

**ALGEBRAIC NUMBERS AND  
ALGEBRAIC FUNCTIONS**

---

## Notes on Mathematics and Its Applications

---

*General Editors: Jacob T. Schwartz, Courant Institute of Mathematical Sciences and Maurice Lévy, Université de Paris*

- E. Artin*, ALGEBRAIC NUMBERS AND ALGEBRAIC FUNCTIONS  
*R. P. Boas*, COLLECTED WORKS OF HIDEHIKO YAMABE  
*M. Davis*, FUNCTIONAL ANALYSIS  
*M. Davis*, LECTURES ON MODERN MATHEMATICS  
*J. Eells, Jr.*, SINGULARITIES OF SMOOTH MAPS  
*K. O. Friedrichs*, ADVANCED ORDINARY DIFFERENTIAL EQUATIONS  
*K. O. Friedrichs*, SPECIAL TOPICS IN FLUID DYNAMICS  
*K. O. Friedrichs and H. N. Shapiro*, INTEGRATION IN HILBERT SPACE  
*M. Hausner and J. T. Schwartz*, LIE GROUPS; LIE ALGEBRAS  
*P. Hilton*, HOMOTOPY THEORY AND DUALITY  
*F. John*, LECTURES ON ADVANCED NUMERICAL ANALYSIS  
*Allen M. Krall*, STABILITY TECHNIQUES  
*H. Mullish*, AN INTRODUCTION TO COMPUTER PROGRAMMING  
*J. T. Schwartz*,  $W^*$  ALGEBRAS  
*A. Silverman*, EXERCISES IN FORTRAN  
*J. J. Stoker*, NONLINEAR ELASTICITY

*Additional volumes in preparation*

# Algebraic Numbers and Algebraic Functions

EMIL ARTIN

*Late of Princeton University*

G  
|  
B

---

**GORDON AND BREACH**  
SCIENCE PUBLISHERS · NEW YORK · LONDON · PARIS

Copyright © 1967 by Gordon and Breach, Science Publishers, Inc.  
150 Fifth Avenue, New York, New York 10011

## General Preface

*Library of Congress Catalog Card Number: 67-26811*

*Editorial Office for Great Britain:*

*Gordon and Breach Science Publishers Ltd.  
8 Bloomsbury Way  
London WC1, England*

*Editorial Office for France:*

*7-9 rue Emile Dubois  
Paris 14<sup>e</sup>*

*Distributed in France by:*

*Dunod Editeur  
92, rue Bonaparte  
Paris 6<sup>e</sup>*

*Distributed in Canada by:*

*The Ryerson Press  
299 Queen Street West  
Toronto 2B, Ontario*

*Printed in Belgium by*

*the Saint Catherine Press, Ltd., Tempelhof, Bruges*

A large number of mathematical books begin as lecture notes; but, since mathematicians are busy, and since the labor required to bring lecture notes up to the level of perfection which authors and the public demand of formally published books is very considerable, it follows that an even larger number of lecture notes make the transition to book form only after great delay or not at all. The present lecture note series aims to fill the resulting gap. It will consist of reprinted lecture notes, edited at least to a satisfactory level of completeness and intelligibility, though not necessarily to the perfection which is expected of a book. In addition to lecture notes, the series will include volumes of collected reprints of journal articles as current developments indicate, and mixed volumes including both notes and reprints.

JACOB T. SCHWARTZ  
MAURICE LÉVY

## Preface

These lecture notes represent the content of a course given at Princeton University during the academic year 1950/51. This course was a revised and extended version of a series of lectures given at New York University during the preceding summer. They cover the theory of valuation, local class field theory, the elements of algebraic number theory and the theory of algebraic function fields of one variable. It is intended to prepare notes for a second part in which global class field theory and other topics will be discussed.

Apart from a knowledge of Galois theory, they presuppose a sufficient familiarity with the elementary notions of point set topology. The reader may get these notions for instance in N. Bourbaki, *Éléments de Mathématique, Livre III, Topologie générale*, Chapitres I-III.

In several places use is made of the theorems on Sylow groups. For the convenience of the reader an appendix has been prepared, containing the proofs of these theorems.

The completion of these notes would not have been possible without the great care, patience and perseverance of Mr. I. T. A. O. Adamson who prepared them. Of equally great importance have been frequent discussions with Mr. J. T. Tate to whom many simplifications of proofs are due. Very helpful was the assistance of Mr. Peter Ceike who gave a lot of his time preparing the stencils for these notes.

Finally I have to thank the Institute for Mathematics and Mechanics, New York University, for mimeographing these notes.

*Princeton University*  
*June 1951*

EMIL ARTIN

# Contents

GENERAL PREFACE . . . . . v  
PREFACE . . . . . vii

## Part I General Valuation Theory

### Chapter 1

#### VALUATIONS OF A FIELD

1. Equivalent Valuations . . . . . 3  
2. The Topology Induced by a Valuation . . . . . 5  
3. Classification of Valuations . . . . . 6  
4. The Approximation Theorem . . . . . 8  
5. Examples . . . . . 10  
6. Completion of a Field . . . . . 17

### Chapter 2

#### COMPLETE FIELDS

1. Normed Linear Spaces . . . . . 19  
2. Extension of the Valuation . . . . . 21  
3. Archimedean Case . . . . . 24  
4. The Non-Archimedean Case . . . . . 28  
5. Newton's Polygon . . . . . 37  
6. The Algebraic Closure of a Complete Field . . . . . 43  
7. Convergent Power Series . . . . . 47

### Chapter 3

#### $e, f$ AND $n$

1. The Ramification and Residue Class Degree . . . . . 53  
2. The Discrete Case . . . . . 56  
3. The General Case . . . . . 60

## Chapter 4

## RAMIFICATION THEORY

1. Unramified Extensions . . . . .	64
2. Tame Ramified Extensions . . . . .	67
3. Characters of Abelian Groups . . . . .	71
4. The Inertia Group and Ramification Group . . . . .	72
5. Higher Ramification Groups . . . . .	77
6. Ramification Theory in the Discrete Case . . . . .	82

## Chapter 5

## THE DIFFERENT

1. The Inverse Different . . . . .	86
2. Complementary Bases . . . . .	89
3. Fields with Separable Residue Class Field . . . . .	93
4. The Ramification Groups of a Subfield . . . . .	95

**Part II Local Class Field Theory**

## Chapter 6

## PREPARATIONS FOR LOCAL CLASS FIELD THEORY

1. Galois Theory for Infinite Extensions . . . . .	103
2. Group Extensions . . . . .	108
3. Galois Cohomology Theory . . . . .	114
4. Continuous Cocycles . . . . .	117

## Chapter 7

## THE FIRST AND SECOND INEQUALITIES

1. Introduction . . . . .	127
2. Unramified Extensions . . . . .	127
3. The First Inequality . . . . .	130
4. The Second Inequality: A Reduction Step . . . . .	133
5. The Second Inequality Concluded . . . . .	135

## Chapter 8

## THE NORM RESIDUE SYMBOL

1. The Temporary Symbol $(c, \kappa   \kappa/\tau)$ . . . . .	144
2. Choice of a Standard Generator $c$ . . . . .	153
3. The Norm Residue Symbol for Finite Extensions . . . . .	158

## Chapter 9

## THE EXISTENCE THEOREM

1. Introduction . . . . .	165
2. The Infinite Product Space $l$ . . . . .	165
3. The New Topology in $K^*$ . . . . .	170
4. The Norm Group and Norm Residue Symbol for Infinite Extensions . . . . .	174
5. Extension Fields with Degree Equal to the Characteristic . . . . .	180
6. The Existence Theorem . . . . .	181
7. Uniqueness of the Norm Residue Symbol . . . . .	187

## Chapter 10

## APPLICATIONS AND ILLUSTRATIONS

1. Fields with Perfect Residue Class Field . . . . .	190
2. The Norm Residue Symbol for Certain Power Series Fields . . . . .	193
3. Differentials in an Arbitrary Power Series Field . . . . .	200
4. The Conductor and Different for Cyclic $p$ -Extensions . . . . .	203
5. The Rational $p$ -adic Field . . . . .	206
6. Computation of the Index $(\alpha : \alpha^n)$ . . . . .	209

