A Study of Absolute Values

Rahul Kumar

A dissertation submitted for the partial fulfilment of BS-MS dual degree in Science

Indian Institute of Science Education and Research Mohali

April 2014

Certificate of Examination

This is to certify that the dissertation titled **A Study of Absolute Values** submitted by **Mr. Rahul Kumar** (Reg. No. MS09101) for the partial fulfilment of BS-MS dual degree programme of the institute, has been examined by the thesis committee duly appointed by the institute. The committee finds the work done by the candidate satisfactory and recommends that the report be accepted.

Prof.I.B.S.Passi	Dr.Amit Kulshrestha	Prof. Sudesh Kaur Khanduja (Supervisor)

Dated: April 25, 2014

Declaration

The work presented in this dissertation has been carried out by me under the guidance of **Prof. Sudesh Kaur Khanduja** at Indian Institute of Science Education and Research Mohali.This work has not been submitted in part or in full for a degree, a diploma, or a fellowship to any other university or institute. This is a bonafide record of original study done by me and all sources listed within have been detailed in the bibliography.

Rahul Kumar
(candidate)
Dated: April 12,2014

In my capacity as the supervisor of the candiadte's project work, I certify that the above statements made by the candidates are true to the best of my knowledge.

Sudesh Kaur Khanduja
(Supervisor)

Acknowledgement

I am gleeful to see that my final year project work has came through. In this regard, I would like to thank my Project supervisor Prof. Sudesh Kaur Khanduja firstly for allowing me to work under her guidance and for introducing me to the topic.

I would also like to thank Dr. Amit kulshrestha for his valuable suggestions. I would also express my gratitude towards institute-library and CAF.

I would be ungrateful to not include my family members who always supported me emotionally and financially. Special thanks goes to my friends Chaudhary, Jyosmita, Titiksh, Amit, Leena, Bablesh Kumari, research scholar, Dept. of Mathematics, Panjab University who always backed me up whenever I felt low.

Rahul Kumar
April,2014.

Contents

Abstract

The notion of an absolute value of a field K is a generalization of the notion of ordinary absolute value of the field $\mathbb{C}$ of complex numbers. A real valued function ϕ defined on a field K into non-negative real numbers is called absolute value of K if $\phi(x) = 0 \Leftrightarrow x = 0, \phi(xy) = \phi(x)\phi(y)$ and $\phi(x + y) \leq \phi(x) + \phi(y)$ $\forall x, y \in K$. In this thesis, we study absolute values and its basic properties and some significant results like Ostrowski's Theorem, Approximation Theorem and Independence Theorem. We also discuss Archimedean and non-Archimedean absolute values, completion of fields with respect to absolute values. A non-Archimedean absolute value gives rise to what is called (additive) valuation. A detailed exposition of discrete valuations is brought out. We also study Hensel's Lemma and some of its applications.

Chapter 1

Archimedean and Non-Archimedean Absolute Values

1.1 Introduction

The development of absolute values has a long history. It has its roots in the theory of p-adic numbers developed by Kurt Hensel in the first decade of 20th century. Motivated by the work of Hensel on the field of p-adic numbers, it was the Hungarian mathematician Josef Kürschàk who gave the formal definition of absolute value during the Cambridge International Congress of Mathematicians in 1912. According to him, the notion of an absolute value of a field K is a generalization of the notion of ordinary absolute value of the field $\mathbb{C}$ of complex numbers. An absolute value of field K is a mapping ϕ from K into real numbers satisfying the following axioms for all $a, b \in K$:

Definition A real valued function ϕ defined on a field K is called an absolute value on K if it satisfies the following three conditions:
(I) $\phi(x) \geq 0, \phi(x) = 0 \Longleftrightarrow x = 0.$
(II) $\phi(xy) = \phi(x)\phi(y)$
(III) $\phi(x + y) \leq \phi(x) + \phi(y) \ \forall \ x, y \in K.$

Definition The absolute value sending every non-zero $x \in K$ to 1 is called the trivial absolute value.

Properties

For an absolute value ϕ, the following holds:

(1) $\phi(\xi) = 1$ for any root of unity $\xi \in K$; in particular $\phi(1) = \phi(-1) = 1$ and $\phi(-x) = \quad \phi(x), \forall\ x \in K$.

(2)$\phi(x^{-1}) = \phi(x)^{-1}$ for all $x \neq 0 \in K$.

(3) $\phi(x-y) \geq \mid \phi(x) - \phi(y) \mid \ \ \forall\ x, y \in K$.

Examples (1) The ordinary absolute values of $\mathbb{R}$ and $\mathbb{C}$.

(2) Let p be a prime number and $0 < c < 1$ be a real number. Any non-zero rational number x can be uniquely written as $x = p^r m/n, r, m, n \in \mathbb{Z}, n > 0, (m, n) = 1, p \nmid mn$.

Define $\phi_p(x) = c^r$. It can be easily checked that $\phi_p(x+y) \leq max\{\phi_p(x), \phi_p(y)\}$ for all $x, y \in \mathbb{Q}$ and thus ϕ_p is an absolute value on $\mathbb{Q}$. It is called a $p-adic$ absolute value of $\mathbb{Q}$.

Remark If R is an integral domain with quotient field K and ϕ is a mapping from R into $\mathbb{R}^+ \cup \{0\}$ satisfying the three properties of an absolute value, then ϕ can be uniquely extended to an absolute value of K in an obvious way.

Proposition 1.1 *The set* $\{\phi(n.1) \mid n \in \mathbb{Z}\}$ *is bounded if and only if* ϕ *satisfies the ultrametric inequality* $\phi(x+y) \leq max\,\{\phi(x), \phi(y)\}\,\forall\ x, y \in K$.

Proof. Suppose first that $\phi(x+y) \leq max\,\{\phi(x), \phi(y)\}$ for all $x, y \in K$. Clearly the set $\{\phi(n.1) \mid n \in \mathbb{Z}\}$ is same as $\{\phi(0), \phi(1), \phi(2), \cdots\}$. For any $n \in \mathbb{N}, \phi(n)$ $\leq$ max $\{\phi(n-1), \phi(1)\}$.Since $\phi(1) = 1$,it follows using induction that $\phi(n) \leq 1\ \forall\ n \in \mathbb{N}$.

Conversely suppose that $\{\phi(n.1) \mid n \in \mathbb{Z}\}$ is bounded by a constant c. Consider

$(\phi(x+y))^n$ for $x, y \in K$ and n a positive integer,

$$(\phi(x+y))^n = \phi((x+y)^n) = \phi(\sum_{m=0}^{n} {}^nC_m x^m y^{n-m})$$

$$\leq \sum_{m=0}^{n} \phi({}^nC_m)(\phi(x)^m \phi(y)^{n-m})$$
$$\leq (n+1)c\ max\left\{\phi(x), \phi(y)\right\}^n$$

Taking nth root and letting $n \longrightarrow \infty$, using the fact that $\lim_{n\to\infty} (n+1)^{1/n} = 1$. we see that $\phi(x+y) \leq max\left\{\phi(x), \phi(y)\right\}$. □

Definition An absolute value ϕ on a field K is said to be non-Archimedean if it satisfies ultrametric inequality i.e. $\phi(x+y) \leq \max\ \{\phi(x), \phi(y)\}$ for all $x, y \in K$, otherwise it is called Archimedean.

Strong triangle law Let ϕ be a non-Archimedean absolute value of a field K. If $x, y \in K$ and $\phi(x) \neq \phi(y)$, then $\phi(x+y) = max\{\phi(x), \phi(y)\}$.

Proof. Assume that $\phi(x) < \phi(y)$.By definition of non-Archimedean absolute value

$$\phi(x+y) \leq max\{\phi(x), \phi(y)\} = \phi(y)$$

Again by definition of non-Archimedean

$$\phi(y) = \phi(x+y-x) \leq max\{\phi(x+y), \phi(x)\} \tag{1.1}$$

and the maximum in (1.1) has to be $\phi(x+y)$ in view of the assumption $\phi(x) < \phi(y)$. Hence $\phi(x+y) = \phi(y)$.

Note If *characteristic* of a field K is non-zero, then K has no Archimedean absolute value in view of Proposition 1.1.

Remark If ϕ is an absolute value on a field K and $0 < \lambda \leq 1$ is a real number, then ϕ^λ is also an absolute value of K.

Proof. It is enough to show that for all $x, y \in K$.

$$(\phi(x+y))^\lambda \leq (\phi(x))^\lambda + (\phi(y))^\lambda$$

without loss of generality, we can assume that $\phi(x) \geq \phi(y)$.

$$(\phi(x+y))^\lambda \leq (\phi(x) + \phi(y))^\lambda = (\phi(x))^\lambda (1 + \phi(y)/\phi(x))^\lambda \tag{1.2}$$

Since 0< $\lambda \leq 1$ and $\phi(y)/\phi(x) \leq 1$, we have

$$(1 + \phi(y)/\phi(x))^\lambda \leq 1 + \phi(y)/\phi(x) \leq 1 + (\phi(y))^\lambda/(\phi(x))^\lambda.$$

The above inequality together with (1.2) implies that

$$(\phi(x+y))^\lambda \leq (\phi(x))^\lambda + (\phi(y))^\lambda.$$

Proposition 1.2 *An absolute value ϕ is non-archimedean iff ϕ^λ is an absolute value for every real λ >0.*

Proof. Suppose first that $\phi(x+y) \leq max\{\phi(x), \phi(y)\} \ \forall \ x, y \in K$. So, $(\phi(x+y))^\lambda \leq (max\{\phi(x), \phi(y)\})^\lambda = max\{\phi(x)^\lambda, \phi(y)^\lambda\} \leq \phi(x)^\lambda + \phi(y)^\lambda \ \forall \ \lambda > 0$ and hence ϕ^λ is an absolute value.

Conversely suppose that ϕ^λ is an absolute value $\forall \ \lambda > 0$. In view of Proposition 1.1, it is enough to show that the set $\{\phi(n.1)/n \in \mathbb{Z}\}$ is bounded. Fix a positive integer n, for any $\lambda > 0$,we have

$$(\phi(n.1))^\lambda \leq \phi(1)^\lambda + \phi(1)^\lambda + \cdots + \phi(1)^\lambda = n\phi(1) = n \tag{1.3}$$

This is possible only when $\phi(n.1) \leq 1$, otherwise the L.H.S. of (1.3) will approach ∞ as λ tends to ∞. Thus we have shown that the set $\{\phi(n) \mid n \in \mathbb{Z}\}$ is bounded and ϕ is non-Archimedean by Proposition 1.1. □

Proposition 1.3 *If ϕ is a function defined on a field K satisfying $\phi(x) > 0$ for every non-zero $x \in K, \phi(0) = 0, \ \phi(xy) = \phi(x)\phi(y)$ for all $x, y \in K$ and $\phi(x+y) \leq 2 \ max\{\phi(x), \phi(y)\}$. Then ϕ is an absolute value on K.*

Proof. We first verify that for any finitely many elements $x_1, \cdots, x_m \; of \; K$, we have

$$\phi(x_1 + x_2 + \cdots + x_m) \leq 2m \sum_{i=0}^{m} \phi(x_i) \tag{1.4}$$

Choose an integer r such that $2^{r-1} \leq m < 2^r$. On taking $x_i = 0$ for $m < i \leq 2^r$ and using the hypothesis $\phi(x+y) \leq 2\, max\{\phi(x), \phi(y)\}$, we see that $\phi(x_1+x_2+\cdots+x_m) = \phi(x_1 + \cdots + x_{2^r}) \leq 2^r max_{(1 \leq i \leq m)}\{\phi(x_i)\}$ which implies (1.4). Taking each $x_i = 1$, the above inequality shows that for each positive integer m, we have

$$\phi(m) \leq 2m \tag{1.5}$$

For any elements $x, y \in K$, we now verify $\phi(x+y) \leq \phi(x) + \phi(y)$.

Let n be a positive integer. Using (1.4),(1.5) and multiplicative property of ϕ, we see that

$$(\phi(x+y))^n = \phi((x+y)^n) = \phi(\sum_{i=0}^{n} {}^nC_i x^i y^{n-i})$$

$$\leq 2(n+1) \sum_{i=0}^{n} \phi({}^nC_i)\phi(x)^i \phi(y)^{n-i}$$

$$\leq 2(n+1) \sum_{i=0}^{n} 2({}^nC_i)\phi(x)^i \phi(y)^{n-i}$$

$$= 4(n+1)(\phi(x) + \phi(y))^n.$$

Taking the nth root of the first and the last term of this inequality and letting n tend to infinity, we obtain $\phi(x+y) \leq \phi(x)+\phi(y)$. □

Definition Two absolute value ϕ_1 and ϕ_2 of K are called equivalent if $\exists$ a real number $\rho > 0$ such that $\phi_1(x) = \phi_2(x)^\rho$ for all $x \in K$.

The following theorem was proved by Alexander Ostrowski in 1916. The proof given below is due to Artin.

Theorem 1.4 ***Ostrowski's Theorem*** *(a) Every Archimedean absolute value on $\mathbb{Q}$ is equivalent to the usual one(ordinary absolute value).*

(b)Every non-trivial non-Archimedean absolute value of $\mathbb{Q}$ is equivalent to a p-adic absolute value.

Proof: (a) Let ϕ be a non-trivial Archimedean absolute values on $\mathbb{Q}$. So, $\exists$ some natural number $a > 0$ for which $\phi(a) > 1$. Since, for any $n \in \mathbb{N}$,

$$\phi(n) = \phi(1 + 1 + \cdots + 1) \leq \phi(1) + \phi(1) + \cdots + \phi(1) = n \tag{1.6}$$

we may set

$$\phi(a) = a^{\alpha} \tag{1.7}$$

where α is a real number $0 < \alpha \leq 1$. We show that any natural number N, $\phi(N) = N^{\alpha}$. Taking an arbitrary natural number N, we decompose it in power of a.
$N = x_0 + x_1 a + \cdots + x_{k-1}a^{k-1}$ where $0 \leq x_i \leq a - 1, 0 \leq i \leq k - 1, x_{k-1} \geq 1$. Clearly N satisfies the inequality

$$a^{k-1} \leq N < a^k.$$

Now formula (1.6) and (1.7) yield

$$\phi(N) \leq \phi(x_0) + \phi(x_1)\phi(a) + \cdots + \phi(x_{k-1})\phi(a)^{k-1}$$

$$\leq (a-1)(1 + a^{\alpha} + a^{2\alpha} + \cdots + a^{(k-1)\alpha})$$

$$= (a-1)\frac{a^{k\alpha} - 1}{a^{\alpha} - 1} < (a-1)\frac{a^{k\alpha}}{a^{\alpha} - 1} = (a-1)\frac{a^{\alpha}a^{(k-1)\alpha}}{a^{\alpha} - 1}.$$

Set $C = (a-1)\frac{a^{\alpha}}{a^{\alpha}-1}$; C does not depend on N. We have shown above that

$$\phi(N) < CN^{\alpha}.$$

Replacing N by N^m in this inequality, for m a natural number, then $\phi(N)^m = \phi(N^m) < CN^{m\alpha}, i.e.\ \phi(N) < C^{1/m}N^{\alpha}$. Letting m tend to infinity, we arrive at

$$\phi(N) \leq N^{\alpha} \tag{1.8}$$

To prove equality in (1.8), we write $N = a^k - b$, where $0 < b \leq a^k - a^{k-1}$. Then $\phi(N) \geq \phi(a^k) - \phi(b) = a^{k\alpha} - \phi(b)$. By virtue of (1.8), $\phi(b) \leq b^{\alpha} \leq (a^k - a^{k-1})^{\alpha}$, so

$$\phi(N) \geq a^{k\alpha} - (a^k - a^{k-1})^{\alpha} = a^{k\alpha}(1 - (1 - \frac{1}{a})^{\alpha}) > C_1 N^{\alpha},$$

where $C_1 = (1-(1-\frac{1}{a})^{\alpha})$ does not depend on N.
If N is replaced by N^m in the preceding inequality, then

$$\phi(N)^m = \phi(N^m) > C_1 N^{m\alpha}$$

which gives $\phi(N) > C_1^{1/m} N^{\alpha}$ and as $m \longrightarrow \infty$, this yields

$$\phi(N) \geq N^{\alpha} \tag{1.9}$$

comparing (1.8) and (1.9), we see that $\phi(N) = N^{\alpha}$ for every natural number N.
Now let $x = \pm N_1/N_2$ be an arbitrary rational number different from zero, then

$$\phi(x) = \phi(N_1/N_2) = \phi(N_1)/\phi(N_2) = N_1^{\alpha}/N_2^{\alpha} = |x|^{\alpha}$$

So ϕ is equivalent to usual absolute value.

(b)We now turn to the case when $\phi(n) \leq 1$ for all numbers n. If for every prime p, we have $\phi(p) = 1$, then by the multiplicative property of absolute value, we have $\phi(n) = 1$ for all $n \in \mathbb{N}$. Thus also $\phi(x) = 1 \ \forall$ rational $x \neq 0$. But this would contradict the assumption that ϕ is non trivial.Thus for some prime p, we have $\phi(p) < 1$. Claim is that if $q \neq p$ is a prime,then $\phi(q) = 1$. Suppose to the contrary $\phi(q) < 1$,then $\exists$ positive exponents k and l so that $\phi(p)^k < 1/2, \ \phi(q)^l < 1/2$.
Since p^k and q^l are relatively prime, there are integers u and v such that $up^k + vq^l = 1$.
As $\phi(u) \leq 1, \phi(v) \leq 1$, we would have

$$1 = \phi(1) = \phi(up^k + vq^l) \leq \phi(u)\phi(p)^k + \phi(v)\phi(q)^l < 1/2 + 1/2.$$

This contradiction proves the claim. Set $\phi(p) = \rho < 1$. Let $x = p^m(a/b)$ be a non-zero rational number, $p \nmid ab, a, b \in \mathbb{Z}$. Then $\phi(x) = \rho^m$.
So,ϕ is a p-adic absolute value in this case. □

Definition An absolute value ϕ on a field K defines a metric on K if the distance between two points $x, y \in K$ is defined as $\phi(x-y)$. This metric and the corresponding topology are said to be induced by ϕ. Clearly equivalent absolute values on a field induce the same topology.The following theorem shows that the converse also holds.

