Analysis and Arithmetic of p-adic Numbers

A thesis submitted to
Indian Institute of Science Education and Research Pune
in partial fulfilment of the requirements for the
Mathematics M.Sc Degree Program
under the supervision of
Dr. Chandrasheel Bhagwat

by
Priyanka Dey
March, 2024

Indian Institute of Science Education and Research Pune
Dr. Homi Bhabha Road, Pashan, Pune India 411008

DECLARATION

I declare that I have written this document from concepts that I have learned from the books mentioned in the bibliography in my own words. I have cited and referenced the original sources of the informations. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. I understand that violation of the above will be cause for disciplinary action by the institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

Dated, Pune
Tuesday, May, 2024

PRIYANKA DEY

This is to certify that this thesis entitled "*Analysis and Arithmetic of p-adic Numbers*" submitted towards the partial fulfilment of the Mathematics M.Sc Degree Program at the Indian Institute of Science Education and Research Pune represents work carried out by *Priyanka Dey* under the supervision of *Dr. Chandrasheel Bhagwat.*

Dr. Chandrasheel Bhagwat
Master's Thesis Supervisor

Prof. Girish Ratnaparkhi
Dean (Academics)

Contents

1 Abstract

"p-adic fields provide rermarkable, easy and natural solutions to problems ,which apparently have no relation to p-adic fields and which otherwise can be resolved, if at all , only by deep and arduous methods".
-J.W.S.CASSELS

p-adic numbers play an important role in modern number theory. They encode important information about congruences between integers. From rational number, one construct the smallest complete field that contains rational numbers for this p-adic number comes.
In this thesis, we study the basic construction of p-adic numbers and p-adic integers.
we saw analytic and algebraic properties of the space of p-adic numbers,Hensel's Lemma,then we derive the abstract theory of valuation on number fields and local fields.

2 Foundations

Absolute values on a Field: A function $|.| : \mathbf{K} \to [0.\infty)$ is called an absolute value on a field $\mathbf{K}$,if for all $x, y \in \mathbf{K}$, it satisfies
1) Definiteness, i.e., $|x| = 0$ iff $x = 0$.
2) Multiplicativity $|xy| = |x|.|y|$.
3)Triangle inequality, i.e., $|x + y| \leq |x| + |y|$.

Examples: *i*) Trivial absolute value on $\mathbf{K}$.

$$|x| = \begin{cases} 1 & \text{if } x \in \mathbf{K}^* \\ 0 & \text{if } x = 0 \end{cases}$$

ii) The usual absolute value on $\mathbb{Q}$.

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x \leq 0 \end{cases}$$

Non-Archimedian Absolute Value
An absolute value on $\mathbf{K}$ is called non-archimedian if $|x + y| \leq \max\{|x|, |y|\} \forall x, y \in \mathbf{K}$.
e.g.,: *i*) Trivial absolute value.
ii) p-adic absolute value. (It will be defined later.)

Proposition: The only absolute value on a finite field $\mathbf{K}$ is a trivial absolute value.

Proof. Suppose,

$$|\cdot| \text{ is an absolute value on } \mathbf{K}$$

.
Then, by definition, $|0| = 0$.
Now,

$$1 = 1.1 \implies |1| = |1|.|1| \implies |1|(|1| - 1) = 0$$

Since $|1| > 0$,

$$|1| = 1$$

Take any nonzero element $x \in K$,
As $\mathbf{K}$ is a finite field,there must exist an integer $\mathbb{Q}$, such that $q = |\mathbf{K}|$, then

$$x^q = x$$

for all $x \in \mathbf{K}$.
Taking absolute value on both sides,

$$|x^q| = |x| \implies |x|^q = |x|$$

As $|x| > 0$ and real

$$\implies |x| = 1$$

$$\therefore |x| = \begin{cases} 1 & \text{if } x \in k^* \\ 0 & \text{if } x = 0 \end{cases}$$

Therefore,

$$|\cdot| \text{ is a trivial absolute value.}$$

□

p-adic valuation

For a fixed prime number p,the p-adic valuation on $\mathbf{Z}$ is a surjective map $v_p : \mathbf{Z} \to \mathbf{Z} \cup \infty$ such that $v_p(0) = \infty$ and for $n \in \mathbf{Z}, n \neq 0$,the p-adic valuation of **n** is defined by $v_p(n)$ such that

$$n = p^{v_p(n)}.n' \text{ where } p \not| n', n' \in \mathbf{Z} - \{0\}$$

If $n = \frac{a}{b} \in \mathbf{Q}^*$, then $n = p^{v_p(n)}.\frac{a'}{b'},\ p \not| a'\ b'$

Or, $v_p(n) = v_p(a) - v_p(b)$.

Remark: The valuation of any rational number is not affected by its representation as quotient of integers.

Examples: $v_5(35) = 1$,$v_3(\frac{126}{12}) = 1$

Lemma: For all $x, y \in \mathbb{Q}$

i)$v_p(xy) = v_p(x) + v_p(y)$

ii)$v_p(x + y) \geq min\{v_p(x), v_p(y)\}$

Proof. Let $x = p^{v_p(x)}.a$ such that $p \not| a$

$y = p^{v_p(y)}.b$ such that $p \not| b$

$$\therefore xy = p^{v_p(x)+v_p(y)}.ab,$$

$$\implies v_p(xy) = v_p(x) + v_p(y)$$

ii)Without loss of generality,
Assume $v_p(x) \leq v_p(y)$.

$$x + y = p^{v_p(x)}a + p^{v_p(y)}b$$
$$= p^{v_p(x)}(a + p^{v_p(y)-v_p(x)}b)$$

$$\implies v_p(x + y) \geq v_p(x)$$

□

p-adic absolute value

For a nonzero $x \in \mathbb{Q}$ we can define the p-adic absolute value of x by

$$|x|_p = p^{-v_p(x)}$$

and $|0|_p = 0$.

e.g.,: $|35|_7 = 7^{-v_7(35)} = \frac{1}{7}$.

Lemma: $|.|_p$ is a non-archimedean Absolute value on $\mathbb{Q}$.

Proof. Definiteness and multiplication follows from the definition.
We need to show that ,

$$|x+y|_p \leq \max\{|x|_p, |y|_p\} \ \forall x, y \in \mathbb{Q}$$

Let, $x = p^m.\frac{a}{b}, y = p^n.\frac{a'}{b'}$
Where a,b,a',b' are coprime to p,
WLOG, $m < n$

$$x + y = p^m(\frac{a}{b} + p^{n-m}\frac{a'}{b'}) = p^m\frac{ab' + p^{n-m}a'b}{bb'}$$

If $|x|_p \neq |y|_p$
Then $n - m > 0$ implies $ab' + p^{n-m}a'b$ is coprime to p

$$|x+y|_p = p^{-m} = max|x|_p, |y|_p$$

If $|x|_p = |y|_p$
Then,

$$ab' + p^{n-m}a'b = ab' + a'b = p^l k$$

for some $l \geq 0$ and K is prime to p

$$\implies |x+y|_p = |p^{m+l}.\frac{k}{bb'}|_p$$
$$= p^{-m-l} \leq max|x|_p, |y|_p$$

□

Theorem: Let **K** be any field with absolute value |.| and ∃ a map $i : \mathbf{Z} \to \mathbf{K}$, If |.| is bounded on $i(\mathbf{Z})$ then |.| is a non archimedean absolute value.

Proof. Lets assume |.| is bounded on $i(\mathbf{Z})$.
which implies $|n| < l \forall n \in \mathbf{Z}$ and $l \in \mathbf{R}_{>0}$.
Choose $x, y \in \mathbf{k}^*$
We need to prove that,

$$|x+y| \leq \max\{|x|, |y|\}$$

$$|x+y|^t = |\sum_{i=0}^{t} \binom{t}{i} x^i y^{t-i}|$$

$$\leq l \sum_{0}^{t} |x^i| \cdot |y^{t-i}|$$

WLOG,

$$|x| \leq |y|$$

Then,

$$|x+y|^t \leq l \sum_{0}^{t} |y^i| \cdot |y^{t-i}| = l \sum_{0}^{t} |y|^t$$

$$\leq l(t+1)|y|^t$$

$$\therefore |x+y| \leq (l(t+1))^{\frac{1}{t}}.|y|$$

As $t \to \infty$

$$|x+y| \leq |y|$$

□

2.1 p-Adic Topology

We can now define a topology on a field **K** by giving a metric.