**Part III****Product Formula and Function Fields in One Variable**

## Chapter 11

## PREPARATIONS FOR THE GLOBAL THEORY

1. The Radical of a Ring . . . . .	215
2. Kronecker Products of Spaces and Rings . . . . .	216
3. Composite Extensions . . . . .	218
4. Extension of the Valuation of a Non-Complete Field . . . . .	223

## Chapter 12

## CHARACTERIZATION OF FIELDS BY THE PRODUCT FORMULA

1. $PF$ -Fields . . . . .	225
2. Upper Bound for the Order of a Parallelotope . . . . .	227
3. Description of all $PF$ -Fields . . . . .	230
4. Finite Extensions of $PF$ -Fields . . . . .	235

## Chapter 13

DIFFERENTIALS IN  $PF$ -FIELDS

1. Valuation Vectors, Ideles, and Divisors . . . . . 238
2. Valuation Vectors in an Extension Field . . . . . 241
3. Some Results on Vector Spaces . . . . . 244
4. Differentials in the Rational Subfield of a  $PF$ -Field . . . . . 245
5. Differentials in a  $PF$ -Field . . . . . 251
6. The Different . . . . . 255

## Chapter 14

## THE RIEMANN-ROCH THEOREM

1. Parallelotopes in a Function Field . . . . . 260
2. First Proof . . . . . 262
3. Second Proof . . . . . 265

## Chapter 15

## CONSTANT FIELD EXTENSIONS

1. The Effective Degree . . . . . 271
2. Divisors in an Extension Field . . . . . 278
3. Finite Algebraic Constant Field Extensions . . . . . 279
4. The Genus in a Purely Transcendental Constant Field Extension . . . . . 284
5. The Genus in an Arbitrary Constant Field Extension . . . . . 287

## Chapter 16

## APPLICATIONS OF THE RIEMANN-ROCH THEOREM

1. Places and Valuation Rings . . . . . 293
2. Algebraic Curves . . . . . 297
3. Linear Series . . . . . 300
4. Fields of Genus Zero . . . . . 302
5. Elliptic Fields . . . . . 306
6. The Curve of Degree  $n$  . . . . . 311
7. Hyperelliptic Fields . . . . . 312
8. The Theorem of Clifford . . . . . 317

## Chapter 17

## DIFFERENTIALS IN FUNCTION FIELDS

1. Preparations . . . . . 321
2. Local Components of Differentials . . . . . 322
3. Differentials and Derivatives in Function Fields . . . . . 324
4. Differentials of the First Kind . . . . . 329

## Appendix

THEOREMS ON  $p$ -GROUPS AND SYLOW GROUPS

1.  $S$ -Equivalence Classes . . . . . 334
2. Theorems About  $p$ -Groups . . . . . 335
3. The Existence of Sylow Subgroups . . . . . 336
4. Theorems About Sylow Subgroups . . . . . 337

- INDEX OF SYMBOLS . . . . . 339
- SUBJECT INDEX . . . . . 343

PART ONE

# General Valuation Theory



## CHAPTER ONE

# Valuations of a Field

A *valuation* of a field  $k$  is a real-valued function  $|x|$ , defined for all  $x \in k$ , satisfying the following requirements:

- (1)  $|x| \geq 0$ ;  $|x| = 0$  if and only if  $x = 0$ ,
- (2)  $|xy| = |x| |y|$ ,
- (3) If  $|x| \leq 1$ , then  $|1 + x| \leq c$ , where  $c$  is a constant;  $c \geq 1$ .

(1) and (2) together imply that a valuation is a homomorphism of the multiplicative group  $k^*$  of non-zero elements of  $k$  into the positive real numbers.

If this homomorphism is trivial, i.e. if  $|x| = 1$  for all  $x \in k^*$ , the valuation is also called *trivial*.

### 1. Equivalent Valuations

Let  $| \cdot |_1$  and  $| \cdot |_2$  be two functions satisfying conditions (1) and (2) above; suppose that  $| \cdot |_1$  is non-trivial. These functions are said to be *equivalent* if  $|a|_1 < 1$  implies  $|a|_2 < 1$ . Obviously for such functions  $|a|_1 > 1$  implies  $|a|_2 > 1$ ; but we can prove more.

**Theorem 1:** Let  $| \cdot |_1$  and  $| \cdot |_2$  be equivalent functions, and suppose  $| \cdot |_1$  is non-trivial. Then  $|a|_1 = 1$  implies  $|a|_2 = 1$ .

*Proof:* Let  $b \neq 0$  be such that  $|b|_1 < 1$ . Then  $|a^n b|_1 < 1$ ; whence  $|a^n b|_2 < 1$ , and so  $|a|_2 < |b|_2^{-1/n}$ . Letting  $n \rightarrow \infty$ , we have  $|a|_2 \leq 1$ . Similarly, replacing  $a$  in this argument by  $1/a$ , we have  $|a|_2 \geq 1$ , which proves the theorem.

**Corollary:** For non-trivial functions of this type, the relation of equivalence is reflexive, symmetric and transitive.

There is a simple relation between equivalent functions, given by

**Theorem 2:** If  $| \cdot |_1$  and  $| \cdot |_2$  are equivalent functions, and  $| \cdot |_1$  is non-trivial, then  $| a |_2 = | a |_1^\alpha$  for all  $a \in k$ , where  $\alpha$  is a fixed positive real number.

*Proof:* Since  $| \cdot |_1$  is non-trivial, we can select an element  $c \in k^*$  such that  $| c |_1 > 1$ ; then  $| c |_2 > 1$  also.

Set  $| a |_1 = | c |_1^\gamma$ , where  $\gamma$  is a non-negative real number. If  $m/n > \gamma$ , then  $| a |_1 < | c |_1^{m/n}$ , whence  $| a^{n/c^m} |_1 < 1$ . Then  $| a^{n/c^m} |_2 < 1$ , from which we deduce that  $| a |_2 < | c |_2^{m/n}$ . Similarly, if  $m/n < \gamma$ , then  $| a |_2 > | c |_2^{m/n}$ . It follows that  $| a |_2 = | c |_2^\gamma$ . Now, clearly,

$$\gamma = \frac{\log | a |_1}{\log | c |_1} = \frac{\log | a |_2}{\log | c |_2}.$$

This proves the theorem, with

$$\alpha = \frac{\log | c |_2}{\log | c |_1}.$$

In view of this result, let us agree that the equivalence class defined by the trivial function shall consist of this function alone.

Our third condition for valuations has replaced the classical "Triangular Inequality" condition, viz.,  $| a + b | \leq | a | + | b |$ . The connection between this condition and ours is given by

**Theorem 3:** Every valuation is equivalent to a valuation for which the triangular inequality holds.

*Proof.* (1) When the constant  $c = 2$ , we shall show that the triangular inequality holds for the valuation itself.

Let  $| a | \leq | b |$ .

Then

$$\left| \frac{a}{b} \right| \leq 1 \Rightarrow \left| 1 + \frac{a}{b} \right| \leq 2 \Rightarrow | a + b | \leq 2 | b | \\ = 2 \max(| a |, | b |).$$

Similarly

$$| a_1 + a_2 + a_3 + a_4 | \leq 4 \max(| a_1 |, \dots, | a_4 |)$$

and

$$| a_1 + \dots + a_{2^r} | \leq 2^r \max(| a_1 |, \dots, | a_{2^r} |).$$

Now given  $a_1, a_2, \dots, a_n$ , we can find an integer  $r$  such that  $n \leq 2^r < 2n$ . Hence

$$| a_1 + \dots + a_n | = | a_1 + \dots + a_n + 0 + \dots + 0 | \\ \leq 2^r \max | a_v | < 2n \max | a_v |.$$

In particular, if we set all the  $a_v = 1$ , we have  $| n | \leq 2n$ . We may also weaken the above inequality, and write

$$| a_1 + \dots + a_n | \leq 2n(| a_1 | + \dots + | a_n |).$$

Consider

$$| a + b |^n = \left| a^n + \binom{n}{1} a^{n-1}b + \dots + b^n \right| \\ \leq 2(n+1) \left\{ | a |^n + \binom{n}{1} | a |^{n-1} | b | + \dots + | b |^n \right\} \\ \leq 4(n+1) \left\{ | a |^n + \binom{n}{1} | a |^{n-1} | b | + \dots + | b |^n \right\} \\ = 4(n+1) \{ | a | + | b | \}^n.$$

Hence

$$| a + b | \leq \sqrt[n]{4(n+1)} (| a | + | b |).$$

Letting  $n \rightarrow \infty$  we obtain the desired result.

