5^2 + 1 \cdot 5^3 + 3 \cdot 5^4 + \dots$$

is even more immediate than the one given for (2.1). Let

$$m = 4 + 1 \cdot 5 + 3 \cdot 5^2 + 1 \cdot 5^3 + 3 \cdot 5^4 + \dots$$

Then

$$\begin{aligned} 3m &= 12 + 3 \cdot 5 + 9 \cdot 5^2 + 3 \cdot 5^3 + 9 \cdot 5^4 + \dots \\ &= 2 + 2 \cdot 5 + 3 \cdot 5 + 9 \cdot 5^2 + 3 \cdot 5^3 + 9 \cdot 5^4 + \dots \\ &= 2 + 5 \cdot 5 + 9 \cdot 5^2 + 3 \cdot 5^3 + 9 \cdot 5^4 + \dots \\ &= 2 + 0 + 10 \cdot 5^2 + 3 \cdot 5^3 + 9 \cdot 5^4 + \dots \\ &= 2 + 0 + 2 \cdot 5^3 + 3 \cdot 5^3 + 9 \cdot 5^4 + \dots \\ &= 2 + 0 + 0 + 5 \cdot 5^3 + 9 \cdot 5^4 + \dots \\ &= 2 + 0 + 0 + 0 + 10 \cdot 5^4 + \dots \end{aligned}$$

where any desired number of zeros occur on the right. Thus at the intuitive stage, $3m = 2$, $m = 2/3$, and (2.2) is acceptable.

In this chapter, a metric topology is defined on the set of rational numbers such that the infinite series of (2.2) is convergent. Then an exact mathematical explanation of (2.2) is given.

The p-adic Integers

Let p be a prime number. If $\sum_{n=0}^{\infty} a_n p^n$ is an infinite series and $s_n = \{\sum_{k=0}^n a_k p^k\}$ is the associated sequence of partial sums, then

$$s_n \equiv s_{n-1} \pmod{p^n}$$

for each $n \geq 1$. The sequence of partial sums of the infinite series of (2.2) is

$$(2.3) \quad \{s_n\} = \{4, 9, 84, 209, 2084, \dots\}.$$

It is clear that $s_n \equiv s_{n-1} \pmod{5^n}$ for each $n \geq 1$.

Definition 2.1. The set S_p consists of all sequences of integers

$$\{x_n\} = \{x_0, x_1, \dots, x_n, \dots\}$$

such that

$$(2.4) \quad x_n \equiv x_{n-1} \pmod{p^n}$$

for each $n \geq 1$.

In Example 1.5, it was observed that the algebraic system $(S, +, \cdot)$ where S is the set of all sequences of rational numbers is a commutative ring with unity. That $(S_p, +, \cdot)$ is a subring of $(S, +, \cdot)$ and hence is a commutative ring with unity is shown in the following theorem:

Theorem 2.2. The system $(S_p, +, \cdot)$ is a commutative ring with unity.

Proof: Since $x_n \equiv x_{n-1} \pmod{p^n}$ and $y_n \equiv y_{n-1} \pmod{p^n}$ implies $x_n - y_n \equiv x_{n-1} - y_{n-1} \pmod{p^n}$ and $x_n y_n \equiv x_{n-1} y_{n-1} \pmod{p^n}$, it follows that if $\{x_n\}$ and $\{y_n\}$ are elements of S_p , then $\{x_n\} - \{y_n\}$ and $\{x_n\} \cdot \{y_n\}$ are elements of S_p . That is, $(S_p, +, \cdot)$ is a subring of $(S, +, \cdot)$. Hence $(S_p, +, \cdot)$ is a commutative ring with unity $\{1\} = \{1, 1, 1, \dots, 1, \dots\}$.

The same procedure followed in the elementary justification of (2.2) implies that

$$(2.5) \quad 2/3 = 9 + 0.5 + 8 \cdot 5^2 + 0.5^3 + 8 \cdot 5^4 + \dots$$

is also acceptable. The sequence of partial sums associated with (2.5) is

$$\{\hat{s}_n\} = \{9, 209, 209, 2084, 2084, \dots\}.$$

Both $\{s_n\}$ of (2.3) and $\{\hat{s}_n\}$ are elements of S_5 . An equality relation is now defined on S_p such that s_n and \hat{s}_n are equal in S_5 .

Definition 2.3. Let $\{x_n\}$ and $\{y_n\}$ be two sequences belonging to S_p .

Then $\{x_n\} = \{y_n\}$ if and only if

$$x_n \equiv y_n \pmod{p^{n+1}}$$

for each $n \geq 0$.

Note that it would be appropriate to subscript "=" with "p" since the definition of = depends upon p and differs from regular equality of sequences. However once aware of the distinction, the reader will not experience any difficulty in determining from context which equality is under consideration.

From the fact that $\equiv (\text{mod } p^{n+1})$ is an equivalence relation on \mathbb{Z} for each $n \geq 0$, it follows that = is an equivalence relation on S_p . Hence the quotient set S_p / \equiv is a partition of S_p .

Definition 2.4. A p-adic integer is an element of S_p / \equiv .

The collection of all p-adic integers is denoted by O_p . It is common to use Greek letters to represent p-adic integers. That is, if $\{x_n\}$ is an element of S_p , then $\alpha = [\{x_n\}]$ is a p-adic integer, $\{x_n\}$ is a representative of α , α is determined by $\{x_n\}$, and it is convenient to write $\alpha \leftrightarrow \{x_n\}$. To distinguish between p-adic integers and the conventional integers of arithmetic, the latter are referred to as rational integers.

It is possible to specify a unique representation of each p-adic integer. Suppose $\alpha \leftrightarrow \{x_n\}$ is a p-adic integer. Let $\{\bar{x}_n\}$ be the unique sequence such that for each $n \geq 0$, \bar{x}_n is the unique non-negative residue modulo p^{n+1} less than p^{n+1} . It follows that $\{x_n\} = \{\bar{x}_n\}$ in the sense of Definition 2.3 and hence that $\alpha \leftrightarrow \{\bar{x}_n\}$.

Since $\bar{x}_n < p^{n+1}$ for $n \geq 0$, there exists sets of integers $\{a_i: 0 \leq a_i < p \text{ whenever } 0 \leq i \leq n-1\}$ and $\{b_i: 0 \leq b_i < p \text{ whenever } 0 \leq i \leq n\}$ such that

$$\bar{x}_{n-1} = a_0 + a_1p + \dots + a_{n-1}p^{n-1}$$

and

$$\bar{x}_n = b_0 + b_1p + \dots + b_{n-1}p^{n-1} + b_n p^n.$$

The fact that $a_i = b_i$ for $0 \leq i \leq n-1$ is proved now by mathematical induction. From $\bar{x}_{n-1} \equiv \bar{x}_n \pmod{p^n}$ for each n and the definitions of a_0 and b_0 , it is clear that $a_0 = b_0$. Assume that $a_i = b_i$ for $0 \leq i \leq m < n-1$. Then

$$a_{m+1} + a_{m+2}p + \dots + a_{n-1}p^{n-m-1}$$

is congruent modulo p to

$$b_{m+1} + b_{m+2}p + \dots + b_{n-1}p^{n-m-1} + b_n p^{n-m}.$$

It follows that $a_{m+1} \equiv b_{m+1} \pmod{p}$ and hence that $a_{m+1} = b_{m+1}$. Therefore $a_i = b_i$ for $0 \leq i \leq m+1 \leq n-1$. Thus for every p -adic integer there corresponds a sequence $\{a_0, a_1, a_2, \dots, a_k, \dots\}$ of integers such that $0 \leq a_k < p$ and

$$\alpha \leftrightarrow \left\{ \sum_{k=0}^n a_k p^k \right\}.$$

These observations are stated in the following theorem:

Theorem 2.5. Every p -adic integer α has a unique representative $\left\{ \sum_{k=0}^n a_k p^k \right\}$ with $0 \leq a_k < p$. Furthermore every such sequence determines some p -adic integer.

Definition 2.6. The unique sequence $\left\{ \sum_{k=0}^n a_k p^k \right\}$ with $0 \leq a_k < p$ which determines α is the canonical sequence of α .

If $\{x_n\}$ and $\{y_n\}$ determine p -adic integers then both $\{x_n + y_n\}$ and $\{x_n y_n\}$ determine p -adic integers since $\equiv \pmod{p^n}$ is compatible with both addition and multiplication.

Definition 2.7. Let $\alpha \leftrightarrow \{x_n\}$ and $\beta \leftrightarrow \{y_n\}$ be p -adic integers. The sum of α and β , $\alpha + \beta$, is the p -adic number determined by $\{x_n + y_n\}$ and the product of α and β , $\alpha\beta$, is the p -adic integer determined by $\{x_n y_n\}$.

If it is also the case that $\alpha \leftrightarrow \{\hat{x}_n\}$ and $\beta \leftrightarrow \{\hat{y}_n\}$, then $x_n \equiv \hat{x}_n \pmod{p^{n+1}}$ and $y_n \equiv \hat{y}_n \pmod{p^{n+1}}$ for each $n \geq 0$. Therefore $x_n + y_n \equiv \hat{x}_n + \hat{y}_n \pmod{p^{n+1}}$, $x_n y_n \equiv \hat{x}_n \hat{y}_n \pmod{p^{n+1}}$, and neither sum nor product of p-adic integers depends upon the representative sequence selected.

Theorem 2.8. The algebraic system $(0_p, +, \cdot)$ is a commutative ring with unity.

Proof: Let $\alpha \leftrightarrow \{x_n\}$ and $\beta \leftrightarrow \{y_n\}$. By Definition 2.7,

$$[\{x_n\}] + [\{y_n\}] = \alpha + \beta = [\{x_n + y_n\}]$$

and

$$[\{x_n\}] \cdot [\{y_n\}] = \alpha\beta = [\{x_n y_n\}].$$

Hence $=$ is compatible with both $+$ and \cdot . Since $0_p = S_p / \equiv$, it follows from Theorems 1.3 and 2.2 that $(0_p, +, \cdot)$ is a commutative ring with unity.

The constant sequence $\{0\} = \{0, 0, \dots, 0, \dots\}$ is an element of S_p such that for each $\{x_n\}$ in S_p , $\{x_n\} + \{0\} = \{x_n\}$. Hence the zero element of $(0_p, +, \cdot)$ is the p-adic integer determined by $\{0, 0, \dots, 0, \dots\}$ and is denoted by 0. Infinitely many other sequences also determine the p-adic zero. If k is any positive integer, then $0 \leftrightarrow \{p^{kn}\}$. In particular, $\{p^n\}$ is a non-constant sequence that determines 0.

For each rational integer z the constant sequence $\{z, z, \dots, z, \dots\}$ is a sequence of S_p that determines a p-adic integer. The relationship between $(Z, +, \cdot)$ and $(0_p, +, \cdot)$ is stated in the following theorem:

Theorem 2.9. The p-adic integers contain an isomorphic copy of the rational integers.

Proof: Let f be a function from Z into 0_p such that for each z in Z ,

$f(z)$ is the p -adic integer determined by the constant sequence $\{z, z, \dots, z, \dots\}$. If $z \neq \hat{z}$ then $f(z) \neq f(\hat{z})$ and f is a 1-1 correspondence between Z and some subset of 0_p . To verify (1.5) and (1.6), note that

$$f(z + \hat{z}) = \{z + \hat{z}, z + \hat{z}, \dots, z + \hat{z}, \dots\} = f(z) + f(\hat{z})$$

and that

$$f(z\hat{z}) = \{z\hat{z}, z\hat{z}, \dots, z\hat{z}, \dots\} = f(z)f(\hat{z}).$$

Thus f is an isomorphism.

As usual, the isomorphism will be de-emphasized and Z will be considered as a subset of 0_p . That is, for each z in Z the p -adic integer z is the equivalence class containing the constant sequence $\{z, z, \dots, z, \dots\}$. However this class will be identified as the p -adic integer z . Thus $1 \leftrightarrow \{1, 1, \dots, 1, \dots\}$ is the unity of $(0_p, +, \cdot)$.

Subtraction and division of p -adic integers are defined in terms of addition and multiplication. That is,

$$\alpha - \beta = \gamma \text{ if and only if } \alpha = \beta + \gamma$$

and

$$\alpha \div \beta = \gamma, \beta \neq 0, \text{ if and only if } \alpha = \beta\gamma.$$

If $\alpha \leftrightarrow \{x_n\}$, $\beta \leftrightarrow \{y_n\}$, and $\gamma \leftrightarrow \{z_n\}$, it is clear that

$\alpha - \beta \leftrightarrow \{x_n - y_n\}$. Hence $\alpha - \beta = \gamma$ if and only if $x_n - y_n \equiv z_n \pmod{p^n}$ for each $n \geq 0$. Furthermore $\alpha/\beta = \gamma$ if and only if $\alpha \leftrightarrow \{y_n z_n\}$ or equivalently, if and only if $x_n \equiv y_n z_n \pmod{p^{n+1}}$ for each $n \geq 0$.

In general, elements of a commutative ring with unity need not have multiplicative inverses. For instance, the only rational integers which have multiplicative inverses are 1 and -1. Many p -adic integers have multiplicative inverses.

Definition 2.10. A p-adic integer α is a unit if and only if there exists a p-adic integer β such that $\alpha\beta = 1$, the multiplicative identity of $(\mathbb{O}_p, +, \cdot)$.

A sequence which represents a p-adic unit can be identified by its first entry as the following theorem shows.

Theorem 2.11. (3) A p-adic integer $\alpha \leftrightarrow \{x_n\}$ is a unit if and only if $x_0 \not\equiv 0 \pmod{p}$.

Proof: Suppose α is a p-adic unit. Then there exists p-adic integer $\beta \leftrightarrow \{y_n\}$ such that $\alpha\beta = 1$. Hence $\{x_n y_n\} = \{1, 1, \dots, 1, \dots\}$ and $x_n y_n \equiv 1 \pmod{p^{n+1}}$ for each $n \geq 0$. In particular, $x_0 y_0 \equiv 1 \pmod{p}$ and $x_0 \not\equiv 0 \pmod{p}$. Conversely, suppose $x_0 \not\equiv 0 \pmod{p}$. Since $x_n \equiv x_{n-1} \pmod{p^n}$ for each $n \geq 1$, $x_n \equiv x_0 \pmod{p}$ and therefore $x_n \not\equiv 0 \pmod{p}$ for each $n \geq 0$. It follows from Theorem 1.7 that for each $n \geq 0$ there is a y_n such that $x_n y_n \equiv 1 \pmod{p^{n+1}}$. Consequently $x_n y_n \equiv x_{n-1} y_{n-1} \pmod{p^n}$, and $y_n \equiv y_{n-1} \pmod{p^n}$, and $\{y_n\}$ determines a p-adic integer. Let $\beta \leftrightarrow \{y_n\}$. Then for each $n \geq 0$, $x_n y_n \equiv 1 \pmod{p^n}$, $\{x_n y_n\} = \{1\}$, and $\alpha\beta = 1$. Therefore α is a p-adic unit.

A p-adic integer α determined by a canonical sequence $\{\sum_{k=0}^n a_k p^k\}$ is a unit, if and only if $a_0 \neq 0$. Since a rational integer z , considered as a p-adic integer, is determined by $\{z, z, \dots\}$, z is a p-adic unit if and only if z is not a multiple of p . Furthermore, z a p-adic unit implies that z^{-1} is a unit and hence that yz^{-1} is a p-adic integer whenever y is a rational integer. In particular, $2/3$ and $3/2$ are in \mathbb{O}_5 .

For each $p \neq 2$, 2 is not a multiple of p and hence 2 is a p-adic unit. Therefore $1/2$ is also a p-adic unit. Let $1/2 \leftrightarrow \{\sum_{k=0}^n a_k p^k\}$ with

$0 \leq a_k < p$. Then $1 \leftrightarrow \{\sum_{k=0}^n 2a_k p^k\}$ and $\sum_{k=0}^n 2a_k p^k \equiv 1 \pmod{p^{n+1}}$ for each $n \geq 0$. Since

$$2a_0 \equiv 1 \pmod{p},$$

$2a_0 - 1 = p$ and $a_0 = (p+1)/2$. From

$$p + 1 + 2a_1 p \equiv 1 \pmod{p^2},$$

it follows that $2a_1 + 1 \equiv 0 \pmod{p}$ and hence that $a_1 = (p-1)/2$. It is now shown by induction that $a_n = (p-1)/2$ for $n \geq 1$. Assume that $a_k = (p-1)/2$ for $1 \leq k \leq n$. Then since

$$p + 1 + (p-1)p + \dots + (p-1)p^n + 2a_{n+1}p^{n+1} \equiv 1 \pmod{p^{n+2}},$$

$2a_{n+1}p^{n+1} + p^{n+1} \equiv 0 \pmod{p^{n+2}}$ and $2a_{n+1} + 1 \equiv 0 \pmod{p}$. That is,

$a_{n+1} = (p-1)/2$. Therefore

$$(2.6) \quad \frac{1}{2} \leftrightarrow \{(p+1)/2 + \sum_{k=1}^n \frac{p-1}{2} p^k\}.$$

Example 2.12. The number $2/3$ is a 5-adic integer. If

$2/3 \leftrightarrow \{\sum_{k=0}^n a_k 5^k\}$, then $\sum_{k=0}^n 3a_k 5^k \equiv 2 \pmod{5^{k+1}}$. It is possible to evaluate a_k for each $k \geq 0$. Since

$$3a_0 \equiv 2 \pmod{5},$$

$a_0 = 4$. From

$$3 \cdot 4 + 3a_1 5 \equiv 2 \pmod{5^2},$$

it follows that $3a_1 5 \equiv -10 \pmod{5^2}$ and hence that $3a_1 \equiv -2 \pmod{5}$.

Therefore $a_1 = 1$. Now

$$3 \cdot 4 + 3 \cdot 1 \cdot 5 + 3 \cdot a_2 \cdot 5^2 \equiv 2 \pmod{5^3}$$

implies that $3a_2 5^2 \equiv -25 \pmod{5^3}$ and hence that $3a_2 \equiv -1 \pmod{5}$. Consequently $a_2 = 3$. Since

$$3 \cdot 4 + 3 \cdot 1 \cdot 5 + 3 \cdot 3 \cdot 5^2 + 3 \cdot a_3 \cdot 5^3 \equiv 2 \pmod{5^4},$$

$3a_3 \equiv -2 \pmod{5}$ and the procedure repeats. Therefore $a_0 = 4$, $a_{2n-1} = 1$, and $a_{2n} = 3$. In 0_5 ,

$$\begin{aligned} 2/3 &\leftrightarrow \{4 + \sum_{k=1}^n (2 + (-1)^k)5^k\} \\ &= \{4, 9, 84, 209, 2084, \dots\}. \end{aligned}$$

From (2.6), it follows that in O_5

$$1/2 \leftrightarrow \{3, 13, 63, 313, 1563, \dots\}$$

and hence that

$$3/2 \leftrightarrow \{4, 14, 64, 314, 1564, \dots\}.$$

Therefore

$$\begin{aligned} 3/2 \cdot 2/3 &\leftrightarrow \{16, 126, 5376, 65626, 3259376, \dots\} \\ &= \{1, 1, 1, 1, 1, \dots\} \leftrightarrow 1 \end{aligned}$$

and $3/2 \cdot 2/3 = 1$ in $(O_5, +, \cdot)$.

The next result is an interesting counter-part to the fundamental theorem of the arithmetic of non-negative integers and gives insight into the arithmetic of p-adic integers.

Theorem 2.13. (3) Every p-adic integer, distinct from zero, has a unique representation in the form

$$\alpha = p^m \epsilon$$

where m is a non-negative integer and ϵ is a unit of the ring $(O_p, +, \cdot)$.

Proof: If α is a unit, then the conclusion follows with $m = 0$. Let $\alpha \leftrightarrow \{x_n\}$ be a non-unit. By Theorem 2.11, $x_0 \equiv 0 \pmod{p}$. Since $\alpha \neq 0$, there exists an n such that $x_n \not\equiv 0 \pmod{p^{n+1}}$. Let m be the smallest integer for which

$$x_m \not\equiv 0 \pmod{p^{m+1}}.$$

For any $s \geq 0$,

$$\begin{aligned} x_{m+s} &\equiv x_{m+s-1} \pmod{p^{m+s}}, \\ x_{m+s-1} &\equiv x_{m+s-2} \pmod{p^{m+s-1}}, \\ &\dots \end{aligned}$$

and

$$x_{m+s-s} \equiv x_{m+s-(s+1)} \pmod{p^{m+s-s}},$$

Hence $x_{m+s} \equiv x_{m-1} \pmod{p^m}$. But $x_{m-1} \equiv 0 \pmod{p^m}$. Therefore the number $y_s = x_{m+s}/p^m$ is an integer. Since $x_{m+s} \equiv x_{m+s-1} \pmod{p^{m+s}}$, it follows that $y_s p^m \equiv y_{s-1} p^m \pmod{p^{m+s}}$ and hence that $y_s \equiv y_{s-1} \pmod{p^s}$ for $s \geq 1$. Thus $\epsilon \leftrightarrow \{y_0, y_1, \dots, y_s, \dots\}$ is a p-adic integer. Furthermore $y_0 = x_m/p^m$ and $x_m \not\equiv 0 \pmod{p^{m+1}}$ implies that $y_0 \not\equiv 0 \pmod{p}$ and hence that ϵ is a unit. From $p^m y_s = x_{m+s} \equiv x_s \pmod{p^{s+1}}$, it follows that $p^m \epsilon = \alpha$ and that α has the desired representation.

It remains to show that the representation is unique. Suppose $\alpha = p^k \eta$ with $k \geq 0$ and $\eta \leftrightarrow \{z_n\}$ a unit. Then since $\{p^m y_s\}$ and $\{p^m z_s\}$ each represent α ,

$$(2.7) \quad p^m y_s \equiv p^k z_s \pmod{p^{s+1}}$$

for each $s \geq 0$. In particular for $s = m$,

$$(2.8) \quad p^m y_m \equiv p^k z_m \pmod{p^{m+1}}$$

and with $s = k$

$$(2.9) \quad p^m y_k \equiv p^k z_k \pmod{p^{k+1}}.$$

But Theorem 2.11 implies p does not divide either y_s or z_s for each $s \geq 0$. Hence (2.8) implies $k \geq m$ and (2.9) implies $m \geq k$. Therefore $m = k$. If in (2.7) s is replaced by $s+m$, the result is

$$p^m y_{s+m} \equiv p^m z_{s+m} \pmod{p^{m+s+1}}$$

or

$$y_{m+s} \equiv z_{m+s} \pmod{p^{s+1}}.$$

Since $y_{m+s} \equiv y_s \pmod{p^{s+1}}$ and $z_{m+s} \equiv z_s \pmod{p^{s+1}}$, it follows that $y_s \equiv z_s \pmod{p^{s+1}}$ for all $s \geq 0$ and hence that $\epsilon = \eta$.

Theorem 2.13 reveals the simplicity of the arithmetic of p-adic

integers. There is a unique prime element in O_p . This prime element is p . Every non-zero element of O_p is a product of a power of p and a unit. Another useful property of O_p is formalized in the following corollary:

Corollary 2.14. The p -adic integer $\alpha \leftrightarrow \{x_n\}$ is divisible by p^k if and only if $x_n \equiv 0 \pmod{p^{n+1}}$ whenever $0 \leq n \leq k-1$.

Proof: If $\alpha = p^m \epsilon$ is divisible by p^k , then p^k divides p^m and $k \leq m$. Since m is the smallest integer such that $x_m \not\equiv 0 \pmod{p^{m+1}}$, $x_n \equiv 0 \pmod{p^{n+1}}$ whenever $0 \leq n \leq k-1$. Conversely, if $x_n \equiv 0 \pmod{p^{n+1}}$ whenever $0 \leq n \leq k-1$, then from $\alpha = p^m \epsilon$ it follows that $m \geq k$ and p^k divides p^m . Hence p^k divides $\alpha = p^m \epsilon$.


Corollary 2.15. The ring $(O_p, +, \cdot)$ is an integral domain.

Proof: It is sufficient to prove that $(O_p, +, \cdot)$ has no zero divisors. Assume that $\alpha\beta = 0$. If $\alpha \neq 0$ and $\beta \neq 0$, then $\alpha = p^m \epsilon$ and $\beta = p^n \eta$ where $\epsilon \leftrightarrow \{x_n\}$ and $\eta \leftrightarrow \{y_n\}$ are units. Hence $p^{m+n} x_0 y_0 \equiv 0 \pmod{p^k}$ for each $k \geq 0$. In particular, $p^{m+n} x_0 y_0 \equiv 0 \pmod{p^{m+n+1}}$ and $x_0 y_0 \equiv 0 \pmod{p}$ while $x_0 \not\equiv 0$ and $y_0 \not\equiv 0$ modulo p . Since this is impossible, $\alpha = 0$ or $\beta = 0$ and $(O_p, +, \cdot)$ is an integral domain.

Thus $(O_p, +, \cdot)$, like $(\mathbb{Z}, +, \cdot)$ is an integral domain. It is in this sense that the elements of $(O_p, +, \cdot)$ are called integers.

Since $(O_p, +, \cdot)$ is a ring, congruence modulo a p -adic integer is defined as for rings in general.

Definition 2.16. Let α and β be p -adic integers. Then $\alpha \equiv \beta \pmod{\gamma}$ if and only if $\alpha - \beta$ is divisible by γ .

But $\alpha - \beta$ is divisible by γ if and only if $\alpha - \beta$ is divisible by $p^m \epsilon$ 

where ϵ is a unit. Therefore $\alpha \equiv \beta \pmod{\gamma}$ only if $\alpha \equiv \beta \pmod{p^m}$ for some m . Hence as far as congruence modulo a p -adic integer is concerned, considerations involving congruences modulo powers of the prime p are sufficient.

Since $(\mathbb{Z}, +, \cdot)$ is a subring of $(\mathbb{O}_p, +, \cdot)$, it is closed under subtraction. Therefore if x and y are rational integers such that $x - y = p^m k$, then the p -adic integer $p^m k$ must be a rational integer and hence k is a rational integer. It follows that $x \equiv y \pmod{p^m}$ in $(\mathbb{Z}, +, \cdot)$ if and only if $x \equiv y \pmod{p^m}$ in $(\mathbb{O}_p, +, \cdot)$. Thus \mathbb{O}_p has at least p^m residue classes modulo p^m . The fact that there are only p^m such residue class completes the proof of the following result:

Theorem 2.17. There are p^m residue classes in \mathbb{O}_p modulo p^m .