Lemma: Let $|\cdot|$ be an absolute value on a field **K**, and define a metric $d(x,y) = |x-y|$,then $|\cdot|$ is a non archimedean absolute value iff for any $x, y, z \in \mathbf{K}$, We have,

$$d(x,y) \leq \max\{d(x,y), d(z,y)\}$$

This inequality is called an Ultrametric inequality.
A space which satisfies this inequality is called ultrametric space.

Corollary: Every triangle in this ultrametric space is isosceles.

Proof. Let $x, y,$ and z be the vertices of a triangle in an ultrametric space.
$\therefore$ Length of each sides are,

$$d(x,y) = |x-y|, d(y,z) = |y-z|, d(x,z) = |x-z|$$

Since,

$$(x-y)+(y-z) = (x-z)$$

If $|x-y| \neq |y-z|$
Then, by ultrametric inequality,

$$|(x-y)+(y-z)| = \max\{|x-y|, |y-z|\} = |x-z|$$

i.e., $|x-z|$ is equal to the bigger one of $|x-y|$ and$\|y-z|$.
$\implies$ At least two of the sides are always equal.

□

So, in this context, we can see that p-adic absolute values give a topology on $\mathbb{Q}$, and with this p-adic topology $\mathbb{Q}$, becomes an ultrametric space.
In ultrametric space, open balls and closed balls behave differently than in the usual metric. In ultrametric space the following holds,

1) Every point of an open (resp.closed) ball is the center of that ball.

2) Any two open(resp. closed) balls are totally disjoint,or one is contained in the other.

2.2 Algebra of Non-Archimedean Absolute Value

Now we will see the algebraic point of view of a field **K** through its absolute value.

Definition: Suppose |.| is a non-archimedean absolute value on a field **K**. Then,we will get the valuation ring defined by

$$O = \overline{B(0,1)} = \{x \in \mathbf{K} : |x| \leq 1\} \subset \mathbf{K}$$

and valuation ideal defined by,

$$\wp = B(0,1) = \{x \in \mathbf{K} : |x| < 1\} \subset O$$

,which is the unique maximal ideal of O.
and

$$k = \frac{O}{\wp}$$

is called residue field of **K** w.r.t |.|.

Proof. Here, $0, 1 \in O$. If $x, y \in O$ then,
$|x + y| \leq \max\{|x|, |y|\} \leq 1$
$\therefore x + y \in O$.
Since

$$|xy| = |x|.|y| \implies |xy| \leq 1$$

Hence, $xy \in O$.
And for all x *in* **K** either $x \in O$ or $x^{-1} \in O$.
Therefore O is a valuation ring.
To show $\wp$ is an ideal, let $x \in O$ and $y \in \wp$
i.e $|x| \leq 1$ and $|y| < 1$
then,

$$|xy| = |x|.|y| < 1 \implies xy \in \wp$$

$\therefore \wp$ is an ideal of O.
Now, if $x \in O$ but $x \notin \wp$ i.e $|x| = 1$ then $|1/x| = 1 \implies 1/x \in O$ i.e $x \in O/\wp$ then $x^{-1} \in O$
let, $a \neq 0$ is an ideal of O such that,

$$\wp \subset a \subseteq O$$

then a will contain such x whuch is an invertible element of O .
$1 \in a$
Hence $a = O$
Therefore, $\wp$ is unique maximal ideal of O. □

For the case $\mathbf{K} = \mathbb{Q}$ with p-adic absolute value
$i)\mathbf{O} = \mathbf{Z_{(p)}} = \{\frac{\mathbf{a}}{\mathbf{b}} \in \mathbb{Q} : \mathbf{p} \not| \mathbf{b}\}$
$ii)\wp = p\mathbf{Z_{(p)}}$
$iii)k = \frac{\mathbf{Z_{(p)}}}{p\mathbf{Z_{(p)}}}$

2.3 Equivalence condition for Absolute values

Let ,$|.|_1$ and $|.|_2$ are two absolute values on $\mathbf{K}$, Then they are equivalent if $\forall\ x \in \mathbf{K}\ \exists$ a positive real number α such that,

$$|x|_1 = |x|_2^{\alpha}$$

There are some equivalent conditions for equivalent absolute values like
For any $x \in \mathbf{K}$ we have $|x|_1 < 1$ iff $|x|_2 < 1$

Theorem: Two absolute values are equivalent iff they induce same topology.

Proof. Forward implication is pretty easy i.e., if $|.|_1 \approx |.|_2$. Then,

$$|x|_1 = |x|_2^{\alpha}$$
$$\implies |x|_1 \to 0 \Leftrightarrow |x|_2 \to 0$$

$\Rightarrow$ Two topologies define same open sets.
$\Rightarrow$ Two topologies are same.
Conversely,Suppose $|.|_1$ and $|.|_2$ induces same topology on $\mathbf{K}$,
Let $x \in \mathbf{K}^*$,such that $|x|_1 > 1$
$\Rightarrow |x^{-1}|_1 < 1$
Let,$x^{-1} = y$

$$\therefore |y^n|_1 = |y|_1^n \to 0$$

as $n \to \infty \implies |y|_2 < 1$
$\implies |x|_2 > 1$
$\implies \{x \in \mathbf{K} : |x|_1 > 1\} \subset \{x \in \mathbf{K} : |x|_2 > 1\}$
$\implies |.|_1 \approx |.|_2$

□

Corollary: For two different primes p and q , $|.|_p$ and $|.|_q$ are always non-equivalent absolute values.

Proof. Let $x \in \mathbb{Q}$ with $|x|_p \neq 1$ such that

$$|x|_p = |x|_q^{\alpha}$$

$$\implies p^{-v_p(x)} = (q^{-v_q(x)})^{\alpha}$$

$$\implies p^{v_p(x)} = (q^{\alpha v_q(x)})$$

But p and q both are primes,
So it contradicts unique prime factorization of x. □

Remark Two equivalent absolute value either both are archimedean or both non archimedean.

Now, we can find all absolute values on $\mathbb{Q}$ and give a relation between them by following theorem given by Ostrowski in 1916.

Theorem 1. *Every non-trivial absolute value on* $\mathbf{Q}$ *is equivalent to either Euclidean absolute value or any p-adic absolute value.*

Product Formula
For every $m \in \mathbf{Q}^*$,we have,

$$\prod_{p \leq \infty} |m|_p = 1$$

Product runs over all prime number p and $|\cdot|_\infty$,

Proof. By the fundamental theorem of arithmetic, m can be written as,

$$m = \pm p_1^{a_1}.p_2^{a_2}....p_k^{a_k}$$

where $p_i's$ are prime numbers. Then,

$$|m|_q = 1 \text{ for } q \neq p_i$$

$$|m|_\infty = p_1^{a_1}.p_2^{a_2}....p_k^{a_k}$$

$$|m|_{p_i} = p_i^{-a_i}$$

Therefore

$$\prod_{p \leq \infty} |m|_p = (\prod_{j=1}^{k} p^{-a_i}).p_1^{a_1}.p_2^{a_2}....p_k^{a_k} = 1$$

□

2.4 Completion of Q

To see the completion of $\mathbb{Q}$,first go to a cauchy sequence

$$x_n = 1 + \frac{1}{2!} + ... + \frac{1}{n!}$$

We saw in real analysis that this sequence $\{x_n\}$ converges to e which is a irrational . So, $\mathbb{Q}$ is not complete with its usual absolute value.

In the usual absolute value case, $\lim_{n\to\infty} |x_{n+1} - x_n| = 0$ does not imply $\{x_n\}$ is cauchy.
For example ,take

$$x_n = 1 + \frac{1}{2} + ... + \frac{1}{n}$$

in $\mathbf{R}$
see,
$\lim_{n\to\infty} |x_{n+1} - x_n| = |\frac{1}{n+1}| \to 0$
But ,
$\{x_n\}$ is not a cauchy sequence. Let's see why.
Let, $m \in \mathbf{N}$, then,

$$|x_{n+m} - x_n| = \frac{1}{n+1} + \frac{1}{n+2} + ... + \frac{1}{n+m}$$

Choose, $n = m$.

$$\therefore |x_{2n} - x_n| = \frac{1}{n+1} + \frac{1}{n+2} + ... + \frac{1}{2n}$$

$$> \frac{1}{2n} + \frac{1}{2n} + ... + \frac{1}{2n} = \frac{1}{2}$$

So, for $\epsilon = \frac{1}{2} \nexists$ any $k \in \mathbf{N}$ such that,

$$|x_{n+m} - x_n| < \epsilon \ \forall n \geq k, m \in \mathbb{N}$$

Therefore , x_n does not satisfy the cauchy criterion.
So, x_n is not cauchy.