We may note that, conversely, the triangular inequality implies that our third requirement is satisfied, and that we may choose  $c = 2$ .

(2) When  $c > 2$ , we may write  $c = 2^\alpha$ . Then it is easily verified that  $| \cdot |^{1/\alpha}$  is an equivalent valuation for which the triangular inequality is satisfied.

## 2. The Topology Induced by a Valuation

Let  $| \cdot |$  be a function satisfying the axioms (1) and (2) for valuations. In terms of this function we may define a topology in  $k$  by

prescribing the fundamental system of neighborhoods of each element  $x_0 \in k$  to be the sets of elements  $x$  such that  $|x - x_0| < \epsilon$ . It is clear that equivalent functions induce the same topology in  $k$ , and that the trivial function induces the discrete topology.

There is an intimate connection between our third axiom for valuations and the topology induced in  $k$ .

**Theorem 4:** The topology induced by  $|\cdot|$  is Hausdorff if and only if axiom (3) is satisfied.

*Proof:* (1) If the topology is Hausdorff, there exist neighborhoods separating 0 and  $-1$ . Thus we can find real numbers  $a$  and  $b$  such that if  $|x| \leq a$ , then  $|1 + x| \geq b$ .

Now let  $x$  be any element with  $|x| \leq 1$ ; then either  $|1 + x| \leq 1/a$  or  $|1 + x| > 1/a$ . In the latter case, set  $y = -x/(1 + x)$ ; then

$$|y| = \frac{|x|}{|1 + x|} \leq \frac{1}{a^{-1}} = a;$$

hence

$$|1 + y| = \left| \frac{1}{1 + x} \right| \geq b,$$

i.e.  $|1 + x| \leq 1/b$ . We conclude, therefore, that if  $|x| \leq 1$ , then  $|1 + x| \leq \max(1/a, 1/b)$ , which is axiom (3).

(2) The converse is obvious if we replace  $|\cdot|$  by the equivalent function for which the triangular inequality holds.

It should be remarked that the field operations are continuous in the topology induced on  $k$  by a valuation.

### 3. Classification of Valuations

If the constant  $c$  of axiom (3) can be chosen to be 1, i.e. if  $|x| \leq 1$  implies  $|1 + x| \leq 1$ , then the valuation is said to be *non-archimedean*. Otherwise the valuation is called *archimedean*. Obviously the valuations of an equivalence class are either all archimedean or all non-archimedean. For non-archimedean valuations we obtain a sharpening of the triangular inequality:

**Theorem 5:** For non-archimedean valuations,

$$|a + b| \leq \max(|a|, |b|).$$

*Proof.* Let  $|a| \leq |b|$ ; then  $|a/b| \leq 1$ . It follows that  $|1 + a/b| \leq 1$ , whence

$$|a + b| \leq |b| = \max(|a|, |b|).$$

**Corollary 5.1:** If  $|a| < |b|$ , then  $|a + b| = |b|$ .

*Proof:*

$$|b| = |-a + (a + b)| \leq \max(|a|, |a + b|),$$

by the Theorem. By hypothesis,  $|b|$  is not  $\leq |a|$ , so that we have  $|b| \leq |a + b|$ . But using the theorem again we have

$$|a + b| \leq \max(|a|, |b|) = |b|.$$

Thus if  $|a| < |b|$ , then  $|a + b| = |b|$ .

We notice that this equality does not necessarily hold when  $|a| = |b|$ ; for example, if  $b = -a$ , we have  $|a + b| = 0 < |a|$ . In general we have

$$|a_1 + \cdots + a_n| \leq |a_1|,$$

where  $|a_1| = \max |a_\nu|$ ; and

$$|a_1 + \cdots + a_n| = |a_1|$$

if, for every  $\nu > 1$ ,  $|a_\nu| < |a_1|$ . This last result is frequently used in the following form:

**Corollary 5.2:** Suppose it is known that  $|a_\nu| \leq |a_1|$  for all  $\nu$ , and that  $|a_1 + \cdots + a_n| < |a_1|$ . Then for some  $\nu > 1$ ,  $|a_\nu| = |a_1|$ .

We now give a necessary and sufficient condition for a field to be non-archimedean:

**Theorem 6:** A valuation is non-archimedean if and only if the values of the rational integers are bounded.

*Proof:* (1) The necessity of the condition is obvious, for if the valuation is non-archimedean, then

$$|m| = |1 + 1 + \cdots + 1| \leq |1|.$$

(2) To prove the sufficiency of the condition we consider the equivalent valuation for which the triangular inequality is satisfied. Obviously the values of the integers are bounded in this valuation also; say  $|m| \leq D$ . Consider

$$\begin{aligned} |a + b|^n &= |(a + b)^n| = \left| a^n + \binom{n}{1} a^{n-1}b + \cdots + b^n \right| \\ &\leq |1| |a^n| + \left| \binom{n}{1} \right| |a|^{n-1} |b| + \cdots + |1| |b|^n \\ &\leq D \{ |a|^n + |a|^{n-1} |b| + \cdots + |b|^n \} \\ &\leq D(n + 1) \{ \max(|a|, |b|) \}^n. \end{aligned}$$

Hence

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

Letting  $n \rightarrow \infty$ , we have the desired result.

**Corollary:** A valuation of a field of characteristic  $p > 0$  is non-archimedean.

We may remark that if  $k_0$  is a subfield of  $k$ , then a valuation of  $k$  is (non-)archimedean on  $k_0$  is (non-)archimedean on the whole of  $k$ . In particular, if the valuation is trivial on  $k_0$ , it is non-archimedean on  $k$ .

#### 4. The Approximation Theorem

Let  $\{a_n\}$  be a sequence of elements of  $k$ ; we say that  $a$  is the limit of this sequence with respect to the valuation if

$$\lim_{n \rightarrow \infty} |a - a_n| = 0.$$

The following examples will be immediately useful:

(a) If  $|a| < 1$ , then

$$\lim_{n \rightarrow \infty} a^n = 0.$$

For  $|a^n - 0| = |a|^n \rightarrow 0$  as  $n \rightarrow \infty$ .

(b) If  $|a| < 1$ , then

$$\lim_{n \rightarrow \infty} \frac{a^n}{1 + a^n} = 0.$$

(c) If  $|a| > 1$ , then

$$\lim_{n \rightarrow \infty} \frac{a^n}{1 + a^n} = 1.$$

For

$$\left| \frac{a^n}{1 + a^n} - 1 \right| = \left| \frac{1}{1 + a^n} \right| = \left| \frac{\left(\frac{1}{a}\right)^n}{1 + \left(\frac{1}{a}\right)^n} \right| \rightarrow 0 \quad \text{as } n \rightarrow \infty.$$

We now examine the possibility of finding a relation between non-equivalent valuations; we shall show that if the number of valuations considered is finite, no relation of a certain simple type is possible.

**Theorem 7:** Let  $| \cdot |_1, \dots, | \cdot |_n$  be a finite number of inequivalent non-trivial valuations of  $k$ . Then there is an element  $a \in k$  such that  $|a|_1 > 1$ , and  $|a|_\nu < 1$  ( $\nu = 2, \dots, n$ ).

*Proof.* First let  $n = 2$ . Then since  $| \cdot |_1$  and  $| \cdot |_2$  are nonequivalent, there certainly exist elements  $b, c \in k$  such that  $|b|_1 < 1$  and  $|b|_2 \geq 1$ , while  $|c|_1 \geq 1$  and  $|c|_2 < 1$ . Then  $a = c/b$  has the required properties.