Proof: To complete the proof, it is sufficient to show that every p -adic integer is congruent to a rational integer modulo p^m . Let $\alpha \leftrightarrow \{x_n\}$ be a p -adic integer. The rational integer x_{m-1} is the p -adic integer determined by the constant sequence $\{x_{m-1}, x_{m-1}, \dots\}$. Since $x_{m-1} \equiv x_k \pmod{p^k}$ for $0 \leq k \leq m-1$,

$$\alpha - x_{m-1} \leftrightarrow \{x_0 - x_{m-1}, x_1 - x_{m-1}, \dots, 0, x_m - x_{m-1}, \dots\}$$

is a p -adic integer such that

$$x_k - x_{m-1} \equiv 0 \pmod{p^k}$$

for $0 \leq k \leq m-1$. From Corollary 2.14, it follows that $\alpha - x_{m-1}$ is divisible by p^m . Hence

$$\alpha \equiv x_{m-1} \pmod{p^m}$$

where x_{m-1} is a rational integer.

Thus $(\mathbb{O}_p, +, \cdot)$ is like $(\mathbb{Z}, +, \cdot)$ in that for each $n \geq 1$, congruence modulo p^n determines respective partitions on each set consisting of exactly p^n residue classes. The p -adic integers are unlike the rational

integers in that there is at least one residue class of p -adic integers that has cardinality of the continuum. This observation is a consequence of the following theorem:

Theorem 2.18. The set of p -adic integers is uncountably infinite.

Proof: From Theorem 2.5, it follows that there is a 1-1 correspondence between the p -adic integers and the canonical sequences. Therefore it is sufficient to show that the canonical sequences are uncountable. Assume that the canonical sequences are countable and hence that there is a 1-1 correspondence between the non-negative integers and the canonical sequences. Thus there is an exhaustive sequence of expansions:

$$\begin{aligned} & a_{00} + a_{01}p + \dots + a_{0n}p^n + \dots \\ & a_{10} + a_{11}p + \dots + a_{1n}p^n + \dots \\ & a_{20} + a_{21}p + \dots + a_{2n}p^n + \dots \\ & \dots \\ & a_{n0} + a_{n1}p + \dots + a_{nn}p^n + \dots \\ & \dots \end{aligned}$$

where $0 \leq a_{ij} < p$ for each $i \geq 0$ and $j \geq 0$. Consider

$$(2.10) \quad b_0 + b_1p + b_2p^2 + \dots + b_kp^k + \dots$$

such that $0 \leq b_k < p$ and $b_k \neq a_{kk}$ for each $k \geq 0$. Since (2.10) is not one of the expansions listed, $\{\sum_{k=0}^n b_k p^k\}$ was not counted. This contradiction to the assumption that the canonical sequences are countable implies that the set of p -adic integers is uncountable.

The p -adic Numbers

In a manner analogous to the development of the rational number field from the rational integers, it is possible to construct a quotient

field containing an isomorphic copy of $(0_p, +, \cdot)$.

Theorem 2.19. There exists a field that contains a subset isomorphic to $(0_p, +, \cdot)$.

Proof: Let $T = \{(\alpha, \beta) : \beta \neq 0\}$ be a subset of $0_p \times 0_p$ and let $+$ and \cdot be operations on T defined by

$$(\alpha, \beta) + (\gamma, \delta) = (\alpha\delta + \beta\gamma, \beta\delta)$$

and

$$(\alpha, \beta) \cdot (\gamma, \delta) = (\alpha\gamma, \beta\delta).$$

Then $(T, +, \cdot)$ is a commutative ring with $(1, 1)$ as unity. A relation \sim on T defined by

$$(\alpha, \beta) \sim (\gamma, \delta) \text{ if and only if } \alpha\delta = \beta\gamma,$$

is an equivalence relation on T . Therefore T/\sim partitions T . Since

$$(\alpha, \beta) + (\gamma, \delta) \sim (\lambda, \mu) + (\nu, \omega) \text{ and } (\alpha, \beta) \cdot (\gamma, \delta) \sim (\lambda, \mu) \cdot (\nu, \omega)$$

$$\text{whenever } (\alpha, \beta) \sim (\lambda, \mu) \text{ and } (\gamma, \delta) \sim (\nu, \omega), \sim \text{ is compatible with both } + \text{ and } \cdot.$$

From Theorem 1.3, it follows that $(T/\sim, +, \cdot)$ is a commutative ring with

unity. The unity is $[(1, 1)]$. It is clear from the definition of \sim

that for each non-zero α in 0_p , (α, α) is an element of $[(1, 1)]$ and hence

is a representative of the unity.

Since $[(\alpha, \beta)] + [(0, \delta)] = [(\alpha, \beta)]$ for each $[(\alpha, \beta)]$ in T/\sim , $[(0, \delta)]$

is the zero element of $(T/\sim, +, \cdot)$. If $[(\alpha, \beta)] \cdot [(\lambda, \mu)] = [(0, \delta)]$, then

$$(\alpha\lambda, \beta\lambda) \text{ is an element of } [(0, \delta)] \text{ and } \alpha\lambda\delta = 0. \text{ It follows that } \alpha\lambda = 0$$

and hence that $[(\alpha, \beta)] = [(0, \delta)]$ or $[(\lambda, \mu)] = [(0, \delta)]$. That is,

$(T/\sim, +, \cdot)$ is an integral domain.

To complete the proof, it is sufficient to show that every non-zero

element of $(T/\sim, +, \cdot)$ has an inverse. If (α, β) is not an element of

$[(0, 1)]$, then α is non-zero and (β, α) is an element of T . Since

$$[(\alpha, \beta)] \cdot [(\beta, \alpha)] = [(\alpha\beta, \alpha\beta)], \text{ the unity of } (T/\sim, +, \cdot), \text{ it follows that}$$

$[(\beta, \alpha)]$ is the inverse of $[(\alpha, \beta)]$. Hence every non-zero element of $(T/\sim, +, \cdot)$ has an inverse.

Let D be the collection of $[(\alpha, 1)]$ such that α is a non-zero element of 0_p and 1 is the p -adic unity. It is clear that D is a subset of T/\sim and is closed under the operations of $(T/\sim, +, \cdot)$. If f is the function from 0_p into T/\sim such that $f(\alpha) = [(\alpha, 1)]$, then f is an isomorphism from $(0_p, +, \cdot)$ onto $(D, +, \cdot)$ and $(T/\sim, +, \cdot)$ contain an isomorphic copy of $(0_p, +, \cdot)$.

The isomorphism is de-emphasized and 0_p is considered as a subset of T/\sim . The set T/\sim is denoted by R_p and the field $(T/\sim, +, \cdot)$ is denoted by $(R_p, +, \cdot)$.

Definition 2.20. For a given prime p , the field $(R_p, +, \cdot) = (T/\sim, +, \cdot)$ is the p -adic number field. Elements of R_p are p -adic numbers.

If α and $\beta \neq 0$ are p -adic integers, then α/β denotes the equivalence class $[(\alpha, \beta)]$ of R_p .

Since $(0_p, +, \cdot)$ contains an isomorphic copy of $(Z, +, \cdot)$, $(R_p, +, \cdot)$ contains an isomorphic copy of $(Z, +, \cdot)$. Hence $(R_p, +, \cdot)$ contains an isomorphic copy of $(Q, +, \cdot)$. As is usual, $(Q, +, \cdot)$ is considered as a subfield of $(R_p, +, \cdot)$.

Each non-zero p -adic number has an unusually simple representation.

Theorem 2.21. Any non-zero p -adic number $\xi = \alpha/\beta$ is uniquely expressed in the form $\xi = p^m \epsilon$ where ϵ is a unit and m is an integer.

Proof: Since α and β are p -adic integers, $\alpha = p^k \eta$ and $\beta = p^h \mu$ where k and h are non-negative integers and where η and μ are units. Hence $\xi = p^{k-h} \epsilon$ where $\epsilon = \eta/\mu$ is a unit and $k-h = m$ is an integer. To verify uniqueness, observe that α and β have unique representation $\alpha = p^k \eta$ and

$\beta = p^h \mu$. Hence the representation $\xi = p^m \epsilon$ must be unique.

The p-value Function

There is an important function from R_p into R called p-value which is analogous to the absolute value function from R into R . A first step towards understanding this function is the definition of order.

Definition 2.22. Let ξ be a p-adic number. If ξ is non-zero, the order of ξ is the unique rational integer $v(\xi)$ such that $\xi = p^{v(\xi)} \epsilon$ with ϵ a unit. The order of 0, $v(0)$, is the number ∞ where ∞ is such that $x < \infty$ for each x in R , $\infty + \infty = \infty$, and $\infty + n = \infty$ for each integer n .

Three important properties of order of p-adic numbers are summarized in the following:

Theorem 2.23. If ξ and ζ are p-adic numbers, then

$$(2.11) \quad v(\xi\zeta) = v(\xi) + v(\zeta),$$

$$(2.12) \quad v(\xi + \zeta) \geq \min(v(\xi), v(\zeta)),$$

$$(2.13) \quad v(\xi + \zeta) = \min(v(\xi), v(\zeta)) \text{ if } v(\xi) \neq v(\zeta).$$

Proof: If either ξ or ζ is zero, all three properties follow immediately from the properties of ∞ . Otherwise

$$\xi\zeta = p^{v(\xi)} \epsilon p^{v(\zeta)} \eta = p^{v(\xi) + v(\zeta)} \mu$$

where ϵ , η , and μ are units. It follows that $v(\xi\zeta) = v(\xi) + v(\zeta)$. To complete the proof, consider

$$(2.14) \quad \xi + \zeta = p^{v(\xi+\zeta)} \hat{\epsilon} = p^{v(\xi)} \hat{\eta} + p^{v(\zeta)} \hat{\lambda} = p^k \hat{\mu}$$

where $\hat{\epsilon}$, $\hat{\eta}$, $\hat{\lambda}$, and $\hat{\mu}$ are units. If $k < \min(v(\xi), v(\zeta))$, then

$$p^{v(\xi) - k} \hat{\eta} + p^{v(\zeta) - k} \hat{\lambda} = \hat{\mu}$$

and p divides $\hat{\mu}$. Since this is not possible, it follows that

$k \geq \min(v(\xi), v(\zeta))$. But (2.14) also implies that $k \leq v(\xi + \zeta)$. There-

fore $v(\xi + \zeta) \geq k \geq \min(v(\xi), v(\zeta))$.

Condition (2.13) is proved by observing that $v(\xi + \zeta)$ greater than $\min(v(\xi), v(\zeta))$ is not possible whenever $v(\xi) \neq v(\zeta)$. From (2.14), it follows that

$$p^{v(\xi + \zeta) - v(\xi)} \hat{\epsilon} = \hat{\eta} + p^{v(\zeta) - v(\xi)} \hat{\lambda}.$$

If $v(\xi) \neq v(\zeta)$, then, without loss of generality, it can be assumed that $v(\xi) < v(\zeta)$ and hence that $v(\xi + \zeta) > v(\xi)$. Therefore $v(\xi + \zeta) - v(\xi)$ is greater than or equal to 1 and $v(\zeta) - v(\xi)$ is greater than or equal to 1 and it follows that p divides the unit $\hat{\eta}$. Since this is impossible, $v(\xi + \zeta) = \min(v(\xi), v(\zeta))$ whenever $v(\xi) \neq v(\zeta)$.

Division of one p -adic number by any non-zero p -adic number is always possible since $(R_p, +, \cdot)$ is a field. Division by any p -adic unit is always possible. However divisibility in $(O_p, +, \cdot)$ is limited. This limited divisibility can be expressed in terms of order.

Theorem 2.24. A p -adic integer α is divisible by the p -adic integer β if and only if $v(\beta) \leq v(\alpha)$.

Proof: If there exists γ in O_p such that $\alpha = \beta\gamma$, then $v(\alpha) = v(\beta) + v(\gamma)$. Since $v(\gamma) \geq 0$, it follows that $v(\beta) \leq v(\alpha)$. Conversely, if $v(\beta) \leq v(\alpha)$, then $\alpha = \beta p^{v(\alpha) - v(\beta)} \epsilon$ where ϵ is a unit. Hence β divides α .

Order can also be used to classify p -adic numbers as p -adic integers and units.

Theorem 2.25. A p -adic number ξ is an integer if and only if $v(\xi) \geq 0$.

Proof: The p -adic number $\xi = p^{v(\xi)} \epsilon$ with ϵ a unit is a p -adic integer if and only if $v(\xi) \geq 0$.

Theorem 2.26. A p-adic integer ξ is a unit if and only if $v(\alpha) = 0$.

Proof: If α^{-1} exists, then $\alpha\alpha^{-1} = 1$ and $v(\alpha) + v(\alpha^{-1}) = 0$. From the fact that $v(\alpha^{-1}) \geq 0$, it follows that $v(\alpha) = 0$. Conversely, $v(\alpha) = 0$ and $\alpha = p^{v(\alpha)}\epsilon$ with ϵ a unit implies that α is a unit.

With the concept of order of a p-adic number as a convenient first step, it is easy to define the p-value function.

Definition 2.27. The p-value function is the function $|\cdot|_p$ from R_p into the non-negative reals such that

$$\begin{aligned} |\xi|_p &= p^{-v(\xi)}, \text{ if } \xi \neq 0 \\ &= 0, \text{ if } \xi = 0. \end{aligned}$$

The real number $|\xi|_p$ is the p-value of the p-adic number ξ .

It follows immediately from Theorem 2.23 and Definition 2.27 that for each ξ and ζ in R_p

$$(2.15) \quad |\xi|_p \geq 0 \text{ with equality only if } \xi = 0,$$

$$(2.16) \quad |\xi\zeta|_p = |\xi|_p |\zeta|_p,$$

$$(2.17) \quad |\xi + \zeta|_p \leq \max(|\xi|_p, |\zeta|_p).$$

The inequality (2.17) is referred to as the non-archimedean property of $|\cdot|_p$. It follows from (2.17) that $|\cdot|_p$ satisfies the standard triangle inequality of $|\cdot|$. That is

$$(2.18) \quad |\xi + \zeta|_p \leq |\xi|_p + |\zeta|_p$$

for each ξ and ζ in R_p .

Two additional properties of $|\cdot|_p$ that follow immediately from (2.16) are that $|1|_p = |-1|_p = 1$ and that $|\xi^n|_p = |\xi|_p^n$. Also the last three theorems can be stated in terms of p-value.

Theorem 2.28. A p-adic integer α is divisible by the p-adic integer β if

and only if $|\alpha|_p \leq |\beta|_p$.

Theorem 2.29. A p-adic number ξ is an integer if and only if $|\xi|_p \leq 1$.

Theorem 2.30. A p-adic integer α is a unit if and only if $|\alpha|_p = 1$.

As $|\cdot|_p$ determines a metric on R , so $|\cdot|_p$ determines a metric on R_p .

Theorem 2.31. The function d_p from $R_p \times R_p$ into R defined by

$$d_p(\xi, \zeta) = |\xi - \zeta|_p \text{ is a metric on } R_p.$$

Proof: Since $|\xi - \zeta|_p \geq 0$ with equality only if $\xi - \zeta = 0$, $d_p(\xi, \zeta) \geq 0$ with equality only if $\xi = \zeta$. The fact that $d_p(\xi, \zeta) = d_p(\zeta, \xi)$ follows from $|\xi - \zeta|_p = |-(\zeta - \xi)|_p = |\zeta - \xi|_p$. Condition (1.9) follows from

$$(2.19) \quad \xi - \psi = \xi - \zeta + \zeta - \psi$$

and (2.18). Hence d_p is a metric on R_p .

The p-adic numbers with metric d_p is a metric space and is denoted by (R_p, d_p) . Since $|\cdot|_p$ satisfies (2.17) it follows from (2.18) that

$$(2.20) \quad d_p(\xi, \psi) \leq \max(d_p(\xi, \zeta), d_p(\zeta, \psi))$$

for each ξ, ζ , and ψ in R_p . Metric spaces with a metric that satisfies condition (2.20) are considered in Chapter IV.

Sequences of p-adic Numbers

Let $\{\xi_n\}$ be a sequence of p-adic numbers. Since (R_p, d_p) is a metric space, it follows from (1.15) that $\{\xi_n\}$ converges to ξ if and only if for each $\varepsilon > 0$ there exists an N such that

$$(2.21) \quad |\xi_n - \xi|_p < \varepsilon \text{ whenever } n \geq N.$$

The sequence $\{\xi_n\}$ is Cauchy if and only if for each $\varepsilon > 0$ there exists an N such that

$$(2.22) \quad |\xi_n - \xi_m|_p < \varepsilon \text{ whenever } n, m \geq N.$$

From the fact that $v(\xi_n - \xi) > M$ is equivalent to $|\xi_n - \xi|_p < p^{-M}$, it follows that $\xi_n \rightarrow \xi$ if and only if for each $M > 0$ there exists an N such that

$$(2.23) \quad v(\xi_n - \xi) > M \text{ whenever } n \geq N.$$

Furthermore, $\{\xi_n\}$ is Cauchy if and only if for each $M > 0$ there exists an N such that

$$(2.24) \quad v(\xi_n - \xi_m) > M \text{ whenever } m, n \geq N.$$

There is another Cauchy criterion that depends upon the non-archimedean nature of $|\cdot|_p$.

Theorem 2.32. A sequence $\{\xi_n\}$ of p -adic numbers is Cauchy if and only if for each $\varepsilon > 0$ there exists an N such that $|\xi_{n+1} - \xi_n|_p < \varepsilon$ whenever $n \geq N$.

Proof: If $\{\xi_n\}$ is Cauchy, then the conclusion follows from (2.22) with $m = n+1$. If for each $\varepsilon > 0$ there exists an N such that $|\xi_{n+1} - \xi_n|_p < \varepsilon$ whenever $n \geq N$, then

$$\begin{aligned} |\xi_m - \xi_n|_p &= \left| \sum_{i=n}^{m-1} (\xi_{i+1} - \xi_i) \right|_p \\ &\leq \max_{n \leq i \leq m-1} |\xi_{i+1} - \xi_i|_p \\ &< \varepsilon \end{aligned}$$

whenever m and n are greater than N . Hence $\{\xi_n\}$ is Cauchy.

The p -value function also provides a criterion for bounded sequences. A sequence $\{\xi_n\}$ of p -adic numbers is bounded above if the corresponding set of p -values is bounded above or equivalently, if the set of real numbers, $\{v(\xi_n)\}$, is bounded below.

Every Cauchy sequence of real numbers is bounded. The corresponding property holds true for p -adic numbers.

Theorem 2.33. Every Cauchy sequence $\{\xi_n\}$ of p-adic numbers is bounded.

Proof: Let $\varepsilon = 1$. Then since $\{\xi_n\}$ is Cauchy, there exists an N such that $n \geq N$ implies $|\xi_n - \xi_N|_p < 1$. For each $n \geq 0$,

$$|\xi_n|_p = |\xi_n - \xi_N + \xi_N|_p \leq \max(|\xi_n - \xi_N|_p, |\xi_N|_p)$$

implies that $|\xi_n|_p \leq \max(|\xi_N|_p, 1)$ whenever $n \geq N$. Let

$M = \max_{0 \leq k \leq N} (|\xi_k|_p, 1)$. Then $|\xi_n|_p \leq M$ for each $n \geq 0$ and $\{\xi_n\}$ is bounded.

As for the real numbers, so the following important property holds true for sequences of p-adic numbers.

Theorem 2.34. (3) From any bounded sequence of p-adic integers, it is possible to select a convergent subsequence.

Proof: The method of proof is to exhibit by mathematical induction a procedure for finding a convergent subsequence. If $\{\alpha_n\}$ is a sequence of p-adic integers, then it follows from Theorem 2.17 that the number of residue classes modulo p in 0_p is finite. Hence there are infinitely many terms of $\{\alpha_n\}$ which are convergent modulo p to some rational integer x_0 . All such terms yield a subsequence $\{\alpha_n^{(1)}\}$ of $\{\alpha_n\}$ such that

$$\alpha_n^{(1)} \equiv x_0 \pmod{p}$$

for some rational integer x_0 . Now since the number of residue classes modulo p^2 is also finite, there are infinitely many terms of $\{\alpha_n^{(1)}\}$, and hence a subsequence $\{\alpha_n^{(2)}\}$, such that for each n

$$\alpha_n^{(2)} \equiv x_1 \pmod{p^2}$$

for some rational integer x_1 with $x_1 \equiv x_0 \pmod{p}$. Suppose there exists $\{\alpha_n^{(k-1)}\}$, a subsequence of $\{\alpha_n\}$ such that

$$\alpha_n^{(k-1)} \equiv x_{k-1} \pmod{p^k}$$

for some rational number x_{k-1} . Then since the number of residue classes

of 0_p modulo p^{k+1} is finite, there is a subsequence $\{\alpha_n^{(k)}\}$ of $\{\alpha_n^{(k-1)}\}$ and hence of $\{\alpha_n\}$ such that

$$\alpha_n^{(k)} \equiv x_k \pmod{p^{k+1}}$$

for some rational number x_k . Also $\alpha_n^{(k)} \equiv x_k \pmod{p^{k+1}}$ and $\alpha_n^{(k)} \equiv x_{k-1} \pmod{p^k}$ implies that

$$x_k \equiv x_{k-1} \pmod{p^k}.$$

Hence by induction, for each $k \geq 1$ there is a subsequence $\{\alpha_n^{(k)}\}$ of $\{\alpha_n\}$ such that $\alpha_n^{(k)} \equiv x_{k-1} \pmod{p^k}$ where x_k is a rational integer and $x_k \equiv x_{k-1} \pmod{p^k}$. Thus the sequence $\{x_0, x_1, x_2, \dots, x_k, \dots\}$ determines some p -adic integer α . Consider the diagonal sequence $\{\alpha_n^{(n)}\}$. Obviously $\{\alpha_n^{(n)}\}$ is a subsequence of $\{\alpha_n\}$. Since $\alpha \equiv x_{n-1} \pmod{p^n}$ and since $\alpha_n^{(n)} \equiv x_{n-1} \pmod{p^n}$ it follows that $\alpha_n^{(n)} \equiv \alpha \pmod{p^n}$ and hence that $\alpha_n^{(n)} - \alpha$ is a multiple of p^n . Therefore $v(\alpha_n^{(n)} - \alpha) = n$, $v(\alpha_n^{(n)} - \alpha) \rightarrow \infty$, and $\{\alpha_n^{(n)}\}$ converges to α . Consequently every sequence of p -adic integers has a convergent subsequence.

Corollary 2.35. From any bounded sequence of p -adic numbers, it is possible to select a convergent subsequence.

Proof: Let $\{\xi_n\}$ be a bounded sequence. If $v(\xi_n) \geq 0$ for all n , then $\{\xi_n\}$ is a sequence of p -adic integers and there exists a convergent subsequence. In case there exists an n such that $v(\xi_n) < 0$, $\{\xi_n\}$ bounded implies there exists a positive rational integer k such that $v(\xi_n) \geq -k$ for each $n \geq 0$. Let $\{\alpha_n\} = \{\xi_n p^k\}$. Since $v(\xi_n p^k) = v(\xi_n) + k$ and $v(\xi_n) + k \geq 0$, it follows that $\{\alpha_n\}$ is a bounded sequence of p -adic integers. By Theorem 2.34, it is possible to select a convergent subsequence $\{\alpha_{n_i}\}$ from $\{\alpha_n\}$. Then $\{\xi_{n_i}\} = \{\alpha_{n_i} p^{-k}\}$ is a convergent subsequence of $\{\xi_n\}$.

Cauchy sequences of rational numbers do not always converge with respect to the $|\cdot|$ -topology to a rational number. For instance, the standard algorithm for approximating the square root of 2 yields a Cauchy sequence of rational numbers that converges to the irrational number $\sqrt{2}$. However every Cauchy sequence of real numbers converges with respect to the $|\cdot|$ -topology to a real number. The same is true for Cauchy sequences of (\mathbb{R}_p, d_p) .

Theorem 2.36. Let $\{\xi_n\}$ be a sequence of p-adic numbers. Then $\{\xi_n\}$ converges to a p-adic number ξ if and only if $\{\xi_n\}$ is Cauchy.

Proof: Assume that $\{\xi_n\}$ converges to ξ . Then for each $\varepsilon > 0$ there exist N_1 and N_2 such that $|\xi_n - \xi|_p < \varepsilon$ whenever $n \geq N_1$ and $|\xi_m - \xi|_p < \varepsilon$ whenever $m \geq N_2$. If $m, n \geq N = \max(N_1, N_2)$, then

$$\begin{aligned} |\xi_n - \xi_m|_p &= |\xi_n - \xi + \xi - \xi_m|_p \\ &\leq \max(|\xi_n - \xi|_p, |\xi_m - \xi|_p) \\ &< \varepsilon \end{aligned}$$

and $\{\xi_n\}$ is Cauchy. Conversely, if $\{\xi_n\}$ is Cauchy, then $\{\xi_n\}$ is bounded and hence contains a subsequence $\{\xi_{n_i}\}$ which converges to ξ , a p-adic number. But $\{\xi_{n_i}\}$ a subsequence of $\{\xi_n\}$ implies that $n_i > n$ and hence that

$$\begin{aligned} |\xi_n - \xi|_p &= |\xi_n - \xi_{n_i} + \xi_{n_i} - \xi|_p \\ &\leq \max(|\xi_n - \xi_{n_i}|_p, |\xi_{n_i} - \xi|_p) \\ &< \varepsilon \end{aligned}$$

whenever $n \geq N$. Therefore $\{\xi_n\}$ converges to ξ .

Corollary 2.37. The field $(\mathbb{R}_p, +, \cdot)$ with the d_p metric is complete.

Since the only Cauchy sequences of rational integers are the con-

stant sequences, every Cauchy sequence of these integers converges to a rational integer with respect to the $|\cdot|$ -topology. Hence (Z, d) is a complete metric space. There are non-constant Cauchy sequences of p -adic integers. For instance, let $\{\epsilon_n\}$ be a sequence of p -adic units. Then $\{\epsilon_0, \epsilon_1 p, \epsilon_2 p^2, \dots, \epsilon_n p^n, \dots\}$ is a non-constant Cauchy sequence that converges with respect to d_p to 0. However $(0_p, d_p)$ is a complete metric space.

Theorem 2.38. The metric space $(0_p, d_p)$ is complete.