Theorem 1.5 *For any non-trivial absolute values ϕ_1, ϕ_2 of a field K, the following statements are equivalent:*
(i) ϕ_1 is equivalent to ϕ_2.
(ii) ϕ_1 and ϕ_2 induce the same topology on K.
(iii) The topology induced by ϕ_1 is stronger than the one induced by ϕ_2.
(iv) For any $x \in K$, $\phi_1(x) < 1$ implies $\phi_2(x) < 1$.
(v) For any $x \in K$, $\phi_1(x) \leq 1$ if and only if $\phi_2(x) \leq 1$.

For the proof of above proposition, we need the following Lemma.

Lemma 1.6 *Let G be an arbitrary group and let ϕ and ψ be homomorphisms from G into the multiplicative group of positive real numbers. Suppose that ϕ is non-trivial and $\psi(a) < 1$ holds whenever $\phi(a) < 1$ holds. Then there exists a positive number α such that $\psi(a) = (\phi(a))^\alpha$ holds for every $a \in G$.*

Proof. Since ϕ is non-trivial, there exits an element $c \in G$ such that $\phi(c) \neq 1$. As $\phi(c^{-1}) = \phi(c)^{-1}$, replacing c by its inverse if necessary we may assume that $\phi(c) > 1$. Then by hypothesis, we have $\psi(c^{-1}) < 1$ and hence $\psi(c) > 1$ holds. Let us set $\phi(c) = \mu$, $\psi(c) = \gamma$ and determine a positive real number α by $\gamma = \mu^\alpha$, we shall now show that $\psi(b) = \phi(b)^\alpha$ holds for any element $b \in G$. Let b be an element of G such that $\phi(b) > 1$. As $\mu > 1$, for any given positive integer m, an integer $n = n(m)$ satisfying the inequalities

$$\mu^{n-1} < \phi(b)^m < \mu^{n+1} \tag{1.10}$$

we clearly have $\lim_{m\to\infty} n(m) = \infty$.
Since $\mu^{n-1}\phi(b)^{-m} = \phi(c^{n-1}b^{-m}) < 1$, it follows from the hypothesis that $\psi(c^{n-1}b^{-m}) < 1$, i.e.,

$$\gamma^{n-1} = \psi(c^{n-1}) < \psi(b)^m \tag{1.11}$$

Similarly $\phi(b)^m < \mu^{n+1}$ gives $\phi(b^m c^{-n-1}) < 1$ which implies that $\psi(b^m c^{-n-1}) < 1$. So

$$\psi(b^m) < \psi(c)^{n+1} = \gamma^{n+1} \tag{1.12}$$

Combining (1.11) and (1.12), we see that

$$\gamma^{n-1} < \psi(b)^m < \gamma^{n+1} \tag{1.13}$$

Taking logarithm, on dividing it follows from (1.10) and (1.13) that

$$\frac{(n-1)\log\mu}{(n+1)\log\gamma} < \frac{\log\phi(b)}{\log\psi(b)} < \frac{(n+1)\log\mu}{(n-1)\log\gamma}$$

Taking the limit as $n \to \infty$, we have

$$\frac{\log\phi(b)}{\log\psi(b)} = \frac{\log\mu}{\log\gamma} = \frac{1}{\alpha}$$

Thus we have shown that if $\phi(b) > 1$, then $\psi(b) = \phi(b)^{\alpha}$.
If $\phi(b) \leq 1$, we have $\phi(b^{-1}) \geq 1$. Recall that $\phi(c) > 1$. So $\phi(b^{-1}c) > 1$. Then by what has been proved above $\psi(cb^{-1}) = \phi(cb^{-1})^{\alpha}$ which implies that $\psi(b) = \phi(b)^{\alpha}$ in view of the equality $\psi(c) = \phi(c)^{\alpha}$. □

Proof of Theorem 1.5 Clearly (i) $\implies$ (ii) and (ii) $\implies$ (iii).
We now prove (iii) $\implies$ (iv).There exists $\epsilon > 0$ such that

$$\{y \in K \mid \phi_1(y) < \epsilon\} \subseteq \{y \in K \mid \phi_2(y) < 1\} \tag{1.14}$$

If $x \in K$ is such that $\phi_1(x) < 1$, then $\phi_1(x^n) < \epsilon$ for some $n \in \mathbb{N}$. Then by (1.14) , $\phi_2(x^n) < 1$; consequently $\phi_2(x) < 1$. This proves (iii) $\implies$ (iv)
Assertion (iv) $\implies$ (i) in view of Lemma 1.6 and thus equivalence of (i) - (iv) is established.

It may be remarked that from the equivalence of (i) - (iv), we observe that for any $x \in K, \phi_1(x) < 1$ iff $\phi_2(x) < 1$. We now prove the equivalence of (iv) and (v). First we show that (iv)$\Rightarrow$(v).
In view of the above remark, it is enough to show that $\phi_1(x) = 1$ iff $\phi_2(x) = 1$. Suppose that $\phi_1(x) = 1$ and $\phi_2(x) \neq 1$, then we must have $\phi_2(x) > 1$, which implies $\phi_2(x^{-1}) < 1$ and hence $\phi_1(x^{-1}) < 1$ which is impossible as $\phi_1(x^{-1}) = 1$. Interchanging the roles of $\phi_1,\ \phi_2$ we see that $\phi_2(x) = 1 \implies \phi_1(x) = 1$.
(v) $\implies$ (iv) Let $x \in K$ be such that $\phi_1(x) < 1$; we need to show that $\phi_2(x) < 1$. By virtue of (v), $\phi_2(x) \leq 1$ but $\phi_2(x) \neq 1$, otherwise $\phi_1(x^{-1}) \leq 1$ i.e., $\phi_1(x) \geq 1$ which is not so. Therefore $\phi_2(x) < 1$. □

1.2 Approximation Theorem

The first instance where the Approximation Theorem had been formulated and proved, including Archimedean absolute values was $Artin - Whaples$ paper of 1945. Hasse' in the first edition of his book $ZahlenTheorie$ which was completed in 1938 but was published in 1949 has proved the Approximation Theorem for Algebraic Number Fields and Algebraic Function Fields.

Theorem 1.7 *Let $\phi_1, \phi_2, \cdots, \phi_n$ be nontrivial, pairwise nonequivalent absolute values of a field K. Then for arbitrary chosen elements $x_1, x_2, \cdots, x_n$ of K and a positive real number ϵ, there exists an element $x \in K$ satisfying the inequalities $\phi_i(x - x_i) < \epsilon$ for $1 \leq i \leq n$.*

For the proof of Approximation theorem we need the following two lemmas.

Lemma 1.8 *Let ϕ be an absolute value of a field K. For an element $a \in K$, the following hold :*
(i) If $\phi(a) < 1$, then $\lim\limits_{n\to\infty} a^n = 0$
(ii) If $\phi(a) < 1$, then $\lim\limits_{n\to\infty} (\dfrac{a^n}{1+a^n}) = 0$
(iii) If $\phi(a) > 1$, then $\lim\limits_{n\to\infty} (\dfrac{a^n}{1+a^n}) = 1$
(Recall that $\lim\limits_{n\to\infty} x_n = x$ if $\lim\limits_{n\to\infty} \phi(x_n - x) = 0$).

Proof. (i) is obvious .
(ii) Since we have $1 - \phi(a)^n \leq \phi(1 + a^n) \leq 1 + \phi(a)^n$
we obtain by squeeze principle $\lim\limits_{n\to\infty} \phi(a^n + 1) = 1$
hence

$$\lim_{n\to\infty} \phi(\frac{a^n}{1+a^n}) = \lim_{n\to\infty} \frac{\phi(a^n)}{\phi(1+a^n)} = 0$$

and (ii) is proved .
(iii) Note that $\lim\limits_{n\to\infty} \phi(\dfrac{a^n}{1+a^n} - 1) = \lim\limits_{n\to\infty} \phi(\dfrac{-a^{-n}}{1+a^{-n}}) = \lim\limits_{n\to\infty} \dfrac{\phi(a^{-n})}{\phi(1+a^{-n})}$
The last limit is zero by virtue (ii).

Lemma 1.9 *Let $\phi_1, \phi_2, \cdots, \phi_s$ be a finite number of mutually non-equivalent absolute values of a field K. Then there exists an element a of K such that*

$$\phi_1(a) > 1, \phi_2(a) < 1, \cdots, \phi_s(a) < 1$$

.

Proof We prove the lemma when $s = 2$. Since $\phi_1(x)$ and $\phi_2(x)$ are not equivalent, by virtue of Proposition 1.2, there exist $b, c \in K$ such that $\phi_1(b) < 1, \phi_2(b) \geq 1, \phi_1(c) \geq 1, \phi_2(c) < 1$.Then the element $a = b^{-1}c$ satisfies $\phi_1(a) > 1, \phi_2(a) < 1$ thereby proving the lemma in this case .

For general s, we utilize induction on s. Assuming that the lemma holds for $s-1$, we choose b, c of K such that the following inequalities will be satisfied

$$\phi_1(b) > 1, \phi_2(b) < 1, \cdots, \phi_{s-1}(b) < 1;\ \phi_1(c) > 1, \phi_s(c) < 1$$

For proving the lemma, we construct a sequence $\{a_n\}$ of elements of K such that $\lim\limits_{n\to\infty} \phi_1(a_n) > 1$ and $\lim\limits_{n\to\infty} \phi_i(a_n) < 1$ for $2 \leq i \leq s$

Consider the following two cases :

(i) $\phi_s(b) \leq 1$. Set $a_n = cb^n$ $(n = 1, 2, \cdots)$, then we have $\phi_1(a_n) > 1$, $\phi_s(a_n) < 1$ and $\lim\limits_{n\to\infty} \phi_i(a_n) = 0$ for $2 \leq i \leq s-1$. Also $\lim\limits_{n\to\infty} \phi_s(a_n) = 0$ or $\phi_s(c) < 1$.

(ii) $\phi_s(b) > 1$. We set $a_n = \frac{cb^n}{1+b^n}$. Then by Lemma 1.8,we have

$$\lim_{n\to\infty} \phi_1(a_n) = \phi_1(c) > 1,$$

$$\lim_{n\to\infty} \phi_s(a_n) = \phi_s(c) < 1, \lim_{n\to\infty} \phi_i(a_n) = 0\ for\ 2 \leq i \leq s-1$$

Proof of Approximation Theorem. Choose $\delta > 0$ such that

$$\delta(\phi_i(x_1) + \cdots + \phi_i(x_s)) < \epsilon for 1 \leq i \leq s \tag{1.15}$$

In view of Lemma 1.9 for each i we can choose an element $y_i \in K$, $1 \leq i \leq s$, such that $\phi_i(y_i) > 1$, $\phi_j(y_i) < 1 (i \neq j)$, $1 \leq i, j \leq s$.

Set $z_{in} = \frac{{y_i}^n}{1+{y_i}^n}$, then by Lemma 1.8, $\phi_j(z_{in}) \longrightarrow 0$ as $n \longrightarrow \infty$ for $i \neq j$,

$\phi_i(z_{in}-1) \longrightarrow 0$ as $n \longrightarrow \infty$. Given $\delta > 0$, choose r sufficiently large such that $\phi_i(z_{ir}-1) < \delta$, $\phi_j(z_{ir}) < \delta$ for $i \neq j$, $1 \leq i,\ j \leq s$. Set $z_i = z_{ir}$ for $1 \leq i \leq s$ so that

$$\phi_i(z_i - 1) < \delta, \phi_j(z_i) < \delta, j \neq i, 1 \leq i, j \leq s \tag{1.16}$$

Then the element $x = x_1z_1 + \cdots + x_sz_s$ satisfies the desired condition. We verify for $i = 1$.

$\phi_1(x - x_1) = \phi_1(x_1(z_1 - 1) + x_2z_2 + \cdots + x_nz_n)$

$$\leq\ \phi_1(x_1)\phi_1(z_1-1) + \phi_1(x_2)\phi_1(z_2) + \cdots + \phi_1(x_n)\phi_1(z_n)$$

$< \delta(\phi_1(x_1)+\phi_1(x_2)+\cdots+\phi_1(x_n)) \leq \varepsilon$ (*in view of* (1.15) *and* (1.16)). □

Corollary 1.10 ***(Independence Theorem)*** *Let $\phi_1, \phi_2, \cdots \phi_n$ be a finite number of mutually non-equivalent non-trivial absolute values of a field K. Then for $1 \leq r \leq n$, there exists an element $a \in K$ such that the inequalities*
$\phi_1(a) > 1, \cdots, \phi_r(a) > 1, \phi_{r+1}(a) < 1, \cdots, \phi_n(a) < 1$ hold.

Proof Choose $x_i \in K$ such that $\phi_i(x_i) > 3/2$ *for* $1 \leq i \leq r$ and $\phi_j(x_i) < 1/2$ for $r + 1 \leq j \leq n$. Then by Approximation theorem, $\exists\ a \in K$ such that $\phi_i(a - x_i) < 1/2$ for $1 \leq i \leq n$. Now $\phi_i(a) \geq \phi_i(x_i) - \phi_i(a - x_i) > 1$ for $1 \leq i \leq r$ and $\phi_i(a) \leq \phi_i(a - x_i) + \phi_i(x_i) < 1/2 + 1/2$ for all $r + 1 \leq i \leq n$. □

Remark The Approximation theorem is equivalent to saying that the diagonal set $\{(x, x, x, \cdots, x)/x \in K\}$ is dense in the product topology $K_1 \times K_2 \times \cdots \times K_n$ where $K_i = K$ for each i, with the topology given by ϕ_i.

1.3 Completions

Definition Topological Field A topological field is a set F, which contains a field structure and a topology satisfying the following axioms:
(i) The mapping $(x, y) \longrightarrow x + y$ of $F \times F \longrightarrow F$ is continuous ;
(ii) The mapping $x \longrightarrow -x$ of $F \longrightarrow F$ is continuous ;
(iii) The mapping $(x, y) \longrightarrow xy$ of $F \times F \longrightarrow F$ is continuous ;
(iv) The mapping $x \longrightarrow x^{-1}$ of $F^* \longrightarrow F^*$ is continuous ;
where $F \times F$ carries the product topology.

Proposition 1.11 *Let K be a field with a absolute value ϕ . Then K is a topological field with respect to the topology induced by ϕ.*

Proof Let x, y, x', y' be elements of K. The continuity of the mapping $(x, y) \longrightarrow x+y$ follows immediately from the inequality

$$\phi((x' + y') - (x + y)) \leq \phi(x' - x) + \phi'(y' - y)$$

For proving continuity of $(x, y) \longrightarrow xy$, it is clearly enough to verify that

$$\phi(x'y' - xy) \leq \phi(x' - x)\phi(y' - y) + \phi(x)\phi(y' - y) + \phi(y)\phi(x' - x) \tag{1.17}$$

Write $x'y' + xy = (x' - x)(y' - y) + xy' + x'y$
i.e., $x'y' - xy = (x' - x)(y' - y) + xy' + x'y - 2xy$
i.e., $x'y' - xy = (x' - x)(y' - y) + x(y' - y) + y(x' - x)$
which quickly yields (1.17). Futhermore, let a be a non-zero element of K and suppose a' is another element such that $\phi(a' - a) < \frac{\phi(a)}{2}$. Then $\phi(a') \geq \phi(a) - \phi(a' - a) > \frac{\phi(a)}{2}$. So $a' \neq 0$ and

$$\phi(a'^{-1} - a^{-1}) = \frac{\phi(a' - a)}{\phi(a')\phi(a)} < \frac{2\phi(a' - a)}{\phi(a)^2}$$

The above ineuality shows that the mapping $x \longrightarrow x^{-1}$ is continuous on K^*. Thus K is a topological field. □

Definition: A sequence $\{a_n\}$ of elements of K is called a Cauchy sequence if to any $\epsilon > 0$, there corresponds a positive integer N such that $\phi(a_n - a_m) < \epsilon$ for all $n, m \geq N$. The sequence $\{a_n\}$ converges to an element a of K if for any $\epsilon > 0$,there exists a positive integer N such that $\phi(a_n - a) < \epsilon$ for all $n \geq N$.
A convergent sequence is a Cauchy sequence but the converse is not always true. When every Cauchy sequence of elements of K is convergent to an element of K, we say that the field K is complete w.r.t. ϕ or that (K, ϕ) is complete field. We now show that every field K with a non-trivial absolute value can be densely embedded into a field complete w.r.t. an absolute value extending the given one.