The proof now proceeds by induction. Suppose the theorem is true for  $n - 1$  valuations; then there is an element  $b \in k$  such that  $|b|_1 > 1$ , and  $|b|_\nu < 1$  ( $\nu = 2, \dots, n - 1$ ). Let  $c$  be an element such that  $|c|_1 > 1$  and  $|c|_n < 1$ . We have two cases to consider:

*Case 1:*  $|b|_n \leq 1$ . Consider the sequence  $a_r = cb^r$ . Then  $|a_r|_1 = |c|_1 |b|_1^r > 1$ , while  $|a_r|_n = |c|_n |b|_n^r < 1$ ; for sufficiently large  $r$ ,  $|a_r|_\nu = |c|_\nu |b|_\nu^r < 1$  ( $\nu = 2, \dots, n - 1$ ). Thus  $a_r$  is a suitable element, and the theorem is proved in this case.

*Case 2:*  $|b|_n > 1$ . Here we consider the sequence

$$a_r = \frac{cb^r}{1 + b^r}.$$

This sequence converges to the limit  $c$  in the topologies induced by  $|\cdot|_1$  and  $|\cdot|_n$ . Thus  $a_r = c + \eta_r$  where  $|\eta_r|_1$  and  $|\eta_r|_n \rightarrow 0$  as  $r \rightarrow \infty$ . Hence for  $r$  large enough,  $|a_r|_1 > 1$  and  $|a_r|_n < 1$ .

For  $\nu = 2, \dots, n-1$ , the sequence  $a_r$  converges to the limit 0 in the topology induced by  $|\cdot|_\nu$ . Hence for large enough values of  $r$ ,  $|a_r|_\nu < 1$  ( $\nu = 2, \dots, n-1$ ). Thus  $a_r$  is a suitable element, for  $r$  large enough, and the theorem is proved in this case also.

**Corollary:** With the conditions of the theorem, there exists an element  $a$  which is close to 1 in  $|\cdot|_1$  and close to 0 in  $|\cdot|_\nu$  ( $\nu = 2, \dots, n-1$ ).

*Proof.* If  $b$  is an element such that  $|b|_1 > 1$  and  $|b|_\nu < 1$  ( $\nu = 2, \dots, n-1$ ), then  $a_r = b^r/(1 + b^r)$  satisfies our requirements for large enough values of  $r$ .

**Theorem 8: (The Approximation Theorem):** Let  $|\cdot|_1, \dots, |\cdot|_n$  be a finite number of non-trivial inequivalent valuations. Given any  $\epsilon > 0$ , and any elements  $a_\nu$  ( $\nu = 1, \dots, n$ ), there exists an element  $a$  such that  $|a - a_\nu|_\nu < \epsilon$ .

*Proof.* We can find elements  $b_i$  ( $i = 1, \dots, n$ ) close to 1 in  $|\cdot|_i$  and close to zero in  $|\cdot|_\nu$  ( $\nu \neq i$ ).

Then  $a = a_1 b_1 + \dots + a_n b_n$  is the required element.

Let us denote by  $(k)_i$  the field  $k$  with the topology of  $|\cdot|_i$  imposed upon it. Consider the Cartesian product  $(k)_1 \times (k)_2 \times \dots \times (k)_n$ . The elements  $(a, a, \dots, a)$  of the diagonal form a field  $k_D$  isomorphic to  $k$ . The Approximation Theorem states that  $k_D$  is everywhere dense in the product space. The theorem shows clearly the impossibility of finding a non-trivial relation of the type

$$\prod_{\nu=1}^n |x|_\nu^{c_\nu} = 1,$$

with real constants  $c_\nu$ .

## 5. Examples

Let  $k$  be the quotient field of an integral domain  $\mathfrak{o}$ ; then it is easily verified that a valuation  $|\cdot|$  of  $k$  induces a function  $\mathfrak{o}$  (which we still denote by  $|\cdot|$ ), satisfying the conditions

- (1)  $|a| \geq 0$ ;  $|a| = 0$  if and only if  $a = 0$ ,
- (2)  $|ab| = |a| |b|$ ,
- (3)  $|a + b| \leq \max(|a|, |b|)$ .

Suppose, conversely, that we are given such a function on  $\mathfrak{o}$ . Then if  $x = a/b$  ( $a, b \in \mathfrak{o}$ ,  $x \in k$ ), we may define  $|x| = |a|/|b|$ ;  $|x|$  is well-defined on  $k$ , and obviously satisfies our axioms (1) and (2) for valuations. To show that axiom (3) is also satisfied, let  $|x| \leq 1$ , i.e.  $|a| \leq |b|$ . Then

$$|1 + x| = \frac{|a + b|}{|b|} \leq \frac{e \max(|a|, |b|)}{|b|} = e.$$

Hence if  $k$  is the quotient field of an integral domain  $\mathfrak{o}$ , the valuations of  $k$  are sufficiently described by their actions on  $\mathfrak{o}$ .

*First Example:* Let  $k = R$ , the field of rational numbers;  $k$  is then the quotient field of the ring of integers  $\mathfrak{o}$ .

Let  $m, n$  be integers  $> 1$ , and write  $m$  in the  $n$ -adic scale:

$$m = a_0 + a_1 n + \dots + a_r n^r$$

$$\left(0 \leq a_i < n; n^r \leq m, \text{ i.e. } r \leq \frac{\log m}{\log n}\right).$$

Let  $|\cdot|$  be a valuation of  $R$ ; suppose  $|\cdot|$  replaced, if necessary, by the equivalent valuation for which the triangular inequality holds. Then  $|a_\nu| < n$ , and we have

$$|m| \leq \left(\frac{\log m}{\log n} + 1\right) n \cdot \{\max(1, |n|\}\}^{\log m / \log n}.$$

Using this estimate for  $|m|^s$ , extracting the  $s$ th root, and letting  $s \rightarrow \infty$ , we have

$$|m| \leq \{\max(1, |n|\}\}^{\log m / \log n}.$$

There are now two cases to consider.

*Case 1:*  $|n| > 1$  for all  $n > 1$ . Then

$$|m| \leq |n|^{\log m / \log n} : |m|^{1/\log m} \leq |n|^{1/\log n}.$$

Since  $|m| > 1$  also, we may interchange the roles of  $m$  and  $n$ , obtaining the reversed inequality. Hence

$$|m|^{1/\log m} = |n|^{1/\log n} = e^\alpha,$$

where  $\alpha$  is a positive real number. It follows that

$$|n| = e^{\alpha \log n} = n^\alpha,$$

so that  $||$  is in this case equivalent to the ordinary "absolute value",  $|x| = \max(x, -x)$ .

*Case 2:* There exists an integer  $n > 1$  such that  $|n| \leq 1$ . Then  $|m| \leq 1$  for all  $m \in \mathfrak{o}$ . If we exclude the trivial valuation, we must have  $|n| < 1$  for some  $n \in \mathfrak{o}$ ; clearly the set of all such integers  $n$  forms an ideal  $(p)$  of  $\mathfrak{o}$ . The generator of this ideal is a prime number; for if  $p = p_1 p_2$ , we have  $|p| = |p_1| |p_2| < 1$ , and hence (say)  $|p_1| < 1$ . This  $p_1 \in (p)$ , i.e.  $p$  divides  $p_1$ ; but  $p_1$  divides  $p$ ; hence  $p$  is a prime. If  $|p| = c$ , and  $n = p^v b$ ,  $(p, b) = 1$ , then  $|n| = c^v$ . Every non-archimedean valuation is therefore defined by a prime number  $p$ .

Conversely, let  $p$  be a prime number in  $\mathfrak{o}$ ,  $c$  a constant,  $0 < c < 1$ . Let  $n = p^v b$ ,  $(p, b) = 1$ , and define the function  $||$  by setting  $|n| = c^v$ . It is easily seen that this function satisfies the three conditions for such functions on  $\mathfrak{o}$ , and hence leads to a valuation on  $R$ . This valuation can be described as follows: let  $x$  be a non-zero rational number, and write it as  $x = p^v y$ , where the numerator and denominator are prime to  $p$ . Then  $|x| = c^v$ .