Proof: If $\{\alpha_n\}$ is a sequence of 0_p such that $\alpha_n \rightarrow \xi$, then for each $\epsilon > 0$ there exists an N such that $|\alpha_n - \xi|_p < \epsilon$ whenever $n \geq N$. Since $|\xi + \alpha_n|_p \leq |\xi|_p + |\alpha_n|_p$, it follows that

$$||\xi|_p - |\alpha_n|_p| \leq |\xi - \alpha_n|_p$$

for each $n \geq 0$. Therefore for each ϵ there exists an N such that

$$|\xi|_p < |\alpha_n|_p + \epsilon$$

whenever $n \geq N$. From Theorem 2.29, it follows that for each $\epsilon > 0$

$$|\xi|_p < 1 + \epsilon.$$

That is, $|\xi|_p \leq 1$ and ξ is a p -adic integer. Thus $(0_p, d_p)$ is a complete metric space.

Infinite Series Representation of p -adic Numbers

Since $(R_p, +, \cdot)$ has a metric structure, it is possible to consider convergence of infinite series. Let $\{x_n\}$ be a sequence of real numbers. The infinite series $\sum_{n=0}^{\infty} x_n$ converges to a real number only if $\{x_n\}$ converges to 0. More is true for infinite series of p -adic numbers.

Theorem 2.39. If $\{\xi_n\}$ is a sequence of p -adic numbers, then $\sum_{n=0}^{\infty} \xi_n$

converges to a p-adic number ℓ if and only if $\{\xi_n\}$ converges to 0.

Proof: If $\sum_{k=0}^n \xi_k \rightarrow \ell$, then $\{\sum_{k=0}^n \xi_k\}$ is Cauchy and for each $\varepsilon > 0$ there exists an N such that $n \geq N$ implies that

$$|\sum_{k=0}^{n+1} \xi_k - \sum_{k=0}^n \xi_k|_p < \varepsilon.$$

Since

$$|\xi_{n+1}|_p = |\sum_{k=0}^{n+1} \xi_k - \sum_{k=0}^n \xi_k|_p$$

for each $n \geq 0$, it follows that

$$|\xi_{n+1} - 0|_p < \varepsilon \text{ whenever } n \geq N.$$

Hence $\xi_n \rightarrow 0$. Conversely, if $\xi_n \rightarrow 0$, then for each $\varepsilon > 0$ there exists an N such that $n \geq N$ implies that

$$|\xi_{n+1} - 0|_p < \varepsilon.$$

From

$$|\xi_{n+1}|_p = |\sum_{k=0}^{n+1} \xi_k - \sum_{k=0}^n \xi_k|_p$$

for each $n \geq 0$, it follows that

$$|\sum_{k=0}^{n+1} \xi_k - \sum_{k=0}^n \xi_k|_p < \varepsilon \text{ whenever } n \geq N.$$

Hence $\{\sum_{k=0}^n \xi_k\}$ is Cauchy and every Cauchy sequence of p-adic numbers converges to a p-adic number. Thus

$$\sum_{k=0}^n \xi_k \rightarrow \sum_{k=0}^{\infty} \xi_k = \ell.$$

A p-adic integer α is determined by a sequence $\{x_n\}$ of rational integers. Since each rational integer is a p-adic integer, a sequence of rational integers is also a sequence of p-adic integers and has the potential for converging to a p-adic integer. The following key result gives additional insight into the structure of the p-adic integers.

Theorem 2.40. If the p-adic integer α is determined by the sequence

$\{\sum_{k=0}^n a_k p^k\}$ of rational integers, then $\{a_k p^k\}$ considered as a

sequence of p-adic integers converges to α . That is, $\alpha = \sum_{k=0}^{\infty} a_k p^k$.

Proof: Let $x_n = \sum_{k=0}^n a_k p^k$ and consider $\alpha - x_n$ where x_n is the p-adic integer determined by $\{x_n, x_n, \dots, x_n, \dots\}$. Then

$$\alpha - x_n \leftrightarrow \{x_0 - x_n, x_1 - x_n, \dots, 0, x_{n+1} - x_n, \dots\}.$$

Since

$$x_m - x_n \equiv 0 \pmod{p^{m+1}}$$

for $0 \leq m \leq n$, it follows from Corollary 2.14 that $\alpha - x_n$ is divisible by p^{n+1} . Therefore $v(\alpha - x_n) \geq n+1$ and $v(\alpha - x_n) \rightarrow \infty$. From (2.23) and the definition of x_n , it is clear that $\{\sum_{k=0}^n a_k p^k\}$ converges to α and hence that $\alpha = \sum_{k=0}^{\infty} a_k p^k$.

In Example 2.12, it was observed that

$$2/3 \leftrightarrow \{4 + \sum_{k=1}^n (2+(-1)^k)5^k\}.$$

Therefore $\{4 + \sum_{k=1}^n (2+(-1)^k)5^k\}$ converges to $2/3$ and

$$(2.25) \quad 2/3 = 4 + 1 \cdot 5 + 3 \cdot 5^2 + 1 \cdot 5^3 + 3 \cdot 5^4 + \dots$$

Every real number is the limit of a sequence of rational numbers.

The same is true of every p-adic number.

Theorem 2.41. Every p-adic number is the limit of a sequence of rational numbers.

Proof: Let $\xi = \alpha/\beta$ be a p-adic number. Since β is a p-adic integer, there exists a rational integer $k \geq 0$ and a p-adic unit ϵ such that $\beta = p^k \epsilon$. Therefore $\xi = \gamma/p^k$ where $\gamma = \alpha \epsilon^{-1}$ is a p-adic integer determined by $\{x_n\}$, a sequence of rational integers. Also

$$v(x_n/p^k - \xi) = v(x_n/p^k - \gamma/p^k) = v(x_n - \gamma) - k.$$

But $v(x_n - \gamma) \rightarrow \infty$. Therefore $v(x_n/p^k - \xi) \rightarrow \infty$ and $\{x_n/p^k\}$ is a sequence of rational numbers that converges to ξ .

Hence Q is a dense subset of R_p with respect to the $|\cdot|_p$ -topology.

From Corollary 2.37, it follows that $(R_p, +, \cdot)$ is a completion of $(Q, +, \cdot)$ relative to the $|\cdot|_p$ -topology.

Every real number has an infinite series representation. Again the same is true for p -adic numbers.

Theorem 2.42. Every p -adic number has an infinite series representation of the form $\sum_{k=0}^{\infty} a_k p^{m+k}$ where m is an integer, and $0 \leq a_k < p$ for $k \geq 0$.

Proof: Let ξ be a p -adic number. If $\xi = 0$, then, from

$0 \leftrightarrow \{0, 0, \dots\} = \{\sum_{k=0}^n 0p^k\}$, it follows that $0 = \sum_{k=0}^{\infty} a_k p^k$. If $\xi \neq 0$,

then there exists an integer m and a unit ϵ such that $\xi = p^m \epsilon$. Since

$\epsilon \leftrightarrow \{\sum_{k=0}^n a_k p^k\}$ with $a_0 \neq 0$ and $0 \leq a_k < p$, $\epsilon = \sum_{k=0}^{\infty} a_k p^k$ and

$$\xi = \sum_{k=0}^{\infty} a_k p^{m+k}.$$

Every rational number is a p -adic number as well as a real number and consequently has both a p -adic series representation

$$a_0 + a_1 p + a_2 p^2 + \dots + a_n p^n + \dots$$

with $0 \leq a_i < p$ for each $n \geq 0$ and a decimal series representation

$$b_0 + b_1 10^{-1} + b_2 10^{-2} + \dots + b_n 10^{-n} + \dots$$

with $0 \leq b_i < 10$ for each $n \geq 0$. Before proceeding to a detailed consideration of relationships between the real and p -adic number fields, some properties common to the respective representatives are explored.

A rational number r/s with r and s relatively prime has a finite decimal expansion if and only if 2 and 5 are the only prime factors of s . The analog for p -adic series representation is that a positive rational number r/s with r and s relatively prime has a finite p -adic series expansion if and only if s is a power of p . If r/s has a finite p -adic expansion, then

$$r/s = p^m(a_0 + a_1p + \dots + a_np^n)$$

with $0 < a_0 < p$, m a negative integer, and $v(a_0 + a_1p + \dots + a_np^n) = 0$.

Therefore r a rational integer implies that $v(r) = v(s) + m = 0$, that

$v(s) = -m$, and hence that $s = p^{-m}\mu$. Since s is a positive rational integer, $\mu = 1$ and s is a power of p . Conversely, if $s = p^k$, then

from $r/s = p^m\varepsilon$ it follows that $r = p^{k+m}\varepsilon$. Hence $k + m = 0$ since

$v(r) = 0$. If $r < p$, then $r/s = r/p^k = p^{-k}r$. Otherwise $r > p$,

$r = \sum_{i=0}^n a_i p^i$, and $r/s = \sum_{i=0}^n a_i p^{i-k}$. Either way, r/s has a finite p -adic expansion.

A decimal series expansion is finite or periodic if and only if it represents a rational number. The corresponding property for p -adic series representation is the following theorem:

Theorem 2.43. (9) A p -adic number has a finite or periodic series expansion if and only if the number is a rational number.

Proof: It will be sufficiently general to consider

$$(2.25) \quad \alpha = A + p^k B + p^{k+m} B + p^{k+2m} B + \dots$$

where

$$A = a_0 + a_1 p + a_2 p^2 + \dots + a_{k-1} p^{k-1}$$

with $0 \leq a_i < p$ and

$$B = b_0 + b_1 p + b_2 p^2 + \dots + b_{m-1} p^{m-1}$$

with $0 \leq b_i < p$. Then

$$\begin{aligned} \alpha - A &= p^k B + p^m (p^k B + p^{k+m} B + \dots) \\ &= p^k B + p^m (\alpha - A). \end{aligned}$$

Hence

$$\begin{aligned} \alpha(1 - p^m) &= A(1 - p^m) + p^k B, \\ \alpha &= A + p^k B / (1 - p^m), \end{aligned}$$

and α is a rational number.

The converse is proved in several parts. Suppose first that $\alpha = r/s$ is a negative irreducible proper rational number with $s > 0$ and s and p relatively prime. From Euler's Theorem, it follows that there exists an integer and hence a smallest integer m such that $p^m \equiv 1 \pmod{s}$. Let $1 - p^m = zs$ with z an integer. It follows that $z < 0$, $zr < 0$, and $\alpha = r/s = zr/(1 - p^m)$. Since α is proper, $zr < p^m - 1 < p^m$ and

$$zr = B = b_0 + b_1p + \dots + b_{m-1}p^{m-1}$$

with $0 \leq b_i < p$ whenever $0 \leq i \leq m-1$. Then

$$(2.26) \quad \alpha = B + Bp^m + Bp^{2m} + \dots$$

since $1/(1 - p^m) = 1 + p^m + p^{2m} + \dots$. Hence α has a periodic series expansion.

In the second case, assume α is a positive irreducible rational number, then $\alpha = N + q/s$ where N is a rational integer and q/s is a negative irreducible proper rational number with $s > 0$. Hence

$$N = a_0 + a_1p + \dots + a_{k-1}p^{k-1} \text{ with } 0 \leq a_i < p \text{ whenever } 0 \leq i \leq k-1,$$

Furthermore q/s has a periodic p -adic expansion of the form (2.26).

Thus α has a periodic p -adic series representation of the form (2.25).

To complete the proof, assume that α is a negative irreducible rational number. Then $-\alpha$ is a positive irreducible rational number and hence has a p -adic series representation of the form (2.25). Since

$$\begin{aligned} 0 &= p + (p-1)p + \dots + (p-1)p^n + \dots, \\ -\alpha &= 0 - \alpha \\ &= A' + p^k B' + p^{k+m} B' + p^{k+2m} B' + \dots \end{aligned}$$

where

$$A' = a_0 + (a_1 - 1)p + (a_2 - p+1)p^2 + \dots + (a_{k-1} - p+1)p^{k-1}$$

with $0 \leq a_i < p$ whenever $0 \leq i \leq k-1$ and

$$B^* = (b_0 - p+1) + (b_1 - p+1)p + \dots + (b_{m-1} - p+1)p^{m-1}$$

with $0 \leq b_i < p$ whenever $0 \leq i \leq m-1$. Hence $-\alpha$ has a periodic p -adic representation.

A Geometric Model for R_p

The p -adic numbers can be placed in a one-to-one correspondence with a subset of the Euclidean plane in many ways. The objective of this section is to establish such a correspondence, and hence a geometric model for R_p , that reflects several of the characteristic properties of the p -adic numbers. From the fact that every p -adic number is uniquely expressed by $p^m \epsilon$ where ϵ is a unit and m is a rational integer, it follows that it is sufficient to establish a one-to-one correspondence between the p -adic units and a subset of the unit circle. Therefore it is adequate to establish a one-to-one correspondence between the p -adic units and a subset of the half open interval $[0,1)$ since the association of a real number θ , $0 \leq \theta < 1$, with the point on the unit circle whose polar coordinates are 1 and $2\pi\theta$ is a one-to-one correspondence.

Every real number in $[0,1)$ has a base $p+1$ expansion

$$\frac{a_0}{p+1} + \frac{a_1}{(p+1)^2} + \frac{a_2}{(p+1)^3} + \dots + \frac{a_n}{(p+1)^{n+1}} + \dots$$

where $0 \leq a_n \leq p$ for each n . Let G be the set of all such expansions with $a_0 \neq 0$ and $a_n \neq p$ for each n . The set of points, also denoted by G , corresponding to the set G has an interesting geometric derivation. Divide the half open interval $[1,0)$ into $p+1$ half open intervals of length $1/(p+1)$ and order the resulting intervals by increasing

initial points. Let E_0^1 denote the union of the first and last sub-intervals. That is

$$E_0^1 = [0, \frac{1}{p+1}) \cup [\frac{p}{p+1}, 1).$$

The set $[1/(p+1), p/(p+1))$, the points of $[0, 1)$ which are not in E_0^1 , is the union of $p-1$ of the original $p+1$ half open intervals. Divide each of these remaining intervals into $p+1$ half open subintervals of equal length and let E_1^k denote the half open $(p+1)$ th subinterval of the $(k+1)$ th original interval. That is,

$$E_1^k = [\frac{kp + k-1}{(p+1)^2}, \frac{k}{p+1})$$

with $1 \leq k \leq p-1$. The sets $E_1^1, E_1^2, \dots, E_1^{p-1}$, are indicated in Figure 1 for $p = 5$.

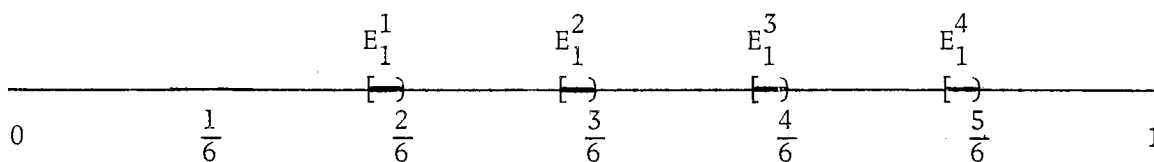


Figure 1. E_1^k with $1 \leq k \leq 4$.

The set of points of $[0, 1)$ which are not in E_0^1 or some E_1^k is the union of $p(p-1)$ half open subintervals of equal length. Divide each of these remaining intervals into $p+1$ subintervals of equal length and let E_2^k , $1 \leq k \leq p(p-1)$, denote the half open $(p+1)$ th subinterval of the $(k+1)$ th one of the remaining $p(p-1)$ intervals. The set

$$[0, 1) - E_0^1 - \bigcup_{k=1}^{p-1} E_1^k - \bigcup_{k=1}^{p(p-1)} E_2^k$$

is the union of $p^2(p-1)$ half open intervals of equal length. It is clear that this procedure can be continued indefinitely. Furthermore

$$G = [0,1) - E_0^1 - \bigcup_{n=1}^{\infty} p^{n-1} \bigcup_{k=1}^{(p-1)} E_n^k.$$

Since for each p -adic unit there is a unique sequence $\{a_n\}$ of rational integers with $a_0 \neq 0$ and $0 \leq a_n < p$ for each n , it is clear that there is a one-to-one correspondence between the p -adic units and the points of the plane with polar coordinates 1 and $2\pi\theta$ where

$$(2.27) \quad \theta = \sum_{k=1}^{\infty} \frac{a_k}{(p+1)^k}$$

is an element of G . If $\varepsilon = \sum_{k=0}^{\infty} a_k p^k$ is a p -adic unit which is also a rational integer, then $\sum_{k=0}^{\infty} a_k p^k$ terminates, θ can be calculated, and the point $(1, 2\pi\theta)$ is easily determined. The location of each rational integer less than 25 which is a 5-adic unit is indicated in Figure 2. The images of the sets E_0^1 , $1 \leq k \leq 4$, are also indicated.

Rational numbers of the form yz^{-1} with y and z in Z , $y \not\equiv 0 \pmod{p}$, and $z \not\equiv 0 \pmod{p}$ are p -adic units which are not rational integers. The p -adic expansion of yz^{-1} , $\sum_{k=0}^{\infty} a_k p^k$, does not terminate since z is not a power of p . Hence yz^{-1} can not be located on the unit circle by a finite process. However its position can be approximated to any degree of accuracy since if $\theta_n = \sum_{k=0}^n a_k p^k$, then $2\pi\theta_n \rightarrow 2\pi\theta$ as $\sum_{k=0}^n a_k p^k \rightarrow yz^{-1}$. For instance, 4, 9, 84, and 209 are the first four terms of the canonical sequence that determines $2/3$ as a 5-adic unit. Therefore

$$\frac{6\pi}{5}, \frac{38\pi}{30}, \frac{234\pi}{180}, \frac{1410\pi}{1080},$$

are the first four terms of $\{2\pi\theta_n\}$. Furthermore

$$2\pi\theta - \frac{1410\pi}{1080} < \frac{\pi}{540}.$$

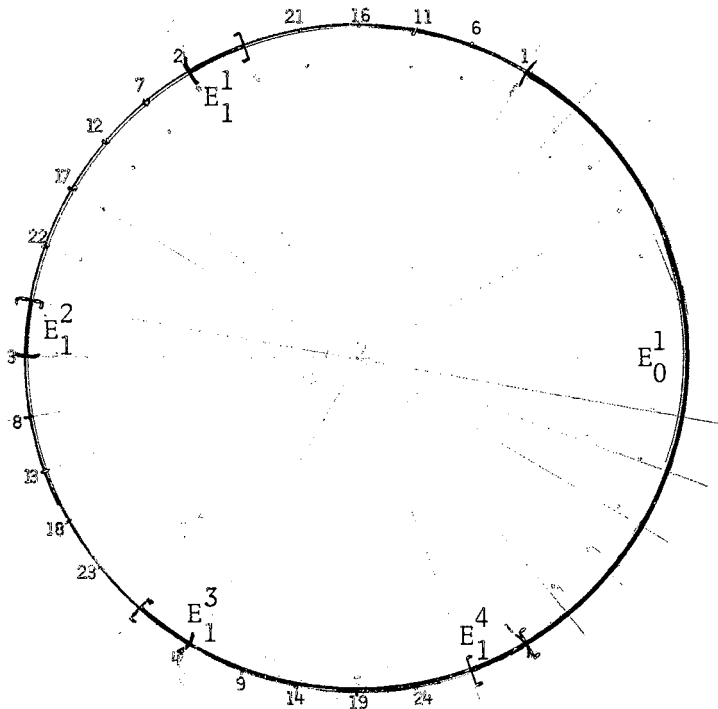


Figure 2. Rational Integers Less Than 25 Which Are 5-adic Units.

Once the units of $(\mathbb{R}_p, +, \cdot)$ are properly associated with a subset of the unit circle, a one-to-one correspondence between the non-zero p -adic numbers and a subset of the plane can be determined. Let ξ be a non-zero p -adic number. Then $\xi = p^m \varepsilon$ where ε is a unit. If ε corresponds to the point $(1, 2\pi\theta)$, then the association of ξ with $(|\xi|_p, 2\pi\theta)$ is a one-to-one correspondence between the non-zero p -adic numbers and a subset of the plane that extends the association of the units with a subset of the unit circle. Thus the geometric model for the non-zero p -adic numbers is a subset of the collection of concentric circles with radius p^{-m} , m in \mathbb{Z} . Since $|0|_p = 0$ and $p^m \rightarrow 0$ with respect to the metric induced by p -value, it is natural to associate the p -adic zero

with the center of the concentric circles.

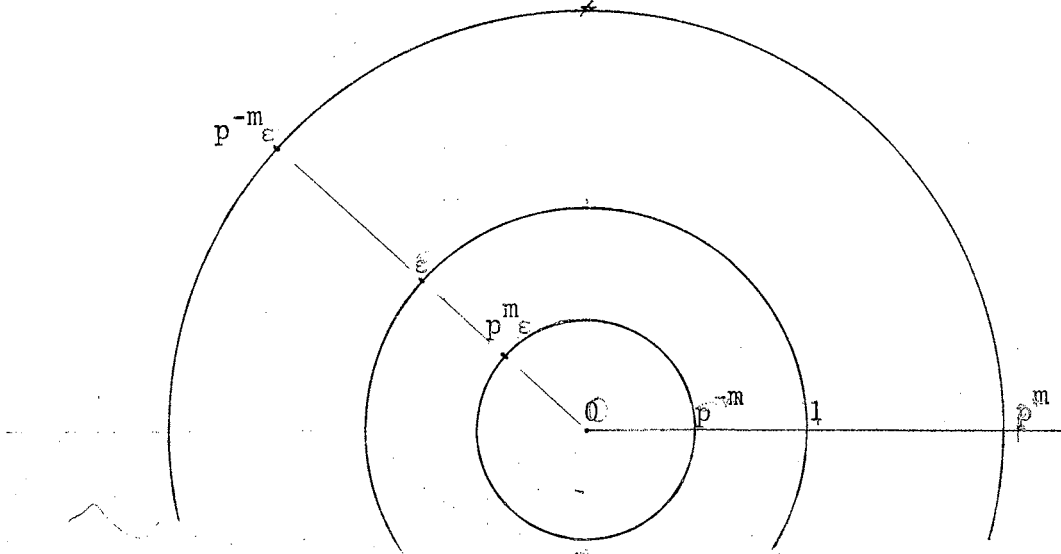


Figure 3. The Relationship Between $p^m \epsilon$, $p^{-m} \epsilon$, and ϵ for ϵ a Unit and $m \geq 0$.

If ξ and ζ are on circles of radius p^m and p^n respectively, then $|\xi - \zeta|_p = \max(1/p^m, 1/p^n)$. Consequently a sequence $\{\xi_n\}$ converges to a non-zero p -adic number ξ only if $\{\xi_n\}$ is eventually on the circle which contains ξ . Since $p^n \rightarrow 0$ with respect to $|\cdot|_p$, the condition $\xi \neq 0$ is necessary. From the fact that all points on any circle have the same p -value, it follows that the sequence of p -values of a non-null Cauchy sequence of p -adic numbers is eventually constant. This important characteristic of the p -adic numbers is a consequence of the non-archimedean nature of $|\cdot|_p$.

Theorem 2.44. Let $\{\xi_n\}$ be a non-null Cauchy Sequence of p -adic numbers.

The sequence $\{|\xi_n|_p\}$ of real numbers is eventually constant.

Proof: Let $\{\xi_n\}$ be a non-null Cauchy sequence of p-adic numbers. Since (R_p, d_p) is complete, there exists a p-adic number ξ such that $\xi_n \rightarrow \xi$.

Therefore there exists an N such that $v(\xi_n - \xi) > v(\xi)$ whenever $n \geq N$.

Hence

$$v(\xi_n - \xi + \xi) = \min(v(\xi_n - \xi), v(\xi)) = v(\xi)$$

and $|\xi_n|_p = |\xi|_p$ whenever $n \geq N$.

Theorem 2.44 has an interesting corollary which states that the images of Q and R_p under $|\cdot|_p$ are identical.

Corollary 2.45. Let $|Q|_p = \{|x|_p : x \text{ is a rational number}\}$ and let

$|R_p|_p = \{|\xi|_p : \xi \text{ is a p-adic number}\}$. Then $|Q|_p = |R_p|_p$.

Proof: Let ξ be a p-adic number. If $\xi = 0$, then $|\xi|_p = 0$ and $|\xi|_p$ is an element of $|Q|_p$. If $\xi \neq 0$, then there exists a non-null Cauchy sequence $\{x_n\}$ of rational numbers such that $x_n \rightarrow \xi$ with respect to $|\cdot|_p$. Hence $|x_n|_p \rightarrow |\xi|_p$ with respect to $|\cdot|$. Furthermore there exists an N such that $|x_n|_p = |x_n|_p$ whenever $n \geq N$. Therefore $|x_N|_p = |\xi|_p$ and $|R_p|_p$ is a subset of $|Q|_p$. Set inclusion the other way is obvious since every rational number is a p-adic number.

Every concentric circle of the geometric model for R_p contains a rational number and every rational number is on some circle. Since a p-adic number ξ is on a circle of radius p^m if and only if $|\xi|_p = p^{-m}$, the geometric model is consistent with Corollary 2.45. Furthermore

$$|R_p|_p = \{\dots, p^{-2}, p^{-1}, 1, p, p^2, \dots\}.$$

CHAPTER III

COMPLETIONS OF THE RATIONAL NUMBER FIELD

Although the real field and the p -adic number fields are not isomorphic, they share many common properties. Some similarities are illustrated by the following pairs of statements:

(3.1) COMPLETENESS

Every Cauchy sequence of p -adic (real) numbers converges to a p -adic (real) number.

(3.2) DENSENESS OF \mathbb{Q}

Each p -adic (real) number is the limit of some sequence of rational numbers.

(3.3) SERIES REPRESENTATION

A p -adic (real) number has a finite or periodic series expansion if and only if the number is rational.

It is the purpose of this chapter to explore in detail the relationship between the real and p -adic number fields. The chapter concludes with the proof that the real and p -adic number fields are mathematically distinct.

Valuations

To provide a setting in which to discuss the relationship between the real and p -adic number systems, it is helpful to consider a function

from a general field into the non-negative real numbers that corresponds to absolute value on \mathbb{R} and p-value on \mathbb{R}_p .