But in non-archimedean absolute value case, it is enough to show that , $\lim_{n\to\infty} |x_{n+1} - x_n| = 0$ to prove $\{x_n\}$ is cauchy in $\mathbf{k}$.
Let's see why.
If $\{x_n\}$ is cauchy sequence in $\mathbf{K}$ then by definition of Cauchy sequence ,for each $\epsilon > 0$ $\exists$ $\mathbf{K} \in \mathbf{N}$ such that

$$|x_m - x_n| < \epsilon \text{ for } m, n \geq \mathbf{K}.$$

taking $m = n + 1$,

$$|x_{n+1} - x_n| \to 0 \text{ as } n \to \infty$$

Conversely, if , $\lim_{n\to\infty} |x_{n+1} - x_n| = 0$
place $m = n + p$

$$|x_m - x_n| = |x_{n+p} - x_n|$$

$$= |x_{n+p} - x_{n+p-1} + x_{n+p-1} - x_{n+p-2} + ... + x_{n+1} - x_n|$$

$$\leq \max \{|x_{n+p} - x_{n+p-1}|, |x_{n+p-1} - x_{n+p-2}|, ...|x_{n+1} - x_n|\}$$

But each $|x_{n+p-i} - x_{n+p-(i-1)}| < \epsilon_j$ for each $0 \leq i \leq p - 1$.
Take ϵ as max, $\{\epsilon_i\}$

$$\therefore |x_m - x_n| < \epsilon \ \forall \ m, n \geq n$$

$\therefore$ $\{x_n\}$ is a cauchy sequence in $\mathbf{K}$.

In the above,we saw that $\mathbb{Q}$ is not a complete field with reference to usual absolute value .
Ostrowski said that ,every nonzero absolute value in $\mathbb{Q}$ is either equivalent to the usual absolute value or any nonzero p-adic absolute value.

Ergo, to show that $\mathbb{Q}$ is not complete w.r.t any of its non-trivial absolute values it's enough to prove for p-adic absolute value.

For the non-completeness of $\mathbb{Q}$ with respect to p-adic absolute value,Let give a counterexample, i.e., a sequence in $\mathbb{Q}$ that is cauchy but does not converge in $\mathbb{Q}$. w.r.t the p-adiq absolute value.

Counter Example
Take a sequence $\{x_n\}$ in $\mathbb{Q}$ such that $x_n = r^{p^n}$. where $1 < r < p - 1$

$$|x_{n+1} - x_n| = |r^{p^{n+1}} - r^{p^n}| = r^{p^n}(r^{p^n(p-1)} - 1)$$

By Fermet's theorem,

$$r^{p^n(p-1)} - 1 \equiv 0(mod\ p^n)$$

So,

$$|x_{n+1} - x_n| \leq p^{-n} \to 0 \text{ as } n \to \infty$$

$\therefore \{x_n\}$ is a cauchy sequence in $\mathbb{Q}$ w.r.t $|.|_p$.
Now , for the contradiction, suppose $\{x_n\}$ converges to x in $\mathbb{Q}$.

$$x = \lim_{n\to\infty} x_n$$

$$\implies lim|x_n|_p = |x|_p$$

$\therefore \forall n, p \not| r^{p^n} \implies |x_n|_p = 1 \implies |x|_p = 1$
It shows that $x \neq 0$
Now using the definition of convergence of a sequence,

$$x = \lim_{n\to\infty} x_n$$

$$= \lim_{n\to\infty} x_{n+1}$$

$$= \lim_{n\to\infty} (x_n)^p$$

$$= (\lim_{n\to\infty} x_n)^p$$

$$= x^p$$

$\therefore x^p = x \implies x^{p-1} = 1.$(since $x \neq 0$)
But $x = 1$ or $x = -1$ are the only solutions in $\mathbb{Q}$.
So,

$$0 < a - x < p \implies p \not| a - x \implies |a - x|_p = 1$$

Since,

$$\{x_n\} \to \text{ as } n \to \infty$$

$\therefore \exists\ n \in \mathbf{N}$ such that

$$|x_n - x|_p < |x - a|_p \forall n > N$$

$$|a^{p^n} - x|_p < |x - a|_p$$

Now,

$$|x - a|_p = |x - a^{p^n} + a^{p^n} - a|_p$$

$$\leq max\{|x - a^{p^n}|_p, |a^{p^n} - a|_p\}$$

But,

$$|x - a^{p^n}|_P < |x - a|_p$$

$$\therefore |x - a| = |a^{p^n} - a|$$

$$\therefore |x-a|_p = |a|_p|a^{p^n}-1| = |a^{p^{n-1}}-1| < 1$$

This contradicts $|x-a|_p = 1$.
$\therefore \{x_n\}$ does not converge in $\mathbb{Q}$ w.r.t $|.|_p$.

2.5 Analytical Way to Construct $\mathbf{Q_p}$

From now on, we will try to find the completion of $\mathbb{Q}$. For that, collect all the cauchy sequences in $\mathbb{Q}$ w.r.t $|.|_p$ and denote as c i.e.,,

$c = c_p(\mathbb{Q}) = \{(x_n) : (x_n)$ is cauchy seqence in $\mathbb{Q}$ w.r.t$|.|_p\}$
$(c, +, .)$ forms a commutative ring with unity as $(1, 1, ...1)$ with operation defined as,

$$(x_n) + (y_n) = (x_n + y_n)$$

$$(x_n).(y_n) = (x_n.y_n)$$

Theorem 2. *Let, a cauchy sequence (g_n) and an arbitrary sequence (h_n) in $\mathbb{Q}$ such that, $\lim_{n\to\infty} |g_n - h_n|_p = 0$ then h_n is also a cauchy sequence . Further if $(g_n) \to a$ then $(h_n) \to a$.*

Proof.

$$|h_n - h_m| = |h_n - g_n + g_n - g_m + g_m - h_m|$$

$$\leq \max\{|h_n - g_n|, |g_n - g_m|, |g_m - h_m|$$

Since (g_n) is cauchy sequence.
Then,for every ϵ $\exists$ a $N \in \mathbf{N}$ such that,

$$|(g_n) - (g_m)| < \epsilon \forall m, n \geq N$$

and $\lim_{n\to\infty} |(g_n) - (h_n)| = 0$
hence,

$$|h_n - h_m| < \epsilon \forall m, n > N$$

$\therefore y_n$ is a cauchy sequence.
Now, for the next part,

Given $(g_n) \to a$ as $n \to \infty$

$$|h_n - a| = |h_n - g_n + g_n - a|$$

$$\leq \{h_n - g_n|, |g_n - a|\}$$

by similar way, we can find N and ϵ for which

$$|h_n - a| < \epsilon \forall n > \mathbf{N}$$

$\therefore \{h_n\} \to a$ □

Remark: There exists an injective ring homomorphism for $\mathbb{Q}$ in C via $x \to (x, x, x, ...)$.

Maximal ideal of C: Let us collect all sequences in C that are tend to zero in $\mathbb{Q}$ with respect to $|.|_p$ and denoted as M, defined by,

$$N = (x_n) : x_n \to 0$$

Lemma: M is a maximal ideal of C.
I am giving an outline for the proof.

Proof. **1st step:** Take a sequence $(g_n) \in C$ such that $(g_n) \notin M$ and Create an ideal G,generated by (g_n), in C.

Claim: $G = C$.
Enough to show the identity element $\tilde{1} = (1, 1, 1, , ,)$ of C contains G.