*Second Example.* Let  $k$  be the field of rational functions over a field  $F$ :  $k = F(x)$ . Then  $k$  is the quotient field of the ring of polynomials  $\mathfrak{o} = F[x]$ . Let  $||$  be a valuation of  $k$  which is trivial on  $F$ ;  $||$  will thus be non-archimedean. We have again two cases to consider.

*Case I:*  $|x| > 1$ . Then if

$$f(x) = c_0 + c_1 x + \cdots + c_n x^n,$$

$c_n \neq 0$ , we have

$$|f(x)| = |x|^n = |x|^{\deg f(x)}.$$

Conversely, if we select a number  $c > 1$  and set

$$|f(x)| = c^{\deg f(x)},$$

our conditions for functions on  $\mathfrak{o}$  are easily verified. Hence this

function yields a valuation of  $k$  described as follows: let  $a = f(x)/g(x)$ , and define

$$\deg a = \deg f(x) - \deg g(x).$$

Then  $|a| = c^{\deg a}$ . Obviously the different choices of  $c$  lead only to equivalent valuations.

*Case 2:*  $|x| < 1$ . Then for any  $f(x) \in \mathfrak{o}$ ,  $|f(x)| \leq 1$ . If we exclude the trivial valuation, we must have  $|f(x)| < 1$  for some  $f(x) \in \mathfrak{o}$ . As in the first example, the set of all such polynomials is an ideal, generated by an irreducible polynomial  $p(x)$ . If  $|p(x)| = c$ , and  $f(x) = (p(x))^v g(x)$ ,  $(p(x), g(x)) = 1$ , then  $|f(x)| = c^v$ .

Conversely, if  $p(x)$  is an irreducible polynomial, it defines a valuation of this type. This is shown in exactly the same way as in the first example.

In both cases, the field  $k = F(x)$  and the field  $k = R$  of the rational numbers, we have found equivalence classes of valuations, one to each prime  $p$  (in the case of  $F(x)$ , one to each irreducible polynomial) with one exception, an equivalence class which does not come from a prime. To remove this exception we introduce in both cases a "symbolic" prime, the so-called *infinite prime*,  $p_\infty$  which we associate with the exceptional equivalence class. So  $|a|_{p_\infty}$  stands for the ordinary absolute value in the case  $k = R$ , and for  $c^{\deg a}$  in the case  $k = F(x)$ . We shall now make a definite choice of the constant  $c$  entering in the definition of the valuation associated with a prime  $p$ .

(I)  $k = R$ . (a)  $p \neq p_\infty$ . We choose  $c = 1/p$ . If, therefore,  $a \neq 0$ , and  $a = p^v b$ , where the numerator and denominator of  $b$  are prime to  $p$ , then we write  $|a|_p = (1/p)^v$ . The exponent  $v$  is called the ordinal of  $a$  at  $p$  and is denoted by  $v = \text{ord}_p a$ .

(b)  $p = p_\infty$ . Then let  $|a|_{p_\infty}$  denote the ordinary absolute value.

(II)  $k = F(x)$ . Select a fixed number  $d$ ,  $0 < d < 1$ .

(a)  $p \neq p_\infty$ , so that  $p$  is an irreducible polynomial; write  $c = d^{\deg p}$ . If  $a \neq 0$  we write as in case I(a),  $a = p^v b$ ,  $v = \text{ord}_p a$ , and so we define  $|a|_p = c^v = d^{\deg p \cdot \text{ord}_p a}$ .

(b)  $p = p_\infty$ , so that  $|a| = c^{\deg a}$ , where  $c > 1$ . We choose  $c = 1/d$ , and so define  $|a|_{p_\infty} = d^{-\deg a}$ .

In all cases we have made a definite choice of  $|a|_p$  in the equivalence class corresponding to  $p$ ; we call this  $|a|_p$  the *normal valuation* at  $p$ .

The case where  $k = F(x)$ , where  $F$  is the field of all complex numbers, can be generalized as follows. Let  $D$  be a domain on the Gauss sphere and  $k$  the field of all functions meromorphic in  $D$ . If  $x_0 \in D$ ,  $x_0 \neq \infty$ , and  $f(x) \in k$ , we may write

$$f(x) = (x - x_0)^{\text{ord}_{x_0} f(x)} g(x),$$

where  $g(x) \in k$  ( $g(x_0) \neq 0$  or  $\infty$ ), and define a valuation by

$$|f(x)|_{x_0} = c^{\text{ord}_{x_0} f(x)}.$$

If  $x_0 = \infty$ , we write

$$f(x) = \left(\frac{1}{x}\right)^{\text{ord}_\infty f(x)} g(x),$$

where  $g(x) \in k$  ( $g(\infty) \neq 0$  or  $\infty$ ), and define

$$|f(x)|_\infty = c^{\text{ord}_\infty f(x)}.$$

This gives for each  $x_0 \in D$  a valuation of  $k$  — axioms (1) and (2) are obviously satisfied, while axiom (3) follows from

$$\begin{aligned} |f|_{x_0} \leq 1 &\Rightarrow f \text{ is regular at } x_0 \\ &\Rightarrow 1 + f \text{ is regular at } x_0 \\ &\Rightarrow |1 + f|_{x_0} \leq 1. \end{aligned}$$

The valuation  $| \cdot |_{x_0}$  obviously describes the behavior of  $f(x)$  at the point  $x_0$ :

If  $|f|_{x_0} < 1$ , or  $\text{ord}_{x_0}(f(x)) = n > 0$ , then  $f(x)$  has a zero of order  $n$  at  $x_0$ .

If  $|f|_{x_0} > 1$ , or  $\text{ord}_{x_0} f(x) = n < 0$ , then  $f(x)$  has a pole of order  $-n$  at  $x_0$ .

If  $|f|_{x_0} = 1$ , then  $f(x)$  is regular and non-zero at  $x_0$ .

Should  $D$  be the whole Gauss sphere, we have  $k = F(x)$ ; in this case the irreducible polynomials are linear of type  $(x - x_0)$ . The valuation  $|f(x)|_{x-x_0}$  as defined previously is now the valuation

denoted by  $|f(x)|_{x_0}$ ; the valuation given by  $|f(x)|_{p_\infty}$  is now denoted by  $|f(x)|_\infty$ . We see that to each point of the Gauss sphere there corresponds one of our valuations.

It was in analogy to this situation, that we introduced in the case  $k = R$ , the field of rational numbers, the “infinite prime” and associated it with the ordinary absolute value.

We now prove a theorem which establishes a relation between the normal valuations at all primes  $p$ :

**Theorem 9:** In both cases,  $k = R$  and  $k = F(x)$ , the product  $\prod_p |a|_p = 1$ .

We have already remarked that a relation of this form cannot be obtained for any finite number of valuations.

*Proof:* Only a finite number of primes (irreducible polynomials) divide a given rational number (rational function). Hence  $|a|_p = 1$  for almost all (i.e. all but a finite number of) primes  $p$ , and so the product  $\prod_p |a|_p$  is well-defined.

If we write  $\phi(a) = \prod_p |a|_p$  we see that  $\phi(ab) = \phi(a)\phi(b)$ ; thus it suffices to prove the result for  $a = q$ , where  $q$  is a prime (irreducible polynomial).

For  $q \in R$ ,

$$\phi(q) = |q|_q |q|_\infty = \left(\frac{1}{q}\right)^{\text{ord}_q q} \cdot q = \frac{1}{q} \cdot q = 1.$$

For  $q \in k(x)$ ,

$$\phi(q) = d^{\deg q \cdot \text{ord}_q q} \cdot d^{-\deg q} = d^{\deg q} \cdot d^{-\deg q} = 1.$$

This completes the proof.