Theorem 1.12 *There exists a field $\hat{K}$,complete under an absolute value $\hat{\phi}$ and an embedding $i : K \longrightarrow \hat{K}$, such that $\phi(x) = \hat{\phi}(i(x)), \forall\ x \in K$. The image $i(K)$ is dense in $\hat{K}$. If $(\hat{K}', \hat{\phi}')$ is another such pair, then there exists a unique continuous isomorphism $f : \hat{K} \longrightarrow \hat{K}'$ preserving the absolute value such that $i' = f \circ i$.*

Proof Step I Existence of $(\hat{K}, \hat{\phi})$ Let $\mathcal{C}$ be the set of all Cauchy sequences $\{x_n\}$ of elements of K with component-wise addition and multiplication. $\mathcal{C}$ is commutative ring with $1 = \{1\}_n$. The set $\mathcal{N} = \{\{x_n\}_{n\in\mathbb{N}} \mid \lim\limits_{n\to\infty} x_n = 0\}$ is an ideal of $\mathcal{C}$. Note that $\{\phi(a_n) \mid n \in \mathbb{N}\}$ associated with a Cauchy sequence $\{a_n\}$ is always bounded.
We now show that $\mathcal{N}$ is maximal ideal of $\mathcal{C}$. Indeed let us suppose that $\mathcal{I}$ is an ideal of $\mathcal{C}$, different from $\mathcal{N}$, such that $\mathcal{C} \supseteq \mathcal{I} \supset \mathcal{N}$. If $\{a_n\}$ is an element of $\mathcal{I}$ which is not contained in $\mathcal{N}$. So, $\exists\ \epsilon_\circ > 0$ such that given any m, $\exists\ n > m$ with $\phi(a_n) \geq \epsilon_\circ$. Since $\{a_n\}$ is Cauchy sequence, for given $\epsilon_\circ$ $\exists\ n_\circ$ such that $\phi(a_n - a_m) < \epsilon_\circ/2\ \forall\ n, m \geq n_\circ$ and $\exists\ n_1 \geq n_\circ$ such that $\phi(a_{n_1}) \geq \epsilon_\circ$. Also $\phi(a_{n_1} - a_m) < \epsilon_\circ/2\ \forall\ m > n_\circ$. So,$\forall\ m > n_\circ$,

$$\phi(a_m) \geq \phi(a_{n_1}) - \phi(a_{n_1} - a_m) \geq \epsilon_\circ - \epsilon_\circ/2 = \epsilon_\circ/2 \tag{1.18}$$

Let $\{b_n\}$ denote the sequence in K defined by $b_n = 1\ \forall\ n \leq n_\circ$ and $b_n = a_n^{-1}\ \forall\ n > n_\circ$. We now verify $\{b_n\}$ is a Cauchy sequence. Let $\epsilon > 0$ be given, $\exists\ N$ such that

$$\phi(a_n - a_m) < \epsilon\epsilon_\circ^2/4\ \forall\ n \geq N \tag{1.19}$$

$\therefore$ for $m, n \geq max\{n_\circ, N\}$, We have by virtue of (1.18) and (1.19)

$$\phi(b_n - b_m) = \phi(a_n^{-1} - a_m^{-1}) = \frac{\phi(a_n - a_m)}{\phi(a_n)\phi(a_m)} < \epsilon.$$

So $\{b_n\}$ is Cauchy sequence and $\{a_n b_n\} \in \mathcal{I}$ is a constant sequence $\forall\ n \geq n_\circ$. Since $\{a_1^{-1}, a_2^{-1}, a_n^{-1} \cdots 0, 0, 0, 0\} \in \mathcal{N} \subseteq \mathcal{I}$. Therefore the constant sequence $\{1, 1, 1 \cdots\} \in \mathcal{I}$. Hence $\mathcal{I} = \mathcal{C}$. So, $\mathcal{N}$ is a maximal ideal of $\mathcal{C}$. We denote the field $\mathcal{C}/\mathcal{N}$ by $\hat{K}$. We now define $\hat{\phi}$ on $\hat{K}$. Let ξ be any element of $\hat{K}$ having a sequence $\{a_n\}$ as a representative. Then for any $\epsilon > 0, \exists$ a positive integer N such that for $n, m \geq N$,

$$\mid \phi(a_n) - \phi(a_m) \mid \leq \phi(a_n - a_m) < \epsilon.$$

Hence $\{\phi(a_n)\}$ is a Cauchy sequence in non negative real numbers and converges to a non negative real number, its limit does not depend upon the choice of representative $\{a_n\}$ of ξ. We define $\hat{\phi}(\xi) = \lim\limits_{n \to \infty} \phi(a_n)$. One can easily check that $\hat{\phi}$ satisfies the properties of an absolute value on $\hat{K}$. The mapping $i : K \longrightarrow \hat{K}$ defined by $a \longrightarrow$ class of constant sequence with entry a is obviously an injective homomorphism by means of which we identify K with a subfield of $\hat{K}$. Clearly $\hat{\phi}(a) = \phi(a)\ \forall\ a \in K$.

Step II Density of K in $\hat{K}$. Let ξ be any element of $\hat{K}$ with the sequence $\{a_n\}$ as a representative. Let $\epsilon > 0$ be given, $\exists$ a positive integer $n_\circ$ such that $\phi(a_n - a_m) < \epsilon/2\ \forall\ n, m \geq n_\circ$. Fix any $m \geq n_\circ$, then $\hat{\phi}(\xi - a_m) = \lim\limits_{n \to \infty} \phi(a_n - a_m) \leq \epsilon/2 < \epsilon$.
This proves that K is dense in $\hat{K}$.

Step III Completeness of $\hat{K}$. Let $\{\xi_n\}$ be a Cauchy sequence in $\hat{K}$. Since K is dense in $\hat{K}$ by step II, $\forall\ n,\ \exists\ a_n \in K$ such that $\hat{\phi}(\xi_n - a_n) < 1/n$. We verify that $\{a_n\}$ is a Cauchy sequence in K. Let $\epsilon > 0$ be given, $\exists\ n_\circ$ such that $\hat{\phi}(\xi_n - \xi_m) < \epsilon/2\ \forall\ n, m \geq n_\circ$. It may further be assumed that $1/n_\circ < \epsilon/4$. Then $\forall\ n, m \geq n_\circ$, we have $\phi(a_n - a_m) \leq \hat{\phi}(a_n - \xi_n) + \hat{\phi}(\xi_n - \xi_m) + \hat{\phi}(\xi_m - a_m) < 1/n + \epsilon/2 + 1/m < \epsilon$. Hence $\{a_n\}$ is a Cauchy sequence in K whose class is an element ξ of $\hat{K}$. We show that (ξ_n) converges to ξ. Let $\epsilon > 0$ be given. $\exists\ N > 2/\epsilon$ such that $\phi(a_n - a_m) < \epsilon/2\ \forall\ n, m \geq N$. Now for any $n \geq N$, $\hat{\phi}(\xi_n - \xi) \leq \hat{\phi}(\xi_n - a_n) + \hat{\phi}(a_n - \xi)$
$< 1/n + \lim\limits_{m \to \infty} \phi(a_n - a_m) < \epsilon/2 + \epsilon/2$. This proves the completeness of $\hat{K}$.

Step IV Uniqueness of completion Let $(\hat{K'}, \hat{\phi'})$ be any other pair with the same properties as $(\hat{K}, i)$.For every $\xi = \{a_n\} + \mathcal{N} \in \hat{K}$, the sequence $\{i'(a_n)\}$ is a Cauchy sequence in $\hat{K'}$. Let ξ' be its limit in $\hat{K'}$. Define $f(\xi) = \xi'$. From uniqueness of limits, it follows that f is a homomorphism and injective map. We now verify f is surjective. Let $\xi' \in \hat{K'}$. As $i'(K)$ is dense in $\hat{K'}$, $\exists$ a sequence $\{a_n\} \in K$ such that $\{i'(a_n)\}$ converges to ξ'. So, $\{i(a_n)\}$ and hence $\{a_n\}$ is a Cauchy sequence which shows that $\xi = \{a_n\} + \mathcal{N}$ is the pre-image of ξ'. We now show that f is absolute value preserving. Let $\xi = \{a_n\} + \mathcal{N} \in \hat{K}$. Then $f(\xi) = \lim_{n\to\infty} i'(a_n)$. Therefore $\hat{\phi}'(f(\xi)) = \lim_{n\longrightarrow\infty} \hat{\phi}'(i'(a_n)) = \lim_{n\longrightarrow\infty} \phi(a_n) = \hat{\phi}(\xi)$ which completes the proof. □

Definition A pair $(\hat{K}, \hat{\phi})$ as in Theorem 1.12 called a completion of the absolute value field (K, ϕ).

Corollary 1.13 *The completion of* $\mathbb{Q}$ *w.r.t. the usual absolute value is* $\mathbb{R}$.

Definition The completion of $\mathbb{Q}$ w.r.t. $p - adic$ absolute value ϕ_p is called the field of $p - adic$ numbers. We shall discuss these fields in Chapter 2.

1.4 Normed Spaces

Definition Let (K, ϕ) be an absolute valued field , and let E be a vector space over K. A real valued function $\parallel x \parallel$ defined for elements x of E is called a norm if it satisfies the following conditions:
(i) $\parallel x \parallel \geq 0$; $\parallel x \parallel = 0 \Longleftrightarrow x = 0$
(ii)for $\alpha \in K$ and $x \in E$, we have $\parallel \alpha x \parallel = \phi(\alpha) \parallel x \parallel$.
(iii) $\parallel x + y \parallel \leq \parallel x \parallel + \parallel y \parallel$.
The vector space E is then called a normed space. A normed space E has the structure of a metric space with distance of $x, y \in E$ defined as $\parallel x - y \parallel$.

Definition Norms $\parallel . \parallel_1$ and $\parallel . \parallel_2$ of a vector space E are called equivalent if there exist constants c_1, c_2 such that $\parallel x \parallel_1 \leq c_1 \parallel x \parallel_2, \parallel x \parallel_2 \leq c_2 \parallel x \parallel_1 \forall x \in E$.

Remark Equivalent norms induce the same topology.

DefinitionLet ϕ be an absolute value of a field K. Let E be a finite dimensional vector space over K with a basis $\{x_1, x_2, \cdots, x_n\}$. A norm $\parallel x \parallel_\circ$ is obtained by setting

$$\parallel x \parallel_\circ = max_i\{(\phi(\alpha_i))\}$$

where $x = \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n$ (called max norm)

Remark The above norm (max norm) induces the product topology on E. Indeed once a basis $\{x_1, x_2, \cdots, x_n\}$ of E is fixed, there is a canonical isomorphism from $K^n \longrightarrow E$ mapping $(\alpha_1, \cdots, \alpha_n)$ to $\alpha_1 x_1 + \cdots + \alpha_n x_n$ where E is endowed with a topology induced by this max norm and K^n with the product topology where on K we take the topology corresponding to ϕ. If K is complete w.r.t. ϕ, then E is complete w.r.t. the max- norm, because product of two complete metric spaces is complete; indeed the product topology of two complete metric spaces $(X_1, d_1), (X_2, d_2)$ is given by the metric $d((x_1, x_2), (y_1, y_2)) = max(d_1(x_1, y_1), d_2(x_2, y_2))$.

Note In case K_1 is a field extension of K, every absolute value ϕ_1 of K_1 that restricts to ϕ on K is a norm of K_1 compatible with ϕ. If K_1 is finite extension of K and K is complete with respect to ϕ, then it will be shown that K_1 admits only one absolute value ϕ_1 restricting to ϕ on K. Moreover K_1 is complete with respect to ϕ_1.

Theorem 1.14 *Let ϕ be a non-trivial absolute value of field K and let E be a vector space over K.Then any two norms $\| \,.\, \|_1$ and $\| \,.\, \|_2$ on E inducing same topology must be equivalent.*

Proof. As ϕ is non trivial absolute value of K, $\therefore$ $\exists$ an $\alpha \in K$ such that $\phi(\alpha) = r > 1$. We need to show that $\exists$ a constant c_1 such that

$$\| x \|_1 \leq c_1 \| x \|_2 \; \forall \; x \in E \tag{1.20}$$

Suppose to the contrary it is not true, so $\forall$ positive integer $m, \exists \; x_m \in E$ such that

$$\| x_m \|_1 > m \| x_m \|_2 \tag{1.21}$$

$\exists \; k \in \mathbb{Z}$, depending on m such that $r^k \leq \| x_m \|_1 < r^{k+1}$, i.e., $1 \leq \| y_m \|_1 < r$, where

$$y_m = x_m / \alpha^k \tag{1.22}$$

but by (1.21), $\| y_m \|_1 > m \| y_m \|_2 \; \forall \; m$. Hence, $\| y_m \|_2 < 1/m \| y_m \|_1 < r/m$. Thus $y_m \longrightarrow 0$ as $m \longrightarrow \infty$ w.r.t.$\|\|_2$, but $y_m \nrightarrow 0$ as $m \longrightarrow \infty$ w.r.t.$\|\|_1$, $\because \| y_m \|_1 \geq 1$ which contradicts the fact that they induce the same topology. Thus (1.20) is proved interchanging the role of $\| \,.\, \|_1$ *and* $\| \,.\, \|_2$ We see that $\exists \; c_2$ such that $\| x \|_2 \leq c_2 \| x \|_1$ $\forall \; x \in E$. □

Theorem 1.15 *Let K be a field complete with respect to a absolute value ϕ. Then any two norms (compatible with ϕ) of finite dimensional K- vector space E are equivalent.*

Proof We shall prove that every norm $\| \,.\, \|$ on E is equivalent to max norm $\| \,.\, \|_\circ$. We apply induction on the dimension n of the K vector space E. For n=1, the statement is obvious. Assume the theorem is true for $n-1, n \geq 2$, Fix a basis $\{w_1, w_2, \cdots, w_n\}$ of E over K and for

$$\xi = \alpha_1 w_1 + \cdots + \alpha_n w_n \in E$$

$$\| \xi \| \leq \phi(\alpha_1) \| w_1 \| + \phi(\alpha_2) \| w_2 \| + \cdots + \phi(\alpha_n) \| w_n \|$$

$$\leq \| \xi \|_\circ (\| w_1 \| + \| w_2 \| + \cdots + \| w_n \|)$$

$$= \mu \| \xi \|_\circ$$

where $\mu = \| w_1 \| + \cdots + \| w_n \|$
Hence it now suffices to show that $\exists$ a constant C such that $\| \xi \|_\circ \leq C \| \xi \|$ always holds. Suppose to the contrary that no such C exists.Then for every positive integer m, there exists $\xi'_m \in E$ such that

$$\xi'_m = \sum \alpha_i w_i, \ \| \xi'_m \|_\circ > m \| \xi'_m \| \tag{1.23}$$

Let j be such that $\phi(\alpha_j) = max_{1 \leq i \leq n}\{\phi(\alpha_i)\}$.Letting $\xi_m = \alpha_j^{-1} \xi'_m$. We conclude from (1.23) that $\| \xi_m \|_\circ = 1$ and thus

$$\| \xi_m \| < 1/m \tag{1.24}$$

Now for every $m \geq 1$ one of the coefficients of components of ξ_m equals 1. Thus there must be an infinite subset T of $\mathbb{N}$ and fixed j such that coefficient of j^{th} component of ξ_m equals to 1 for all $m \in T$. We fix this number j from now on until the end.
Consider the subspace E_1 of E consisting of all vectors whose j^{th} co-ordinate is equal to 0, equipped with the norm induced by $\| \, . \, \|$. By induction, the restrictions of $\| \, . \, \|$ and $\| \, . \, \|_\circ$ to E_1 are equivalent. For each $m \in T$, we can write $\xi_m = w_j + \zeta_m$ with $\zeta_m \in E_1$.We verify $\{\zeta_m\}$ is a Cauchy sequence in E_1. Let $\epsilon > 0$ be given $\exists$ N such that $2/N < \epsilon$. If $m, n \geq N; m, n \in T$,then

$$\| \zeta_m - \zeta_n \| = \| \zeta_m + w_j - w_j - \zeta_n \| \leq \| \xi_m - \xi_n \|$$

$$\leq \| \xi_m \| + \| \xi_n \| < \ 1/m + 1/n \ \leq \ 2/N < \epsilon$$

Consequently $\{\zeta_m\}_{m \in T}$ is a Cauchy sequence with respect to the restriction of $\| \, . \, \|$ to E_1.By induction it follows that $\{\xi_m\}$ is also Cauchy w.r.t. $\| \, . \, \|_\circ$. Since E_1 is complete w.r.t. $\parallel . \parallel_\circ$, $\{\zeta_m\}$ converges to some $\zeta \in E_1$. By (1.24), $\parallel \xi_m \parallel = \parallel w_j + \zeta_m \parallel < 1/m$ for every $m \in T$. So ζ_m converges to $-w_j$. Therefore, $\zeta = -w_j$ but $-w_j \notin E_1$. Thus contradiction proves the theorem. □

The following corollaries will be quickly deduced from the above theorem.

Corollary 1.16 *If (K, ϕ) is complete absolute valued field and (K_1, ϕ_1) is a finite extension of (K, ϕ), then (K_1, ϕ_1) is complete.*

Corollary 1.17 *Let K be a field with absolute value ϕ. Let (K_1, ϕ_1) be a finite extension. Let $(\hat{K}, \hat{\phi})$ be completion of (K, ϕ), then $\hat{K}_1 = \hat{K}K_1$.*

Proof. Since $\hat{K}K_1 \subseteq \hat{K}_1$ and $\hat{K}K_1$ is complete being a finite extension of $\hat{K}$(by the above corollary), therefore, $\hat{K} \subseteq \hat{K}K_1$. So, equality holds i.e. $\hat{K}_1 = \hat{K}K_1$.

Corollary 1.18 *Let ϕ be an absolute value of K w.r.t. which it is complete. The extension of ϕ as an absolute value to a finite extension K_1 of K, if it exists, is unique.*

Proof. Let ϕ_1, ψ_1 be extension of (ϕ, K), then by Theorem 1.15, ψ_1, ϕ_1 induce the same topology on K_1, therefore by Theorem 1.5, $\exists$ positive real number λ such that $\psi_1 = \phi_1^\lambda$ but ϕ_1 and ψ_1 coincide on K.So, $\lambda = 1$ if ϕ is non trivial. But if ϕ is trivial on K, then topology on K is discrete.The topology on K_1 induced by ϕ_1, ψ_1 are both discrete. So the absolute values ϕ_1, ψ_1 are both trivial. □

The following theorem gives another proof of corollary 1.18.

Theorem 1.19 *Let K be a field complete w.r.t. an absolute value ϕ and let K_1 be a finite extension of K. Suppose that K_1 admits an extension ϕ_1 of ϕ. Then we have*

$$\phi_1(\alpha) = (\phi(N_{K_1/K}(\alpha)))^{1/r}, r = [K_1 : K]$$

and with respect to ϕ_1, K_1 is complete.

Proof. The absolute value ϕ_1 is a norm on the vector space K_1 over K, and coincides with ϕ on K. Let $\{w_1, w_2, \cdots, w_r\}$ be a base of K_1 over K and for an element

$\alpha = a_1w_1 + a_2w_2 + \cdots + a_rw_r$ of K_1, we set $\parallel \alpha \parallel_\circ = max_i\{\phi(a_i)\}$. Then as norm ϕ_1 is equivalent to $\parallel \parallel_\circ$ by the Theorem 1.15, whence we see that K_1 is complete with respect to ϕ_1. Suppose now that $\phi_1(\alpha) < 1$.Then we can show that $(\phi(N_{K_1/K}(\alpha)) < 1$ as follows. Write $\alpha^n = a_1^{(n)}w_1 + \cdots + a_r^{(n)}w_r$. Since ϕ_1 is equivalent to max norm and $\phi_1(\alpha^n) \longrightarrow 0$ as $n \longrightarrow \infty$, it is clear that $\phi({a_i}^{(n)}) \longrightarrow 0$ as $n \longrightarrow \infty$ for $1 \leq i \leq r$. Note that $N_{K_1/K}(\alpha^n)$ is a homogeneous polynomial of degree r in $a_1^{(n)}, \cdots, a_r^{(n)}$ and hence $\phi(N_{K_1/K}(\alpha^n)) \longrightarrow 0$ as $n \longrightarrow \infty, i.e., \phi(N_{K_1/K}(\alpha))^n$ as $n \longrightarrow \infty$ which proves that $\phi(N_{K_1/K}(\alpha)) < 1$. We have consequently $\phi(N_{K_1/K}(\alpha)) > 1$ when $\phi_1(\alpha) > 1$. Hence we have whenever $\phi(N_{K_1/K}(\alpha)) = 1$, then $\phi_1(\alpha) = 1$.Now when we are given an element $\alpha \in K_1^*$, we have $N_{K_1/K}(\frac{\alpha^r}{N_{K_1/K}(\alpha)}) = 1$ and hence we obtain

$$\phi_1(\frac{\alpha^r}{N_{K_1/K}(\alpha)}) = \phi(\alpha^r)/\phi(N_{K_1/K}(\alpha)) = 1$$

. $\Longrightarrow \phi_1(\alpha) = (\phi(N_{K_1/K}(\alpha))^{1/r}$. This completes the proof. □

Note If $n = 2,\ N_{K_1/K}(\alpha^n) = (a_1^{(n)}\sigma_1(w_1) + a_2^{(n)}\sigma_1(w_2))(a_2^{(n)}\sigma_2(w_1) + a_2^{(n)}\sigma_2(w_2))$

$$= (a_1^{(n)})^2 N_{K_1/K}(w_1) + a_1^{(n)}a_2^{(n)}Tr_{K_1/K}(w_1w_2) + (a_2^{(n)})^2(N_{K_1/K}(w_2))$$

.