2nd step: Since $(g_n) \not\to 0$ and (g_n) is a cauchy sequence,then $\exists c > 0, N \in \mathbf{N}$ such that $|g_n| \geq c > 0$ when $n \geq \mathbf{N}$
$\therefore$ We can define a new sequence by,

$$h_n = \begin{cases} \frac{1}{g_n} & \text{for } n \geq N \\ 0 & \text{for } n < N \end{cases}$$

3rd step: check h_n is cauchy sequence.
so,

$$h_n \in C$$

4th step: see,

$$g_n.h_n = \begin{cases} 0 & \text{if } n < N \\ 1 & \text{if } n \geq N \end{cases}$$

So in this sequence $\{g_n.h_n\}$ only finite terms are 0 and the rest are 1's.
If we substruct $\{g_n\}.\{h_n\}$ from the constant sequence $\tilde{1}$,then it will go to 0 , it means,

$$\tilde{1} - g_n h_n \to 0$$
$$\implies \tilde{1} - g_n h_n \in N$$

$\therefore \tilde{1}$ can be written as multiple of g_n with the sum of an element of M.
$\implies \tilde{1} \in G$
Hence, $\implies G = C$ $\therefore$ M is a maximal ideal of C. □

Now ,if we quotient out the ring C by its maximal ideal M,then it gives a field,this field is known as $\mathbb{Q}_p$, or field of p-adic numbers. i.e.,,

$$\mathbb{Q}_p = \frac{C}{M}$$

We can define absolute value in $\mathbb{Q}_p$ by,

$$||\cdot|| : \mathbb{Q}_p \mapsto \mathbf{R_{>0}}$$

if $\lambda \in \mathbb{Q}_p$, where $\lambda = a_n,$ where $a_n \in \mathbb{Q}$ such that,

$$||\lambda||_p = \lim_{n\to\infty} |a_n|_p$$

$\exists$ an inclusion of $\mathbb{Q}$ to $\mathbf{Q_P}$ via,

$$i : \mathbb{Q} \mapsto \mathbf{Q_p}$$

such that,

$$a \mapsto (a, a, a, ...)$$

Theorem 3. *Image of $\mathbb{Q}$ under the map i, i.e., $i(\mathbf{Q})$ is dense in $\mathbf{Q_p}$.*

Proof. We have to prove that ,every open ball around $\lambda \in \mathbf{Q_p}$ contains a element of $i(\mathbf{Q})$.
Let us choose an open ball around λ with radius ϵ i.e., $B(\lambda, \epsilon)$.
Let, $\lambda = \{x_n\}$ then by definition of cauchy sequence $\exists N \in \mathbf{N}$,
So, $\exists\ \epsilon'$ with ,$0 < \epsilon' < \epsilon$ such that,

$$|x_n - x_m|_p < \epsilon'$$

for all $n, m \geq N$
Let, $y = x_n$ and $i(y) = \tilde{y} = (x_N, x_N, ...)$

Claim: $\tilde{y} \in B(\lambda, \epsilon)$
Here, $\lambda - \tilde{y}$ is represented by $(x_n - y)$.
$\therefore |x_n - y|_p = \lim\limits_{n\to\infty} |x_n - y|_p$
But, when $n \geq N$,

$$|(x_n - y)|_p = |x_n - x_N|_p < \epsilon'$$

So by taking limit ,

$$\lim_{n\to\infty} |(x_n - y)|_p \leq \epsilon' < \epsilon$$

$\therefore (y) = \tilde{y} \in B(\lambda, \epsilon)$. □

Theorem 4. $\mathbf{Q_p}$ *is a complete field with respect to* $|.|_p$.

Proof. Suppose,$\lambda_1, \lambda_2, ..., \lambda_n$ be a cauchy sequence of elements of $\mathbf{Q_P}$.
where, $\lambda_i = (x_k^i)$ cauchy sequence in $\mathbb{Q}$ up to equivalence,
Since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$,
$\therefore$ for each i, $y_i \in \mathbb{Q}$.
The constant sequence $\tilde{y_i} = (y_i, y_i, , ,)$ close to λ_i
i.e.,,

$$|\lambda_i - \tilde{y_i}|_p < \epsilon$$

$$\lim_{n\to\infty} |\lambda_n - y_n|_p = 0$$

Now, by the previous Theorem 1, since λ_n is a cauchy sequence ,
$\therefore y_n$ is also a cauchy sequence in $\mathbb{Q}$.
say, λ represent y_n
$\therefore \lambda = (y_n)$ is a cauchy sequence,

$$\implies |y_n - y_m| < \epsilon\ \forall n, m \geq N$$

Now,

$$\lambda - \tilde{y_n} = y_m - y_n$$

$$|\lambda - \tilde{y}_n|_p = \lim_{n\to\infty} |y_m - y_n|_P < \epsilon$$

$\therefore \lambda - (\tilde{y_n})$ converge to 0 in $\mathbf{Q_P}$.
$\therefore (\tilde{y_n}) \longrightarrow (y_n)$
Now, $|\lambda_n - \tilde{y_n}| \longrightarrow 0$
Since, $\tilde{y_n} \to \lambda$
Again , by Theorem 1,

$$\therefore \lambda_n \to \lambda$$

Hence, every cauchy sequence converges in $\mathbf{Q_p}$.
Therefore,$\mathbf{Q_p}$ is complete field w.r.t $|.|_p$. □

2.6 p-adic integrs

The ring of p-adic integers is the subring of p-adic numbers $\mathbf{Q_p}$ defined by,

$$\mathbf{Z_p} = \{x \in \mathbf{Q_p} : |x|_p \leq 1\}$$

Since, $\mathbf{Z_p}$ is a closed unit ball ,i.e., a closed set , each convergent sequence in $\mathbf{Z_p}$ has limit in $\mathbf{Z_p}$. As, $\mathbf{Q_p}$ is a complete ring and $\mathbf{Z_p}$ is its subring ,
So, every cauchy sequence in $\mathbf{Z_p}$ converges.
Hence, $\mathbf{Z_p}$ is a complete metric space as well as open set.

Theorem 5. $\mathbf{Z_p}$ *is the closure of* $\mathbf{Z}$ *with respect to* $|.|_p$ *in* $\mathbf{Q_p}$.

Proof. Let choose a cauchy sequence $\{x_n\}$ in $\mathbf{Z}$ which converges to x. i.e.,,

$$\lim_{n\to\infty} \{x_n\} = x$$

If, $|x_n| \leq 1 \implies |x| \leq 1 \therefore x \in \mathbf{Z_p}$.
Conversely, let $x \in \mathbf{Z_p}$ with,

$$\lim_{n\to\infty} \{x_n\} = x$$

where $\{x_n\}$ is cauchy sequence in $\mathbb{Q}$.
Then $\exists$ a $n_0 \in \mathbf{N}$ such that,

$$|x|_p = |x_n|_p \ \forall \ n \geq n_0$$

which means, $x_n = \frac{r_n}{m_n}$ with $r_n, m_n \in \mathbf{Z}, (m_n, p) = 1$
Now , for each $n \geq n_0$ choose a solution $a_n \in \mathbf{Z}$ of the congruence $m_n a_n \equiv r_n \mathrm{mod} p^n$
Then, $|x_n - a_n| \leq \frac{1}{p^n}$
Hence, $x = \lim_{n\to\infty} a_n$
Therefore, x belongs to the closure of $\mathbf{Z}$. □

Units of $\mathbf{Z_p}$ are,

$$\mathbf{Z_p}^* = \{x \in \mathbf{Z_p} : |x|_p = 1\}$$

Every element of $\mathbf{Q_p}^*$ can be written as uniquely as $x = p^n.u$ with $n \in \mathbf{Z}$ and u is a unit element of $\mathbf{Z_p^*}$.