We notice that this is essentially the only relation of the form  $\prod |a|_p^e = 1$ . For if  $\psi(a) = \prod |a|_p^e = 1$ , we have for each prime  $q$

$$\psi(q) = |q|_q^e |q|_\infty^e.$$

But  $|q|_q |q|_\infty = 1$  by the theorem; hence

$$\psi(q) = |q|_\infty^{-e} = 1.$$

Thus  $e_q = e_\infty$ , and our relation is simply a power of the one established before.

The product formula has a simple interpretation in the classical case of the field of rational functions with complex coefficients. In this case

$$\phi(a) = d \text{ number of zeros} - \text{number of poles} = 1;$$

so a rational function has as many zeros as poles.

Now that the valuations of the field of rational numbers have been determined, we can find the best constant  $c$  for our axiom (3).

**Theorem 10:** For any valuation, we may take

$$c = \max(|1|, |2|).$$

*Proof.* (1) When the valuation is non-archimedean,

$$c = 1 = |1| \geq |2|.$$

(2) When the valuation is archimedean,  $k$  must have characteristic zero; hence  $k$  contains  $R$ , the field of rational numbers. The valuation is archimedean on  $R$ , and hence is equivalent to the ordinary absolute value; suppose that for the rational integers  $n$  we have  $|n| = n^\beta$ . Write  $c = 2^\alpha$ ; then

$$|a + b| \leq 2^\alpha \max(|a|, |b|).$$

By the method of Theorem 3, we can deduce

$$|a_1 + \cdots + a_m| \leq (2m)^\alpha \max |a_\nu|.$$

As a special case of this we have

$$|a + b|^m \leq (2(m+1))^\alpha \max_\nu \binom{m}{\nu} |a|^\nu |b|^{m-\nu}.$$

Now

$$\binom{m}{\nu} \leq \binom{m}{\nu}^\beta \leq 2^{m\beta},$$

since

$$\sum \binom{m}{\nu} = (1+1)^m = 2^m.$$

Hence we have

$$|a + b|^m \leq (2(m+1))^\alpha 2^{m\beta} (\max(|a|, |b|))^m.$$

Taking the  $m$ -th root, and letting  $m \rightarrow \infty$ , we obtain

$$|a + b| \leq 2^\beta \max(|a|, |b|).$$

Since

$$2^\beta = |2| = \max(|1|, |2|),$$

our theorem is proved in this case also. Since the constant  $c$  for an extension field is the same as for the prime field contained in it, it follows that if the valuation satisfies the triangular inequality on the prime field, then it does so also on the extension field.

## 6. Completion of a Field

Let  $||$  be a valuation of a field  $k$ ; replace  $| |$ , if necessary, by an equivalent valuation for which the triangular inequality holds. A sequence of elements  $\{a_\nu\}$  is said to form a *Cauchy sequence* with respect to  $||$  if, corresponding to every  $\epsilon > 0$  there exists an integer  $N$  such that for  $\mu, \nu \geq N$ ,  $|a_\mu - a_\nu| < \epsilon$ .

A sequence  $\{a_\nu\}$  is said to form a *null-sequence* with respect to  $||$  if, corresponding to every  $\epsilon > 0$ , there exists an integer  $N$  such that for  $\nu \geq N$ ,  $|a_\nu| < \epsilon$ .

$k$  is said to be *complete* with respect to  $||$  if every Cauchy sequence with respect to  $||$  converges to a limit in  $k$ . We shall now sketch the process of forming the completion of a field  $k$ .

The Cauchy sequences form a ring  $P$  under termwise addition and multiplication:

$$\{a_\nu\} + \{b_\nu\} = \{a_\nu + b_\nu\}, \quad \{a_\nu\} \{b_\nu\} = \{a_\nu b_\nu\}.$$

It is easily shown that the null-sequences form a maximal ideal  $N$  in  $P$ ; hence the residue class ring  $P/N$  is a field  $\tilde{k}$ .

The valuation  $||$  of  $k$  naturally induces a valuation on  $\tilde{k}$ ; we still denote this valuation by  $||$ . For if  $a \in \tilde{k}$  is defined by the residue class of  $P/N$  containing the sequence  $\{a_\nu\}$ , we define  $|a|$  to be  $\lim_{\nu \rightarrow \infty} |a_\nu|$ . To justify this definition we must prove

(a) that if  $\{a_\nu\}$  is a Cauchy sequence, then so is  $\{|a_\nu|\}$ ,



(b) that if  $\{a_\nu\} \equiv \{b_\nu\} \pmod N$ , then  $\lim |a_\nu| = \lim |b_\nu|$ ,

(c) that the valuation axioms are satisfied.

The proofs of these statements are left to the reader.

If  $a \in k$ , let  $a'$  denote the equivalence class of Cauchy sequences containing  $(a, a, a, \dots)$ ;  $a' \in \tilde{k}$ . If  $a' = b'$ , then the sequence  $((a - b), (a - b), \dots) \in N$ , so that  $a = b$ . Hence the mapping  $\phi$  of  $k$  into  $\tilde{k}$  defined by  $\phi(a) = a'$  is  $(1, 1)$ ; it is easily seen to be an isomorphism under which valuations are preserved:  $|a'| = |a|$ . Let  $k' = \phi(k)$ ; we shall now show that  $k'$  is everywhere dense in  $\tilde{k}$ . To this end, let  $\alpha$  be an element of  $\tilde{k}$  defined by the sequence  $\{a_\nu\}$ . We shall show that for large enough values of  $\nu$ ,  $|\alpha - a'_\nu|$  is as small as we please. The element  $\alpha - a'_\nu$  is defined by the Cauchy sequence  $\{(a_1 - a_\nu), (a_2 - a_\nu), \dots\}$ , and

$$|\alpha - a'_\nu| = \lim_{\mu \rightarrow \infty} |a_\mu - a_\nu|;$$

but since  $\{a_\nu\}$  is a Cauchy sequence, this limit may be made as small as we please by taking  $\nu$  large enough.

Finally we prove that  $\tilde{k}$  is complete. Let  $\{a_\nu\}$  be a Cauchy sequence in  $\tilde{k}$ . Since  $k'$  is everywhere dense in  $\tilde{k}$ , we can find a sequence  $\{a'_\nu\}$  in  $k'$  such that  $|a'_\nu - a_\nu| < 1/\nu$ . This means that  $\{(a'_\nu - a_\nu)\}$  is a null-sequence in  $\tilde{k}$ ; hence  $\{a'_\nu\}$  is a Cauchy sequence in  $\tilde{k}$ . Since absolute values are preserved under the mapping  $\phi$ ,  $\{a_\nu\}$  is a Cauchy sequence in  $k$ . This defines an element  $\beta \in \tilde{k}$  such that  $\lim_{\nu \rightarrow \infty} |a'_\nu - \beta| = 0$ . Hence  $\lim_{\nu \rightarrow \infty} |\alpha_\nu - \beta| = 0$ , i.e.  $\beta = \lim \alpha_\nu$ , and so  $\tilde{k}$  is complete.

We now agree to identify the elements of  $k'$  with the corresponding elements of  $k$ ; then  $\tilde{k}$  may be regarded as an extension of  $k$ . When  $k$  is the field of rational numbers, the completion under the ordinary absolute value ("the completion at the infinite prime") is the real number field; the completion under the valuation corresponding to a finite prime  $p$  ("the completion at  $p$ ") is called the *field of  $p$ -adic numbers*.

## CHAPTER TWO

# Complete Fields

### 1. Normed Linear Spaces

Let  $k$  be a field complete under the valuation  $|\cdot|$ , and let  $S$  be a finite-dimensional vector space over  $k$ , with basis  $\omega_1, \omega_2, \dots, \omega_n$ . Suppose  $S$  is normed; i.e. to each element  $\alpha \in S$  corresponds a real number  $\|\alpha\|$ , which has the properties

- (1)  $\|\alpha\| \geq 0$ ;  $\|\alpha\| = 0$  if and only if  $\alpha = 0$ ,
- (2)  $\|\alpha + \beta\| \leq \|\alpha\| + \|\beta\|$ ,
- (3)  $\|x\alpha\| = |x| \|\alpha\|$  for all  $x \in k$ .