Note If $(K, \phi), (K_1, \phi_1)$ defined as in the above theorem, then we shall prove in next chapter by using Hensel's lemma that the mapping ϕ_1 defined by $\phi_1(\alpha) = (\phi(N_{K_1/K}(\alpha)))^{1/r}$ is indeed an absolute value of K_1.

1.5 The determination of complete Archimedean valued fields

Suppose K is a complete field with respect to an Archimedean absolute value ϕ. Since the set $\{\phi(n.1)/\in \mathbb{Z}\}$ is not bounded, char K=0. Thus K contains the field $\mathbb{Q}$ of rational numbers. By Theorem 1.4, ϕ restricted to $\mathbb{Q}$ is equivalent to usual absolute value of $\mathbb{Q}$. Thus, the complete field K contains completion of $\mathbb{Q}$ with respect to the ordinary absolute value ,i.e., Kcontains $\mathbb{R}$ as a closed subfield. We shall then show that K must be isomorphic to $\mathbb{C}$ or $\mathbb{R}$. This result was first proved by *Ostrowski in 1917. the proof given here is due to Hasse. Recall that if K, L are fields with absolute values ϕ and ψ. Then (K,ϕ) is said isomorphic (L,ψ) (as absolute valued field), if $\exists$ a field isomorphism $f : K$ onto L preserving absolute values i.e., $\psi(f(x)) = \phi(x)\forall x \in K$.*

Lemma 1.20 *Let K be a field complete w.r.t. an absolute value ϕ and E be quadratic extension of K.Then a real valued function $\phi_E : E \longrightarrow \mathbb{R}$ defined by*

$$\phi_E(\alpha) = \sqrt{\phi(N(\alpha))}$$

where N is the norm $N_{E/K}$, is an absolute value on E.

Proof *For the purpose of showing that ϕ_E is an absolute value , it is sufficient to show that the inequality*

$$\phi_E(\alpha - 1) \leq 1 + \phi_E(\alpha) \tag{1.25}$$

holds for every element $\alpha \in E$. Suppose that there exists an element $\alpha \in E, (\alpha \not\ni K)$ such that $\phi_E(\alpha - 1) > 1 + \phi_E(\alpha)$. We set $\bar{\alpha}$ to be the conjugate of α (w.r.t. K) and set $(X-\alpha)(X-\bar{\alpha}) = X^2 + bX + c$; $b, c \in K$, $c \neq 0$. We now have by our assumption

$$\phi_E(\alpha - 1) = \sqrt{\phi(N(\alpha - 1))} = \sqrt{\phi(\alpha - 1)\phi(\bar{\alpha} - 1)} = \sqrt{\phi(1 + b + c)}$$

and

$$\phi_E(\alpha) = \sqrt{\phi(N(\alpha)} = \sqrt{\phi(\alpha\bar{\alpha})} = \sqrt{\phi(c)}$$

$$\therefore \sqrt{\phi(1 + b + c)} > 1 + \sqrt{\phi(c)}$$

$$\Longrightarrow \phi(1+b+c) > 1 + 2\sqrt{\phi(c)} + \phi(c)$$

$$\Longrightarrow 1 + \phi(b) + \phi(c) \geq \phi(1+b+c) > 1 + 2\sqrt{\phi(c)} + \phi(c)$$

$$\Longrightarrow (\phi(b))^2 > 4\phi(c) \tag{1.26}$$

Since $c \neq 0$, we have $\phi(b) > 0$, we then set $a_\circ = b$ and construct a sequence $a_1, a_2, \cdots$ by defining

$$a_{n+1} = -b - c/a_n$$

We now show a_n is never zero and the sequence $\{a_n\}$ is Cauchy sequence. Since K is complete, so $\{a_n\}$ converges and therefore there exists an element $a \in K$ to which $\{a_n\}$ converges and hence we have

$$a = -b - c/a \text{ i.e. } a^2 = -ba - c$$

which implies that $\alpha = a \in K$ which is contradiction. Thus the proof is complete, once we show that $a_n \neq 0$ and $\{a_n\}$ is Cauchy sequence. To show that $a_n \neq 0$, it suffices to show that

$$\phi(a_n) \geq \phi(b)/2 \tag{1.27}$$

Clearly $\phi(a_\circ) \geq \phi(b)/2$, suppose $\phi(a_n) \geq \phi(b)/2$, then

$$\phi(a_{n+1}) \geq \phi(b) - \phi(c)/\phi(a_n) \geq \phi(b) - 2\phi(c)/\phi(b) > \phi(b) - \phi(b)/2 = \phi(b)/2.$$

The last inequality holds in view of (1.26). Thus $a_{n+1} \neq 0$. It only remains to check that $\{a_n\}$ is a Cauchy sequence. For $n \geq 0$, keeping in mind (1.27), we have

$$\phi(a_{n+1} - a_n) = \phi(c/a_n - c/a_{n-1}) = \phi(c)\phi(a_n - a_{n-1})/\phi(a_n)\phi(a_{n-1})$$

$$\leq 4\phi(c)\phi(a_n - a_{n-1})/\phi(b)^2.$$

Set $\rho = 4\phi(c)/\phi(b)^2$. By $(1.26), \rho < 1$, The above inequality gives

$$\phi(a_{n+1} - a_n) \leq \rho\phi(a_n - a_{n-1}) \tag{1.28}$$

Therefore the series $\sum_{n=1}^{\infty} \phi(a_n - a_{n-1})$ is majorised by $\phi(a_1 - a_0)\sum_{k=0}^{\infty} \rho^k$ and hence is convergent. In particular

$$\lim_{n \longrightarrow \infty} \phi(a_{n+1} - a_n) = 0 \tag{1.29}$$

For any $n \geq 0, k \geq 1$, by virtue of (1.28), we have

$$\phi(a_n - a_{n+k}) \leq \phi(a_n - a_{n+1})(1 + \rho + \cdots + \rho^{k-1}).$$

which tends to zero as $n \longrightarrow \infty$ in view of (1.29), there by proving that $\{a_n\}$ is a Cauchy sequence.

Theorem 1.21 *(Ostrowski, 1917)Let K be a field complete with respect to an Archimedean absolute value ϕ. Then (K, ϕ) is isomorphic to $(\mathbb{R}, |.|^{\lambda})$ or $(\mathbb{C}, |.|^{\lambda})$ for some $\lambda > 0$.*

***Proof**. Since K is complete with respect to Archimedean absolute value. So characteristic of K is zero. We may consider K as an extension of $\mathbb{Q}$. Since the restriction of ϕ to $\mathbb{Q}$ is the usual absolute value $|.|$ and the completion of $\mathbb{Q}$ under the metric $|\ |$ is the real number field $\mathbb{R}$. Hence we may assume that K is the extension of $\mathbb{R}$ and restriction of ϕ to $\mathbb{R}$ is usual absolute value $|.|$. Suppose first that the equation $X^2 + 1 = 0$ is solvable in K, then we assume that K contains $\mathbb{C}$. For element $a + b\sqrt{-1} \in \mathbb{C}$, we have by Theorem 1.19*

$$\phi(a + b\sqrt{-1}) = \sqrt{|N(a + b\sqrt{-1})|} = \sqrt{a^2 + b^2}\ ;\ a, b\ \in\ \mathbb{R}$$

Hence K contains $\mathbb{C}$ not just as an algebraic subfield but as a field with absoute value. Now we show that K equals to $\mathbb{C}$. Suppose to contrary K contains $\mathbb{C}$ properly. Fix an element $a \in k$ such that $a \notin \mathbb{C}$. Consider the mapping $z \longrightarrow \phi(z - a)$ defined on $\mathbb{C}$. It is continuous on $\mathbb{C}$. Note that for $|z| > 2\phi(a)$, $\phi(z - a) \geq \phi(z) - \phi(a) = |z| - \phi(a) > \phi(a)$. So

$$min\{\phi(z - a)|z \in \mathbb{C}\} = min\{\phi(z - a) \mid |z| \leq 2\phi(a), z \in \mathbb{C}\} \tag{1.30}$$

Since the set $\{z \in \mathbb{C} \mid |z| \leq 2\phi(a)\}$ is compact subset of $\mathbb{C}$ and the mapping $z \longrightarrow \phi(z - a)$ is continuous on $\mathbb{C}$, therefore the set on the R.H.S. of (1.30) is a compact subset of positive real numbers. So $\exists\ z_o \in \mathbb{C}$ such that $\phi(z_o - a) = min\{\phi(z - a)|z \in \mathbb{C}\}$, set $a_1 = a - z_o$ and denote $\phi(a - z_o) = \phi(a_1)$ by λ. Fix an element $z \neq 0$ in $\mathbb{C}$ with $|z| < \lambda$. We shall show that,

$$\phi(mz - a_1) = \lambda\ \forall\ m \in \mathbb{N}; \tag{1.31}$$

this will give us a contradiction because

$$\phi(mz-a_1) \geq \phi(mz)-\phi(a_1) = m|z|-\phi(a_1) \longrightarrow \infty \ as \ m \longrightarrow \infty.$$

We first prove (1.31) for $m=1$. *Let* n *be a positive integer and* ξ *be a primitive* $n-th$ *root of unity. Since* $z^n - {a_1}^n = \prod_{i=1}^{n}(\xi^i z - a_1)$ *we have*

$$\prod_{i=1}^{n} \phi(\xi^i z - a_1) = \phi(z^n - {a_1}^n) \leq \phi(z)^n + \phi({a_1}^n) = \phi(z)^n + \lambda^n$$

which by virtue of $\phi(\xi^i z - a_1) = \phi(\xi^i z - a + z_o) \geq \lambda$ *implies that*

$$\phi(z-a_1) \leq \frac{\phi(z)^n + \lambda^n}{\prod_{i=1}^{n-1}\phi(\xi^i z - a_1)} \leq \frac{\phi(z)^n + \lambda^n}{\lambda^{n-1}} = |z|(\frac{|z|}{\lambda})^{n-1} + \lambda.$$

Since $|z| < \lambda$, *letting* $n \longrightarrow \infty$ *the above inequality implies that* $\phi(z-a_1) \leq \lambda$. *Since* $\phi(z-a_1) = \phi(z+z_o-a) \geq \lambda$, *it follows that* $\phi(z-a_1) = \lambda$. *Repeating the above argument replacing* a_1 *by* $a_1 - z = a_2$ *(say) we shall obtain* $\phi(z-a_2) = \phi(2z-a_1) = \lambda$. *In this way (1.31) is proved and hence the theorem is this case.*

Consider the case when K *does not contain* $\sqrt{-1}$, *By Lemma 1.20,* ϕ *can be extended to an absolute value* ϕ_1, *of the field* $K(\sqrt{-1})$ *with respect to which* $K(\sqrt{-1})$ *is complete by Theorem 1.15. By case I,* $K(\sqrt{-1}) = \mathbb{C}$. *Since* $K \supseteq \mathbb{R}$, *we conclude* $K = \mathbb{R}$. □

Remark *It is immediate from the above theorem that* (K, ϕ) *is complete Archimedean, and* K_1 *is a finite extension of* K, *then* ϕ *can be extended to an absolute value of* K_1. *The analogous result, when* ϕ *is non-Archimedean will be proved in the next chapter using Hensel's Lemma.*

Lemma 1.22 *(a)* $\mathbb{R}$ *has only one automorphism.*
(b) $\mathbb{C}$ *has only two continuous automorphisms viz. identity and complex conjugation.*

Proof *(a)Let* f *be automorphism of* $\mathbb{R}$. *Then* f *is identity on* $\mathbb{Q}$. *Since* f *maps squares to squares. So* f *maps positive real numbers to positive real numbers, i.e.,* *whenever $a < b$ then $f(a) < f(b)$. Let r be any real number .There exist a sequence $\{p_n/q_n\}$ of rational numbers such that*

$$| r - p_n/q_n |< 1/n, \text{ i.e. } r - 1/n < p_n/q_n < r + 1/n$$

So, $f(r - 1/n) < f(p_n/q_n) < f(r + 1/n)$, i.e., $f(r) - 1/n < p_n/q_n < f(r) + 1/n$
So, $\{p_n/q_n\}$ converges to $f(r)$. Hence $f(r) = r$.

(b)Let f be an automorphism of $\mathbb{C}$. Then f is identity on $\mathbb{Q}$. It is enough to prove that f is identity on $\mathbb{R}$. Let r be any real number, there exist a sequence $\{p_n/q_n\}$ in $\mathbb{Q}$ converging to r. Then the sequence $\{f(p_n/q_n)\}$ converges to $f(r)$. But $f(p_n/q_n) = p_n/q_n$. So $f(r) = r$. □

Notation *Suppose K is a field embeddable in $\mathbb{C}$, i.e., there exists a isomorphism σ from K into $\mathbb{C}$. In this situation, we denote by ϕ_σ an absolute value of K defined by $\phi_\sigma(x) =| \sigma(x) | \forall x \in K$. Note that for isomorphisms $\sigma, \varsigma : K \longrightarrow \mathbb{C}, \phi_\sigma \sim \phi_\varsigma \Longleftrightarrow \phi_\sigma = \phi_\varsigma$.*

Proposition 1.23 *With the above notation, let σ and ς be isomorphisms of a field K into $\mathbb{C}$ with $\phi_\sigma = \phi_\varsigma$. The following hold:*
(1) If $\sigma(K) \subseteq \mathbb{R}$, then $\sigma = \varsigma$
(2) If $\sigma(K) \nsubseteq \mathbb{R}$, then $\varsigma = \sigma$ or $\varsigma = \bar{\sigma}$.

Proof *(1) By definition of completion, the completion of (K, ϕ_σ) is $(\mathbb{R}, | \ . \ |)$.The completion of (K, ϕ_ς) is $(\mathbb{R}, | \ . \ |)$ or $(\mathbb{C}, | \ . \ |)$. By definition of completion,it has to be $(\mathbb{R}, | \ . \ |)$. So, $\exists$ an automorphism $f : \mathbb{R} \longrightarrow \mathbb{R}$ such that $f \circ \sigma = \varsigma$. By above lemma, f is identity on $\mathbb{R}$. So $\sigma = \varsigma$.*

(2) $\sigma(K) \nsubseteq \mathbb{R}$. By definition, completion of (K, ϕ_σ) is $(\mathbb{C}, | \ |)$.The completion of (K, ϕ_ς) is $(\mathbb{R}, | \ |)$or $(\mathbb{C}, | \ |)$. By uniqueness of completion, it has to be $(\mathbb{C}, | \ . \ |)$. So, there exists an automorphism $f : \mathbb{C} \longrightarrow \mathbb{C}, | f(z) |=| z | \forall z \in \mathbb{C}$ such that $f \circ \sigma = \varsigma$. Such a function f is continuous.Hence, by the above lemma, f = identity or complex conjugation. So,

$$\sigma = \varsigma \text{ or } \bar{\sigma} = \varsigma$$

.