Proposition: In the ring $\mathbf{Z_p}$ nonzero ideals are $p^n\mathbf{Z} = \{x \in \mathbf{Q_p} : v_p(x) \geq n\}$ where $n \in \mathbf{N}$ and also

$$\frac{\mathbf{Z_p}}{p^n\mathbf{Z_p}} \cong \frac{\mathbf{Z}}{p^n\mathbf{Z}}$$

Proof. Let choose a nonzero ideal of $\mathbf{Z_p}$,say $\mathbf{a}$ and an element x from $\mathbf{a}$
Since ,
$|x|_p \leq 1$ then there must exist a $m \geq 0$ such that $m = \min\{v_p(x) : x \in \alpha \text{ and } x \neq 0\}$, then,
$x = p^m.u$ where $u \in \mathbf{Z_p}^*$

Claim: $\mathbf{a} = p^m\mathbf{Z_p}$
If there exists another element y of $\mathbf{a}$ with,
$y = p^n.u^{'}$ where $u \in \mathbf{Z_p}^*$

$$\implies y = (p^{n-m}.u^{'})p^m$$

since $n \geq m$
$\implies y \in p^m\mathbf{Z_p}$
Therefore, $\mathbf{a} = p^m\mathbf{Z_p}$
For further part, use the homomorphism,

$$\phi : \mathbf{Z} \longmapsto \frac{\mathbf{Z_p}}{p^n\mathbf{Z_p}}$$

$$a \longmapsto a \bmod p^n\mathbf{Z_p}$$

$\therefore \ker(\phi) = p^n\mathbf{Z_p}$
for surjectivity, since $\mathbf{Z}$ is dense in $\mathbf{Z_p}$.
Then, for $x \in \mathbf{Z_p}$ there exists an $a \in \mathbf{Z}$ such that,

$$|x - a|_p \leq \frac{1}{p^n}$$

$$\implies v_p(x - a) \geq n$$

$$\implies x - a \in p^n\mathbf{Z_p}$$

$$\therefore x \equiv a \bmod p^n\mathbf{Z_p}$$

So, ϕ is a surjective homomorphism with kernel $p^n\mathbf{Z_p}$,

$$\therefore \frac{\mathbf{Z_p}}{p^n\mathbf{Z_p}} \cong \frac{\mathbf{Z}}{p^n\mathbf{Z}}$$

□

Remark: $\mathbf{Q_p}$ is totally disconnected Hausdorff topological space.

3 Hensel's Lemma

Theorem 6. *Suppose $F(x)$ be a polynomial in $\mathbf{Z_p}[x]$, If there exists a $\alpha_1 \in \mathbf{Z_p}$ of $F(x)$ such that,*

$$F(\alpha_1) \equiv 0 \ mod \ (p\mathbf{Z_p})$$

and,

$$F'(\alpha_1) \not\equiv 0 \ mod \ ((p\mathbf{Z_p})$$

Then there exists a unique $\alpha \in \mathbf{Z_p}$ such that,

$$\alpha \equiv \alpha_1 \ mod \ (p\mathbf{Z_p})$$

with $F(\alpha) = 0$.

Proof. To prove this theorem , we will create a sequence of p-adic integers $\alpha_1, \alpha_2, ...\alpha_n, ...$ such that

$$F(\alpha_n) \equiv 0 \bmod p^n$$

for every $n \in \mathbf{N}$
and

$$\alpha_{n+1} \equiv \alpha_n \bmod p^n$$

Then this sequence is cauchy and it will coverges to α such that, $\alpha \equiv \alpha_1 \ (modp)$ and $F(\alpha) = 0$
So, let α_1 exists, we need to show α_2 exists in such way,

$$\alpha_2 = \alpha_1 + b_1 p$$

for a $b_1 \in \mathbf{Z_p}$
put this value α_2 in $F(x)$

$$\therefore F(\alpha_2) = F(\alpha_1 + b_1 p)$$

expanding this,

$$F(\alpha_2) = F(\alpha_1) + F'(\alpha_1).b_1 p + \text{ terms of } p^n$$

$$\equiv F(\alpha_1) + F'(\alpha_1).b_1 p \bmod p^2$$

To prove the existence of α_2 it is enough to find b_1 such that,

$$F(\alpha_1) + F'(\alpha_1).b_1 p \equiv 0 \bmod p^2$$

Using

$$F(\alpha_1) \equiv 0 \bmod \text{p}$$

$$\implies F(\alpha_1) = px$$

for an x.

$$\therefore px + F'(\alpha_1).b_1 p \equiv 0 \bmod p^2$$

$$\implies x + F'(\alpha_1).b_1 \equiv 0 \bmod p$$

Since, $p \not| F'(\alpha_1)$, it has a inverse in $\mathbf{Z_p}$

$$\therefore b_1 \equiv -x(F'(\alpha_1))^{-1}$$

For such unique b_1 in $\mathbf{Z}$ with $0 \leq b_1 \leq p-1$ we can set $\alpha_2 = \alpha_1 + b_1 p$

In a similar way, we can construct α_{n+1} from α_n,which gives me the whole sequence converging to α, which proved the theorem.

□

[Con15] **Example:** Let,

$$f(x) = x^2 + 1, \text{ then } f(2) \equiv 0(mod 5)$$

But,

$$f'(2) \not\equiv 0(mod 5)$$

It means, $f(x)$ has a root in $\frac{\mathbf{Z}}{5\mathbf{Z}}$ then, by Hensel's lemma,it has a lift, i.e., a root in $\mathbf{Z_p}$.

The Hensel lemma is similar to what we did to find a root in real analysis by Newton Raphson method.
There is another version of Hensel's lemma, which says,
Suppose, $f(x) = a_0 + a_1 x + ... + a_n x^n$, where $a_i' s \in \mathbf{Z_p}$
If there exists a $\alpha_1 \in \mathbf{Z_p}$ then for each $n \geq 1$,

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

define a convergent sequence which converges to a unique $\alpha_1 \in \mathbf{Z_P}$ such that $|\alpha - \alpha_1| < 1$ and $f(\alpha) = 0$.

Remark: Without the condition $f'(\alpha) \equiv 0 \ (mod\ p)$ this theorem does not hold.
See an example,

$$f(x) \equiv x^2 - 3(mod\ 2)$$

here,

$$f(1) \equiv 0(mod\ 2)$$

but $f'(1) \equiv 0(mod\ 2)$
so,

$$x^2 - 3$$

does not have any roots in $\mathbf{Q_2}$.

Advanced version of Hensel's lemma
Let $f(x) \in \mathbf{Z_p}[\mathbf{x}]$ and $\exists\ \alpha_1 \in \mathbf{Z_p}$ such that,

$$|f(\alpha_1)| < |f'(\alpha_1)|^2$$

then $\exists$ a unique $\alpha \in \mathbf{Z_p}$ such that $f(\alpha) = 0$.
I will give the outlines for this proof,

Proof. we will use the iteration,

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

For $n = 1$ take $b_1 = -\frac{f(\alpha_1)}{f'(\alpha_1)}$
Since,

$$|b_1| = \frac{|f(\alpha_1)|}{|f'(\alpha_1|} < |f'(\alpha_1)| \leq 1$$

$$\therefore b_1 \in \mathbf{Z_p}$$

Now, using Taylor expansion,$\exists\ m \in \mathbf{Z_p}$ such that,

$$f(\alpha_1 + b_1) = f(\alpha_1) + f'(\alpha_1)b_1 + mb_1^2$$

but our b_1 gives ,

$$f(\alpha_1) + b_1 f'(\alpha) = 0$$

$$\therefore |f(\alpha_1 + b_1) \leq |b_1|^2 < |f(\alpha_1)|$$

and,

$$|f'(\alpha_1 + b_1) - f'(\alpha_1)| \leq b_1 < |f'(\alpha_1)|$$

using ultrametric inequality,

$$|f'(\alpha_1 + b_1)| = |f'(\alpha_1)|$$

Now, set

$$\alpha_2 = \alpha_1 + b_1 = \alpha_1 - \frac{f(\alpha_1)}{f'(\alpha_1}$$

$$\implies f(\alpha_2) < f(\alpha_1)$$

but,

$$|f'(\alpha_2)| = |f(\alpha_1)|$$

$\implies f(\alpha_n)$ going to smaller, but $f'(\alpha_n)$ will remain unchanged.

$$\implies |\alpha - \alpha_1| \leq \frac{f(\alpha)}{f'(\alpha_1)}$$

This α will be the unique root of $f(x)$ satisfying those conditions. □

Example: let,

$$f(x) = x^2 - 17$$

see,

$$f(1) \equiv 0(mod\ 2)$$

$$f'(x) = 2x(mod\ 2)$$

$$\implies f'(x) = 0(mod\ 2)$$

So, here we can't use Hensel's lemma,
If we choose $\alpha_1 = 1$ then,

$$|f(\alpha_1)| = 2^{-4}, |f'(\alpha_1)| = 2^{-1}$$

$$\implies |f(\alpha_1)| \leq |f'(\alpha_1)|^2$$

Now, we can use the advanced version of Hensel's lemma,
and say $x^2 - 17 = 0$ has a root in $\mathbf{Q_2}$.