(We shall later specialize  $S$  to be a finite extension field of  $k$ ; the norm  $\|\cdot\|$  will then be an extension of the valuation  $|\cdot|$ .) There are many possible norms for  $S$ ; for example, if

$$\beta = x_1\omega_1 + \dots + x_n\omega_n,$$

then

$$\|\beta\|_0 = \max_\nu |x_\nu|$$

is a norm. This particular norm will be used in proving

**Theorem 1:** All norms induce the same topology in  $S$ .

*Proof:* The theorem is obviously true when the dimension  $n = 1$ . For then  $\beta = x\omega$  and  $\|\beta\| = |x| \|\omega\| = c|x|$  ( $c \neq 0$ ); hence any two norms can differ only in the constant factor  $c$ ; this does not alter the topology.

We may now proceed by induction; so we assume the theorem true for spaces of dimension up to  $n - 1$ .

We first contend that for any  $\epsilon > 0$  there exists an  $\eta > 0$  such that  $\|\alpha\| < \eta$  implies  $|x_n| < \epsilon$ .

For if not, there is an  $\epsilon > 0$  such that for every  $\eta > 0$  we can find an element  $\alpha$  with  $\|\alpha\| < \eta$ , but  $|x_n| \geq \epsilon$ . Set  $\beta = \alpha/x_n$ ; then

$$\|\beta\| = \frac{\|\alpha\|}{|x_n|} \leq \frac{\eta}{\epsilon}, \quad \text{and} \quad \beta = y_1\omega_1 + \cdots + y_{n-1}\omega_{n-1} + \omega_n.$$

Thus if we replace  $\eta$  by  $\eta\epsilon$ , we see that for every  $\eta > 0$  we can find an element  $\beta$  of this form with  $\|\beta\| < \eta$ . We may therefore form a sequence  $\{\beta_\nu\}$ :

$$\beta_\nu = y_1^{(\nu)}\omega_1 + \cdots + y_{n-1}^{(\nu)}\omega_{n-1} + \omega_n,$$

with  $\|\beta_\nu\| < 1/\nu$ . Then

$$\beta_\nu - \beta_\mu = \sum_{i=1}^{n-1} (y_i^{(\nu)} - y_i^{(\mu)})\omega_i,$$

and

$$\|\beta_\nu - \beta_\mu\| \leq \|\beta_\nu\| + \|\beta_\mu\| < \frac{1}{\nu} + \frac{1}{\mu}.$$

By the induction hypothesis, the norm  $\|\cdot\|$  on the  $(n-1)$ -dimensional subspace  $(\omega_1, \dots, \omega_{n-1})$  induces the same topology as the special norm  $\|\cdot\|_0$ . That is,

$$\|\beta_\nu - \beta_\mu\| \text{ small} \Rightarrow \|\beta_\nu - \beta_\mu\|_0 \text{ small} \Rightarrow |y_i^{(\nu)} - y_i^{(\mu)}|$$

small if  $\nu, \mu$  are large  $\Rightarrow \{y^{(\nu)}\}$  is a Cauchy sequence in  $k$ . Since  $k$  is complete, there exist elements  $z_i \in k$  such that

$$z_i = \lim_{\nu \rightarrow \infty} \{y_i^{(\nu)}\}.$$

Set

$$\gamma = z_1\omega_1 + \cdots + z_{n-1}\omega_{n-1} + \omega_n.$$

Then

$$\begin{aligned} \|\gamma - \beta_\nu\| &= \| (z_1 - y_1^{(\nu)})\omega_1 + \cdots + (z_{n-1} - y_{n-1}^{(\nu)})\omega_{n-1} \| \\ &\leq |z_1 - y_1^{(\nu)}| \|\omega_1\| + \cdots + |z_{n-1} - y_{n-1}^{(\nu)}| \|\omega_{n-1}\| < \epsilon \end{aligned}$$

if  $\nu$  is large enough. Hence

$$\|\gamma\| = \|\gamma - \beta_\nu + \beta_\nu\| \leq \|\gamma - \beta_\nu\| + \|\beta_\nu\| < \epsilon + \frac{1}{\nu};$$

i.e.  $\|\gamma\|$  is smaller than any chosen  $\eta$ :  $\|\gamma\| = 0$ , and so  $\gamma = 0$ . In other words,

$$z_1\omega_1 + \cdots + z_{n-1}\omega_{n-1} + \omega_n = 0,$$

which contradicts the linear independence of the basis elements  $\omega_1, \dots, \omega_n$ . This completes the proof of our assertion. From this we deduce at once that:

For any  $\epsilon > 0$ , there exists an  $\eta > 0$  such that if  $\|\alpha\| < \eta$ , then  $\|\alpha\|_0 < \epsilon$ . Thus the topology induced by norm  $\|\cdot\|$  is stronger than that induced by the special norm  $\|\cdot\|_0$ .

Finally, since

$$\begin{aligned} \|\alpha\| &\leq |x_1| \|\omega_1\| + \cdots + |x_n| \|\omega_n\| \\ &\leq \|\alpha\|_0 (\|\omega_1\| + \cdots + \|\omega_n\|), \end{aligned}$$

the topology induced by  $\|\cdot\|_0$  is stronger than that induced by  $\|\cdot\|$ .

This completes the proof of our theorem.

**Corollary:** Let  $\{\beta_\nu\}$ ,  $\beta_\nu = \sum x_i^{(\nu)}\omega_i$  be a Cauchy sequence in  $S$ . Then the sequences  $\{x_i^{(\nu)}\}$  ( $i = 1, \dots, n$ ) are Cauchy sequences in  $k$ , and conversely.

## 2. Extension of the Valuation

We now apply these results to the case of an extension field. Let  $k$  be a complete field,  $E$  a finite extension of  $k$ . Our task is to extend the valuation of  $k$  to  $E$ . Suppose for the moment we have carried out this extension; then the extended valuation  $|\cdot|$  on  $E$  is a norm of  $E$  considered as a vector space over  $k$ , and we have

**Theorem 2:**  $E$  is complete under the extended valuation.

*Proof:* Let  $\{\beta_\nu\}$  be a Cauchy sequence in  $E$ :  $\beta_\nu = \sum x_i^{(\nu)}\omega_i$ . By the corollary to Theorem 1, each  $\{x_i^{(\nu)}\}$  is a Cauchy sequence in  $k$ , and so has a limit  $y_i \in k$ . Hence

$$\lim \beta_\nu = \sum y_i\omega_i \in E.$$

Thus  $E$  is complete. Now let  $\alpha$  be an element of  $E$  for which  $|\alpha| < 1$ ; then  $|\alpha|^v \rightarrow 0$ ; hence  $\{\alpha^v\}$  is a null-sequence. Thus if

$$\alpha^v = x_1^{(v)}\omega_1 + \cdots + x_n^{(v)}\omega_n,$$

each sequence  $\{x_i^{(v)}\}$  is a null-sequence in  $k$ .