Theorem 1.24 *Let ϕ be an Archimedean absolute value of a field K. Then $\exists$ an isomorphism σ from K into $\mathbb{C}$ such that $\phi \sim \phi_\sigma$.*

Proof *ϕ restricted to $\mathbb{Q}$ is equivalent to the usual absolute value. By Theorem 1.21, the completion $(\hat{K}, \hat{\phi})$ of (K, ϕ) is isomorphic to $(\mathbb{R}, |\ .\ |^\lambda)$ or $(\mathbb{C}, |\ .\ |^\lambda)$ for some λ positive. In any case there is an isomorphism $\hat{\sigma} : \hat{K}$ into $\mathbb{C}$ such that $\hat{\phi}(\alpha) = |\hat{\sigma}(\alpha)|^\lambda$ for $\alpha \in \hat{K}$. Now there exists an isomorphism i from K into $\hat{K}$ such that $\phi(x) = \hat{\phi}(i(x))$ $\forall\ x \in K$.*

Consider the mapping $\hat{\sigma} \circ i\ : K \longrightarrow \mathbb{C}$, denote it by σ. Now for any $x \in K, \phi(x) = \hat{\phi}(i(x)) =|\ \hat{\sigma}(i(x))\ |^\lambda =|\ \sigma(x)\ |^\lambda$. So, $\phi \sim \phi_\sigma$ for some isomorphism σ from K into $\mathbb{C}$. □

Theorem 1.25 *Let (K, ϕ_σ) be an Archimedean valued field and K_1 be an extension of K.If σ_1 is an isomorphism from K_1 into $\mathbb{C}$ extending σ or $\bar{\sigma}$, then ϕ_σ can be extended as an absolute value ϕ_{σ_1} on K_1. Conversely, every absolute value of K_1 extending ϕ_σ is obtained in same manner.*

Proof *First statement is obvious. Conversely, let ϕ_1 be an absolute value of K_1 extending ϕ_σ to K_1.Then by Theorem 1.21, there is an isomorphism $\tau_1 :\ K_1$ into $\mathbb{C}$ and $\lambda > 0$ such that $\phi_1(x_1) =|\ \tau_1(x_1)\ |^\lambda\ \ \forall\ x_1 \in K_1$. Let τ denote the restriction of τ_1 to K, then for any rational number p/q,*

$$|\ p/q\ | = |\ \sigma(p/q)\ | = \phi_\sigma(p/q) = \phi_1(p/q) = |\ \tau(p/q)\ |^\lambda = |\ p/q\ |^\lambda$$

So $\lambda = 1$, consequently $\phi_1(x_1) =|\ \tau_1(x_1)\ |\ \ \forall\ x_1 \in K_1$,
which implies that $\phi_\sigma(x) =|\ \tau(x)\ |\ \ \forall\ x \in \tau$. Hence, By Proposition 1.23, $\tau = \sigma$ or $\bar{\sigma}$. So, τ_1 extends σ or $\bar{\sigma}$. □

Corollary 1.26 *Let K_1/K be an algebraic extension. Then every Archimedean absolute value of K can be extended to K_1.*

Proof *Let ϕ be an Archimedean absolute value of K. Then there exists an isomorphism σ from K into $\mathbb{C}$ such that $\phi \sim \phi_\sigma$. Since σ can be extended to isomorphism of*

K_1 into $\mathbb{C}$, then by Theorem 1.25, ϕ_σ has an extension ϕ_{σ_1} to K_1 and hence ϕ is extendible to K_1. □

Warning *The above corollary is not true when K_1/K is not an algebraic extension. For example, Consider $K = \mathbb{C}$ and $K_1 = \mathbb{C}(t)$ where t is transcendental element. Then the usual absolute value of K cannot be extended to K_1.Suppose if ϕ_1 is an absolute value of K_1 extending the usual absolute value of K. Then by Theorem 1.21, the completion of (K_1, ϕ_1) is isomorphic to $(\mathbb{C}, |\ |)$. So there exists an isomorphism $\sigma : K_1 \longrightarrow \mathbb{C}$ which is identity on $\mathbb{C}$.But such an isomorphism does not exist.*

Remark *The analogue of Corollary 1.26 also holds for non-Archimedean values and will be proved in the second chapter using Hensel's Lemma.*

Corollary 1.27 *Let ϕ be an Archimedean absolute value of K. Let $K_1 = K(\theta)$ be a extension of K of degree n.Let $r_1, 2r_2$ denote respectively the number of real, complex roots of the minimal polynomial of θ over K. Then the number of extensions of ϕ to K_1 are $r_1 + r_2$ or n according as the completion of (K, ϕ) is $\mathbb{R}$ or $\mathbb{C}$.*

Proof *Let $\sigma : K \longrightarrow \mathbb{C}$ be an isomorphism such that $\phi \sim \phi_\sigma$.The number of extensions of ϕ_σ to K_1 is same as the extensions of ϕ to K_1. Let $\sigma_1, \cdots, \sigma_r$ be all the isomorphisms from $K_1 \longrightarrow \mathbb{C}$ extending σ such that $\sigma_1, \cdots, \sigma_r$ are real and $\sigma_{r+1}, \sigma_{r+2}, \cdots, \sigma_{r_1+2r_2}$ are complex with $\bar{\sigma}_{r_1+j} = \sigma_{r_1+r_2+j}$. By Proposition 1.23, $\phi_{\sigma_i} = \phi_{\sigma_j} \Longleftrightarrow \sigma_j = (\bar{\sigma}_i)$ which is possible when $\sigma = \bar{\sigma}$, i.e., $\sigma(K) \subseteq \mathbb{R}$. So if $\sigma(K) \nsubseteq \mathbb{R}$, then all $\phi_{\sigma_i}, 1 \leq i \leq n$ are distinct and if $\sigma(K) \subseteq \mathbb{R}$, then $\{\phi_{\sigma_1}, \phi_{\sigma_2}, \cdots, \phi_{\sigma_{r_1}}, \phi_{\sigma_{r_1+1}}, \cdots, \phi_{\sigma_{r_1+r_2}}\}$ are all the distinct extensions of ϕ_σ to K_1.*

Chapter 2

Real Valuations

2.1 Real Valuations via Non-Archimedean absolute values

Let ϕ be a non-Archimedean absolute value of a field K. Define $v : K \longrightarrow \mathbb{R} \cup \{\infty\}$ by setting $v(0) = \infty, v(x) = -log\ \phi(x)$ for non-zero $x \in K$. Then v satisfies the following properties for all $x, y \in K$.
(1) $v(x) = \infty$ if and only if $x = 0$
(2) $v(xy) = v(x) + v(y)$,
(3) $v(x + y) \geq min\{v(x), v(y)\}$.

Definition *A mapping $v : K \longrightarrow \mathbb{R} \cup \{\infty\}$ satisfying the above three properties is called a real valuation or classical valuation of K. The pair (K, v) is called a valued field. Conversely if v is a real valuation of a field K, then v gives rise to a non-Archimedean absolute value ϕ on K defined by $\phi = e^{-v}$.*
The trivial valuation of K is defined to be the one for which $v(x) = 0$ for every non-zero $x \in K$.

Definition *Two real valuations v, v' are said to be equivalent if there exists a real number $\rho > 0$ such that $v'(x) = \rho v(x)$ for every $x \in K$.*

Remark *Let K be a field. There is a natural one to one correspondence between the set of equivalence classes of real valuations of K and the set of equivalence classes of non-Archimedean absolute values of K given by $v \longrightarrow \phi = e^{-v}; \phi \longrightarrow v = -log_{e^{\phi}}$. Also it is clear that under this one-to-one correspondence, the trivial absolute value corresponds to the trivial valuation of K.*

Definitions and Notations *Let v be a valuation of a field K.*

Valuation Ring *The set $\mathcal{O}_v = \{x \in K \mid v(x) \geq 0\}$ is a subring of K called the valuation ring of v. Since $v(x^{-1}) = -v(x)$, for any element $x \in K$ either $x \in \mathcal{O}_v$ or $x^{-1} \in \mathcal{O}_v$. So, $\mathcal{O}_v$ has K as a field of quotients.*

Maximal Ideal *The set $\mathcal{M}_v = \{x \in K \mid v(x) > 0\}$ is an ideal of $\mathcal{O}_v$. As $\mathcal{M}_v$ consists exactly of all the non-units of $\mathcal{O}_v$, $\mathcal{M}_v$ is maximal ideal and infact is the only maximal ideal of $\mathcal{O}_v$. Thus $\mathcal{O}_v$ is a local ring.*

Residue field *$\mathcal{O}_v/\mathcal{M}_v$ is called the Residue Field of v or Residue Class Field of v and the image of an element $\alpha \in \mathcal{O}_v$ under the canonical homomorphism from $\mathcal{O}_v$ onto $\mathcal{O}_v/\mathcal{M}_v$ is called the $v - residue$ of α and will be denoted by $\bar{\alpha}$.*

Value Group*The group $v(K^*)$ is called the value group of v.*

Remark *If R is an integral domain with quotient field K and v is a mapping on R satisfying the three conditions of valuation, then v gives rise to a valuation on K in a natural manner.*

Notations *Let R be a U.F.D. and π be a prime element of R, then we denote by v_π the $\pi - adic$ valuation of K defined for any non-zero $x \in R$ by $v_\pi(x) = r$, where $x = \pi^r y, y \in R, \pi \nmid y$. Its valuation ring $\mathcal{O}_{v_\pi}$ is the localization of R at prime ideal πR. In view of the following remark the residue field of v_π is isomorphic to the* *quotient field of $R/\pi R$. In the particular case when $R = \mathbb{Z}$ and p is a prime number, v_p will denote the $p-adic$ valuation of $\mathbb{Q}$.*

Remark *Let R be a commutative ring and P be a prime ideal of R. Let $R_P = \left\{\frac{x}{y} \mid x \in R, y \in R \setminus P\right\}$ and $M_P = \left\{\frac{x}{y} \mid x \in P, y \in R \setminus P\right\}$. Prove that $R_P/M_P \cong$ quotient field of R/P.*

Proof *We define a map $f : R_P \longrightarrow$ quotient field of R/P by defining the image of an element $\frac{x}{y} \in R_P, x \in R, y \in R \setminus P$ by $f(x/y) = (x+P)(y+P)^{-1}$.*
Clearly f is well defined, a ring homomorphism and $\frac{x}{y} \in\ ker f \Longleftrightarrow f(\frac{x}{y}) = \frac{x+P}{y+P} = P \Longleftrightarrow x \in P$. So, $ker f = M_P$. Thus $R_P/M_P \cong quotient\ field\ of\ R/P$.

Strong triangle law *Let v be a valuation of a field K. If $x, y \in K$ are such that $v(x) \neq v(y)$. Then $v(x+y) = min\left\{v(x), v(y)\right\}$.*

Proof *Assume that $v(x) < v(y)$. By definition of valuation*

$$v(x+y) \geq min\{v(x), v(y)\} = v(x) \tag{2.1}$$

Again by definition of valuation

$$v(x) = v(x+y-y) \geq min\{v(x+y), v(y)\}$$

and the above minimum has to be $v(x+y)$ in view of the assumption $v(x) < v(y)$. Hence $v(x+y) = v(x)$ in view of equation (2.1).

Topology defined by a Real valuation *Let v be a real valuation of a field K. Then v induces a metric on K; infact it is the metric given by the corresponding absolute value on K. A base for the neighbourhood system at a point x is the family of all sets $N_m(x) = \{y \in K \mid v(x-y) > m\}$ where m runs over all positive integers. Note that the topology corresponding to a valuation is discrete $\Longleftrightarrow$ corresponding valuation is trivial.*

Remark *Let (K, v) is a valued field with v real valuation. A sequence $\{x_n\}$ is Cauchy in $K \Longleftrightarrow v(x_{n+k} - x_n) \longrightarrow \infty$ as $n, k \longrightarrow \infty \Longleftrightarrow v(x_{n+1} - x_n) \longrightarrow \infty$ as $n \longrightarrow \infty$, $\because v(x_{n+k} - x_n) = v(x_{n+k} - x_{n+k-1} + x_{n+k-1} \cdots - x_n)$*

$$\geq min\{v(x_{n+k} - x_{n+k-1}), v(x_{n+k-1} - x_{n+k-2}), \cdots, v(x_{n+1} - x_n)\}$$

Notation *Let (K, v) be a valued field. We shall denote by $(\hat{K}, \hat{v})$ the completion of (K, v) with respect to the topology defined above.*

Theorem 2.1 *Let (K, v) be a valued field with a real valuation v. Then the value groups of v and $\hat{v}$ are same, the valuation ring $\mathcal{O}_{\hat{v}}$ of $\hat{v}$ equals to $\mathcal{O}_v + \mathcal{M}_{\hat{v}}$ and the residue fields of v and $\hat{v}$ are canonically isomorphic.*

Proof *Let $x \in \hat{K}^*$ be given. By the density of K in $\hat{K}$ there exists $z \in K$ with $\hat{v}(z - x) > \hat{v}(x)$. But then by Strong Triangle Law, we have $\hat{v}(z) = min\{\hat{v}(z - x), \hat{v}(x)\} = \hat{v}(x)$. So, the value groups of v and $\hat{v}$ are same. For any given $\alpha \in \mathcal{O}_{\hat{v}}, \exists\, a \in \mathcal{O}_v$ such that $\hat{v}(\alpha - a) > 0$, So, $\mathcal{O}_{\hat{v}} = \mathcal{O}_v + \mathcal{M}_{\hat{v}}$. Also, clearly $\mathcal{M}_v = \mathcal{O}_v \cap \mathcal{M}_{\hat{v}}$. Therefore by second theorem of isomorphism, we have $\mathcal{O}_{\hat{v}}/\mathcal{M}_{\hat{v}} \cong \mathcal{O}_v/\mathcal{O}_v \cap \mathcal{M}_{\hat{v}} = \mathcal{O}_v/\mathcal{M}_v$.* □

For the valuations of field K, there is a stronger view of Approximation Theorem given by

Theorem 2.2 *Let $v_1, v_2, \cdots, v_n$ be pairwise inequivalent valuations of a field K with value groups $\Gamma_1, \Gamma_2, \cdots, \Gamma_n$. Then for any $x_1, \cdots, x_n \in K$ and $\gamma_i \in \Gamma_i$, $1 \leq i \leq n$, $\exists\, x \in K$ such that $v_i(x - x_i) = \gamma_i$.*

Proof *Atmost one of v_i can be trivial, say v_1 is trivial. Choose $y_i \in K$ such that*

$$v_i(y_i) = \gamma_i \; for \; 2 \leq i \leq n \tag{2.2}$$

By Approximation Theorem, $\exists\ z, y \in K$ *such that*

$$v_i(z - x_i) > \gamma_i, v_i(y - y_i) > \gamma_i \ for\ 2 \leq i \leq n \tag{2.3}$$

Infact y *and* z *can be chosen such that* $y + z \neq x_1$. $\because$ *if* $y + z = x_1$, *we replace* y *by* $y' = y + y_o$ *where* $y_o \in K$ *is a non-zero element with* $v_i(y_o) > \gamma_i$ *for each* $i \geq\ 2$, *such an element* y_o *exists(in view of Approximation Theorem). Now* $v_1(y+z-x_1) = 0 = \gamma_1$. *For* $2 \leq i \leq n$, *we have by (2.2),(2.3) and Strong Triangle Law*

$$v_i(y) = v_i(y - y_i + y_i) = min\{v_i(y - y_i), v_i(y_i)\} = v_i(y_i) = \gamma_i$$

$$v_i(y + z - x_i) = min\{v_i(y), v_i(z - x_i)\} = \gamma_i$$

So, $x = y+z$ *satisfies the desired property.* □

Remark *The above theorem does not hold for Archimedean absolute values. For example, let* $\phi =$ *the usual absolute value on* $K = \mathbb{Q}(\sqrt{5}), \psi$ *be the absolute value defined by* $\psi(a + b\sqrt{5}) =\mid a - b\sqrt{5} \mid$, *and* ψ_5 *be the normalized absolute value corresponding to the* $5 - adic$ *value of* K, *i.e., Claim:* $\psi_5(x) = (1/5)^{v_5(x)}$. *Claim that there does not exist any* $x \in K$ *such that* $\phi(x) = 1, \psi(x) = 3, \psi_5(x) = 1$. *Suppose such an element* $x = a + b\sqrt{5}$ *exists, then* $\mid a^2 - 5b^2 \mid= 3$. *Write* $a = \frac{a_1}{a_2}, b = \frac{b_1}{b_2}, (a_1, a_2) = 1 = (b_1, b_2),\ a_i, b_i \in \mathbb{Z}$. *Since* $\psi_5(a) \neq \psi_5(b\sqrt{5})$. $\because$ *R.H.S. is power of* $1/5$ *multiplied by* $1/\sqrt{5}$ *and L.H.S. is a power of* $1/5$. *So, by Strong Triangle Law,* $\psi_5(a + b\sqrt{5}) = max\{\psi_5(a), \psi_5(b\sqrt{5})\} = 1$. $\psi_5(b\sqrt{5}) \neq 1$.*So,* $5 \nmid b_2$ *and* $5 \nmid a_1a_2$, *so we see* ${a_1}^2{b_2}^2 - 5{a_2}^2{b_1}^2 = \pm 3{a_2}^2{b_2}^2$ *which shows that* $X^2 \equiv \pm 3(mod\ 5)$ *is solvable. This contradiction proves the claim.*

We now determine all valuation of $K(X)$ *which are trivial on* K, *where* K *is a field and* X *is an in determinate. For this we first prove the following theorem.*

Theorem 2.3 *Let* R *be a P.I.D. with quotient field* K. *Let* v *be a real valuation on* K *such that the valuation ring of* v *contains* R. *Then* v *is equivalent to* v_π *for some irreducible element* π *of* R.

Proof *Let v be a non-trivial real valuation on K. Let $\mathcal{O}_v$ be the valuation ring of K and $\mathcal{M}_v$ be the maximal ideal, then $\mathcal{M}_v \cap R$ is a non-zero prime ideal of R. Therefore, there exists an irreducible element $\pi \in R$ such that $\mathcal{M}_v \cap R = \pi R$. For this $\pi, v(\pi) > 0$.*

Consider $a \in R \setminus \pi R$, then $a \notin \mathcal{M}_v$. $\therefore$ a is a unit of $\mathcal{O}_v$ and hence $v(a) = 0$. Also $v_\pi(a) = 0$. Now for any $x = \pi^m a/b; a, b \in R, \pi \nmid ab, v(x) = mv(\pi)$ as $v(ab) = 0$ as $ab \notin \pi R$. Also $v_\pi(x) = m$. $\therefore$ v is equivalent to v_π. Hence proved. □

Theorem 2.4 *Every non-trivial valuation on $K(X)$, trivial on K is either equivalent to the degree valuation v_∞ defined by $v_\infty(\frac{f(X)}{g(X)}) = deg(g(X)) - deg(f(X))$ or $p(X) - adic$ valuation for some irreducible polynomial $p(X) \in K[X]$.*

Proof

***Case I**: $\{v(X) \geq 0\}$*

Take $R = K[X]$. Then $R \subseteq O_v$. So, by Theorem 2.3, v is equivalent to $p(X) - adic$ valuation for some irreducible element $p(X)$ of $K[X]$.

***Case II** $v(X) < 0$,*

Then $v(X^m) < v(X^n)$ whenever $0 \leq n < m$. Since $v(a) = 0 \ \forall \ a \in K^*$, we get by Strong Triangle Law,

$$v(a_n X^n + a_{-1}X^{n-1} + \cdots + a_o) = v(a_n X^n) = nv(X) \ if a_n \neq 0$$

$$\therefore v(\frac{f(X)}{g(X)}) = (deg \ f(X) - deg \ g(X))v(X)$$

So v is equivalent to v_∞.

We now determine a class of valuations of $K[X]$ which are non-trivial on K, where K is a field and X is an indeterminate. □

Theorem 2.5 *Let (K, v) be a real valued field, let μ be a real number, and let $w : K[X] \longrightarrow \mathbb{R} \cup \{\infty\}$ be the mapping defined by,*

$$w(\sum_{i-0}^{n} a_i X^i) = min\{v(a_i) + i\mu \mid 0 \leq i \leq n\}$$

$w(\frac{f(X)}{g(X)}) = w(f(X)) - w(g(X))$ where $f(X), g(X) \in K[X], g(X) \neq 0$. Then w is a valuation on $K[X]$ whose restriction to K is equal to v, and whose value group is the subgroup of $\mathbb{R}$ generated by $v(K)$ and μ.