Definition 3.1. A valuation is a function ϕ from $(F, +, \cdot)$ into the non-negative real numbers such that

$$(3.4) \quad \phi(a) \geq 0 \text{ with equality only if } a = 0,$$

$$(3.5) \quad \phi(ab) = \phi(a) \cdot \phi(b),$$

$$(3.6) \quad \phi(a + b) \leq \phi(a) + \phi(b).$$

It is clear that $| \cdot |$ and $| \cdot |_p$ are valuations on the real and p-adic number fields respectively. Both $| \cdot |$ and $| \cdot |_p$ are also valuations on the rational number field.

As one further example of a valuation on the rational number field $(\mathbb{Q}, +, \cdot)$ consider ψ from \mathbb{Q} into \mathbb{R} such that for each a in \mathbb{Q} , $\psi(a) = 1$ if $a \neq 0$ and $\psi(0) = 0$. It is clear that ψ is a valuation.

Definition 3.2. The trivial valuation on a field $(F, +, \cdot)$ is the valuation ϕ on $(F, +, \cdot)$ such that for each a in F ,

$$\begin{aligned} \phi(a) &= 1, \text{ if } a \neq 0 \\ &= 0, \text{ if } a = 0. \end{aligned}$$

Some important properties of valuations in general are summarized in the next theorem. These are familiar properties of the absolute value valuation and were established for p-value in Chapter II.

Theorem 3.3. If ϕ is a valuation on $(F, +, \cdot)$, then

$$(3.7) \quad \phi(1) = 1,$$

$$(3.8) \quad \phi(-a) = \phi(a),$$

$$(3.9) \quad \phi(a^{-1}) = (\phi(a))^{-1},$$

$$(3.10) \quad |\phi(a) - \phi(b)| \leq \phi(a - b)$$

where a and b are in F and 1 represents the unity of $(F, +, \cdot)$ as well as the unity of $(R, +, \cdot)$.

Proof: Since $1 \cdot a = a$ for each a in F , it follows that

$$\phi(a) = \phi(1 \cdot a) = \phi(1)\phi(a),$$

Therefore $\phi(1) = 1$. Since $\phi(-1) \geq 0$, and since

$$\phi(-1)\phi(-1) = \phi((-1)^2) = \phi(1) = 1,$$

it follows that $\phi(-1) = 1$. Hence

$$\phi(-a) = \phi(-1 \cdot a) = \phi(-1)\phi(a) = \phi(a).$$

Condition (3.9) follows from $aa^{-1} = 1$ and property (3.5). To complete the proof, note that property (3.6) implies that

$$(3.11) \quad \phi(a) - \phi(b) \leq \phi(a - b)$$

and

$$(3.12) \quad \phi(b) - \phi(a) \leq \phi(b - a).$$

From (3.8), (3.11), and (3.12), it follows that

$$-\phi(a - b) \leq \phi(a) - \phi(b) \leq \phi(a - b)$$

and consequently that $|\phi(a) - \phi(b)| \leq \phi(a - b)$.

Non-Archimedean Valuations

It has been observed that $|\cdot|_p$ is a valuation on $(Q, +, \cdot)$. From (2.14) it is clear that $|\cdot|_p$ satisfies the additional condition

$$(3.13) \quad \phi(a + b) \leq \max(\phi(a), \phi(b)).$$

Since $\max(\phi(a), \phi(b)) \leq \phi(a) + \phi(b)$, any valuation that satisfies (3.13) also satisfies (3.6).

Definition 3.4. A valuation that satisfies condition (3.13) in addition to (3.6) is a non-archimedean valuation. If a valuation fails to satisfy (3.13), then it is Archimedean.

Formula (3.10) provides an important interplay between absolute value and a valuation. The refinement of (3.10) for non-archimedean valuations takes the following form:

Theorem 3.5. If ϕ is a non-archimedean valuation on F and if $\phi(a) > \phi(b)$, then $\phi(a + b) = \phi(a)$.

Proof: Let ϕ be non-archimedean and assume $\phi(a) > \phi(b)$. Then $\phi(a) = \phi(a + b - b) \leq \max(\phi(a + b), \phi(b))$. If $\phi(a + b) < \phi(b)$, then $\max(\phi(a + b), \phi(b)) = \phi(b)$ and hence $\phi(a) \leq \phi(b)$. This contradicts the assumption that $\phi(a) > \phi(b)$. Therefore $\phi(a + b) \geq \phi(b)$ and $\max(\phi(a + b), \phi(b)) = \phi(a + b)$. It follows that

$$\phi(a) \leq \phi(a + b) \leq \max(\phi(a), \phi(b)) = \phi(a)$$

and hence that $\phi(a + b) = \phi(a)$.

One useful alternate characterization of a non-archimedean valuation is given in the following theorem:

Theorem 3.6. A valuation ϕ on a field $(F, +, \cdot)$ is non-archimedean if and only if for each x in F

$$(3.14) \quad \phi(x) \leq 1 \text{ implies } \phi(1 + x) \leq 1.$$

Proof: If ϕ is non-archimedean, then $\phi(1 + x) \leq \max(\phi(x), 1)$. Since $\phi(1) = 1$, $\phi(x) \leq 1$ implies that $\phi(1 + x) \leq 1$. Conversely, assume that (3.14) is true and that ϕ is a valuation on $(F, +, \cdot)$. It is necessary to prove that $\phi(x + y) \leq \max(\phi(x), \phi(y))$ for every x and y in F . This is trivially the case if either x or y is zero. Suppose that both x and y are non-zero elements of F . Without loss of generality, it is possible to assume that $\phi(x) \leq \phi(y)$. Then $\phi(x/y) \leq 1$. It follows that $\phi(1 + x/y) \leq 1$. That is, $\phi(\frac{x + y}{y}) \leq 1$. Therefore $\phi(x + y) \leq \phi(y)$. Since $\phi(y) = \max(\phi(x), \phi(y))$, $\phi(x + y) \leq \max(\phi(x), \phi(y))$ for every x

and y in F .

Corollary 3.7. A valuation ϕ on the rational numbers is non-archimedean if and only if $\phi(n) \leq 1$ for each n in Z .

Proof: If ϕ is non-archimedean and n is a non-zero element of Z , then $\phi(n) = \phi(1 + 1 + \dots + 1) \leq \max(\phi(1), \phi(1), \dots, \phi(1)) = \phi(1) = 1$. Since $\phi(-n) = \phi(n)$, $\phi(n) \leq 1$ for each n in Z . Conversely, assume $\phi(n) \leq 1$ for each n in Z . To show that ϕ is non-archimedean, it is sufficient to show that $\phi(x) \leq 1$ implies $\phi(x + 1) \leq 1$ for each rational number x . From the Binomial Theorem, it follows that

$$\begin{aligned} (\phi(1 + x))^n &= \phi((1 + x)^n) = \phi\left(\sum_{k=0}^n \binom{n}{k} x^k\right) \\ &\leq \sum_{k=0}^n \phi\left(\binom{n}{k} \phi(x^k)\right). \end{aligned}$$

for each $n \geq 0$. If $\phi(x) \leq 1$, then $\phi(1 + x) \leq (n + 1)^{\frac{1}{n}}$. Therefore $\phi(1 + x) \leq \lim(n + 1)^{\frac{1}{n}} = 1$ and ϕ is a non-archimedean valuation.

It is clear from a re-examination of the proof of Theorem 2.31 that if ϕ is a valuation on a field $(F, +, \cdot)$, then a function d from $F \times F$ into R such that

$$(3.15) \quad d(x, y) = \phi(x - y)$$

for each x and y in F is a metric on F . Thus (F, d) is a metric space. It follows that ϕ determines both a convergence and a Cauchy criteria for sequences of elements from F . If $\{x_n\}$ is a sequence of F , then $\{x_n\}$ converges to x if and only if for each $\epsilon > 0$ there exists an N such that

$$(3.16) \quad \phi(x_n - x) < \epsilon \text{ whenever } n \geq N$$

and $\{x_n\}$ is Cauchy if and only if for each $\epsilon > 0$ there exists an N such that

$$(3.17) \quad \phi(x_m - x_n) < \varepsilon \text{ whenever } m, n \geq N.$$

If ψ is another valuation on $(F, +, \cdot)$, then ψ also determines both a convergence and a Cauchy criteria. There is no reason to assume that the two valuations, ϕ and ψ , determine the same or even related criteria. A sequence which satisfies (3.16) is said to converge with respect to ϕ . The convergence of $\{x_n\}$ to x with respect to ϕ is denoted by $x_n \rightarrow x$ (wrt ϕ). A sequence $\{x_n\}$ satisfies (3.16) if and only if there exists an x in F such that $\{\phi(x_n - x)\}$ is a sequence of real numbers that converges to 0. Therefore $x_n \rightarrow x$ (wrt ϕ) if and only if $\phi(x_n - x) \rightarrow 0$ (wrt $|\cdot|$).

Definition 3.8. Two valuations ϕ and ψ determine the same convergence criteria if for each sequence $\{x_n\}$ there exists an x such that

$$(3.18) \quad \phi(x_n - x) \rightarrow 0 \text{ (wrt } |\cdot| \text{) if and only if } \psi(x_n - x) \rightarrow 0 \text{ (wrt } |\cdot| \text{)}.$$

For example, consider the sequence $\{p^n\}$ with p a prime number. It is clear that $\{p^n\}$ is not convergent (wrt $|\cdot|$). However $\{p^n\}$ is convergent (wrt $|\cdot|_p$). Furthermore $\{p^n\}$ is convergent (wrt $|\cdot|_p^{\frac{1}{2}}$). Both $|\cdot|_p$ and $|\cdot|_p^{\frac{1}{2}}$ determine the same convergence criteria while $|\cdot|_p$ and $|\cdot|$ do not.

Equivalent Valuations

Every valuation generates a family of valuations since ϕ^c , $0 < c \leq 1$, defined by

$$\phi^c(x) = (\phi(x))^c$$

is a valuation if and only if ϕ is. This is proved in the following theorem:

Theorem 3.9. If c is a real number such that $0 < c \leq 1$, then ϕ^c is a valuation on $(F, +, \cdot)$ if and only if ϕ is a valuation on $(F, +, \cdot)$.

Proof: It is evident that ϕ^c satisfies (3.4) and (3.5) if and only if ϕ does. It remains to show that

$$\phi^c(x + y) \leq \phi^c(x) + \phi^c(y) \text{ if and only if } \phi(x + y) \leq \phi(x) + \phi(y)$$

for each x and y in F . Let x and y be elements of F such that $\phi(y) \leq \phi(x)$. If $x = 0$, then $y = 0$ and the condition is satisfied. Assume $x \neq 0$ and that $\phi(x + y) \leq \phi(x) + \phi(y)$. Then

$$\begin{aligned} \phi^c(x + y) &= \phi^c(x) \phi^c\left(1 + \frac{y}{x}\right) \\ &\leq \phi^c(x) \left(1 + \phi\left(\frac{y}{x}\right)\right)^c \\ &\leq \phi^c(x) \left(1 + \phi\left(\frac{y}{x}\right)\right) \\ &\leq \phi^c(x) \left(1 + \phi\left(\frac{y}{x}\right)^c\right) \\ &= \phi^c(x) \left(\frac{\phi^c(x) + \phi^c(y)}{\phi^c(x)}\right) \\ &= \phi^c(x) + \phi^c(y). \end{aligned}$$

It is clear that $\phi^c(x + y) \leq \phi^c(x) + \phi^c(y)$ for $0 < c \leq 1$ implies that $\phi(x + y) \leq \phi(x) + \phi(y)$.

It is natural to ask whether valuations generated in this way have any common properties. In particular, do such valuations determine the same convergence criteria. Crucial to the results of this Chapter is the fact that the valuations of Theorem 3.9, generated by ϕ , do determine the same convergence criterion. However the same is true of a more general class of valuations. This exact relationship between valuations is investigated in the more general context.

Definition 3.10. Let ϕ and ψ be two non-trivial valuations on a field $(F, +, \cdot)$. Then ϕ and ψ are equivalent, $\phi \sim \psi$, if for each x in F such that $\phi(x) < 1$, it follows that $\psi(x) < 1$.

It is clear that equivalence of valuations is both a reflexive and transitive relation. It follows from the following theorem that equivalence of valuations is also a symmetric relation.

Theorem 3.11. (1) If ϕ and ψ are equivalent valuations on $(F, +, \cdot)$, then for each x in F such that $\phi(x) = 1$, it follows that $\psi(x) = 1$.

Proof: Since ϕ is non-trivial, there exists y in F such that $y \neq 0$ and $\phi(y) < 1$. For each x in F such that $\phi(x) = 1$, it follows that

$$\phi(x^n y) = \{\phi(x)\}^n \phi(y) = \phi(y) < 1$$

and hence that $\psi(x^n y) < 1$ for each $n \geq 0$. That is, $\psi(x) < \{\psi(y)\}^{-\frac{1}{n}}$ for each $n \geq 0$. Therefore

$$\psi(x) \leq \lim_{n \rightarrow \infty} \{\psi(y)\}^{-\frac{1}{n}} = 1.$$

Since $\phi(x) = 1$ if and only if $\phi(1/x) = 1$, it follows from the above argument that $\psi(x) \geq 1$ also. Therefore $\psi(x) = 1$ for each x in F such that $\phi(x) = 1$.

Corollary 3.12. Equivalence of valuations is an equivalence relation.

Proof: As noted previously, reflexivity and transitivity are immediate. Assume $\phi \sim \psi$, $\psi(x) < 1$, and consider the three cases for $\phi(x)$. If $\phi(x) > 1$, then $\phi(1/x) < 1$, $\psi(1/x) < 1$, and $\psi(x) > 1$. If $\phi(x) = 1$, then $\psi(x) = 1$. It follows that $\psi(x) < 1$ implies $\phi(x) < 1$. Therefore $\phi \sim \psi$ implies $\psi \sim \phi$ and \sim is symmetric.

Theorem 3.13. Let ψ and ϕ be valuations on $(F, +, \cdot)$. If $\psi = \phi^c$ where $c > 0$, then $\psi \sim \phi$.

Proof: For each x in F such that $\phi^c(x) < 1$, $(\phi(x))^c < 1$ and hence $\phi(x) < 1$.

The key result of this section is the following theorem:

Theorem 3.14. Two non-trivial valuations ϕ and ψ on $(F, +, \cdot)$ are equivalent if and only if they determine the same convergence criterion.

Proof: Two valuations ϕ and ψ are equivalent if it is the case that

$$(3.19) \quad \phi(x) < 1 \text{ if and only if } \psi(x) < 1$$

for each x in F . The proof is completed by showing that (3.18) holds if and only if (3.19) is true. Assume (3.18) to be true. If $\phi(x) < 1$, then $\{(\phi(x))^n\} = \{\phi(x^n)\}$ is a sequence of real numbers which converges to 0. Therefore $\{\psi(x^n)\}$ converges to 0 and $\psi(x) < 1$. Since the argument is symmetrical with respect to ϕ and ψ , (3.18) implies (3.19).

Now suppose (3.19) to be true for $\{x_n\}$, a sequence of F . If $\phi(x_n - x) \rightarrow 0$ (wrt $|\cdot|$), then there exists x_m such that $\phi(x_m - x) < 1$ and hence such that $\psi(x_m - x) < 1$. Therefore for each $\varepsilon > 0$ there exists k such that $\psi^k(x_m - x) < \varepsilon$. But for each k there exists an N such that $n > N$ implies $\phi(x_n - x) < (\phi(x_m - x))^k$ since $\phi(x_n - x) \rightarrow 0$ (wrt $|\cdot|$). Hence

$$\phi\left(\frac{x_n - x}{(x_m - x)^k}\right) < 1,$$

$$\psi\left(\frac{x_n - x}{(x_m - x)^k}\right) < 1,$$

and

$$\psi(x_n - x) < \psi\{(x_m - x)^k\} = \{\psi(x_m - x)\}^k.$$

It follows that for each $\varepsilon > 0$ there exists an N such that $\psi(x_n - x) < \varepsilon$ whenever $n \geq N$. Hence $\psi(x_n - x) \rightarrow 0$ (wrt $|\cdot|$). Likewise $\psi(x_n - x) \rightarrow 0$ (wrt $|\cdot|$) implies $\phi(x_n - x) \rightarrow 0$ (wrt $|\cdot|$) whenever (3.19) holds. Therefore (3.19) implies (3.18) and the proof is complete.

Using the ideas utilized in the proof of Theorem 3.14, it is possible to

prove that two valuations are equivalent if and only if they determine the same Cauchy criterion.

Let ϕ_1 and ϕ_2 be equivalent valuations on $(Q, +, \cdot)$ and assume that $(F_1, +, \cdot)$ with valuation ψ_1 and $(F_2, +, \cdot)$ with valuation ψ_2 are completions of $(Q, +, \cdot)$ with respect to the metrics induced by ϕ_1 and ϕ_2 respectively. For each x in F_1 there exists a Cauchy (wrt ϕ_1) sequence of rational numbers $\{x_n\}$ such that $x_n \rightarrow x$ (wrt ψ_1). Since $\{x_n\}$ is also Cauchy (wrt ϕ_2), there exists y in F_2 such that $x_n \rightarrow y$ (wrt ψ_2). The mapping f on F_1 defined by $f(x) = y$ is a well-defined one-to-one correspondence from F_1 onto F_2 . Then from the fact that the limit of a sum (product) of two convergent sequences is the sum (product) of the limits, it follows that f is an isomorphism. Furthermore it can be shown that f is metric preserving. Let $\{x_n\}$ and $\{w_n\}$ be sequences of Q such that $x_n \rightarrow x$ (wrt ψ_1), $x_n \rightarrow y$ (wrt ψ_2), $w_n \rightarrow w$ (wrt ψ_1), and $w_n \rightarrow z$ (wrt ψ_2). From

$$\begin{aligned}\psi_1(x - w) &= \psi_1(x - x_n + x_n - w_n + w_n - w) \\ &\leq \psi_1(x - x_n) + \phi_1(x_n - w_n) + \psi_1(w_n - w)\end{aligned}$$

for each $n \geq 0$, it follows that $\psi_1(x - w) \leq \lim \phi_1(x_n - w_n)$. Also

$$\begin{aligned}\phi_2(x_n - w_n) &= \psi_2(x_n - y + y - z + z - w_n) \\ &\leq \psi_2(x_n - y) + \psi_2(y - z) + \psi_2(z - w_n)\end{aligned}$$

implies that $\lim \phi_2(x_n - w_n) \leq \psi_2(y - z)$. Since $\lim \phi_2(x_n - w_n) = \lim \phi_1(x_n - w_n)$, it follows that $\psi_1(x - w) \leq \psi_2(f(x) - f(w))$. In like manner, it can be proved that $\psi_2(f(x) - f(w)) \leq \psi_1(x - w)$. Hence $(F_1, +, \cdot)$ and $(F_2, +, \cdot)$ are isometric.

For each prime p , the p -adic numbers is a completion of the rational numbers with respect to $|\cdot|_p$.

Definition 3.15. Two completions of a valued field are distinct if they are not isometric.

Theorem 3.16. The valued fields $(\mathbb{R}_p, +, \cdot)$, p a prime, and $(\mathbb{R}, +, \cdot)$ are distinct completions of the rational numbers.

Proof: Let $(\mathbb{R}_{p_0}, d_{p_0})$ be a completion of \mathbb{Q} with respect to $|\cdot|_{p_0}$. Suppose there exists a p such that (\mathbb{R}_p, d_p) is also a completion of \mathbb{Q} with respect to $|\cdot|_{p_0}$. By the preceding discussion, (\mathbb{R}_p, d_p) and $(\mathbb{R}_{p_0}, d_{p_0})$ are isometric. Let f be an isomorphism from $(\mathbb{R}_p, +, \cdot)$ onto $(\mathbb{R}_{p_0}, +, \cdot)$. Then $f(1) = 1$ and $f(p_0) = p_0$. But $|p_0|_{p_0} = 1/p_0$ while $|p_0|_p = 1$. Hence f is not metric preserving and (\mathbb{R}_p, d_p) and $(\mathbb{R}_{p_0}, d_{p_0})$ are not isometric. These conflicting results imply that (\mathbb{R}_p, d_p) is not a completion of \mathbb{Q} with respect to $|\cdot|_{p_0}$. Similarly from the fact that $|p|_p = 1/p$ while $|p|_{p_0} = p$, it follows that $(\mathbb{R}_{p_0}, d_{p_0})$ is not a completion of \mathbb{Q} with respect to $|\cdot|_p$. Thus all completions of \mathbb{Q} with respect to $|\cdot|_p$ or $|\cdot|_{p_0}$ are distinct.

Ostrowski's Theorem

The theorem of this section states that any non-trivial valuation on \mathbb{Q} is equivalent to either absolute value or p -value for some p and hence implies that there are no other distinct completions of \mathbb{Q} with respect to a valuation.

Theorem 3.17. The only non-trivial valuations on $(\mathbb{Q}, +, \cdot)$ are those equivalent to $|\cdot|_p$ or $|\cdot|$.

Proof: Let n be a rational integer greater than 1. Every m in \mathbb{Z} can be expressed in the form

$$m = a_0 + a_1 n + \dots + a_k n^k$$

where $0 \leq a_i \leq n-1$ for $i = 0, 1, 2, \dots, k$. It follows that $n^k \leq m$ and hence that $k \leq (\log m)/(\log n)$. Since a_i is an integer,

$$\begin{aligned}\phi(a_i) &= \phi(1 + 1 + \dots + 1) \\ &\leq \phi(1) + \dots + \phi(1) \\ &\leq n.\end{aligned}$$

Thus

$$\begin{aligned}\phi(m) &\leq \phi(a_0) + \phi(a_1) \phi(n) + \dots + \phi(a_k) \{\phi(n)\}^k \\ &\leq n (1 + \phi(n) + \dots + \{\phi(n)\}^k).\end{aligned}$$

If $\phi(n) \leq 1$, then

$$n(1 + \phi(n) + \dots + \phi^k(n)) \leq n(k + 1).$$

If $\phi(n) > 1$, then $\phi^k(n) > \phi(n)$ and

$$n(1 + \phi(n) + \dots + \phi^k(n)) \leq n(k + 1)\phi^k(n).$$

Therefore

$$\phi(m) \leq n(k + 1) \max(1, \phi^k(n)).$$

It follows that

$$(3.20) \quad \phi(m) \leq n \left(\frac{\log m}{\log n} + 1 \right) \max(1, \phi(n))^{\frac{\log m}{\log n}}$$

for $m, n > 1$. Now replacing m by m^τ , (3.20) yields

$$\phi(m) \leq \left(n^{\frac{\tau \log m}{\log n}} + n \right)^{\frac{1}{\tau}} \max(1, \phi(n))^{\frac{\log m}{\log n}}.$$

Letting $\tau \rightarrow \infty$ and using the fact that $\lim(c_1 + c_2)^{\frac{1}{\tau}} = 1$ where c_1 and c_2 are constants, it follows that

$$(3.21) \quad \phi(m) \leq \max(1, \phi(n))^{\frac{\log m}{\log n}}.$$

There are two distinct cases to consider.

Case I: There exists an $n > 1$ such that $\phi(n) \leq 1$. For each $m > 1$, $\log m > 0$. Hence $(\log m)/(\log n) > 0$ and it follows from (3.21) that $\phi(m) \leq 1$. Therefore ϕ is a non-archimedean valuation.

It remains to determine the exact nature of ϕ . Since ϕ is not trivial, there exists an m in \mathbb{Z} such that $\phi(m) < 1$. Let p be the smallest non-zero rational integer such that $\phi(p) < 1$. Since $p = ab$ with a and b positive and less than p implies

$$\phi(p) = \phi(a) \phi(b) = 1 \cdot 1 = 1,$$

p is prime. From $\phi(m) < 1$, it follows that $m \geq p$ and hence that $m = qp + r$ with $0 \leq r < p$. If $r \neq 0$, then $\phi(r) = 1$ since r is a rational integer less than p and ϕ is non-archimedean. Also $\phi(qp) = \phi(p + p + \dots + p) \leq \phi(p) < 1$ and $\phi(m) = \max(\phi(qp), \phi(r))$. It follows that $\phi(m) < 1$ implies that $r = 0$ and hence that p divides m . Conversely, if p divides m , then $m = qp$ and $\phi(m) < 1$. Thus $\phi(m) < 1$ if and only if p divides m .

Now let x be a non-zero rational number. Then

$$x = p^{\nu(x)} a/b$$

where p does not divide either a or b . Therefore

$$\phi(x) = \phi(p^{\nu(x)}) \frac{\phi(a)}{\phi(b)}.$$

Since p does not divide either a or b , $\phi(a) = \phi(b) = 1$ and

$$\phi(x) = (\phi(p))^{\nu(x)}.$$

However $\phi(p) < 1$ implies there exists a real number $c > 0$ such that

$(1/p)^c = \phi(p)$. Consequently

$$\phi(x) = (\phi(p))^{\nu(x)} = (1/p)^{c\nu(x)} = |x|_p^c.$$

From Theorem 3.13, it follows that ϕ is equivalent to $|\cdot|_p$ for some p .

Thus in Case I, ϕ is a non-archimedean valuation equivalent to $|\cdot|_p$ for some p .

Case II: For each $n > 1$ it is the case that $\phi(n) > 1$. From (3.21) it follows that

$$\phi(m)^{\frac{1}{\log m}} \leq \phi(n)^{\frac{1}{\log n}}.$$

Since $m > 1$ whenever $n > 1$ and since $\phi(m) \leq 1$ with $m > 1$ is Case I, both m and $\phi(m)$ are greater than one. Therefore the roles of m and n can be interchanged and

$$\phi(m)^{\frac{1}{\log m}} = \phi(n)^{\frac{1}{\log n}} = h$$

where h is independent of m . Furthermore h is greater than one since $\phi(n)$ is. Hence there exists a real number $c > 0$ such that $h = e^c$.

That is, $\phi(m) = m^c$. Now $m > 1$ implies $m^c = |m|^c$. Since $\phi(-m) = \phi(m)$ and $\phi(0) = 0$, it follows that

$$\phi(m) = |m|^c$$

with $c > 0$ for each m in \mathbb{Z} . Thus for each rational number $x = a/b$ where a and b are rational integers,

$$\phi(x) = \phi(a/b) = \phi(a)/\phi(b) = |a|^c/|b|^c = |a/b|^c = |x|^c.$$

Hence ϕ is equivalent to $|\cdot|^c$.

Ostrowski's Theorem and Theorem 3.17 express the relationship between the real, p -adic, and rational number fields. There are infinitely many distinct completions of the rational number field with respect to a valuation. These completions are the real and p -adic number fields with their respective valuations and there are no other such completions.