Polynomial version of Hensel's Lemma:
If for a polynomial $F(x) \in \mathbf{Z_p}[x]$ there exists two polynomials $G_1[x]$ and $H_1[x]$ coeffiecients from $\mathbf{Z_p}[x]$ such that,

i) $G_1(x)$ is a monic polynomial.
ii)$G_1(x)$ and $H_1(x)$ are relatively prime modulo p.
iii) $F_1(x) \equiv G_1(x).H_1(x)$ $(mod\ p)$.
Then, there must exist two polynomials $G(x), H(x) \in \mathbf{Z_p}[\mathbf{x}]$ such that,
i) $G(x)$ is a monic polynomial.
ii)$G(x) \equiv G_1(x)(mod\ p)$ and $H(x) \equiv H_1 \equiv (x)(mod\ p)$
iii)$F(x) = G(x)H(x)$

3.1 Application of Hensel's Lemma

In this section, we try to find roots of unity and square elements in $\mathbf{Q_p}$.

Theorem 7. *For a prime p and a number r such that $p \not| r$, then there exists an integer α such that $\alpha^r \equiv 1(mod\ p)$ but $\alpha \not\equiv 1(mod\ p)$ iff $(r, p-1) > 1$ and also for every such α the least positive integer r such that $\alpha^k \equiv 1$ must divide $p-1$.*

Proof. Let, there exist a α such that,

$$\alpha^r \equiv 1(mod\ p)$$

then the image of α in $\frac{Z}{pZ}$ is an element with order dividing r in the cyclic group $(\frac{\mathbf{Z}}{p\mathbf{Z}})^*$ of order p-1.

$$\implies g.c.d(r, p-1) \neq 1$$

unless $\alpha \equiv 1(modp)$.
Further, the least k with this property must divide the g.c.d., which means $p-1$
for converse part, in a cyclic group of order $p-1$, if $m|p-1$ and a generator x , then $x^{\frac{p-1}{m}}$ is of order m,The set of elements of order m is a cyclic group generated by $x^{\frac{p-1}{m}}$.

□

Lemma: For a prime p and a positive inte.g.,er m not divisible by p,there exists m-th root of unity in $\mathbf{Q_p}$ iff m divides $p-1$.

Proof. Now using previous lemma, for each m dividing $p-1$ we can find m incongruent roots of

$$x^m - 1 \equiv 0(mod\ p)$$

and then Hensel's lemma gives $\exists m$ different roots of $x^m - 1$, which are mth roots of unity.
The only part is that remaining there are no other roots of unity,

claim:if $\gamma^k \equiv 1$ and $p \not| k$
then $\gamma^m \equiv 1$ for some $m|p-1$
Suppose,

$$\gamma^k = 1$$

$$\implies \gamma^k \equiv 1(mod\ p)$$

where $p \not| k$
Then, by theorem 6, there is a $m|p-1$ such that,

$$\gamma^m \equiv 1(mod\ p)$$

by Hensel's Lemma,
There is a unique γ_1 such that,

$$\gamma_1 \equiv \gamma(mod\ p)$$

and,

$$\gamma_1 = 1$$

but since $m|k$

$$\implies \gamma_1 \text{ is a root of } x^k - 1 \text{ as well}$$

.
and its congruent mod p to γ then by the uniqueness of Hensel's lemma forces, $\gamma_1 = \gamma$.
□

4 Local and Global principal

Theorem 8. *A rational number $m \in \mathbb{Q}$ is a square in $\mathbb{Q}$ iff it is a square element in all $\mathbf{Q_p}$. where $p \leq \infty$*

Proof. We know, for a rational number $m \in \mathbb{Q}$,

$$m = \pm \prod_{p<\infty} p^{v_{p(m)}}$$

if it is square in $\mathbb{Q}$, then , m is positive,

$$m = x^2$$

for a $x \in \mathbb{Q}$
$\implies$ each prime factor has even power.
So , each p-adic valuation will be even.

for converse part,
let m is squared at p, then valuation of m, i.e., $v_p(x)$ is even.
Now if m is square in $\mathbf{Q_p}$ for all primes $p < \infty$, then $v_p(x)$ is even for all p.
Then using prime factorization, this m is square in $\mathbb{Q}$. □

Theorem 9. *The existence or non-existence of (global) solutions of diophantine equations in $\mathbb{Q}$ can be concluded by looking for (local) solutions of that equation in $\mathbf{Q_p}$, for every prime $p \leq \infty$.*

One implication is easy to understand that if solution exists for an equation in $\mathbf{Q}$ then solution exists in $\mathbf{Q_p}$.

But converse is not true, let's see by a counter example,

Counterexample Let,

$$g(x) = (x^2 - 2)(x^2 - 17)(x^2 - 34)$$

then $g(x)$ has roots in $\mathbf{Q_p}$ for all primes p, but does not have any root $\mathbb{Q}$.

Proof. Here, $g(x)$ has solutions in $\mathbf{R}$ but $2, 17, 34$ they are not squares of any rational number, so it does not have any root in $\mathbb{Q}$.
Now, for the solutions in $\mathbf{Q_p}$,

case 1: If $p \neq 2, 17$, then
if $x^2 \equiv 2(mod\ p)$ and $x^2 \equiv 17(mod\ p)$
equations does not have any solution ,then since $(\frac{\mathbf{Z}}{p\mathbf{Z}})^*$ is cyclic group of order $p-1$,
Then an element $x \in (\frac{\mathbf{Z}}{p\mathbf{Z}})^*$ will be a square element if it is an even power of a generator of $(\frac{\mathbf{Z}}{p\mathbf{Z}})^*$.
This implies, $2, 17$ are the elements equal to odd power of a generator of the group,
The product of two odd power elements will be even power element,
$\implies$ product of $2, 17$, i.e., 34 is a square element of $(\frac{\mathbf{Z}}{p\mathbf{Z}})^*$
$\implies$ $x^2 \equiv 34$ has a root in $(\frac{\mathbf{Z}}{p\mathbf{Z}})$,
Now, by Hensel's lemma, it has a root in $\mathbf{Q_p}$.

case 2 for $p = 17$
$f(x) = x^2 = 2$ has a root in $\mathbf{Q_{17}}$

$$6^2 \equiv 0(mod\ 17)$$

$$\implies f(x) \equiv 0(mod\ 17)$$

and

$$f'(6) \equiv 12(mod\ 17)$$

$$f'(x) \not\equiv 0(mod\ 17)$$

$\therefore$ by Hensel Lemma, f(x) has a root in $\mathbf{Q_{17}}$.
case 3: If $p = 2$
then,

$$x^2 \equiv 17(mod\ 2)$$

has a root in $\mathbf{Q_2}$
For $p = \infty$ it has six distinct roots.
Therefore, $g(x)$ has roots in $\mathbf{Q_p}$ for all p. □

To solve this problem, Mathematicians Hasse and Minkowski give a result for which polynomials this principal successfully holds.

Theorem 10. ***The Hasse-Minkowski Theorem:***
Let, $h(x_1, x_2, ...x_n)$ *be a homogeneous polynomial of degree 2 in* $\mathbb{Q}[x_1, x_2, ...x_n]$ *, then*

$$h(x_1, x_2, ...x_n) = 0$$

has non-trivial solutions in $\mathbb{Q}$ *if and only if it has non-trivial solutions in* $\mathbf{Q_p}$ *for every* $p \leq \infty$*.*

5 Power series in p-adic numbers

In this section we are going to knowregion of convergence of power series in $\mathbf{Q_p}$ and also defines range and domains for logarithmic and exponential functions by using power series in $\mathbf{Q_p}$.
Similar to real analysis, for finding a radius of convergence, I am giving a proposition in below.

Proposition 1. *[GG97] Suppose,*
$g(x) = \sum_{n=0}^{\infty} b_n x^n$ *and define,*

$$r = \frac{1}{\lim\limits_{n\to\infty} sup(|b_n|)^{\frac{1}{n}}}$$

then we have followings,
i) If $r = 0$ *then* $g(x)$ *will converge only when* $x = 0$*.*
ii) If $r = \infty$ *then,* $g(x)$ *will converge for all* $x \in \mathbf{Q_p}$*.*
iii) If $0 < r < \infty$ *and* $\lim\limits_{n\to\infty} |b_n| r^n = 0$ *for this* $g(x)$ *will converge iff* $|x| \leq r$*.*
iv) If $0 < r < \infty$ *and* $\lim\limits_{n\to\infty} |b_n| r^n \neq 0$ *for this* $g(x)$ *will converges iff* $|x| < r$*.*

Now, using this proposition, let's define Logarithmic and exponential functions.