Proof *(1) For $f(X) = 0, w(f(X)) = \infty$.*
(2) To show that if $f = \sum_{i=0}^{n} a_i X^i, g = \sum_{j=0}^{m} b_j X^j$ are polynomials in $K[X]$, then $w(fg) = w(f) + w(g),\ w(f+g) \geq min\{w(f), w(g)\}$.
Write $fg = \sum_{k=0}^{m+n} c_k X^k$ where $c_k = \sum_{i+j=k} a_i b_j$. Let i_o, j_o be chosen so that

$$i_o = min\{i \mid v(a_i) + i\mu = w(f)\},\ j_o = min\{j \mid v(b_j) + i\mu = w(g)\}$$

then

$$c_{i_o+j_o} = a_{i_o} b_{j_o} + \sum_{i+j=i_o+j_o, i\neq i_o} a_i b_j \tag{2.4}$$

Since $i \neq i_o, i + j = i_o + j_o$ implies $i > i_o$ or $j > j_o$, then $v(a_{i_o} b_{j_o}) + (i_o + j_o)\mu = (v(a_{i_o}) + i\mu) + (v(b_{j_o}) + j_o\mu) < min\{v(a_i) + i\mu) + (v(b_j) + j\mu) \mid i + j = i_o + j_o, i \neq i_o\}$ Hence by(2.4) and Strong Triangle Law, we have

$$v(c_{i_o} + j_o) + (i_o + j_o)\mu = v(a_{i_o} b_{j_o}) + (i_o + j_o)\mu = w(f) + w(g)$$

Thus we have shown that,

$$w(fg) \leq v(c_{i_o+j_o}) + (i_o + j_o)\mu = w(f) + w(g) \tag{2.5}$$

On the other hand, for any $k, 0 \leq k \leq m + n$,

$$v(c_k) + k\mu = v(\sum_{i+j=k} a_i b_j) + k\mu$$

$$\geq \min_{i,j}\{v(a_i) + v(b_j) \mid i + j = k\} + k\mu$$

$$= \min_{i,j}\{(v(a_i) + i\mu) + (v(b_j) + j\mu) \mid i + j = k\}$$

$$\geq w(f) + w(g).$$

So

$$w(fg) \geq w(f) + w(g) \tag{2.6}$$

By (2.5)and(2.6), we have $w(fg) = w(f) + w(g)$. We now verify the triangle inequality. Assume without loss of generality that $n = max\{degf, deg\ g\}$. Set $a_i = 0$ if $m + 1 \leq i \leq n$. Then

$$w(f+g) = \min_{0 \leq i \leq n} \{v(a_i + b_i) + i\mu \mid 0 \leq i \leq n\}$$

$$\geq \min_{0 \leq i \leq n} \{min(v(a_i) + i\mu, v(b_i) + i\mu) \mid 0 \leq i \leq n\}$$

$$= min\{w(f), w(g)\}.$$

Definition *Let v be a valuation of K.The valuation v^x of $K[X]$ extending the valuation v of K defined by $v^x(\sum_{i=0}^{n} a_i X^i) = min_i v(a_i)$ is called the Gaussian extension of v to $K[X]$. A polynomial $f(X) \in K[X]$ is said to be primitive w.r.t. v if $v^x(f(X)) = 0$. Since for polynomials $f, g \in K[X]$, $v^x(f, g) = v^x(f) + v^x(g)$, it follows that a product of primitive polynomials is primitive. This is the analogue for valued fields of the well known Gauss's lemma for polynomial with coefficients in a U.F.D.*

Proposition 2.6 *Let $\bar{K}$ be the residue field of a valuation v of K. Then the residue field of v^x is the simple transcendental extension $\bar{K}(\bar{X})$ of $\bar{K}$.*

Proof *Note that the $v^x - residue \bar{X}$ of X is the transcendental over $\bar{K}$, because if $\bar{a}_i \in \bar{K}$ are such that $\sum_{i=0}^{n} \bar{a}_i \bar{X}^i = \bar{0}$, $a_i \in \bar{O}_v$, then $v^x(\sum_{i=0}^{n} a_i X^i) > 0$. So $v(a_i) > 0\ \forall\ i$, i.e., $\bar{a}_i = \bar{0}$. We now show that the residue field of v^x is $\bar{K}(\bar{X})$. Let $\xi = \frac{f(X)}{g(X)}$ be any element of $K[X]$ with $v^x(\xi) = 0$. Write $f(X) = c_1 f_1(X), c_1 \in K$ and $v^x(f_1(X)) = 0,\ g(X) = d_1 g_1(X),\ d_1 \in K, v^x(g_1(X)) = 0$. Since $v^x(f/g) = 0 \Rightarrow$ $v(c_1) = v^x(c_1 f_1) = v^x(d_1 g_1) = v(d_1)$.*
So, $\bar{\xi} = (\bar{\frac{c_1}{d_1}\frac{f_1(X)}{g_1(X)}}) = (\bar{\frac{c_1}{d_1}})(\bar{\frac{f_1(X)}{g_1(X)}}) = (\bar{\frac{c_1}{d_1}})\frac{\bar{f_1}(\bar{X})}{\bar{g_1}(\bar{X})} \in \bar{K}[\bar{X}]$. □

2.2 Discrete Valuations

Definition *Let K be a field and v be a valuation on K. Then v is said to be discrete if the value group $v(K^*)$ is isomorphic to additive group $\mathbb{Z}$. In view of the following lemma v is discrete if the value group of v is discrete subset of $\mathbb{R}$ w.r.t. usual topology.*

Lemma 2.7 *Let G be a non-trivial subgroup of $(\mathbb{R}, +)$. The following conditions are equivalent:*
(1) G is a discrete subgroup of $\mathbb{R}$.
(2) G is not dense in $\mathbb{R}$.
(3) G has a least positive element.
(4) G is cyclic group.

Proof *(1)⇒(2) is trivial. We prove (2)⇒(3):*
Suppose (3) does not hold. Let g_0 be any positive element of G, $\exists\ g_1 \in G$ such that $0 < g_1 < g_0$. If $g_1 \leq g_o/2$, then fine otherwise we can replace g_1 by $g_0 - g_1$ so that we can assume without loss of generality that $0 < g_1 \leq g_0/2$. $\exists$ an $g_2 \in G$ such that $0 < g_2 \leq g_1/2 \leq g_o/2^2$. Proceeding in this way $\exists\ g_i \in G$ such that $0 < g_i \leq g_o/2^i$. If r is any positive real number and $(r - \epsilon, r + \epsilon)$ is any neighbourhood of r, then $\exists$ an i such that $g_i < \epsilon$. $\therefore \exists$ an integer m such that $mg_i \in (r - \epsilon, r + \epsilon)$. Therefore, r is a closure point of G. This shows that G is dense in $\mathbb{R}$ which contradicts (2) and proves that (2)⇒(3). Now,(3)⇒(4): Let g_0 be the least positive element of G. For any $g \in G$ there is an $n \in \mathbb{Z}$ such that $ng_0 \leq g < (n+1)g_0,\ 0 \leq g - ng_0 < g_0$. As g_0 is the least positive element of G, $g - ng_0 = 0$ i.e. $g = ng_0$. Hence $G = g_0\mathbb{Z}$.
(4)⇒(1): Let $G = g_0\mathbb{Z},\ g_0 > 0$. If r is any real number, then $(r - g_0/2, r + g_0/2)$ can contain at most one point of G. So r is not a limit point of G.

Definition *Let v be a discrete valuation of K. Let g_0 be the smallest positive element in the value group of v. An element π of K with $v(\pi) = g_o$ is called an uniformizer of v.*

Remark *Let K be a field and v be a discrete valuation on K with value group $\mathbb{Z}$. An* *element $x \in K^*$ can be written as $u\pi^r$, where u is the unit of $\mathcal{O}_v, v(x) = r$. Indeed if $r = v(x)$, then $v(x\pi^{-r}) = v(x) - rv(\pi) = 0$. Thus $u = x\pi^{-r}$ is a unit of $\mathcal{O}_v$. Also the maximal ideal $\mathcal{M}_v$ is a principal ideal generated by π and every other ideal $J \neq 0$ of $\mathcal{O}_v$ is a principal ideal generated by some power π^n where $n = min\{v(a) \mid a \in J\}$. So $\mathcal{O}_v$ is a P.I.D., hence Noetherian. The converse is also true as proved by the following theorem.*

Theorem 2.8 *Let v be a non-trivial real valuation of K with valuation ring $\mathcal{O}_v$ having maximal ideal $\mathcal{M}_v$. Then the following statements are equivalent:*
(1)v is a discrete valuation.
(2) Every non-zero ideal of $\mathcal{O}_v$ is power of $\mathcal{M}_v$.
(3) $\mathcal{O}_v$ is Noetherian ring.
(4) $\mathcal{M}_v$ is a principal ideal.
(5) Every ideal of $\mathcal{O}_v$ is principal.
(6) Every finitely generated fractional ideal of K (relative to $\mathcal{O}_v$) is principal.
(7) The set of non-zero fractional ideals of K is a multiplicative group; and
(8) $\mathcal{M}_v \neq {\mathcal{M}_v}^2$.

Proof (1) $\Rightarrow$ (2) *Let $J \neq 0$ be any ideal of $\mathcal{O}_v$. By hypothesis $v(K^*) \simeq \mathbb{Z}$, hence there exists $\lambda > 0$ such that $v(K^*) = \mathbb{Z}\lambda$. Let $t \in \mathcal{M}_v$ be such that $v(t) = \lambda$. Then $\mathcal{M}_v = \mathcal{O}_v t$, because if $v(x) > 0$, then $v(x) \geq \lambda$. So $x = (x/t)t \in \mathcal{O}_v t$. Let*

$$m\lambda = min\{v(y) \mid y \in J\} \tag{2.7}$$

let $x \in J$ be such that $v(x) = m\lambda$. Then by view of (2.7) $\mathcal{O}_v x \subseteq J \subseteq \mathcal{O}_v t^m$, because if $y \in J$, then $v(yt^{-m}) \geq 0$. On writing $t^m = (t^m x^{-1})x \in \mathcal{O}_v x$, we conclude that $J = \mathcal{O}_v t^m$.
(2)$\Rightarrow$(3): We note that if $0 \leq k \leq l$ are integers, then ${\mathcal{M}_v}^l \subseteq {\mathcal{M}_v}^k$. Since every ideal of $\mathcal{O}_v$ is a power of M_v, then any strictly ascending chain of ideals of $\mathcal{O}_v$ is finite, so $\mathcal{O}_v$ is a Noetherian ring.
(3)$\Rightarrow$(4): By hypothesis, every ideal of $\mathcal{O}_v$ is finitely generated. Let J be a non-zero finitely generated ideal of $\mathcal{O}_v$ generated by the elements $x_1, \cdots, x_n$; let us assume that $v(x_1) \leq v(x_i)$ for every $i = 2, \cdots, n$. Then $x_i = (x_i {x_1}^{-1})x_1 \in \mathcal{O}_v x_1$ because

$v(x_i{x_1}^{-1}) \geq 0$ for every $i = 2, 3, \cdots n$. Hence $J = O_v x_1 + \cdots + O_v x_n = O_v x_1$. Thus $\mathcal{M}_v$ must be a principal ideal.
(4)⇒(5): Let $\mathcal{M}_v = \mathcal{O}_v t$, so $v(t) > 0$. Let J be any non-zero ideal of $\mathcal{O}_v$. Let $\gamma = inf\{v(x) \mid x \in J\}$. If there exists $y \in J$ such that $v(y) = \gamma$, then $J = \mathcal{O}_v y$, because if $x \in J$, then $x = (xy^{-1})y$ with $v(xy^{-1}) \geq 0$, so $x \in \mathcal{O}_v y$. However, if $v(x) > \gamma$ for every $x \in J$, there exists $y \in J$ such that $\gamma < v(y) < \gamma + v(t)$ and also $z \in J$ such that $\gamma < v(z) < v(y)$; therefore $0 < v(yz^{-1}) < v(t)$, so $yz^{-1} \in \mathcal{M}_v = \mathcal{O}_v t$. So $v(yz^{-1}) \geq v(t)$, a contradiction.
(5)⇒(6): Let J be a non-zero finitely generated fractional ideal, so there exists $a \in O_v, a \neq 0$, such that $aJ \subseteq \mathcal{O}_v$, hence by hypothesis $aJ = \mathcal{O}_v x$ where $x \in \mathcal{O}_v$ and so $J = \mathcal{O}_v a^{-1} x$.
(6)⇒(7): Indeed, each non-zero finitely generated fractional ideal $J = \mathcal{O}_v x$ has inverse $J^{-1} = \mathcal{O}_v x^{-1}$.
(7)⇒(8): If $\mathcal{M}_v = {\mathcal{M}_v}^2$ then $\mathcal{O}_v = \mathcal{M}_v^{-1}\mathcal{M}_v = \mathcal{M}_v^{-1}{\mathcal{M}_v}^2 = \mathcal{M}_v$ which is impossible.
(8)⇒(1): Let $t \in \mathcal{M}_v, t \notin {\mathcal{M}_v}^2$, for every element $x \in \mathcal{O}_v, x \neq 0$, there exists an integer $n \geq 0$ such that $nv(t) \leq v(x) < (n+1)v(t)$. If $nv(t) < v(x)$, then x/t^n and $t^{n+1}/x \in \mathcal{M}_v$, hence $t = \frac{x}{t^n}\frac{t^{n+1}}{x} \in \mathcal{M}_v^2$, which is contradiction. This shows that $v(x) = nv(t)$, hence $v(K) \cong \mathbb{Z}$. □

It must be emphasized at once that not at all valuation are discrete. A non-trivial valuation of an algebraically closed field can't be discrete as the following remark shows.

Remark *Let K be an algebraically closed field and v is a non-trivial valuation of K, then the group $v(K^*)$ is divisible, i.e., given $n \in \mathbb{Z}, n > 0$ and $v(z) \in v(K^*)$, then there exists $\gamma \in v(K^*)$ such that $n\gamma = v(z)$. Choose $y \in K^*$ such that $y^n = z$. Then $nv(y) = v(z)$.*

2.3 Complete discrete valued fields

Suppose that K is both complete and discrete with respect to a valuation v with value group $\mathbb{Z}$. Let $\{\pi_n \mid n \in \mathbb{Z}\}$ be the set of elements of K with

$$v(\pi_n) = n \tag{2.8}$$

Then for given $c_i \in \mathcal{O}_v, (i \geq r)$, the series $\sum_{i=r}^{\infty} c_i\pi_i$ converges in K. If c_r is unit Of $\mathcal{O}_v$ then using Strong Triangle Law, we can verify that $v(\sum_{i=r}^{\infty} c_i\pi_i) = r$.

***Notation** A sum $\sum_{i=-\infty}^{\infty} a_i$ where $a_i = 0$ for all but finitely many negative i will be denoted by $\sum_{i>>-\infty} a_i$.*

***Definition** By a system of representation of the residue field $\mathcal{O}_v/\mathcal{M}_v$, we mean a subset $\mathcal{C}$ of $\mathcal{O}_v$ satisfying the following properties:*
(1) zero $\in \mathcal{C}$
(2) $c_1, c_2 \in \mathcal{C}, c_1 \neq c_2 \Rightarrow c_1 \equiv c_2 (mod\ \mathcal{M}_v)$
(3) For any $a \in \mathcal{O}_v, \exists\ c \in \mathcal{C}$ such that $a \equiv c(mod\ \mathcal{M}_v)$.

Theorem 2.9 *Let K be a field complete, discrete with respect to a valuation v with value group $\mathbb{Z}$. Let $\mathcal{C}$ be a complete system of representatives of the residue field $\mathcal{O}_v/\mathcal{M}_v$ containing zero. Let $\pi_n \in K$ be such that satisfying (2.8). Then an arbitrary element $a \in K$ can be uniquely written as*

$$a = \sum_{i>>-\infty} c_i\pi_i,\ c_i \in \mathcal{C} \tag{2.9}$$

More specifically if π is a uniformizer of K, we may write

$$a = \sum_{i>>-\infty} c_i\pi^i \tag{2.10}$$

When furthermore $v(a) = n$ in (2.9)and(2.10), we have $c_n \neq 0, c_i = 0\ \forall\ i < n$.