Discrete Valuations

A real-valued function is discrete if 0 is the only accumulation point of its range. A valuation is discrete if it is a discrete function. It is clear that absolute value is not a discrete valuation.

However it follows from

$$|\mathbb{R}_p|_p = \{\dots, p^{-2}, p^{-1}, 1, p, p^2, \dots\}$$

that p -value is a discrete valuation for each p .

Definition 3.18. A valuated field is discrete if the valuation is discrete.

For each p , $(\mathbb{R}_p, +, \cdot)$ is a discrete field while $(\mathbb{R}, +, \cdot)$ is not a discrete field.

There is no connection between a set having an algebraic structure which is a discrete field and it having a discrete topological structure. The discrete topology for a set is the collection of all subsets of the set. Since $\{p^n\}$ converges (wrt $|\cdot|_p$) to 0 while $|p^n|_p \neq 0$ for each $n \geq 0$, it is clear that $\{\xi: |\xi|_p > 0\}$ is not a closed subset of (\mathbb{R}_p, d_p) . Hence $\{0\}$ is not open with respect to the $|\cdot|_p$ -topology. Consequently the metric space (\mathbb{R}_p, d_p) is not discrete.

There is, however, an interesting relationship between the trivial valuation on a field $(F, +, \cdot)$ and the discrete topology for the set F .

Theorem 3.19. Let $(F, +, \cdot)$ be a valuated field with valuation ϕ . Then ϕ is trivial if and only if the ϕ -topology is the discrete topology for F .

Proof: If a topology for F is discrete, then every subset of F is open. In particular, $\{a\}$ is open for each a in F . It is known that $\phi(0) = 0$. Assume that there exists a in F such that $a \neq 0$ and $\phi(a) \neq 1$. Then $\phi(a) < 1$ or $\phi(a) > 1$. If $\phi(a) < 1$, then $\{a^n\}$ is a sequence of F such that $a^n \rightarrow 0$ (wrt ϕ). Now $\{0\}$ open implies that $F - \{0\}$ is closed and hence that 0 is not a limit point of any sequence of distinct points of

F. Therefore there exists an N such that $a^n = 0$ whenever $n \geq N$. Since this can happen only if $a = 0$ and since by assumption $a \neq 0$, it follows that $\phi(a) \geq 1$. If $\phi(a) > 1$, then $\phi(1/a) < 1$ and it follows as before that $\phi(1/a) \geq 1$. That is, $\phi(a) \leq 1$. Hence $\phi(a) = 1$ for each a in F such that $a \neq 0$ and ϕ is trivial. Conversely, assume ϕ is the trivial valuation. Then for each ϵ such that $0 < \epsilon < 1$ and for each a in F , $\{a\} = \{x: \phi(x - a) < \epsilon\}$ is open. It follows that every subset of F is open and the topology for F induced by ϕ is the discrete topology.

CHAPTER IV

SOME CONSEQUENCES OF THE NON-ARCHIMEDEAN PROPERTY

The set of p -adic numbers has both an algebraic and a topological structure. Standard algebraic methods have been used to prove that $(\mathbb{O}_p, +, \cdot)$ is an integral domain and that $(\mathbb{R}_p, +, \cdot)$ is a field. The metric induced by p -value has provided the essential topological properties prerequisite to the concept of convergence of sequences. In this chapter, some additional algebraic and topological properties of $(\mathbb{R}_p, +, \cdot)$ and $(\mathbb{O}_p, +, \cdot)$ which depend upon the non-archimedean property of p -value are considered and compared with corresponding properties of $(\mathbb{R}, +, \cdot)$ and $(\mathbb{Z}, +, \cdot)$. General characteristics of a metric space with metric d that satisfies the inequality $d(x, z) \leq \max(d(x, y), d(y, z))$ are developed.

Ideals of $(\mathbb{O}_p, +, \cdot)$

The set of p -adic integers consists of those p -adic numbers whose p -value is less than or equal to 1. A p -adic integer α is a unit if and only if $|\alpha|_p = 1$. Let P be the subset of \mathbb{O}_p consisting of the non-units. That is,

$$P = \{\alpha: \alpha \text{ is in } \mathbb{O}_p \text{ and } |\alpha|_p < 1\}.$$

The set P plays an important role in describing all the ideals of $(\mathbb{O}_p, +, \cdot)$. This role is now made clear.

Theorem 4.1. If P is the set of non-units of \mathbb{O}_p , then $(P, +, \cdot)$ is the

unique maximal ideal of $(0_p, +, \cdot)$. Furthermore $(P, +, \cdot)$ is a prime ideal.

Proof: For each α and β in 0_p , if α is also in P , then

$$(4.1) \quad |\alpha\beta|_p = |\alpha|_p |\beta|_p < 1$$

and $\alpha\beta$ is an element of P . If both α and β are elements of P , then

$$|\alpha - \beta|_p \leq \max(|\alpha|_p, |\beta|_p) < 1$$

and $\alpha - \beta$ is an element of P . Hence $(P, +, \cdot)$ is an ideal of $(0_p, +, \cdot)$.

Furthermore if $(M, +, \cdot)$ is an ideal of $(0_p, +, \cdot)$ such that M properly contains P , then α in M but not in P implies that α is a unit of 0_p .

Since the inverse of a unit is a unit, α^{-1} is in 0_p and 1 is an element of M . Thus $M = 0_p$ and $(P, +, \cdot)$ is a maximal ideal of $(0_p, +, \cdot)$.

Assume $(S, +, \cdot)$ is also a maximal ideal of $(0_p, +, \cdot)$. If α is an element of S such that $|\alpha|_p = 1$, then α^{-1} is in 0_p , 1 is in S , and $S = 0_p$. Since this is impossible, $(S, +, \cdot)$ maximal implies that $|\alpha|_p < 1$ for each α in S . Hence S is a subset of P . But this is impossible unless $S = P$. Therefore $(P, +, \cdot)$ is the unique maximal ideal of $(0_p, +, \cdot)$.

To complete the proof, assume that $\alpha\beta$ is an element of P . Then from (4.1) it follows that $|\alpha|_p < 1$ or $|\beta|_p < 1$. Hence $(P, +, \cdot)$ is a prime ideal.

It is possible to characterize all ideals of $(0_p, +, \cdot)$ in terms of P in a rather elementary manner. An important step in this direction is the fact that $(P, +, \cdot)$ is the principal ideal generated by p .

Theorem 4.2. The principal ideal of $(0_p, +, \cdot)$ generated by p , $((p), +, \cdot)$, is the ideal $(P, +, \cdot)$.

Proof: Assume α is in (p) . Then there exists β in 0_p such that $\alpha = p\beta$. From $|\alpha|_p = |p|_p |\beta|_p = (1/p) |\beta|_p \leq (1/p)$, it follows that α is in P and

hence that (p) is a subset of P . If α is in P , then $\alpha = p^m \varepsilon$ with $m \geq 1$. Therefore $\alpha = p \cdot p^{m-1} \varepsilon$ and $p^{m-1} \varepsilon$ is in 0_p . Hence P is a subset of (p) .

Corollary 4.3. The ideal $((p), +, \cdot)$ is prime and is the unique maximal ideal of $(0_p, +, \cdot)$.

The importance of Theorem 4.2 lies in the fact that every ideal of $(0_p, +, \cdot)$ is related to $P = (p)$.

Theorem 4.4. Every non-zero ideal of $(0_p, +, \cdot)$ is of the form $(p^k, +, \cdot)$ where $p^k = (p)^k = (p^k)$.

Proof: Let $(M, +, \cdot)$ be a non-zero ideal of $(0_p, +, \cdot)$ and let

$K = \{\nu(\alpha) : 0 \neq \alpha \in M\}$. Then K is a non-empty set of positive integers.

Hence by the well-ordering principle, there exists a smallest integer k in K . Since the inverse of a unit is a p -adic integer, $p^k \varepsilon$ in M implies p^k is also an element of M . Thus from the fact that $(M, +, \cdot)$ is an ideal of $(0_p, +, \cdot)$, it follows that (p^k) is a subset of M . Since each element of M has order greater than or equal to k , M is also a subset of (p^k) . Hence $M = (p^k)$.

The fact that $(p)^k = (p^k)$ for each k is established by induction on k . It is clear that $(p)^k = (p^k)$ for $k = 1$. Assume $(p)^n = (p^n)$. Then α in (p^{n+1}) implies $\alpha = p^{n+1} \beta = p^n(p\beta)$. Since $p^n(p\beta)$ is an element of $(p^n)(p) = (p)^n(p) = (p)^{n+1}$, (p^{n+1}) is contained in $(p)^{n+1}$. If α is in $(p)^{n+1}$, then α is an element of $(p)^n(p)$. It follows that α is in $(p^n)(p)$ and $\alpha = p^n \beta p \gamma = p^{n+1} \beta \gamma$. Hence $(p)^{n+1}$ is a subset of (p^{n+1}) . Thus $(p)^{n+1} = (p^{n+1})$ whenever $(p)^n = (p^n)$ and the proof of the theorem is complete.

Corollary 4.5. Every non-zero ideal of $(0_p, +, \cdot)$ is a principal ideal.

Thus $(0_p, +, \cdot)$ is a principal ideal domain and the following theorem from general ideal theory (2) holds true for $(0_p, +, \cdot)$.

Theorem 4.6. A non-zero ideal of $(0_p, +, \cdot)$ is prime if and only if it is maximal.

Corollary 4.7. The ideal $(P, +, \cdot)$ of $(0_p, +, \cdot)$ is the unique prime ideal of $(0_p, +, \cdot)$.

Thus the ideals of $(0_p, +, \cdot)$ have a simple relationship to each other. As in $(Z, +, \cdot)$, every ideal of $(0_p, +, \cdot)$ is principal. In both $(Z, +, \cdot)$ and $(0_p, +, \cdot)$, only prime ideals are maximal and conversely. There are infinitely many prime (maximal) ideals of $(Z, +, \cdot)$. However $(0_p, +, \cdot)$ has a unique prime (maximal) ideal which in a sense generates all other ideals. This difference is certainly anticipated since $(Z, +, \cdot)$ has infinitely many primes while $(0_p, +, \cdot)$ has a unique prime.

Since $(0_p, +, \cdot)$ is a commutative ring with unity and since $(P, +, \cdot)$ is maximal, $(0_p/P, +, \cdot)$ is a field. The elements of $0_p/P$ are the residue classes of 0_p modulo p . By Theorem 2.17, there are exactly p such classes. Hence $(0_p/P, +, \cdot)$ is a finite field.

Definition 4.8. The field $(0_p/P, +, \cdot)$ is the residue class field.

From the fact that $(Z/(p), +, \cdot)$ and $(0_p/P, +, \cdot)$ each have p elements, it is clear that there is a one-to-one correspondence between these two finite fields. That these two fields are isomorphic is a special case of the following theorem:

Theorem 4.9. The residue class fields $(0_p/P^k, +, \cdot)$ and $(Z/(p)^k, +, \cdot)$ are isomorphic.

Proof: For each $[x]$ in $Z/(p)^k$ there exists $[\alpha]$ in $0_p/p^k$ such that x is in $[\alpha]$. Define ϕ from $Z/(p)^k$ into $0_p/P$ by $\phi([x]) = [\alpha]$. Since two rational integers are congruent modulo p^k only if they are congruent modulo p^k as p -adic integers, ϕ is well-defined. It is clear that ϕ is onto since each p -adic integer is congruent modulo p^k to a rational integer. Let α and β be p -adic integers and let x and y be rational integers such that x is in $[\alpha]$ and y is in $[\beta]$. Then $x \equiv \alpha \pmod{p^k}$ and $y \equiv \beta \pmod{p^k}$. If $[\alpha] = [\beta]$, then $\alpha \equiv \beta \pmod{p^k}$ and $x \equiv y \pmod{p^k}$. Thus $[x] = [y]$ and ϕ is 1-1. Also $x + y \equiv \alpha + \beta \pmod{p^k}$, $xy \equiv \alpha\beta \pmod{p^k}$, and it follows that ϕ is an isomorphism.

In terms of the geometric model for R_p , the p -adic integers are on the circles having radius less than or equal to one. The unique prime maximal ideal P consists of all p -adic integers on the circles having radius less than one. Since α in P^m implies $|\alpha|_p \leq p^{-m}$, it follows that all points of P^m are on circles having radius less than or equal to p^{-m} . It is evident from the geometric model, as well as from the definition of a principal ideal, that P^m is a subset of P^n whenever $m \geq n \geq 1$.

The residue class modulo p^n determined by $\alpha = p^m \epsilon$ has a simple representation. If $m \geq n \geq 1$, then $\alpha + P^n = P^n$ since α in P^m , a subset of P^n , implies α is in P^n . In case $0 \leq m < n$, let $\epsilon = \sum_{k=0}^{\infty} a_k p^k$. Hence

$$\alpha = a_0 p^m + a_1 p^{m+1} + \dots + a_k p^{m+k} + \dots$$

A p -adic integer

$$\beta = b_0 + b_1 p + \dots + b_{m+k} p^{m+k} + \dots$$

is an element of $\alpha + P^n$ if and only if $\alpha \equiv \beta \pmod{p^n}$ and consequently if and only if $b_0 = b_1 = \dots = b_{m-1} = 0$ while

$$a_k = b_{m+k}$$

for $0 \leq k \leq n-m-1$. Thus $\alpha + P^n$ is contained in the arc consisting of the points with polar coordinates p^{-m} and $2\pi\theta$ where

$$\sum_{k=0}^{n-m-1} \frac{a_k}{(p+1)^{k+1}} \leq \theta < \sum_{k=0}^{n-m} \frac{a_k}{(p+1)^{k+1}}.$$

This half open arc that contains $\alpha + P^n$ has the rational integer $\sum_{k=0}^{n-m-1} a_k p^k$ as its initial point. Its central angle is $2\pi a_{n-m}/(p+1)^{n-m+1}$ and its length is $2\pi a_{n-m}/(p+1)^{n+1}$. The residue classes of 0_5 modulo $(5)^2$ determined by $p^m \varepsilon$ with $0 \leq m \leq 2$ are subsets of the half open arcs indicated in Figure 4. The initial points are given for arcs on the circle of radius $1/5$. Initial points of the arcs on the circle of radius 1 can be determined from Figure 2. The zero residue class consists of all p-adic integers on circles of radius $1/5^n$ with $n \geq 2$.

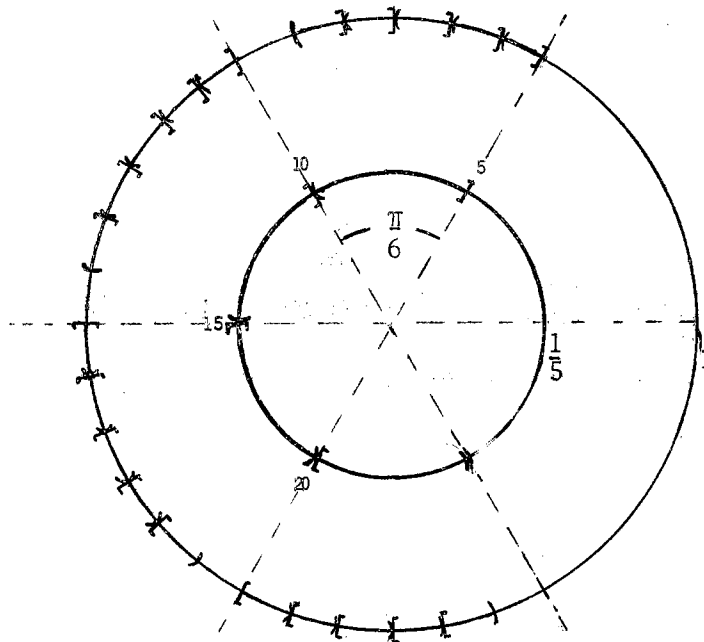


Figure 4. Arcs Containing the Non-Zero Residue Classes of 0_5 Modulo $(5)^2$.

The distance between two p -adic numbers is determined by the metric induced by p -value. If two p -adic numbers are located on distinct circles, then the distance between them is the radius of the larger circle. Furthermore two points on the same circle can not be farther apart than the radius of the circle containing them. On each circle there are p -adic numbers with the distance between them equal to the radius of the circle. For instance $2p^m$ and p^m are p -adic numbers on the circle of radius p^{-m} and $|2p^m - p^m|_p = p^{-m}$. No closed sphere with center on a circle of radius p^{-m} can include a point on a circle of radius p^{-n} , $m \neq n$, unless it contains all points on all circles of radius less than or equal to p^{-n} .

The closed spheres that have a unit as center are easily characterized in terms of their radius. Let ε be a unit and let r be a non-negative real number. If $r \geq 1$, then there exists an $n \geq 0$ such that $p^n \leq r < p^{n+1}$ and

$$S[\varepsilon, r] = \{\xi: |\xi|_p \leq p^n\}.$$

In particular, the p -adic integers is the closed sphere with any unit as center and with radius greater than or equal to 1 and less than p . If $r < 1$, then $S[\varepsilon, r]$ is a subset of the p -adic units. Each closed sphere which is a subset of the units can be expressed in terms of the elements of the residue classes. That is,

$$S[\varepsilon, r] = \varepsilon + p^m$$

whenever $p^{-m} \leq r < p^{-m+1} < 1$. For example, the closed spheres that have a unit as center and radius greater than or equal to $1/25$ and less than $1/5$ consist of the p -adic numbers on the half open arcs of the circle of radius one in Figure 4.

Much of the above analysis holds in general for closed spheres with

center at a p -adic number. Let $\xi = p^m \epsilon$ with m in \mathbb{Z} . If $r \geq p^{-m}$, then there exists an n such that $p^{-m} \leq p^{-n} \leq r < p^{-n+1}$ and

$$S[\xi, r] = \{\zeta: |\zeta|_p \leq p^{-n}\}.$$

Now consider the case where $r < p^{-m}$. If ζ is in $S[\xi, r]$, then ζ and ξ are on the same circle and $\zeta = p^m \eta$. Since ζ is in $S[\xi, r]$ if and only if η is in $S[\epsilon, rp^{-m}]$ and since $S[\epsilon, rp^{-m}] = \epsilon + p^{m+n}$ whenever $p^{-m-n} \leq rp^{-m} < p^{-m-n+1}$, it follows that ζ is in $S[\xi, r]$ if and only if η is in $\epsilon + p^{m+n}$ whenever $p^{-n} \leq r < p^{-n+1} \leq p^{-m}$.

Thus the closed spheres of \mathbb{R}_p can be characterized in terms of circles of radius less than or equal to a given radius and residue classes. Since

$$S(\xi, p^{-n}) = S[\xi, p^{-n-1}],$$

the open sphere can be expressed in the same manner. This relationship between the algebraic structure $(\mathbb{O}_p, +, \cdot)$ and the topological structure (\mathbb{R}_p, d_p) is a key to some surprising results related to compactness.

Theorem 4.10. Let $(P, +, \cdot)$ be the unique maximal ideal of $(\mathbb{O}_p, +, \cdot)$, let α be an element of \mathbb{O}_p , and let $S(\alpha, r)$ be an open sphere with center α and radius $r > 0$. Then there exists an n such that $\alpha + P^n$ is a subset of $S(\alpha, r)$.

Proof: Let n be the smallest integer such that $p^{-n} < r$. If γ is in $\alpha + P^n$, then

$$|\gamma - \alpha|_p \leq p^{-n} < r$$

and γ is in $S(\alpha, r)$. Therefore $S(\alpha, r)$ contains $\alpha + P^n$.

Compactness

Let (X, d) be a metric space, let S be a subset of X , and let \mathcal{C} be a family of subsets of S such that each point of S is an element of

some member of \mathcal{C} . Then \mathcal{C} is a covering of S and \mathcal{C} is said to cover S . If each subset of \mathcal{C} is an open set of the metric topology, then \mathcal{C} is an open covering.

Definition 4.11. A subset of a metric space is compact if every open covering has a finite subcovering.

A consequence of Theorem 4.10 is the following result which reveals a remarkable difference between (R_p, d_p) and (R, d) .

Theorem 4.12. The set 0_p is a compact subset of (R_p, d_p) .

Proof: Assume that $\{G_\lambda : \lambda \text{ is in } \Lambda\}$ is an open covering of 0_p which does not have a finite subcovering and let $\Sigma = 0_p/P$. Since

$$(4.2) \quad 0_p = \bigcup_{[\alpha] \in \Sigma} (\alpha + P)$$

and Σ is finite, there exists α_0 in 0_p such that

$$\alpha_0 + P$$

is not finitely covered. But $P = p0_p$ and

$$\alpha_0 + P = \bigcup_{[\alpha] \in \Sigma} (\alpha_0 + p(\alpha + P)).$$

Therefore there must be α_1 in 0_p such that

$$\alpha_0 + \alpha_1 p + P^2$$

is not finitely covered. It follows by mathematical induction that there exists $\{\alpha_m\}$ such that for each $m \geq 1$,

$$\alpha_0 + \alpha_1 p + \alpha_2 p^2 + \dots + \alpha_{m-1} p^{m-1} + P^m$$

is not finitely covered. Let

$$\alpha = \alpha_0 + \alpha_1 p + \dots + \alpha_m p^m + \dots$$

Since α is in 0_p , there exists a G_λ such that α is in G_λ . Hence there

exists an m_0 such that $\alpha + P^{m_0}$ is a subset of G_λ . But $\alpha_0 + \alpha_1 p + \dots + \alpha_{m_0-1} p^{m_0-1} + P^{m_0}$ is a subset of $\alpha + P^{m_0}$ and consequently is a subset of G_λ . Therefore $\alpha_0 + \alpha_1 p + \dots + \alpha_{m_0-1} p^{m_0-1} + P^{m_0}$ is finitely covered. Since the assumption that there exists an open covering of O_p with no finite subcovering leads to contradictory conclusions, every open covering of O_p contains a finite subcovering and O_p is compact.

Thus (R_p, d_p) contains a compact set which in turn contains the rational integers as a subset. No compact set of real numbers has this property. This interesting observation relative to Z as a subset of the metric space (R_p, d_p) can be stated more precisely.

Definition 4.13. Let (X, d) be a metric space and let S be a subset of X . The closure of S is the union of S and the set of all accumulation points of S .

Definition 4.14. Let (X, d) be a metric space and let S be a subset of X such that the closure of S is a compact subset of (X, d) . Then S is conditionally compact.

Theorem 4.15. The set Z of rational integers is a conditionally compact subset of (R_p, d_p) .

Proof: Since every p -adic integer α is the limit of the sequence of rational integers which determines it, the closure of Z contains O_p . Conversely, let α be a p -adic integer. For each $n > 0$ there exists a rational integer y_n such that $\alpha \equiv y_n \pmod{p^n}$. The sequence $\{y_n\}$ converges to α with respect to $|\cdot|_p$. Hence O_p contains the closure of Z .

In a metric space, a set S is bounded if there exists an open sphere that contains S as a subset. Compact sets of a metric space are

closed and bounded. Hence the following Corollary to Theorem 4.12.

Corollary 4.16. The set of p -adic integers is a closed and bounded subset of R_p with respect to the $|\cdot|_p$ -topology.

In general metric spaces, it is not the case that closed and bounded sets are compact. However closed and bounded sets of real numbers are compact relative to the $|\cdot|$ -topology. The same is true for the p -adic numbers with the $|\cdot|_p$ -topology.

Theorem 4.17. Any closed and bounded subset of R_p is compact with respect to the $|\cdot|_p$ -topology.

Proof: Let H be a closed and bounded subset of R_p . Then there exists m in Z such that for each ξ in H , $v(\xi) \geq m$. Let

$$K = \{\xi/p^m : \xi \in H\}.$$

The set K is a set of p -adic integers. If α is an accumulation point of K then there exists a sequence $\{\xi_n/p^m\}$ of K such that $\{\xi_n/p^m\}$ converges to α . That is, for each $\epsilon > 0$ there exists N such that

$$|\xi_n/p^m - \alpha|_p < \epsilon/p^m \text{ whenever } n \geq N.$$

It follows that for each $\epsilon > 0$ there exists an N such that

$$|\xi_n - p^m \alpha|_p < \epsilon \text{ whenever } n \geq N.$$

Consequently $\{\xi_n\}$ converges to $p^m \alpha$. Now H closed implies that $p^m \alpha$ is an element of H and hence that α is an element of K . Therefore K is closed. As a closed subset of 0_p , K is compact since a closed subset of a compact space is compact. Thus every open covering of K has a finite subcovering. Let $\{G_\lambda : \lambda \in \Lambda\}$ be an open covering of H . For each λ in Λ , let $M_\lambda = \{\xi/p^m : \xi \text{ is in } G_\lambda\}$. Since G_λ is open, for each ξ in G_λ there exists an $\epsilon > 0$ such that $S(\xi, \epsilon)$ is a subset of G_λ . Hence

$S(\xi/p^m, \varepsilon p^m)$ is an open sphere containing ξ/p^m and contained in M_λ . It follows that M_λ is an open set and $\{M_\lambda : \lambda \text{ is in } \Lambda\}$ is an open covering of K . Therefore there exists a finite subcovering, say

$\{M_{\lambda_1}, M_{\lambda_2}, \dots, M_{\lambda_n}\}$, which covers K . Hence $\{G_{\lambda_1}, G_{\lambda_2}, \dots, G_{\lambda_n}\}$ covers H and H is compact.

Connectedness

It has been observed that if α is a unit, then

$$0_p = S[\alpha, 1] = S(\alpha, p).$$

Hence 0_p is both an open and a closed subset of (R_p, d_p) . This property of 0_p implies that (R_p, d_p) is not a connected space. A stronger statement can be made. No subset of R_p consisting of two or more points is connected.

Theorem 4.18. The only connected subsets of (R_p, d_p) are those sets consisting of a single point.

Proof: Let H be a subset of (R_p, d_p) and let ξ_1 and ξ_2 be two distinct points of H . There exists an n such that $|\xi_1 - \xi_2|_p = p^{-n}$. Let S denote the union of all closed spheres of R_p of radius p^{-n} . Since $S[\xi, p^{-n}] = S(\xi, p^{-n+1})$, every closed sphere of R_p is open in (R_p, d_p) and S is an open set of (R_p, d_p) . However the relationship between $S[\xi, p^{-n}]$ and the residue classes implies there are only finitely many closed spheres of radius p^{-n} . Therefore S is also a closed subset of (R_p, d_p) . It follows that $H \cap S$ is both an open and a closed subset of (H, d_p) . From Theorem 1.9, it is clear that H is not a connected subset of (R_p, d_p) . The theorem follows since every singleton set is connected.