The norm of  $\alpha$ ,  $N(\alpha)$ , is a homogeneous polynomial in  $x_1, \dots, x_n$ . Hence

$$N(\alpha^v) \rightarrow 0 \Rightarrow (N(\alpha))^v \rightarrow 0 \Rightarrow |N(\alpha)|^v \rightarrow 0 \Rightarrow |N(\alpha)| < 1.$$

Hence we have proved that  $|\alpha| < 1 \Rightarrow |N(\alpha)| < 1$ ; similarly we can obtain  $|\alpha| > 1 \Rightarrow |N(\alpha)| > 1$ . Thus

$$|N(\alpha)| = 1 \Rightarrow |\alpha| = 1.$$

Now consider any  $\alpha \in E$ , and set  $\beta = \alpha^n/N(\alpha)$  where

$$n = \deg(E|k).$$

Then

$$N(\beta) = \frac{N(\alpha^n)}{N(N(\alpha))} = \frac{(N(\alpha))^n}{(N(\alpha))^n} = 1,$$

hence  $|\beta| = 1$ . Therefore

$$|\alpha|^n = |N(\alpha)| \text{ and } |\alpha| = \sqrt[n]{|N(\alpha)|}.$$

We have proved that if it is possible to find an extension of the valuation to  $E$ , then  $E$  is complete under the extension; and the extended valuation is given by  $|\alpha| = \sqrt[n]{|N(\alpha)|}$ . Hence to establish the possibility of extending the valuation, it will be sufficient to show that  $f(\alpha) = \sqrt[n]{|N(\alpha)|}$  coincides with  $|\alpha|$  for  $\alpha \in k$ , and satisfies the valuation axioms for  $\alpha \in E$ . Certainly if  $\alpha \in k$ ,

$$\sqrt[n]{|N(\alpha)|} = \sqrt[n]{|\alpha|^n} = |\alpha|;$$

and using the properties of the norm  $N(\alpha)$ , we can easily verify that axioms (1) and (2) are satisfied. Thus it remains to prove that for some  $C$ ,

$$|N(\alpha)| \leq 1 \Rightarrow |N(1 + \alpha)| \leq C.$$

To establish this we must treat the archimedean and non-archimedean cases separately.

**Theorem 3:** If  $k$  is complete under the valuation  $|\cdot|$ , then the valuation can be extended to  $E = k(i)$  where  $i^2 + 1 = 0$ .

*Proof:* (1) If  $i \in k$ , then  $E = k$ , and the proof is trivial. (2) If  $i \notin k$ , then  $E$  consists of elements  $\alpha = a + bi$ , ( $a, b \in k$ ),  $N(\alpha) = a^2 + b^2$ . Hence we must show that

$$|a^2 + b^2| \leq 1 \Rightarrow |(1 + a)^2 + b^2| \leq C,$$

or, equivalently, that  $|a| \leq D$  for some  $D$ .

Suppose that this is not the case; then for some  $\alpha = a + ib$ ,  $|1 + b^2/a^2| \leq |1/a^2|$  is arbitrarily small. Thus  $|x^2 + 1|$  takes on arbitrarily small values. We construct a sequence  $\{x_v\}$  in  $k$  such that

$$|x_v^2 + 1| \leq \frac{1}{2 \cdot 4^v}.$$

Then

$$|x_v^2 - x_{v+1}^2| = |(x_v^2 + 1) - (x_{v+1}^2 + 1)| \leq \frac{1}{4^v},$$

or

$$|x_v - x_{v+1}| |x_v + x_{v+1}| \leq \frac{1}{4^v};$$

hence one factor  $\leq 1/2^v$ . We now adjust the signs of the  $\{x_v\}$ ; suppose this has been done as far as  $x_v$ ; then we adjust the sign of  $x_{v+1}$  in such a way that  $|x_v - x_{v+1}| \leq 1/2^v$ . This adjusted sequence is a Cauchy sequence, for

$$\begin{aligned} |x_v - x_{v+\mu}| &\leq |x_v - x_{v+1}| + |x_{v+1} - x_{v+2}| + \cdots \\ &\quad + |x_{v+\mu-1} - x_{v+\mu}| \leq \frac{1}{2^{v-1}}. \end{aligned}$$

Since  $k$  is complete, this sequence has a limit  $j \in k$ . Then

$$j^2 + 1 = \lim_{v \rightarrow \infty} x_v^2 + 1 = 0,$$

contradicting our hypothesis that  $\sqrt{-1} \notin k$ . This completes the proof.

## 3. Archimedean Case

The following theorem now completes our investigation in the case of complete archimedean fields.

**Theorem 4:** The only complete archimedean fields are the real numbers and the complex numbers.

*Proof:* Let  $k$  be a field complete under an archimedean valuation. Then  $k$  has characteristic zero, and so contains a subfield  $R$  isomorphic to the rational numbers. The only archimedean valuations of the rationals are those equivalent to the ordinary absolute value; so we may assume that the valuation of  $k$  induces the ordinary absolute value on  $R$ . Hence  $k$  contains the completion of  $R$  under this valuation, namely the real number field  $P$ ; thus  $E = k(i)$  contains the field of complex numbers  $P(i)$ . We shall prove that  $E$  is in fact itself the field of complex numbers.

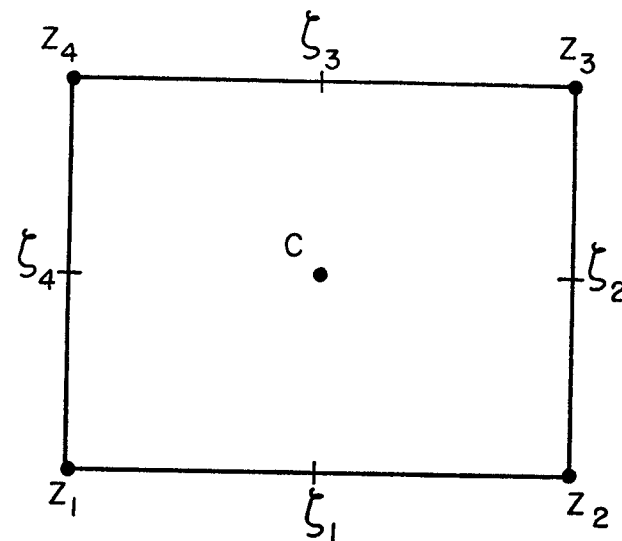
We can, and shall, in fact, prove rather more than this—namely, that any complete normed field over the complex numbers is itself the field of complex numbers. In a normed field, a function  $\| \cdot \|$  is defined for all elements of the field, with real values, satisfying the following conditions:

- (1)  $\| \alpha \| \geq 0$ ;  $\| \alpha \| = 0$  if and only if  $\alpha = 0$ ,
- (2)  $\| \alpha + \beta \| \leq \| \alpha \| + \| \beta \|$ ,
- (3)  $\| z\alpha \| = |z| \| \alpha \|$  for  $z \in P(i)$ ,
- (4)  $\| \alpha\beta \| \leq \| \alpha \| \cdot \| \beta \|$ .

We shall show that any such field  $E = P(i)$ . The proof can be carried through by developing a theory of “complex integration” for  $E$ , similar to that for the complex numbers; the result follows by applying the analogue of Cauchy’s Theorem. Here we avoid the use of the integral, by using approximating sums.

Given a square  $(z_1, z_2, z_3, z_4)$  in the complex plane, having  $c$  as center and  $\zeta_1, \zeta_2, \zeta_3, \zeta_4$  as midpoints of the sides, we define an operator  $L_Q$  by

$$L_Q = \sum (z_{\nu+1} - z_\nu) f(\zeta_\nu).$$



It is easily verified that  $L$  is a linear homogeneous functional, such that  $L(z) = L(1) = 0$ , and hence vanishing on every linear function.

First we show that  $1/x$  is continuous for  $x = \beta \neq 0$  ( $\beta \in E$ ). Let  $\xi \in E$  and  $\| \xi \| < \| \beta^{-1} \|^{-1}$ ; then  $\| \xi/\beta \| \leq \| \xi \| \| \beta^{-1} \| < 1$ . Since  $\| (\xi/\beta)^n \| \leq \| \xi/\beta \|^n$ , the geometric series  $1/\beta \sum_0^\infty \xi^n/\beta^n$  converges absolutely; hence it converges to an element of  $E$  which is easily seen to be  $1/(\beta - \xi)$ . Now take  $\| \xi \| \leq \frac{1}{2} \| \beta^{-1} \|^{-1}$ . We have

$$\frac{1}{\beta - \xi} - \frac{1}{\beta} = \frac{1}{\beta} \sum_1^\infty \frac{\xi^n}{\beta^n},$$

so that

$$\left\| \frac{1}{\beta - \xi} - \frac{1}{\beta} \right\| \leq \left\| \frac{1}{\beta} \right\| \sum_1^\infty \| \xi \|^n \| \beta^{-1} \|^n \leq \| \xi \| \| \beta^{-1} \|^2,$$

which can be made as small as we please by choosing  $\| \xi \|$  small enough. This is precisely the condition that  $1/x$  be continuous at  $x = \beta$ .