Proof *If $a = 0$, we take $c_i = 0$. So, suppose $v(a) = n$. We shall first set $c_i = 0$ for all $i < n$. As $u = a\pi^{-1}$ is a unit, so $\exists$ an element $c_n(\neq\ 0) \in\ \mathcal{C}$ such that $u \equiv c_n(mod\ \mathcal{M}_v)$ Then clearly $v(a\pi_n^{-1} - c_n) > 0$ or equivalently $v(a - c_n\pi_n) > v(\pi_n) = n$. Let $a_1 = a - c_n\pi_n$ and $n_1 = v(a_1) > n$. Here we set $c_i = 0$ for $n < i < n_1$. So $\exists\ c_{n_1} \in \mathcal{C}$ such that $\frac{a_1}{\pi_{n_1}} \equiv c_{n_1}(mod\ \mathcal{M}_v), v(a_1 - c_{n_1}\pi_{n_1}) > n_1$. Set $a_2 = a_1 - c_{n_1}\pi_{n_1}$, say $v(a_2) = n_2 > n_1 \geq n + 1$. Set $c_i = 0$ for $n_1 < i < n_2$. Choose c_{n_2} such that $\frac{a_2}{\pi_{n_2}} \equiv c_{n_2}(mod\ \mathcal{M}_v), v(a_2 - c_{n_2}\pi_{n_2}) > n_2$. Set $a_3 = a_2 - c_{n_2}\pi_{n_2}$, say $v(a_3) = n_3 > n_2 \geq n + 2$. Set $c_i = 0$ for $n_2 < i < n_3$. Repeating this process and adding zero co-efficient if necessary, we obtain the existence of the sequence*

$$a \equiv c_n\pi_n + c_{n+1}\pi_{n+1} + \cdots + c_{n_m}\pi_{n_m} + a_{m+1}$$

where $v(a_{m+1}) > n_m \geq n + m\ \forall\ m \geq 1$. Letting $m \longrightarrow \infty$, we have

$$a = \sum_{i=n}^{\infty} c_i\pi_i = \sum_{i>>-\infty} c_i\pi_i.$$

Uniqueness *Suppose we have two expansions of a, $a = \sum\limits_{i>>-\infty} c_i\pi_i,\ c_i \in \mathcal{C}$ and $a = \sum\limits_{i>>-\infty} c_i'\pi_i,\ c_i' \in \mathcal{C}$ with $c_i \neq c_i'$ for some i. Let i_o be the minimum of such i for which $c_i \neq c_i'$. Then $\sum\limits_{i=i_o}^{\infty} c_i\pi_i = \sum\limits_{i=i_o}^{\infty} c_i'\pi_i$. $\therefore (c_{i_o} - c_{i_o}')\pi_{i_o} = -\sum\limits_{i=i_o+1}^{\infty}(c_i - c_i')\pi_i$ and hence $v((c_{i_o} - c_{i_o}')\pi_{i_o}) \geq i_o + 1 \Rightarrow c_{i_o} - c_{i_o}' \in \mathcal{M}_v$, i.e., $c_{i_o} \equiv c_{i_o}'(mod\ \mathcal{M}_v)$ which is not possible. Thus the expansion is unique.*

Corollary *A complete valued field is uncountable.*

Definition *Let $R = F[X]$ be the ring of polynomials over any field K in an indeterminate X. Let v denote $X-adic$ valuation on $K = F[X]$, corresponding to the prime element X of R. The residue field of v is isomorphic to $F[X]/\langle X\rangle \cong F$. Since $\mathcal{O}_{\hat{v}}/\mathcal{M}_{\hat{v}} \cong \{\mathcal{O}_v/\mathcal{M}_v\} \cong F$. We may take F as complete system representatives of $\mathcal{O}_{\hat{v}}$ modulo $\mathcal{M}_{\hat{v}}$. $\therefore$ by Theorem 2.9, every element of $\hat{K}$ can be uniquely written as $\sum\limits_{i>>-\infty} a_iX^i,\ a \in F,\ \hat{K}$ is called the field of Laurent Series over F. The valuation* *ring $\hat{\mathcal{O}}_v$ is called the ring of formal power series over F and is denoted by $F[[X]]$. It consists of series of type $\sum\limits_{i=0}^{\infty} a_i X^i,\ a_i \in F$.*

Remark *Let (K, v) be complete discrete valued field. If char(K) is same as the char of residue field of v, then it was proved in 1936 that $\exists$ subfield F of $\mathcal{O}_v$which can be chosen as a complete system of representatives of $\mathcal{O}_v/\mathcal{M}_v$. So in this situation $K = F((\pi))$ where π is a uniformizer of v. Thus every complete discrete valued field whose char is same as that of its residue field is isomorphic to the field of Laurent Series.*

2.4 $p - adic$ numbers

Definition *Let $\mathbb{Q}$ be equipped with $p - adic$ valuation v_p corresponding to the prime p defined for any integer n, taking $v_p(n) =$ the highest power of p dividing n and $\mathbb{Q}_p$ be the completion of $\mathbb{Q}$ with respect to v_p. Then $\mathbb{Q}_p$ is called the field of $p - adic$ numbers. The valuation ring of $\hat{v_p}$ is called ring of $p - adic$ integers.*

Remark *Keeping in mind the residue field of $\hat{v_p}$ is isomorphic to that of v_p in view of Theorem 2.1 and latter is isomorphic to $\mathbb{Z}/p\mathbb{Z}$, So we may choose $\mathcal{C} = \{0, 1, \cdots, p-1\}$ as a complete system of representatives of residue field of $\hat{v_p}$. Therefore in view of Theorem 2.9, every $x \in \mathbb{Q}_p$ can be uniquely written as $\sum\limits_{i>>-\infty} a_i p^i$ where $0 \leq a_i \leq p-1$ for each i. A $p - adic$ integer can be uniquely written as $\sum\limits_{i=0}^{\infty} a_i p^i, 0 \leq a_i \leq p-1$ for each i.*

Example *(1)* $3 - adic$ *expansion of* -1

$-1 \equiv a_o (mod\ 3) \Rightarrow a_o = 2$

$\frac{-1-a_o}{3} \equiv a_1 (mod\ 3) \Rightarrow -1 \equiv a_1 (mod\ 3) \Rightarrow a_1 = 2.$

$\frac{-1-a_1}{3} \equiv a_2 (mod\ 3) \Rightarrow -1 \equiv a_2 (mod\ 3) \Rightarrow a_2 = 2.$

$\therefore -1 = 2 + 2.3 + 2.3^2 + 2.3^3 + \cdots$

Indeed the sum of series on R.H.S. is

$$2(1 + 3 + 3^2 + \cdots) = \frac{2}{1-3} = -1$$

(2) $3-$ *adic expansion of* $\frac{1}{5}$

$\frac{1}{5} \equiv a_o(mod\ 3) \Rightarrow a_o = 2$

$\frac{1/5 - a_o}{3} \equiv a_1(mod\ 3) \Rightarrow \frac{-3}{5} \equiv a_1(mod\ 3) \Rightarrow a_1 = 0$

$\frac{\frac{-3}{5}}{3} \equiv a_2(mod\ 3) i.e.,\ \frac{-1}{5} \equiv a_2(mod\ 3) \Rightarrow a_2 = 1$

$\frac{\frac{-1}{5} - 1}{3} \equiv a_3(mod\ 3)\ i.e.\ \frac{-2}{5} \equiv a_3(mod\ 3) \Rightarrow a_3 = 2$

$\frac{\frac{-2}{5} - 2}{3} \equiv a_4(mod\ 3)\ i.e.,\ \frac{-4}{5}(mod\ 3) \Rightarrow a_4 = 1$

$\frac{\frac{-4}{5} - 1}{3} \equiv a_5(mod\ 3)\ i.e., \frac{-3}{5} \equiv a_5(mod\ 3) \Rightarrow a_5 = 0, a_6 = 1, a_7 = 2, a_8 = 1, \cdots$

So, $\frac{1}{5} = 2 + 0 \times 3 + 1 \times 3^2 + 2 \times 3^3 + 1 \times 3^4 + 0 \times 3^5 + \cdots$

$$= 2 + (0 + 9 + 54 + 81)(1 + 3^4 + 3^8 + \cdots)$$
$$= 2 + \frac{144}{1 - 3^4} = 2 - \frac{9}{5} = \frac{1}{5}.$$

The following theorem shows that the $p-$ *adic expansion of each rational number is periodic.*

Definition *A* $p-$ *adic Expansion of a* $p-$ *adic integer* $z \in \mathbb{Q}_p$ *is* $z = \sum_{i=0}^{\infty} a_i p^i$ *is said to be finite if* $a_i = 0$ *for all but finitely many* i*, and is said to be* $periodic\ infinte$ *if there exists* $m \geq 0$ *and* $k \geq 1$ *such that* $a_s = a_t$ *where* $s \equiv t\ (mod\ k)$ *for* $s, t \geq m$.

Theorem 2.10 *Let* z *be a non-zero* $p-$ *adic integer. Then*

(1) z *has a finite* $p-$ *adic expansion iff* z *is a natural number.*

(2) z *has a periodic infinite* $p-$ *adic expansion iff* z *is a* $p-$ *adic integer such that* $z \in \mathbb{Q} \setminus \mathbb{N}$.

Proof (1) *Clearly finite* $p-$ *adic expansion has sum equal to a natural number. Conversely, Suppose* $z(\neq 0)$ *be a natural number. We prove by induction. Assume that the result is true for all integers* $y, 0 \leq y < z$*. Let* $k \geq 0$ *be such that* $p^k \leq z < p^{k+1}$ *then* $z = a_k p^k + y$ *where* $1 \leq a_k \leq p-1$ *and* $0 \leq y < p^k$*. By induction hypothesis,*

$y = a_{k-1}p^{k-1} + \cdots + a_1 p + a_o$ with $0 \leq a_i \leq p-1$. Thus z has finite $p-$adic expansion.

Proof (2) *Suppose that $p-$adic integer z has periodic infinite series $\sum_{i=0}^{\infty} a_i p^i$ say $\exists\ m \geq 0$ and $k \geq 1$ such that $a_s = a_t$ where $s \equiv t(mod\ k)$ for $s, t \geq\ m$. Let $c = \sum_{i=0}^{m-1} a_i p^i,\ b = \sum_{i=m}^{m+k-1} a_i p^i$. So*

$$z = \sum_{i=0}^{\infty} a_i p^i = \sum_{i=0}^{m-1} a_i p^i + \sum_{i=m}^{\infty} a_i p^i.$$

$$z - c = \sum_{i=m}^{\infty} a_i p^i = b + \sum_{i=m+k}^{\infty} a_i p^i$$

$$= b + p^k(\sum_{i=m}^{\infty} a_i p^i) = b + p^k(z-c)$$

i.e.$(z-c)(1-p^k) = b$ and $z = c + \frac{b}{1-p^k} \in \mathbb{Q}$.
We verify that $z \notin \mathbb{N}$. If $z \in \mathbb{Z}$, then $(p^k - 1) \mid\ b$ which is possible only when $a_i = p-1$ for $m \leq i \leq m+k-1$. In this situation $b = p^m(p^k-1)$ and so $z = \sum_{i=0}^{m-1} a_i p^i - p^m < 0$.
Coversely, Suppose $z \in \mathbb{Q} \setminus \mathbb{N}$. We first show that there exists $m, k \in\ \mathbb{N}$ and $t, u \in \mathbb{Z}$ such that $0 \leq t < p^m,\ 0 \leq u < p^k$ and

$$z = t + \frac{up^m}{(1-p^k)} \tag{2.11}$$

Let $z = \frac{a}{d}$ where $a, d \in \mathbb{Z},\ d > 0$ and $(p, d) = 1$. Hence there exists $k \geq 1$ such that $p^k \equiv 1(mod\ d)$, hence $z = b(p^k - 1)^{-1}$ for some $b \in \mathbb{Z}$. Choose $m \in \mathbb{N}$ such that $-p^m \leq b < p^m$. Since $(p^m, p^k - 1) = 1$, there are $t, u \in \mathbb{Z}$ such that $b = t(p^k-1) - up^m$ and u can be chosen such that $0 \leq u < p^k - 1$ if $z > 0$ and $1 \leq u < p^k$ if $z < 0$. This is possible because we can solve the congruence $Xp^m + b \equiv 0(mod\ p^k - 1)$ with u as desired, say

$$up^m + b = (p^k - 1)t \tag{2.12}$$

We now verify $0 \leq t < p^m$. Consider first the case when $z > 0$. Since $u \leq p^k - 2$ and $b < p^m$, it follows that the L.H.S. of (2.12) is strictly less than $(p^k - 1)p^m$, comparing *with the R.H.S. of (2.12), we see that* $0 \leq t < p^m$. *When* $z < 0, i.e.,$ $b < 0$, *then keeping in mind that* $u \leq p^k - 1$, *we have* $up^m + b < (p^k - 1)p^m$ *and hence (2.12) implies that* $t < p^m$. *Further using the fact* $u \geq 1$ *and* $b \geq -p^m$, *we see that* $up^m + b \geq 0$ *and hence* $t \geq 0$ *by (2.12). Thus* $0 \leq t < p^m$ *in both cases and hence (2.11) is proved. Recall that* $0 \leq u < p^k$, *infact* $u > 0$ *because otherwise* $z \in \mathbb{N}$. *So there exists* $a_o, a_1, \cdots, a_{m+k-1} \in \{0, 1, , \cdots, p-1\}$ *such that* $t = \sum_{i=0}^{m-1} a_i p^i$ *and* $u = \sum_{i=0}^{k-1} a_{m+1} p^i$. $\therefore$

we conclude using (2.11) that $z = t + \frac{up^m}{1-p^k} = \sum_{i=0}^{m-1} a_i p^i + \frac{\sum_{i=0}^{k-1} a_{m+i} p^{m+i}}{1 - p^k}$.

Since $\frac{1}{1-p^k} = \sum_{j=0}^{\infty} (p^k)^i$, *we have* $z = \sum_{i=0}^{m-1} a_i p^i + \sum_{i=0}^{k-1} a_{m+i} p^{m+i} (1 + p^k + p^{2k} + \cdots +)$

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

where for $i,\ j \geq m,\ i \equiv j (mod\, m), a_i = a_j$. □

The proof of the above gives an easy method to write down the $p-adic$ *expansion of a rational number.*

Some Examples

(1) $7 - adic$ *expansion of* -1

$-1 \equiv a_o (mod\ 7) \Rightarrow a_o = 6$

$\frac{-1-a_o}{7} \equiv a_1 (mod\ 7) \Rightarrow a_1 = 6$

$\frac{-1-a_1}{7} \equiv a_2 (mod\ 7) \Rightarrow a_2 = 6$

$\therefore -1 = 6 + 6 \times 7 + 6 \times 7^2 + \cdots$

Indeed the sum of series on

$$R.H.S. = 6 + 6(7 + 7^2 + \cdots)$$

$$= 6 + 6(7)(1 + 7 + 7^2 + \cdots)$$

$$= 6 + \frac{42}{1-7} = 6 + (-7) = -1.$$

(2) $7-$ *adic expansion of* $\frac{3}{5}$

$\frac{3}{5}\equiv a_o(mod\ 7)\Rightarrow a_o=2$

$\frac{\frac{3}{5}-2}{7}\equiv a_1(mod\ 7)\Rightarrow \frac{-1}{5}\equiv a_1(mod\ 7)\therefore a_1=4$

$\frac{\frac{-1}{5}-a_1}{7}\equiv a_2(mod\ 7)\Rightarrow \frac{-3}{5}\equiv a_2(mod\ 7),\ \therefore a_2=5$

$\frac{\frac{-3}{5}-a_2}{7}\equiv a_3(mod\ 7)\Rightarrow \frac{-4}{5}\equiv a_3(mod\ 7),\ \therefore a_3=2$

$\frac{\frac{-4}{5}-a_3}{7}\equiv a_4(mod\ 7)\Rightarrow \frac{-2}{5}\equiv a_4(mod\ 7),\ \therefore a_4=1$

$\frac{\frac{-2}{5}-a_4}{7}\equiv a_5(mod\ 7)\Rightarrow \frac{-1}{5}\equiv a_5(mod\ 7),\ \therefore a_5=4$

Similarly $a_6=5,\ a_7=2,\ a_8=1,\cdots$

$\therefore \frac{3}{5}=2+4\times 7+5\times 7^2+2\times 7^3+1\times 7^4+4\times 7^5+5\times 7^6+2\times 7^7+1\times 7^8+\cdots$

$=2+7(4+5\times 7+2\times 7^2+1\times 7^3)+7^5(4+5\times 7+2\times 7^2+1\times 7^3)+7^9(4+5\times 7+2\times 7^2+1\times 7^3)+\cdots$ *Let us cross check the sum of above series; It is*

$$=2+7(4+5\times 7+2\times 7^2+1\times 7^3)(1+7^4+7^8+\cdots)$$

$$=2+7\times 480\times\frac{1}{1-7^4}=2-\frac{7}{5}=\frac{3}{5}.$$

(3) $7-$ *adic expansion of* $\frac{-3}{5}$

$\frac{-3}{5}\equiv a_o(mod\ 7),\therefore a_o=5$

$\frac{\frac{-3}{5}-a_o}{7}\equiv a_1(mod\ 7)\Rightarrow \frac{-4}{5}\equiv a_1(mod\ 7).\therefore a_1=2$

$\frac{\frac{-4}{5}-a_1}{7}\equiv a_2(mod\ 7)\Rightarrow \frac{-2}{5}\equiv a_2(mod\ 7),\therefore a_2=1$

$\frac{\frac{-2}{5}-a_2}{7}\equiv a_3(mod\ 7)\Rightarrow \frac{-1}{5}\equiv a_3(mod\ 7),\therefore a_3=4$

$\frac{\frac{-1}{5}-a_3}{7}\equiv a_4(mod\ 7)\Rightarrow \frac{-3}{5}\equiv a_4(mod\ 7).\therefore a_4=5.$

Similarly $a_5=2,\ a_6=1,\ a_7=4,\cdots$

$\therefore \frac{-3}{5}=5+2.7+1.7^2+4.7^3+5.7^4+2.7^5+1.7^6+4.7^7+\cdots$

Indeed the sum of series on R.H.S. is

$$(5+2\times 7+1\times 7^2+4\times 7^3)(1+7^4+7^8\cdots)=\frac{1440}{1-7^4}=\frac{-3}{5}.$$

2.5 Hensel's Lemma and its applications

In 1904, *Hensel proved a remarkable result which shows that under certain condition, the factorisation of a polynomial $F(x) \in \mathbb{Z}[x]$ modulo a prime p is related to its factorisation over the ring of $p-$ adic integers. We now study this result known as Hensel's Lemma for complete valued fields.*

Theorem 2.11 ***Hensel's Lemma*** *Let (K, v) be a complete valued field, where v is a real valuation with valuation ring $\mathcal{O}_v$ having maximal ideal $\mathcal{M}_v$ and residue field $\bar{K} = \mathcal{O}_v/\mathcal{M}_v$. Let $F(X), G_o(X), H_o(X)$ be polynomials belonging to $\mathcal{O}_v[X]$ satisfying the following conditions:*
(i) $F(X) \equiv G_o(X)H_o(X)(mod\mathcal{M}_v)$
(ii) The leading co-efficient g of $G_o(X)$ is a units of $\mathcal{O}_v$.
(iii) $\bar{G}_o(X)$ and $\bar{H}_o(X)$ are relatively prime in $\bar{K}[X]$
Then there exists polynomials $G(X), H(X) \in O_v[X]$ satisfying the following conditions.
(a) $F(X) = G(X)H(X)$
(b) deg $G(X) =$ deg $G_o(X)$, g is the leading coefficient of $G(X)$
(c) $G(X) \equiv G_o(X), H(X) \equiv H_o(X)$ (mod $\mathcal{M}_v$)

Proof *Let r, s denote respectively the degree of $G_o(X), F(X)$. Then deg $\bar{H}_o(X) \leq s - r$. So there exists a polynomial $h_o(X) \in \mathcal{O}_v[X]$ with deg $h_o(X) \leq s - r$ such that $h_o(X) \equiv H_o(X)$ (mod $\mathcal{M}_v$). Replacing $H_o(X)$ by $h_o(X)$, we may assume without loss of generality that deg$H_o(X) \leq s - r$. Since $\bar{G}_o(X)$ and $\bar{H}_o(X)$ are coprime , $\exists\ C(X), D(X) \in \mathcal{O}_v[X]$ such that*

$$\bar{G}_o(X)\bar{C}(X) + \bar{H}_o(X)\bar{D}(X) = \bar{1}$$

Set

$$\mu = min\{v^x(F - G_oH_o), v^x(G_o(X)C(X) + H_o(X)D(X) - 1)\} \tag{2.13}$$

clearly $\mu > 0$. Choose $z \in \mathcal{O}_v$ such that $0 < v(z) \leq \mu$. Then the polynomial $W_o(X) = z^{-1}(F(X) - G_o(X)H_o(X)) \in \mathcal{O}_v[x]$. We divide the proof into two steps.