A metric space that has only singleton sets as connected sets is said to

be totally disconnected. The p-adic numbers with the $|\cdot|_p$ -topology is totally disconnected.

Non-Archimedean Metric Spaces

Since for each n there are at most p^n closed spheres of p-adic numbers with radius p^{-n} but infinitely many potential centers, some closed sphere must have infinitely many centers. The truth is that every point of any sphere, open or closed, is a center for the sphere. In \mathbb{Q}_p , this is an immediate consequence of the fact that $S[\alpha, p^{-n}] = \alpha + p^n$. That is, β in $S[\alpha, p^{-n}]$ implies that β is in $\alpha + p^n$ and hence that

$$S[\alpha, p^{-n}] = \alpha + p^n = \beta + p^n = S[\beta, p^{-n}].$$

More generally, this unusual result is a consequence of the non-archimedean property of the metric d_p for \mathbb{R}_p and is considered in the more general context of a non-archimedean metric space.

Let ϕ be a valuation on a field $(F, +, \cdot)$ such that

$$\phi(a + b) \leq \max(\phi(a), \phi(b))$$

for each a and b in F . If d is the metric on the set F defined by $d(a, b) = \phi(a - b)$ for each a and b in F , then

$$(4.3) \quad d(x, z) \leq \max(d(x, y), d(y, z))$$

for each x , y , and z in F .

Definition 4.19. Let (X, d) be a metric space such that d satisfies (4.3). Then (X, d) is a non-archimedean metric space.

Theorem 4.20. Every point of a closed (open) sphere of a non-archimedean metric space is a center of the sphere.

Proof: The proof is given for closed spheres. The modification

required for open spheres is clear. Let y be an element of the closed sphere $S[x,r]$, and consider $S[y,r]$. From $d(x,z) \leq \max(d(x,y), d(y,z))$ and $d(y,z) \leq \max(d(x,y), d(x,z))$, it follows that $d(x,z) \leq r$ if and only if $d(y,z) \leq r$. Hence z is in $S[x,r]$ if and only if z is in $S[y,r]$. That is, $S[x,r] = S[y,r]$ and each point of a closed sphere is a center of the sphere.

If two spheres of p -adic numbers intersect, then one contains the other. The same is true of spheres of a general non-archimedean metric space.

Theorem 4.21. If two spheres of a non-archimedean metric space have a non-empty intersection, then one of the spheres contains the other.

Proof: From z in both $S[x,r_1]$ and $S[y,r_2]$, it follows that $S[x,r_1] = S[z,r_1]$ and $S[y,r_2] = S[z,r_2]$. Hence $S[x,r_1]$ contains $S[y,r_2]$ or $S[y,r_2]$ contains $S[x,r_1]$ as $r_2 \leq r_1$ or $r_1 \leq r_2$. The proof for open spheres is similar.

Corollary 4.22. If a set of spheres in a non-archimedean metric space is such that any two intersect, then the set is a nest.

Since non-archimedean metric spaces are metric spaces, open spheres are open sets and closed spheres are closed sets. Each open sphere of p -adic numbers is a closed sphere. Consequently each open sphere is a closed set. Similarly each closed sphere of p -adic numbers is open. The next two theorems generalize these observations for non-archimedean metric spaces.

Theorem 4.23. Every open sphere of a non-archimedean metric space (X,d) is a closed set in X .

Proof: Let y be an accumulation point of $S(x,r)$. Then there exists a

sequence $\{x_n\}$ in X such that $x_n \rightarrow y$. It follows that there exists an N such that $n \geq N$ implies $1/n < r$ and $d(x_n, y) < 1/n$. Hence

$$d(x, y) \leq \max(d(x_n, x), d(x_n, y)) < r$$

and y is an element of $S(x, r)$.

Theorem 4.24. Every closed sphere of a non-archimedean metric space (X, d) is an open set in X .

Proof: Let $S[x, r]$ be a closed sphere and let y be an element of $S[x, r]$. Then $S[y, r] = S[x, r]$. Therefore z an element of $S(y, r)$ implies z is also in $S[x, r]$. That is, for each y in $S[x, r]$ there exists an open set $S(y, r)$ such that y is in $S(y, r)$ and $S(y, r)$ is a subset of $S[x, r]$. Hence $S[x, r]$ is open in X .

Since (R_p, d_p) is a metric space, the concept of a continuous function from R_p into any metric space is available. By Theorem 1.11, a function f from R_p into R_p is continuous on R_p if and only if for each $\varepsilon > 0$ there exists a δ such that

$$|f(\xi) - f(\zeta)|_p < \varepsilon \text{ whenever } |\xi - \zeta|_p < \delta$$

with ζ in R_p . Similarly a function f from R_p into R is continuous on R_p if and only if for each $\varepsilon > 0$ there exists a δ such that

$$(4.4) \quad |f(\xi) - f(\zeta)| < \varepsilon \text{ whenever } |\xi - \zeta|_p < \delta$$

with ζ in R_p .

Theorem 4.25. The p -value function $|\cdot|_p$ is a continuous function from R_p into R .

Proof: From $||\xi|_p - |\zeta|_p| \leq |\xi - \zeta|_p$, it follows that (4.4) is satisfied by $|\cdot|_p$ whenever $\delta = \varepsilon$.

Addition and multiplication of p -adic numbers are p -adic valued

functions on $R_p \times R_p$. To investigate the continuity of addition and multiplication, a topology for $R_p \times R_p$ is required.

Theorem 4.26. Let (X_1, d_1) and (X_2, d_2) be two non-archimedean metric spaces. The function D from $(X_1 \times X_2) \times (X_1 \times X_2)$ into R such that

$$D((w,x), (y,z)) = \max(d_1(w,y), d_2(x,z))$$

is a metric on $X_1 \times X_2$.

Proof: It is clear that D satisfies (1.7) and (1.8). Since

$$\begin{aligned} \max(d_1(u,y), d_2(v,z)) &\leq \max(\max(d_1(u,w), d_2(w,y)), \max(d_1(u,x), d_2(x,z))) \\ &= \max(\max(d_1(u,w), d_2(v,x)), \max(d_1(w,y), d_2(x,z))) \end{aligned}$$

for each (u,v) , (w,x) , and (y,z) in $X_1 \times X_2$, it follows that

$$D((u,v), (y,z)) \leq \max(D((u,v), (w,x)), D((w,x), (y,z)))$$

and hence that D satisfies (4.3). But condition (4.3) implies condition (1.9). Therefore D is a non-archimedean metric on $X_1 \times X_2$.

Thus $(R_p \times R_p, D_p)$ where $D_p((\xi, \zeta), (\lambda, \mu)) = \max(d_p(\xi, \lambda), d_p(\zeta, \mu))$ for each (ξ, ζ) and (λ, μ) in $R_p \times R_p$ is a metric space. The metric topology for $R_p \times R_p$ determined by D_p provides a criterion for continuity of any function defined on $R_p \times R_p$.

Theorem 4.27. Addition and multiplication of p -adic numbers are continuous functions from $R_p \times R_p$ into R_p .

Proof: For each (ξ, ζ) and (λ, μ) in $R_p \times R_p$,

$$\begin{aligned} |\xi + \zeta - (\lambda + \mu)|_p &= |\xi - \lambda + \zeta - \mu|_p \\ &\leq \max(|\xi - \lambda|_p, |\zeta - \mu|_p) \\ &\leq D_p((\xi, \zeta), (\lambda, \mu)). \end{aligned}$$

It follows that for each (ξ, ζ) in $R_p \times R_p$ and for each $\epsilon > 0$ there exists a $\delta = \epsilon$ such that

$$|\xi + \zeta - (\lambda + \mu)|_p < \epsilon \text{ whenever } D_p((\xi, \zeta), (\lambda, \mu)) < \delta$$

with (λ, μ) in $R_p \times R_p$. Hence addition is continuous. Also

$$\begin{aligned} |\xi\zeta - \lambda\mu|_p &= |\xi\zeta - \xi\mu + \xi\mu - \lambda\mu|_p \\ &= |\xi(\zeta - \mu) + (\xi - \lambda)\mu|_p \\ &\leq \max(|\xi|_p |\zeta - \mu|_p, |\mu|_p |\xi - \lambda|_p) \\ &\leq \max(|\xi|_p, |\mu|_p) \max(|\zeta - \mu|_p, |\xi - \lambda|_p) \\ &\leq \max(|\xi|_p, |\mu|_p) D_p((\xi, \zeta), (\lambda, \mu)) \end{aligned}$$

and $|\zeta - \mu|_p < 1$ implies that $|\mu|_p < 1 + |\zeta|_p$. It follows that for each (ξ, ζ) in $R_p \times R_p$ and for each $\varepsilon > 0$ there exists $\delta = \min(1, \frac{\varepsilon}{|\xi|_p(1 + |\zeta|_p)})$ such that

$$|\xi\zeta - \lambda\mu|_p < \varepsilon \text{ whenever } D_p((\xi, \zeta), (\lambda, \mu)) < \delta$$

with (λ, μ) in $R_p \times R_p$. Therefore multiplication is a continuous function on $R_p \times R_p$.

Definition 4.28. A field with a metric such that the field operations are continuous with respect to the metric topology is a topological field.

From Theorem 4.27, it is clear that $(R_p, +, \cdot)$ is a topological field.

CHAPTER V

NON-ARCHIMEDEAN NORMED LINEAR SPACES

In many of the common examples of linear spaces the associated scalar field is either the rational, the real, or the complex number field. Since the knowledge of a beginning student is limited to these fields, this is understandable. However after the preceding introduction to p-adic number fields, it is natural to consider linear spaces over the p-adic number fields. In this chapter, normed linear spaces over $(\mathbb{R}_p, +, \cdot)$ are considered. Although not all normed linear spaces over $(\mathbb{R}_p, +, \cdot)$ have a non-archimedean norm, attention is restricted in this chapter to the case where the norm does satisfy the non-archimedean property.

Normed Linear Spaces

A norm for a linear space is a real-valued function that is, in many respects, comparable to a valuation for a field.

Definition 5.1. Let $(F, +, \cdot)$ be a field with valuation ϕ and let $(V, F, +, \cdot)$ be a linear space over $(F, +, \cdot)$. A real-valued function $\| \cdot \|$ defined on V , is a norm on V if

$$(5.1) \quad \|v\| \geq 0 \text{ and equals } 0 \text{ only if } v = 0,$$

$$(5.2) \quad \|v + w\| \leq \|v\| + \|w\|,$$

$$(5.3) \quad \|av\| = \phi(a) \|v\|$$

for each v and w in V and a in F . If

$$(5.4) \quad \|v + w\| \leq \max(\|v\|, \|w\|)$$

for each v and w in V , then $\| \cdot \|$ is a non-archimedean norm on V .

Definition 5.2. Let $(F, +, \cdot)$ be a field with valuation ϕ and let $(V, F, +, \cdot)$ be a linear space over F with norm $\| \cdot \|$ on V . Then $(V, F, +, \cdot)$ is a normed linear space over $(F, +, \cdot)$. Such a normed linear space is denoted by $(V, F, +, \cdot, \| \cdot \|)$. If $\| \cdot \|$ is non-archimedean, then $(V, F, +, \cdot, \| \cdot \|)$ is a non-archimedean normed linear space over F .

In the study of real vector spaces, the student learns that an n -dimensional vector space can be constructed by taking all n -tuples of real numbers as vectors. This linear space is denoted by $(\mathbb{R}^n, \mathbb{R}, +, \cdot)$. If $\| \cdot \|$ is defined on \mathbb{R}^n such that

$$\|(x_1, x_2, \dots, x_n)\| = \max_{1 \leq i \leq n} |x_i|,$$

then $\| \cdot \|$ is a norm and $(\mathbb{R}^n, \mathbb{R}, +, \cdot, \| \cdot \|)$ is a normed linear space. In a similar way, an n -dimensional linear space over the p -adic numbers can be constructed with n -tuples of p -adic numbers as vectors.

Example 5.3. Let \mathbb{R}_p^n denote the collection of all n -tuples of p -adic numbers. Then $(\mathbb{R}_p^n, \mathbb{R}_p, +, \cdot)$ is an n -dimensional linear space over $(\mathbb{R}_p, +, \cdot)$. If $\| \cdot \|$ is defined on \mathbb{R}_p^n such that

$$(5.6) \quad \|(\xi_1, \xi_2, \dots, \xi_n)\| = \max_{1 \leq i \leq n} |\xi_i|_p,$$

then $\|(\xi_1, \xi_2, \dots, \xi_n)\| \geq 0$ with equality only if $\max_{1 \leq i \leq n} |\xi_i|_p = 0$ and condition (5.1) follows. From

$$\begin{aligned} \|\xi(\xi_1, \xi_2, \dots, \xi_n)\| &= \|(\xi\xi_1, \xi\xi_2, \dots, \xi\xi_n)\| \\ &= \max_{1 \leq i \leq n} |\xi\xi_i|_p \\ &= |\xi|_p \max_{1 \leq i \leq n} |\xi_i|_p, \end{aligned}$$

it follows that property (5.3) is true. The non-archimedean property for $\| \cdot \|$ can be established as follows:

$$\begin{aligned}
 \|(\xi_1, \dots, \xi_n) + (\zeta_1, \dots, \zeta_n)\| &= \|(\xi_1 + \zeta_1, \dots, \xi_n + \zeta_n)\| \\
 &= \max_{1 \leq i \leq n} |\xi_i + \zeta_i|_p \\
 &\leq \max_{1 \leq i \leq n} (\max(|\xi_i|_p, |\zeta_i|_p)) \\
 &= \max\left\{ \max_{1 \leq i \leq n} (|\xi_i|_p, |\zeta_i|_p) \right\} \\
 &\leq \max\{\|(\xi_1, \dots, \xi_n)\|, \|(\zeta_1, \dots, \zeta_n)\|\}.
 \end{aligned}$$

Since the non-archimedean property implies (5.2), it follows that

$(R_p^n, R_p, +, \cdot, \| \cdot \|)$ is a non-archimedean normed linear space of dimension n .

A field can be considered as a linear space over itself. That is $(F, F, +, \cdot)$ is a linear space whenever $(F, +, \cdot)$ is a field. Also $(R, Q, +, \cdot)$ and $(R_p, Q, +, \cdot)$ are linear spaces. If $(F, +, \cdot)$ is a field with valuation ϕ , then $(F, F, +, \cdot, \phi)$ is a normed linear space. Furthermore $(R, Q, +, \cdot, | \cdot |)$ and $(R_p, Q, +, \cdot, | \cdot |_p)$ are normed linear spaces whenever $| \cdot |$ and $| \cdot |_p$ are taken as the respective valuations on $(Q, +, \cdot)$. If $| \cdot |_p$ is the valuation on $(Q, +, \cdot)$, then $(R_p, Q, +, \cdot, | \cdot |_p)$ is a non-archimedean normed linear space. However $(R_p, Q, +, \cdot, | \cdot |_p)$ is not a normed linear space when $| \cdot |$ is the valuation on $(Q, +, \cdot)$. To see this, note that property (5.3) fails in this case since

$$|2p|_p = |p + p|_p \leq \max(|p|_p, |p|_p) = 1/p$$

while

$$|2| |p|_p = 2(1/p) = 2/p.$$

Let $(V, F, +, \cdot, \| \cdot \|)$ be a non-archimedean normed linear space and let ϕ be the valuation on $(F, +, \cdot)$. The following argument shows that ϕ

must be non-archimedean. There exists a non-zero v in V such that

$$\begin{aligned}\phi(x + y) \|v\| &= \|(x + y)v\| \\ &= \|xv + yv\| \\ &\leq \max(\|xv\| + \|yv\|) \\ &= \max(\phi(x)\|v\|, \phi(y)\|v\|) \\ &= \|v\| \max(\phi(x), \phi(y))\end{aligned}$$

whenever x and y are in F . It follows that

$$\phi(x + y) \leq \max(\phi(x), \phi(y))$$

and hence that ϕ is a non-archimedean valuation on $(F, +, \cdot)$. Thus ϕ non-archimedean on $(F, +, \cdot)$ is necessary for $(V, F, +, \cdot, \| \cdot \|)$ to be non-archimedean. To see that this condition is not sufficient for the normed linear space to be non-archimedean, consider the following example which describes a normed linear space over R_p which fails to be non-archimedean.

Example 5.4. Let S denote the set of all sequences $\{\xi_n\}$ of p -adic numbers such that $\sum_{k=0}^{\infty} |\xi_n|_p$ is bounded. Then $(S, R_p, +, \cdot)$ is a linear space. Define $\| \cdot \|$ on S by

$$(5.7) \quad \|\{\xi_n\}\| = \sum_{k=0}^{\infty} |\xi_n|_p.$$

Then $\|\{\xi_n\}\| \geq 0$ with equality only if $\{\xi_n\} = \{0\}$. Since

$$\sum_{n=0}^{\infty} |\xi|_p |\xi_n|_p = |\xi|_p \sum_{n=0}^{\infty} |\xi_n|_p,$$

it follows from (5.7) that $\|\xi\{\xi_n\}\| = |\xi|_p \|\{\xi_n\}\|$. Also

$$\begin{aligned}\|\{\xi_n\} + \{\zeta_n\}\| &= \|\{\xi_n + \zeta_n\}\| \\ &= \sum_{n=0}^{\infty} |\xi_n + \zeta_n|_p\end{aligned}$$

whenever $\{\xi_n\}$ and $\{\zeta_n\}$ are in S . But

$$\sum_{k=0}^n |\xi_k + \zeta_k|_p \leq \sum_{k=0}^n |\xi_k|_p + \sum_{k=0}^n |\zeta_k|_p$$

for each $n \geq 0$ implies that

$$\sum_{n=0}^{\infty} |\xi_n + \zeta_n|_p \leq \sum_{k=0}^{\infty} |\xi_k|_p + \sum_{k=0}^{\infty} |\zeta_k|_p.$$

Therefore

$$\|\{\xi_n\} + \{\zeta_n\}\| \leq \|\{\xi_n\}\| + \|\{\zeta_n\}\|.$$

Hence $\|\cdot\|$ is a norm and $(S, R_p, +, \cdot, \|\cdot\|)$ is a normed linear space. However the non-archimedean property does not hold. To see this, consider

$$\{\xi_n\} = \{1, 0, 0, \dots, 0, \dots\}$$

and

$$\{\zeta_n\} = \{0, 1, 0, 0, \dots, 0, \dots\}.$$

Then

$$\{\xi_n\} + \{\zeta_n\} = \{1, 1, 0, 0, \dots, 0, \dots\}$$

and $\|\{\xi_n\} + \{\zeta_n\}\| = 2$ while the $\max(\|\{\xi_n\}\|, \|\{\zeta_n\}\|) = 1$. Therefore it is not the case that $\|\{\xi_n\} + \{\zeta_n\}\| \leq \max(\|\{\xi_n\}\|, \|\{\zeta_n\}\|)$.

Let $(V, F, +, \cdot, \|\cdot\|)$ be a normed linear space. In a manner analogous to the verification of (3.10) in the proof of Theorem 3.3, it follows that

$$(5.8) \quad \|\|v - w\|\| \leq \|v - w\|$$

for each v and w in V . If $\|\cdot\|$ is non-archimedean, then it follows as in Theorem 3.5 that

$$(5.9) \quad \|v + w\| = \|v\| \text{ whenever } \|v\| > \|w\|.$$

The $\|\cdot\|$ -Topology

If $\|\cdot\|$ is a norm on V , then a function d from $V \times V$ into R defined by

$$d(v,w) = \|v - w\|$$

for each v and w in V is a metric on V . Therefore (V,d) is a metric space. If $\| \cdot \|$ is non-archimedean, then (V,d) is a non-archimedean metric space. Hence the discussion relative to non-archimedean metric spaces in Chapter IV, as well as the discussion of metric spaces in Chapter I, apply to the non-archimedean space $(V, R_p, +, \cdot, \| \cdot \|)$ with the $\| \cdot \|$ -topology. Of particular importance are the ideas of open and closed sets, continuous functions, convergent sequences, Cauchy sequences, and the relationship between open spheres, closed spheres, open sets, and closed sets.

Let $(V, F, +, \cdot, \| \cdot \|_1)$ and $(W, F, +, \cdot, \| \cdot \|_2)$ be two non-archimedean normed linear spaces, and let f be a function from V into W . In accordance with Theorem 1.11, f is continuous on V if and only if for each v in V and for each $\epsilon > 0$ there exists a δ such that

$$\|f(v) - f(w)\|_2 < \epsilon \text{ whenever } \|v - w\|_1$$

with w in V . Let $\{v_n\}$ be a sequence from V . Then $\{v_n\}$ converges to v with respect to $\| \cdot \|_1$ if and only if for each $\epsilon > 0$ there exists an N such that

$$(5.10) \quad \|v_n - v\|_1 < \epsilon \text{ whenever } n \geq N.$$

The sequence $\{v_n\}$ is Cauchy (wrt $\| \cdot \|_1$) if and only if for each $\epsilon > 0$ there exists an N such that

$$(5.11) \quad \|v_m - v_n\|_1 < \epsilon \text{ whenever } m, n \geq N.$$

Furthermore $\{v_n\}$ is Cauchy if and only if for each $\epsilon > 0$ there exists an N such that

$$(5.12) \quad \|v_n - v_{n+1}\|_1 < \epsilon \text{ whenever } n \geq N.$$

As for a series of p -adic numbers, so it follows from (5.12) that an

infinite series $\sum_{k=0}^{\infty} v_k$ has a sum if and only if $v_n \rightarrow 0$ (wrt $\| \cdot \|_1$).

The following useful alternate characterization of continuity is an immediate consequence of the fact that non-archimedean normed linear spaces are metric spaces.

Theorem 5.5. If $(V, F, +, \cdot, \| \cdot \|_1)$ and $(W, F, +, \cdot, \| \cdot \|_2)$ are non-archimedean normed linear spaces and $\{v_n\}$ is a sequence from V , then a function f from V into W is continuous if and only if

$$(5.13) \quad v_n \rightarrow v \text{ (wrt } \| \cdot \|_1) \text{ implies } f(v_n) \rightarrow f(v) \text{ (wrt } \| \cdot \|_2).$$

Let $\{v_n\}$ be a non-null Cauchy sequence of $(V, F, +, \cdot, \| \cdot \|)$, a non-archimedean space. Since $\|v + w\| = \|v\|$ whenever $\|v\| > \|w\|$, it follows as in Theorem 3.18 for $(R_p, +, \cdot)$ that $\{\|v_n\|\}$ is eventually constant. This important consequence of the non-archimedean nature of $\| \cdot \|$ is stated for future reference.

Theorem 5.6. If $\{v_n\}$ is a non-null Cauchy sequence of a non-archimedean normed linear space, then $\{\|v_n\|\}$ is eventually constant.

Any property of normed linear spaces over the real number field which depends only on properties (1.10), (1.11), and (1.12) of $| \cdot |$ and is independent of any special property of the real numbers, such as order, holds true for non-archimedean normed linear spaces. For example, the following theorem states a property of normed linear spaces that is dependent on properties common to any valuated field.

Theorem 5.7. Let $(V, F, +, \cdot, \| \cdot \|_1)$ and $(W, F, +, \cdot, \| \cdot \|_2)$ be two normed linear spaces and let T be a linear function from V into W . Then T is continuous at every point of V or T is continuous at no point of V . In particular, T is continuous on V if and only if T is continuous at 0.

Proof: Let v and w be any two points of V and assume T is continuous at v . Then for each $\varepsilon > 0$ there exists a $\delta > 0$ such that

$$\|T(v) - T(w)\|_2 < \varepsilon \text{ whenever } \|v - w\|_1 < \delta$$

with w in V . If y is an element of V such that $\|y - w\|_1 < \delta$ then

$$\|(w + v - y) - v\|_1 < \delta.$$

Since $w + v - y$ is in V and $T(w + v - y) = T(w) + T(v) - T(y)$, it follows that

$$\|T(y) - T(w)\|_2 = \|T(w + v - y) - T(v)\|_2$$

and

$$\|T(y) - T(w)\|_2 < \varepsilon \text{ whenever } \|y - w\|_1 < \delta.$$

Hence T is continuous at y .

A linear function T from $(V, F, +, \cdot, \| \cdot \|_1)$ into $(W, G, +, \cdot, \| \cdot \|_2)$ is bounded if there is a real number M such that

$$\|T(v)\|_2 \leq M \|v\|_1$$

for each v in V . The norm of T is defined as

$$\|T\| = \inf \{M: \|T(v)\|_2 \leq M \|v\|_1\}.$$

Just as a linear function on a real normed linear space is continuous if and only if it is bounded, so a linear function on any non-archimedean normed linear space over a p -adic number field is continuous if and only if it is bounded. However the proof is more complicated in the p -adic case.

Theorem 5.8. Let $(V, R_p, +, \cdot, \| \cdot \|_1)$ be a non-archimedean normed linear space. A linear function defined on V is continuous if and only if it is bounded.

Proof: Let T be defined from V into W where $(W, R_p, +, \cdot, \| \cdot \|_2)$ is a normed

linear space. Suppose T is a continuous linear function which is not bounded. That is, for each $M > 0$ there exists v in V such that

$$\|T(v)\|_2 > M\|v\|_1.$$

In particular, there exists a sequence $\{v_n\}$ in V and $\{M_n\}$ in \mathbb{R} such that $M_n \rightarrow \infty$ and

$$(5.14) \quad \|T(v_n)\|_2 > M_n\|v_n\|_1.$$

From $p > 0$, it follows that there exists a smallest integer k such that $p^{-k} \leq 1/(M_n\|v_n\|_1)$. Hence for each $n \geq 1$ there exists k such that

$$\frac{1}{p^M\|v_n\|_1} \leq p^{-k} \leq \frac{1}{M_n\|v_n\|_1}.$$

Since

$$|R_p|_p = \{p^{-n} : n \text{ is in } \mathbb{Z}\},$$

there exists a sequence $\{\xi_n\}$ in R_p such that

$$\frac{1}{p^M\|v_n\|_1} \leq \xi_n \leq \frac{1}{M_n\|v_n\|_1}.$$

From (5.14) and the fact that $T(0) = 0$, it follows that $\|v_n\|_1 \neq 0$ for each n . Thus if $y_n = \xi_n v_n$ for each $n > 0$, then $\{y_n\}$ is a sequence in V such that

$$\|y_n\|_1 = |\xi_n|_p\|v_n\|_1 \leq 1/M_n.$$

But $1/M_n \rightarrow 0$ (wrt $|\cdot|_1$). Therefore $y_n \rightarrow 0$ (wrt $\|\cdot\|_1$). Moreover

$$\begin{aligned} \|T(y_n)\|_2 &= \|\xi_n T(v_n)\|_2 = |\xi_n|_p \|T(v_n)\|_2 \\ &\geq \frac{\|T(v_n)\|_2}{p^M\|v_n\|_1} \geq \frac{1}{p} \end{aligned}$$

and $\{T(y_n)\}$ does not converge to 0 with respect to $\|\cdot\|_2$. This is impossible since T is continuous and $y_n \rightarrow 0$ (wrt $\|\cdot\|_1$) implies

$T(y_n) \rightarrow 0$ (wrt $\|\cdot\|_2$). Hence there exists an M such that

$$(5.15) \quad \|T(v)\|_2 \leq M \|v\|_1$$

for each v in V and T is bounded.