5.1 Logarithm Function

Let's start with our usual power series of the logarithm function.
Let,

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

where, $x \in \mathbf{Q_p}$
So, here

$$b_m = \frac{(-1)^m}{m}$$

$$|b_m|^{\frac{1}{m}} = |\frac{(-1)^m}{m}| = p^{\frac{v_p(m)}{m}}$$

Now, $v_p(m)$ is the largest n for which $p^n | m$.

$$\therefore n = v_p(m) \leq \frac{log(m)}{logp}$$

$$\implies \frac{v_p(m)}{m} \leq \frac{log(m)}{mlogp} \longrightarrow 0 \text{ as } n \longrightarrow \infty$$

Hence,

$$|b_m|^{\frac{1}{m}} \longrightarrow 1 \text{ as } m \longrightarrow \infty$$

$\therefore$ In this case, $r = 1$.
Now , let's see what happens at $|x| = 1$

$$|b_m|r^m = |\frac{1}{m}|.1^m = |\frac{1}{m}| \not\longrightarrow 0$$

Since, for any nonzero m, when p does not divide m ,it will be equal to 1.
Now, using the previous proposition ,
The series

$$g(x) = x - \frac{x^2}{2} + \frac{x^3}{3} + ...$$

converges only for $|x| < 1$.

Definition 1. *Let $U_1 = x \in \mathbf{Z_p} : |x - 1| < 1$. For this domain, we can define p-adic logarithm by,*

$$log_p(x) = log(1 + (x - 1)) = \sum_{m=1}^{\infty} (-1)^{m+1} \frac{(x-1)^m}{m}$$

for all $x \in U_1$.

We can check that , This p-adic logarithm satisfies functional equations,
i.e., for $m, n \in U_1$,

$$log_p(m.n) = log_p(m) + log_p(n)$$

.

5.2 Exponential Function

First, we will find the radius of convergence of the function,

$$h(x) = \sum_{m=0}^{\infty} \frac{x^m}{m!}$$

where $x \in \mathbf{Q_p}$.
for this, lets prove a lemma,
Lemma
For a prime number p,

$$v_p(m!) = \sum_{m=1}^{\infty} \lfloor \frac{m}{p!} \rfloor < \frac{m}{p-1}$$

Where $\lfloor . \rfloor$ is called greatest integer function.

Proof.

$$m! = m.(m-1)...1$$

Number of elements that are multiples of p(i.e.,, p,2p,3p,... $= \lfloor \frac{m}{p} \rfloor$
similarly,

Number of elements which are multiple of $p^2(i.e.,,p^2,2p^2,3p^2,...) = \lfloor \frac{m}{p^2} \rfloor$
continuing this,
We get, Number of elements which are multiples of $p^i(i.e.,,p^i,2p^i,3p^i,...) = \lfloor \frac{m}{p^i} \rfloor$

$$\therefore v_p(m!) = \sum_{m=1}^{\infty} \lfloor \frac{m}{p!} \rfloor$$

Now, we know ,

$$\lfloor x \rfloor \leq x$$

$$\implies \sum_{m=1}^{\infty} \lfloor \frac{m}{p!} \rfloor \leq \sum_{m=1}^{\infty} \frac{m}{p!} = \frac{m}{p-1}$$

□

Radius of convergence for h(x)
Now, for the function $h(x)$ (defined above),

$$|b_m| = |\frac{1}{m!}| = p^{v_p(m!)} < p^{\frac{m}{p-1}}$$

$$r = \frac{1}{\lim\limits_{n\to\infty} sup(|b_n|)^{\frac{1}{n}}} \leq \frac{1}{\frac{1}{p-1}}$$

$$\implies r \geq \frac{-1}{p-1}$$

Therefore the series converges for $|x| < p^{\frac{-1}{p-1}}$.
Now, for $|x| = p^{\frac{-1}{p-1}}$.
assume $m = p^n$ for a $n \in \mathbf{Z}$

$$v_p(m!) = v_p(p^n!) = 1 + p + p^2 + ... + p^{n-1} = \frac{p^n - 1}{p-1}$$

As $v_p(x) = \frac{1}{p-1}$

$$\implies v_p(\frac{x^m}{m!}) = v_p(\frac{x^{p^m}}{p^m!}) = p^m v_p(x) - v_p(p^m!) = p^m.\frac{1}{p-1} - \frac{p^m - 1}{p-1} = \frac{1}{p-1}$$

which does not depend on n,

$$\therefore \frac{x^m}{m!} \not\longrightarrow 0 \text{ as} m \longrightarrow \infty$$

Hence, $h(x)$ does not converge for $|x| = p^{\frac{-1}{p-1}}$.
Since,region of convergence is always a disk, $h(x)$ does not converge out side of disk $|x| < p^{\frac{-1}{p-1}}$.

Definition 2. *Let,* $B = \{x \in \mathbf{Z_p} : |x| < p^{\frac{-1}{p-1}}\}$ *in this domain , we can defined p-adic exponential function by* $exp_p : B \longmapsto \mathbf{Q_P}$ *by,*

$$exp_p(x) = \sum_{m=0}^{\infty} \frac{x^m}{m!}$$

Relation between p-adic Logarithm and p-adic Exponential [GG97] For $x \in \mathbf{Z_p}$ such that $|x| < p^{\frac{-1}{p-1}}$ then,

$$|exp_p(x) - 1| < 1$$

so, range of $exp_p(x)$ sits inside domain of log_p and

$$log_p(exp_p(x)) = x$$

Conversely, for $|x| < p^{\frac{-1}{p-1}}$,

$$|log_p(1 + x)| < p^{\frac{-1}{p-1}}$$

then range of $log_p(x)$ sits inside the domain of exp_p and

$$exp_p(log_p(1 + x) = 1 + x$$

6 Valuation Theory for Field

Earlier, we defined valuation for an arbitrary field $\mathbf{K}$. In this section, we will prove some theorem related to fields with non-archimedean absolute values.In non archimedean absolute value associate valuation is called exponential valuation.

Let's define some important structures,
Let $\mathbf{K}$ be a field with an exponential valuation. Then
The subset,

$$O = \{x \in \mathbf{K} : v(x) \geq 0\}$$

is form a ring and

$$O^* = \{x \in \mathbf{K} : v(x) = 0\}$$

is a group of units of O.
and there exists a unique maximal ideal

$$\gamma = \{x \in \mathbf{K} : v(x) > 0\}$$

Discrete Valuation:
If exponential valuation has a smallest positive value , then it is called Discrete Valuation.
An element $\rho \in O$ is called prime element , if

$$v(\rho) = 1$$

Proposition 2. *[Neu13] For discrete valuation v on $\mathbf{K}$, the ring O is a Principal Ideal Domain. If the smallest positive value of v is 1 then*

$$\gamma^m = \rho^m O = \{x \in \mathbf{K} : v(x) \geq m\}$$

where $m \geq 0$ and ρ is prime element
are nonzero ideals of O.Further,

$$\frac{\gamma^m}{\gamma^{m+1}} \cong \frac{O}{\gamma}$$

Proof. Let, take an ideal $b \neq 0$ of O and a nonzero element x from b with the smallest possible valuation $v(x) = m$.
Then,

$$x = \rho^m.u_1 \text{ where } u_1 \in O^*$$

$$\implies \rho^m \subseteq b$$

Now, choose another arbitrary element $y \neq 0$ from b such that,

$$y = \rho^n.u_2 \text{ where } u_2 \in O^*$$

Since, $n = v(y) \geq m$

$$\implies y = (\rho^{n-m}.u_2).\rho^m \subseteq \rho^m O$$

$$\implies b = \rho^m O$$

For the next part,
Take a map

$$\gamma^m \longmapsto \frac{O}{\gamma}$$

via,

$$a\rho^m \longmapsto a \bmod \gamma$$

Which is a surjective map with kernel ρ^{m+1},
Therefore, the result follows from first isomorphism theorem.

□

For a discrete valued field,we have a filtration of ideals,

$$...\rho^3 \subseteq \rho^2 \subseteq \rho^1 \subseteq O$$

Unit Group:
Define,

$$U^{(m)} = 1 + \gamma^m = \{x \in \mathbf{K}^* : |1 - x| < \frac{1}{q^m - 1}\}$$

Where, $|\cdot| = q^{-v}, q > 1$ and v is the exponential valuation , which admits the lowest value 1.
$U^{(m)}$ is a subgroup of O^*.