Step I *We construct sequences of polynomials $G_i(X), H_i(X), W_i(X) \in \mathcal{O}_v[x]$ satisfying the following three properties for $i = 0, 1, 2, \cdots$*
(I) $degG_i(X) = r$, deg $H_i(X) \leq s - r$, leading coefficient of $G_i(X)$ is g.
(II) $G_i(X) - G_{i-1}(X) \in z^i\mathcal{O}_v[X], H_i(X) - H_{i-1}(X) \in z^i\mathcal{O}_v[X]$
(III) $F(X) - G_i(X)H_i(X) = z^{i+1}W_i(X)$.
Clearly $G_o(X), H_o(X)$ satisfy (I), (III), for $i = 0$ and condition (II) is void. As induction hypothesis, suppose that there are polynomials, $G_i(X), H_i(X), W_i(X)$ satisfying (I) - (III) for $0 \leq i \leq n-1$. We now construct $G_n(X), H_n(X)$. Since the leading coefficient of $G_o(X)$ is a unit of $\mathcal{O}_v$, by division $\exists$ $Q_n(X), U_n(X) \in \mathcal{O}_v[X]$ with deg $U_n(X) < r$ such that

$$W_{n-1}(X)D(X) = Q_n(X)G_o(X) + U_n(X) \tag{2.14}$$

Let $V_n(X) \in \mathcal{O}_v[X]$ be a polynomial of least degree such that

$$W_{n-1}(X)C(X) + Q_n(X)H_o(X) - V_n(X) \in z\ O_v[X] \tag{2.15}$$

Then leading coefficient of $V_n(X) \notin z\mathcal{O}_v$. We now verify that

$$V_n(X)G_o(X) + U_n(X)H_o(X) - W_{n-1}(X) \in z\mathcal{O}_v[X] \tag{2.16}$$

On substituting for $U_n(X)$ from (2.14), we see that

$$V_n(X)G_o(X) + U_n(X)H_o(X) - W_{n-1}(X)$$

$$= V_n(X)G_o(X) + (W_{n-1}(X)D(X) - Q_n(X)G_o(X))H_o(X) - W_{n-1}(X)$$

$$= W_{n-1}(X)(D(X)H_o(X) - 1) - G_o(X)(Q_n(X)H_o(X) - V_n(X))$$

$$= W_{n-1}(X)(C(X)G_o(X)+D(X)H_o(X)-1)-G_o(X)(W_{n-1}(X)C(X)+D(X)H_o(X)-V_n(X))$$

By choice of $z, C(X)G_o(X) + D(X)H_o(X) - 1 \in z\mathcal{O}_v[x]$; also by view of (2.15),
$W_{n-1}(X)C(X) + Q_n(X)H_o(X) - V_n(X) \in z\mathcal{O}_v[x]$. So (2.16) is verified.
Claim is that $degV_n(X) \leq s - r$. Suppose to the contrary $degV_n(X) > s - r$. Keeping in mind that $degW_{n-1}(X) \leq s$ by induction , the above supposition show that

$$deg(U_n(X)H_o(X) - W_{n-1}(X)) \leq max\{deg(V_n(X)H_o(X), degW_{n-1}(X)\} \leq s < deg(V_n(X)G_o(X))$$

By virtue of (2.16), the above inequality implies that the leading coefficient $(V_n(X)G_o(X)) \in z\mathcal{O}_v$. *As leading coefficient of* G_o *is a unit of* O_v, *we would have leading coefficient* $(V_n) \in z\mathcal{O}_v$, *Which is impossible in view of choice of* $V_n(X)$ *and hence the claim is proved.*

Define polynomials $G_n(X), H_n(X)$ *by*

$$G_n(X) = G_{n-1}(X) + z^n U_n(X), H_n(X) = H_{n-1}(X) + z^n V_n(X) \tag{2.17}$$

Recall that deg $U_n < r$, *also by the claim deg*$V_n \leq s - r$, *so* $G_n(X), H_n(X)$ *satisfy condition (I) ; clearly condition (II) is satisfied. To verify condition (III) write*

$$F(X) - G_n(X)H_n(X) = F(X) - (G_{n-1}(X) + z^n U_n(X))(H_{n-1}(X) + z^n V_n(X))$$

$$= F(X) - G_{n-1}(X)H_{n-1}(X) - z^n(V_n(X)G_{n-1}(X) + U_n(X)H_{n-1}(X)) - z^{2n}U_n(X)V_n(X)$$

Note that $V_n(X)G_{n-1}(X)+U_n(X)H_{n-1}(X)-W_{n-1} \in z\mathcal{O}_v[X]$, *because* $V_n(X)G_o(X)+U_n(X)H_o(X) - W_{n-1}(X) \in z\mathcal{O}_v[X]$ *by (2.16) and* $G_{n-1} - G_o, H_{n-1} - H_o$ *belonging to* $z\mathcal{O}_v[X]$ *in view of condition (II) being satisfied for* $1 \leq i \leq n-1$.

Step II *We show that there exists polynomials* $G(X), H(X)$ *in* $\mathcal{O}_v[X]$ *with the desired properties. Write* $G_i(X) = \sum_{j=0}^{r} g_{ij}X^j, H_i(X) = \sum_{j=0}^{s-r} h_{ij}X^j$, *Since condition (II) is satisfied, the sequences* $(g_{i_o})_{i\in\mathbb{N}}, \cdots, (g_{i_r})_{i\in\mathbb{N}}, (h_{i_o})_{i\in\mathbb{N}}, \cdots, (h_{i_{s-r}})_{i\in\mathbb{N}}$ *are v - Cauchy, hence v - convergent. Let* $g_o, \cdots, g_r, h_o, \cdots, h_{s-r}$ *be their respective v - limits. Set* $G(X) = \sum_{j=0}^{r} g_i(X)^j, H(X) = \sum_{j=0}^{s-r} h_j X^j$. *Clearly* $G(X)$ *has degree r with l.c. g. Since* $G(X) - G_n(X), H(X) - H_n(X), F(X) - G_n(X)H_n(X)$ *as in* $z^n\mathcal{O}_v[X]$ *for any* $n \in \mathbb{N}$, *we have* $F(X) - G(X)H(X) \in \bigcap_{n\in\mathbb{N}} z^n\mathcal{O}_v[X]$. *Hence* $F(X) = G(X)H(X)$ *as desired.* □

The following theorem is an immediate corollary of Hensel's Lemma

Corollary 2.12 *Let* (K, v) *be as in the above theorem. If* $F(X) \in \mathcal{O}_v[X]$ *has a simple zero* $\bar{C}_o$ *in the residue class field* $\bar{K}_v$, *i.e.* , $\bar{F}(\bar{C}_o) = \bar{O}$ *and* $\bar{F}'(\bar{C}_o) \neq \bar{O}$, *then* $F(X)$ *has a zero* $C \in \mathcal{O}_v$ *such that* $\bar{C} = \bar{C}_o$.

We can prove very nice results using Hensel's Lemma.

Theorem 2.13 *If p and q are distinct primes , there exists no isomorphism between the fields $\mathbb{Q}_p, \mathbb{Q}_q$.*

Proof *It is enough to show that there exists a polynomial $h(X) \in \mathbb{Q}[X]$ which is irreducible in $\mathbb{Q}_p[X]$, but reducible in $\mathbb{Q}_q[X]$. Let $r \in \mathbb{Z}$ be an integer such that $r \equiv 0(mod\ p), r \equiv 1(mod\ q)$. Let $h(X) = X^2 + rX + pq$. Using Eisenstein's irreducibility criterion in $\mathbb{Z}_p$, we deduce that $h(X)$ is irreducible in $\mathbb{Q}_p[X]$. Since $X^2 + rX + pq \equiv X^2 + X \equiv X(X+1)$ $(mod\ \mathcal{M}_{v_q})$. By Hensel's lemma in $\mathbb{Q}_q, X^2 + rX + pq$ is reducible in $\mathbb{Q}_q[X]$.* □

Note *For any prime p, there exists no isomorphism between the fields $\mathbb{R}$ and $\mathbb{Q}_p$. Since p is a square in $\mathbb{R}$ but not a square in $\mathbb{Q}_p$.*

Theorem 2.14 *The only endomorphism of $\mathbb{Q}_p$ is the identity.*

Proof *Let $f : \mathbb{Q}_p \to \mathbb{Q}_p$ be an endomorphism , hence $f(r) = r$ for every rational number $r \in \mathbb{Q}$. If $x \in \mathbb{Q}_p$, then we may write $x = \mu p^{v_{p(x)}}$, where $\mu \in \mathbb{Q}_p$ is a unit of the valuation ring $\mathbb{Z}_p$. It follows that $f(x) = f(\mu)p^{v_{p(x)}}$. If we show that $f(u)$ is unit , this mean that $v_p(f(x)) = v_p(x)$ for every $x \in \mathbb{Q}_p$, therefore f is a continuous mapping in the topology defined by the valuation v_p. Since $\mathbb{Q}$ is dense in its completion $\mathbb{Q}_p$ and f is identity on $\mathbb{Q}$, it follows from continuity of f that f is must be identity on $\mathbb{Q}_p$.* □

We still have to show that $f(\mu)$ is unit of $\mathbb{Q}_p$, for every unit μ. For this, we will prove the following theorem.

Theorem 2.15 *$\mu \in \mathbb{Z}_p$ is a unit of $\mathbb{Z}_p$ if and only if there exist infinitely many integers $n > 0$ such that μ^{p-1} has an nth root in $\mathbb{Z}_p$.*

Proof *If there exist an integer $n > 0$ for which μ^{p-1} has an nth root $t \in \mathbb{Q}_p$, then $t^n = \mu^{p-1}$ implies $nv(t) = (p-1)v_p(\mu)$, therefore $(p-1)v_p(\mu)$ is a multiple of n. As it is true for infinitely many integers n, we must have $v_p(\mu) = 0$.*

Conversely, suppose $v_p(\mu) = 0$, then the image of μ in the residue field of v_p

is not zero, but $\mathbb{Z}_p \mid < p > \cong F_p$. So $\bar{\mu}^{p-1} = \bar{1}$. Since $X^n - \mu^{p-1} \equiv X^n - 1 \equiv (X-1)(X^{n-1} + \cdots + X + 1)(mod\ \mathcal{M}_{v_p})$. So, $\mu^{p-1} \equiv 1(mod\ \mathcal{M}_{v_p})$. If n is not a multiple of p, then $\bar{1}$ is not repeated root of $X^n - \bar{1}$. Thus $X - \bar{1}, X^{n-1} + \cdots + X + \bar{1}$ are relatively prime polynomials. Since $\mathbb{Q}_p$ is complete valued field, by Hensel's Lemma , $X^n - \mu^{p-1}$ has a linear factor $X - C \in \mathbb{Z}_p[X]$, so μ^{p-1} has an nth root in $\mathbb{Z}_p$, for every n not a multiple of p.

Thus, it is indeed true that if μ is a unit of $\mathbb{Z}_p$ and f is an isomorphism, then $f(\mu)$ has the same characteristic property of μ and so it is also a unit of $\mathbb{Z}_p$.

Remark *Let $p \geq 3$ be prime. The analogue of **Fermat's Last Theorem** does not hold in $\mathbb{Q}_p$. $\exists\ \alpha, \beta, \gamma \in \mathbb{Q}_q, q \neq p$, not all zero such that $\alpha^p + \beta^p = \gamma^p$. Consider $F(X) = X^p + q^p + (-1)^p$. Then $F(X) = X^p - 1\ mod\ q$. Since 1 is a simple root of $F(X)$ modulo q, by Hensel's Lemma $\exists\ \alpha \in \mathbb{Z}_p$ such that $\alpha^p + q^p + (-1)^p = 0$.*

Hensel's Lemma can also be used to check irreducibility of polynomials over complete valued fields as shown by the following theorem.

Theorem 2.16 *Let (K, v) be complete valued field, where v is a real valuation with valuation ring $\mathcal{O}_v$ having maximal ideal $\mathcal{M}_v$. Let $F(X) = a_oX^n + \cdots + a_n (a_o \neq 0)$ be a polynomial $\in \mathcal{O}_v[X]$ with $a_o \equiv 0(mod\ \mathcal{M}_v)$. If any one of $a_1, \cdots, a_{n-1}$ is unit of $\mathcal{O}_v$, then $F(X)$ is reducible in $\mathcal{O}_v[X]$.*

Proof *Let a_i be the first unit appearing among the co-efficients of $F(X)$. Set $G_o(X) = a_iX^{n-i} + \cdots + a_n, H_o(X) = 1$, then we have $G_o(X), H_o(X) \in \mathcal{O}_v[X]$ and $F(X) - G_o(X)H_o(X) = a_oX^n + \cdots + a_{i-1}X^{n-1+i} \equiv 0(mod\ \mathcal{M}_v)$. Hence by Hensel's Lemma, there exists $G(X), H(X) \in \mathcal{O}_v[X]$ such that*

$$F(X) = G(X)H(X), degG(X) = degG_o(X) = n - i, 0 < n - i < n$$

The polynomial $F(X)$ is therefore reducible in $\mathcal{O}_v[X]$. □

Theorem 2.17 *Let (K, v) be complete valued field and let $f(X) = X^n + a_1X^{n-1} + \cdots + a_n$ be an irreducible polynomial in $K[X]$. If the coefficient a_n belongs to $\mathcal{O}_v$, then all other co-efficients a_i are contained in $\mathcal{O}_v$.*

Proof *Suppose that* $min_{1\leq j\leq n}\{v(a_j)\} = v(a_{j_o}) < 0$ *, then the polynomial*

$$F[X] = a_{j_o}^{-1}(f(X)) = b_oX^n + \cdots + b_n$$

is contained in $\mathcal{O}_v[X]$ *and* $b_o \equiv 0(mod\ \mathcal{M}_v)$. *Since* $a_n \in \mathcal{O}_v, v(b_n) > 0$ *so* $0 < j_o < n$ *, and* $b_{j_o} = 1$. *Since by previous theorem,* $F(X)$ *is reducible in* $\mathcal{O}_v[X]$ *and therefore* $f(X)$ *is reducible in* $K[X]$. *This contradiction proves the theorem.* □

We now prove one of the most important applications of Hensel's Lemma viz. if (K, v) *is a complete valued field, then* v *can be extended to any finite extension of* K*, the uniqueness of extension was already proved in Theorem 1.19.*

Theorem 2.18 *Let* (K, v) *be complete valued field and let* K_1*, be an extension of degree* n. *Then* v *can be extended (uniquely) to a valuation of* K_1*, which is given by* $v_1(\alpha) = \frac{v(N_{K_1|K}(\alpha))}{n}, \alpha \in K_1$.

Proof *For* $\alpha, \beta \in K_1$*, clearly* $v_1(\alpha) = \infty \Leftrightarrow N_{K_1|K}(\alpha) = 0 \Leftrightarrow \alpha = 0$ *and* $v_1(\alpha\beta) = v_1(\alpha) + v_1(\beta)$. *To verify* $v_1(\alpha+\beta) \geq min\{v_1(\alpha), v_1(\beta)\}$ *, we prove that for* $\alpha \in K_1$*, whenever* $v_1(\alpha) \geq 0$ *, then* $v_1(\alpha + 1) \geq 0$. *Suppose* $v_1(\alpha) \geq 0$ *for some element* $\alpha \in K_1$. *Then*

$$v(N_{K_1|K}(\alpha)) \geq 0 \tag{2.18}$$

Let $f(X) = X^n + a_1X^{n-1} + \cdots + a_n$ *be the minimial polynomial of* α *over* K. *Recall that* $N_{K_1|K}(\alpha) = \pm a_n^{[K_1:K(\alpha)]}$. (2.18) $\Longrightarrow v(a_n) \geq 0, \therefore$ *by Theorem 2.17 all* $a_i \in \mathcal{O}_v$. *Now* $f(X-1)$ *is the minimial polynomial of* $\alpha + 1$ *over* K *and the constant term of* $f(X-1)$ *is* $f(-1)$*, so*

$$N_{K_1|K}(\alpha + 1) = \pm(f(-1))^{[K_1:K(\alpha)]}$$

Since $f(X) \in \mathcal{O}_v[X]$, $f(-1) \in \mathcal{O}_v$, $\therefore$ $N_{K_1|K}(\alpha+1) \in \mathcal{O}_v \Rightarrow v_1(\alpha+1) \geq 0$ *as desired.* □

Corollary 2.19 *Let* (K, v) *be a complete valued field with respect to a real valuation* v. *Then* v *can be (uniquely) extended to a valuation* $\widetilde{v}$ *of the algebraic closer* $\widetilde{K}$ *of* K.

Proof *For arbitrary* $\alpha, \beta \in \widetilde{K}$ *, we define* $\widetilde{v}(\alpha) = \frac{v(N_{K(\alpha)|K}(\alpha))}{[K(\alpha):K]}$.
Note that for any finite extension K_1 *of* $K(\alpha)$*,*

$$\widetilde{v}(\alpha) = \frac{v(N_{K_1|K}(\alpha))}{[K_1 : K]}$$

For $\alpha, \beta \in \widetilde{K}$*, we have to verify*

$$\widetilde{v}(\alpha + \beta) \geq min\{\widetilde{v}(\alpha), \widetilde{v}(\beta)\}, \widetilde{v}(\alpha\beta) = \widetilde{v}(\alpha) + \widetilde{v}(\beta)$$

Fix one such pair $\alpha, \beta \in \widetilde{K}$ *and take* $K_1 = K(\alpha, \beta)$ *, then by above theorem* $\widetilde{v}/K_1$ *is valuation of* K_1*. Hence the corollary.* □

Bibliography

[1] S. Iyanaga, The Theory of Numbers, Oxford University Press, North-Holland, 1975.

[2] P. Roquette, *History of Valuation Theory - Part I, Valuation Theory and its Applications Vol-I, Fields Institute Communications, eds. F.-V. Kuhlmann, S. Kuhlmann and M.Marshal, 32 (2002), 291-355.*

[3] K.Iwasawa, Local Class Field Theory, Oxford University Press, New York, Clarendon Press, Oxford, 1986.

[4] P. Ribenboim, *The Theory of classical valuations, Springer Edition, 1998.*

[5] Larsen Max D. and Mc Carthy, Paul J., Multiplicative theory of Ideals, N.Y. Academic Press, 1971.