Conversely, assume (5.15) holds. Then for each $\varepsilon > 0$ there exists $\delta = \varepsilon/M$ such that

$$\|T(v) - T(0)\|_2 < \varepsilon \text{ whenever } \|v - 0\|_1 < \delta$$

and T is continuous at 0 . Hence T is continuous on V .

Discrete Non-Archimedean Normed Linear Spaces

A normed linear space is discrete if the norm is discrete. That is, a normed space is discrete if zero is the only accumulation point of the image of the set of vectors under the norm function. The next example indicates that there are discrete normed linear spaces.

Example 5.8. Let $(R_p^n, R_p, +, \cdot, \|\cdot\|)$ be as in Example 5.3 and let $\{(\xi_1^{(m)}, \xi_2^{(m)}, \dots, \xi_n^{(m)})\}$ be a Cauchy (wrt $\|\cdot\|$) sequence in R_p^n . For each $\varepsilon > 0$ there exists an M such that

$$\|(\xi_1^{(m+1)} - \xi_1^{(m)}, \dots, \xi_n^{(m+1)} - \xi_n^{(m)})\| < \varepsilon$$

whenever $m \geq M$. It follows that

$$\max_{1 \leq i \leq n} |\xi_i^{(m+1)} - \xi_i^{(m)}|_p < \varepsilon$$

and hence that

$$|\xi_i^{(m+1)} - \xi_i^{(m)}|_p < \varepsilon \text{ whenever } m > M$$

for each i , $1 \leq i \leq n$. Now $(R_p, +, \cdot)$ discrete and $\{\xi_i^{(m)}\}$ Cauchy (wrt $|\cdot|_p$) for each i , $1 \leq i \leq n$, implies that for any given i , $|\xi_i^{(m)}|_p \rightarrow 0$ (wrt $|\cdot|_p$) or $\{|\xi_i^{(m)}|_p\}$ is eventually constant. There are two cases. If for each i , $1 \leq i \leq n$,

$$|\xi_i^{(m)}|_p \rightarrow 0 \text{ (wrt } |\cdot|),$$

then $\|(\xi_1^{(m)}, \xi_2^{(m)}, \dots, \xi_n^{(m)})\| \rightarrow 0$ (wrt $|\cdot|$). If there exists some i such that $|\xi_i^{(m)}|_p$ is eventually constant and non-zero, then

$$\|(\xi_1^{(m)}, \xi_2^{(m)}, \dots, \xi_n^{(m)})\| = \max_{1 \leq i \leq n} |\xi_i^{(m)}|_p \text{ is eventually constant.}$$

Thus no non-zero element of $\|R_p^n\|$ is an accumulation point. However 0 is an accumulation point of $\|R_p^n\|$ since $\{\|(p^n, 0, \dots, 0)\|\}$ converges to 0 (wrt $|\cdot|$). Hence $(R_p^n, R_p, +, \cdot, \|\cdot\|)$ is a discrete normed linear space.

The scalar field in Example 5.8 is discrete as the next theorem shows that it must be. However there are non-archimedean normed linear spaces over discrete fields which are not discrete.

Theorem 5.9. A necessary but not sufficient condition for a non-archimedean normed linear space $(V, F, +, \cdot, \|\cdot\|)$ to be discrete is that $(F, +, \cdot)$ is discrete.

Proof: If $(F, +, \cdot)$ is not discrete, then there exists a sequence $\{\phi(\xi_n)\}$ of distinct values in $(R, +, \cdot)$ such that $\phi(\xi_n) \rightarrow r \neq 0$ (wrt $|\cdot|$). Since $V \neq \{0\}$, there exists v in V such that $\|v\| \neq 0$. Therefore $\{\xi_n v\}$ is a sequence in V such that

$$\|\xi_n v\| = \phi(\xi_n) \|v\|$$

for each $n \geq 0$. Hence $\|\xi_n v\| \rightarrow r \|v\| \neq 0$ (wrt $|\cdot|$) and $(V, F, +, \cdot, \|\cdot\|)$ is not discrete. It follows that if $(V, F, +, \cdot, \|\cdot\|)$ is discrete, then $(F, +, \cdot)$ is a discrete field. The following example shows that the condition is not sufficient.

Example 5.10. Let V consist of the sequences $\{x_n\} = \{\sum_{i=0}^n a_i p^{r+i}\}$ with $0 \leq a < p$ and r a rational number. Define addition and multiplication on V such that

$$\{x_n\} + \{y_n\} = \{x_n + y_n\}$$

and

$$\{x_n\} \{y_n\} = \{x_n y_n\}$$

for each $\{x_n\}$ and $\{y_n\}$ in V . It is clear from the definition of addition and multiplication of p -adic numbers and Theorem 2.42 that $(V, +, \cdot)$ contains a subfield $(K, +, \cdot)$ isomorphic to $(R_p, +, \cdot)$. Furthermore $(V, K, +, \cdot)$ is a linear space. Let $\| \cdot \|$ from V into R be defined by

$$\begin{aligned} \left\| \left\{ \sum_{i=0}^n a_i p^{r+i} \right\} \right\| &= p^{-r-k} \text{ if } k \text{ is the least integer such that } a_k \neq 0 \\ &= 0 \text{ if } a_k = 0 \text{ for each } k \geq 0. \end{aligned}$$

As for $| \cdot |_p$ in Chapter II, so $\| \cdot \|$ can be shown to be a non-archimedean norm on $(V, +, \cdot)$ and hence a valuation on $(K, +, \cdot)$. The valuated field $(K, +, \cdot)$ is discrete. It remains to show that $(V, K, +, \cdot, \| \cdot \|)$ is not discrete. Let p^{-r-k} be a non-zero element of $\|V\|$. Then

$$\left\{ \frac{n}{n+1} r + k \right\}$$

is a sequence of distinct rational numbers which converges to $r+k$.

Since the function f defined by $f(x) = p^x$ is continuous,

$$\left\{ p^{\frac{n}{n+1} r + k} \right\}$$

is a sequence of distinct terms that converges to p^{-r-k} . Hence p^{-r-k} is a non-zero accumulation point of $\|V\|$ and $(V, K, +, \cdot, \| \cdot \|)$ is not discrete.

It has been observed that $(R_p^n, R_p, +, \cdot, \| \cdot \|)$ with $\| \cdot \|$ as in (5.6) is a discrete normed linear space and that the $\| \cdot \|$ -topology is not the discrete topology. Therefore the metric topology for a linear space induced by a discrete non-archimedean norm does not need to be the discrete topology for the space.

Topological Linear Spaces

A normed linear space has both a topological and an algebraic structure. There is an interesting relation between the metric topology for a linear space determined by a norm and the algebraic operations defined on the set of vectors. Some consequences of this relation are explored in this section.

Let $(V, R_p, +, \cdot, \| \cdot \|)$ be non-archimedean. Since $\| \cdot \|$ determines a non-archimedean metric for V , it follows from Theorem 4.26 that $\| \cdot \|$ determines a topology for $V \times V$. Furthermore $\| \cdot \|$ and $| \cdot |_p$ together determine a topology for $R_p \times V$.

Definition 5.11. A linear space $(V, R_p, +, \cdot)$ is a topological linear space if vector addition is a continuous function on $V \times V$ and scalar multiplication is a continuous function on $R_p \times V$.

For each x, y, z , and w in V ,

$$\begin{aligned} \|x + y - (w + z)\| &= \|x - w + y - z\| \\ &\leq \max(\|x - w\|, \|y - z\|). \end{aligned}$$

Hence vector addition is a continuous function on $V \times V$. Let D be the metric on $R_p \times V$ induced by $| \cdot |_p$ and $\| \cdot \|$. That is,

$$D((\xi, x), (\zeta, y)) = \max(|\xi - \zeta|_p, \|x - y\|).$$

Then for each (ξ, x) and (ζ, y) in $R_p \times V$,

$$\begin{aligned} \|\xi x - \zeta y\| &= \|\xi x - \xi y + \xi y - \zeta y\| \\ &= \|\xi(x - y) + (\xi - \zeta)y\| \\ &\leq \max(\|\xi(x - y)\|, \|(\xi - \zeta)y\|) \\ &= \max(|\xi|_p \|x - y\|, |\xi - \zeta|_p \|y\|) \\ &\leq \max(|\xi|_p, \|y\|) \max(|\xi - \zeta|_p, \|x - y\|) \\ &= \max(|\xi|_p, \|y\|) D((\xi, x), (\zeta, y)) \end{aligned}$$

Also $\|x - y\| < 1$ implies that $\|y\| < 1 + \|x\|$. It follows that for each $\varepsilon > 0$ there exists

$$\delta = \min \left(1, \frac{\varepsilon}{|\xi|_p (\|x\| + 1)} \right)$$

such that $\|\xi x - \zeta y\| < \varepsilon$ whenever $D((\xi, x), (\zeta, y)) < \delta$. Therefore scalar multiplication is also continuous. Hence non-archimedean normed linear spaces over $(R_p, +, \cdot)$ are topological linear spaces.

Definition 5.14. Two topological linear spaces over the same scalar field are topologically isomorphic if there exists a vector space isomorphism f between the two spaces such that both f and f^{-1} are continuous.

Any n -dimensional normed linear space over the real field is topologically isomorphic to $(R^n, R, +, \cdot, \|\ \|)$ where

$$\|(x_1, x_2, \dots, x_n)\| = |x_1| + |x_2| + \dots + |x_n|$$

for each (x_1, x_2, \dots, x_n) in R^n . A similar result holds true for n -dimensional non-archimedean normed linear spaces over R_p . The following sequence of theorems, due to Cohen (5), culminates with this interesting result and provides additional insight into the nature of non-archimedean normed linear spaces over $(R_p, +, \cdot)$.

Theorem 5.15. Let $(V, R_p, +, \cdot, \|\ \|)$ be non-archimedean, let $(W, R_p, +, \cdot, \|\ \|)$ be a closed subspace, and let v be a vector in V which is not in W . If the sequence $\{w_n + \xi_n v\}$ converges (wrt $\|\ \|$) to a vector in V , where w_n is in W and ξ_n is in R_p , then both $\{w_n\}$ and $\{\xi_n\}$ have limits.

Proof: Assume that $\{w_n + \xi_n v\}$ converges (wrt $\|\ \|$) to 0 and that $\{\xi_n\}$ does not converge (wrt $|\ \ |_p$) to 0. Then there exists a subsequence

$\{\xi_{n_k}\}$ and an $\varepsilon > 0$ such that for each k , $|\xi_{n_k}|_p \geq \varepsilon$. Hence

$$\begin{aligned} \|\xi_{n_k}^{-1}(w_{n_k} + \xi_{n_k}v)\| &= |\xi_{n_k}^{-1}|_p \|w_{n_k} + \xi_{n_k}v\| \\ &\leq (1/\varepsilon) \|w_{n_k} + \xi_{n_k}v\|. \end{aligned}$$

But for each $\varepsilon > 0$ there exists an N such that

$$\|w_{n_k} + \xi_{n_k}v\| < \varepsilon^2 \text{ whenever } k \geq N.$$

Consequently

$$\|\|\xi_{n_k}^{-1}w_{n_k}\| - \|-v\|\| \leq \|\|\xi_{n_k}^{-1}w_{n_k} + v\|\| < \varepsilon \text{ whenever } k \geq N$$

and $\{\xi_{n_k}^{-1}w_{n_k}\}$ converges to $-v$. But this is impossible since W is closed and $-v$ is not in W . Therefore it follows that if $\{w_n + \xi_n v\}$ converges to 0, then $\{\xi_n\}$ is a null sequence of p -adic numbers.

To complete the proof, suppose that the sequence $\{w_n + \xi_n v\}$ converges (wrt $\|\cdot\|$) but not necessarily to 0. Then $\{w_n + \xi_n v\}$ is Cauchy and for each $\varepsilon > 0$ there exists an N such that

$$\|w_{n+1} + \xi_{n+1}v - w_n - \xi_n v\| < \varepsilon \text{ whenever } n \geq N.$$

Therefore

$$\|w_{n+1} - w_n + (\xi_{n+1} - \xi_n)v\| < \varepsilon \text{ whenever } n \geq N$$

and it follows from the first part of the proof that $\{\xi_{n+1} - \xi_n\}$ converges to 0. Hence $\{\xi_n\}$ is Cauchy. Since $(R_p, +, \cdot)$ is complete, there exists a ξ in R_p such that for each $\varepsilon > 0$ there exists an N_1 such that

$$\|\xi_n v - \xi v\| < \varepsilon \text{ whenever } n \geq N_1.$$

By hypothesis, $\{w_n + \xi_n v\}$ converges to some vector, say z , in V . Hence there exists an N_2 such that

$$\|w_n + \xi_n v - z\| < \varepsilon \text{ whenever } n \geq N_2.$$

Since

$$\begin{aligned} \|w_n - (z - \xi v)\| &= \|w_n + \xi_n v - z - \xi_n v + \xi v\| \\ &\leq \max(\|w_n + \xi_n v - z\|, \|\xi_n v - \xi v\|), \end{aligned}$$

it follows that $w_n \rightarrow z - \xi v$ (wrt $\|\cdot\|$). Therefore both $\{w_n\}$ and $\{\xi_n\}$ have limits.

Theorem 5.16. Let $(V, R_p, +, \cdot, \|\cdot\|)$ be non-archimedean. If W is a closed subset of V and v_1, v_2, \dots, v_m are elements of V , then

$W + R_p v_1 + \dots + R_p v_m$ is closed. In particular, any finite dimensional subspace of $(V, R_p, +, \cdot, \|\cdot\|)$ is closed.

Proof: The proof is by induction on m . Suppose $m = 1$. If v_1 is in W , then $W + R_p v_1 = W$ and hence is closed. Assume v_1 is not in W but is in V and that z is an accumulation point of $W + R_p v_1$. Thus there exists a sequence of $\{w_n + \xi_n v_1\}$ in $W + R_p v_1$ that converges to z . Hence $\{w_n\}$ has limit w and $\{\xi_n\}$ has limit ξ in R_p . Since W is closed, w is in W . Therefore $\{w_n + \xi_n v_1\}$ converges to $w + \xi v_1$ in $W + R_p v_1$. But in a metric space limits are unique and therefore $z = w + \xi v_1$. It follows that $W + R_p v_1$ contains z and is hence closed.

To complete the induction, assume $G = W + R_p v_1 + \dots + R_p v_m$ is closed and v is in V but not in G . Let y be an accumulation point of $G + R_p v$. Then there exists a sequence $\{g_n + \xi_n v\}$ in $G + R_p v$ converging to y . By the same reasoning as before, $G + R_p v = W + R_p v_1 + \dots + R_p v_m + R_p v$ contains y and therefore is closed. Hence for each $m \geq 0$, $W + R_p v_1 + \dots + R_p v_m$ is closed. Since $\{0\}$ is a closed subset of V , it follows that $R_p v_1 + \dots + R_p v_m$ is closed. That is, any finite dimensional subspace of $(V, R_p, +, \cdot, \|\cdot\|)$ is closed.

Theorem 5.17. Any n -dimensional non-archimedean normed linear space

over $(R_p, +, \cdot)$ is topologically isomorphic to $(R_p^n, R_p, +, \cdot, \|\cdot\|)$ and is complete.

Proof: Let $(V, R_p, +, \cdot, \|\cdot\|_1)$ be non-archimedean and recall that

$$\|(\xi_1, \xi_2, \dots, \xi_n)\| = \max_{1 \leq i \leq n} |\xi_i|_p$$

for each $(\xi_1, \xi_2, \dots, \xi_n)$ in R_p^n . Suppose that $\{v_1, v_2, \dots, v_n\}$ is a basis for $(V, R_p, +, \cdot, \|\cdot\|_1)$. Define a function T from R_p^n into V such that

$$T((\xi_1, \xi_2, \dots, \xi_n)) = \sum_{i=1}^n \xi_i v_i.$$

Since

$$\sum_{i=1}^n \xi_i v_i = \sum_{i=1}^n \zeta_i v_i$$

implies $\xi_i = \zeta_i$ for $i, 1 \leq i \leq n$, it follows that T is well-defined.

It is clear that T is linear and onto. Since $\sum_{i=1}^n \xi_i v_i \neq \sum_{i=1}^n \zeta_i v_i$ implies $\sum_{i=1}^n (\xi_i - \zeta_i) v_i \neq 0$ and $\sum_{i=1}^n (\xi_i - \zeta_i) v_i \neq 0$ implies there exists i such that $\xi_i \neq \zeta_i$, it follows that $T(\xi_1, \xi_2, \dots, \xi_n) \neq T(\zeta_1, \zeta_2, \dots, \zeta_n)$ implies that $(\xi_1, \xi_2, \dots, \xi_n) \neq (\zeta_1, \zeta_2, \dots, \zeta_n)$ and hence that T is 1-1. Therefore T is an isomorphism and T^{-1} exists.

Let $\{T(\xi_1^{(m)}, \xi_2^{(m)}, \dots, \xi_n^{(m)})\} = \{\sum_{i=1}^n \xi_i^{(m)} v_i\}$ be a sequence in V that converges to 0 with respect to $\|\cdot\|_1$ -topology. With $W = R_p v_1 + \dots + R_p v_{n-1}$ and $v = v_n$, it follows as in the proof of Theorem 5.15 that $\{\xi_n^{(m)}\}$ converges to 0 in R_p and $\{\sum_{i=1}^{n-1} \xi_i^{(m)} v_i\}$ converges to 0 in V . By repeating the argument $n-1$ times, it is clear that $\{\xi_i^{(m)}\}$ converges to 0 for $i, 1 \leq i \leq n$. Hence $T(\xi_1^{(m)}, \xi_2^{(m)}, \dots, \xi_n^{(m)}) \rightarrow 0$ (wrt $\|\cdot\|_1$) implies that $T^{-1}(T(\xi_1^{(m)}, \xi_2^{(m)}, \dots, \xi_n^{(m)})) \rightarrow 0$ (wrt $\|\cdot\|$) and therefore that T^{-1} is continuous.

To see that $(R_p^n, R_p, +, \cdot, \|\cdot\|)$ is complete, let

$$\{x_n\} = \{(\xi_1^{(m)}, \xi_2^{(m)}, \dots, \xi_n^{(m)})\}$$

be a Cauchy (wrt $\|\cdot\|$) sequence of R_p^n . Then for each $\epsilon > 0$ there exists

an N such that

$$\|x_{m+1} - x_m\| = \max_{1 \leq i \leq n} |\xi_i^{(m+1)} - \xi_i^{(m)}|_p < \varepsilon \text{ whenever } m \geq N.$$

Hence for each i , $1 \leq i \leq n$,

$$|\xi_i^{(m+1)} - \xi_i^{(m)}|_p < \varepsilon \text{ whenever } m \geq N$$

and $\{\xi_i^{(m)}\}$ is Cauchy (wrt $|\cdot|_p$). Since $(R_p, +, \cdot)$ is complete, there exists $\hat{\xi}_i$ such that $\xi_i^{(m)} \rightarrow \hat{\xi}_i$ (wrt $|\cdot|_p$). Now $\hat{x} = (\hat{\xi}_1, \hat{\xi}_2, \dots, \hat{\xi}_n)$ is in R_p^n . Furthermore

$$\|x_m - \hat{x}\| = \max_{1 \leq i \leq n} |\xi_i^{(m)} - \hat{\xi}_i| < \varepsilon$$

whenever $m \geq N$, $x_n \rightarrow \hat{x}$ (wrt $\|\cdot\|$), and $(R_p^n, R_p, +, \cdot, \|\cdot\|)$ is complete.

Corollary 5.18. Two non-archimedean normed linear spaces of the same finite dimension are topologically isomorphic.

Extension of Linear Functions

Let $(W, F, +, \cdot, \|\cdot\|_2)$ and $(V, F, +, \cdot, \|\cdot\|_1)$ be two normed linear spaces. Assume that $(W_0, F, +, \cdot, \|\cdot\|_2)$ is a subspace of $(W, F, +, \cdot, \|\cdot\|_2)$ and that T_0 is a linear function from W_0 into V . Then T from W into V is an extension of T_0 if T is linear, $\|T\| = \|T_0\|$, and $T(w) = T_0(w)$ for each w in W_0 . Every continuous linear functional defined on a subspace of a normed linear space can be extended to the whole space so that it remains linear and continuous and has the same norm. This result is known as the Hahn-Banach theorem. The extension of continuous linear functions between two real normed linear spaces has been studied by Nachbin (13). In his paper, Nachbin gives a necessary and sufficient condition for such an extension to be possible. Cohen (5) and Ingleton (7) have studied extension problems for non-archimedean normed linear

spaces. Their results are summarized in the remainder of this chapter.

Definition 5.19. A normed linear space $(V, F, +, \cdot, \| \cdot \|_1)$ is said to have the extension property if, for any space $(W, F, +, \cdot, \| \cdot \|_2)$, every continuous linear function from a subspace of $(W, F, +, \cdot, \| \cdot \|_2)$ into $(V, F, +, \cdot, \| \cdot \|_1)$ possesses an extension of the same norm whose domain is the whole of W .

Definition 5.20. A valuated field $(F, +, \cdot)$ is said to have the Hahn-Banach property if, for any space $(V, F, +, \cdot, \| \cdot \|_1)$, every continuous linear functional defined on a subspace of $(V, F, +, \cdot, \| \cdot \|_1)$ possesses an extension of the same norm defined on the whole of V .

The first step in the consideration of the extension properties of continuous linear functions into non-archimedean normed linear spaces is a general result that is dependent upon Zorn's Lemma.

Zorn's Lemma. Let P be a non-empty partially ordered set with the property that every completely ordered subset of P has an upper bound in P . Then P contains at least one maximal element.

Theorem 5.21. Let $(V, F, +, \cdot, \| \cdot \|_1)$ and $(W, F, +, \cdot, \| \cdot \|_2)$ be non-archimedean, let $(M, F, +, \cdot, \| \cdot \|_2)$ be a proper subspace of $(W, F, +, \cdot, \| \cdot \|_2)$, and let v be in W but not in M . Then if f is a continuous linear function from M into V that can be extended to a continuous linear function with norm $\|f\|$ and defined on $M + Fv$, f can be extended to a continuous linear function that is defined on all of W and has norm $\|f\|$.

Proof: Let D_g denote the domain of a function g into V . Define P to be the set of all continuous linear functions g such that

$(D_g, F, +, \cdot, \| \cdot \|_2)$ is a subspace of $(M + Fv, F, +, \cdot, \| \cdot \|_2)$, $g(x) = f(x)$ for

for each x in M and $\|g\| = \|f\|$. Since f is in P , P is not empty. Define a partial ordering $>$ on P as follows: For g_1 and g_2 in P , $g_1 > g_2$ if and only if D_{g_1} contains D_{g_2} and $g_1(x) = g_2(x)$ for each x in D_{g_2} .

Let Q be a completely ordered subset of P . An upper bound for Q can be constructed as follows: Suppose G is a function into V such that D_G is the union of the domain of all functions in Q and for each x in D_G , $G(x) = g(x)$ where g is some function of Q such that x is in D_g . Since for each x and y in D_G there exists g_1 and g_2 with x in D_{g_1} and y in D_{g_2} and since $g_1 > g_2$ or $g_2 > g_1$, it follows that $x = y$ implies $G(x) = G(y)$ and hence that G is well-defined. It is clear that G is an upper bound for Q .

To apply Zorn's Lemma, it remains to prove that G is in P . If x and y are elements of D_G , then there is a g in P such that x and y are in D_g . Hence for each α in F , αx and $x - y$ are in D_g . This implies that αx and $x - y$ are in D_G and consequently that $(D_G, F, +, \cdot, \| \cdot \|_2)$ is a subspace of $(M + Fx, F, +, \cdot, \| \cdot \|_2)$. Also for α and β in F ,

$$\begin{aligned} G(\alpha x + \beta y) &= g(\alpha x + \beta y) \\ &= \alpha g(x) + \beta g(y) \\ &= \alpha G(x) + \beta G(y) \end{aligned}$$

implies that G is linear. Since G extends f , it follows from Definition 5.9 that $\|G\| \geq \|f\|$. But for each x in D_G the fact that there exists a g in P such that $G(x) = g(x)$ implies

$$(5.19) \quad \|G(x)\|_1 = \|g(x)\|_1 \leq \|g\| \|x\|_2 = \|f\| \|x\|_2.$$

Therefore $\|G\| \leq \|f\|$ and hence $\|G\| = \|f\|$. It follows from (5.19) and Theorem 5.12 that G is also a continuous linear function. Thus G is in P and from Zorn's Lemma it is known that P has at least one maximal element. Let ϕ be a maximal element of P . If D_ϕ is not all of W , then

there is a w in W which is not in D_ϕ . Hence ϕ can be extended to all of $D_\phi + Fw$ and ϕ is not maximal. Since this is a contradiction, $D_\phi = W$, ϕ extends f , $\|\phi\| = \|f\|$, and ϕ is a continuous linear function.

The Hahn-Banach theorem for a non-archimedean normed linear space over any p -adic number field is a corollary to the following theorem:

Theorem 5.22. (5) Let $(F, +, \cdot)$ be a discrete field with non-trivial valuation ψ . Then $(F, +, \cdot)$ has the Hahn-Banach property.