Proof. $(1 + \gamma^m)$ is closed under multiplication.
let, $x \in U^m$

$$\therefore |1 - x^{-1}| = |x|^{-1}|x - 1| = |1 - x| < \frac{1}{q^{m-1}}$$

$$\implies x^{-1} \in U^m$$

□

The group $U^{(1)}$ is called the group of principal units.

Theorem 11. $\frac{O^*}{U^{(m)}} \cong (\frac{O}{\gamma^m})^*$ *and* $\frac{U^{(m)}}{U^{(m+1)}} \cong \frac{O}{\gamma}$

Proof. For proving the first isomorphism,
Let's take a map,

$$\phi : O^* \longmapsto (\frac{O}{\gamma^m})^*$$

$$u \longmapsto u \text{ mod} \gamma^m$$

This is a canonical homomorphism. Which is obviously surjective.

claim: $ker\phi = U^{(m)}$
One sided containment is easy, i.e.,

$$1 + \gamma^m \in ker\phi$$

$$\implies U^{(m)} \subseteq ker\phi$$

On the other side,
let, $U \in ker\phi$

$$\therefore U \text{ mod } \gamma^m = 1 \text{ mod } \gamma^m$$

$$\implies U = 1 + \gamma^m$$

$$\implies ker\phi \subseteq U^{(m)}$$

$$\therefore ker\phi = U^{(m)}$$

Hence, $\frac{O^*}{U^{(m)}} \cong (\frac{O}{\gamma^m})^*$

For the 2nd isomorphism,
Take the surjective homomorphism,

$$\phi_1 : U^{(m)} \longmapsto \frac{O}{\gamma}$$

defined by

$$1 + \rho^m a \longmapsto a \text{ mod } \gamma$$

By similar way we can prove $ker\phi_1 = U^{m+1}$
Then by Isomorphism Theorem,

$$\frac{U^{(m)}}{U^{(m+1)}} \cong \frac{O}{\gamma}$$

□

Ostrowski's Theorem for Complete Field:[Neu13]
Let, $\mathbf{k}$ be a complete field with an archimedean valuation $|\cdot|$. Then there exists an isomorphism ϕ from $\mathbf{k}$ to $\mathbf{R}$ or $\mathbf{C}$ satisfying

$$|a| = |\phi a|^s$$

where $s \in (0, 1]$ is a fixed number.

6.1 Extension of valuation

In this section we will see , for an algebraic extension, how a valuation from the base field can be extended to the above field.

Lemma 11.1. *Suppose* $\mathbf{K}$ *is a complete field with respect to non-archimedean valuation* $|\cdot|$.
Let $g(x) = b_0 + b_1x + ... + b_nx^n \in \mathbf{K}[\mathbf{x}]$ *be a irreducible polynomial of degree n, such that* $b_0.b_n \neq 0$ *Then,*

$$|g| = \ max\ \{|b_0|, |b_n|\}$$

When, $b_n = 1$ *and* $b_0 \in O$ *then* $g \in O[x]$.

Theorem 12. *Suppose* $\mathbf{K}$ *be a complete field with respect to an archimedean valuation* $|\cdot|$. *Let* $\mathbf{M}|\mathbf{K}$ *be a finite degree algebraic extension . Then we can extend the valuation* $|\cdot|$ *uniquely to* $\mathbf{L}$ *by,*

$$|\alpha| = \sqrt[n]{|N_{\mathbf{M}|\mathbf{K}}(\alpha)|}$$

Where,$[\mathbf{L} : \mathbf{K}] = n$

Proof. If $|\cdot|$ is archimedean valuation, then from Ostrowski's theorem we can say, $\mathbf{K} = \mathbf{R}$ or $\mathbf{C}$
Then,

$$\sqrt[2]{|N_{\mathbf{C}|\mathbf{R}}(z)|} = \sqrt[2]{z.\bar{z}} = \sqrt[2]{|z|^2} = |z|$$

so, valuation is the same.
Now, if $|\cdot|$ is non archimedean.
Existence of Extended Valuation: Let ,
O = The valuation ring of $\mathbf{K}$ and
O_M = integralclosure of O in $\mathbf{M}$.
Then,$(*)$

$$O_M = \{\alpha \in \mathbf{M} : N_{\mathbf{M}|\mathbf{K}}(\alpha) \in \mathbf{O}\}$$

If $\alpha \in O_M \implies N_{\mathbf{M}|\mathbf{K}}(\alpha) \in O$ this part is evident.
for converse part,
let $\alpha \in \mathbf{L}^*$ and $N_{\mathbf{M}|\mathbf{K}}(\alpha) \in O$
Let, $g(x)$ be the minimal polynomial of α over $\mathbf{K}$ such that'

$$g(x) = x^m + a_{m-1}x^{m-1} + ... + a_0 \in \mathbf{K}[x]$$

Then,

$$N_{\mathbf{M}|\mathbf{K}}(\alpha) \in O = \pm a_0^m \in O$$

$$\implies |a_0^m| \leq 1$$

$$\implies |a_0| \leq 1 \implies a_0 \in O$$

Then, by Lemma10.1, $g(x) \in O[x] \implies \alpha \in O_M$

Now, the function $|\alpha| = \sqrt[n]{|N_{\mathbf{M}|\mathbf{K}}(\alpha)|}$ satisfies definiteness and multiplicativity trivially, for strong inequality,

$$|\alpha + \beta| \leq \max\{|\alpha|, |\beta|\}$$

dividing by β it reduces to

$$|\alpha| \leq 1 \implies |\alpha + 1| \leq 1$$

then, by $(*)$ If

$$\alpha \in O_M \implies \alpha \in O_{M+1}$$

Thus, the function $|\alpha| = \sqrt[n]{|N_{\mathbf{M}|\mathbf{K}}(\alpha)|}$ defines a valuation of $\mathbf{M}$ whose restriction to $\mathbf{K}$ gives the valuation of $\mathbf{K}$ and O_M is the valuation ring of $\mathbf{L}$.

Uniqueness Let, there exist another extension $|\cdot|'$ with valuation O'_M.
Suppose $\Gamma,$ and Γ' are the maximal ideals of O_M and O'_M respectively.

Let, $\alpha \in O_M$ but $\alpha \notin O'_M$ and

$$g(x) = x^m + a_{m-1}x^{m-1} + ... + a_0$$

be the minimal polynomial of α over $\mathbf{K}$.
Then, $, a_0 a_1, a_2, ...a_n \in O$ and $\alpha^{-1}\Gamma'$

$$1 = -a_{m-1}\alpha^{-1} - ... - a_0(\alpha^{-1})^m \in \Gamma'$$

which contradicts the maximality of Γ'.
It implies $O_M \subseteq O'_M$

$$\therefore |\alpha| \leq 1 \implies |\alpha|' \leq 1$$

It means the valuations $|\cdot|$ and $|\cdot|'$ are equivalent.
Since when we restrict them on $\mathbf{K}$, they will give same value so $|.|$ and $|\cdot|'$ are equal valuation.

□

Remark: In this case, $\mathbf{M}$ will be a complete field.

6.2 Local fields

Definition 3. *A field* $\mathbf{K}$ *is called local field if it is complete with respect to discrete valuation and its residue field is finite.*

Proposition 3. *A local field is locally compact and its valuation ring is compact.*

Remark: A local field is finite extensions of $\mathbf{Q_p}$ and $\mathbf{F_p}((t))$.
Decomposition of $\mathbf{K}^*$:
For a local field $\mathbf{K}$, its multiplicative group is decomposed as,

$$\mathbf{K}^* = (\rho) \times \mu_{q-1} \times U^{(1)}$$

.
Where, ρ is defined as prime element, $(\rho) = \{\rho^k : k \in \mathbf{Z}\}$, q is the cardinality of the residue field and $U^{(1)}$ is the group of principal units.

References

[Con15] Keith Conrad. Hensel's lemma. *Unpublished notes. Available athttps://kconrad. math. uconn. edu/blurbs/gradnumthy/hensel. pdf*, 2015.

[GG97] Fernando Q Gouvêa and Fernando Q Gouvêa. *p-adic Numbers*. Springer, 1997.

[Neu13] Jürgen Neukirch. *Algebraic number theory*, volume 322. Springer Science & Business Media, 2013.

Acknowledgement

I would like to extend my heartfelt gratitude to my thesis supervisor, Dr.Chandrasheel Bhagwat. His guidance and Encouragement helped me to stay on this project and Thank you for patiently clearifying my doubts.