Proof: Let $(W, F, +, \cdot, \|\cdot\|)$ be non-archimedean, let $(M, F, +, \cdot, \|\cdot\|)$ be a subspace of $(W, F, +, \cdot, \|\cdot\|)$ and let f be a linear functional on M . It follows from Theorem 5.21 that it is sufficient to prove the theorem when $V = W + R_p v$. Let x be an element of the closure of W . Then there exists a sequence $\{x_n\}$ such that $x_n \rightarrow x$ (wrt $\|\cdot\|$). Define g by

$$g(x) = \lim f(x_n).$$

It is clear that g is linear and extends f to the closure of W .

Furthermore $f(x_n) \rightarrow g(x)$ (wrt ψ) and since F is discrete either $\psi(f(x_n))$ is eventually constant or $g(x) = 0$. Either way, for each x in the closure of W there exists x_N in W such that $\psi(g(x)) = \psi(f(x_N))$. It follows that $\|g\| \leq \|f\|$. But g an extension of f implies $\|f\| \leq \|g\|$. Hence $\|f\| = \|g\|$ and g is continuous. Therefore it is sufficient to prove the theorem when $V = W + Fv$ and W is closed.

If W is closed, then there exists $\epsilon > 0$ such that

$\{x \text{ in } V: \|x - v\| \leq \epsilon\}$ does not intersect W . If d is defined by

$$(5.20) \quad d = \inf \{\|x - v\|: x \text{ in } W\},$$

then $d \geq \epsilon > 0$. Let k be the unique integer such that

$$(5.21) \quad \|f\|^{-1} p^{k-1} \leq d < \|f\|^{-1} p^k$$

with p some prime number. From (5.20) and (5.21), it follows that

there is \hat{x} in W such that $\|\hat{x} - v\| < \|f\|^{-1}p^k$. Otherwise $\|x - v\| \geq \|f\|^{-1}p^k$ for each x in W and d is not the greatest lower bound. Let $\hat{v} = v - \hat{x}$. Then

$$(5.22) \quad \|\hat{v}\| = \|v - \hat{x}\| < \|f\|^{-1}p^k$$

and since $x + \hat{x}$ is in W whenever x is,

$$(5.23) \quad \|\hat{v} - x\| = \|v - (\hat{x} + x)\| \geq d$$

for all x in W .

If z is in V , then $z = x + \xi v$ with x in W and ξ in F . Therefore

$$z = x + \xi v = x + \xi \hat{x} + \xi \hat{v} = w + \xi \hat{v}$$

with $w = x + \xi \hat{x}$ in W and ξ in F . Define ϕ from V into F such that

$$\phi(z) = \phi(w + \xi \hat{v}) = f(w)$$

for each z in V . It is clear that ϕ extends f . Since

$$\begin{aligned} \phi(\lambda z_1 + \mu z_2) &= \phi(\lambda(w_1 + \xi \hat{v}) + \mu(w_2 + \xi \hat{v})) \\ &= \phi(\lambda w_1 + \mu w_2 + \xi(\lambda + \mu)\hat{v}) \\ &= f(\lambda w_1 + \mu w_2) \\ &= \lambda f(w_1) + \mu f(w_2) \\ &= \lambda \phi(z_1) + \mu \phi(z_2), \end{aligned}$$

ϕ is linear and therefore is a linear functional.

It remains to show that $\|\phi\| = \|f\|$. Since ϕ extends f , $\|\phi\| \geq \|f\|$. If $\|w\| > \|\xi \hat{v}\|$, then it follows from (5.9) that $\|w + \xi \hat{v}\| = \|w\|$. Also if $\|w\| < \|\xi \hat{v}\|$, then $\|w + \xi \hat{v}\| = \|\xi \hat{v}\| > \|w\|$. Therefore $\|w\| \leq \|w + \xi \hat{v}\|$ whenever $\|w\| \neq \|\xi \hat{v}\|$. It follows that for each z in V ,

$$\begin{aligned} \psi(\phi(z)) &= \psi(\phi(w + \xi \hat{v})) \\ &= \psi(f(w)) \\ &\leq \|f\| \|w\| \\ &\leq \|f\| \|w + \xi \hat{v}\| \end{aligned}$$

$$\leq \|f\| \|z\|.$$

That is, $\psi(\phi(z)) \leq \|f\| \|z\|$ for each z in V whenever $\|w\| \neq \|\xi\hat{v}\|$. If $\|w\| = \|\xi\hat{v}\|$, then $\|\xi^{-1}w\| = \|\hat{v}\| < \|f\|^{-1}p^k$ by (5.22). Hence $\psi(f(\xi^{-1}w)) \leq \|f\| \|\xi^{-1}w\| < p^k$. It follows from the discrete nature of $(F, +, \cdot)$ and linearity of f that $\psi(f(w)) \leq \psi(\xi)p^{k-1}$ and that for each z in V ,

$$\begin{aligned}\psi(\phi(z)) &= \psi(f(w)) \leq \psi(\xi)p^{k-1} \\ &\leq \psi(\xi)\|f\|d\end{aligned}$$

by (5.21). But $\xi^{-1}w$ in W implies $d \leq \|\hat{v} + \xi^{-1}w\|$ and consequently that

$$\begin{aligned}\psi(\phi(z)) &\leq \psi(\xi)\|f\|\|\hat{v} + \xi^{-1}w\| \\ &= \|f\|\|w + \xi\hat{v}\| \\ &= \|f\|\|z\|\end{aligned}$$

for each z in V whenever $\|w\| = \|\xi\hat{v}\|$. Therefore for each z in V

$$\psi(\phi(z)) \leq \|f\| \|z\|$$

and $\|\phi\| \leq \|f\|$.

Corollary 5.23. (Hahn-Banach Theorem) Every continuous linear functional defined on a linear subspace of a p -adic normed linear space can be extended to the whole space so that it remains linear and continuous and has the same norm.

Corollary 5.24. Let $(V, R_p, +, \cdot, \|\cdot\|_1)$ be a non-archimedean normed linear space over R_p . Then for each non-zero v in V there is a linear functional f on V such that $f(v) = 1$ and $\|f\| = \|v\|_1^{-1}$.

Proof: Define g from $R_p v$ into R_p such that for each ξv in $R_p v$

$$g(\xi v) = \xi.$$

Since

$$\begin{aligned}g(\lambda(\xi v) + \mu(\zeta v)) &= g((\lambda\xi)v + (\mu\zeta)v) \\ &= g((\lambda\xi + \mu\zeta)v)\end{aligned}$$

$$\begin{aligned}
 &= \lambda \xi + \mu \zeta \\
 &= \lambda g(\xi v) + \mu g(\zeta v),
 \end{aligned}$$

g is linear. Also for each ξv in $R_p v$.

$$|g(\xi v)|_p = |\xi|_p = \frac{\|\xi v\|_1}{\|v\|_1}$$

and $\|g\| \leq \|v\|_1^{-1}$. But

$$|g(v)|_p = |1|_p = 1 = \|v\|_1^{-1} \|v\|_1$$

implies $\|g\| \geq \|v\|_1^{-1}$. Hence $\|g\| = \|v\|_1^{-1}$. By Theorem 5.22, there exists f extending g such that $\|f\| = \|v\|_1^{-1}$. It is clear that $f(v) = 1$.

The following theorem provides a converse to Theorem 5.22.

Theorem 5.25. (7) If the Hahn-Banach Theorem holds in a normed linear space $(V, R_p, +, \cdot, \| \cdot \|)$ then $\| \cdot \|$ is a non-archimedean norm.

Proof: From Corollary 5.24, it follows that if the Hahn-Banach Property holds for $(V, R_p, +, \cdot, \| \cdot \|)$, then there is a linear functional f from V into R_p such that for each x and y in V with $x + y \neq 0$

$$|f(x + y)|_p = |1|_p = 1 = \|f\| \|x + y\|.$$

But

$$\begin{aligned}
 |f(x + y)|_p &= |f(x) + f(y)|_p \leq \max(|f(x)|_p, |f(y)|_p) \\
 &\leq \max(\|f\| \|x\|, \|f\| \|y\|) \\
 &= \|f\| \max(\|x\|, \|y\|).
 \end{aligned}$$

Therefore $\|x + y\| \leq \max(\|x\|, \|y\|)$ and $\| \cdot \|$ is non-archimedean.

Cohen published Theorem 5.22 in 1948. In 1950, Nachbin showed that a real linear space has the extension property if and only if it, considered as a metric space, is spherically complete. Two years later

Ingleton proved the following analog to Nachbin's result for non-archimedean normed linear spaces.

Theorem 5.25. (7) A non-archimedean normed linear space $(V, F, +, \cdot, \| \cdot \|_1)$ has the extension property if and only if the non-archimedean metric space (V, d) with $d(v, w) = \|v - w\|_1$ is spherically complete.

Proof: Since $(V, F, +, \cdot, \| \cdot \|_1)$ is non-archimedean, the valuation ϕ on F is non-archimedean. Assume that $(W, F, +, \cdot, \| \cdot \|_2)$ is non-archimedean and that $(M, F, +, \cdot, \| \cdot \|_2)$ is a proper subspace. Suppose the metric space (V, d) is spherically complete. Let T be a continuous linear function from M into V and let x_0 be a vector in W but not in M .

To prove that T can be extended to $M + Fx_0$, consider the collection of closed spheres indexed by M such that for each y in M

$$S[y] = S[T(y), \rho(y)] = \{z: z \in V \text{ and } \|T(y) - z\|_1 \leq \rho(y)\}$$

where $\rho(y) = \|T\| \|y - x_0\|_2$. Since

$$\begin{aligned} \|T(y_1) - T(y_2)\|_1 &= \|T(y_1 - y_2)\|_1 \\ &\leq \|T\| \|y_1 - y_2\|_2 \\ &= \|T\| \|y_1 - x_0 + x_0 - y_2\|_2 \\ &\leq \|T\| \max(\|y_1 - x_0\|_2, \|y_2 - x_0\|_2) \\ &= \max(\rho(y_1), \rho(y_2)), \end{aligned}$$

$T(y_1)$ is in $S[y_2]$ or $T(y_2)$ is in $S[y_1]$. Hence any two of the spheres intersect. Since (V, d) is a non-archimedean metric space, it follows from Theorem 4.21 that the set of spheres is a nest. Since (V, d) is spherically complete there exists a point z_0 in $S[y]$ for each y in M .

For any $x = y + \nu z_0$ in $M + Fz_0$, define L from $M + Fz_0$ into V such that

$$L(x) = L(y + \nu z_0) = T(y) + \nu z_0.$$

Clearly L is well-defined. Since

$$\begin{aligned} L(\lambda x_1 + \mu x_2) &= T(\lambda y_1 + \lambda y_2) + (\nu_1 \lambda + \nu_2 \mu) z_0 \\ &= \lambda(T(y_1) + \nu_1 z_0) + \mu(T(y_2) + \nu_2 z_0) \\ &= \lambda L(x_1) + \mu L(x_2), \end{aligned}$$

L is linear. For each y in M , $y = y + 0 \cdot z_0$, $L(y) = T(y)$ and L extends T . Also if $\nu \neq 0$, then

$$\begin{aligned} \|L(x)\|_1 &= \|T(y) + \nu z_0\|_1 \\ &= \phi(\nu) \|\nu^{-1} T(y) + z_0\|_1 \\ &= \phi(\nu) \|T(-\nu^{-1}y) - z_0\|_1. \end{aligned}$$

But y in M implies $-\nu^{-1}y$ is an element of M . Hence z_0 is an element of $S[(-\nu^{-1}y)]$. Therefore $\|T(-\nu^{-1}y) - z_0\|_1 \leq \rho(-\nu^{-1}y)$ and

$$\|L(x)\|_1 \leq \phi(\nu) \rho(-\nu^{-1}y).$$

Since $\rho(-\nu^{-1}y) = \|T\| \|\nu^{-1}y - z_0\|_2 = \|T\| \|(\nu^{-1})y + z_0\|_2$, it follows that

$$\|L(x)\|_1 \leq \phi(\nu) \|T\| \|\nu^{-1}y + z_0\|_2 = \|T\| \|x\|_2.$$

So $\|L\| \leq \|T\|$. Also L an extension of T implies $\|L\| \geq \|T\|$. It follows from Theorem 5.21 that $(V, F, +, \cdot, \|\cdot\|_1)$ has the extension property.

To prove the converse, suppose $(V, F, +, \cdot, \|\cdot\|_1)$ contains a nest of spheres $S[\rho]$ of radius ρ , where ρ runs through some set P of positive real numbers, such that there is no point common to all spheres. Define a real-valued function f on V as follows: For any ρ such that x is not in $S[\rho]$ and any y in $S[\rho]$ let $f(x) = \|x - y\|_1$. If $S[\rho_1]$ and $S[\rho_2]$ are any two spheres of the nest, then $S[\rho_1]$ is a subset of $S[\rho_2]$ or $S[\rho_1]$ contains $S[\rho_2]$. Assume that $S[\rho_1]$ contains $S[\rho_2]$. For each x

such that x is in neither $S[\rho_1]$ or $S[\rho_2]$, if y_1 is in $S[\rho_1]$ and y_2 is in $S[\rho_2]$ then y_2 is also in $S[\rho_1]$ and

$$\|y_2 - y_1\|_1 \leq \rho_1 < \|x - y_1\|_1.$$

From (5.9), it follows that

$$\begin{aligned} \|x - y_2\|_1 &= \|(x - y_1) + (y_1 - y_2)\|_1 \\ &= \|x - y_1\|_1. \end{aligned}$$

That is, f is independent of the closed spheres involved in the definition of f . Furthermore $x \neq y$ implies $f(x) = \|x - y\|_1 > 0$. Since no point x of V is contained in all spheres $S[\rho]$, $\rho \in P$, f is defined and positive for all x in V .

If x is in $S[\rho]$ but not in $S[\rho_1]$, then $S[\rho]$ contains $S[\rho_1]$ since the collection of spheres is a nest. It follows that if y is in $S[\rho_1]$ then y is in $S[\rho]$ and $\|x - y\|_1 \leq \rho$. Therefore

$$(5.24) \quad f(x) \leq \rho \text{ whenever } x \text{ is in } S[\rho].$$

Consider

$$H = \{z = (x, \lambda) : x \in V, \lambda \in F\}.$$

Define addition and scalar multiplication as follows:

$$z_1 + z_2 = (x_1, \lambda_1) + (x_2, \lambda_2) = (x_1 + x_2, \lambda_1 + \lambda_2),$$

$$\mu z = \mu(x, \lambda) = (\mu x, \mu \lambda).$$

With these operations, H is a linear space. The additive identity is $(0, 0)$. A real-valued function $\|\cdot\|_3$ on H defined by

$$\begin{aligned} \|z\|_3 &= \phi(\lambda) f(\lambda^{-1}x), \lambda \neq 0 \\ &= \|x\|_1, \lambda = 0 \end{aligned}$$

is a non-archimedean norm. To see this, note that if $z = (x, \lambda) \neq (0, 0)$ then $x \neq 0$ or $\lambda \neq 0$ and $\|z\|_3 > 0$. Since f is strictly positive,

$\|z\|_3 = 0$ requires λ to be zero and hence that $\|x\|_1 = 0$. But this is possible only if $x = 0$. Therefore $\|z\|_3 \geq 0$ and equals 0 only if $z = 0$.

Since for μ in F and $z = (x, \lambda)$ in H ,

$$\begin{aligned}\|\mu z\|_3 &= \phi(\mu\lambda) f(\lambda^{-1}\mu^{-1}x) \\ &= \phi(\mu) \phi(\lambda) \phi(\lambda^{-1}) f(\lambda^{-1}x) \\ &= \phi(\mu) \|z\|_3\end{aligned}$$

if $\lambda \neq 0$, and

$$\|\mu z\|_3 = \|\mu x\|_1 = \phi(\mu)\|x\|_1 = \phi(\mu)\|z\|_3$$

if $\lambda = 0$, $\|\mu z\|_3 = \phi(\mu)\|z\|_3$. It remains to prove the non-archimedean property.

Let $z = (x, \lambda)$ be an element of H . If $\lambda \neq 0$, there is a ρ in P such that

$$\|z\|_3 = \phi(\lambda) \|y - \lambda^{-1}x\|_1 = \|x - \lambda y\|_1$$

for any y in $S[\rho]$. Since the same is trivially the case whenever $\lambda = 0$, there exists a ρ in P such that $\|z\|_3 = \|x - \lambda y\|_1$ for any y in $S[\rho]$. Let

$z_1 = (x_1, \lambda_1)$ and $z_2 = (x_2, \lambda_2)$ be any two points of H . Suppose x_1 is not in $S[\rho_1]$ and x_2 is not in $S[\rho_2]$. If x_2 is in $S[\rho_1]$, then $S[\rho_1]$ contains $S[\rho_2]$ and x_1 is not in $S[\rho_2]$. Thus there exists ρ in P such that not

both x_1 and x_2 are in $S[\rho]$. Furthermore the same reasoning implies

there exists ρ in P such that none of x_1 , x_2 , and $x_1 + x_2$ are in $S[\rho]$.

Therefore for any y in $S[\rho]$, $\|z_1\|_3 = \|x_1 - \lambda_1 y\|_1$, $\|z_2\|_3 = \|x_2 - \lambda_2 y\|_1$,

and $\|z_1 + z_2\|_3 = \|x_1 + x_2 - (\lambda_1 + \lambda_2)y\|_1$ simultaneously. Since

$$\|x_1 + x_2 - (\lambda_1 + \lambda_2)y\|_1 \leq \max(\|x_1 - \lambda_1 y\|_1, \|x_2 - \lambda_2 y\|_1),$$

it follows that

$$\|z_1 + z_2\|_3 \leq \max(\|z_1\|_3, \|z_2\|_3)$$

and hence that $\|\cdot\|_3$ is a non-archimedean norm defined on H . Therefore

$(H, F, +, \cdot, \| \cdot \|_3)$ is non-archimedean.

If $V' = \{(x, 0) : x \in V\}$, then $(V', F, +, \cdot, \| \cdot \|_3)$ is a subspace of $(H, F, +, \cdot, \| \cdot \|_3)$ which is topologically isomorphic to $(V, F, +, \cdot, \| \cdot \|)$. Now if $(V, F, +, \cdot, \| \cdot \|_1)$ has the extension property, then so does $(V', F, +, \cdot, \| \cdot \|_3)$. Thus the identity mapping I from V' into V' can be extended to a linear mapping L from H into V' such that $\|L\| = \|I\| = 1$. Suppose

$$L((0, -1) = (x_0, 0)).$$

Then for any x in V ,

$$L((x, 1)) = (x - x_0, 0)$$

since $L((0, -1) + (x, 1)) = L((x, 0)) = I((x, 0)) = (x, 0)$. Hence

$$\|L((x, 1))\|_3 = \|(x - x_0, 0)\|_3 = \|x - x_0\|_1$$

and

$$\|L((x, 1))\|_3 \leq \|L\| \|(x, 1)\|_3 = \|(x, 1)\|_3$$

for each x in V . But

$$\|(x, 1)\|_3 = \phi(1) f(1^{-1}x) = f(x).$$

Therefore for each x in V ,

$$\|x - x_0\|_1 \leq f(x).$$

In particular, for any ρ in P and any y in $S[\rho]$ it follows from (5.22) that

$$\|y - x_0\|_1 \leq f(x) \leq \rho.$$

That is, x_0 is common to all $S[\rho]$, in P . This contradiction to the original assumption implies that V does not have the extension property. Thus if V has the extension property then V is spherically complete.

Since F may be regarded as a one-dimensional non-archimedean space over itself, F has the Hahn-Banach property if and only if F is spherically complete.

ically complete. The following property of the p-adic number field is an immediate consequence of Theorem 5.22 and 5.25:

Theorem 5.26. The metric space (R_p, d) is spherically complete.

The next development in the literature relating to non-archimedean normed linear spaces pertains to completeness. A non-archimedean Banach space is a complete non-archimedean normed linear space. It is known, Theorem 5.17, that every finite dimensional non-archimedean normed linear space is a non-archimedean Banach space. In particular, $(R_p^n, R_p, +, \cdot, \| \cdot \|)$ where $\| \cdot \|$ is defined in (5.6) is such a space. Furthermore Rangachari and Srinivasan (15) show that if X is the set of all convergent sequences of R_p^n , then $(X, R_p, +, \cdot, \| \cdot \|_1)$ with

$$\begin{aligned} \| \{x_k\} \|_1 &= \| \{(\xi_1^{(k)}, \xi_2^{(k)}, \dots, \xi_n^{(k)})\} \|_1 \\ &= \sup_k \| (\xi_1^{(k)}, \xi_2^{(k)}, \dots, \xi_n^{(k)}) \| \end{aligned}$$

is an infinite dimensional non-archimedean Banach space. Also if M is the set of bounded sequences, then $(M, R_p, +, \cdot, \| \cdot \|_1)$ is a non-archimedean Banach space.

Let $(V, R_p, +, \cdot)$ be an algebra and let $\| \cdot \|$ be defined on V such that for each x and y in V ,

$$\|xy\| = \|x\| \|y\|$$

and

$$\|e\| = 1$$

where e is the multiplicative identity of $(V, R_p, +, \cdot)$. Then

$(V, R_p, +, \cdot, \| \cdot \|)$ is a non-archimedean Banach algebra whenever V is complete with respect to the metric induced by $\| \cdot \|$. Non-archimedean Banach algebras have been investigated by Monna (12) as well as

Rangachari and Srinivasan. Rangachari and Srinivasan were concerned with matrix transformations on non-archimedean fields. They showed that if Γ is the set of all convergence preserving matrices and $\| \cdot \|$ is defined by

$$\|A\| = \sup_{m,n} |\xi_{mn}|_p,$$

then $(\Gamma, R_p, +, \cdot, \| \cdot \|)$ is a non-archimedean Banach algebra. In his subsequent article, Srinivasan (16) further develops summation processes in the p-adic number fields.

In the past four years, a theory of locally convex spaces over non-archimedean valued fields in general, and p-adic fields in particular, has been developed and appears to be an excellent area for continued investigation. However the objective of this paper has been realized. The p-adic number fields have been developed in such a manner as to be accessible to senior mathematics majors. In the process of leading the reader to areas of current mathematical investigations, several similarities and differences between the real and p-adic numbers have been noted. This study of the p-adic number fields suggests some interesting questions. For example, (Q, d) is neither complete or spherically complete while (R_p, d_p) is both complete and spherically complete. The metric space (R, d) is complete but not spherically complete. Thus every complete space is not spherically complete. Is every spherically complete space complete? Also since Q is a subset of R_p and since (R_p, d_p) is a unique completion of (Q, d_p) in accordance with Theorem 1.12, it seems reasonable to ask if every metric space can be embedded in a spherically complete metric space. And if so, is there a standard process by which a non-spherically complete metric space can be completed?

A SELECTED BIBLIOGRAPHY

1. Bachman, George. Introduction to p-adic Numbers and Valuation Theory, New York: Academic Press, 1964.
2. Barnes, Wilfred E. Introduction to Abstract Algebra, Boston: D. C. Heath and Company, 1963.
3. Borevich, Z. I. and I. R. Shafarevich. Number Theory, trans. Newcomb Greenleaf, New York: Academic Press, 1966.
4. Cassels, J. W. S. "Global Fields," Algebraic Number Theory - Proceedings of an Instructional Conference Organized by the London Mathematical Society, Washington D.C.: Thompson, 1967.
5. Cohen, I. S. "On non-Archimedean Normed Spaces," Indagationes Mathematicae, 10 (1948), 244-49.
6. Hamilton, Norman T. and Joseph Landen. The Structure of Arithmetic, Boston: Allyn and Bacon, Inc., 1961.
7. Ingleton, A. W. "The Hahn-Banach Theorem for non-Archimedean Valued Fields," Proceedings Cambridge Philosophical Society, 48 (1952), 41-45.
8. Kelley, John L. General Topology, Princeton: D. Van Nostrand Company, Inc., 1955.
9. MacDuffee, C. C. "The p-adic Numbers of Hensel," The American Mathematical Monthly, 45 (1938), 500-508.
10. McCoy, Neal H. The Theory of Numbers, New York: The Macmillan Company, 1965.
11. Monna, A. F. "Linear Topological Spaces over non-Archimedean Valued Fields," Proceedings of a Conference on Local Fields, ed. T. A. Springer, New York: Springer-Verlag, 1967.
12. Monna, A. F. "Sur la Structure des Espaces de Banach Nonarchimediens," Koninklyke Nederlandse Akademie Van Wetenschappen, Proceedings, A68 (1965), 602-14.
13. Monna, A. F. "Sur les Espaces Lineaires Normes," Indagationes Mathematicae, 8 (1946), 682-9.

13. Nachbin, L. "A Theorem of the Hahn-Banach Type for Linear Transformations", Transaction of the American Mathematical Society, 68 (1950), 28-40.
14. Olmsted, John M. H. The Real Number System, New York: Meredith Publishing Company, 1962.
15. Rangachari, M. S. and V. K. Srinivasan. "Matrix Transformations in non-Archimedean Fields," Indagationes Mathematicae, 26 (1964), 422-429.
16. Srinivasan, V. K. "On Certain Summation Processes in the p-adic Fields," Koninklyke Nederlandse Akademie Van Wetenschappen Proceedings, A68 (1965), 319-25.
17. Taylor, Angus E. Introduction to Functional Analysis, New York: John Wiley and Sons, Inc., 1957.
18. Warner, Seth. Modern Algebra, Vol. I, Englewood Cliffs: Prentice-Hall, 1965.
19. Weil, Andre. Basic Number Theory, Berlin: Springer-Verlag, 1967.

VITA

2

VERBAL MERLE SNOOK

Candidate for the Degree of
Doctor of Education

Thesis: A STUDY OF P-ADIC NUMBER FIELDS

Major Field: Higher Education

Biographical:

Personal Data: Born in Chester, Oklahoma, January 15, 1934,
the son of Howard C. and F. Blanche Snook.

Education: Graduated from Sweet Home Union High School, Sweet
Home, Oregon in 1952; received the Bachelor of Science degree
from the University of Oregon in June, 1956; received the
Master of Science degree from the University of Oregon in
June, 1962; received the Master of Arts degree from the
University of Illinois in August, 1962; completed the require-
ments for the Doctor of Education degree at Oklahoma State
University in May, 1970.

Professional Experience: High school instructor of mathematics
and science, Yoncalla Union High School, Yoncalla, Oregon,
1956-58; instructor of mathematics and science, McMinnville
High School, McMinnville, Oregon, 1958-61 and 1962-1965;
Assistant Professor of Mathematics, Oral Roberts University,
Tulsa, Oklahoma, 1965.

Professional Organizations: Mathematical Association of America,
Oklahoma Education Association.